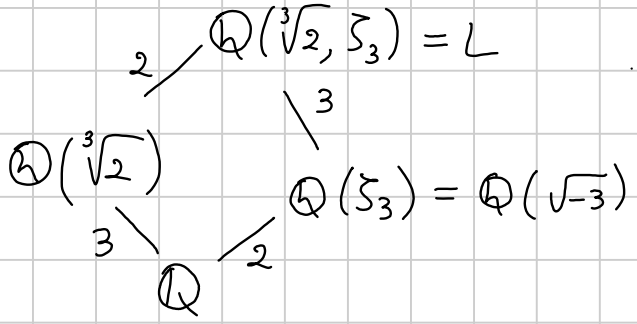
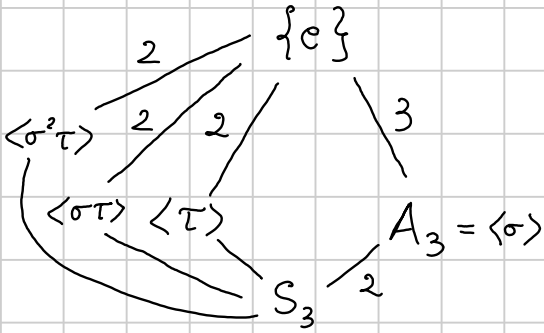
TEORIA DI GALOIS - APPLICAZIONI

Note Title 18/12/2018

Campo di spezzamento $x^3 - 2$





$L/\mathbb{Q}$ è Galois con gruppo S_3

Generatori gruppo di Galois:

$$\sigma : \begin{cases} \sqrt[3]{2} \mapsto \zeta_3 \sqrt[3]{2} \\ \zeta_3 \mapsto \zeta_3 \end{cases} \longleftrightarrow (1,2,3)$$

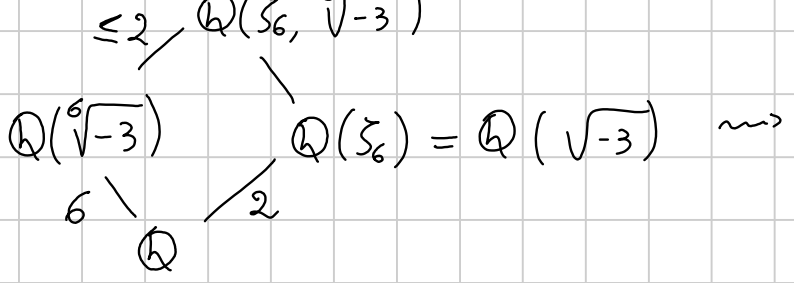
Siano $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \zeta_3 \sqrt[3]{2}$, $\alpha_3 = \zeta_3^2 \sqrt[3]{2}$

$$\tau = \text{coniugio complesso}|_L : \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \zeta_3 \mapsto \zeta_3^2 \end{cases} \longleftrightarrow (1)(2,3)$$

$\sigma\tau = (1,2,3)(2,3) = (2,1) \rightsquigarrow$ campo fisso è $\mathbb{Q}(\alpha_3) = \mathbb{Q}(\sqrt[3]{2} \cdot \zeta_3^2)$

$\sigma^2\tau = (1,3) \rightsquigarrow$ campo fisso è $\mathbb{Q}(\alpha_2) = \mathbb{Q}(\sqrt[3]{2}\,\zeta_3)$

C.d.s. di $x^6 + 3$



c.d.s. $= \mathbb{Q}(\sqrt[6]{-3})$, $[\mathbb{Q}(\sqrt[6]{-3}) : \mathbb{Q}] = 6$

$$G := \mathrm{Gal}(\mathbb{Q}(\sqrt[6]{-3})/\mathbb{Q}) \simeq S_3 \;/\; \mathbb{Z}/6\mathbb{Z}$$

$$\sigma_i : \sqrt[6]{-3} \longmapsto \zeta_6^i \sqrt[6]{-3}$$

$$\zeta_6 = \frac{1+\sqrt{-3}}{2} = \frac{1+(\sqrt[6]{-3})^3}{2}$$

$$\sigma_i(\zeta_6) = \sigma_i\left(\frac{1+(\sqrt[6]{-3})^3}{2}\right) = \frac{1+(-1)^i(\sqrt[6]{-3})^3}{2}$$

$$= \begin{cases} \zeta_6 & \text{se } i \text{ è pari} \\ \bar{\zeta}_6 & \text{se } i \text{ è dispari} \end{cases}$$

