Capitolo 7: Teoria di Galois:

Teoria di Galois:

Sia E estensione normale di K (Si indica anche con E/K), L chiusura di algebrica di K.
Studieremo i gruppi di Galois per ricavare informazioni sull'estensione.

Definizione (Estensione normale):

Sono caratterizzazione equivalenti:

1. E/K è un'estensione normale
2. E è il campo di spezzamento su K di un polinomio di $K[x]$
3. Ogni automorfismo di L che lasci fisso K manda E in se stesso.

Proprietà:

Sia E un'estensione normale di un campo K ; F un campo intermedio | $K \subseteq F \subseteq E$, allora E/F è un'estensione normale.

Osservazione:

F/K in generale non è normale.

Se G è un'altra estensione normale di K allora EG/K ; $E \cap G/K$ sono estensioni normali.

Osservazione:

Vale $[E_1E_2 : K] = [E_1 : K] \cdot [E_2 : K]$

Tutti i campi di spezzamento sono estensioni normali.
La chiusura algebrica è sempre un'estensione normale.
Tutte le estensioni di grado 2 sono normali.

Esempio:

$\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ è un'estensione normale in quanto campo di spezzamento de polinomio $x^2 - 2 \in \mathbb{Q}[x]$

$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ non è un'estensione normale in quanto il polinomio minimo in $\mathbb{Q}$ di $\sqrt[3]{2}$ è $x^3 - 2$ e $\mathbb{Q}(\sqrt[3]{2})$ non contiene le altre due radici di questo polinomio (Idea intuitiva, non banale formalizzarlo)

Teorema dell'elemento primitivo:

Sia K campo, se E/K un'estensione finita, allora $\exists \alpha \in E \mid E = K(\alpha)$.

Definizione (Gruppo di Galois):

È il gruppo formato dagli omomorfismi da E/K a $L \mid K$ resti invariato.

$G = Gal(E/K) = \mathrm{Hom}(E, L) \mid \sigma_{|K} = \mathrm{Id}$

Equivalente:

$Gal(E/K) = \{f \in \mathrm{Aut}(E) \ f_{|K} = \mathrm{Id}_K\}$

Osservazione:

$|Gal(E/K)| = [E:K]$

Esempi:

$Gal(\mathbb{C}/\mathbb{R}) = \{\mathrm{Id}, \bar{f} \mid f(i) = -i\}$

$Gal(\mathbb{Q}(\sqrt{2}, \xi_3)/\mathbb{Q}) \cong S_3$

$Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{\mathrm{Id}, f \mid f(\sqrt{2}) = -\sqrt{2}\}$

L'idea è di vedere come $\mathbb{Q}$-spazio vettoriale $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ e considerare l'insieme delle sue radici ricordandosi che possono solamente scambiarsi fra loro mantenendo la struttura in quanto automorfismo. In questo caso sono $\{1, \sqrt{2}, -\sqrt{2}\}$ e gli unici automorfismi sono quelli prima descritti.

Importante:

Gli automorfismi del gruppo di Galois devono preservare ogni combinazione algebrica che dia come risultato un valore in K (In quanto quel valore è fissato dall'automorfismo per ipotesi).
Dunque date A, B radici per ricavare esplicitamente il gruppo di Galois si verificano i valori di $A + B$; AB ; $etc.$

Teorema:

Sia $E = K(\alpha_1, \dots, \alpha_n)$ campo di spezzamento di $f(x) \in K[x]$ irriducibile.
Allora $Gal(E/K) \cong H < S_n$.

Costruzione:

Sia $\sigma \in G$ agisce sull'insieme delle radici di $f(x)$ come una permutazione, quindi $\forall\, i \leq n\ \sigma(a_i) = a_{\lambda(i)}$ con $\lambda \in S_n$.

