

GRUPPO DI GALOIS COME

117

GRUPPO DI PERMUTAZIONI DI RADICI

Siano:

- $q(x) \in F[x]$ polinomio monico, non costante e separabile
- E campo di spezzamento di $q(x)$
- $\{r_1, \dots, r_m\}$ radici distinte di $q(x)$ in E da cui $E = F(r_1, \dots, r_m)$

Vi ricordo che esiste un monomorfismo

$$\varphi: \text{Gal}(E/F) \longrightarrow S_m \cong S(\{r_1, \dots, r_m\})$$

e si definisce $G_q = \varphi(\text{Gal}(E/F)) \leq S_m$

Domanda: chi è $\gamma_{\text{Alt}}(A_m \cap G_q)$?

$\nearrow$
gruppo
alternante

Teorema $F, q(x), E, \{r_1, \dots, r_m\}$ come definiti precedentemente

Definiamo $D = \prod_{1 \leq i < j \leq m} (r_i - r_j)$

Se $\text{char } F \neq 2$ allora $\gamma_{\text{Alt}}(A_m \cap G_q) = \neq (D)$

Dim Consideriamo $FL[x_1, \dots, x_n]$

118

Ricordo che dato $\pi \in S_n \exists! \xi(\pi) \in \text{Aut}(FL[x_1, \dots, x_n])$
tale che $\xi(\pi)(a) = a$ e $\xi(\pi)(x_i) = x_{\pi(i)}$

Inoltre se $\pi_1, \pi_2 \in S_n \xi(\pi_1 \circ \pi_2) = \xi(\pi_1) \circ \xi(\pi_2)$

Definiamo $\Delta = \prod_{1 \leq i < j \leq n} (x_i - x_j) \in FL[x_1, \dots, x_n]$

Claim: se $\tau = (k, e)$ trasposizione allora
 $\xi(\tau)(\Delta) = -\Delta$

Supponiamo $k < e$ [consideriamo l'azione di $\xi(\tau)$ sui fattori $x_i - x_j$]

• se $\{i, j\} = \{k, e\}$

$$\xi(\tau)(x_k - x_e) = (x_e - x_k) = -(x_k - x_e)$$

• se $\{i, j\} \cap \{k, e\} = \{j\}$ (cioè $j = k$ o $j = e$)

• suppongo $i < k < e$

$$\begin{aligned} \xi(\tau)(x_i - x_k) &= (x_i - x_e) \\ \xi(\tau)(x_i - x_e) &= (x_i - x_k) \end{aligned} \left. \begin{array}{l} \\ \end{array} \right\} \begin{array}{l} \text{scambio} \\ 2 \text{ fattori} \\ \text{di } \Delta \end{array}$$

• suppongo $k < e < i$

$$\begin{aligned} \xi(\tau)(x_k - x_i) &= (x_e - x_i) \\ \xi(\tau)(x_e - x_i) &= (x_k - x_i) \end{aligned} \left. \begin{array}{l} \\ \end{array} \right\} \begin{array}{l} \text{scambio} \\ 2 \text{ fattori} \\ \text{di } \Delta \end{array}$$

• Suppongo $k < i < l$

$$\left. \begin{aligned} \xi(\tau)(\pi_l - \pi_i) &= -(\pi_i - \pi_k) \\ \xi(\tau)(\pi_i - \pi_k) &= -(\pi_l - \pi_i) \end{aligned} \right\} \begin{array}{l} \text{Scambia due} \\ \text{fattori di } \Delta \\ \text{cambiando} \\ \text{entrambi di} \\ \text{segno} \end{array}$$

• se $\{i, j\} \cap \{k, l\} = \emptyset$

$$\xi(\tau)(\pi_i - \pi_j) = (\pi_i - \pi_j)$$

Concludo che:

$$\xi(\tau)(\Delta) = -\Delta$$

La dimostrazione del claim è conclusa.

