ESAME DI ALGEBRA 3, 22/02/2017

COGNOME e Nome .....

MATRICOLA .....

Esercizio 1. Sia K il campo di spezzamento di $(X^7-11)(X^2+7) \in \mathbb{Q}[X]$.

i. Mostrare che $\mathbb{Q} \subset K$ è una estensione finita di Galois. Determinarne il grado.
ii. Sia G il gruppo di Galois dell'estensione $\mathbb{Q} \subset K$. Descrivere il gruppo G.
iii. Trovare tutti i sottocampi aventi grado 3 su $\mathbb{Q}$ e per ciascuno di essi esibire un generatore come estensione su $\mathbb{Q}$.
iv. Provare che la seguente affermazione è falsa: Esistono *contemporaneamente* un *unico* sottocampo di grado 14 e un *unico* sottocampo di grado 21 dentro K.

Soluzione: i) Siccome $\mathbb{Q}$ è un campo di caratteristica 0, è perfetto, e quindi $(X^7-11)(X^2+7)$ è un polinomio separabile, e dunque $\mathbb{Q} \subseteq K$ è un'estensione finita di Galois. Notiamo che le radici del polinomio $f(X) = (X^7-11))$ sono $R_f = \{\sqrt[7]{11}\zeta_7^j\}_{j=0}^6$, dove ζ_7 è una radice primitiva settima dell'unità e che le radici di $g(X) := X^2+7$ sono $R_g = \{\pm\sqrt{-7}\}$. In particolare, il campo di spezzamento di f è $L = \mathbb{Q}(\zeta_7, \sqrt[7]{11}) = \mathbb{Q}(\zeta_7)\mathbb{Q}(\sqrt[7]{11})$, poichè $L \subseteq \mathbb{Q}(\zeta_7, \sqrt[7]{11})$, dato che $\mathbb{Q}(\zeta_7, \sqrt[7]{11})$ contiene tutte le radici di $f(X)$, e $\mathbb{Q}(\zeta_7, \sqrt[7]{11}) \subseteq L$ dato che $\zeta_7 = \frac{\zeta_7\sqrt[7]{11}}{\sqrt[7]{11}}$. Notiamo che L contiene il settimo campo ciclotomico e, dalla teoria dei campi ciclotomici, sappiamo che ogni campo ciclotomico primo contiene un campo quadratico. Poichè $-7 \equiv 1$ modulo 4, sappiamo che questo campo quadratico coincide con $\mathbb{Q}(\sqrt{-7})$, e quindi $L = K$. Sappiamo anche che $[\mathbb{Q}(\zeta_7) : \mathbb{Q}] = \phi(7) = 6$ e, dato che (X^7-11) è irriducibile per il criterio di Eisenstein applicato al primo $p = 11$, concludiamo che $[\mathbb{Q}(\sqrt[7]{11}) : \mathbb{Q}] = 2$. Infine, per moltiplicatività dei gradi, sappiamo che il grado di $\mathbb{Q}(\zeta_7) \cap \mathbb{Q}(\sqrt[7]{11})$ divide sia 6 che 2, quindi o l'intersezione è ridotta al solo $\mathbb{Q}$, oppure ha grado 2 su $\mathbb{Q}$ e in tal caso deve coincidere con $\mathbb{Q}(\sqrt[7]{11})$. D'altra parte sappiamo che i campi ciclotomici primi contengono una sola estensione quadratica, che in tal caso, per quanto detto, non coincide con $\mathbb{Q}(\sqrt[7]{11})$, dunque l'intersezione è ridotta a $\mathbb{Q}$ e, per moltiplicatività dei gradi, concludiamo allora che $[K : \mathbb{Q}] = 42$.

ii) Poichè l'estensione $\mathbb{Q}(\zeta_7)/\mathbb{Q}$ è di Galois, la mappa di restrizione $\sigma \mapsto \sigma_{|\mathbb{Q}(\zeta)}$ induce un isomorfismo di gruppi

$$\mathrm{Gal}\left(K/\mathbb{Q}(\sqrt[7]{11})\right) \cong \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$$

