

TEOREMA FONDAMENTALE DELLA TEORIA DI GALOIS

(41)

Sia $E \supseteq F$ un'estensione di Galois

Definiamo $G \stackrel{\text{def}}{=} \text{Gal}(E/F)$

$$\Gamma \stackrel{\text{def}}{=} \{H \mid H \leq G\}$$

$$\Sigma \stackrel{\text{def}}{=} \{K \text{ sottocampo di } E \mid F \subset K\}$$

(i sottocampi di E che contengono F si dicono
Sottocampi di E/F)

Allora le mappe

$$\Gamma \longrightarrow \Sigma$$

$$H \longrightarrow \text{Inv}(H)$$

e

$$\Sigma \longrightarrow \Gamma$$

$$K \longrightarrow \text{Gal}(E/K)$$

sono biettive e sono l'inverse dell'altra
Inoltre

$$\alpha) H_1, H_2 \in \Gamma \text{ allora } H_1 \supseteq H_2 \iff \text{Inv}(H_1) \subseteq \text{Inv}(H_2)$$

$$\beta) H \in \Gamma \text{ allora } |H| = [E : \text{Inv}(H)] \text{ e } |G : H| = [\text{Inv}(H) : F] \quad \text{(indice di } G \text{ in } H)$$

$$\gamma) H \in \Gamma \text{ allora } H \triangleleft G \iff \text{Inv}(H) \text{ è normale su } F$$

$$\text{se } H \triangleleft G \text{ abbiamo che } \text{Gal}(\text{Inv}(H)/F) = G/H$$

Osservazioni: 1) se E è separabile su F
allora $K \in \Sigma$ è separabile su F

(42)

2) la corrispondenza biunivoca fra Π e Σ
viene detta di Galois (Galois pairing)

Dimostrazione teorema: $\triangleright$ Sia $H \in \Pi$ ($H \leq \text{Gal}(\bar{E}/F)$)

allora $F = Y_{\text{nr}}(G)$ da cui $F \subseteq Y_{\text{nr}}(H)$

$E \supseteq F$ è un'estensione di Galois $\Rightarrow E$ campo
di spezzamento di $q(x) \in F[x]$ separabile

Possiamo considerare $q(x) \in Y_{\text{nr}}(H)[x]$
ottenendo $E \supseteq Y_{\text{nr}}(H)$ estensione di Galois

Per il teorema di caratterizzazione estensioni di Galois
abbiamo che $\text{Gal}(\bar{E}/Y_{\text{nr}}(H)) = H$ i.e. Gal inverse
sinistre di Y_{nr}

$$\triangleright |H| = |\text{Gal}(\bar{E}/Y_{\text{nr}}(H))| = [E:Y_{\text{nr}}(H)]$$

(Lemma 1)

otteniamo così le prime porte del punto β

$\triangleright K \in \Sigma$ i.e. K sottocampo di $\bar{E}/F$ allora

$$\text{Notiamo che } \text{Gal}(\bar{E}/K) \subseteq \text{Gal}(\bar{E}/F)$$

Come nel punto iniziale possiamo ottenere
che $E \supseteq K$ è un'estensione di Galois

Quindi per teor. car. est. di Galois vale che

$$K = \gamma_{mv} (G_{ol} (E/K))$$

i.e. G_{ol} è l'inversa destra di γ_{mv}

Concludiamo che $G_{ol}: \Sigma \rightarrow \Gamma$ e $\gamma_{mv}: \Gamma \rightarrow \Sigma$

sono una l'inverse dell'altra.

► (dimostrazione α)

• $H_1 \supseteq H_2 \Rightarrow \gamma_{mv} H_1 \subseteq \gamma_{mv} H_2$ per definizione

$$\begin{array}{ccc} \gamma_{mv} H_1 \subseteq \gamma_{mv} H_2 & \xRightarrow{\text{(per def.)}} & G_{ol} \left(\frac{E}{\gamma_{mv} H_1} \right) \supseteq G_{ol} \left(\frac{E}{\gamma_{mv} H_2} \right) \\ & & \begin{array}{cc} \parallel & \parallel \\ H_1 & H_2 \end{array} \end{array}$$

punti precedenti

$$\Rightarrow H_1 \supseteq H_2$$

► (dimostrazione II parte β)

$$|G| = [E:F] = [E:\gamma_{mv} H] [\gamma_{mv} H:F]$$

← lemma 1

$$\cancel{|H|} |G:H| = |G| = \cancel{|H|} [\gamma_{mv} H:F]$$

Teor. Lagrange per lemma 1

$$\Rightarrow |G:H| = [\gamma_{mv} H:F]$$

▶ Rimane la parte *

44

Siano $H \in \Gamma$ (i.e. $H \leq G = \text{Gal}(E/F)$) e $\eta \in G$

Osserviamo che per ogni $\xi \in G$ o $k \in E$

$$\xi(k) = k \iff \eta \circ \xi \circ \eta^{-1}(\eta(k)) = \eta(k) \quad (*)$$

$$\boxed{\text{Claim 1: } \gamma_{\text{inv}}(\eta H \eta^{-1}) = \eta(\gamma_{\text{inv}} H)}$$

