

L' EQUAZIONE GENERALE. DI GRADO n

Sia F campo e $t_1, \dots, t_n$ indeterminate di $F[t_1, \dots, t_n]$

Definiamo:

$$q(x) = x^n - t_1 x^{n-1} + t_2 x - \dots + (-1)^n t_n = 0$$

equazione generale di grado n su F

Si dice risolvibile se $q(x)$ è risolubile
per radicali sul campo $F(t_1, \dots, t_n)$
(campo dei quozienti di $F[t_1, \dots, t_n]$)

Osservazione: $\text{char } F \neq 2$ l'equazione generale
di grado 2 è risolubile

$$x_{1,2} = \frac{1}{2} t_1 \pm \frac{1}{2} \sqrt{t_1^2 - 4t_2} \quad \text{sono le soluzioni}$$

Le radici (ed il campo di spezzamento) sono contenute
in $F(t_1, t_2)(D)$ con $D^2 = t_1^2 - 4t_2 \in F(t_1, t_2)$

Cerchiamo di capire se $q(x)$ è risolubile per radicali su $F(t_1, \dots, t_m)$ studiando Gq e usando il criterio di Galois

Sia E il campo di spezzamento di $q(x)$

Su $F(t_1, \dots, t_m)$ e $q(x) = (x-y_1)(x-y_2)\dots(x-y_m) \in E[x]$

da cui $E = F(t_1, \dots, t_m)(y_1, \dots, y_m)$

Da $q(x) = (x-y_1)\dots(x-y_m)$ ricaviamo

$$t_1 = \sum_{i=1}^m y_i \quad t_2 = \sum_{i < j} y_i y_j \quad \dots \quad t_m = y_1 y_2 \dots y_m$$

da cui $E = F(y_1, \dots, y_m)$

Ricordo cose abbiamo ottenuto sul campo delle funzioni razionali a n variabili:

• Se $P_1 = x_1 + \dots + x_n$ $P_2 = \sum_{i < j} x_i x_j$ $\dots$ $P_n = x_1 \dots x_n$

sono le funzioni simmetriche elementari

allora $F(p_1, \dots, p_n)$ è il campo delle funzioni

simmetriche (funzioni lasciate invariate dalle permutazioni delle variabili)

- $F(x_1, \dots, x_n)$ è il campo di spezzamento di $h(x) = \prod_{i=1}^n (x - x_i) = x^n - P_1 x^{n-1} + \dots + (-1)^n P_n$
 $\text{Su } F(P_1, \dots, P_n) \quad \left(\frac{F(x_1, \dots, x_n)}{F(P_1, \dots, P_n)} \right)$ è est di Galois
 - $\text{Gal} \left(\frac{F(x_1, \dots, x_n)}{F(P_1, \dots, P_n)} \right) \cong G_h \cong S_n$
-

Costruiamo $\hookrightarrow: F[t_1, \dots, t_n] \longrightarrow F[P_1, \dots, P_n]$ omomorfismo tale che $\hookrightarrow(a) = a$ per ogni $a \in F$ e $\hookrightarrow(t_i) = P_i$

[Posso farlo perché $F[t_1, \dots, t_n]$ anello di polinomi a n variabili]

Osserviamo che:

- $\hookrightarrow$ è suriettivo per definizione
- $\hookrightarrow$ è iniettivo [costruiamo inverse sinistra]

Sia $\chi: F[x_1, \dots, x_n] \longrightarrow F[y_1, \dots, y_n]$

tale che $\chi(a) = a \quad \forall a \in F$ e $\chi(x_i) = y_i$

[y_i radici di $q(x)$
 $F[x_1, \dots, x_n]$ anello di polinomi a n variabili]

Considero il seguente diagramma:

$$\begin{array}{ccc} F[x_1, \dots, x_n] & \xrightarrow{\chi} & F[y_1, \dots, y_n] \\ \cup & & \cup \\ F[p_1, \dots, p_n] & \longleftarrow & F[t_1, \dots, t_n] \end{array}$$

$$\chi \circ \iota(t_i) = \chi(p_i) = \chi\left(\sum_{j_1 < \dots < j_i} x_{j_1} \dots x_{j_i}\right)$$

$$= \sum_{j_1 < \dots < j_i} y_{j_1} \dots y_{j_i} = t_i$$

da cui $\chi \circ \iota = \text{Id}_{F[t_1, \dots, t_n]} \Rightarrow \chi$ suriettivo

conclusione: $\hookrightarrow$ isomorfismo

Estendo $\hookrightarrow$ due volte

• [prima estensione] $\hookrightarrow \exists \varphi: F(t_1, \dots, t_n) \rightarrow F(p_1, \dots, p_n)$
isomorfismo