Per la teoria delle estensioni ciclotomiche, sappiamo che

$$\mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q}) \cong \left(\frac{\mathbb{Z}}{7\mathbb{Z}}\right)^\times \cong \frac{\mathbb{Z}}{6\mathbb{Z}}.$$

Poichè la classe [2] genera $\left(\frac{\mathbb{Z}}{7\mathbb{Z}}\right)^\times$, esiste uno e un solo $\sigma \in \mathrm{Gal}\left(\mathbb{Q}(\zeta_7)/\mathbb{Q}\right)$ tale che $\sigma(\zeta_7) = \zeta_7^2$ e $\sigma(\sqrt[7]{11}) = \sqrt[7]{11}$. Tale elemento ha ordine 6 e genera il sottogruppo $H := \mathrm{Gal}\left(K/\mathbb{Q}(\sqrt[7]{11})\right)$ di $\mathrm{Gal}(K/\mathbb{Q})$. Inoltre, poichè $\mu_7 \subseteq \mathbb{Q}(\zeta_7)$, dalla teoria delle estensioni cicliche, possiamo concludere che

$$\mathrm{Gal}(K/\mathbb{Q}(\zeta_7)) \cong \mu_7$$

mediante la mappa $g \mapsto \frac{g(\sqrt[7]{11})}{\sqrt[7]{11}}$. Dunque esiste uno e un solo elemento $\tau \in \mathrm{Gal}(K/\mathbb{Q}(\zeta)_7)$ per cui $\tau(\sqrt[7]{11}) = \zeta_7\sqrt[7]{11}$ e $\tau(\zeta_7) = \zeta_7$. Tale elemento ha ordine 7 e genera il sottogruppo $N := \mathrm{Gal}(K/\mathbb{Q}(\zeta_7))$ di G. Siccome poi l'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_7)$ è normale, per la Teoria di Galois, possiamo concludere che tale sottogruppo e normale e pertanto N e H soddisfano le proprietà definitorie di una struttura di prodotto semidiretto. Infine, l'ordine di HN è 42, esattamente l'ordine di G e quindi G è prodotto

semidiretto di H ed N. Pertanto ogni elemento di G si scrive come $\tau^i\sigma^j$, con $0 \leq i \leq 6$ e $0 \leq j \leq 5$ unici. Notiamo che vale:

$$\sigma^j\tau^i\sigma^{-j}(\sqrt[7]{11}) = \sigma^j\left(\zeta_7^i\sqrt[7]{11}\right) = \zeta_7^{2^j i}\sqrt[7]{11}$$

da cui deduciamo che la legge di composizione è data da $\sigma^j\tau^i\sigma^{-j} = \tau^{2^j i}$.

iii) Per la teoria di Galois, sappiamo che i sottocampi di K aventi grado 3 su $\mathbb{Q}$ sono in corrispondenza biunivoca con i sottogruppi di indice 3, ovvero di ordine 14 di G. Sia M un tale sottogruppo di G. Allora per il Teorema di Sylow, M deve contenere un sottogruppo di ordine 7. Poichè la massima potenza di 7 che divide l'ordine di G è 7 stesso, tale 7-Sylow di M deve essere anche un 7-Sylow di G, ma sappiamo che in G c'è un unico 7-Sylow normale, che è il sottogruppo N del punto precedente. Ne consegue che $N \leq M$. Ma allora, dato che la biiezione nel Teorema Fondamentale della Teoria di Galois inverte le inclusioni, concludiamo che un'estensione di grado 3 su $\mathbb{Q}$ contenuta in K deve essere contenuta nel campo ciclotomico $\mathbb{Q}(\zeta_7)$. Poichè infine il gruppo di Galois di $\mathbb{Q}(\zeta_7)$ su $\mathbb{Q}$ è ciclico di ordine 6, concludiamo che esso possiede un solo sottogruppo di ordine 2, corrispondente pertanto ad un'unica estensione di grado 3 su $\mathbb{Q}$, quindi K contiene un solo sottocampo di grado 3 su $\mathbb{Q}$. Un generatore per questa estensione è $\alpha := \zeta_7 + \zeta_7^6$. Infatti, detto $\rho : \zeta_7 \mapsto \zeta_7^2$ il generatore di $\mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q})$, la sottoestensione di grado 3 corrisponde al sottocampo di $\mathbb{Q}(\zeta_7)$ fissato da ρ^3, e notiamo che

