Teoria di Galois

Note Title 12/12/2018

Equazioni biquadratiche

$p(x) = x^4 + ax^2 + b \in \mathbb{Q}[x]$ irriducibile

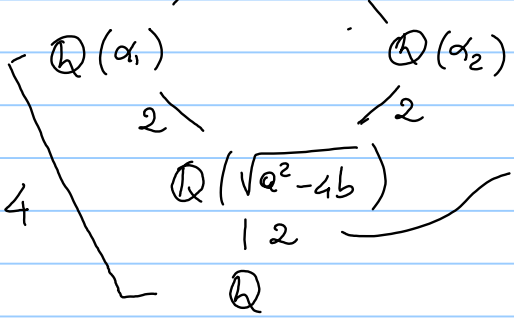
K = cds di $p(x)$

$G = Gal(K/\mathbb{Q})$

$$\alpha_1 = \sqrt{\frac{-a + \sqrt{a^2-4b}}{2}}$$

$$\pm \sqrt{\frac{-a \pm \sqrt{a^2-4b}}{2}}$$

$$\alpha_2 = \sqrt{\frac{-a - \sqrt{a^2-4b}}{2}}$$



se $a^2-4b \in \mathbb{Q}^{\times 2}$ allora $p(x)$ riducibile

$[K:\mathbb{Q}] \in \{4, 8\}$

$G \hookrightarrow S_4$ $\quad \#S_4 = 24 \Rightarrow$ se $\#G = 8$, allora $G \simeq$ 2-Sylow di S_4

$\Rightarrow G \simeq D_4$

$\#G = 4 \iff \mathbb{Q}(\alpha_1) = \mathbb{Q}(\alpha_2) \iff$

$\iff \frac{-a + \sqrt{a^2-4b}}{2}$ e $\frac{-a - \sqrt{a^2-4b}}{2}$ differiscono per un quadrato in $\mathbb{Q}(\sqrt{a^2-4b})$

$\iff \frac{-a + \sqrt{a^2-4b}}{2} \cdot \frac{-a - \sqrt{a^2-4b}}{2} = \square$ in $\mathbb{Q}(\sqrt{a^2-4b})$

$\iff b = \left(x + y\sqrt{a^2-4b}\right)^2$ con $x, y \in \mathbb{Q}$

$\iff b = x^2 + y^2 \cdot (a^2-4b) + 2xy\sqrt{a^2-4b}$

Due casi: $x=0$ e $b = y^2 \cdot (a^2-4b)$

$\iff b\cdot(a^2-4b) \in \mathbb{Q}^{\times 2}$

$y=0 \iff b = x^2 \in \mathbb{Q}^{\times 2}$

Se $b \in \mathbb{Q}^{\times 2}$ o $b\cdot(a^2-4b) \in \mathbb{Q}^{\times 2} \Rightarrow \#G = 4$

Altrimenti $\#G = 8$, $G \simeq D_4$

Consideriamo più in dettaglio il caso $\#G = 4$.

Un automorfismo φ di $\mathbb{Q}(\alpha_1)$ manda α_1 in α_1, α_2, $-\alpha_1$, $-\alpha_2$

$\alpha_1 \longrightarrow id$; $-\alpha_1$ ord 2

Se $\varphi(\alpha_1) = -\alpha_1$, allora $\varphi(-\alpha_1) = \alpha_1$

e quindi $\varphi(\alpha_2) = \pm\alpha_2$ $\quad \varphi(-\alpha_2) = \mp\alpha_2$

Un tale automorfismo rispetta $\varphi^2 = id$

Consideriamo allora $\psi: \mathbb{Q}(\alpha_1) \longrightarrow \mathbb{Q}(\alpha_1)$

$\alpha_1 \longmapsto \alpha_2$

$\alpha_1\alpha_2 = \sqrt{b} \Rightarrow \psi(\alpha_1)\psi(\alpha_2) = \psi(\sqrt{b})$

$\alpha_2\,\psi(\alpha_2) = \psi(\sqrt{b})$

* Se $b \in \mathbb{Q}^{\times 2}$, allora $\alpha_2\,\psi(\alpha_2) = \sqrt{b} = \alpha_1\alpha_2$

$\Rightarrow \psi(\alpha_2) = \alpha_1$

e quindi ψ è di ordine 2.

