Esercitazioni sulla teoria di Galois

tratti dalle lezioni del prof. Callegaro

1 Lezione del 23/11

Esercizio 1. Consideriamo in $\mathbb{Q}[x]$ il polinomio $\phi_5(x) = x^4 + x^3 + x^2 + x + 1$. Vogliamo vedere cosa possiamo dire di esso. Sappiamo intanto che è irriducibile in $\mathbb{Q}$. Ma vogliamo anche vedere se ϕ_5 è riducibile anche su $\mathbb{Q}(\iota)$. Sappiamo che le sue radici sono ζ_5^i, con i che varia da 1 a 4; possiamo inoltre dire che $\overline{\zeta_5} = \zeta_5^4$ mentre invece $\overline{\zeta_5^2} = \zeta_5^3$. Per dimostrare che è irriducibile su $\mathbb{Q}(\iota)$ dobbiamo innanzitutto cercare di scomporlo come prodotto di polinomi di secondo grado o cercare delle radici. Sappiamo che $\phi_5(x)$ non può avere radici in $\mathbb{Q}(\iota)$, queste infatti sono radici di un polinomio irriducibile in $\mathbb{Q}$ di grado 4, dunque possono appartenere solo ad un'estensione di grado almeno 4 ma, come sappiamo, $\mathbb{Q}(\iota)$ è un'estensione di grado 2 su $\mathbb{Q}$. Allora se $\phi_5(x)$ fosse riducibile in $\mathbb{Q}(\iota)$ si dovrebbe fattorizzare come prodotto di polinomi irriducibili di grado 2 in $\mathbb{Q}(i)$. Ma allora quanto potrebbe valere il termine noto di questi polinomi? Iniziamo pensando al fatto che

$$\phi_5(x) = \prod_{i=1}^{k} (x - \zeta_5^i)$$

Quindi se $\phi_5(x) = f(x)g(x)$ in $\mathbb{Q}(\iota)$ allora sia $f(x)$ che $g(x)$ devono essere prodotti di radici quinte dell'unità. Ma

$$\zeta_5\zeta_3^2 = \zeta_5^3 \notin \mathbb{Q}(\iota) \qquad \zeta_5\zeta_3^3 = \zeta_5^4 \notin \mathbb{Q}(\iota) \qquad \zeta_5\zeta_3^4 = \zeta_5^5 \in \mathbb{Q}(\iota)$$

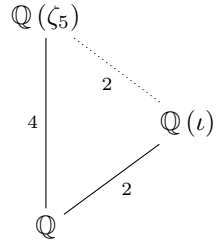
Quindi le uniche possibilità sarebbero:

$$f(x) = (x - \zeta_5)(x - \zeta_5^4) = x^2 - (\zeta_5 + \zeta_5^4)x + 1$$
$$g(x) = (x - \zeta_5^2)(x - \zeta_5^3) = x^2 - (\zeta_5^2 + \zeta_5^3)x + 1$$

Questi polinomi appartengono ad $\mathbb{R}[x]$, dunque se esistessero in $\mathbb{Q}(\iota)[x]$ apparterrebbero a $\mathbb{Q}[x]$ (dovrebbero appartenere all'intersezione tra $\mathbb{R}[x]$ e $\mathbb{Q}(\iota)[x]$) ma questo è assurdo, visto che $\phi_5(x)$ non è riducibile su $\mathbb{Q}[x]$.

Proviamo a risolvere l'esercizio in un modo alternativo.
Sappiamo che $\mathbb{Q}(\iota)$ è un'estensione di Galois di $\mathbb{Q}$ di grado 2, mentre invece $\mathbb{Q}(\zeta_5)$ è sempre un'estensione di Galois su $\mathbb{Q}$ (visto che è il campo di spezzamento di un polinomio irriducibile in un campo a caratteristica 0) ma di grado 4. Sappiamo dunque per la teoria che $G = Gal\left(\mathbb{Q}(\zeta_5)/\mathbb{Q}\right)$ è un gruppo di cardinalità 4, inoltre i suoi elementi devono mandare radici di ϕ_5 in altre radici,

dunque deve essere che, se $\sigma \in G$, $\sigma(\zeta_5) = \zeta_5^i$ per qualche i da 1 a 4 (ma sappiamo anche che scelte due qualsiasi radici a e b di un polinomio irriducibile esiste un automorfismo che manda a in b e lascia fisso il campo di base). Dunque i σ di questo tipo sono tutti e soli gli elementi di G, che dunque è isomorfo a $\mathbb{Z}_4$. Se ϕ_5 fosse riducibile su $\mathbb{Q}(\iota)$ avremmo:

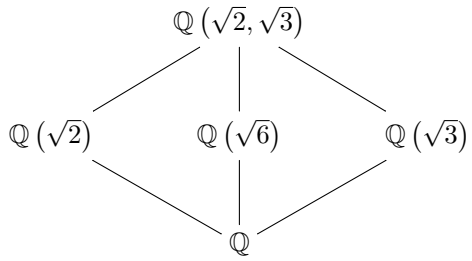


Ma sappiamo che $\mathbb{Z}_4$ ha un unico sottogruppo non banale, se quindi $\mathbb{Q}(\iota)$ fosse incluso in $\mathbb{Q}(\zeta_5)$ dovrebbe essere il sottocampo fissato dall'unico elemento di G di ordine 2, cioè il coniugio di $\mathbb{C}$ ristretto al nostro campo. Ma osserviamo invece qual è il sottocampo fissato dal coniugio; abbiamo per esempio che $a = \zeta_5 + \overline{\zeta_5}$ è un elemento di $\mathbb{Q}(\zeta_5)$ fissato dal coniugio, se fosse vero che $\mathbb{Q}(\iota) \subseteq \mathbb{Q}(\zeta_5)$ dovremmo avere che $a \in \mathbb{Z}_\iota$. Vediamo subito che questo è assurdo, infatti il polinomio minimo di a è $x^2 + x - 1$, quindi abbiamo solo due possibili valori per a, cioè $a = -1 \pm \sqrt{5}$, quindi $\mathbb{Q}(a) = \mathbb{Q}(\sqrt{5})$, che è il campo fisso dell'unico sottogruppo di G, non è sottogruppo di $\mathbb{Q}(\iota)$, dunque $\mathbb{Q}(\iota)$ non è il sottocampo fissato che cercavamo e quindi $\phi_5(x)$ deve continuare ad essere irriducibile in $\mathbb{Q}(\iota)$.

Esercizio 2. Vediamo se $\mathbb{Q}(\sqrt{2})$ e $\mathbb{Q}(\sqrt{3})$ sono tra di loro isomorfi.
Sappiamo che un eventuale isomorfismo tra i due campi dovrebbe essere tale che $\phi(1) = 1$, dunque anche $\phi(2) = 2$. Ma 2 è un quadrato nel primo campo, mentre non lo è nel secondo (verifica immediata ma necessaria). Questo è assurdo, infatti gli isomorfismi mandano quadrati in quadrati.

Esercizio 3. Cerchiamo di capire se $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.
Un'inclusione è ovvia; chiamiamo dunque $a = \sqrt{2} + \sqrt{3}$, già dal fatto che $a^2 - 5 = 2\sqrt{6}$ possiamo intuire che il polinomio minimo di a non può avere grado 2 e da questo potremmo dire allora che $\mathbb{Q}(a)$ è un'estensione di grado 4 su $\mathbb{Q}$ compresa in un'altra estensione di grado 4 su $\mathbb{Q}$, devono dunque essere uguali. Un metodo alternativo comunque consiste nel dire che $\sqrt{2} = \frac{a^5 - 89a}{20} \in \mathbb{Q}(a)$, il che dimostra l'altra inclusione.
Abbiamo visto anche che il gruppo di Galois $G = Gal\left(\mathbb{Q}(\sqrt{2}, \sqrt{3}) / \mathbb{Q}\right)$ è $\mathbb{Z}_2^2$, ma potevamo già affermarlo prima, infatti abbiamo già trovato 3 sottoestensioni

distinte di $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$:



e quindi sappiamo che G deve essere un gruppo di 4 elementi con 3 sottogruppi distinti, non può essere altri che $\mathbb{Z}_2^2$. I possibili automorfismi di G sono tutti e soli i:

$$\sigma : \begin{cases} \sqrt{2} \mapsto \pm\sqrt{2} \\ \sqrt{3} \mapsto \pm\sqrt{3} \end{cases}$$

Al variare arbitrario dei segni in arrivo.

Esercizio 4. Sia $p(x) = x^3 + ax^2 + bx + c$ polinomio irriducibile su $\mathbb{Q}[x]$. Come può essere fatto il gruppo di Galois del suo campo di spezzamento K su $\mathbb{Q}$?
Sappiamo che possiamo dividere due casi, infatti K può avere grado 3 o 6 su $\mathbb{Q}$. Nel primo caso il gruppo di Galois deve essere $\mathbb{Z}_3$, nel secondo caso invece, anche se ci sono, a meno di isomorfismi, due diversi tipi di gruppi di ordine 6 possiamo essere solo nel caso di $\mathcal{S}_3$, infatti un automorfismo del gruppo di Galois di un campo di spezzamento di un polinomio irriducibile è determinato univocamente da dove manda le radici del polinomio, dunque il gruppo degli automorfismi possibili deve comunque essere un sottogruppo di $\mathcal{S}_3$, dunque nel secondo caso sarebbe $\mathcal{S}_3$.
Comunque il polinomio $p(x)$ ha tre radici nel suo campo di spezzamento, quindi possiamo dire $p(x) = (x-a_1)(x-a_2)(x-a_3)$, questo ci fa notare che dobbiamo avere

$$K \ni \delta = (a_1 - a_2)(a_1 - a_3)(a_2 - a_3)$$

Sappiamo che $\Delta = \delta^2$ viene fissato sempre. Quindi appartiene al campo fisso del gruppo di Galois su $\mathbb{Q}$, dunque $\Delta \in \mathbb{Q}$ (altrimenti l'estensione non sarebbe di Galois). Inoltre $p(x)$ lo si può scrivere (a meno di traslazione di x) come $f(x) = x^3 + ax + b$. In tale caso abbiamo:

$$\Delta = \delta^2 = 4a^3 - 27b^2$$

infatti $b = -a_1a_2a_3$ e $a = a_1a_2 + a_2a_3 + a_1a_3$; cosa succede se permutiamo ciclicamente a_1, a_2, a_3, ciè se mandiamo $a_1 \mapsto a_2 \mapsto a_3 \mapsto a_1$? Abbiamo che δ viene mandato in se stesso. Se invece permutiamo a_1 e a_2 e lasciamo invariato a_3 abbiamo che $\delta \mapsto -\delta$. Ma allora Δ è un quadrato in $\mathbb{Q}$? Se non è un quadrato allora dobbiamo estendere $\mathbb{Q}$ a $\mathbb{Q}(\delta)$, infatti, come abbiamo detto, $\delta = \sqrt{\Delta}$ deve appartenere al campo di spezzamento K. Se al contrario Δ è un quadrato in $\mathbb{Q}$ non possiamo avere permutazioni dispari nel gruppo di Galois $G' = Gal\left(K/\mathbb{Q}\right)$, quindi $G' \simeq \mathcal{A}_3 \simeq \mathbb{Z}_3$.
Se δ non è un quadrato in $\mathbb{Q}$, invece, allora rispetto $\mathbb{Q}(\delta)$ abbiamo

$$K \supsetneq \mathbb{Q}(\delta) \supsetneq \mathbb{Q}$$

Quindi il grado di K su $\mathbb{Q}$ è 6 e il gruppo di Galois è isomorfo a $\mathcal{S}_3$.
Vediamo invece ora cosa possiamo dire grazie alla derivata, sappiamo che $f'(x) = 3x^2 + a$, che si annulla in $x_{1,2} = \pm\sqrt{-\frac{a}{3}}$, se abbiamo che $f(x_1)f(x_2) > 0$ allora abbiamo una sola radice reale, altrimenti ne abbiamo tre (per questioni analitiche: si tratta pur sempre di un polinomio di terzo grado in $\mathbb{Q}[x]$. Ma possiamo anche dire:

$$\left.\begin{array}{l} f(x_1) = -\frac{a}{3}\sqrt{\frac{a}{3}} + a\sqrt{\frac{a}{3}} + b \\ f(x_2) = \frac{a}{3}\sqrt{\frac{a}{3}} - a\sqrt{\frac{a}{3}} + b \end{array}\right\} \implies f(x_1)f(x_2) = b^2 - \left(\frac{2}{3}a\sqrt{\frac{a}{3}}\right)^2 = b^2 - \frac{4}{27}a^3$$

Quindi, usando l'analisi, possiamo dire che se la derivata si annulla in due punti e i due valori critici sono concordi (ovvero $f(x_1)f(x_2) > 0$) il polinomio ammette solo una radice reale, dunque altre due radici sono complesse] coniugate e quindi esiste un automorfismo del campo di spezzamento, dato dal coniugio, che ha ordine 2. Quindi in questo caso il gruppo di Galois deve essere $\mathcal{S}_3$ (caso particolare di quanto possiamo dedurre con l'argomento precedente).