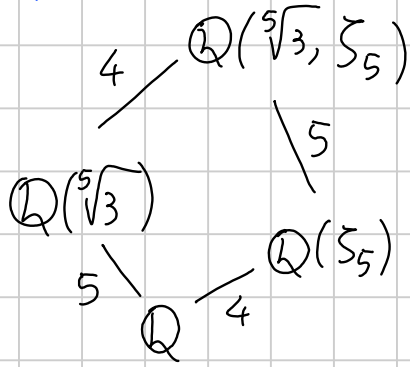
$$\sigma_i\sigma_j(\sqrt[6]{-3}) = \sigma_i(\zeta_6^j \sqrt[6]{-3})$$

$$= \sigma_i(\zeta_6)^j \, \sigma_i(\sqrt[6]{-3}) = \begin{cases} \zeta_6^j \cdot \zeta_6^i \sqrt[6]{-3} & (i \text{ pari}) \\ \zeta_6^{-j} \cdot \zeta_6^i \sqrt[6]{-3} & (i \text{ dispari}) \end{cases}$$

$$\sigma_1 \circ \sigma_3 (\sqrt[6]{-3}) = \zeta_6^{-2} \sqrt[6]{-3}$$

$$\sigma_3 \circ \sigma_1 (\sqrt[6]{-3}) = \zeta_6^2 \sqrt[6]{-3} \quad \Rightarrow \quad G \text{ non commut} \Rightarrow G \simeq S_3$$

Campo di spezzamento di $x^5 - 3$



$$G := \mathrm{Gal} \simeq (\mathbb{Z}/5\mathbb{Z}) \rtimes (\mathbb{Z}/5\mathbb{Z})^\times$$

Vorrei tutte le estensioni intermedie

$|G| = 20$

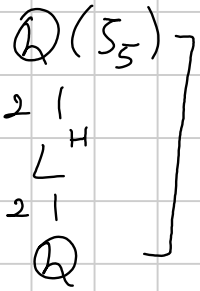
- Estensioni di grado 2 $\longleftrightarrow$ sottogp. indice 2 = card. 10

  Se $H < G$, $[G:H] = 2 \Rightarrow H$ contiene il 5-Sylow

  Il campo fisso del 5-Sylow ha grado 4 su $\mathbb{Q}$, e per unicità è $\mathbb{Q}(\zeta_5)$

  $$\Rightarrow L^H \subseteq L^{\mathbb{Z}/5\mathbb{Z}} = \mathbb{Q}(\zeta_5)$$

  Siccome $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$,



c'è un unico sottogp di indice 2 $\Rightarrow$ un unico sottocampo di grado 2.

H induce un sottogp $H' < Gal(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ di ordine 2. $H' = \{id, \text{coniugio cpx}\}$

$$\mathbb{Q}(\zeta_5)^{H'} \ni \zeta_5 + \overline{\zeta_5} = \zeta_5 + \zeta_5^{-1} =: \alpha$$

$$\alpha^2 = \zeta_5^2 + 2 + \zeta_5^{-2} \qquad \alpha = \zeta_5 + \zeta_5^{-1}$$

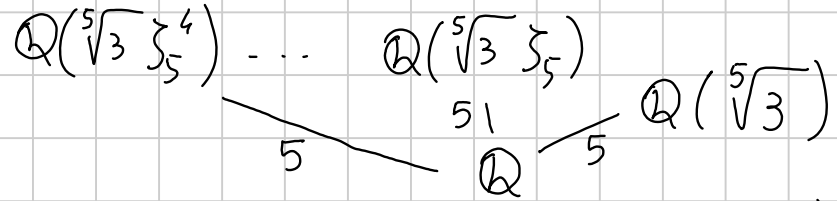
$$\underbrace{\alpha^2 + \alpha}_{2 + \underbrace{\zeta_5^4 + \zeta_5^3 + \zeta_5^2 + \zeta_5}_{=-1}} = 1 \qquad \alpha = \frac{-1 \pm \sqrt{5}}{2}$$