$$\rho^3(\alpha) = \zeta_7 + \zeta_7^6$$

iv) Supponiamo per assurdo che esistano contemporaneamente una sola estensione di grado 14 e una sola estensione di grado 21 su $\mathbb{Q}$ contenute in K. Allora, per il Teorema Fondamentale della Teoria di Galois, queste estensioni corrispondono rispettivamente ad un sottogruppo di ordine 3 e ad un sottogruppo di ordine 2 in G. Inoltre, tali sottogruppi devono essere unici poichè uniche sono le estensioni corrispondenti e la mappa data dal Teorema Fondamentale è una biiezione. Poichè G ha ordine 42, e già sappiamo che esiste un unico 7-Sylow normale, la considerazione precedente ci permette di affermare che anche i 2 e i 3-Sylow sono unici, e in particolare sono normali. Chiamiamo P_2 (rispettivamente P_3) questo unico 2 (rispettivamente 3)-Sylow di G. Notiamo che, per normalità, il sottoinsieme dato dal prodotto P_2P_3 è un sottogruppo di G e inoltre è normale. Inoltre, per il Teorema di Lagrange, P_2 e P_3 hanno intersezione banale e quindi il prodotto P_2P_3 dentro a G è per definizione un prodotto diretto di ordine 6. Facendo la stessa considerazione si conclude che anche il prodotto $(P_2 \times P_3)N$, dove N era il 7-Sylow, è un prodotto diretto contenuto in G. Ma siccome l'ordine di questo prodotto diretto è 42, deve essere che tale prodotto diretto coincide con tutto G. Infine, poichè tutti i Sylow che compaiono sono ciclici, possiamo concludere che G è addirittura ciclico, assurdo poichè ad esempio K contiene l'estensione $\mathbb{Q}(\sqrt[7]{11})/\mathbb{Q}$ che non è normale.

Esercizio 2. Sia K il campo di spezzamento di $X^4 - 8X^2 + 15 \in \mathbb{Q}[X]$ ed $L = \mathbb{Q}\left(\sqrt{7}\right)$.

i. Descrivere il campo composto $M := KL$, esibendone una $\mathbb{Q}$-base e calcolarne il grado.
ii. Calcolare il reticolo dei sottocampi di M.
iii. Descrivere l'anello degli interi di K esibendone una $\mathbb{Z}$-base e calcolare $\mathrm{disc}_{K/\mathbb{Q}}$.

Soluzione: i) Il polinomio $f(X) = X^4 - 8X^2 + 15$ ammette come soluzioni $\mathcal{R}_f = \{\pm\sqrt{5}, \pm\sqrt{3}\}$. Pertanto, $K = \mathbb{Q}(\sqrt{5}, \sqrt{3})$ ha grado 4 su $\mathbb{Q}$ e gruppo di Galois $H \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}}$, generato dagli automorfismi $\sigma : \begin{bmatrix} \sqrt{5} \mapsto -\sqrt{5} \\ \sqrt{3} \mapsto \sqrt{3} \end{bmatrix}$ e $\tau : \begin{bmatrix} \sqrt{5} \mapsto \sqrt{5} \\ \sqrt{3} \mapsto -\sqrt{3} \end{bmatrix}$(vedere primo punto dell'esercizio 1 per un'argomentazione più dettagliata). Inoltre l'intersezione $K \cap L$ dentro K è ridotta al solo $\mathbb{Q}$. Infatti, se fosse diversa da $\mathbb{Q}$ dovrebbe essere un'estensione di grado 2 su $\mathbb{Q}$, e quindi dovrebbe contenere L, che si vede però non essere contenuto in K. Dunque, per moltiplicatività dei gradi, possiamo concludere che $[M : \mathbb{Q}] = 8$ e che