Esercizio 5. Consideriamo ora il polinomio $p(x) = x^4 - 6x^2 + 25$ e sia K il suo campo di spezzamento su $\mathbb{Q}$. Cerchiamo di dire quanto possibile.
Per quanto visto prima possiamo intanto dire che $Gal\left(K/\mathbb{Q}\right)$ si immerge in $\mathcal{S}_4$. Sia $y = x^2$ allora abbiamo $p(x) = y^2 - 6y + 25$, il determinante di questo polinomio è -64, dunque $\sqrt{\Delta} = 8\iota$. Le radici del polinomio in y sono dunque $y_{1,2} = 2 \pm 4\iota$. Possiamo quindi dire che in $\mathbb{Q}(\iota)$ il polinomio si spezza almeno in due fattori di grado 2, infatti abbiamo:

$$p(x) = (x^2 - 3 - 4\iota)(x^2 - 3 + 4\iota)$$

Ci dobbiamo dunque chiedere se $3 + 4\iota$ e $3 - 4\iota$ sono quadrati in $\mathbb{Q}(\iota)$. Notiamo che $(3 + 4\iota)(3 - 4\iota) = 25$ è un quadrato in $\mathbb{Q}$ e dunque se uno tra $3 + 4\iota$ e $3 - 4\iota$ è un quadrato uno lo è anche l'altro. In generale se consideriamo il prodotto $(x^2 - a)(x^2 - \overline{a})$ ci possiamo chiedere se $a\overline{a} = |a|^2$ è un quadrato in $\mathbb{Q}\left(\sqrt{\Delta}\right)$; se la risposta è affermativa allora potremmo dire che $\overline{a}$ è un quadrato in $\mathbb{Q}\left(\sqrt{\Delta}, \sqrt{a}\right)$, infatti $\overline{a} = \frac{a\overline{a}}{a}$ e il rapporto tra due quadrati è un quadrato.
Dobbiamo dunque chiederci, in generale:

- Δ è un quadrato in $\mathbb{Q}$? Se lo è il polinomio biquadratico si fattorizza come prodotto di due fattori di secondo grado nella forma $(x^2 - \omega_1)(x^2 - \omega_2)$, altrimenti occorre estendere il campo con $\sqrt{\Delta}$ per poter fattorizzare il polinomio in tale modo.

- $\omega_1\omega_2$, che poi è il remine noto del polinomio, è un quadrato in $\mathbb{Q}$? Se non è un quadrato in $\mathbb{Q}$, è almeno un quadrato in $\mathbb{Q}\left(\sqrt{\Delta}\right)$? Se è un quadrato in $\mathbb{Q}$ allora il prodotto $\omega_1\omega_2$ sarà invariante rispetto all'azione del gruppo di Galois. Altrimenti se è un quadrato in $\mathbb{Q}\left(\sqrt{\Delta}\right)$ sarà invariante solo per quegli automorfismi che fissano $\sqrt{\Delta}$, mentre cambierà segno quando $\sqrt{\Delta}$ cambia segno.

- ω_1 è un quadrato in $\mathbb{Q}\left(\sqrt{\Delta}, \sqrt{\omega_1\omega_2}\right)$? Se non lo è abbiamo bisogno di aggiungere la radice quadrata di ω_1 per poter fattorizzare completamente

il polinomio. In caso contrario si può vedere che il polinomio biquadratico non era irriducibile. In ogni caso è vero che se consideriamo un'estensione di $\mathbb{Q}$ contenente $\sqrt{\Delta}$, $\sqrt{\omega_1\omega_2}$ e $\sqrt{\omega_1}$, in essa possiamo trovare tutte le radici del polinomio biquadratico.

Queste informazioni sono sufficienti per determinare il gruppo di Galois. Vediamo un esempio nell'esercizio successivo.

Esercizio 6. Sia $p(x)$ un polinomio biquadratico di quarto grado. Per quanto visto nell'esercizio precedente il suo campo di spezzamento deve avere grado una potenza di 2, non superiore ad 8 e il suo gruppo di Galois deve essere un sottogruppo di $\mathcal{S}_4$. Ma l'unico sottogruppo di $\mathcal{S}_4$ di cardinalià 8 è $\mathcal{D}_4$. Dunque in generale chi può essere $Gal\left(K/\mathbb{Q}\right)$ se K è campo di spezzamento di $x^4 + ax^2 + b$? Dovendo essere un sottogruppo del 2-Sylow $\mathcal{D}_4$ abbiamo che può essere solamente $\mathbb{Z}_2$, $\mathbb{Z}_4$, $\mathbb{Z}_2^2$ oppure $\mathcal{D}_4$. Cosa succede per esempio nel caso $p(x) = x^4 + 1$? Le radici di $p(x)$ sono le radici ottave dell'unità, abbiamo infatti che:

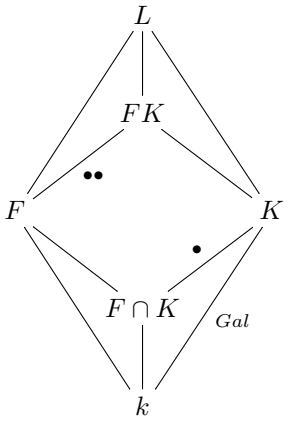
$$x^8 - 1 = (x^4 + 1)(x^2 + 1)(x + 1)(x - 1)$$

dove le radici del primo fattore sono le radici primitive ottave dell'unità, visto che le radici del secondo sono $\pm\iota$, e le altre due appartengono a $\mathbb{Q}$. Applicando quindi quanto visto sopra troviamo che $\Delta = -4$, se estendiamo $\mathbb{Q}$ con ι otteniamo una prima fattorizzazione come $p(x) = (x^2 + \iota)(x^2 - \iota)$. Il termine noto è razionale: non occorre aggiungere il suo quadrato. Infine ci chiediamo se ι è un quadrato in $\mathbb{Q}(\iota)$, questo non è vero, infatti le radici di $\mathbb{Q}(\iota)$ sono $\pm\left(\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}\iota\right)$, dobbiamo cioè aggiungere $\sqrt{2}$. Quindi il campo di spezzamento ha grado 4 su $\mathbb{Q}$.
Abbiamo quindi che le quattro radici, due a due coniugate, sono $a_1, \overline{a_1} = a_2, a_3, \overline{a_3} = a_4$, quindi $x^2 + \iota$ avrà avuto come radici a_1, a_3 mentre inceve $x^2 - \iota$ avrà avuto le altre due. Il termine noto, pari al prodotto $(\iota)(-\iota)$, è un quadrato in $\mathbb{Q}$, quindi il prodotto a_1a_3 è razionale e dunque invariante. Quindi l'azione di un automorfismo su a_1 determina l'automorfismo su a_3 e lo stesso vale per a_2 e a_4. In particolare è facile vedere che ci sono due automorfismi di ordine 2: quello che manda $a_1 \mapsto a_3$ e $a_3 \mapsto a_1$ e quello che manda $a_1 \mapsto a_2$, $a_3 \mapsto a_4$. Dunque il gruppo di Galois deve essere $\mathbb{Z}_2 \times \mathbb{Z}_2$.

2 Lezione del 29/11

Proposizione 1. *Sia k un campo, F una sua estensione e K un'estensione di Galois di k. Diciamo inoltre FK il più piccolo campo contente F e K e L una*

sua estensione. Cioè riassumendo abbiamo:



Possiamo allora dire che $\mathcal{A}ut\left(FK/F\right) \xrightarrow{\Phi} \mathcal{A}ut\left(K/F\cap K\right)$ *(omomorfismo di restrizione) è un isomorfismo. Inoltre le estensioni segnate (con i* $\bullet$*) sono di Galois.*

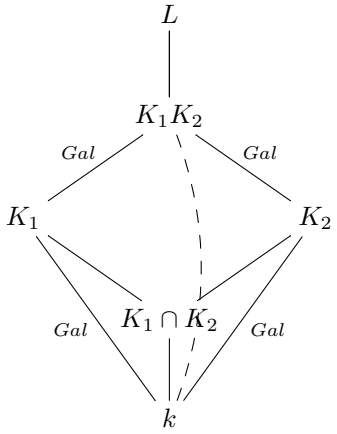
Dimostrazione. Vediamo innanzitutto perché le estensioni segnate sono di Galois.

- Sappiamo che K è campo di spezzamento di $p(x)$ su k, ma allora è anche campo di spezzamento di $p(x)$ su $F \cap K$.
- $\bullet\bullet$ Vale la stessa cosa anche per questa estensione. Infatti se consideriamo il più piccolo campo che contiene F e le radici di $p(x)$ allora questo è il più piccolo campo contentente F e K, dunque è FK. FK è quindi il campo di spezzamento di $p(x)$ su F.

Vediamo innanzitutto che Φ è iniettivo, questo è vero perché, preso $\phi \in \mathcal{A}ut\left(FK/F\right)$, se $\phi\mid_K = id_K$ allora $\phi = id_{FK}$. Infatti sappiamo che K è un'estensione primitiva di k, possiamo quindi dire $FK = F(\gamma)$ per un qualche elemento $\gamma \in K$. Ma allora un elemento del nucleo di Φ lascia invariato sia γ che F, dunque è l'identità in FK.
Inoltre Φ è surgettiva: sia $H \in \mathcal{A}ut\left(K/F\cap K\right)$ l'immagine di Φ. Il gruppo H fissa $F \cap K$ e se un elemento $\alpha \in K$ è fissato da H, allora α è fissato anche da $\mathcal{A}ut\left(FK/F\right)$ e quindi il campo fisso di H è esattamente $F \cap K$. Ma allora per la corrispondenza di Galois H è proprio il gruppo $\mathcal{A}ut\left(K/F\cap K\right)$ e dunque Φ è surgettiva. □

Proposizione 2. *Sia k un campo e K_1, K_2 due sue estensioni di Galois e L un'estensione che comprenda entrambe. Affermiamo che anche K_1K_2, il più piccolo campo contenente K_1 e K_2, è un'estensione di Galois rispetto a k (sappiamo già che lo è su K_1 e su K_2 per l'ultima proposizione vista). Diciamo inoltre che* $\mathcal{A}ut\left(K_1K_2/k\right) \xrightarrow{\Phi} \mathcal{A}ut\left(K_1/k\right) \times \mathcal{A}ut\left(K_2/k\right)$ *è un omomorfismo*

iniettivo, inoltre se $K_1 \cap K_2 = k$ l'ommorfismo è anche surgettivo.



Dimostrazione. Se K_1 è campo di spezzamento di $p_1(x)$ su k e K_2 la stessa cosa per $p_2(x)$, abbiamo allora che K_1K_2 è campo di spezzamento di $(p_1p_2)(x)$ (se infatti p_1p_2 non fosse separabile su k avremmo che ci dovrebbe essere un fattore irriducibile di p_1p_2 a derivata nulla, ma allora questo sarebbe un fattore di p_1 o un fattore di p_2, ma questo è assurdo, visto che K_1 e K_2 sono di Galois).
Consideriamo ora $\phi \in Ker(\Phi)$, dobbiamo avere che $\phi\,|_{K_1} = id_{K_1}$ e anche $\phi\,|_{K_2} = id_{K_2}$; ma questo implica che ϕ è l'identità di $\mathcal{A}ut\left(K_1K_2/k\right)$.
Inoltre se $K_1 \cap K_2 = k$, per il teorema precedente abbiamo che, dato un elemento $\sigma_1 \in \mathcal{A}ut\left(K_1/k\right)$ esiste un elemento $\sigma \in \mathcal{A}ut\left(K_1K_2/K_2\right)$ che si restringe a σ_1 e dunque a maggior ragione esiste un elemento (sempre σ) appartenente $\mathcal{A}ut\left(K_1K_2/k\right)$ che si restringe a σ_1 e induce l'identità su K_2. Quindi $\mathcal{A}ut\left(K_1/K_1 \cap K_2\right) \times \{e\}$ è nell'immagine di Φ. Ribaltando l'argomento possiamo concludere che se $K_1 \cap K_2 = k$ la mappa Φ è surgettiva e abbiamo:

$$\mathcal{A}ut\left(K_1K_2/k\right) \;\simeq\; \mathcal{A}ut\left(K_1/k\right) \;\simeq\; \mathcal{A}ut\left(K_2/k\right)$$

□

Esercizio 7. Trovare il gruppo di Galois del campo di spezzamento di $q(x) = (x^4+1)(x^2-m)$ su $\mathbb{Q}$, dato $m \in \mathbb{Z}$ tale che $|m|$ non sia un quadrato perfetto.