Corollario:

$|Gal(E/K)| \mid n!$

Proposizione:

Sia E/K un'estensione normale; $G = Gal(E/K)$; $\mathrm{Fix}(G) = \{x \in E \mid \forall \sigma \in G: \sigma(x) = x\} = K$

Teorema (Campi finiti):

Il gruppo di Galois $Gal\left(\mathbb{F}_{p^n}/\mathbb{F}_p\right)$ è ciclico di grado *n* ed è generato dall'automorfismo di Frobenius

$\phi: \mathbb{F}_{p^n} \to \overline{\mathbb{F}_p} \mid \forall x \in \mathbb{F}_{p^n}\ \phi(x) = x^p$

Osservazione:

$Gal\left(\mathbb{F}_{p^n}/\mathbb{F}_{p^m}\right) < Gal\left(\mathbb{F}_{p^n}/\mathbb{F}_p\right)$ quindi sono tutti generati dall'automorfismo:

$\sigma(x) = x^{p^m}$

Corrispondenza di Galois:

Idea:

Mettere in corrispondenza biunivoca i campi intermedi $F \mid K \subseteq F \subseteq E$ e i sottogruppi di $G = Gal(E/K)$.

$\to_\lambda$ Ad ogni F posso assegnare il sottogruppo $Gal(E/F)$.

$\leftarrow_\mu$ $\forall H < G$ associo il campo intermedio $\mathrm{Fix}(H) = \{x \in E \mid \forall \sigma \in H: \sigma(x) = x\}$

Attenzione:

Stare attenti a cosa associamo ad un sottogruppo. L'estensione con cui stiamo lavorando (Quella da associare) è della forma $F/K \to$ è di grado 2 se $[F:K] = 2$ NON se $[E:F] = 2$

Quindi un'estensione di grado 2 avrà sottogruppo di Galois associato di dimensione $\frac{|G|}{2}$

Proposizione:

$\lambda \circ \mu = \mu \circ \lambda = \mathrm{Id}$

Proposizione (Quando un'estensione intermedia è normale):

$K \subseteq F \subseteq E$ campi, E/K estensione normale allora:

F/K è un'estensione normale $\leftrightarrow H = Gal(E/F) \lhd G$

Osservazione (Abeliano):

Se un gruppo di Galois ha un sottogruppo non normale (Quindi una sottoestensione associata non normale) non può essere abeliano.

Corollario:

Sia E/K un'estensione normale, F campo intermedio e $H = Gal(E/F) < Gal(E/K)$

Se F/K è un'estensione normale (Dunque $Gal(E/F) \lhd Gal(E/K)$

Allora $Gal(F/K) \cong {}^{G}/_{H}$

Osservazione interessante:

Se non sappiamo distinguere fra $Galois \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ e $Galois \cong \mathbb{Z}_4$ mi basta mostrare che ∃! Estensione di grado 2 → ∃! Sottogruppo isomorfo a $\mathbb{Z}_2 \to Galois \cong \mathbb{Z}_4$

Prodotti diretti e gruppi di Galois:
Se abbiamo un polinomio dato dal prodotto di due polinomi distinti, chiamate E_1, E_2 i campi di spezzamento dei due polinomi. Se $E_1 \cap E_2 = K$; $E_1 E_2 = E$, con E il c.d.s dell'intero polinomio, allora $Gal(E/K) \cong Gal(E_1/K) \times Gal(E_2/K)$

Osservazione 1 (Estensioni ciclotomiche):
Per ogni estensione ciclotomica $\mathbb{Q}(\xi_n)/\mathbb{Q}$ allora il suo gruppo di Galois è isomorfo a $(\mathbb{Z}_n)^*$

Si può controllare a cosa sia isomorfo studiandone esplicitamente gli elementi.

Esempio:
$Gal(\mathbb{Q}(\xi_{15})/\mathbb{Q}) \cong (\mathbb{Z}_{15})^* \cong (\mathbb{Z}_5)^* \times (\mathbb{Z}_3)^* \cong \mathbb{Z}_4 \times \mathbb{Z}_2$

Osservazione 2 (Estensioni ciclotomiche):
Per ogni estensione ciclotomica $\mathbb{Q}(\xi_n)/\mathbb{Q}$ allora $\mathbb{Q}(\xi_n + \xi_n^{-1})$ non solo è un'estensione reale ma è la più grande fra quelle reali. Di conseguenza possiamo sfruttare questo fatto per capire quando l'intersezione fra un'estensione ciclotomica e un'altra estensione si riduce a $\mathbb{Q}$.
Per fare questo possiamo anche studiare il grado di $\mathbb{Q}(\xi_n + \xi_n^{-1})$ considerando che sarà minore di quello di $\mathbb{Q}(\xi_n)$ e un fattore 2 (La parte complessa) deve essere dato da $\mathbb{Q}(\xi_n)/\mathbb{Q}(\xi_n + \xi_n^{-1})$