L'unica sottoest. quadr. è quindi $\mathbb{Q}(\sqrt{5})$

- Estensioni di grado 4 $\longleftrightarrow$ sottogp indice 4 = sottogp ordine 5 = 5-Sylow, ce n'è uno solo

Quindi c'è un'unica sottoest. di grado 4, che deve essere $\mathbb{Q}(\zeta_5)$

- Estensioni di grado 5 $\longleftrightarrow$ sottogp indice 5 = 2-Sylow, e ce ne sono 5



Sono tutte distinte: se $\mathbb{Q}(\sqrt[5]{3}\,\zeta_5^i) = \mathbb{Q}(\sqrt[5]{3}\,\zeta_5^j)$,

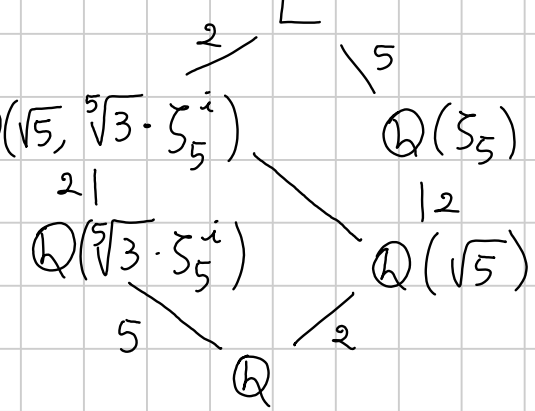
allora questo campo conterrebbe $\zeta_5^{i-j} = \dfrac{\sqrt[5]{3}\,\zeta_5^i}{\sqrt[5]{3}\,\zeta_5^j}$

$\Rightarrow$ avrebbe grado multiplo di $4 = [\mathbb{Q}(\zeta_5) : \mathbb{Q}]$, assurdo

- Estensioni di grado 10

$$L = \mathbb{Q}(\sqrt[5]{3}, \zeta_5) = \mathbb{Q}(\zeta_5 + \sqrt[5]{3})$$

$$\mathbb{Q}(\sqrt{5}+\sqrt[5]{3}\zeta_5^i) = \mathbb{Q}(\sqrt{5}, \sqrt[5]{3}\cdot\zeta_5^i)$$



Vorremmo vedere che $\mathbb{Q}(\sqrt{5}, \sqrt[5]{3}\cdot\zeta_5^i)$ sono le uniche sottoext di grado 10. $\longleftrightarrow$ sottogp di ordine 2 $\longleftrightarrow$ elementi di ordine 2; questi sono 5 (calcolo diretto, oppure notando che c'è un unico el. di ordine 2 in ogni 2-Sylow)

Osserviamo che $L = \mathbb{Q}(\sqrt[5]{3} + \zeta_5)$. $\supseteq$ ovvio.

$\subseteq$: supponiamo per assurdo che $\mathbb{Q}(\sqrt[5]{3}+\zeta_5) \subsetneq L$

$$\Rightarrow \mathbb{Q}(\sqrt[5]{3}+\zeta_5) \subseteq \begin{cases} \mathbb{Q}(\zeta_5) & ① \\ \mathbb{Q}(\sqrt{5}, \sqrt[5]{3}\cdot\zeta_5^i) & ② \end{cases}$$

① Allora $\mathbb{Q}(\zeta_5) \ni (\sqrt[5]{3}+\zeta_5) - \zeta_5 = \sqrt[5]{3}$, assurdo.

② Descriviamo $\mathbb{Q}(\sqrt{5}, \sqrt[5]{3}\cdot\zeta_5^i)$ come campo fisso di un sottogruppo.

Un el. del gruppo di Galois manda

$$\sigma: \begin{cases} \sqrt[5]{3} \mapsto \zeta_5^j \sqrt[5]{3} \\ \zeta_5 \mapsto \zeta_5^k = \zeta_5^{-1} \end{cases}$$

Se $\text{ord}(\sigma) = 2$, allora $k = -1$.

Voglio imporre $\sigma(\sqrt[5]{3}\,\zeta_5^{\,i}) = \sqrt[5]{3}\cdot\zeta_5^{\,i}$

$\zeta_5^{\,j}\cdot\sqrt[5]{3}\cdot\zeta_5^{\,-i}$

Quindi devo scegliere $j = 2i$.