Dimostrazione. Dividiamo il problema in due parti;

- Cerchiamo innanzitutto il campo di spezzamento di $p(x) = x^4+1$ su $\mathbb{Q}$. Sappiamo che p è un polinomio ciclotomico, quindi irriducibile; le sue radici sono le radici ottave dell'unità elevate a potenze prime con 8. Cioè le radici di p sono le varie ζ_8^i con $(i,8)=1$; dunque il suo campo di spezzamento è dato da $L = \mathbb{Q}(\zeta_8)$. Visto che gli automorfismi del gruppo di Galois corrispondono agli automorfismi di $\mathcal{A}ut\left(\mathbb{Q}(\zeta_8)/\mathbb{Q}\right)$ abbiamo che questi sono determinati unicamente dall'immagine di ζ_8, che deve essere mandato in una radice dell'unità di ordine 8. Abbiamo dunque che il gruppo di Galois che cerchiamo è isomorfo a $\mathbb{Z}_8^*$ che, come sappiamo, è isomorfo a $\mathbb{Z}_2^2$.

- Possiamo a questo punto notare che $\iota = \zeta_8^2 \in L$, inoltre $\zeta_8 + \zeta_8^{-1} = \sqrt{2}$, infatti vale che:

$$\left(\zeta_8 + \zeta_8^{-1}\right)^2 = \zeta_8^2 - \zeta_8^2 + 2 = 2$$

Possiamo quindi dire $L \supseteq \mathbb{Q}\left(\sqrt{2}, \iota\right)$. Questo ci fa comprendere la condizione secondo la quale $|m|$ non è un quadrato perfetto; altrimenti l'ulteriore estensione a campo di spezzamento di $q(x)$ sarebbe banale (notiamo inoltre che sarebbe banale anche se avessimo $m = 2^k r$ con r dispari e quadrato in $\mathbb{Q}$).

- Osserviamo ora l'intersezione $\mathbb{Q}(\zeta_8) \cap \mathbb{Q}(\sqrt{m})$, questa può essere $\mathbb{Q}$ o una sottoestensione di $\mathbb{Q}(\zeta_8)$ di grado 2 su $\mathbb{Q}$. Ma quante sottoestensioni del genere esistono? Sappiamo che sono tante quante i sottogruppi di indice 2 in $\mathbb{Z}_2^2$, cioè 3. I sottogruppi di indice 2 in $\mathbb{Z}_8^*$ sappiamo che sono: $\{1,7\}, \{1,3\}, \{1,5\}$; a ciascuno di questi corrisponde un sottocampo: quello degli elementi lasciati fissi dagli automorfismi del sottogruppo di Galois considerato.
Comunque conosciamo già tre sottoestensioni di $\mathbb{Q}(\zeta_8)$ e cioè $\mathbb{Q}(\iota)$, $\mathbb{Q}\left(\sqrt{2}\right)$ e $\mathbb{Q}\left(\iota\sqrt{2}\right)$, quindi è sufficiente constatare che sono tra loro distinte per concludere (per esempio possiamo notare che una è reale e se le due non reali coincidessero, conterrebbero quella reale). Dunque l'intersezione $\mathbb{Q}(\zeta_8) \cap \mathbb{Q}(\sqrt{m})$ è diversa da $\mathbb{Q}$ se e solo se m si può scrivere come $\pm 2^a b^2$, con $a \in \mathbb{N}, b \in \mathbb{Q}$. In questi casi il gruppo di Galois del campo di spezzamento è dunque $\mathbb{Z}_2^2$.

- Infine se m non si può scrivere come $\pm 2^a b^2$, con $a \in \mathbb{N}, b \in \mathbb{Q}$ allora $\mathbb{Q}(\zeta_8) \cap \mathbb{Q}(\sqrt{m}) = \mathbb{Q}$ e $\mathbb{Q}(\sqrt{m}) \neq \mathbb{Q}$. Dunque la proposizione vista prima ci dice che il gruppo di Galois del campo di spezzamento di $q(x)$ su $\mathbb{Q}$ è il prodotto

$$\mathcal{A}ut\left(\mathbb{Q}(\zeta_8)/\mathbb{Q}\right) \times \mathcal{A}ut\left(\mathbb{Q}\left(\sqrt{m}\right)/\mathbb{Q}\right) = \mathbb{Z}_2^2 \times \mathbb{Z}_2.$$

□

Esercizio 8. Sia $q(x) \in \mathbb{Q}[x]$ un polinomio irriducibile di grado p, con p numero primo. Supponiamo che q abbia esattamente due radici non reali. Allora, detto L il campo di spezzamento di $q(x)$ su $\mathbb{Q}$ abbiamo che:

$$\mathcal{A}ut\left(L/\mathbb{Q}\right) \simeq \mathcal{S}_p$$

Dimostrazione. Sappiamo innanzitutto che $p \mid \left|\mathcal{A}ut\left(L/\mathbb{Q}\right)\right|$, questo lo sappiamo perché L è un'estensione di $\mathbb{Q}[x]/(q(x))$ che ha grado p su $\mathbb{Q}$.
Poiché possiamo immergere il gruppo di Galois G in $\mathcal{S}_p$, sapendo che $p \mid |G|$ e abbiamo che G contiene un elemento di ordine p, quindi necessariamente un p-ciclo; inoltre la restrizione a L del coniugio in $\mathbb{C}$ ha ordine 2 e scambia solo le radici non reali, è quindi un 2-ciclo, visto che scambia solamente due radici. Concludiamo perché sappiamo che, se p è primo, $\mathcal{S}_p$ è generato da un p-ciclo e da un qualsiasi 2-ciclo. □

Esempio 1. Consideriamo il polinomio $p(x) = x^5 - 4x + 2$. Questo polinomio è irriducibile per Eisenstein, trovare il gruppo di Galois del suo campo di spezzamento su $\mathbb{Q}$.

Dimostrazione. Sappiamo che la derivata di $p(x)$ è $p'(x) = 5x^4 - 4$, che ha radici reali in $\pm\sqrt[4]{\frac{4}{5}}$. La valutazione di $p(x)$ è positiva nella minore delle radici della sua derivata ed è negativa nella maggiore. Vediamo dunque che $p(x)$ ha esattamente tre radici reali (e quindi solamente due radici complesse). Possiamo concludere dicendo che il gruppo di Galois della sua estensione è isomorfo a $\mathcal{S}_5$. □

Esercizio 9. Cosa possiamo dire del campo di spezzamento (e del suo gruppo di Galois) su $\mathbb{Q}$ di $p(x) = x^4 + ax^2 + b$ al variare di $a, b \in \mathbb{Q}$?

Dimostrazione. Indichiamo il discriminante del polinomio come $\Delta = a^2 - 4b$. Ci possiamo trovare di fronte a diversi casi:

a) Se Δ è un quadrato in $\mathbb{Q}$ allora il polinomio $p(x)$ si fattorizza in due fattori di grado 2 e dunque il gruppo di Galois è un sottogruppo di $\mathbb{Z}_2 \times \mathbb{Z}_2$, comunque non è interessante.

b) Consideriamo quindi il caso in cui Δ non è un quadrato in $\mathbb{Q}$. Anche in questo punto possiamo trovarci in diverse situazioni:

   - Sia b un quadrato in $\mathbb{Q}\left(\sqrt{\Delta}\right)$. Chiamiamo ω_1 e ω_2 le radici di $y^2 + ay + b$, sappiamo allora che le radici di $p(x)$ sono $\pm\sqrt{\omega_1}$ e $\pm\sqrt{\omega_2}$ e dunque $b = \omega_1\omega_2$. Allora è sufficiente estendere $\mathbb{Q}\left(\sqrt{\Delta}\right)$ a $\mathbb{Q}\left(\sqrt{\Delta}, \sqrt{\omega_1}\right)$, otteniamo in questo modo che $\omega_2 = b\omega_1^{-1}$ è un quadrato in $\mathbb{Q}\left(\sqrt{\Delta}, \sqrt{\omega_1}\right)$, quindi le sue radici quadrate (e quindi tutte le radici quadrate del polinomio) appartengono a $\mathbb{Q}\left(\sqrt{\Delta}, \sqrt{\omega_1}\right)$. Abbiamo comunque due casi:

     * Se b è un quadrato in $\mathbb{Q}$ e $\mathbb{Q}\left(\sqrt{\Delta}, \sqrt{\omega_1}\right) \neq \mathbb{Q}\left(\sqrt{\Delta}\right)$ allora gli automorfismi del gruppo di Galois non possiamo sceglierli con molta libertà. Sia infatti $\phi \neq e$ uno di questi automorfismi, abbiamo allora che $\phi\sqrt{\omega_1} = \pm\sqrt{\omega_1} \implies \phi\sqrt{\omega_2} = \pm\sqrt{\omega_2}$. In alternativa, dato un automorfismo ψ tale che $\psi\sqrt{\omega_1} \neq \pm\sqrt{\omega_1}$, allora ψ manda ω_1 in ω_2 e viceversa. Supponiamo ad esempio $\psi\sqrt{\omega_1} = \sqrt{\omega_2}$ (il caso $\psi\sqrt{\omega_1} = -\sqrt{\omega_2}$ è equivalente). Abbiamo quindi il seguente schema di automorfismi possibili:

$$\begin{array}{ccc} \sqrt{\omega_1} & \overset{\phi}{\longleftrightarrow} & -\sqrt{\omega_1} \\ \psi \updownarrow & & \updownarrow \psi \\ \sqrt{\omega_2} & \underset{\phi}{\longleftrightarrow} & -\sqrt{\omega_2} \end{array}$$

     Abbiamo quindi che in questo caso il gruppo di Galois è isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$.

* Se b non è quadrato in $\mathbb{Q}$ ma è quadrato in $\mathbb{Q}\left(\sqrt{\Delta}\right)$. Sia allora ϕ un automorfismo del gruppo di Galois di $\mathbb{Q}\left(\sqrt{\Delta}, \sqrt{\omega_1}\right)$ tale che $\phi(\sqrt{\Delta}) = -\sqrt{\Delta}$. Allora $\phi\sqrt{b} = -\sqrt{b}$ e abbiamo allora che deve essere $\phi(\sqrt{\omega_1}\sqrt{\omega_2}) = -\sqrt{\omega_1}\sqrt{\omega_2}$, e vanno bene tutti gli automorfismi che consentono questo, dunque se $\phi(\sqrt{\omega_1}) = \pm\sqrt{\omega_1}$ abbiamo che $\phi(\sqrt{\omega_2})$ deve valere $\mp\sqrt{\omega_2}$. Se invece $\psi(\sqrt{\Delta}) = -\sqrt{\Delta}$ abbiamo che $\psi(\sqrt{\omega_1}) = \pm\sqrt{\omega_2}$ implica che $\psi(\sqrt{\omega_2}) = \mp\sqrt{\omega_1}$.
  Si può dunque verificare che il sottogruppo è isomorfo a $\mathbb{Z}_4$.

- Sia b non quadrato in $\mathbb{Q}\left(\sqrt{\Delta}\right)$. Allora se $\omega_1 \notin \mathbb{Q}\left(\sqrt{\Delta}, \sqrt{b}\right)$ il campo di spezzamento del polinomio ha grado 8, è quindi isomorfo a $\mathcal{D}_4$.