Esempio 1:
$\mathbb{Q}(\xi_6 + \xi_6^{-1}) \subseteq \mathbb{Q}(\xi_6)$ e siccome $[\mathbb{Q}(\xi_6) : \mathbb{Q}] = 6 \to [\mathbb{Q}(\xi_6 + \xi_6^{-1}) : \mathbb{Q}] = 3$
Ricordiamoci che vale la catena $\mathbb{Q}(\xi_3) \subseteq \mathbb{Q}(\xi_6)$ oppure $\mathbb{Q}(\xi_3) \subseteq \mathbb{Q}(\xi_9)$

Esempio 2:
Studiamo $\mathbb{Q}(\xi_{11}, \sqrt{2})$, vogliamo ricavarne il gruppo di Galois.
Osserviamo che $\mathbb{Q}(\xi_{11}, \sqrt{2}) = \mathbb{Q}(\xi_{11})\mathbb{Q}(\sqrt{2})$. Sappiamo che
$Gal(\mathbb{Q}(\xi_{11})/\mathbb{Q}) \cong \mathbb{Z}_{10}$; $Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong \mathbb{Z}_2$
Concludiamo mostrando che $\mathbb{Q}(\xi_{11}) \cap \mathbb{Q}(\sqrt{2}) = \mathbb{Q}$; essendo $\mathbb{Q}(\sqrt{2})$ reale questa è infatti equivalente a:
$\mathbb{Q}(\xi_{11} + \xi_{11}^{-1}) \cap \mathbb{Q}(\sqrt{2})$
Per il discorso precedente $\mathbb{Q}(\xi_{11} + \xi_{11}^{-1})$ è un'estensione di grado 5 e $\sqrt{2}$ è un elemento di grado 2 che non può appartenere ad un'estensione di grado 5.
Quindi $Gal(\mathbb{Q}(\xi_{11}, \sqrt{2})/\mathbb{Q}) \cong \mathbb{Z}_{10} \times \mathbb{Z}_2$

Approfondimento Estensioni Ciclotomiche:

Proposizione GG:
Tutti gli elementi della forma $x_1 + \cdots + x_n$ con $\{x_1, \dots, x_n\}$ classe di equivalenza per f sono punti fissi di un automorfismo f di un gruppo generato da una radice p-esima dell'unità

Idea :
Se $\{x_1, \dots, x_n\}$ è una classe di equivalenza per f allora:
$f(x_1 + \cdots + x_n) = f(x_1) + \cdots + f(x_n) = x_{\sigma(1)} + \cdots + x_{\sigma(n)}$ con σ permutazione degli elementi.

Idea applicazione:
Possiamo sfruttare questa proposizione per costruire in maniera esplicita un'estensione di grado fissato.

Esempio applicazione teorema:
Consideriamo $Gal(K/\mathbb{Q})$ con K C.d.S. di $x^7 - 1$. Vogliamo individuare in maniera esplicita un'estensione quadratica.
Sappiamo già che $Gal(K/\mathbb{Q}) \cong (\mathbb{Z}_7)^* \cong \mathbb{Z}_6$
Quindi stiamo cercando l'estensione associata al sottogruppo di ordine 3 in $Gal(K/\mathbb{Q})$.
Un sottogruppo di ordine 3 significa individuare i due automorfismi di ordine 3 e capire cosa sono gli elementi da essi fissati.

Osservazione 1:
Studiare uno dei due è come studiare l'altro perché appartenendo entrambi allo stesso sottogruppo di ordine 3 (Ciclico) devono essere l'uno generato dall'altro, quindi fissano gli stessi punti.

Idea:
Ricordiamo che gli automorfismi delle radici p-esime dell'unità sono tutti e soli quelli della forma $f(\zeta_p) = \zeta_p^n$ con n coprimo con p.

Dunque studiamo in $(\mathbb{Z}_7)^*$ quali sono gli elementi con ordine moltiplicativo 3:
2 in quanto $2 \to 4 \to 1$ e 4 poiché $4 \to 2 \to 1$ che sono associati agli automorfismo: $f(x) = x^2$; $g(x) = x^4$

Ma allora prendiamo tutte le radici settime dell'unità e le suddividiamo per classe di equivalenza per uno dei due automorfismi (Per l'Osservazione 1 le due funzioni danno la stessa partizione delle radici).
$Cl_1 = \{\zeta_7^1, \zeta_7^2, \zeta_7^4\}$; $Cl_2 = \{\zeta_7^3, \zeta_7^6, \zeta_7^5\}$

Per la Proposizione GG $\zeta_7^1 + \zeta_7^2 + \zeta_7^4$ e $\zeta_7^3 + \zeta_7^6 + \zeta_7^5$ sono due punti fissati da f.