$$G := \mathrm{Gal}(M/\mathbb{Q}) = \langle \sigma, \tau, \rho \rangle \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}}$$

dove $\rho : \begin{bmatrix} \sqrt{7} \mapsto -\sqrt{7} \\ \sqrt{3} \mapsto \sqrt{3} \\ \sqrt{5} \mapsto \sqrt{5} \end{bmatrix}$. Notiamo il piccolo abuso di notazione, dato che per σ e τ si intendono i corrispondenti automorfismi che si comportano come sopra e in più fissano $\sqrt{7}$. Poichè sappiamo che il grado di M su $\mathbb{Q}$ è 8, possiamo facilmente concludere che una $\mathbb{Q}$-base di K è data da $\{1, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{15}, \sqrt{21}, \sqrt{35}, \sqrt{105}\}$.

ii) Per il Teorema Fondamentale della Teoria di Galois, calcolare il reticolo dei sottocampi di K corrisponde a calcolare il reticolo dei sottogruppi di G. Notiamo che G ammette se stesso come unico sottogruppo di ordine 8 e l'unità come unico sottogruppo di ordine 1. Per il resto ammette sottogruppi ciclici di ordine 2 e sottogruppi di ordine 4 che possono essere solamente isomorfi al gruppo di Klein. Calcoliamo pertanto i sottogruppi del gruppo astratto $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^3$. Elenchiamo i suoi elementi in questo modo:

$$\begin{array}{lll} e = (0,0,0) & g = (1,1,1) & \\ a = (1,0,0) & b = (1,1,0) & c = (1,0,1) \\ d = (0,1,0) & f = (0,1,1) & \\ h = (0,0,1) & & \end{array}$$

Tutti questi elementi hanno naturalmente ordine 2, escluso e. Per costruire un sottogruppo di ordine 4 è sufficiente partire da due di questi elementi, diciamo x e y distinti, e costruire $x+y$. Allora, dato che il gruppo è abeliano, anche l'ordine di $x+y$ è 2. Ci sono $\binom{7}{2=21}$ scelte possibili di coppie di elementi di ordine 2, ma è chiaro che per ciascuna tale coppia $\{x, y\}$, anche $\{y, x+y\}$ e $\{x, x+y\}$ determinano lo stesso sottogruppo di ordine 4. Questo ci dice che ci sono $21/3 = 7$ sottogruppi di ordine 4, dati da

$$\begin{array}{lll} \langle a, d\rangle & \langle a, h\rangle & \langle d, c\rangle \\ \langle a, g\rangle & \langle d, h\rangle & \\ \langle b, h\rangle & \langle b, c\rangle & \end{array}$$