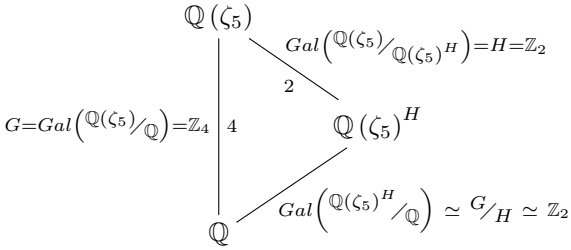
□

3 Lezione del 2/12

Esercizio 10. Ci chiediamo, al variare di $n \in \mathbb{Z}$, se $\sqrt{n} \in \mathbb{Q}(\zeta_5)$.
Cercando $\sqrt{n}$ cerchiamo un'estensione di grado al più 2 su $\mathbb{Q}$, sappiamo che $Gal\left(\mathbb{Q}(\zeta_5)/\mathbb{Q}\right) \simeq \mathbb{Z}_4$, dunque vi è un unico sottogruppo di ordine 2, quindi vi è un unico sottocampo di $\mathbb{Q}(\zeta_5)$ di grado 2 su $\mathbb{Q}$. Questo campo intermedio è $\mathbb{Q}(\zeta_5)^H$, cioè il campo fissato da H, l'unico sottogruppo non banale di $\mathbb{Z}_4$. Quindi per capire se n è un quadrato in $\mathbb{Q}(\zeta_5)$ ci è sufficiente vedere se $\mathbb{Q}(\sqrt{n}) = \mathbb{Q}(\zeta_5)^H$, ma il generatore di H è il coniugio di $\mathbb{C}$ ristretto a $\mathbb{Q}(\zeta_5)$, e in particolare manda ζ_5 in ζ_5^4. Sappiamo infatti che possiamo descrivere il gruppo di Galois di $\mathbb{Q}(\zeta_5)$ su $\mathbb{Q}$ come:

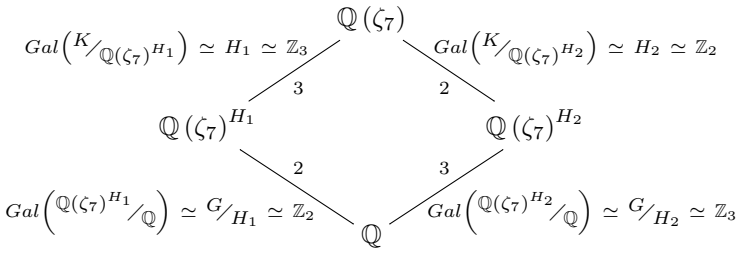
$$Gal\left(\mathbb{Q}(\zeta_5)/\mathbb{Q}\right) = \left\{\mathbb{Q}(\zeta_5) \xrightarrow{\phi} \mathbb{Q}(\zeta_5) \ t.c.\ \phi(\zeta_5) = \zeta_5^i,\ con\ i_1^4\right\}$$

Possiamo quindi riassumere la situazione come:



Notiamo che possiamo dire che $\mathbb{Q}(\zeta_5)^H$ è un'estensione di Galois di $\mathbb{Q}$ solo perché il sottogruppo di G che la fissa è normale in G. Vediamo quindi per esempio che un elemento di $\mathbb{Q}(\zeta_5)^H$ è $a = \zeta_5 + \zeta_5^4$, infatti questo elemento non viene variato dal generatore di H. Ma possiamo facilmente vedere che a è radice di $x^2 + x - 1$, dunque $a = \frac{-1 \pm \sqrt{5}}{2}$ e quindi $a \notin \mathbb{Q}$; Abbiamo quindi in particolare che $\mathbb{Q}(a) = \mathbb{Q}\left(\sqrt{5}\right) = \mathbb{Q}(\zeta_5)^H$.
Possiamo dire quindi che n è un quadrato in $\mathbb{Q}(\zeta_5)$ solamente se lo è in $\mathbb{Q}(a) = \mathbb{Q}\left(\sqrt{5}\right)$, dunque solo se $n = 5b^2$ per qualche $b \in \mathbb{Z}$.

Esercizio 11. Quali sono le sottoestensioni di $K = \mathbb{Q}(\zeta_7)$ su $\mathbb{Q}$?
Sappiamo innanzitutto che $[K : \mathbb{Q}] = \phi(7) = 6$ e inoltre $Gal\left(K/\mathbb{Q}\right) \simeq \mathbb{Z}_7^* \simeq \mathbb{Z}_6$, sappiamo inoltre che $\mathbb{Z}_6$ contiene due sottogruppi (entrambi normali), uno di ordine 3, che è $2\mathbb{Z}_6 = H_1$ e uno di ordine 2 che chiameremo H_2, ciascuno di questi fissa un sottocampo. Abbiamo quindi la seguente situazione:



Chi genera però $G = Gal\left(\mathbb{Q}(\zeta_7)/\mathbb{Q}\right)$? È l'automorfismo $\zeta_5 \xrightarrow{\phi} \zeta_5^3$. Cerchiamo dunque un elemento di K fissato da H_1 (che ricordiamoci essere generato da ϕ^2), certamente troviamo $a = \zeta_7 + \phi^2(\zeta_7) + \phi^4\zeta_7$, abbiamo allora che:

$$a = \zeta_7 + \zeta_7^2 + \zeta_7^4 \implies a^2 = \zeta_7^2 + \zeta_7^4 + \zeta_7 + 2\zeta_7^3 + 2\zeta_7^5 + 2\zeta_7^6$$

Possiamo quindi vedere piuttosto facilmente che il polinomio minimo di a è dato da $x^2 + x + 2$, inoltre $a \in \mathbb{Q}\left(\sqrt{\Delta}\right) = \mathbb{Q}\left(\iota\sqrt{7}\right)$. Dunque $\mathbb{Q}(a) = K^{H_1}$. Per collegarci all'esercizio precedente ora possiamo dire che un non quadrato n in $\mathbb{Q}$ è quadrato in $\mathbb{Q}\left(\sqrt{7}\right)$ se e solo se $n = -7b^2$ per qualche b.

Consideriamo ora l'altro sottogruppo di G, cioè $H_2 =< \phi^3 >$ con $\zeta_7 \xrightarrow{\phi^3} \zeta_7^{-1}$, un elemento lasciato fisso da H_2 è per esempio $b = \zeta_7 + \zeta_7^{-1}$; per mostrare che b genera su $\mathbb{Q}$ l'estensione K^{H_2} dovremmo trovare il polinomio minimo di b su $\mathbb{Q}$ di grado 3, oppure, alternativamente, trovare un polinomio di grado 2 in $\mathbb{Q}(b)$ che si annulli in ζ_7; se lo trovassimo vorrebbe in effetti dire che $\mathbb{Q}(b)$ è una sottoestensione non banale di K. In particolare troviamo che $x^2 - bx + 1$ si annulla in ζ_7, quindi è il suo polinomio minimo, visto che non può essere di grado minore di 2 senza che sia $\zeta_7 \in \mathbb{Q}(b)$ (il che sarebbe assurdo).

Esercizio 12. Troviamo K tale che $Gal\left(K/\mathbb{Q}\right) \simeq \mathbb{Z}_8$.

Sappiamo che $G = Gal\left(\mathbb{Q}(\zeta_{17})/\mathbb{Q}\right)$ è isomorfo a $\mathbb{Z}_{16}$, ma in $\mathbb{Z}_{16}$ vi è un sottogruppo H di indice 8, abbiamo dunque che il sottocampo di K fissato da H è una estensione di Galois (tutti i sottogruppi di un gruppo abeliano sono normali) di $\mathbb{Q}$ tale che $Gal\left(K^H/\mathbb{Q}\right) \simeq G/H$. Un elemento di ordine 2 in G è $\zeta_{17} \xrightarrow{\phi} \zeta_{17^{-1}}$. Prendiamo quindi $c = \zeta_{17} + \zeta_{17}^{-1} \in K^H$; possiamo considerare che in $\mathbb{Q}(c)[x]$ il polinomio minimo di ζ_{17} è $z^2 - cx + 1$, quindi $[\mathbb{Q}(\zeta_{17}) : \mathbb{Q}(c)] \leq 2$. Inoltre per costruzione $\mathbb{Q}(c) \subset \mathbb{Q}(\zeta_{16})^H$ e dunque ha grado al più 8 su $\mathbb{Q}$. Dalla torre di estensioni segue che il grado di $\mathbb{Q}(c)$ su $\mathbb{Q}$ è esattamente 8.

Esercizio 13. Consideriamo $p(x) = x^4 + ax^2 + b$. Il gruppo di Galois del suo campo di spezzamento deve essere contenuto in $\mathcal{D}_4$ e può quindi essere $\mathbb{Z}_2, \mathbb{Z}_2^2, \mathbb{Z}_4, \mathcal{D}_4$. Tutti questi casi possono in effetti accadere, e abbiamo trovato

un campo che abbia gruppo di Galois $\mathbb{Z}_8$ su $\mathbb{Q}$. Ma può esistere un campo che abbia gruppo di Galois $\mathcal{Q}_8$ su $\mathbb{Q}$?
Siano

$$E = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) \ e \ L = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}, \overbrace{\sqrt{(\sqrt{2}+2)(\sqrt{3}+3)}}^{a}\right)$$

Sappiamo che E ha grado 4 su $\mathbb{Q}$ e che il suo gruppo di galois è isomorfo a $\mathbb{Z}_2^2$, i suoi generatori sono:

$$\sigma : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases} \qquad \tau : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases}$$

Chiaramente L ha grado 2 su E e dunque ha grado al più 8 su $\mathbb{Q}$. È facile vedere che se $a \notin E$, a ha 8 coniugati: $a_i = \pm\sqrt{(\pm\sqrt{2}+2)(\pm\sqrt{3}+3)}$. Quindi a è radice del polinomio a coefficienti razionali

$$\prod_i (x - a_i).$$

Mostrando che $a \notin E$ e che tutti i coniugati di a stanno in L possiamo concludere che L è di Galois su $\mathbb{Q}$. Consideriamo ora come agiscono gli automorfismi visti su a; abbiamo che $\sigma(a^2) = \sigma((\sqrt{2}+2)(\sqrt{3}+3)) = (-\sqrt{2}+2)(\sqrt{3}+3)$. Dividendo per a^2 otteniamo:

$$\frac{\sigma(a^2)}{a^2} = \ldots = (\sqrt{2}-1)^2$$

Ma ancora non sappiamo se $[L : E]$ ha grado 2 oppure 1. Se però fosse $a \in E$ avremmo allora che $\sigma(a)$ dovrebbe valere $\pm(\sqrt{2}-1)a$ (per il conto appena fatto) e in questo caso avremmo che $\sigma^2(a) = -a$, assurdo, visto che σ ha ordine 2. Abbiamo quindi che il grado dell'estensione $[L : \mathbb{Q}]$ è proprio uguale a 8.
Dobbiamo ancora far vedere che tutti i coniugati di a stanno in L. Il calcolo precedente ci dice che se ci troviamo in un campo in cui abbiamo $\sqrt{2}, \sqrt{3}$ e a (e ovviamente abbiamo $-a$), allora anche $(-\sqrt{2}+2)(\sqrt{3}+3)$ è un quadrato, dunque abbiamo trovato 2 coniugati di a. Per trovare gli altri 4 coniugati basta vedere (calcolo analogo) che $\tau(a^2)/a^2$ e $(\sigma \circ \tau)(a^2)/$ sono quadrati in E.
Dobbiamo ancora mostrare che il gruppo di Galois di L su $\mathbb{Q}$ è uguale a $\mathcal{Q}_8$, per farlo mostriamo che ci sono due elementi di ordine 4 che non commutano tra di loro.
Sappiamo per la teoria che possiamo estendere σ e τ ad automorfismi di $Gal\left(L/\mathbb{Q}\right)$ che chiameremo s e t. Sappiamo che

$$s(a) = \pm(\sqrt{2}-1)a \implies s^2(a) = -a \implies s^4(a) = a$$

Abbiamo dunque che s ha ordine almeno 4 in L. Possiamo portare avanti un ragionamento del tutto analogo per t, infatti

$$\frac{\tau(a^2)}{a^2} = \left(\frac{3-\sqrt{3}}{\sqrt{6}}\right)^2 \implies o(t) = 4$$

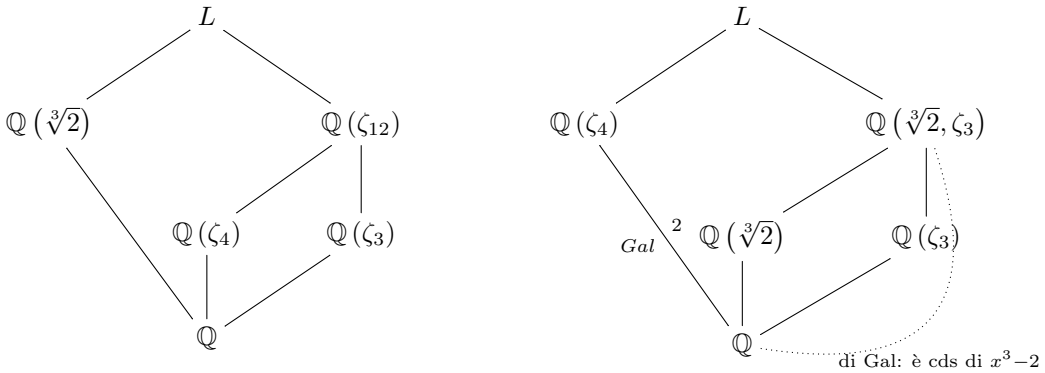
Ma abbiamo che s e t non commutano, infatti:

$$st(a) = \left(\frac{3-\sqrt{3}}{-\sqrt{6}}\right)\left(\sqrt{2}-1\right)a$$
$$ts(a) = \left(\frac{3-\sqrt{3}}{\sqrt{6}}\right)\left(\sqrt{2}-1\right)a$$

Quindi abbiamo elementi di ordine 4 che non commutano tra di loro e quindi l'unico gruppo al quale può essere isomorfo G è il gruppo dei quaternioni.