Quindi le due estensioni $\mathbb{Q}(\zeta_7^1 + \zeta_7^2 + \zeta_7^4)$; $\mathbb{Q}(\zeta_7^3 + \zeta_7^6 + \zeta_7^5)$ sono di Galois e fissate da f.
Per l'osservazione 2 le estensioni coincidono.

Osservazione 2:
Quando dobbiamo verificare che due estensioni coincidano abbiamo i due seguenti strumenti:

1. Sfruttando i risultati noti dalla teoria di Galois, in questo caso sappiamo che essendoci solo un sottogruppo di $Gal(K/\mathbb{Q})$ di ordine 3 può esserci solamente un'estensione quadratica di Galois, quindi $\mathbb{Q}(\zeta_7^1+\zeta_7^2+\zeta_7^4) = \mathbb{Q}(\zeta_7^3+\zeta_7^6+\zeta_7^5)$
2. Sfruttando la definizione di punto fisso e il fatto che se x è punto fisso per f omomorfismo allora $f(x^{-1}) = f(x)^{-1} = x^{-1}$ è punto fisso per f. Quindi in questo caso siccome ne ho solo due devono essere l'uno l'inversa dell'altra (Verificabile facilmente anche in maniera diretta) e dunque le due estensioni coincidono.

Osservazione 3:
Possono esserci anche 3 o più classi, ad esempio basta considerare sempre su questo stesso gruppo di Galois una g di ordine 2. Le classi di equivalenza saranno:

$$Cl_1 = \{\zeta_7^1, \zeta_7^{-1}\}; Cl_2 = \{\zeta_7^2, \zeta_7^{-2}\}; Cl_3 = \{\zeta_7^3, \zeta_7^{-3}\}$$

E le tre estensioni $\mathbb{Q}(\zeta_7^1+\zeta_7^{-1})$; $\mathbb{Q}(\zeta_7^2+\zeta_7^{-2})$; $\mathbb{Q}(\zeta_7^3+\zeta_7^{-3})$coincidono per semplice verifica diretta.

Esempio: $(\zeta_7^1+\zeta_7^{-1})^2 - 2 = \zeta_7^2+\zeta_7^{-2}$

<u>Applicazione interessante:</u>
È possibile sfruttare le osservazioni fatte fino ad ora per individuare il polinomio minimo di uno degli elementi che caratterizzano questa estensione. Il polinomio minimo spesso ci permette di caratterizzare in maniera più semplice l'estensione.

Esempio:
Cerchiamo il polinomio minimo di $\zeta_7^1+\zeta_7^{-1}$, dalla teoria di Galois sappiamo che $\mathbb{Q}(\zeta_7^1+\zeta_7^{-1})$ ha grado 3 su $\mathbb{Q}$, questo ci assicura che il polinomio minimo cercato abbia grado esattamente 3.
Scriviamo le potenze successive di $\zeta_7^1+\zeta_7^{-1}$:
$1; x = \zeta_7^1+\zeta_7^{-1}; x^2 = (\zeta_7^1+\zeta_7^{-1})^2 = \zeta_7^2+\zeta_7^{-2}+2; x^3 = (\zeta_7^1+\zeta_7^{-1})^3 = \zeta_7^3+\zeta_7^{-3}+3(\zeta_7^1+\zeta_7^{-1})$
Ma allora:

$$x^3 = \zeta_7^3+\zeta_7^{-3}+3(\zeta_7^1+\zeta_7^{-1})$$
$$x^3+x^2 = \zeta_7^3+\zeta_7^{-3}+3(\zeta_7^1+\zeta_7^{-1})+\zeta_7^2+\zeta_7^{-2}+2$$
$$x^3+x^2-2x = \zeta_7^3+\zeta_7^{-3}+\zeta_7^1+\zeta_7^{-1}+\zeta_7^2+\zeta_7^{-2}+2 = \zeta_7^6+\zeta_7^5+\cdots+\zeta_7^1+2 = 1$$
$$x^3+x^2-2x-1 = 0$$