E' possibile che σ fissi $\sqrt[5]{3}+\zeta_5$?

$$\sigma(\sqrt[5]{3}+\zeta_5) = \sqrt[5]{3}+\zeta_5$$

$$\zeta_5^{2i}\sqrt[5]{3}+\zeta_5^{-1}$$

$$\Leftrightarrow \quad \sqrt[5]{3}\left(\zeta_5^{\,2i}-1\right) = \zeta_5-\overline{\zeta_5}$$

assurdo

questo non è immag. puro

$\zeta_5-\overline{\zeta_5}$ è immaginario puro

Estensioni cicliche di grado 3

K = campo di caratt $\neq 3$

F/K est. di Galois con gruppo $\mathbb{Z}/3\mathbb{Z}$

* Se $\zeta_3 \in K$, allora $\exists\, a \in K^\times$ t.c. $F = K(\sqrt[3]{a})$

$F = K(\beta)$ $\qquad$ $\sigma \in Gal(F/K)$

$\sigma(\sqrt[3]{a}) = \zeta_3^{\,i} \cdot \sqrt[3]{a}$

Siano $\beta_1 = \beta, \beta_2, \beta_3$ le altre radici del polin. minimo di β (CONIUGATI DI β)

$$\sigma(c_1\beta_1 + c_2\beta_2 + c_3\beta_3) = c_1\beta_2 + c_2\beta_3 + c_3\beta_1$$
$$\stackrel{?}{=} \zeta_3(c_1\beta_1 + c_2\beta_2 + c_3\beta_3)$$

Imponendo l'uguaglianza di ogni coefficiente,

$$\begin{cases} c_3 = \zeta_3 c_1 \\ c_1 = \zeta_3 c_2 \\ c_2 = \zeta_3 c_3 \end{cases} \qquad \begin{cases} c_3 = \zeta_3 c_1 \\ c_1 = c_1 \\ c_2 = \zeta_3(\zeta_3 c_1) = \zeta_3^2 c_1 \end{cases}$$

Posso quindi prendere $\beta_1 + \zeta_3^2\beta_2 + \zeta_3\beta_3 =: \gamma$

$$\sigma(\beta_1 + \zeta_3^2\beta_2 + \zeta_3\beta_3) = \beta_2 + \zeta_3^2\beta_3 + \zeta_3\beta_1$$

Voglio mostrare che $F = K(\gamma)$ e che $\gamma^3 \in K$

- $\gamma^3 \in K$: se e solo se $\sigma(\gamma^3) = \gamma^3$
  $\iff$ $\sigma(\gamma)^3 = \gamma^3$
  $\iff$ $(\zeta_3\gamma)^3 = \gamma^3$ ok
- $\gamma \notin K$: $\sigma(\gamma) \neq \gamma \iff \zeta_3\gamma \neq \gamma$, ok purché γ non sia zero.

Un calcolo mostra che $\gamma \cdot (\beta_1 + \zeta_3 \beta_2 + \zeta_3^2 \beta_3) = -3p$,

dove il pol. minimo di β è $\beta^3 + p\beta + q = 0$. Quindi siamo

a posto se $p \neq 0$, e se $p = 0$ allora $\beta_2 = \zeta_3 \beta_1$, $\beta_3 = \zeta_3^2 \beta_1$,
da cui $\gamma = \beta_1 + \zeta_3^2 \beta_2 + \zeta_3 \beta_3 = 3\beta_1 \neq 0$.

$* \quad K(\sqrt[3]{a}) = K(\sqrt[3]{b}) \iff a/b \in K^{\times 3}$ oppure
$a^2/b \in K^{\times 3}$

$\Leftarrow$ Se $\sqrt[3]{b} = k \cdot \sqrt[3]{a^2} \Rightarrow \sqrt[3]{b} \in K(\sqrt[3]{a})$

$\Downarrow$

$\sqrt[3]{b^2} = k^2 \cdot a \cdot \sqrt[3]{a} \Rightarrow \sqrt[3]{a} \in K(\sqrt[3]{b})$