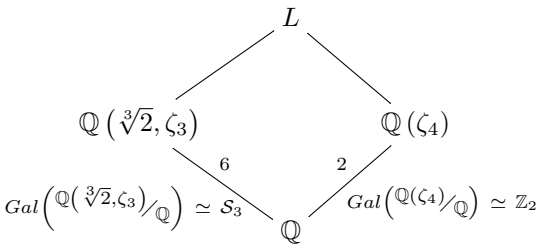
Esercizio 14. Consideriamo $\mathbb{Q}(\zeta_p)$ con p primo. Questa contiene un'unica sottoestensione di grado 2 su $\mathbb{Q}$. Dire, al variare di p, se questa è un'estensione reale.

Esercizio 15. Sia $L = \mathbb{Q}\left(\zeta_{12}, \sqrt[3]{2}\right)$. Mostrare che questa è un'estensione di Galois e trovarne il gruppo.
Sia intanto $a = \sqrt[3]{2}$, il polinomio minimo di a sarà dunque $x^3 - 2$, le cui radici sono $a,\ \zeta_3 a,\ \zeta_3^2 a$. Fino a questo punto possiamo vedere quindi la situazione in almeno due modi differenti:



Ma ζ_3 ha grado 2 su $\mathbb{Q}$, mentre invece $\sqrt[3]{2}$ ha grado 3, quindi $\mathbb{Q}\left(\zeta_3, \sqrt[3]{2}\right)$ è un'estensione di $\mathbb{Q}$ di grado 6; inoltre queste due si intersecano solamente in $\mathbb{Q}$ infatti $\mathbb{Q}(\zeta_3)$ non ha componenti reali, a parte $\mathbb{Q}$. Possiamo comunque riflettere sul fatto che quello che stiamo analizzando è il campo di spezzamento di un polinomio di grado 3, dunque il suo gruppo di Galois deve essere sottogruppo di $\mathcal{S}_3$, ma l'unico sottogruppo di $\mathcal{S}_3$ di cardinalità 6 è $\mathcal{S}_3$ stesso.
Abbiamo quindi a questo punto che $\mathbb{Q}(\zeta_3)$ corrisponde al campo fisso dell'unico sottogruppo normale di indice 2 di $Gal\left(\mathbb{Q}\left(\sqrt[3]{2}, \zeta_3\right)/\mathbb{Q}\right)$.
Ma dobbiamo ancora considerare ζ_4. Per quanto appena detto, visto che $\mathbb{Q}(\zeta_3)$ è l'unica sottoestensione di grado 2 di $\mathbb{Q}\left(\zeta_3, \sqrt[3]{2}\right)$, abbiamo che $\mathbb{Q}(\zeta_4) \cap \mathbb{Q}\left(\zeta_3, \sqrt[3]{2}\right) = \mathbb{Q}(\zeta_4) \cap \mathbb{Q}(\zeta_3)$. Vediamo immediatamente che $\mathbb{Q}(\zeta_4) \cap \mathbb{Q}(\zeta_3) = \mathbb{Q}$, infatti sono estensioni di gradi primi tra di loro inoltre $\mathbb{Q}(\zeta_4)$ è un'estensione di Galois su

$\mathbb{Q}$. Abbiamo quindi la situazione:



Visto che l'intersezione tra le due è banale e le estensioni basse sono di Galois possiamo concludere che $Gal\left(L/\mathbb{Q}\right) \simeq \mathcal{S}_3 \times \mathbb{Z}_2$.

4 Lezione del 6/12

Riflessione 1. Sia $\mathbb{Q} \subseteq F = \mathbb{Q}\left(\sqrt{2},\sqrt{3}\right) \subseteq K = \mathbb{Q}\left(\sqrt{2},\sqrt{3},a\right)$ una torre di estensioni di campi tale che K sia di Galois su F e F sia di Galois su $\mathbb{Q}$.
In generale non è per nulla detto che se la parte alta e la parte bassa di una torre di estensione sono di Galois allora tutta l'estensione sia di Galois. Un controesempio ci è dato da $\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt{2}\right) \subseteq \sqrt[4]{2}$, infatti $\mathbb{Q}\left(\sqrt[4]{2}\right)$ non è un'estensione di Galois di $\mathbb{Q}$, mentre inceve lo sono $\mathbb{Q}\left(\sqrt{2}\right)$ di $\mathbb{Q}$ e $\mathbb{Q}\left(\sqrt[4]{2}\right)$ di $\mathbb{Q}\left(\sqrt{2}\right)$.
Ma nel caso specifico, se prendiamo $a = \sqrt{(\sqrt{2}+2)(\sqrt{3}+3)}$, la cosa funziona, infatti tutti i coniugati a' di a, sono tali che i quozienti a^2/a'^2 sono quadrati in $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$, per esempio:

$$\frac{a}{a'} = \sqrt{\frac{\sqrt{2}+2}{-\sqrt{2}+2}} \in \mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$$

Questo ci dice che una volta aggiunta la radice a abbiamo anche aggiunto tutti i suoi coniugati.

Introduciamo una notazione prima di addentrarci nel prossimo esercizio, dato p un numero primo e a un intero qualsiasi, introduciamo il simbolo di Legendre, che vale:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 \iff p \mid a \\ 1 \iff \exists k \mid k^2 \equiv a \ (p) \\ -1 \iff \nexists k \mid k^2 \equiv a \ (p) \end{cases}$$

Esercizio 16. Sia $K = \mathbb{Q}\left(\zeta_n\right)$. Abbiamo già detto che l'estenione è di Galois con gruppo di Galois $G = Gal\left(K/\mathbb{Q}\right) \simeq \mathbb{Z}_n^*$. Se n è primo abbiamo che G è ciclico, e dunque contiene un solo sottogruppo di indice 2, sia N questo sottogruppo. Ci chiediamo chi è K^N, l'unico sottocampo di K di grado 2 su $\mathbb{Q}$. Chiamiamo allora $S = \sum_{i=1}^{p-1} \left(\frac{i}{p}\right) \zeta_p^i \in \mathbb{Q}\left(\zeta_p\right)$, ci chiediamo allora chi sia S^2.

Possiamo dire:

$$\begin{aligned}
S^2 &= \sum_{i=1}^{p-1}\sum_{j=1}^{p-1}\left(\frac{i}{p}\right)\left(\frac{j}{p}\right)\zeta_p^{i+j} = \sum_{i,j=1}^{p-1}\left(\frac{ij}{p}\right)\zeta_p^{i+j} \\
&\overset{j=ik}{=} \sum_{i=1}^{p-1}\sum_{k=1}^{p-1}\left(\frac{i^2k}{p}\right)\zeta_p^{i+ik} = \sum_{k,i=1}^{p-1}\left(\frac{k}{p}\right)\zeta_p^{(k+1)i} \\
&= \sum_{k=1}^{p-1}\left(\frac{k}{p}\right)\sum_{i=1}^{p-1}\zeta_p^{(k+1)i} \\
&\overset{*}{=} -\sum_{k=1}^{p-2}\left(\frac{k}{p}\right) + \left(\frac{-1}{p}\right)(p-1) \\
&= -\sum_{k=1}^{p-1}\left(\frac{k}{p}\right) + p\left(\frac{-1}{p}\right) \overset{**}{=} p\left(\frac{-1}{p}\right)
\end{aligned}$$

Dove:

- $*$ è dovuto al fatto che se $p \mid k+1$ otteniamo $p-1$, altrimenti abbiamo tutte le radici tranne 1, otteniamo in questo caso -1. Abbiamo comunque l'uguaglianza indicata.
- $**$ è dovuto al fatto che $\sum_{k=1}^{p-1}\left(\frac{k}{p}\right) = 0$

Abbiamo quindi solo due casi possibili:

- Se -1 è un quadrato in $\mathbb{Z}_p$ allora l'unica sottoestensione di grado 2 su $\mathbb{Q}$ di $\mathbb{Q}(\zeta_p)$ è $\mathbb{Q}\left(\sqrt{p}\right)$.
- Se 1 non è un quadrato modulo p allora l'unica sottoestensione di grado 2 su $\mathbb{Q}$ di $\mathbb{Q}(\mathbb{Z}_p)$ è $\mathbb{Q}(\sqrt{-p})$.

Esercizio 17. Sia $p(x) = x^4 - 4x^2 + 6$. Ci chiediamo allora, detto K il campo di spezzamento di $p(x)$ su $\mathbb{Q}$:

- Chi sono i sottocampi di K di grado 2 su $\mathbb{Q}$?
- A cosa è isomorfo $Gal\left(K/\mathbb{Q}\right)$?

Definizione 1. Sia $p(x) \in F[x]$ un polinomio in un campo a caratteristica 0. Si dice che $p(x)$ è risolubile per radicali se, detto K il campo di spezzamento di $p(x)$ su F, esistono delle estensioni del tipo:

$$F = F_0 \subseteq F_1 = F_0(a_1) \subseteq \ldots \subseteq F_n = F_{n-1}(a_n) = L \quad t.c.\ K \subseteq L$$

tali che $\exists h_1, \ldots, h_n \in \mathbb{N}$ tali che $\forall i \in \{1, \ldots, n\},\ a_i^{h_i} \in F_{i-1}$. Diciamo cioè che un polinomio è risolubile per radicali se il suo campo di spezzamento è sottocampo di un'estensione L che può essere scritta come una catena di estensioni semplici F_i, ciascuna delle quali è data dall'aggiunta di una radice h_i esima di un elemento di F_{i-1}.

Osservazione 1. Per decidere se un polinomio è risolubile per radicali, possiamo supporre che il campo di partenza contenga tutte le radici dell'unità che possono servire. Ovvero se $p(x)$ è risolubile per radicali in un campo F di caratteristica 0 che abbia certe radici dell'unità, allora è risolubile anche su F privato delle radici dell'unità e viceversa. Cioè se F non contiene le radici m-esime dell'unità e $p(x)$ è risolubile per radicali in $F(\zeta_m)$, allora è risolubile per radicali anche su F.