Quindi il polinomio minimo di $\zeta_7^1+\zeta_7^{-1}$ è $p(x) = x^3+x^2-2x-1$

Osservazione 4:
Per risolvere questo sistema possiamo sfruttare la proprietà delle radici p-esime:
$\zeta_7^{p-1}+\zeta_7^{p-2}+\cdots+\zeta_7^1+1 = 0$

Osservazione 5:
Il polinomio minimo può essere utilizzato per semplificare la scrittura di un'estensione.
Nel caso sia possibile ricavarne le radici (Ad esempio se il polinomio è di secondo grado) l'unica componente della soluzione che $\notin \mathbb{Q}$ sarà quella sotto radice.

Conclusione esempio:

Mostriamo che nell'esempio precedente la ricerca del polinomio semplifica la scrittura dell'estensione: $\mathbb{Q}(\zeta_7^1+\zeta_7^2+\zeta_7^4)$ ha grado 2 su $\mathbb{Q}$ quindi mi basta ricercare un polinomio di secondo grado.

$$1; x=\zeta_7^1+\zeta_7^2+\zeta_7^4; x^2=\zeta_7^1+\zeta_7^2+\zeta_7^4+2\left(\zeta_7^3+\zeta_7^5+\zeta_7^6\right)$$

Allora:

$$x^2=\zeta_7^1+\zeta_7^2+\zeta_7^4+2\left(\zeta_7^3+\zeta_7^5+\zeta_7^6\right)$$
$$x^2+x=2\left(\zeta_7^1+\zeta_7^2+\zeta_7^4+\zeta_7^3+\zeta_7^5+\zeta_7^6\right)$$
$$x^2+x+2=2\left(\zeta_7^1+\zeta_7^2+\zeta_7^3+\zeta_7^4+\zeta_7^5+\zeta_7^6+1\right)=0$$

Quindi il polinomio minimo di $\zeta_7^1+\zeta_7^2+\zeta_7^4$ è x^2+x+2

Le cui radici sono: $\frac{-1\pm\sqrt{1-8}}{2}$ quindi:

$$\mathbb{Q}(\zeta_7^1+\zeta_7^2+\zeta_7^4)=\mathbb{Q}\left(\frac{-1+\sqrt{1-8}}{2};\frac{-1-\sqrt{1-8}}{2}\right)=\mathbb{Q}\left(\sqrt{-7}\right)$$

Esempi ed esercizi:

Esempio 0 (<u>Risultati noti</u>):

Il gruppo di Galois del campo di spezzamento di $x^4 - 2$ è: $G\left(\mathbb{Q}\left(\sqrt[4]{2}, i\right)/\mathbb{Q}\right) \cong \mathbb{Z}_4 \rtimes \mathbb{Z}_2 \cong D_4$

In generale $[\mathbb{Q}(\xi_m): \mathbb{Q}] = \Phi(m)$

Esempio 1 (<u>Gruppo di Galois dato un polinomio</u>):

Determinare esplicitamente il Gruppo di Galois del campo di spezzamento del polinomio $x^2 - 4x + 1$ su $\mathbb{Q}$

Ricaviamo le radici di questo polinomio: $\begin{cases} A = 2 + \sqrt{3} \\ B = 2 - \sqrt{3} \end{cases}$

Osserviamo che $A + B = 4 \in \mathbb{Q}$; $AB = 1 \in \mathbb{Q}$ → Ogni automorfismo deve preservare queste due operazioni.

Per un risultato di teoria $\left|Gal\left(\mathbb{Q}\left(\sqrt{3}\right)/\mathbb{Q}\right)\right| = \left[\mathbb{Q}\left(\sqrt{3}\right) : \mathbb{Q}\right] = 2$

L'identità ovviamente va bene e per verifica sulle operazioni precedenti anche $f \mid f(A) = B$ rispetta quelle operazioni.

Dunque $Gal\left(\mathbb{Q}\left(\sqrt{3}\right)/\mathbb{Q}\right) = \{\mathrm{Id}, f\}$

Attenzione (Su quali equazioni verificare):

Non prendo equazioni della forma $A + 3B$ perché il risultato non appartiene a $\mathbb{Q}$ e non prendo equazioni della forma $A - B - 2\sqrt{3}$ perché $\notin \mathbb{Q}[x]$

In generale:

Dato un polinomio di secondo grado su $\mathbb{Q}[x]$:

Se ha una sola radice o due radici appartenenti a $\mathbb{Q}$ il gruppo di Galois è sempre banale.