Claim

+

$$\left. \begin{aligned} \xi(\pi_1 \circ \pi_2) &= \xi(\pi_1) \circ \xi(\pi_2) \end{aligned} \right\} \Rightarrow \boxed{\xi(\pi)(\Delta) = \text{sgn } \pi \cdot \Delta} (*)$$

Siano:

- $\eta \in \text{Gal}(\bar{E}/F)$ e $\pi \in S(\{x_1, \dots, x_m\})$ indotta da η
- $\alpha: F[x_1, \dots, x_m] \rightarrow E = F[x_1, \dots, x_m]$ omonomorfismo
con $\alpha(a)$ per ogni $a \in F$ e $\alpha(x_i) = x_i$

Otteniamo che $\alpha(\Delta) = D$ e $\alpha(\xi(\pi)(\Delta)) = \eta(D)$

$$\text{Quindi } \eta(D) = \alpha(\xi(\pi)(\Delta)) = \alpha(\text{sgn } \pi \cdot \Delta) = \text{sgn } \pi \cdot \alpha(\Delta) = \text{sgn } \pi \cdot D$$

Ottengo infine $\eta(D) = \text{sgn } \pi D$ da cui

$$\boxed{\eta(D) = D \iff \pi \in A_m} \quad \left[\begin{array}{l} \text{qua si usa} \\ \text{char } F \neq 2 \end{array} \right]$$

quindi

$$\eta \in \text{Gal}\left(\frac{E}{F(D)}\right) \iff \pi \in A_m \cap G_q$$

$$\text{Gal}\left(\frac{E}{F(D)}\right) \cong A_m \cap G_q$$

$$(\text{tramite } \varphi: \text{Gal}\left(\frac{E}{F}\right) \xrightarrow{\cong} G_q \leq S_m)$$

$$\gamma_{\text{inv}}(\text{Gal}\left(\frac{E}{F(D)}\right)) = F(D)$$



Osservazione 1) per teor. fund. teoria di Galois

$$\text{Gal}(E/F(D)) = \text{Gal}(E/F)$$

$$\iff$$

$$F(D) = \gamma_{\text{inv}}(\text{Gal}(E/F(D))) = \gamma_{\text{inv}}(\text{Gal}(E/F)) = F$$

da cui:

$$D \in F \iff F(D) = F \iff A_m \cap G_q = G_q \iff G_q \leq A_m$$

2) per ogni $\eta \in \text{Gal}(\mathbb{E}/\mathbb{F})$ $\eta(D) = D \circ \eta(D) = -D$

quindi per ogni $\eta \in \text{Gal}(\mathbb{E}/\mathbb{F})$ $\eta(D^2) = D^2$

$$\Rightarrow d = D^2 \in \mathbb{F} = \text{Inv}(\text{Gal}(\mathbb{E}/\mathbb{F}))$$

Corollario

$$G_q \leq A_m$$

$$\Leftrightarrow$$

$$d = \prod_{1 \leq i < j \leq m} (r_i - r_j)^2 \text{ è il quadrato di un}$$

elemento di $\mathbb{F}$

Def $d = \prod_{1 \leq i < j \leq m} (r_i - r_j)^2 \in \mathbb{F}$ viene detto

il discriminante di $q(x)$

PROCEDURA PER CALCOLARE IL DISCRIMINANTE
A PARTIRE DAI COEFFICIENTI DI $q(x)$

$$q(x) = x^m - a_1 x^{m-1} + \dots + (-1)^m a_m = \prod_{i=1}^m (x - r_i)$$

da cui $a_1 = \sum_{i=1}^m r_i$ $a_2 = \sum_{i < j} r_i r_j$

$$\dots a_m = \prod_{i=1}^m r_i$$

de finiamo

$$V = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \kappa_1 & \kappa_2 & \dots & \kappa_m \\ \vdots & \vdots & \ddots & \vdots \\ \kappa_1^{n-1} & \kappa_2^{n-1} & \dots & \kappa_m^{n-1} \end{pmatrix}$$

$$\det V = \prod_{i>j} (\kappa_i - \kappa_j) \quad (\text{matrice di Vandermonde})$$

$$\det V V^t = \det V \cdot \det V^t = (\det V)^2 = \prod_{i>j} (\kappa_i - \kappa_j)^2 = \Delta$$

$$V V^t = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \kappa_1 & \kappa_2 & \dots & \kappa_m \\ \kappa_1^2 & \kappa_2^2 & \dots & \kappa_m^2 \\ \vdots & \vdots & \ddots & \vdots \\ \kappa_1^{n-1} & \kappa_2^{n-1} & \dots & \kappa_m^{n-1} \end{pmatrix} \begin{pmatrix} 1 & \kappa_1 & \dots & \kappa_1^{n-1} \\ 1 & \kappa_2 & \dots & \kappa_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \kappa_m & \dots & \kappa_m^{n-1} \end{pmatrix}$$