" $\supseteq$ " sia $k \in \gamma_{\text{inv}}(H) \Rightarrow$ per ogni $\xi \in H$ $\xi(k) = k$

$$\stackrel{(*)}{\Rightarrow} \text{ per ogni } \xi \in H \quad \eta \xi \eta^{-1}(\eta(k)) = \eta(k)$$

$$\Rightarrow \eta(k) \in \gamma_{\text{inv}}(\eta H \eta^{-1})$$

" $\subseteq$ " sia $a \in \gamma_{\text{inv}}(\eta H \eta^{-1}) \Rightarrow \eta \xi \eta^{-1}(a) = a \quad \forall \xi \in H$

$$\text{Se } a = \eta(b) \Rightarrow \eta \xi \eta^{-1}(\eta(b)) = \eta(b) \quad \forall \xi \in H$$

$$\Rightarrow \xi(b) = b \quad \forall \xi \in H \Rightarrow b \in \gamma_{\text{inv}}(H) \Rightarrow$$

$$\Rightarrow a = \eta(b) \in \eta(\gamma_{\text{inv}}(H))$$

$$\boxed{\text{Claim 2: } H \triangleleft G \iff \eta(\gamma_{\text{inv}} H) = \gamma_{\text{inv}} H \text{ per ogni } \eta \in G}$$

" $\Rightarrow$ " direttamente da Claim 1

$$" $\Leftarrow$ " $\eta(\gamma_{\text{inv}} H) = \gamma_{\text{inv}} H \stackrel{\text{Claim 1}}{\Rightarrow} \gamma_{\text{inv}} H = \gamma_{\text{inv}}(\eta H \eta^{-1})$$$

$$\Rightarrow \text{Gal}(\gamma_{\text{inv}}(\eta H \eta^{-1})) = \text{Gal}(\gamma_{\text{inv}} H) \Rightarrow \eta H \eta^{-1} = H$$

siccome η generico elemento di G $H \triangleleft G$

Ora supponiamo $H \triangleleft G$ (ed mostriamo $\gamma_{\text{nr}} H$ normale su F)

$$H \triangleleft G \Rightarrow \eta(\gamma_{\text{nr}} H) = \gamma_{\text{nr}} H \text{ per ogni } \eta \in G$$

Posso quindi considerare $\bar{\eta} = \eta|_{\gamma_{\text{nr}} H} \in \text{Gal}(\gamma_{\text{nr}} H / F)$

e otteniamo un omomorfismo di gruppi

$$\begin{aligned} \varphi: G = \text{Gal}(\bar{E}/F) &\longrightarrow \text{Gal}(\gamma_{\text{nr}} H / F) \\ \eta &\longmapsto \bar{\eta} \end{aligned}$$

$$\varphi(G) \leq \text{Gal}(\gamma_{\text{nr}} H / F) \text{ e } \gamma_{\text{nr}}(\varphi(G)) = F$$

per teor. car. est. Galois $\Rightarrow \gamma_{\text{nr}} H$ è normale su $F = \gamma_{\text{nr}}(\varphi(G))$

$$\text{Inoltre } \text{Gal}(\gamma_{\text{nr}} H / F) = \text{Gal}\left(\frac{\gamma_{\text{nr}} H}{\gamma_{\text{nr}} \varphi(G)}\right) = \varphi(G) \text{ e}$$

$$\ker \varphi = \left\{ \eta \in G \mid \eta|_{\gamma_{\text{nr}}(H)} = \text{Id} \right\} = \text{Gal}\left(\frac{\bar{E}}{\gamma_{\text{nr}} H}\right) = H$$

Per teorema isom.

$$\text{Gal}(\gamma_{\text{nr}} H / F) = \varphi(G) \cong \frac{G}{\ker \varphi} = \frac{G}{H}$$

(parte addizionale punto ∇)

Infine supponiamo $K = \gamma_{mv} H$ normale su F

(e dimostriamo $H \triangleleft G$)

