Gruppi di Galois

Note Title 12/7/2018

Prop K campo, $f(x) \in K[x]$ irriducibile, $L =$ cds di $f(x)$ su K. Supponiamo che $f(x)$ non abbia radici multiple in L. Allora

$$\# \mathrm{Gal}(L/K) = [L:K]$$

Dim. L/K e' normale (visto a lezione).

Immergiamo K, L in una chiusura algebrica E.

$$\begin{array}{l} L \\ | \\ K \xhookrightarrow[id]{} E \end{array}$$

Teo visto a lez $\Rightarrow \exists\ [L:K]$ omomorf. $L \to E$ che estendono id. Siccome L/K e' normale, ognuno di questi e' in realta' un omomorfismo $L \to L$, cioe' un elemento di $\mathrm{Gal}(L/K)$ $\square$

GRADO 2 $\mathrm{char}(K) \neq 2$, sia L/K un'est. quadratica.

L/K e' automatic. normale, e quindi

$$\mathrm{Gal}(L/K) \simeq \mathbb{Z}/2\mathbb{Z}$$

$L = K \oplus K\alpha$. Siccome $\mathrm{char}(K) \neq 2$, posso scegliere α in modo tale che $\alpha^2 \in K$

Infatti: sia $m_\alpha(x) = x^2 + bx + c$ il pol. min. di α. Allora $\underbrace{\left(\alpha + \frac{b}{2}\right)}_{\text{genera } L \text{ su } K}^2 + c - \frac{b^2}{4} = 0$,

si ha $L = K \oplus K \underbrace{\left(\alpha + \frac{b}{2}\right)}_{\alpha'}$ e $(\alpha')^2 = \frac{b^2}{4} - c \in K$

L'automorfismo non banale $L \longrightarrow L$ è

$$x + y\alpha' \longmapsto x - y\alpha'$$

⌜In generale: $\alpha \longmapsto -b - \alpha$. Funziona anche in char $= 2$ ⌟

Lemma L_1 L_2 due estensioni normali.

$$\begin{array}{ccc} L_1 & & L_2 \\ & \diagdown \; \diagup & \\ & K & \end{array}$$

Allora: (i) $L_1 L_2 / K$ è normale

(ii) $\mathrm{Gal}(L_1 L_2 / K) \hookrightarrow \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$

Dim Sia E una chiusura alg. che contiene tutto

Consideriamo $\varphi : L_1 L_2 \longrightarrow E$

$\varphi|_{L_1} : L_1 \longrightarrow E$, con img. $L_1 \subseteq L_1 L_2$

$\varphi|_{L_2} : L_2 \longrightarrow E$, ——— $L_2 \subseteq L_1 L_2$

Siccome L_1 e L_2 generano L_1L_2, otteniamo che $\varphi(L_1L_2) \subseteq L_1L_2$.

Inoltre: $\operatorname{im}\varphi \supseteq L_1$, $\operatorname{im}\varphi \supseteq L_2 \Rightarrow \varphi(L_1L_2) \supseteq L_1L_2$

(ii) $$\operatorname{Gal}(L_1L_2/K) \longrightarrow \operatorname{Gal}(L_1/K) \times \operatorname{Gal}(L_2/K)$$
$$\varphi \longmapsto (\varphi|_{L_1}, \varphi|_{L_2})$$

φ omom: $L_1L_2 \longrightarrow E$

Ben definito perché L_1, L_2 sono normali $/K$
Iniettivo perché L_1, L_2 generano L_1L_2, quindi conoscere φ su L_1 e su L_2 è sufficiente a conoscere φ su tutto L_1L_2. □

Cor. $\mathbb{Q}(\sqrt{a})$, $\mathbb{Q}(\sqrt{b})$ due est. quadr. distinte di $\mathbb{Q}$.

$$\operatorname{Gal}(\mathbb{Q}(\sqrt{a}, \sqrt{b})/\mathbb{Q}) = ?$$

Dim
- $\mathbb{Q}(\sqrt{a}, \sqrt{b}) =: K$ è normale su $\mathbb{Q}$ in quanto composto di ext quadr ($\Rightarrow$ normali)
- $\# \operatorname{Gal}(\mathbb{Q}(\sqrt{a}, \sqrt{b})/\mathbb{Q}) = [K : \mathbb{Q}] = 4$
- $\operatorname{Gal}(K/\mathbb{Q}) \hookrightarrow \underbrace{\operatorname{Gal}(\mathbb{Q}(\sqrt{a})/\mathbb{Q})}_{\mathbb{Z}/2\mathbb{Z}} \times \underbrace{\operatorname{Gal}(\mathbb{Q}(\sqrt{b})/\mathbb{Q})}_{\mathbb{Z}/2\mathbb{Z}}$

per cardinalità è un isomorfismo.