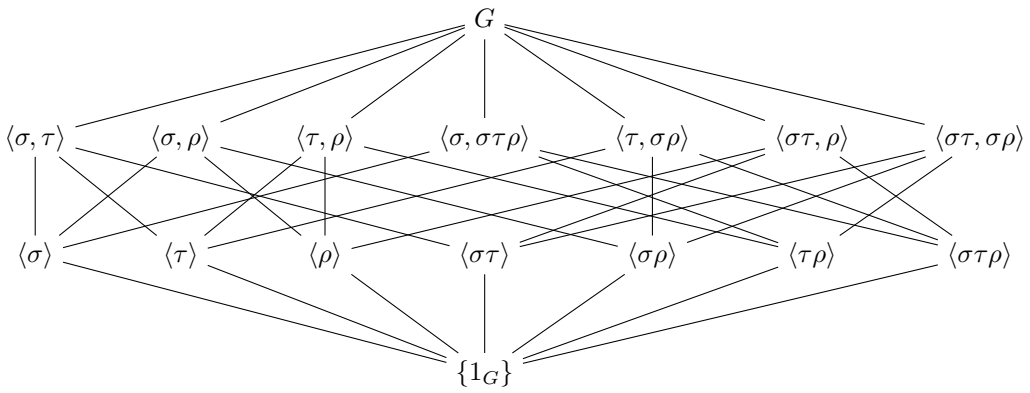
I sottogruppi di ordine 2 sono naturalmente gruppi ciclici e corrispondono dunque a tutti gli elementi di ordine 2 di $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^3$. Seguendo l'elenco precedente, vediamo che ci sono 7 sottogruppi di ordine 2 dati da

$$\begin{array}{lll} \langle a\rangle & \langle b\rangle & \langle c\rangle \\ \langle d\rangle & \langle f\rangle & \\ \langle g\rangle & \langle h\rangle & \end{array}$$

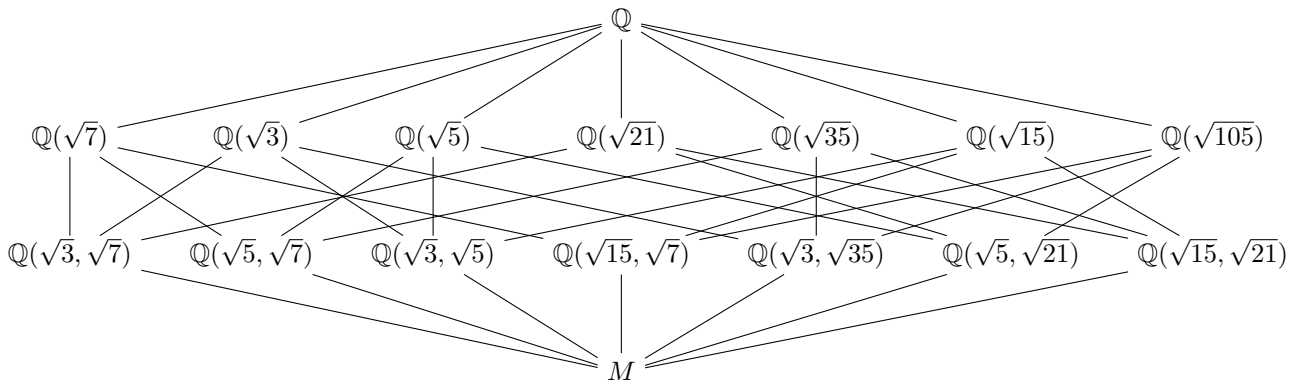
Pertanto, tornando al nostro gruppo G, ed effettuando le identificazioni:

$$\sigma = a \quad \tau = d \quad \rho = h$$

possiamo scrivere il reticolo dei sottogruppi di G come



Mediante il Teorema Fondamentale della Teoria di Galois possiamo allora scrivere il reticolo dei sottocampi corrispondente al precedente reticolo e dato da



iii) Poichè $5 \equiv 1$ modulo 4 e naturalmente 3 è congruo a se stesso modulo 4, sappiamo dalla teoria delle estensioni quadratiche che

$$\mathcal{O}_{\mathbb{Q}(\sqrt{3})} = \mathbb{Z}[\sqrt{3}] \quad \mathcal{O}_{\mathbb{Q}(\sqrt{5})} = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$$

Inoltre sappiamo che i discriminanti valgono rispettivamente:

$$\mathrm{disc}_{\mathbb{Q}(\sqrt{3})/\mathbb{Q}} = 12 \quad \mathrm{disc}_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}} = 5$$

e, dato che i discriminanti sono coprimi, per il Corollario 4.13 delle note, possiamo concludere che una base intera per $\mathcal{O}_K$ è data da

$$\left\{1, \sqrt{3}, \frac{1+\sqrt{5}}{2}, \frac{\sqrt{3}+\sqrt{15}}{2}\right\}$$

