$\mathrm{Gal}(E/K)$

?:

Teorema CORRISPONDENZA DI GALOIS

Sia E/K un'estensione di Galois.

1) La corrispondenza

$$F \longmapsto \mathrm{Gal}(E/F)$$

definisce una biezione

$$\left\{ \begin{array}{l} \text{campi intermedi} \\ K \subseteq F \subseteq E \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{sottogruppi} \\ \text{di } \mathrm{Gal}(E/K) \end{array} \right\}$$

2) Dato un campo intermedio F

$$F/K \text{ è Galois} \iff \mathrm{Gal}(E/F) \triangleleft \mathrm{Gal}(E/K)$$

↳ sottogruppo normale

e la restrizione $\sigma \longmapsto \sigma|_F$ induce un epimorfismo

$$\mathrm{Gal}(E/K) \longrightarrow \mathrm{Gal}(F/K)$$

il cui nucleo è $\mathrm{Gal}(E/F)$..

Quindi (Teorema di isomorfismo)

$$\mathrm{Gal}(E/K) \big/ \mathrm{Gal}(E/F) \simeq \mathrm{Gal}(F/K).$$

3) Per un campo intermedio F qualsiasi, gli elementi di $\mathcal{I}(F/K)$ corrispondono biunivocamente ai laterali sinistri di $Gal(E/F)$ in $Gal(E/K)$.
↳ ($\neq$ Procesi)

<u>Dim.</u>

1) Avevamo visto $\theta : \{\text{campi int}\} \longrightarrow \{\text{sottogruppi}\}$

$$\{\quad\} \longleftarrow \{\quad\} : \nu$$

che $T \subseteq \theta\nu(T)$ $\forall\, T \leq Gal(E/K)$ cioè $H \subseteq Gal(E/E^H)$

$F = \nu\theta(F)$ $\forall\, F$ campo intermedio.

Per dimostrare che θ è una biezione (restringendo il codominio ai sgp) basta dimostrare che

$\theta\nu(H) \subseteq H$ per ogni sottogruppo H di $Gal(E/K)$, cioè

$$Gal(E/E^H) \subseteq H \quad \text{cioè che } [E : E^H] \leq n = |H|$$

Per il teorema dell'elemento primitivo, esiste α t.c. $E = K(\alpha)$, quindi $E = E^H(\alpha)$.

Basta provare che α è radice di un polinomio di grado $\leq m$ a coeff. in E^H. Consideriamo $f(x) = \prod_{\sigma \in H} (x - \sigma(\alpha)) \in E^H(\alpha)$ e ha grado $|H|$.

2)

F/K è di Galois $\iff$ $\forall$ ogni K-omom. φ da F in $\overline{\mathbb{Q}}$ si ha $\varphi(F) \subseteq F$

Se F/K è Galois, consideriamo la restrizione

$$\mathrm{Res}: \mathrm{Gal}(E/K) \longrightarrow \mathrm{Gal}(F/K)$$

è un omomorfismo di gruppi: $\mathrm{Res}(\sigma \circ \tau) = \mathrm{Res}(\sigma) \circ \mathrm{Res}(\tau)$

è suriettivo, per il teorema di sollevamento.

Il suo nucleo è

$$\{\sigma \in \mathrm{Gal}(E/K) \mid \sigma|_F = id_F\} = \mathcal{G}(E/F) = \mathrm{Gal}(E/F)$$

Quindi

$\mathrm{Gal}(E/F) \triangleleft \mathrm{Gal}(E/K)$ e la restrizione induce isom. di gruppi $\mathrm{Gal}(E/K) / \mathrm{Gal}(E/F) \simeq \mathrm{Gal}(F/K)$

Osserviamo che $\forall \sigma \in Gal(E/K)$, e $\forall F$ intermedio
$$Gal\left(E/\sigma(F)\right) = \sigma\, Gal(E/F)\, \sigma^{-1}$$

Infatti se $\alpha \in F$ e $\tau \in Gal(E/F)$
$$\sigma \tau \sigma^{-1} \sigma(\alpha) = \sigma \tau(\alpha) = \sigma(\alpha)$$
$$\Rightarrow \sigma\, Gal(E/F)\, \sigma^{-1} \subseteq Gal\left(E/\sigma(F)\right)$$
$\Rightarrow$ sono uguali (hanno lo stesso ordine).