$$K \ni x_0 + x_1\sqrt{a} + x_2\sqrt{b} + x_3\sqrt{ab} \longmapsto x_0 \pm x_1\sqrt{a} \pm x_2\sqrt{b} \pm x_3\sqrt{ab}$$

dove il terzo $\pm$ è il prodotto dei primi due $\square$

PATOLOGIE: assenza di separabilità

Def. Un polinomio $p(x) \in K[x]$ è detto SEPARABILE se non ha radici multiple.

Esempio Sia $K = \mathbb{F}_2(x,y) = \left\{ \dfrac{a(x,y)}{b(x,y)} \;\middle|\; \begin{array}{c} a,b \in \mathbb{F}_2[x,y] \\ b \neq 0 \end{array} \right\}$

$L \subseteq K, \quad L = \mathbb{F}_2(x^2, y^2)$

K/L è un'estensione di grado 4.

$$\left.\begin{tikzcd}
 & L(x,y)=K \arrow[dl, dash] \arrow[dr, dash] & \\
L(x) \arrow[dr, dash, "2"'] & & L(y) \arrow[dl, dash, "2"] \\
 & L &
\end{tikzcd}\right] \leq 4$$

$[L(x):L] \geq 2$: ovvio perché $x \notin L$

Se $[K:L]=2 \implies L(x) = L(y) \implies \left(x/y\right)^2$ è un quadrato IN L

$L(\sqrt{x^2}) = L(\sqrt{y^2})$

Se lo fosse, $x/y \in L$ $\quad \dfrac{x}{y} = \dfrac{a(x^2,y^2)}{b(x^2,y^2)}$, ma

questo è assurdo: $\underbrace{x\, b(x^2,y^2)}_{\deg_x \text{ dispari}} = \underbrace{y\, a(x^2,y^2)}_{\deg_x \text{ pari}}$

- Qual è il polinomio minimo di x su L?
  $p(t) \in L[t]$ t.c. $p(x) = 0$

$$p(t) = t^2 - x^2 \underset{\text{in } K[x]}{=} (t-x)^2$$

Abbiamo trovato un polinomio minimo (irriducibile) non separabile!

- K/L non e' semplice: supponiamo $K = L(f)$

$$f = \frac{a(x,y)}{b(x,y)} \qquad f^2 = \frac{a(x,y)^2}{b(x,y)^2} = \frac{a(x^2,y^2)}{b(x^2,y^2)} \in L$$

Quindi f soddisfa polinomio di grado 2 a coeff. in $L \Rightarrow [L(f):L] \leq 2 \Rightarrow L(f) \neq K$.

- Esistono infinite est. intermedie

$$\begin{array}{c} K \\ |\ 2 \\ F \\ |\ 2 \\ L \end{array}$$

$$F = L(\sqrt{g}) \qquad g \in \mathbb{F}_2[x^2, y^2].$$

Due estensioni di questo tipo coincidono se e solo se g, g' differiscono per un quadrato in $\mathbb{F}_2(x^2,y^2)$

Basta allora prendere infiniti g irriducibili diversi.

(Piu' precisamente: $\tilde{g}(x^2,y^2)$ con $\tilde{g} \in \mathbb{F}_2[x,y]$ irrid.)

$$x^2 + x^2y^2 + y^4 = (x + xy + y^2)^2$$

GRADO 3

Esempio $\zeta = \zeta_7 \in \mathbb{C}$, $K = \mathbb{Q}(\zeta_7)$, $\alpha := \zeta + \zeta^{-1}$, $L = \mathbb{Q}(\alpha)$. $\quad \alpha \in \mathbb{R}$

(i) $[L : \mathbb{Q}] = 3$

$[K : \mathbb{Q}] = 6 = 7 - 1$ perché $\dfrac{x^7 - 1}{x - 1} = 1 + x + \dots + x^6$ è irrid (Eisenstein)

$$6\left[\begin{array}{c} K \\ | \\ L \\ | \\ \mathbb{Q} \end{array}\right. \qquad \left.\begin{array}{c} K \\ | \\ L \end{array}\right] \geq 2 : \quad L \subseteq \mathbb{R}, \ K \nsubseteq \mathbb{R}$$