$\Rightarrow G$ non contiene el. ord 4 $\Rightarrow G \simeq (\mathbb{Z}/2\mathbb{Z})^2$

* Se $b \notin \mathbb{Q}^{\times 2}$ ma $b\cdot(a^2-4b) \in \mathbb{Q}^{\times 2}$

$b = k^2\cdot(a^2-4b) \Rightarrow \sqrt{b} = \pm k\sqrt{a^2-4b}$

$\alpha_1 = \sqrt{\dfrac{-a+\sqrt{a^2-4b}}{2}} \Rightarrow 2\alpha_1^2 + a = \sqrt{a^2-4b}$

Applichiamo ψ: $\quad 2\alpha_2^2 + a = \psi\left(\sqrt{a^2-4b}\right)$

$$\| \\ -\sqrt{a^2-4b}$$

$$\Rightarrow \psi(\sqrt{b}) = \psi\left(\pm k\sqrt{a^2-4b}\right) = \pm k \cdot \left(-\sqrt{a^2-4b}\right) = -\sqrt{b}$$

$$\alpha_2\ \psi(\alpha_2) = \psi(\sqrt{b}) \Rightarrow \alpha_2 \cdot \psi(\alpha_2) = -\sqrt{b} = -\alpha_1\alpha_2$$

$$\Rightarrow \psi(\alpha_2) = -\alpha_1$$

Questo ψ agisce come segue:

$$\begin{array}{ccc} \alpha_1 & \longrightarrow & \alpha_2 \\ \uparrow & & \downarrow \\ -\alpha_2 & \longleftarrow & -\alpha_1 \end{array}$$

Conclusione: G è $(\mathbb{Z}/2\mathbb{Z})^2$ se $b = \square$

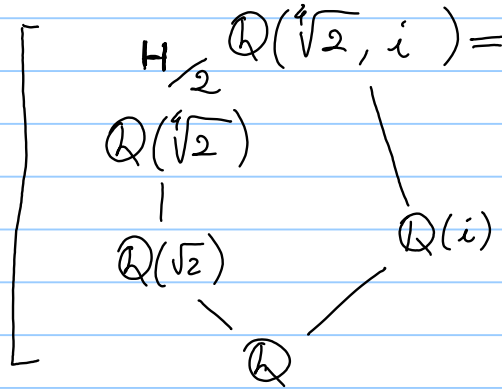
è $(\mathbb{Z}/4\mathbb{Z})$ se $b\cdot(a^2-4b) = \square$

è D_4 altrimenti.

Esercizio $\mathbb{Q}(\sqrt[4]{2})$ ha come unica sottoestensione $\mathbb{Q}(\sqrt{2})$

Soluzione

$G \simeq D_4$



$x^4 - 2$ (biquadratica $a=0$, $b=-2$)

Un automorfismo di K manda $\begin{array}{l} i \longmapsto \pm i \\ \sqrt[4]{2} \longmapsto i^k \sqrt[4]{2} \end{array}$

e tutte le scelte sono possibili, perché ci sono solo 2×4 scelte totali e $\#G = 8$.

$$r := \begin{cases} i \mapsto i \\ \sqrt[4]{2} \mapsto i \cdot \sqrt[4]{2} \end{cases} \qquad s: \begin{cases} i \longmapsto -i \\ \sqrt[4]{2} \longmapsto \sqrt[4]{2} \end{cases}$$

Qual è il gruppo corrispondente a $\mathbb{Q}(\sqrt[4]{2})$? $\langle s \rangle$

Infatti: * $\langle s \rangle$ fissa $\mathbb{Q}(\sqrt[4]{2})$ per definizione

* $\left| Gal\left(K / \mathbb{Q}(\sqrt[4]{2}) \right) \right| = [K : \mathbb{Q}(\sqrt[4]{2})] = 2$

Via corrisp. di Galois, devo trovare i sottogruppi

L di D_4 t.c. $\quad \langle s \rangle \underset{2}{\subseteq} L \underset{4}{\subseteq} D_4$