Per il calcolo del discriminante si può procedere utilizzando la definizione, o alternativamente ricordando che

$$\mathrm{disc}_{K/\mathbb{Q}} = (\mathrm{disc}_{\mathbb{Q}(\sqrt{3})/\mathbb{Q}})^2(\mathrm{disc}_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}})^2$$

da cui, $\mathrm{disc}_{M/\mathbb{Q}} = 3600$. Volendo invece usare la definizione, e ricordando che il gruppo di Galois di K su $\mathbb{Q}$ è generato dagli automorfismi σ e τ, ci si riduce al calcolo del quadrato del seguente discriminante:

$$\det \begin{pmatrix} 1 & \sqrt{3} & \frac{1+\sqrt{5}}{2} & \frac{\sqrt{3}+\sqrt{15}}{2} \\ 1 & -\sqrt{3} & \frac{1+\sqrt{5}}{2} & \frac{-\sqrt{3}-\sqrt{15}}{2} \\ 1 & \sqrt{3} & \frac{1+-\sqrt{5}}{2} & \frac{\sqrt{3}+-\sqrt{15}}{2} \\ 1 & -\sqrt{3} & \frac{1-\sqrt{5}}{2} & \frac{-\sqrt{3}+\sqrt{15}}{2} \end{pmatrix}$$

Esercizio 3. Sia ζ_6 una radice primitiva sesta dell'unità e sia $\alpha := \zeta_6 + \sqrt{5}$.

i. Determinare il grado su $\mathbb{Q}$ e l'anello degli interi di $K := \mathbb{Q}(\alpha)$.
ii. Calcolare il discriminante di $\mathcal{O}_K$ su $\mathbb{Z}$.
iii. Determinare i primi di $\mathbb{Z}$ che ramificano in $\mathcal{O}_K$.

Soluzione: i) Proviamo che $K/\mathbb{Q} = \mathbb{Q}(\zeta_3)\mathbb{Q}(\sqrt{5})$. Infatti, si ricordi prima di tutto che $\mathbb{Q}(\zeta_6) = \mathbb{Q}(\zeta_3)$, dove un'inclusione è ovvia, dato che $\zeta_6^2 = \zeta_3$ e l'altra consegue dal fatto che entrambe le estensioni hanno grado 2 su $\mathbb{Q}$. Ma questo implica l'inclusione $K \subseteq \mathbb{Q}(\zeta_6)\mathbb{Q}(\sqrt{5}) = \mathbb{Q}(\zeta_3)\mathbb{Q}(\sqrt{5})$. Per l'altra inclusione, notiamo che $[\mathbb{Q}(\zeta_3)\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 4$, esattamente usando lo stesso argomento dell'esercizio precedente, e che $\mathrm{Gal}(\mathbb{Q}(\zeta_3)\mathbb{Q}(\sqrt{5})/\mathbb{Q}) \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}}$, generato da σ che coniuga ζ_3 e fissa $\sqrt{5}$ e da τ che

fissa ζ_3 e manda $\sqrt{5}$ in $-\sqrt{5}$. Ma allora notiamo che si ha

$$(\sigma,1)(\zeta_6+\sqrt{5}) = -\zeta_6+\sqrt{5}$$
$$(1,\tau)(\zeta_6+\sqrt{5}) = \zeta_6-\sqrt{5}$$
$$(\sigma,\tau)(\zeta_6+\sqrt{5}) = -\zeta_6-\sqrt{5}$$

da cui concludiamo che α è fissato solo dall'identità di $\mathrm{Gal}(\mathbb{Q}(\zeta_3)\mathbb{Q}(\sqrt{5})/\mathbb{Q})$, e quindi l'estensione $\mathbb{Q}(\alpha)$ deve avere grado almeno 4, da cui si ottiene la seconda inclusione.