Se $Gal(E/F) \triangleleft Gal(E/K)$ si ha allora
$$Gal(E/F) = Gal\left(E/\sigma(F)\right) \Rightarrow \forall \sigma \in Gal(E/K).$$
$$E^{Gal(E/F)} = E^{Gal(E/\sigma(F))} \Rightarrow \sigma(F) = F$$
$\Rightarrow F$ Galois.

3) La relazione $\sigma\, Gal(E/F)\, \sigma^{-1} = Gal\left(E/\sigma(F)\right)$ vale anche se $Gal(E/F)$ non è normale.

Inoltre la restrizione definisce una funzione suriettiva $Res: Gal(E/K) \longrightarrow \mathcal{J}(F/K)$

Per ogni $\varphi \in \mathcal{J}(F/K)$, sia $\sigma \in Gal(E/K)$ t.c. $\sigma|_F = \varphi$. Se $\tau|_F = \varphi$ allora $\sigma^{-1}\tau|_F = id|_F$
$\Rightarrow \sigma^{-1}\tau \in Gal(E/F) \Rightarrow \tau \in \sigma\, Gal(E/F)$; Viceversa se $\tau \in \sigma\, Gal(E/F)$ allora $\forall \beta \in F$, $\tau(\beta) = \sigma(\beta)$
$\Rightarrow \tau|_F = \varphi$.

Quindi $\forall \varphi \in \mathcal{G}(F/K)$

$\{\sigma \in Gal(E/K) \mid Res|_F\, \sigma = \varphi\}$ è un laterale sinistro di $Gal(E/F)$ in $Gal(E/K)$. $\blacksquare$

Esercizio

1) Determinare il gruppo di Galois (su $\mathbb{Q}$) dei seguenti polinomi

$$x^4-2 \qquad x^5-3 \qquad x^3-x+10$$

2) Per ognuno dei campi di spezzam. dei polinomi sopra, determinare i campi intermedi e per ognuno di essi un elem. generante.

3) Determinare $Gal\left(\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5},\sqrt{7})/\mathbb{Q}\right)$ e un elem. primitivo.

Dire quali sono le est. quadratiche di $\mathbb{Q}$ contenute in $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5},\sqrt{7})$.

Esempio

Consideriamo il polinomio x^3-2

3 radici $\sqrt[3]{2},\ \omega\sqrt[3]{2},\ \omega^2\sqrt[3]{2}$ $\qquad \omega = e^{\frac{2\pi i}{3}}$

Sappiamo che $[E:\mathbb{Q}] = 6$ e $Gal\left(E/\mathbb{Q}\right) \leq S_3$ $\rightsquigarrow$ $Gal\left(E/\mathbb{Q}\right) = S_3$

(identifichiamo $\sqrt[3]{2} \rightsquigarrow 1$, $\omega\sqrt[3]{2} \rightsquigarrow 2$, $\omega^2\sqrt[3]{2} \rightsquigarrow 3$