Se ha due radici non appartenenti a $\mathbb{Q}$ allora il gruppo di Galois è sempre della forma $\{\mathrm{Id}, f\}$ come prima.

Esempio 2 (<u>Gruppo di Galois dato un polinomio</u>):

Determinare esplicitamente il Gruppo di Galois del campo di spezzamento del polinomio $x^4 - 10x^2 + 1$ su $\mathbb{Q}$

Le radici sono: $\begin{cases} A = \sqrt{2} + \sqrt{3} \\ B = \sqrt{2} - \sqrt{3} \\ C = -\sqrt{2} + \sqrt{3} \\ D = -\sqrt{2} - \sqrt{3} \end{cases}$

Il mio automorfismo deve rispettare ogni composizione algebrica con risultato in $\mathbb{Q}$; ad esempio $A + D = 0$; $(A + B)^2 = 8$

Un esempio di automorfismo che non la rispetta è $f \mid f(A, B, C, D) = (A, B, D, C)$

Per la teoria: $|Gal(\mathbb{Q}(A, B, C, D)/\mathbb{Q})| = 4$

Continuando ad eliminare (è più facile eliminare una permutazione che dimostrare che una rispetta tutte le composizioni algebriche) rimangono:

$\mathrm{Id}, f(A, B, C, D) = (C, D, A, B)$; $f(A, B, C, D) = (B, A, D, C)$; $f(A, B, C, D) = (D, C, B, A)$

Che è isomorfo al gruppi di Klein.

Esempio 3:

Calcolare il grado del campo di spezzamento e il gruppo di Galois di $f(x) = x^3 - 2$ su $\mathbb{Q}$.

Studio del campo di spezzamento:

Individuo le radici di $f(x) \to \left\{\sqrt[3]{2}, \varepsilon_3\sqrt[3]{2}, \varepsilon_3^2\sqrt[3]{2}\right\}$ con $\varepsilon_3 = \frac{-1+i\sqrt{3}}{2}$ con polinomio minimo $x^2 + x + 1$

Il campo di spezzamento sarà $E = \mathbb{Q}(\varepsilon_3, \sqrt[3]{2})$ e siccome deve essere multiplo di tutti i fattori (3 e 2) e minore di 3! con 3 grado del polinomio avremo: $[E : \mathbb{Q}] = 6$

Studio del gruppo di Galois:

Sappiamo che (Avendo il polinomio 3 radici) il gruppo di Galois $Gal(E) < S_3$ quindi $Gal(E) \cong S_3$

Come è fatto? (Utile per poter costruirlo al contrario)

Cerco i sottogruppi di G

$\{\mathrm{Id}\}$; G ; il 3-ciclo $H = \{\mathrm{Id}, (123), (321)\}$; i 3 gruppi generati dalle trasposizioni $M_1 = \{\mathrm{Id}, (12)\}$; $M_2 = \{\mathrm{Id}, (23)\}$; $M_3 = \{\mathrm{Id}, (13)\}$

Li associo ai campi secondo la corrispondenza di Galois:

$\{\mathrm{Id}\} \to$ tutto ciò che viene fissato da Id, tutto E.

$G \to$ ciò che è fissato da tutto, ossia $\mathbb{Q}$

M_1 ; M_2 ; $M_3 \to$ lasciano fissi $\mathbb{Q}\left(\varepsilon_3^2\sqrt[3]{2}\right)$; $\mathbb{Q}\left(\sqrt[3]{2}\right)$; $\mathbb{Q}\left(\varepsilon_3\sqrt[3]{2}\right)$

Per capire cosa viene associato ad H osserviamo che $\left|Gal(E/_{\mathbb{Q}(\varepsilon_3)}\right| = 3 = |H| \to H$ lo associamo a $\mathbb{Q}(\varepsilon_3)$.

Esempio 4:

Calcolare il grado del campo di spezzamento e il gruppo di Galois di $(x^3+1)(x^3-5)$ su $\mathbb{Q}$.

Studio del campo di spezzamento:

Studiamo i due diversi fattori:

$(x^3+1) = (x-1)(x^2-x+1)$ su $\mathbb{Q}$.

(x^3-5) è irriducibile per Eisenstein.