ii) Dalla teoria delle estensioni ciclotomiche ricaviamo che

$$\mathrm{disc}_{\mathbb{Q}(\zeta_3)/\mathbb{Q}} = -3$$

mentre sappiamo che, dato che $5 \equiv 1$ modulo 4,

$$\mathrm{disc}_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}} = 5$$

Per calcolare il discriminante del composto possiamo procedere come nell'esercizio precedente, ricavando

$$\mathrm{disc}_{\mathbb{Q}(\alpha)/\mathbb{Q}} = 225$$

iii) Poichè gli unici primi che dividono 225 sono 5 e 3, sappiamo dal Teorema 6.10 delle note, che questi sono tutti e soli i primi di $\mathbb{Z}$ che ramificano in $\mathcal{O}_K$.

Esercizio 4. (*TeoGal*)$^{(*)}$ Sia $K \subset L$ una estensione di campi finiti di grado n.

i. Dimostrare che l'estensione $K \subset L$ è di Galois.
ii. Determinare il gruppo di Galois $\mathrm{Gal}(L/K)$.
iii. Determinare il reticolo delle estensioni intermedie $K \subset L$.

Esercizio 5. (*TeoNum*)

Sia ζ_p una radice primitiva p-esima dell'unità con p un primo dispari e sia $K = \mathbb{Q}(\zeta_p)$ il p-esimo campo ciclotomico.

i. Calcolare l'anello degli interi e il discriminante di K illustrando tutti i passaggi.
ii. Mostrare che K contiene un campo quadratico. Esibirne un generatore come estensione di $\mathbb{Q}$.
iii. Cosa si può dire riguardo ai campi quadratici contenuti nell'n-esimo campo ciclotomico nel caso in cui $n = pq$, $p, q \in \mathbb{N}$ primi distinti?

Soluzione: Per i punti *i*) e *ii*) si vedano le note del corso. Per il punto *iii*), iniziamo col caso in cui sia p che q sono dispari. Ricordiamo che

$$\begin{aligned}\mathrm{Gal}(\mathbb{Q}(\zeta_{pq})/\mathbb{Q}) \cong \mathrm{Aut}(\mu_{pq}) &\cong \mathrm{Aut}\left(\frac{\mathbb{Z}}{pq\mathbb{Z}}\right)\\ &\cong \mathrm{Aut}\left(\frac{\mathbb{Z}}{p\mathbb{Z}} \oplus \frac{\mathbb{Z}}{q\mathbb{Z}}\right) \cong \mathrm{Aut}\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right) \times \mathrm{Aut}\left(\frac{\mathbb{Z}}{q\mathbb{Z}}\right)\\ &\cong \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^{\times} \oplus \left(\frac{\mathbb{Z}}{q\mathbb{Z}}\right)^{\times} \cong \frac{\mathbb{Z}}{(p-1)\mathbb{Z}} \oplus \frac{\mathbb{Z}}{(q-1)\mathbb{Z}}\end{aligned}$$