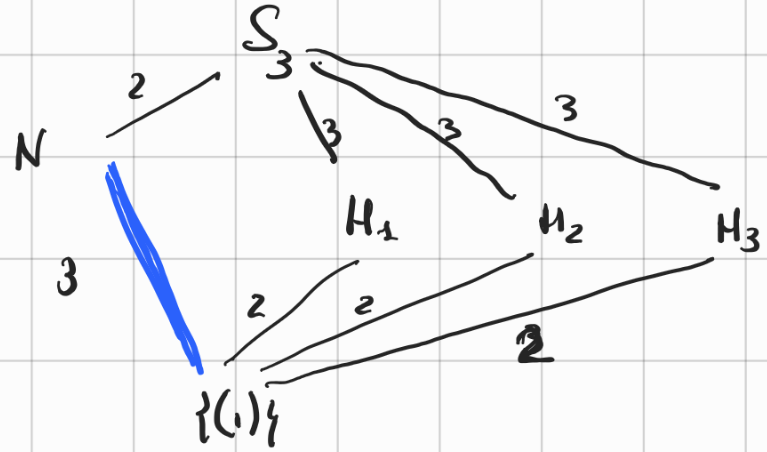
$S_3 = \{(1), (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$

I sottogruppi di S_3 sono

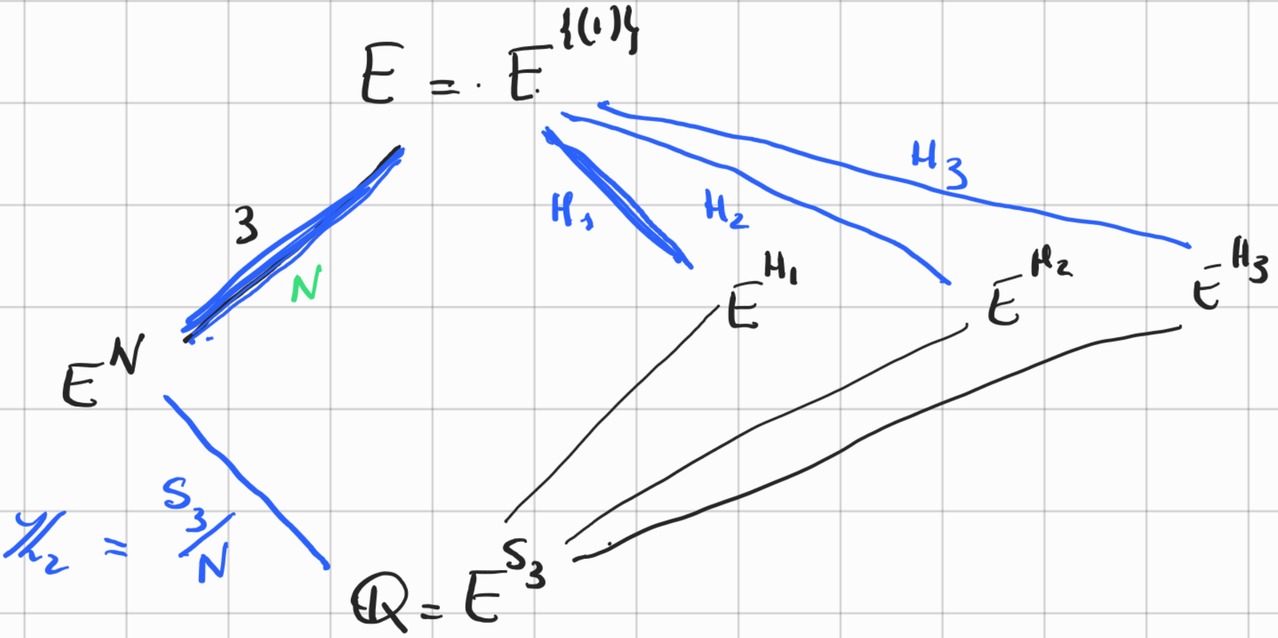
$\{(1)\}$, S_3, $\underbrace{<(1\ 2\ 3)>}_{= N} = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$

$H_1 = <(1\ 2)>$ $\quad H_2 = <(1\ 3)>$ $\quad H_3 = <(2\ 3)>$

Reticolo dei sottogruppi



Corrispondentemente possiamo costruire il reticolo dei sottocampi di E



(Oss N è il ker dell'omom. segno)

Vogliamo determinare generatori per ognuno dei campi intermedi.