D'altro canto, $\zeta + \zeta^{-1} = \alpha \Rightarrow \zeta^2 + 1 - \alpha\zeta = 0$,

cioè $X^2 - \alpha X + 1 \in L[X]$ ha ζ come radice

Quindi $[L(\zeta) : L] \leq 2$, ma $K = L(\zeta)$

(ii) Sia $L_i = \mathbb{Q}(\zeta^i + \zeta^{-i})$ $\quad i \geq 1$ intero

Dim che $L_i \subseteq L$ $\quad \forall i$

Supponiamo di no:

$$\begin{tikzcd} & K \arrow[dl, dash, "2"'] \arrow[dr, dash] & \\ L \arrow[dr, dash, "3"'] & & L_i \arrow[dl, dash] \\ & \mathbb{Q} & \end{tikzcd}$$

$\left(K = L L_i \text{ perché } [L L_i : L] \geq 2 \right)$

Quindi: se $L_i \nsubseteq L \Rightarrow K = L L_i$, assurdo perché $L L_i \subseteq \mathbb{R}$ ma K no.

(iii) $\psi : L \longrightarrow \mathbb{C}$ omom. non nullo.

Lo estendo a $\psi_K : K \longrightarrow \mathbb{C}$.

$\psi(L) = \psi_K(L) \subseteq \psi_K(K) = K$, perché $K/\mathbb{Q}$ e' normale (cds polinomio $x^7 - 1$)

$$\psi_K(\zeta) = \zeta^i \quad \text{con} \quad (i, 7) = 1$$

$$\psi(\zeta + \zeta^{-1}) = \psi_K(\zeta + \zeta^{-1})$$

$$= \psi_K(\zeta) + \psi_K(\zeta)^{-1} = \underbrace{\zeta^i + \zeta^{-i}}_{\in\, L_i \subseteq L}.$$

Conclusione: $\psi(L) \subseteq L \Rightarrow L/\mathbb{Q}$ normale.

$\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$ per cardinalita'

$$\{ id,\ \zeta + \zeta^{-1} \mapsto \zeta^2 + \zeta^{-2},\ \zeta + \zeta^{-1} \mapsto \zeta^3 + \zeta^{-3} \}$$

Infatti so che sono tutti del tipo $\zeta + \zeta^{-1} \mapsto \zeta^i + \zeta^{-i}$, e $i = 1, 2, 3$ ne danno 3 diversi
ogni altro i riproduce uno di questi

(iv) $1 + \zeta + \zeta^2 + \dots + \zeta^6 = 0$

$$\zeta^{-3} + \underbrace{\zeta^{-2} + \underbrace{\zeta^{-1} + 1 + \zeta}_{\alpha} + \zeta^2}_{\alpha^2 - 2} + \zeta^3 = 0$$

$$1+\alpha+(\alpha^2-2)+(\alpha^3-3\alpha)=0$$

$$(\zeta+\zeta^{-1})^3=\zeta^3+\zeta^{-3}+3\zeta^{2-1}+3\zeta^{1-2}$$
$$=\zeta^3+\zeta^{-3}+3\alpha$$

Siccome sappiamo che α e' di grado 3, il suo pol minimo e' $x^3+x^2-2x-1=0$

$\boxed{\text{GRADO 3}}$ $f(x)\in K[x]$ di grado 3 irrid. separabile ($\operatorname{char} K\neq 2,3$)

$$\begin{array}{c} L=\operatorname{cds} f(x) \\ | \\ K(\alpha) \\ 3\,| \\ K \end{array}$$

α = radice di $f(x)$ in una chiusura algebrica

$\alpha=\alpha_1,\alpha_2,\alpha_3$ tutte le radici di $f(x)$

Sappiamo:
- L/K normale
- $|\operatorname{Gal}(L/K)|=[L:K]$
- $\operatorname{Gal}(L/K)\subseteq S_3$

$\operatorname{Gal}(L/K)\in\{A_3,S_3\}$. Come si distinguono?