Osservazione 2. Se $p(x)$ è risolubile per radicali su F possiamo sempre supporre che la catenza di risoluzione

$$F = F_0 \subseteq F_1 \subseteq \ldots \subseteq F_n = L \supseteq K$$

sia tale che L sia di Galois su F. Sia infatti $F_0 \subseteq F_1 = F_0(a_1)$ tale che $a_1^{h_1} = a_0 \in F_0$. Se questa estensione non è di Galois allora sia g_1 il polinomio minimo di a_1 su F_0, allora $g_1 \mid x^{h_1} - b_0 \in F_0[x]$, siano allora $a_{1,1}, \ldots, a_{1,s_1}$ le altre radici di g_1. Allora possiamo dire che:

$$F_0 \subseteq F_0(a_1) \subseteq F_0(a_1, a_{1,1}) \subseteq \ldots \subseteq F_0(a_1, a_{1,1}, \ldots, a_{1,s_1})$$

Queste estensioni sono tutte del tipo che stavamo cercando, perché ciascuno degli elementi con cui abbiamo esteso il campo precedente è radice h_1-esima di qualche elemento appartenente al campo precedente. Ciascuna di queste estensioni è risolubile, inoltre l'estensione grande è di Galois su F_0.
Possiamo quindi andare avanti, stando sempre attenti al fatto che vogliamo sempre avere estensioni che siano campi di spezzamento. Continueremo quindi come:

$$F_0 \subseteq F_0(a_1, a_{1,1}, \ldots, a_{1,s_1}) = \overline{F_1} \subseteq \overline{F_1}(a_2)$$

Sia ora g_2 il polinomio minimo di a_2 su F_1, sappiamo quindi che esiste h_2 tale che $a_2^{h_2} = b_1 \in F_1$, continuiamo aggiungendo tutte le radici di g_2, otteniamo quindi:

$$\overline{F_1}(a_2) \subseteq \overline{F_1}(a_2, a_{2,1}) \subseteq \ldots \subseteq \overline{F_1}(a_2, a_{2,1}, \ldots, a_{2,s_2})$$

Tutto quello che costruiamo ci porta ad estensioni di Galois, visto che continuiamo ad espandere il campo base con campi di spezzamento di polinomi. Inoltre ogni estensione è per radicali, infatti $g_i \mid x^{h_i} - a_i$. Possiamo dunque enunciare il seguente Teorema.

Teorema 1. *Sia $p(x) \in F[x]$ un polinomio risolubile per radicali. Sia K il campo di spezzamento di $p(x)$ su F. Allora $G = Gal\left({}^{K}\!/_{F}\right)$ è un gruppo risolubile (e quindi risolubile per commutatori), abbiamo infatti che esiste una successione del tipo:*

$$G = G_0 \triangleright G_1 \triangleright \ldots \triangleright \{e\}$$

in cui il quoziente di due termini consecutivi è un gruppo abeliano.

Dimostrazione.

- Osserviamo innanzitutto che che un sottogruppo di un gruppo risolubile è risolubile. Infatti se $G = G_0 \triangleright G_1 \triangleright \ldots \triangleright \{e\}$ e $H < G$, detto $H_i = H \cap G_i$, abbiamo che ${}^{H_i}\!/_{H_{i+1}}$ è sottogruppo di ${}^{G_i}\!/_{G_{i+1}}$, quindi è abeliano.

- Quozienti di gruppi risolubili sono risolubili. Se infatti abbiamo un'omomorfismo surgettivo $G \xrightarrow{\phi} H$ allora è vero anche che ${}^{H_i}\!/_{H_{i+1}} = \phi\left({}^{G_i}\!/_{G_{i+1}}\right)$, dunque anche i vari quozienti ${}^{H_i}\!/_{H_{i+1}}$ sono abeliani.

Abbiamo anche visto che possiamo supporre che tutte le radici dell'unità che ci sono necessarie siano già appartenenti a F. A questo punto utilizziamo il seguente

Lemma 1. *Se un campo F contiene ζ_n e $a \in F$ elemento non nullo; se K è campo di spezzamento di $x^n - a$ allora:*

- *$K = F(u)$ con u radice di $x^n - a$.*
- *$Gal\left({}^{K}\!/_{F}\right)$ è abeliano.*

Dimostrazione del Lemma. Se u è una radice del polinomio, sono radici anche $u\zeta_n, \ldots, u\zeta_n^{n-1}$, tutte radici distinte che quindi generano il campo di spezzamento. Ma allora ogni elemento di $Gal\left({}^{K}\!/_{F}\right)$ è determinato da dove viene mandato u, che però è costretto ad andare in un'altra delle radici del polinomio; quindi data $\sigma \in Gal\left({}^{K}\!/_{F}\right)$ deve essere che $\sigma(u) = u\zeta_n^i$. Ma allora non è difficile vedere che questi automorfismi commutano, e quindi $Gal\left({}^{K}\!/_{F}\right)$ è un gruppo commutativo e un sottogruppo di $\mathbb{Z}_n^*$. □

Abbiamo quindi la catena che conosciamo di estensioni (L è il campo dell'Oss. 2, pag. 16):

$$F_0 \subseteq F_1 \subseteq \ldots \subseteq F_n = L$$

A questo punto sappiamo che $G = Gal\left({}^{L}\!/_{F}\right)$ è risolubile, abbiamo infatti:

$$G > Gal\left({}^{L}\!/_{F_1}\right) > Gal\left({}^{L}\!/_{F_2}\right) > \ldots > Gal\left({}^{L}\!/_{L}\right)$$

Possiamo sempre supporre che F_i sia un'estensione normale di F_{i-1} e quindi

$$Gal\left({}^{F_i}\!/_{F_{i-1}}\right) \simeq {}^{Gal\left({}^{L}\!/_{F_{i-1}}\right)}\!/_{Gal\left({}^{L}\!/_{F_i}\right)} \qquad Gal\left({}^{K}\!/_{F}\right) = {}^{Gal\left({}^{L}\!/_{F}\right)}\!/_{Gal\left({}^{L}\!/_{K}\right)}$$

Dunque sappiamo che $Gal\left({}^{L}\!/_{F}\right)$ è risolubile e quindi anche che $Gal\left({}^{K}\!/_{F}\right)$ è risolubile, in quanto quoziente di risolubili. □

Viceversa vedremo che se il gruppo di Galois del campo di spezzamento di $p(x)$ è risolubile, allora banalmente $p(x)$ è risolubile per radicali.

Esempio 2. A questo punto possiamo dire, sapendo che $\mathcal{S}_5$ non è risolubile, che se $p(x)$ è tale che il gruppo di Galois del suo campo di spezzamento su $\mathbb{Q}$ è isomorfo a $\mathcal{S}_5$, allora $p(x)$ non ha una formula per radicali delle sue radici, ovvero non è risolubile per radicali.

5 Lezione del 9/12

Lemma 2. *Sia K campo e $\sigma_1, \ldots, \sigma_n$ elementi di $\mathcal{A}ut(K)$ distinti. Sappiamo che, dato un insieme qualsiasi X, l'insieme delle funzioni da X a K è un K-spazio vettoriale. Diciamo allora che, se $\sigma_1, \ldots, \sigma_n$ sono distinti tra di loro, sono linearmente indipendenti, cioè $\nexists \lambda_1, \ldots, \lambda_n$ non tutti nulli tali che*

$$\lambda_1\sigma_1 + \ldots + \lambda_n\sigma_n = 0$$

Dimostrazione. Sia $\lambda_1\sigma_1 + \ldots + \lambda_m\sigma_m = 0$ una combinazione nulla di lunghezza minima a coefficienti non tutti nulli (in particolare nessun coefficiente può essere nullo, altrimenti esisterebbe una combinazione nulla di lunghezza minore).
i) $m \neq 1$, infatti la funzione nulla non è un automorfismo.
ii) Sia allora $m > 1$, abbiamo allora che $\exists c \in K$ tale che $\sigma_2(c) \neq \sigma_1(c)$ (altrimenti i due automorfismi sarebbero uguali). Abbiamo allora che:

1) $\sum_{i=1}^{m} \lambda_i\sigma_i(ac) = 0 \implies \sum_{i=1}^{m} \lambda_i\sigma_i(a)\sigma_i(c) = 0.$

2) $\sum_{i=1}^{m} \lambda_i\sigma_i(a) = 0 \implies \sigma_1(c)\,(\sum_{i=1}^{m} \lambda_i\sigma_i(a) = 0) = 0$

Questi due punti insieme ci permettono di dire che

$$\sum_{i=2}^{m} \lambda_i(\sigma_i(c) - \sigma_1(c))\sigma_i(a) = 0$$

Ma questo è assurdo, abbiamo infatti trovato una combinazione nulla di lunghezza minore della lunghezza della minima combinazione nulla. □

Teorema 2. *Se K è campo di spezzamento su F di un polinomio $p(x)$ e $G = Gal\left(K/F\right)$ è risolubile, allora è risolubile per radicali.*

Dimostrazione. Abbiamo già visto che possiamo supporre che F contenga le radici dell'unità. Visto che G è risolubile abbiamo certamente una catena del tipo:

$$G = G_0 \triangleright G_1 \triangleright \ldots \triangleright G_n = \{e\}$$

Quindi possiamo dire che:

$$K = K^{G_n} = F_n \supseteq F_{n-1} = K^{G_{n-1}} \supseteq \ldots \supseteq F_{n-i} = K^{G_{n-i}} \supseteq \ldots \supseteq K^G = F_0 = F$$

Visto che possiamo supporre che il quoziente di due gruppi successivi è ciclico, abbiamo che $Gal\left(F_k/F_{k-1}\right)$ è anch'esso ciclico. Abbiamo infatti:

$$Gal\left(F_n/F_{n-i}\right) = G_{n-i} \triangleright G_{n-i+1} = Gal\left(F_n/F_{m-i+1}\right)$$

Quindi F_{n-i} è di Galois su F_{n-i+1} e il suo gruppo di Galois è ciclico e dato da G_{n-1}/G_{n-i+1}.
Allora il teorema è dimostrato se facciamo vedere che è vera la proposizione:

$$Gal\left(K/F\right) \text{ ciclico} \implies K = F(\omega) \text{ t.c. } \omega^n \in F$$

Dimostrazione. Sia $Gal\left(K/F\right) = \mathbb{Z}_n$ e sia $\zeta_n \in F$ (lo avevamo tra le ipotesi). Sia σ un generatore di $Gal\left(K/F\right)$. Abbiamo allora che $id, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ sono elementi distinti degli automorfismi di K, sono quindi linearmente indipendenti. Abbiamo quindi che non è nulla la funzione

$$\psi = id_K + \zeta_n^{-1}\sigma + \zeta_n^{-2}\sigma^2 + \ldots + \zeta_n^{-n+1}\sigma^{n-1}$$

Ma allora deve esistere un elemento b in K tale che $\psi(b) = a \neq 0$. Abbiamo allora che:

$$\begin{aligned}\sigma(a) &= \sigma(b) + \zeta_n^{-1}\sigma^2(b) + \ldots + \zeta_n^{n+1}\sigma^n(b)\\ &= \zeta_n\left(b + \zeta_n^{-}1\sigma(b) + \ldots + \zeta_n^{-n+1}\sigma^{n-1}(b)\right)\\ &= \zeta_n a\end{aligned}$$

Quindi $\sigma(a) = \zeta_n a, \ldots, \sigma^{n-1}(a) = \zeta_n^{n-1}a$ sono tutti elementi distinti. Quindi il polinomio minimo di a su F ha grado almeno n. Ma $a \in K$ e $[K : F] = n$. Quindi $K = F(a)$ per questioni di grado. Inoltre $a^n \in F$. Infatti abbiamo che:

$$a \cdot \sigma(a) \cdot \sigma^2(a) \cdot \cdots \cdot \sigma^{n-1}(a) \in G$$

Infatti questo elemento è invariante per σ. Ma in particolare è uguale a

$$a \cdot \zeta_n \cdot a \cdot \zeta_n^2 \cdot a \cdot \ldots \cdot \zeta_n^{n-1} \cdot a = a^n \zeta_n^{\binom{n}{2}}$$

Ma $\binom{n}{2}$ è multiplo di n se n è primo.
Ma per avere gruppi ciclici di ordine primo possiamo sempre spezzare i quozienti, possiamo cioè ricondurci al caso in cui G_i/G_{i+1} sia ciclico di ordine primo. □

□

Esercizio 18. Sia $p(x) = x^4 - 4x^2 + 6$ trovare il gruppo di Galois e le sottoestensioni quadratiche.
Sia K il campo di spezzamento di $p(x)$ con $K = \mathbb{Q}\left(\sqrt{\Delta}, \sqrt{t}, a\right)$ con t il termine noto e a una radice del polinomio. Abbiamo quindi in questo caso $K = \mathbb{Q}\left(\sqrt{-2}, \sqrt{6}, \sqrt{2+\sqrt{-2}}\right)$ Quindi abbiamo che $\sqrt{-2}$ e $\sqrt{6}$ sono sufficienti a creare un'estensione di Galois di grado 4 che è campo di spezzamento di $(x^2+2)(x^2-6)$. Il gruppo di Galois di questa estensione è $\mathbb{Z}_2^2$, contiene infatti due sottoestensioni di grado due. Ma non sappiamo ancora se $a \in \mathbb{Q}\left(\sqrt{-2}, \sqrt{6}\right)$; chi può essere allora $Gal\left(K/\mathbb{Q}\right)$? Ci sono due possibilità:

- $a \in \mathbb{Q}\left(\sqrt{-2}, \sqrt{6}\right) \implies Gal\left(K/\mathbb{Q}\right) \simeq \mathbb{Z}_2^2$.
- $a \notin \mathbb{Q}\left(\sqrt{-2}, \sqrt{6}\right) \implies Gal\left(K/\mathbb{Q}\right)$ è un gruppo di grado 8 contenuto in $\mathcal{D}_4$, deve essere quindi $\mathcal{D}_4$ stesso.