- $(1\ 2\ 3) \rightsquigarrow \varphi_1 : \sqrt[3]{2} \longrightarrow \omega\sqrt[3]{2}$ $\qquad \omega = \dfrac{\omega\sqrt[3]{2}}{\sqrt[3]{2}} \rightsquigarrow \dfrac{\omega^2\sqrt[3]{2}}{\omega\sqrt[3]{2}} = \omega$

$$\omega\sqrt[3]{2} \longrightarrow \omega^2\sqrt[3]{2}$$
$$\omega^2\sqrt[3]{2} \longrightarrow \sqrt[3]{2}$$

$\omega \in E^N$ e $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2 \rightsquigarrow E^N = \mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3})$

- $(1\ 2) \rightsquigarrow \varphi_2 : \sqrt[3]{2} \longmapsto \omega\sqrt[3]{2}$ $\qquad \omega \rightsquigarrow \dfrac{\sqrt[3]{2}}{\omega\sqrt[3]{2}} = \omega^2$

$$\omega\sqrt[3]{2} \longrightarrow \sqrt[3]{2}$$
$$\omega^2\sqrt[3]{2} \longrightarrow \omega^2\sqrt[3]{2}$$

$\omega^2\sqrt[3]{2} \in E^{H_1}$ e ha grado 3 $\rightsquigarrow E^{H_1} = \mathbb{Q}(\omega^2\sqrt[3]{2})$

- Analogamente $E^{H_2} = \mathbb{Q}(\omega\sqrt[3]{2})$
- $E^{H_3} = \mathbb{Q}(\sqrt[3]{2})$.

Osservo che $(2\ 3)$ è la restrizione a E del coniugio complesso, quindi

$$E^{H_3} = E \cap \mathbb{R} = \mathbb{Q}(\sqrt[3]{2}).$$

campo fissato dal coniugio cpx

Estensioni ciclotomiche

Vogliamo studiare il campo di spezzamento del polinomio $f(x) = X^n - 1$ su $\mathbb{Q}$ $(n \geq 1)$

Abbiamo visto che è $\mathbb{Q}(\xi)$, ξ radice primitiva n-esima di 1

$\left(\xi = e^{\frac{2\pi i}{n}} = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}\right.$, o più in gen. $e^{\frac{2\pi i k}{n}}$ con $\left.(k,n)=1\right)$.

Vogliamo determinare il polinomio minimo di ξ su $\mathbb{Q}$.

Per ogni $d \mid n$ sia $I_d = \{$radici primitive d-esime dell'unità$\}$

e $\Phi_d(x) = \prod_{\alpha \in I} (x - \alpha)$ d-esimo polinomio ciclotomico

Si ha

$$X^n - 1 = \prod_{d \mid n} \Phi_d(x)$$ perché ogni radice n-esima di 1 è radice primitiva d-esima per qc. $d \mid n$.

In particolare $\Phi_n(x) = \prod_{(k,n)=1} (x - \xi^k)$

$\deg \Phi_n(x) = \varphi(n)$ funzione di Eulero.

Prop.

1) $\Phi_n(x)$ è un polinomio monico a coeff in $\mathbb{Z}$
2) $\Phi_n(x)$ è irriducibile in $\mathbb{Q}[x]$ e quindi è il polinomio minimo di ξ

Dim.

1) Induzione su n. Per $n=1$ $\Phi_1(x) = x - 1$ ok.

Per $n > 1$
$$X^n - 1 = \Phi_n(x) \underbrace{\prod_{\substack{d \mid n \\ d \neq n}} \Phi_d(x)}_{\text{monico a coeff in } \mathbb{Z} \text{ e divide } X^n-1}$$

$\Rightarrow \Phi_n(x)$ è monico a coeff. in $\mathbb{Z}$. (lemma di Gauss)