i segni
invertiti
non danno
fastidio

$$V V^t = \begin{pmatrix} n & \Delta_1 & \Delta_2 & \dots & \Delta_{n-1} \\ \Delta_1 & \Delta_2 & & & \\ \Delta_2 & & & & \\ \vdots & & & & \\ \Delta_{n-1} & \dots & \Delta_{2n-3} & \Delta_{2n-2} \end{pmatrix}$$

con

$$\Delta_1 = \kappa_1 + \dots + \kappa_m$$

$$\Delta_2 = \kappa_1^2 + \dots + \kappa_m^2$$

$$\vdots$$

$$\Delta_i = \kappa_1^i + \dots + \kappa_m^i$$

Δ_i sono simmetriche rispetto agli κ_i

$\Rightarrow \leftarrow$ [una delle prime applicazioni
teoria di Galois]

gli Δ_i sono esprimibili in forma polinomiale
portando le funzioni simmetriche elementari

$$a_1 = \sum \kappa_i \quad a_2 = \sum_{i<j} \kappa_i \kappa_j \quad \dots \quad a_m = \prod_i \kappa_i$$

Conclusione: gli Δ_i si possono esprimere
in funzione degli a_i

$\Rightarrow$

o si può esprimere in funzione degli a_i

Esempi $\boxed{n=2}$ $q(x) = (x-r_1)(x-r_2)$

$$a_1 = r_1 + r_2 \quad a_2 = r_1 r_2$$

$$\Delta_1 = a_1 \quad \Delta_2 = r_1^2 + r_2^2 = (r_1 + r_2)^2 - 2r_1 r_2 = a_1^2 - 2a_2$$

$$d = \det \begin{pmatrix} 2 & \Delta_1 \\ \Delta_1 & \Delta_2 \end{pmatrix} = \det \begin{pmatrix} 2 & a_1 \\ a_1 & a_1^2 - 2a_2 \end{pmatrix} = 2a_1^2 - 4a_2 - a_1^2 = a_1^2 - 4a_2$$

[Vi ricorda qualche cosa?]

$\boxed{n=3}$ $q(x) = (x-r_1)(x-r_2)(x-r_3)$

$$a_1 = r_1 + r_2 + r_3 \quad a_2 = r_1 r_2 + r_1 r_3 + r_2 r_3 \quad a_3 = r_1 r_2 r_3$$

$$\boxed{\underline{\underline{\Delta_1 = a_1}}}$$

$$\boxed{\underline{\underline{\Delta_2 = r_1^2 + r_2^2 + r_3^2 = (r_1 + r_2 + r_3)^2 - 2(r_1 r_2 + r_1 r_3 + r_2 r_3) = a_1^2 - 2a_2}}}$$

[Δ_3 lo abbiamo fatto a mano in un esercizio
qua impostiamo un modo più generale]

$$a_1 r_k^2 - a_2 r_k + a_3 =$$

$$= r_1 r_k^2 + r_2 r_k^2 + r_3 r_k^2 - r_1 r_2 r_k - r_1 r_3 r_k - r_2 r_3 r_k + r_1 r_2 r_3$$

$$= r_k^3$$

← fare il conto per $k=1,2,3$

da cui $r_k^4 = a_1 r_k^3 - a_2 r_k^2 + a_3 r_k$

$$\underline{\underline{J_3}} = r_1^3 + r_2^3 + r_3^3 = \sum_{k=1}^3 (a_1 r_k^2 - a_2 r_k + a_3)$$

$$= a_1 (r_1^2 + r_2^2 + r_3^2) - a_2 (r_1 + r_2 + r_3) + 3a_3$$

$$= a_1 (a_1^2 - 2a_2) - a_2 a_1 + 3a_3$$

$$= a_1^3 - 3a_1 a_2 + 3a_3$$

$$\underline{\underline{J_4}} = r_1^4 + r_2^4 + r_3^4 = a_1 (r_1^3 + r_2^3 + r_3^3) - a_2 (r_1^2 + r_2^2 + r_3^2) + a_3 (r_1 + r_2 + r_3)$$

$$= a_1 (a_1^3 - 3a_1 a_2 + 3a_3) - a_2 (a_1^2 - 2a_2) + a_3 a_1$$

$$= a_1^4 - 3a_1^2 a_2 + 3a_1 a_3 - a_1^2 a_2 + 2a_2^2 + a_3 a_1$$

$$= a_1^4 - 4a_1^2 a_2 + 4a_1 a_3 + 2a_2^2$$

$$d = \det \begin{pmatrix} 3 & J_1 & J_2 \\ J_1 & J_2 & J_3 \\ J_2 & J_3 & J_4 \end{pmatrix} = 3J_2 J_4 + 2J_1 J_2 J_3 - J_2^3 - 3J_3^2 - J_1 J_1^2$$

$$= -4a_1^3 a_3 + a_1^2 a_2^2 + 18a_1 a_2 a_3 -$$

Facendo i conti

$$-4a_2^3 - 27a_3^2$$

[torneremo su questo]