• [seconda estensione] $\hookrightarrow \exists \psi: F(t_1, \dots, t_n)[x] \rightarrow F(p_1, \dots, p_n)[x]$
isomorfismo

Osserviamo che:

$$x^n - p_1 x^{n-1} + p_2 x^{n-2} - \dots + (-1)^n p_n$$

• $\hookrightarrow$ manda $q(x)$ in $h(x)$
 $\parallel$

$$x^n - t_1 x^{n-1} + \dots + (-1)^n t_n = 0$$

• $F(y_1, \dots, y_m)$ campo di spezzamento di $q(x)$ su $F(t_1, \dots, t_m)$

$F(x_1, \dots, x_m)$ campo di spezzamento di $h(x)$ su $F(p_1, \dots, p_m)$

$\implies$

esiste un isomorfismo da $F(y_1, \dots, y_m)$

a $F(x_1, \dots, x_m)$ che estende $\hookrightarrow$

$\implies$

$$\text{gal} \left(\frac{F(y_1, \dots, y_m)}{F(t_1, \dots, t_m)} \right) \cong \text{gal} \left(\frac{F(x_1, \dots, x_m)}{F(p_1, \dots, p_m)} \right) \cong S_m$$

i.e. $G_q \cong G_h \cong S_m$

$\implies$

$q(x)$ non ha radici multiple

e $q(x)$ irriducibile su $F(t_1, \dots, t_m)$

(G_q agisce transitivamente sulle radici)

Teorema l'equazione generale di grado n $q(x)=0$
 è irriducibile in $F(t_1, \dots, t_n)[x]$, le radici
 distinte e $G_q \cong S_n$

Teorema di Abel-Ruffini se $\text{char } F = 0$

l'equazione generale di grado n non
 è risolubile per $n \geq 5$

Dim. $G_q \cong S_n$ non risolubile per $n \geq 5$

Usando criterio di risolubilità per radicali
 ottengo $q(x)=0$ non risolubile 

Oss: se $\text{char } F = 0$ il criterio di risolubilità
 di Galois ci assicura la risolubilità per
 $n=3, 4$ ($n=1$ banale, $n=2$ già visto)

[Vediamo ora le formule per il caso 3]

LA CUBICA GENERALE

Supponiamo $\text{char } F \neq 2$ e $\text{char } F \neq 3$

[ci mettiamo in un caso più generale rispetto a $\text{char } F = 0$]

$$q(x) = x^3 - t_1 x^2 + t_2 x - t_3 = (x - y_1)(x - y_2)(x - y_3)$$

y_i radici di $q(x)$ nel campo di spezzamento
di $q(x)$ su $F(t_1, t_2, t_3)$

Abbiamo visto che è utile avere in F
tre distinte radici cubiche dell'unità

Una radice cubica dell'unità diversa da 1

è una radice di $x^2 + x + 1$ ($x^3 - 1 = (x - 1)(x^2 + x + 1)$)

Usando la formula per le eq. di secondo grado
otteniamo che le due radici sono

$$w = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$$

[qua serve $\text{char } F \neq 2$]

$$w^{-1} = -\frac{1}{2} - \frac{1}{2}\sqrt{-3}$$

Supponiamo $w \in F$

Rimpiazziamo $x_i = y_i - \frac{1}{3}(y_1 + y_2 + y_3) = y_i - \frac{1}{3}t_1$

Otteniamo:

y_1 soluzione di $x^3 - t_1 x^2 + t_2 x - t_3$

$\Leftrightarrow$

x_1 soluzione di $(x + \frac{1}{3} t_1)^3 - t_1 (x + \frac{1}{3} t_1)^2 + t_2 (x + \frac{1}{3} t_1) - t_3$

$$(x + \frac{1}{3} t_1)^3 - t_1 (x + \frac{1}{3} t_1)^2 + t_2 (x + \frac{1}{3} t_1) - t_3 =$$

$$= x^3 + \frac{1}{27} t_1^3 + x^2 t_1 + \frac{1}{3} x t_1^2 - t_1 (x^2 + \frac{2}{3} t_1 x + t_1^2) +$$

$$+ t_2 x + \frac{1}{3} t_1 t_2 - t_3$$

$$= x^3 + \frac{1}{27} t_1^3 + \boxed{x^2 t_1} + \boxed{\frac{1}{3} x t_1^2} - \boxed{t_1 x^2} - \boxed{\frac{2}{3} t_1^2 x} - t_1^3$$