Introduciamo $\Delta:=\left((\alpha_1-\alpha_2)(\alpha_2-\alpha_3)(\alpha_3-\alpha_1)\right)^2$

- $\Delta\in K$: e' una funzione simmetrica di $\alpha_1,\alpha_2,\alpha_3$

$$\Delta(\alpha_1,\alpha_2,\alpha_3)=\Delta(\alpha_2,\alpha_1,\alpha_3)$$

$\boxed{\text{FATTO}}$ Ogni funzione simmetrica si esprime in funzione di $\alpha_1+\alpha_2+\alpha_3$, $\alpha_1\alpha_2+\alpha_2\alpha_3+\alpha_3\alpha_1$, $\alpha_1\alpha_2\alpha_3$

Nel nostro caso, sono elementi di K!

Sottoproblema Calcoliamo $\mathrm{disc}(x^3+ax+b)$

$$x^3+a_2x^2+a_1x+a_0$$

$$\left(x+\frac{a_2}{3}\right)^3+\dots$$

$$\mathrm{disc}(x^3+ax+b) = \det\begin{pmatrix} 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \end{pmatrix}^2$$

$$= \det\begin{pmatrix} 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \end{pmatrix}\begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 \\ 1 & \alpha_2 & \alpha_2^2 \\ 1 & \alpha_3 & \alpha_3^2 \end{pmatrix} =$$

$$= \det\begin{pmatrix} 3 & s_1 & s_2 \\ s_1 & s_2 & s_3 \\ s_2 & s_3 & s_4 \end{pmatrix} \qquad s_j = \alpha_1^j+\alpha_2^j+\alpha_3^j$$

$$s_1 = 0$$

$$s_2 = \alpha_1^2+\alpha_2^2+\alpha_3^2 = (\alpha_1+\alpha_2+\alpha_3)^2-2(\alpha_1\alpha_2+\alpha_2\alpha_3+\alpha_3\alpha_1)$$
$$= -2a$$

$$s_4 = \alpha_1^4+\alpha_2^4+\alpha_3^4 = (\alpha_1^2+\alpha_2^2+\alpha_3^2)^2 +$$
$$-2(\alpha_1^2\alpha_2^2+\alpha_2^2\alpha_3^2+\alpha_3^2\alpha_1^2)$$
$$= 4a^2-2\left[(\alpha_1\alpha_2+\alpha_2\alpha_3+\alpha_3\alpha_1)^2 - 2\alpha_1\alpha_2\alpha_3(\alpha_1+\alpha_2+\alpha_3)\right]$$
$$= 2a^2$$

$$s_3 = -3b$$

$$\operatorname{disc}(x^3+ax+b) = -4a^3 - 27b^2$$

$$\begin{tikzcd}[column sep=small]
 & L=K(\alpha_1,\alpha_2,\alpha_3) \arrow[dl, dash] \arrow[dr, dash] & \\
K(\alpha) \arrow[dr, dash, "3"'] & & K(\sqrt{\Delta}) \arrow[dl, dash, "\leq 2"] \\
 & K &
\end{tikzcd}$$

$$\sqrt{\Delta} = (\alpha_1-\alpha_2)(\alpha_2-\alpha_3)(\alpha_3-\alpha_1)$$

Dimostriamo che $L = K(\alpha, \sqrt{\Delta})$.

$$\sqrt{\Delta} = \alpha_1^2(\alpha_3-\alpha_2) + \alpha_1(-\alpha_3^2+\alpha_2^2) + {}$$
$$-\alpha_2^2\alpha_3 + \alpha_3^2\alpha_2$$
$$= (\alpha_3-\alpha_2)\left[\alpha_1^2 + \alpha_1(-\alpha_3-\alpha_2) + \alpha_2\alpha_3\right]$$
$$= (\alpha_3-\alpha_2)\left[\alpha_1^2 + \alpha_1(\alpha_1) + \frac{\alpha_1\alpha_2\alpha_3}{\alpha_1}\right]$$
$$= (\alpha_3-\alpha_2)\left[2\alpha_1^2 - b/\alpha_1\right]$$

In $K(\sqrt{\Delta}, \alpha_1)$ c'è $\dfrac{\sqrt{\Delta}}{2\alpha_1^2 - b/\alpha_1} = \alpha_3 - \alpha_2$

e anche $\alpha_2 + \alpha_3 = -\alpha_1$

$$\Rightarrow K(\sqrt{\Delta}, \alpha_1) \supseteq K(\alpha_1, \alpha_2, \alpha_3)$$

CONCLUSIONE: $[L:K] = \begin{cases} 3 & \text{se } \sqrt{\Delta} \in K \\ 6 & \text{se } \sqrt{\Delta} \notin K \end{cases}$