Sia $a \in K$, $q(x) \in F[x]$ pol. minimo per a

$$\Rightarrow \text{in } K[x] \quad q(x) = (x - a_1) \cdots (x - a_k) \text{ con } a = a_1$$

$\uparrow$

K normale su F

Se $\eta \in G$: $q(\eta(a)) = 0$ (usuale argomento)

$$\Rightarrow \eta(a) = a_i \text{ per qualche } i$$

$$\Rightarrow \eta(a) \in K$$

Abbiamo ottenuto che $\eta(K) \subseteq K$ che
 Implica $\eta(K) = K$ (spazi vettoriali su F della
 stessa dimensione)

$$\text{Quindi } \eta(\gamma_{mv} H) = \gamma_{mv} H$$

$$\Rightarrow (\text{Claim 2 e genericità di } \eta)$$

$$H \triangleleft G$$



Sia $x^3 - 2 \in \mathbb{Q}[x]$ e E il campo di
Spezzamento di $x^3 - 2$

Calcolare $\text{Gal}(E/\mathbb{Q})$ e i sottocompi di $E/\mathbb{Q}$

usando la corrispondenza di Galois

Risoluzione: osserviamo

- $x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4})$
- $x^3 - 2$ ha una radice reale ($\sqrt[3]{2}$)
e due radici complesse coniugate (non appartenenti a $\mathbb{R}$)
- $x^3 - 2$ è irriducibile su $\mathbb{Q}$
(grado 3 + riducibile $\Rightarrow$ ha una radice in $\mathbb{Q}$)
- $x^2 + \sqrt[3]{2}x + \sqrt[3]{4}$ è irriducibile su $\mathbb{Q}[\sqrt[3]{2}] \subseteq \mathbb{R}$
(definiamo $p(x) \stackrel{\text{def}}{=} x^2 + \sqrt[3]{2}x + \sqrt[3]{4}$)
- $E = \frac{\mathbb{Q}[\sqrt[3]{2}][x]}{(p(x))}$ è un campo di

Spezzamento di $x^3 - 2$ su $\mathbb{Q}$

- $[E:\mathbb{Q}] = \underbrace{[E:\mathbb{Q}[\sqrt[3]{2}]]}_{=2} \underbrace{[\mathbb{Q}[\sqrt[3]{2}]:\mathbb{Q}]}_{=3} = 6$

per cui $|\text{Gal}(\bar{E}/\mathbb{Q})| = [\bar{E} : \mathbb{Q}] = 6$

- $\bar{E} = \mathbb{Q}[\sqrt[3]{2}, u]$ dove u radice di $p(x)$
e $\{1, \sqrt[3]{2}, \sqrt[3]{4}, u, u\sqrt[3]{2}, u\sqrt[3]{4}\}$ è una base
di $\bar{E}$ come $\mathbb{Q}$ spazio vettoriale

- Se $f \in \text{Gal}(\bar{E}/\mathbb{Q})$, allora f è determinato
da $f(\sqrt[3]{2})$ e $f(u)$

- f agisce sull'insieme delle radici di $x^3 - 2$
che è $\{\sqrt[3]{2}, u, v = \overline{u}\}$

Otteniamo quindi un omomorfismo

$$\varphi: \text{Gal}(\bar{E}/\mathbb{Q}) \longrightarrow S^3$$

▷ φ è iniettivo perché
 $f \in \text{Gal}(\bar{E}/\mathbb{Q})$ è determinato
da $f(\sqrt[3]{2})$ e $f(u)$

▷ φ è suriettivo perché
 φ iniettivo e
 $|\text{Gal}(\bar{E}/\mathbb{Q})| = |S^3| = 6$

$$\text{Gal}(\bar{E}/\mathbb{Q}) \cong S^3$$

Elementi di $\text{Gal}(\bar{\mathbb{E}}/\mathbb{Q})$:

$$\begin{array}{l} \text{Id: } \sqrt[3]{2} \rightarrow \sqrt[3]{2} \\ u \rightarrow u \\ v \rightarrow v \end{array}$$

$$\begin{array}{l} f_1: \sqrt[3]{2} \rightarrow u \\ u \rightarrow \sqrt[3]{2} \\ v \rightarrow v \end{array}$$

$$\begin{array}{l} f_2: \sqrt[3]{2} \rightarrow \sqrt[3]{2} \\ u \rightarrow v \\ v \rightarrow u \end{array}$$

$$\begin{array}{l} f_3: \sqrt[3]{2} \rightarrow v \\ u \rightarrow u \\ v \rightarrow \sqrt[3]{2} \end{array}$$

$$\begin{array}{l} f_4: \sqrt[3]{2} \rightarrow u \\ u \rightarrow v \\ v \rightarrow \sqrt[3]{2} \end{array}$$

$$\begin{array}{l} f_5: \sqrt[3]{2} \rightarrow v \\ u \rightarrow \sqrt[2]{3} \\ v \rightarrow u \end{array}$$