CRITERIO PER RIDUCIBILITÀ POLINOMI TRAMITE GRUPPO DI GALOIS

Def: Sia G gruppo che agisce su X insieme
L'azione di G su X è detta transitiva
se esiste un'unica orbita
(i.e. per ogni $x, z \in X \exists g \in G \text{ t.c. } g(x) = z$)

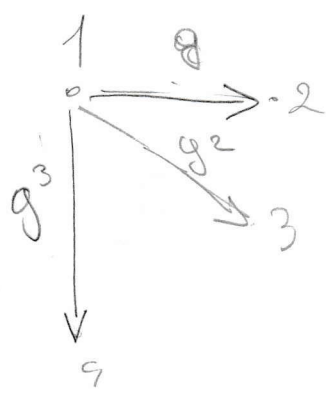
Esempi

ricordo: $O_G(p) = \{g(p) \mid g \in G\}$ è l'orbita di p rispetto all'azione di G
• le orbite formano una partizione di X

Considero azioni di sottogruppi di S_4 su $\{1, 2, 3, 4\}$

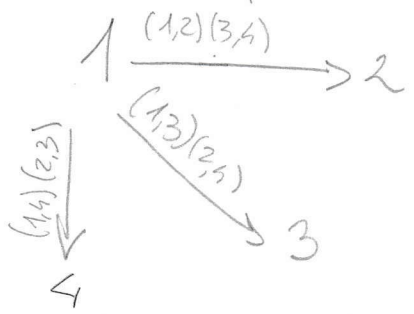
i) $G = \langle \underbrace{(1, 2, 3, 4)}_{g \text{ def}} \rangle$

gruppo
generato
da $(1, 2, 3, 4)$



$O_G(1) = \{1, 2, 3, 4\}$
e
l'azione è
transitiva

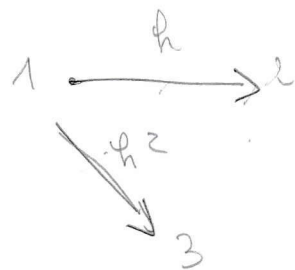
ii) $G = \{Id, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$



$O_G(1) = \{1, 2, 3, 4\}$
e
l'azione è transitiva

$$iii) \quad G = \langle (1, 2, 3) \rangle$$

$\begin{matrix} \text{def} \\ \hline \end{matrix}$



• 4

$O_G(114) = \{1, 2, 3\}$ e azione non transitiva

Teorema: $q(x) \in \mathbb{F}[x]$ senza radici multiple

$q(x)$ irriducibile $\iff G_q$ agisce transitivamente su $\{r_1, \dots, r_n\}$ radici di $q(x)$

Dim.

" $\implies$ "

Supponiamo $q(x)$ irriducibile

Sia α una radice di $q(x)$ nel campo di spezz. di $q(x)$.
Definiamo β omomorfismo tale che:

$$\beta: \mathbb{F}[x] \longrightarrow \mathbb{F}[\alpha]$$

$$p(x) \longrightarrow p(\alpha)$$

$$x \longrightarrow \alpha$$

da cui otteniamo

$$\frac{\mathbb{F}[x]}{(q(x))} \xrightarrow[\bar{\alpha}]{\bar{\beta}} \mathbb{F}[\alpha] \quad \bar{\beta} \text{ isomorfismo}$$

$$x + (q(x)) \longrightarrow \alpha$$

Siano α_i, α_j due radici di $q(x)$:

- posso costruire φ un isomorfismo

$$\begin{array}{ccc} \mathbb{F}(\alpha_i) & \xleftarrow{\cong} & \frac{\mathbb{F}[x]}{(q(x))} \xrightarrow{\cong} \mathbb{F}(\alpha_j) \\ & \searrow & \nearrow \\ & \varphi & \end{array}$$

con φ tale che $\varphi(a) = a \quad \forall a \in \mathbb{F}$
e $\varphi(\alpha_i) = \alpha_j$