Scriviamo la fattorizzazione in irriducibili:

$f(x) = (x-1)(x^2-x+1)(x^3-5)$

Individuiamo le radici dei fattori irriducibili:

$$(x^2-x+1) \to \left\{\frac{1+i\sqrt{3}}{2}, \frac{1-i\sqrt{3}}{2}\right\}$$
$$(x^3-5) \to \left\{\sqrt[3]{5}, \varepsilon_3\sqrt[3]{5}, \varepsilon_3^2\sqrt[3]{5}\right\}$$

Il campo di spezzamento è quindi (eliminando ciò che può essere ottenuto dal campo $\mathbb{Q}$):

$E = \mathbb{Q}\left(i\sqrt{3}, \sqrt[3]{5}, \varepsilon_3\right)$

Cerchiamo di eliminare ciò che può essere ottenuto da un altro fattore, in questo caso:

$\varepsilon_3 = \frac{-1+i\sqrt{3}}{2} \to \mathbb{Q}\left(i\sqrt{3}\right) = \mathbb{Q}(\varepsilon_3)$

Quindi $E = \mathbb{Q}\left(\varepsilon_3, \sqrt[3]{5}\right)$

Individuiamo i gradi dei polinomi minimi (Per $\sqrt[3]{5}$ è 3 mentre per ε_3 è 2).

Quindi per il teorema di estensioni per torri, siccome le due estensioni non coincidono essendo una reale e l'altra immaginaria vale:

$$\left[\mathbb{Q}\left(\varepsilon_3, \sqrt[3]{5}\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\varepsilon_3, \sqrt[3]{5}\right) : \mathbb{Q}\left(\sqrt[3]{5}\right)\right] \cdot \left[\mathbb{Q}\left(\sqrt[3]{5}\right) : \mathbb{Q}\right] = 6$$

Studio del gruppo di Galois:

G è isomorfo ad un sottogruppo di S_3 in quanto permuta le radici di (x^3-5)

G ha cardinalità uguale al grado dell'estensione (6), quindi $G = S_3$

Esempio 4 bis:

Calcolare il grado del campo di spezzamento e il gruppo di Galois di $(x^3+1)(x^3-5)$ su $\mathbb{F}$.

Studio del campo di spezzamento:

Calcoliamo i possibili valori per x^3:

$$\begin{cases} 1^3=1 \\ 2^3=1 \\ 3^3=6 \\ 4^3=1 \\ 5^3=6 \\ 6^3=6 \end{cases}$$

Scriviamo la fattorizzazione in irriducibili:

$f(x)=(x-3)(x-5)(x-6)(x^3-5)$

Dove (x^3-5) è irriducibile per verifica diretta.

Quindi il grado dell'estensione è $3 \rightarrow E=\mathbb{F}_{7^3}$

Studio del gruppo di Galois:

Il gruppo di Galois ha ordine 3 quindi (A prescindere di quale S_n sia sottogruppo) è isomorfo a $\mathbb{Z}/_{3\mathbb{Z}}$

Notazione:

Un gruppo di Galois di ordine primo *p* sarà isomorfo a $\mathbb{Z}/_{p\mathbb{Z}}$ che verrà indicato con C_p.

Esempio 5 (<u>Studio dell'intersezione fra estensioni</u>):

Se abbiamo le due estensioni (Normali) $\mathbb{Q}(i\sqrt{3},\sqrt[3]{2})$; $\mathbb{Q}(i,\sqrt[4]{2})$ e dobbiamo studiarne l'intersezione (Per ricavare se Galois di entrambe è il prodotto diretto delle due) possiamo osservare che:

Osservazione:

L'intersezione fra estensioni è un'estensione e ha grado che divide quello di entrambe le estensioni.

Dunque siccome: $[\mathbb{Q}(i\sqrt{3},\sqrt[3]{2}):\mathbb{Q}]=6$; $[\mathbb{Q}(i,\sqrt[4]{2}):\mathbb{Q}]=8$ allora l'intersezione può essere di grado 1 o 2.