dove tutte le radici dell'unità sono scelte primitive e dove la seconda uguaglianza consegue dal fatto che un sottogruppo del gruppo moltiplicativo di un campo è ciclico e la terza consegue dal Teorema Cinese del Resto. Poichè le estensioni quadratiche contenute in $\mathbb{Q}(\zeta_{pq})$ sono in corrispondenza biunivoca con i sottogruppi di $\mathrm{Gal}(\mathbb{Q}(\zeta_{pq})/\mathbb{Q})$ di indice 2, ci basta capire quanti sottogruppi di indice 2 riusciamo a trovare per capire quante sono le estensioni quadratiche contenute in K. Sicuramente, poichè p e q sono entrambi dispari, K contiene le estensioni quadratiche L ed M date dalle sole estensioni quadratiche contenute in $\mathbb{Q}(\zeta_p)$ e $\mathbb{Q}(\zeta_q)$, corrispondenti rispettivamente ai sottogruppi $\frac{\frac{p-1}{2}\mathbb{Z}}{(p-1)\mathbb{Z}} \times \frac{\mathbb{Z}}{(q-1)\mathbb{Z}}$ e $\frac{\mathbb{Z}}{(q-1)\mathbb{Z}} \times \frac{\frac{q-1}{2}\mathbb{Z}}{(q-1)\mathbb{Z}}$. Per capire se ce ne sono altri possiamo notare il fatto seguente. Se $2^k | p-1$ e $2^l | q-1$ e sono le massime potenze di 2 che dividono $p-1$ e $q-1$, allora il gruppo di Galois è isomorfo ad un prodotto diretto di un sottogruppo G di ordine dispari con il sottogruppo $\frac{\mathbb{Z}}{2^k\mathbb{Z}} \times \frac{\mathbb{Z}}{2^l\mathbb{Z}}$, pertanto i soli sottogruppi di indice 2 possono derivare dai sottogruppi della forma $H \times G$ con H sottogruppo di

indice 2 in $\frac{\mathbb{Z}}{2^k\mathbb{Z}} \times \frac{\mathbb{Z}}{2^l\mathbb{Z}}$. In particolare, i sottogruppi di indice 2 in $\frac{\mathbb{Z}}{2^k\mathbb{Z}} \times \frac{\mathbb{Z}}{2^l\mathbb{Z}}$ sono i sottogruppi di ordine 2^{k+l-1} in $\frac{\mathbb{Z}}{2^k\mathbb{Z}} \times \frac{\mathbb{Z}}{2^l\mathbb{Z}}$. Calcoliamo i sottogruppi di indice 2 di $F := \frac{\mathbb{Z}}{2^k\mathbb{Z}} \times \frac{\mathbb{Z}}{2^l\mathbb{Z}}$. Prendiamo $E \subseteq F$ di indice 2. Allora, F/E ha ordine 2 e quindi $(xE)^2 = E$ per ogni $x \in F$, che significa che $x^2 \in E$, da cui segue che $F^2 \subseteq E$, dove F^2 è il sottogruppo generato dai quadrati di elementi di F. Ma allora possiamo considerare il sottogruppo di F/F^2 dato da E/F^2, che ha ancora indice 2 in F/E. Definiamo allora una mappa di insiemi che manda un sottogruppo $A \subseteq F$ di indice 2 nel sottogruppo A/F^2 di F/F^2 corrispondente. Tale sottogruppo ha allora indice 2 e si vede pertanto che tale mappa è ben definita. Inoltre, mediante il Teorema di Corrispondenza, è chiaro che realizza una biiezione. In particolare, questo significa che i sottogruppi di indice 2 di F sono in corrispondenza biunivoca con i sottogruppi di indice 2 di F/F^2. Inoltre, poichè in F/F^2 ogni elemento ha ordine 2 per definizione, ricaviamo che $F/F^2 \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}}$. Inoltre, si verifica facilmente che il gruppo di Klein ammette 3 sottogruppi di ordine 2, rispettivamente $0 \times \frac{\mathbb{Z}}{2\mathbb{Z}}$, $\frac{\mathbb{Z}}{2\mathbb{Z}} \times 0$ e quello generato dalla diagonale $(1,1)$. Pertanto possiamo concludere che in K esistono 3 sottocampi quadratici, che sono L, M e N, generato su $\mathbb{Q}$ dal prodotto dei generatori di L ed M su $\mathbb{Q}$. Il caso in cui $p = 2$ è ancora più facile dato che in questo caso il gruppo di Galois é ridotto al gruppo ciclico di ordine $q - 1$ e pertanto in K esiste solo il campo quadratico contenuto in $\mathbb{Q}(\zeta_q)$.