$\Rightarrow$ $\sqrt[3]{b} \in K(\sqrt[3]{a}) \Rightarrow \sqrt[3]{b} = c_0 + c_1 \sqrt[3]{a} + c_2 (\sqrt[3]{a})^2$

e $K(\sqrt[3]{a})/K$ è di Galois. Sia σ l'automorfismo
che manda $\sqrt[3]{a} \mapsto \zeta_3 \cdot \sqrt[3]{a}$

Applicando σ all'uguagl. di sopra,

$$\sqrt[3]{b} \cdot \zeta_3^i = c_0 + c_1 \cdot \zeta_3 \sqrt[3]{a} + c_2 \zeta_3^2 (\sqrt[3]{a})^2$$
$$\| \quad c_0 \zeta_3^i + c_1 \zeta_3^i \sqrt[3]{a} + c_2 \zeta_3^i (\sqrt[3]{a})^2$$

Siccome $1, \sqrt[3]{a}, (\sqrt[3]{a})^2$ è una base,

$$\begin{cases} c_0 = c_0 \cdot \zeta_3^i \\ c_1 \zeta_3 = c_1 \cdot \zeta_3^i \\ c_2 \zeta_3^2 = c_2 \cdot \zeta_3^i \end{cases} \Rightarrow \text{2 dei 3 coeff. sono 0, il terzo è libero}$$

Quindi: $\sqrt[3]{b} \in K(\sqrt[3]{a}) \Rightarrow$

$\sqrt[3]{b} = c_0 \rightsquigarrow b \in K^{\times 3}$

$\sqrt[3]{b} = c_1 \sqrt[3]{a} \rightsquigarrow b/a \in K^{\times 3}$

$\sqrt[3]{b} = c_2 (\sqrt[3]{a})^2 \rightsquigarrow b/a^2 \in K^{\times 3}$

Formula risolutiva per $x^3 + px + q = 0$

$x = u + v$ $\qquad u^3 + v^3 + 3uv(u+v) + p(u+v) + q = 0$

$$\begin{cases} u^3 + v^3 + (u+v)(p+3uv) + q = 0 \\ p + 3uv = 0 \end{cases}$$

$$\begin{cases} u^3 + v^3 = -q \\ u^3 \cdot v^3 = -p^3/27 \end{cases} \qquad u^3, v^3 = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

$$\mathrm{disc}(x^3 + px + q) = -4p^3 - 27q^2 = -108 \cdot \left(\frac{q^2}{4} + \frac{p^3}{27}\right)$$

$$= (-3) \cdot 36 \cdot \left(\frac{q^2}{4} + \frac{p^3}{27}\right)$$

$\mathbb{Q}(x_1, x_2, x_3)$ — $\mathbb{Q}(\zeta_3, x_1, x_2, x_3)$

$3 \mid$ — $\mathbb{Q}(\sqrt{\Delta}, \zeta_3)$ — ottenuta aggiungendo $\sqrt[3]{\text{qualcosa}}$

$\mathbb{Q}(\sqrt{\Delta})$ — $\mathbb{Q}(\zeta_3)$

$\leq 2 \mid$

$\mathbb{Q}$

$w_1 = x_1 + \zeta_3^2 x_2 + \zeta_3 x_3 \rightsquigarrow w_1^3 \in \mathbb{Q}(\sqrt{\Delta}, \zeta_3)$

$w_2 = x_1 + \zeta_3 x_2 + \zeta_3^2 x_3 \rightsquigarrow w_2^3 \in \mathbb{Q}(\sqrt{\Delta}, \zeta_3)$

$w_1 + w_2 + (x_1 + x_2 + x_3) = 3x_1$

$x_1 = \frac{w_1 + w_2}{3}$ $\qquad$ Con qualche calcolo si mostra che $\frac{w_1}{3}, \frac{w_2}{3}$ sono gli u, v di Cardano,

perché in effetti $\left(\frac{w_1}{3}\right)^3 + \left(\frac{w_2}{3}\right)^3 = -q$ e $\left(\frac{w_1}{3}\right)\left(\frac{w_2}{3}\right) = -p/3$

Osserviamo infine che $\mathrm{disc} = -3 \cdot 6^2 \cdot \left(\frac{q^2}{4} + \frac{p^3}{27}\right)$,

quindi $\mathbb{Q}(\zeta_3, \sqrt{\mathrm{disc}}) = \mathbb{Q}\left(\zeta_3, \sqrt{q^2/4 + p^3/27}\right)$