Se fosse di grado 2 allora siccome sappiamo che $Gal(\mathbb{Q}(i\sqrt{3},\sqrt[3]{2})/\mathbb{Q}) \cong S_3$esiste un unico sottogruppo di cardinalità 3 (Quindi associato ad un'estensione quadratica, precisamente $\mathbb{Q}(i\sqrt{3})$. Ma dunque se fosse davvero questa l'estensione intersezione $\rightarrow i\sqrt{3} \in \mathbb{Q}(i,\sqrt[4]{2})$, Assurdo. Quindi è di grado 1 e $Gal=Gal(\mathbb{Q}(i\sqrt{3},\sqrt[3]{2})/\mathbb{Q}) \times Gal(\mathbb{Q}(i,\sqrt[4]{2})/\mathbb{Q})$

Esempio 6:

Data $\xi_{15} \in \mathbb{C}$ radice 15-esima primitiva dell'unità. Contare le sottoestensioni K di $\mathbb{Q}(\xi_{15})$ di grado 2 ed esprimerle come $\mathbb{Q}(\sqrt{z})$ con $z \in \mathbb{Z}$.

Soluzione:

Osserviamo che il problema è ben posto in quanto $\mathbb{Q}(\xi_{15})$ è un'estensione normale essendo campo di spezzamento del polinomio $x^{15} - 1$.

Ricordando le proprietà delle estensioni ciclotomiche vale:

$|Gal(\mathbb{Q}(\xi_{15})/\mathbb{Q})| = [\mathbb{Q}(\xi_{15}) : \mathbb{Q}] = \Phi(15) = 8$ e $Gal(\mathbb{Q}(\xi_{15})/\mathbb{Q}) \cong (\mathbb{Z}_{15})^* \cong (\mathbb{Z}_5)^* \times (\mathbb{Z}_3)^* \cong$
$\cong \mathbb{Z}_4 \times \mathbb{Z}_2$

La seconda parte del ragionamento ci serve per determinare quali sono le sottoestensioni quadratiche.

Una sottoestensione quadratica K avrà gruppo di Galois associato $Gal(\mathbb{Q}(\xi_{15})/K)$ di cardinalità 4.

In $\mathbb{Z}_4 \times \mathbb{Z}_2$ ci sono 3 sottogruppo di ordine 4. I due ciclici $\langle(1,0)\rangle$; $\langle(1,1)\rangle$ e quello
$\{e, (2,0), (0,1), (2,1)\}$

Osserviamo adesso che $\mathbb{Q}(\xi_{15}) = \mathbb{Q}(\xi_5)\mathbb{Q}(\xi_3)$, infatti $\xi_5 = \xi_{15}^3 \in \mathbb{Q}(\xi_{15})$; $\xi_3 = \xi_{15}^5 \in \mathbb{Q}(\xi_{15})$ e
$\xi_{15} = e^{\frac{2\pi i}{15}} = e^{\frac{2\pi i}{15}(k\cdot 3 + h\cdot 5)} = e^{\frac{2\pi i}{5}(2)} e^{\frac{2\pi i}{3}(-1)} = \xi_5^2 \xi_3^{-1} \in \mathbb{Q}(\xi_5)\mathbb{Q}(\xi_3)$

Studiamo dunque le due estensioni singolarmente:

$\mathbb{Q}(\xi_3)/\mathbb{Q}$ estensione normale in quanto campo di spezzamento di $x^3 - 1$
$[\mathbb{Q}(\xi_3) : \mathbb{Q}] = 2 \to Gal(\mathbb{Q}(\xi_3)/\mathbb{Q}) \cong \mathbb{Z}_2$
Osserviamo che $\mathbb{Q}(\xi_3) = \mathbb{Q}(\sqrt{-3})$ è un'estensione quadratica con $Gal(\mathbb{Q}(\sqrt{-3})/\mathbb{Q}) \cong \mathbb{Z}_4$

$\mathbb{Q}(\xi_5)/\mathbb{Q}$ estensione normale in quanto campo di spezzamento di $x^5 - 1$
$[\mathbb{Q}(\xi_5) : \mathbb{Q}] = 4 \to Gal(\mathbb{Q}(\xi_5)/\mathbb{Q}) \cong (\mathbb{Z}_5)^* \cong \mathbb{Z}_4$
Questa estensione ha una sola sottestensione quadratica ed è $\mathbb{Q}(\xi_5 + \xi_5^{-1}) = \mathbb{Q}(\sqrt{5})$ con $Gal(\mathbb{Q}(\sqrt{5})/\mathbb{Q}) \cong \mathbb{Z}_4$

L'ultima estensione quadratica è $\mathbb{Q}(\sqrt{-15})$ e $Gal(\mathbb{Q}(\sqrt{-15})/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$