L'unico L possibile è $\langle s, r^2 \rangle$; verifichiamo che corrisponde a $\mathbb{Q}(\sqrt{2})$.

$$[K : K^L] = \#L = 4 \Rightarrow [K^L : \mathbb{Q}] = \frac{\#G}{4} = 2$$

($[K:\mathbb{Q}]$ sopra $\#G$; $[K:K^L]$ sotto 4)

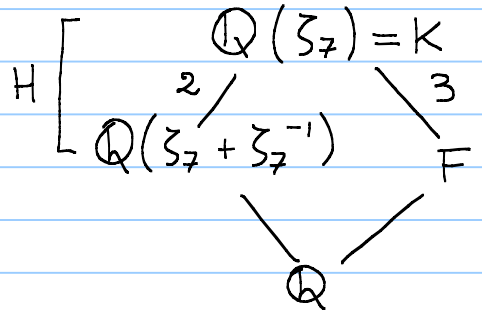
$$s : \begin{matrix} i \mapsto -i \\ \sqrt[4]{2} \mapsto \sqrt[4]{2} \end{matrix} \qquad r^2 : \begin{cases} i \mapsto i \\ \sqrt[4]{2} \mapsto -\sqrt[4]{2} \end{cases}$$

Un el. fisso è $a_0 + a_1 \sqrt[4]{2} + a_2 (\sqrt[4]{2})^2 + a_3 (\sqrt[4]{2})^3$

t.c. $\quad a_0 - a_1 \sqrt[4]{2} + a_2 \overset{11}{(\sqrt[4]{2})^2} - a_3 (\sqrt[4]{2})^3$

Campo fisso $= \{ a_0 + a_2 \sqrt{2} \} = \mathbb{Q}(\sqrt{2})$

$\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$



$K/\mathbb{Q}$ Galois

$\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/7\mathbb{Z})^\times$

$\{\varphi : \zeta_7 \mapsto \zeta_7^i \mid (i,7) = 1\}$

Chi è H? $H \supseteq \{id,\ \zeta_7 \mapsto \zeta_7^{-1}\}$

$=$ per cardinalità

$$\mathrm{Gal}\left(\mathbb{Q}(\zeta_7 + \zeta_7^{-1})/\mathbb{Q}\right) \simeq G/H \simeq \frac{\mathbb{Z}/6\mathbb{Z}}{\mathbb{Z}/2\mathbb{Z}} \simeq \mathbb{Z}/3\mathbb{Z}$$

$H_3 < (\mathbb{Z}/7\mathbb{Z})^\times$ sgrp ord. 3, $H_3 = \{1, 2, 4\}$

$F = K^{H_3}$ $\qquad [F:\mathbb{Q}] = [G:H_3] = 6/3 = 2$

Un elemento invariante è $\beta = \underbrace{\zeta + \zeta^2 + \zeta^4}_{\text{orbita di } \zeta \text{ per l'az. di } H_3} \in F$

$$\beta^2 = \zeta^2 + \zeta^4 + \zeta + 2(\zeta^3 + \zeta^5 + \zeta^6)$$

$$= \beta + 2(\underbrace{\zeta^3 + \zeta^5 + \zeta^6 + \beta - \beta}_{= -1,\ \text{perché } 1+\zeta+\zeta^2+\dots+\zeta^6 = 0})$$

$$= \beta - 2 - 2\beta = -\beta - 2$$

$$\beta^2 + \beta + 2 = 0 \qquad \beta = \frac{-1 \pm \sqrt{-7}}{2}$$

$$\Rightarrow F = \mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{-7})$$

Polinomi con gruppo di Galois S_p

Sia $f(x) \in \mathbb{Q}[x]$ irrid, di grado p primo, con esattamente $p-2$ radici reali. $K =$ cds di $f(x)$.

$$G := \mathrm{Gal}(K/\mathbb{Q}) \simeq S_p$$

(i) $\#G = [K:\mathbb{Q}] \mid p!$ e $p \mid \#G$

(perché $p = [\mathbb{Q}(\alpha_1):\mathbb{Q}]$ divide $[K:\mathbb{Q}]$)

K
|
$\mathbb{Q}(\alpha_1)$] p
|
$\mathbb{Q}$

$\xRightarrow{\text{Cauchy}}$ G contiene un p-ciclo

(ii) Consideriamo la restrizione di $\tau: \begin{matrix} \mathbb{C} \to \mathbb{C} \\ z \mapsto \bar{z} \end{matrix}$ a K

$\tau|_K \in S_p$ come è fatto? È una trasposizione

(delle 2 radici cpx coniugate)

(iii) $G \ni$ p-ciclo, trasposizione $\Rightarrow$ $G \simeq S_p$

↑ esercizio!