Nel primo caso le sottoestensioni sono date dai 3 sottocampi di indice 2, corrispondono quindi ai campi fissi dei 3 sottogruppi di incice due in $\mathbb{Z}_2^2$. Possiamo prendere 3 generatori di questi sottogruppi:

$$\sigma_1 : \begin{cases}\sqrt{-2} \mapsto -\sqrt{-2}\\ \sqrt{6} \mapsto \sqrt{6}\end{cases} \qquad \sigma_2 : \begin{cases}\sqrt{-2} \mapsto \sqrt{-2}\\ \sqrt{6} \mapsto -\sqrt{6}\end{cases} \qquad \sigma_3 : \begin{cases}\sqrt{-2} \mapsto -\sqrt{-2}\\ \sqrt{6} \mapsto -\sqrt{6}\end{cases}$$

Abbiamo quindi:

$$K^{<\sigma_1>} = \mathbb{Q}\left(\sqrt{6}\right) \qquad K^{<\sigma_2>} = \mathbb{Q}\left(\sqrt{-2}\right) \qquad K^{<\sigma_3>} = \mathbb{Q}\left(\sqrt{-3}\right)$$

L'ultima cosa che ci resta da fare è veramente chiederci se $a \in \mathbb{Q}\left(\sqrt{-2}, \sqrt{6}\right)$; infatti in entrambi i casi abbiamo che ci sono solo 3 sottocampi di grado 2 su $\mathbb{Q}$, e li abbiamo già trovati.
Un modo per vedere se $a \in \mathbb{Q}\left(\sqrt{-2}, \sqrt{6}\right)$ è utilizzare la forza bruta. Ci chiediamo infatti se è possibile scrivere a come:

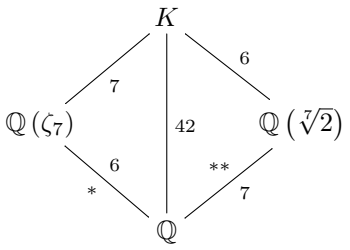
$$a = \alpha + \beta\sqrt{-2} + \gamma\sqrt{6} + \delta\sqrt{-3}$$

Un altro modo per vedere l'appartenenza è considerare il fatto che $a^2 = 2 + \sqrt{-2}$ e quindi che $\sigma_2(a^2) = a^2$, quindi deve essere che, se $a \in \mathbb{Q}\left(\sqrt{-2}, \sqrt{6}\right)$, si deve avere $\sigma_2(a) = \pm a$, quindi a dovrebbe appartenere all'autospazio di $+1$ o all'autospazio di -1 dell'automorfismo σ_2. Ma l'autospazio relativo a 1 di σ_2 è generato da 1 e $\sqrt{-2}$, mentre l'autospazio relativo a -1 è generato da $\sqrt{6}, \sqrt{-3}$. Si vede facilmente che entrambi i casi sono non hanno soluzione, quindi $a \notin \mathbb{Q}\left(\sqrt{-2}, \sqrt{6}\right)$ e il gruppo di Galois è D_4.

Esercizio 19. Sia $p(x) = x^7 - 2$.

- Trovare il campo di spezzamento di $p(x)$ su $\mathbb{Q}$.
- $[K \cap \mathbb{R} : \mathbb{Q}] = ?$.
- $K \cap \mathbb{R}$ è di Galois su $\mathbb{Q}$?
- Qual'è il massimo sottocampo di $K \cap \mathbb{R}$ che sia a sua volta di Galois su $\mathbb{Q}$?

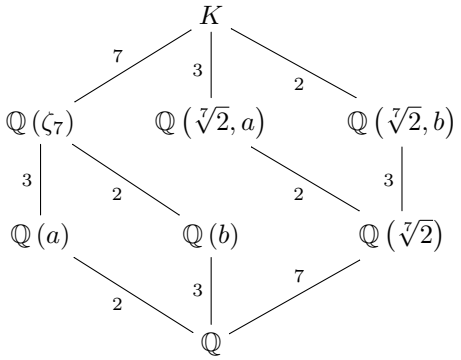
Sappiamo dire intanto che $\mathbb{Q}\left(\sqrt[7]{2}, \zeta_7\right) \subseteq K$, visto che sappiamo che le radici di $p(x)$ sono $\sqrt[7]{2}$, $\sqrt[7]{2}\zeta_7, \ldots, \sqrt[7]{2}\zeta_7^6$. Possiamo intanto fare delle prime considerazioni:



Avendo inteso per:

- $*$ Questa estensione è di Galois, vale quindi che $Gal\left(K/\mathbb{Q}(\zeta_7)\right)$ è sottogruppo normale di $Gal\left(K/\mathbb{Q}\right)$ che quindi ha certamente un sottogruppo normale di ordine 7. Inoltre ha un sottogruppo non normale di ordine 6.
- $**$ Questa estensione non è di Galois, visto che $\mathbb{Q}\left(\sqrt[7]{2}\right)$ non è campo di spezzamento di alcun polinomio in $\mathbb{Q}$.

Ma questa divisione ci fa sospettare della possibile esistenza di estensioni intermedie. Non possiamo cioè escludere che avvenga qualcosa del tipo:



In realtà sappiamo che queste sottoestensioni esistono, visto che il gruppo $Gal\left(\mathbb{Q}(\zeta_7)/\mathbb{Q}\right) \simeq \mathbb{Z}_6$ che ha due sottogruppi. Chi è dunque $K \cap \mathbb{R}$? Dobbiamo prendere gli elementi fissati dal coniugio ristretto al nostro campo. Il ramo dell'estensione generato da $\sqrt[7]{2}$ non ci crea problemi, visto che $\sqrt[7]{2}$ è reale. Dobbiamo quindi vedere se esistono sottoestensioni reali di $\mathbb{Q}(\zeta_7)$, se questa esiste deve essere fissata dal coniugio, che è l'automorfismo di $Gal\left(\zeta_7/\mathbb{Q}\right)$ di ordine 2. Un elemento fissato da questo automorfismo è per esempio $\zeta_7 + \zeta_7^{-1}$; abbiamo quindi che $\mathbb{Q}\left(\sqrt[7]{2}, \zeta_7 + \zeta_7^{-1}\right) \subseteq K \cap \mathbb{R}$ e inoltre ha grado 21 su $\mathbb{Q}$. Questa estensione è la massima possibile in $\mathbb{R}$. Consideriamo a questo punto che $K \cap \mathbb{R}$ non è di Galois su $\mathbb{Q}$, infatti $\sqrt[7]{2} \in K \cap \mathbb{R}$, ma $K \cap \mathbb{R}$ non contiene un campo di spezzamento del polinomio minimo di $\sqrt[7]{2}$.
Cerchiamo di analizzare meglio $Gal\left(K/\mathbb{Q}\right)$. Sappiamo che i suoi elementi sono tutti e soli gli automorfismi ϕ della forma:

$$\phi : \begin{cases} \sqrt[7]{2} \mapsto \zeta_7^i \sqrt[7]{2} \\ \zeta_7 \mapsto \zeta_7^j \end{cases} \qquad con\ (j,7) = 1,\ i_1^7$$

Abbiamo quindi che $G \simeq \mathbb{Z}_7 \rtimes \mathbb{Z}_7^*$; più esplicitamente possiamo scrivere:

$$G = \left\{ \phi : \begin{cases} \sqrt[7]{2} \mapsto \zeta_7^i \sqrt[7]{2} \\ \zeta_7 \mapsto \zeta_7 \end{cases} \right\} \rtimes \left\{ \psi : \begin{cases} \sqrt[7]{2} \mapsto \sqrt[7]{2} \\ \zeta_7 \mapsto \zeta_7^j \end{cases} \right\}$$

Cercando un sottogruppo normale che contenga il coniugio (che corrisponderebbe ad un'estensione di Galois in $\mathbb{R}$) troviamo che un sottogruppo di questo tipo dovrebbe avere almeno $2 \cdot 7$ elementi (infatti deve contenere il coniugio, che è un elemento di ordine 2 e deve contenere il prodotto del coniugio per un suo coniugato, e si può facilmente vedere che un tale elemento ha ordine 7) e deve avere indice al massimo 3. Il suo campo fisso è dunque un'estensione normale di $\mathbb{Q}$ di grado 3, reale e conosciamo già un'estensione con queste caratteristiche, ovvero $\mathbb{Q}\left(\zeta_7 + \zeta_7^{-1}\right)$, deve quindi essere quella cercata.

6 Lezione del 13/12

Proposizione 3. *$\forall p$ primo, $n \neq 0 \in \mathbb{N}$, $\exists! K$ campo di cardinalità p^n, questo viene chiamato $\mathbb{F}_{p^n}$ ed è il campo di spezzamento di $x^{p^n} - x$ su $\mathbb{F}_p$. Gli elementi*

di $\mathbb{F}_{p^n}$ sono tutte e sole le radici distinte di questo polinomio. Ogni campo finito è isomorfo a uno di questi $\mathbb{F}_{p^n}$.

Riflessione 2. Come sono fatti i gruppi di automorfismi di questi campi? Dati $m, n \geq 1,\ n \mid m$, vorremmo sapere:

- Vale che $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m}$?
- $Gal\left(\mathbb{F}_{p^m} \diagup \mathbb{F}_{p^n}\right)$ a cosa è isomorfo?

Il primo punto è vero. Infatti i polinomi di cui sono campi di spezzamento sono uno divisore dell'altro.

Proposizione 4. *Se K è un campo di caratteristica p chiamiamo ϕ l'automorfismo di Frobenius. Diciamo che $Gal\left(\mathbb{F}_{p^n} \diagup \mathbb{F}_{p}\right) =< \phi >$, gruppo ciclico di ordine n.*

Dimostrazione. Sappiamo innanzitutto che $\phi^n = id$, infatti ogni elemento di $\mathbb{F}_{p^n}$ è radice di $x^{p^n} - x$. Abbiamo quindi che l'ordine di ϕ divide n, ma se l'ordine fosse strettamente minore (diciamo d) avremmo che $x^{p^d} = x,\ \forall x \in \mathbb{F}_{p^n}$. Ma questo non è possibile, infatti l'equazione ha al massimo p^d soluzioni. □

Corollario. *Dati $n, m \geq 1,\ t.c.\ n \mid m$ abbiamo $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m}$, inoltre $\mathbb{F}_{p^n}$ è il sottocampo fissato da ϕ^n quindi $\mathbb{F}_{p^m}$ è un'estensione normale e separabile di $\mathbb{F}_{p^m}$, dunque il gruppo di Galois è*

$$Gal\left(\mathbb{F}_{p^m} \diagup \mathbb{F}_{p^n}\right) =< \phi^n > \ \simeq\ \mathbb{Z}_{\frac{m}{n}}$$

Riflessione 3. Cerchiamo adesso di costruire un campo algebricamente chiuso a caratteristica p. Partiamo da $\mathbb{F}_p$, vogliamo che il nostro campo contenga le radici di $f(x)$ per ogni $f(x) \in \mathbb{F}_p[x]$. Sappiamo però che $\forall f(x) \in \mathbb{F}_p[x]$ esiste un n tale che $\mathbb{F}_{p^n}$ è campo di spezzamento di $f(x)$ su $\mathbb{F}_p$. A questo punto osserviamo che vale la catena di inclusioni:

$$\mathbb{F}_p \subseteq \mathbb{F}_{p^{2!}} \subseteq \mathbb{F}_{p^{3!}} \subseteq \ldots \mathbb{F}_{p^{i!}} \subseteq \ldots \subseteq \ldots$$

Possiamo quindi definire

$$\overline{\mathbb{F}}_p = \bigcup_{i \in \mathbb{N}} \mathbb{F}_{p^{i!}}$$

Proposizione 5. *$\overline{\mathbb{F}}_p$ è un campo algebricamente chiuso di caratteristica p, inoltre $\mathbb{F}_{p^n} \subseteq \overline{\mathbb{F}}_p, \forall n \in \mathbb{N}$.*

Dimostrazione. In realtà questa affermazione è banale, vediamone comunque i vari punti.