Denotiamo con E il campo di spezzamento di $q(x)$ su $\mathbb{F}$, quindi $E = \mathbb{F}(\alpha_1, \dots, \alpha_k)$ con $\{\alpha_i\}$ radici di $q(x)$

$$\left. \begin{array}{l} E = \mathbb{F}(\alpha_i)(\alpha_1, \dots, \alpha_{i-1}, \alpha_{i+1}, \dots, \alpha_k) \\ E = \mathbb{F}(\alpha_j)(\alpha_1, \dots, \alpha_{j-1}, \alpha_{j+1}, \dots, \alpha_k) \end{array} \right\} \Rightarrow \begin{array}{l} E \text{ campo di} \\ \text{Spezzamento} \\ \text{di } q(x) \text{ su } \mathbb{F}(\alpha_i) \\ \text{e } \mathbb{F}(\alpha_j) \end{array}$$

Per un teorema che abbiamo dimostrato all'inizio delle porte sui campi (che implica l'unicità del campo di spezzamento a meno di isomorfismi) otteniamo che

posso estendere φ ad E cioè esiste

$\eta: E \rightarrow E$ automorfismo tale che

$$\eta|_{F(r_i)} = \varphi \quad \text{in particolare}$$

$$\eta(a) = a \text{ per ogni } a \in F \text{ e } \eta(r_i) = r_j$$

$$\Rightarrow \eta \in \text{Gal}(E/F) \text{ e } \eta(r_i) = r_j$$

Siccome r_i, r_j sono due generiche radici di $q(x)$ ottengo che l'azione di $\text{Gal}(E/F)$ sulle radici è transitiva 

" $\Leftarrow$ " Supponiamo che l'azione sia transitiva

Sia $q_1(x)$ fattore irriducibile di $q(x)$

Sia r_1 radice di $q_1(x)$ e r_i radice generica di $q(x)$

G_q agisce transitivamente $\Rightarrow \exists \eta \in \text{Gal}(E/F)$ t.c. $\eta(r_1) = r_i$

(con E denotiamo il campo di spezzamento di $q(x)$)

$$0 = \eta(\underbrace{q_1(r_1)}_0) = q_1(\eta(r_1)) = q_1(r_i)$$

$\nearrow$
 q_1 ha
 coefficienti
 in F

tutte le radici di $q(z)$ sono radici di $q_1(z)$

Siccome $q(z)$ non ha radici multiple

$\deg q(z) = \deg q_1(z)$ e $q(z) = q_1(z)$ (a meno di moltiplicazioni per costanti)

$\Rightarrow q(z)$ irriducibile



Applicazioni:

- 1) supponiamo $\text{char } F \neq 2$ e $q(z) = z^2 - a_1 z + a_2$
con $q(z)$ senza radici multiple

$$G_q \leq S_2 = \{1, (1, 2)\}$$

$$G_q \leq A_2 = \{1\} \iff d = a_1^2 - 4a_2 \text{ ha una radice quadrata in } F$$

se $d = a_1^2 - 4a_2$ ha radici in $F \Rightarrow G_q = \{1\}$

(ed è automaticamente riducibile per teor. precedente)

se $d = a_1^2 - 4a_2$ non ha radici in $F \Rightarrow G_q = S_2$

(ed è automaticamente irriducibile per teor. prec.)

[In questo caso la riducibilità / irriducibilità può essere provata facendo i conti a mano]

Sopponiamo:

2) $\text{char } F \neq 2$ e $q(x) = x^3 - a_1 x^2 + a_2 x + a_3 \in F[x]$
senza radici multiple

(130)

Se $q(x) = (x - \alpha) q_1(x) \Rightarrow G_q = G_{q_1}$

Se $q(x)$ irriducibile

$G_q \leq S_3$ con azione transitive

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

G_q azione transitive $\Rightarrow G_q = A_3$ oppure $G_q = S_3$
" $\langle (1,2,3) \rangle$

$G_q = A_3 \Leftrightarrow d = -a_1^3 a_3 + a_1^2 a_2^2 + 18 a_1 a_2 a_3 - 4 a_2^3 - 27 a_3^2$
ha radici in F

$G_q = S_3 \Leftrightarrow d$ non ha radici in F

[d ha un ruolo importante]