□

Cerchiamo polinomi che rispettino le ipotesi $h = \frac{p-3}{2}$

$$d \times (x^2-4)(x^2-(2\cdot 2)^2)(x^2-(2\cdot 3)^2)\cdots(x^2-(2h)^2)(x^2+4)+2$$

d intero dispari

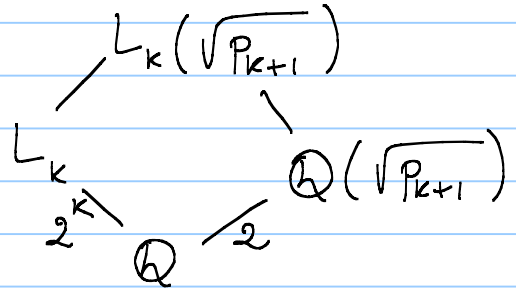
- Irriducibile per Eisenstein
- Radici: valori intermedi + continuità radici nei coefficienti.

$\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_k})$

- $L_k = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_k})/\mathbb{Q}$ normale
- $\mathrm{Gal}(L_k/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^k$

(p_i primi distinti)

Per induzione su k.



Ultima volta: composto ext. normali è normale;

$$\mathrm{Gal}(L_k(\sqrt{p_{k+1}})/\mathbb{Q}) \hookrightarrow \mathrm{Gal}(L_k/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\sqrt{p_{k+1}})/\mathbb{Q})$$

$$12 \qquad (\mathbb{Z}/2\mathbb{Z})^k \times \mathbb{Z}/2\mathbb{Z}$$

Serve: $\sqrt{p_{k+1}} \notin L_k$.

Cerchiamo tutte le sottoext quadr. di L_k.

Tante le conosciamo: dato $I \subseteq \{1, \dots, k\}$, $I \neq \emptyset$,

in L_k c'è $\sqrt{\prod_{i \in I} p_i}$

Queste sono $2^k - 1$, e sono distinte:

$$\left(\prod_{i \in I_1} p_i\right)\left(\prod_{i \in I_2} p_i\right) = \square \rightarrow I_1 = I_2 \text{ per fattorizz. unica}$$

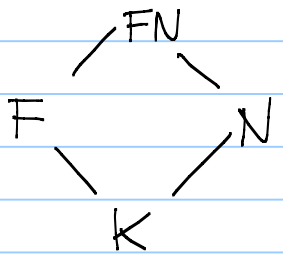
Per corrisp. Galois, ext quadr = sgrup indice 2 in $(\mathbb{Z}/2\mathbb{Z})^k$

Definito da 1 eqz. lineare $a_1 x_1 + \dots + a_k x_k = 0$

ce ne sono esattamente $2^k - 1$

Nessuna delle estensioni quadr. trovate è $\sqrt{P_{k+1}}$, e questo completa il passo induttivo. □

Shift di un'estensione di Galois



N/K normale

F/K qualunque

FN/F normale e

$$\mathrm{Gal}(FN/F) \hookrightarrow \mathrm{Gal}(N/K)$$
$$\varphi \longmapsto \varphi|_N$$

- N = cds di un certo $p(x) \in K[x]$

  $\Rightarrow FN$ = cds di $p(x) \in F[x]$

- $\varphi \mapsto \varphi|_N$ è ben def. perché N normale

  Se $\varphi \in \mathrm{Gal}(FN/F)$, fissa F
  se in più $\varphi|_N = id \in \mathrm{Gal}(N/K)$, allora φ fissa N

  $\Rightarrow \varphi$ fissa $FN \Rightarrow \varphi = id$. □