- $\forall x, y \in \overline{\mathbb{F}}_p,\ \exists m, n \in \mathbb{N}\ t.c.\ x \in \mathbb{F}_{p^m},\ y \in \mathbb{F}_{p^n} \implies x, y \in \mathbb{F}_{p^{(m+n)!}}$. Ma in $\mathbb{F}_{p^{(m+n)!}}$, e quindi in $\overline{\mathbb{F}}_p$, questi elementi hanno una somma, un prodotto ed un inverso e tutte le operazioni che possiamo fare con questi due elementi godono delle proprietà dei campi.
- Dato $f(x) \in \overline{\mathbb{F}}_p[x]$, questo avrà un numero finito di coefficienti, esiste dunque un n abbastanza grande tale che $f(x) \in \mathbb{F}_{p^{n!}}$, a questo punto il campo di spezzamento di $f(x)$ su questo campo è un'estensione finita, è quindi contenuta in $\mathbb{F}_{p^{N!}}$ per qualche $N \geq n$ sufficientemente grande. Quindi in $\overline{\mathbb{F}}_p$ abbiamo tutte le radici di $f(x)$.

□

Corollario. *La chiusura algebrica di $\mathbb{F}_p$ è numerabile, è infatti unione numerabile di insiemi finiti.*

Riflessione 4. Chi sono gli automorfismi di $\overline{\mathbb{F}}_p$? $\forall n,\ \mathbb{F}_{p^n} \subseteq \overline{\mathbb{F}}_p$, possiamo quindi certamente prendere un automorfismo di $\overline{\mathbb{F}}_p$ e restringerlo ad un automorfismo di $\mathbb{F}_{p^n}$ per ottenere questa mappa:

$$G = Gal\left(\overline{\mathbb{F}}_p \big/ \mathbb{F}_p\right) \xrightarrow{\rho_n} Gal\left(\mathbb{F}_{p^n} \big/ \mathbb{F}_p\right) = \mathbb{Z}_n$$

Quello che abbiamo trovato è un omomorfismo surgettivo (infatti per esempio l'automorfismo di Frobenius è un elemento di G la cui immagine genera $Gal\left(\mathbb{F}_{p^n} \big/ \mathbb{F}_p\right)$). Vorremmo quindi studiare meglio la natura di G, per farlo consideriamo un'altra mappa, ispirata alla precedente, che speriamo essere iniettiva:

$$G \xrightarrow{\Pi_{\rho_n}} \prod_{n\in\mathbb{N}} \mathbb{Z}_n$$

Vorremmo dire che questo omomorfismo è iniettivo, ma questo è vero, indatti dato un elemento $\sigma \in G$ diverso dall'identità, deve esistere $x \in \overline{\mathbb{F}}_p$ tale che $\sigma(x) \neq x$. Ma allora $x \in \mathbb{F}_{p^{n!}}$ per qualche n e quindi $\rho_n(\sigma) \neq id$. Questa mappa però non è surgettiva, infatti se abbiamo che $m \mid n$ deve essere commutativo il diagramma:

$$\begin{array}{ccc} G & \xrightarrow{\rho_n} & \mathbb{Z}_n \\ & \searrow^{\rho_m} & \downarrow \tau \\ & & \mathbb{Z}_m \end{array}$$

Con τ l'omomorfismo che manda l'automorfismo di Frobenius nell'automorfismo di Frobenius del gruppo di arrivo. Gli elementi dell'immagine di $\prod \rho_n$ sono delle successioni $(\sigma_n)_{n\in\mathbb{N}}$ tali che se $m \mid n$ che σ_m proiettato su n dia proprio σ_n.

Definizione 2. Dato un insieme parzialmente ordinato $(I, \prec)$, diciamo che esso è un insieme diretto se $\forall i_1, i_2 \in I,\ \exists j \in I\ t.c. i_1 \prec j, i_2 \prec j$.

Esempio 3. Per esempio $\mathbb{N}$ è un insieme diretto con l'ordine parziale: $n \prec m \iff n \mid m$.

Definizione 3. Supponimo di avere su I insieme diretto una famiglia di gruppi $\{G_i\}_{i\in I}$ e una famiglia di funzioni $\{\phi_{i,j}\}_{\substack{i,j\in I \\ i\prec j}}$ con $\phi_{ij} \in Hom(G_j, G_i)$. Se $\phi_{ij} \circ \phi_{jk} = \phi_{ik},\ \forall i \prec j \prec k$, e se inoltre $\phi_{ii} = e_{G_i}$, allora diciamo che $\left(\{G_i\}_{i\in I}, \{\phi_{i,j}\}_{\substack{i,j\in I \\ i\prec j}}\right)$ è un sistema inverso.

Se I è un insieme diretto e $\left(\{G_i\}_{i\in I}, \{\phi_{i,j}\}_{\substack{i,j\in I \\ i\prec j}}\right)$ un sistema inverso su I, allora definiamo:

$$\varprojlim G_n = D = \left\{(x_i)_{i\in I} \in \prod_{i\in I} G_i\ t.c.\ \phi_{ij}(x_j) = x_i,\ \forall i \prec j\right\}$$

il limite inverso di $\{G_i\}_{i\in I}, \{\phi_{i,j}\}_{\substack{i,j\in I \\ i\prec j}}$.

Riflessione 5. Riprendendo l'esempio di prima, avevamo osservato la mappa

$$\mathcal{A}ut\left(\overline{\mathbb{F}}_p\right) \xrightarrow{\prod \rho_n} \prod_{n\in\mathbb{N}} G_i = \prod_{n\in\mathbb{N}} \mathcal{A}ut\left(\mathbb{F}_{p^n}\right)$$

Come abbiamo detto questa mappa è iniettiva, inoltre la sua immagine è contenuta nel limite inverso dei $\{G_i\} = \{\mathbb{Z}_i\}$; in realtà l'immagine è proprio il limite inverso. Infatti se $\{\sigma_n\}_{n\in\mathbb{N}}$ appartiene al limite inverso di

$$\lim_{\leftarrow} Gal\left(\mathbb{F}_{p^n}\diagup\mathbb{F}_p\right)$$

allora definisce, $\forall N$, un elemento di $Gal\left(\mathbb{F}_{p^N}\diagup\mathbb{F}_p\right)$, inoltre se $N \mid m$ allora σ_m si restringe a σ_N. Quindi $\{\sigma_n\}$ definisce un automorfismo di

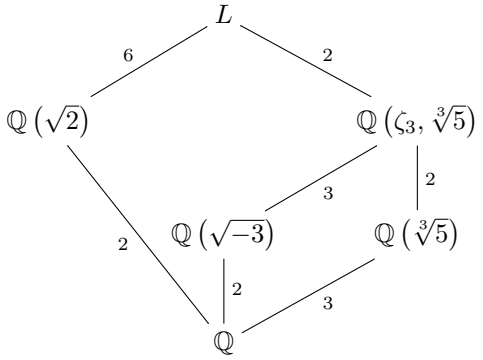
$$\bigcup_{n\in\mathbb{N}} \mathbb{F}_{p^n} = \bigcup_{m\in\mathbb{N}} \mathbb{F}_{p^{m!}}$$

dove possiamo considerare tutti i campi dell'unione a sinistra come sottocampi dell'unione a destra ed è quindi facile vedere che le due unioni coincidono.

Esercizio 20. Sia $K = \mathbb{Q}\left(\sqrt{2}, \sqrt{-3}, \sqrt[3]{5}\right)$. Cerchiamo di capire:

- se K è estensione di Galois su $\mathbb{Q}$.
- quanto vale $Gal\left(K\diagup\mathbb{Q}\right)$.
- quali sono i sottogruppi normali del gruppo di Galois (e quindi quali sono le sottoestensioni di Galois).

Possiamo sospettare che in qualche modo ci possa interessare il polinomio $p(x) = (x^3-5)(x^2-2)(x^2+3)$; sappiamo infatti che K è certamente contenuto in un campo di spezzamento di $p(x)$, inoltre K è di Galois se e solo se è proprio uguale a quel campo di spezzamento, infatti contiene delle radici di tutti e tre i polinomi irriducibili che lo compongono, se non ne contenesse qualcuna non potrebbe essere campo di spezzamento di un polinomio separabile. Comunque ci viene in aiuto il fatto che $\zeta_3 = -\frac{1}{2} + \iota\frac{\sqrt{3}}{2}$, quindi un'estensione che contenga $\sqrt{-3}$, come K, contiene anche le radici terze dell'unità, e quindi se contiene una radice di un polinomio irriducibile di terzo grado deve contenere anche le altre. Quindi abbiamo che K è il campo di spezzamento di $p(x)$.
Possiamo a questo punto chiederci chi è il gruppo di Galois di K su $\mathbb{Q}$. Ci troviamo in una situazione del tipo:



Sappiamo diverse cose a proposito dei vari gruppi di Galois e della situazione delle sottoestensioni:

- Non ci sono intersezioni non banali tra $\mathbb{Q}\left(\sqrt{2}\right)$ e $\mathbb{Q}\left(\zeta_3, \sqrt[3]{5}\right) = L$
- Per mostrare il punto precedente possiamo chiederci chi sono le sottoestensioni di grado 2 dentro $\mathbb{Q}\left(\zeta_3, \sqrt[3]{5}\right)$). Sappiamo che $Gal\left(L/\mathbb{Q}\right)$ ha cardinalità 6 e ha un sottogruppo non normale (visto che $\mathbb{Q}\left(\sqrt[3]{5}\right)$ non è un'estensione di Galois); deve essere quindi per forza $\mathcal{S}_3$, ma allora abbiamo che esiste un unico sottogruppo di indice 2 (il cui campo fisso a questo punto sappiamo essere $\mathbb{Q}\left(\sqrt{-3}\right)$).
- Possiamo quindi dire che $L \cap \mathbb{Q}\left(\sqrt{2}\right)$ può avere solo grado 1 o 2 su $\mathbb{Q}$, ma se avesse grado 2 su $\mathbb{Q}$ e fosse contenuta in L dovrebbe essere $\mathbb{Q}\left(\sqrt{-3}\right)$, ma sappiamo che non è vero. Abbiamo quindi intersezione banale.
- Possiamo quindi ora dire tranquillamente che $[K : \mathbb{Q}]$ ha grado 12 e il suo gruppo di Galois è dato da

$$Gal\left(K/\mathbb{Q}\right) = Gal\left(\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}\right) \times Gal\left(L/\mathbb{Q}\right) \simeq \mathbb{Z}_2 \times \mathcal{S}_3$$

Proviamo ora a scrivere esplicitamente dei generatori di $Gal\left(K/\mathbb{Q}\right)$, per farlo cerchiamo τ generatore di $\mathbb{Z}_2 \times \{e\}$ e poi σ, ρ dei generatori di $\{e\} \times \mathcal{S}_3$. Prendiamo quindi:

$$\tau : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt[3]{5} \mapsto \sqrt[3]{5} \\ \zeta_3 \mapsto \zeta_3 \end{cases} \qquad \sigma : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt[3]{5} \mapsto \zeta_3 \sqrt[3]{5} \\ \zeta_3 \mapsto \zeta_3 \end{cases} \qquad \rho : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt[3]{5} \mapsto \sqrt[3]{5} \\ \zeta_3 \mapsto \zeta_3^{-1} \end{cases}$$

Possiamo a questo punto trovare tutti i 7 sottogruppi normali di $\mathbb{Z}_2 \times \mathcal{S}_3$ (compresi quelli banali) e individuare quali sono i loro campi fissi.

Esercizio 21. Sia E campo di spezzamento di $x^8 - 2$ su $\mathbb{Q}$.

- Trovare il suo gruppo di Galois su $\mathbb{Q}$.
- Trovare dei generatori del gruppo di Galois.
- Dette $a = \sqrt[8]{2}$ e $b = \zeta_8$ mostrare che il gruppo di Galois G contiene θ e σ tali che: $\theta(a) = ba$, inoltre $\theta(\iota) = \iota$. Ma anche $\sigma(a) = a$ e $\sigma(\iota) = -\iota$.
- Fatto questo trovare i sottocampi fissati da: $< \theta >, < \theta^2 >, < \theta^4 >, < \sigma >$, $< \sigma, \theta^4 >$.