(danno tutte origine ad un automorfismo di $\bar{\mathbb{E}}/\mathbb{Q}$)
perchè $|\text{Gal}(\bar{\mathbb{E}}/\mathbb{Q})| = 6$ e φ suriettivo

$$|f_1| = |f_2| = |f_3| = 2 \quad \text{e} \quad |f_4| = |f_5| = 3$$

Sottogruppi di S_3 $\{ \text{Id} \}, S_3, \{ \text{Id}, f_1 \}, \{ \text{Id}, f_2 \},$
 $\{ \text{Id}, f_3 \}, \{ \text{Id}, f_4, f_5 \}$

Sottocampi di $\bar{\mathbb{E}}/\mathbb{Q}$ Li otteniamo tramite
la corrispondenze di Galois

Ricordo che $[G:H] = [\gamma_{\text{nr}} H : \mathbb{F}]$

per cui $[\gamma_{\text{nr}} \{ \text{Id}, f_i \} : \mathbb{Q}] = 3$ per $i=1,2,3$

$$[\gamma_{\text{nr}} \{ \text{Id}, f_4, f_5 \} : \mathbb{Q}] = 2$$

Ricordo anche che $\omega, \sqrt[3]{2}, u$ hanno grado 3 su $\mathbb{Q}$

Questo ci permette di ottenere subito:

$$\langle \text{Id} \rangle \xrightarrow{\gamma_{\text{no}}} E, \text{ (per definizione)}$$

$$\text{Gal}(E/\mathbb{Q}) \longrightarrow \mathbb{Q} = \gamma_{\text{no}}(\text{Gal}(E/\mathbb{Q}))$$

$$\left. \begin{aligned} \langle \text{Id}, f_1 \rangle &\longrightarrow \mathbb{Q}[\omega] \\ \langle \text{Id}, f_2 \rangle &\longrightarrow \mathbb{Q}[\sqrt[3]{2}] \\ \langle \text{Id}, f_3 \rangle &\longrightarrow \mathbb{Q}[u] \end{aligned} \right\} \begin{aligned} &\text{Siccome } f_1(\omega) = \omega \\ &\gamma_{\text{no}}(\langle \text{Id}, f_1 \rangle) \supseteq \mathbb{Q}[\omega] \\ &\text{I gradi delle due estensioni} \\ &\text{coincidono e otteniamo} \\ &\text{la stessa estensione} \\ &\text{Analogo per gli altri} \\ &\text{due sottogruppi di} \\ &\text{ordine 2} \end{aligned}$$

Rimane da individuare $\gamma_{\text{no}} \langle \text{Id}, f_4, f_5 \rangle$

Svolgendo i conti ottengo

$$u, v = \frac{\sqrt[3]{2} \pm \sqrt[3]{2} \sqrt{3} i}{2} \quad \text{e } u-v = \sqrt[3]{2} \sqrt{3} i$$

Si osserva facilmente che $\sqrt{3}i \in E$

Considero $\mathbb{Q}[\sqrt{3}i]$ estensione di grado 2
 di $\mathbb{Q}$ ($\sqrt{3}i$ radice di x^2+3 polinomio irriducibile)

In $\text{Gal}(\bar{\mathbb{E}}/\mathbb{Q}) \cong S^3$ esiste un unico sottogruppo di indice 2. La corrispondenza di Galois ci dice che c'è un'unica estensione di $\mathbb{Q}$ contenuta in $\bar{\mathbb{E}}$ di grado 2 e deve essere per forza $\mathbb{Q}[\sqrt{3}i]$.

Questa è l'unica estensione diversa da $\mathbb{Q}$ ed $\bar{\mathbb{E}}$ che è normale (corrisponde all'unico sottogruppo proprio, non banale e normale di $\text{Gal}(\bar{\mathbb{E}}/\mathbb{Q})$)

Esercizio mostrare direttamente che $f_4(i\sqrt{3}) = i\sqrt{3}$
e $f_5(i\sqrt{3}) = i\sqrt{3}$

Problema: 1) dimostrare che le estensioni di grado due sono normali

2) mostrare un'estensione di grado due che non è di Galois