$$+ t_2 x + \frac{1}{3} t_1 t_2 - t_3$$

grad 2
grad 3

$$= x^3 + \left(\frac{1}{3} t_1^2 + t_2 \right) x + \left(-\frac{26}{27} t_1^3 + \frac{1}{3} t_1 t_2 - t_3 \right)$$

$$= x^3 + p x + q \quad [\text{è sparito il grado 2}]$$

Cerchiamo x_1, x_2, x_3 radici di $x^3 + p x + q$

$$\text{con } x_1 + x_2 + x_3 = 0$$

$\neq (t_1, t_2, t_3) (y_1, y_2, y_3)$ è campo di spezzamento

sia di $q(x)$ che di $f(x) \stackrel{\text{def}}{=} x^3 + p x + q$

su $F(t_1, t_2, t_3)$

Ricordo che

139

- $G_f \cong S_3$ i.e. $\text{Gal}\left(\frac{F(t_1, t_2, t_3)(x_1, x_2, x_3)}{F(t_1, t_2, t_3)}\right) \cong S_3$

quindi anche il gruppo di Galois di $f(x)$ su $F(t_1, t_2, t_3)$ è isomorfo a S_3

Considero $F(p, q)$:

- Il gruppo di Galois di $f(x)$ su $F(p, q)$ (che chiameremo G_f) è un sottogruppo di S_3 ($f(x)$ ha tre radici)

- Il gruppo di Galois di $f(x)$ su $F(t_1, t_2, t_3)$ è isomorfo ad un sottogruppo di G_f per Lemma 4 preparentorio alla dimostrazione del Criterio di Galois

- $G_f \leq S_3$ ha un sottogruppo isomorfo a S_3

$\implies$

$$G_f \cong S_3$$

Chiamiamo $K \stackrel{\text{def}}{=} F(p, q)$ e $E = K(x_1, x_2, x_3)$

il campo di spezzamento di $f(x)$ su K

Consideriamo la serie subnormale

$$\{1\} \triangleleft A_3 \triangleleft S_3$$

- Il sottocampo di E/K corrispondente a A_3 è $K(D)$ con $D^2 = d$ (discriminante di f)
e $d = -4p^3 - 27q^2$

$$\left[\begin{array}{l} \text{in generale } d = -4a_1^3 a_3 + a_1^2 a_2^2 + 18a_1 a_2 a_3 - 4a_1^3 - 27a_3^2 \\ \text{nel nostro caso } a_1 = 0 \quad a_2 = p \quad a_3 = q \end{array} \right]$$

per il teorema fondamentale delle teorie di Galois:

- $3 = |A_3| = [E : \bigcup_{\text{inv}} A_3] = [E : K(D)]$
- $\text{Gal}(E/K(D)) = \text{Gal}(E/\bigcup_{\text{inv}} A_3) \cong A_3 \cong \mathbb{Z}_3$

Ricordo Lemma 3: Siano p primo, F contenente p radici p -esime distinte dell'unità, E estensione ciclica di F con $[E:F] = p$, allora $E = F(b)$ con $b^p \in F$

della dimostrazione si ottiene:

Se $c \in E \setminus F$ posso scegliere come b una delle risolvanti di Lagrange

$$(w_i, c) = c + \eta(c) w_i + \eta^2(c) w_i^2 + \dots + \eta^{p-1}(c) w_i^{p-1}$$

dove w_i radice p -esima dell'unità e

η generatore di $\text{Gal}(E/F)$

come treccia uso Lemma 3 e dim. per il nostro caso (abbiamo supposto F contiene 3 radici cubiche distinte)

Considero le tre risolventi in questo caso

- η generatore di $\text{Gal}(E/K(D))$ con

$$\eta(\alpha_1) = \alpha_2 \quad \eta(\alpha_2) = \alpha_3 \quad \eta(\alpha_3) = \alpha_1$$

- ω radice primitiva dell'unità

$$\begin{aligned} z_1 &\stackrel{\text{def}}{=} (\omega, \alpha_1) = \alpha_1 + \omega \alpha_2 + \omega^2 \alpha_3 \\ z_2 &\stackrel{\text{def}}{=} (\omega^2, \alpha_1) = \alpha_1 + \omega^2 \alpha_2 + \omega \alpha_3 \\ z_3 &\stackrel{\text{def}}{=} (1, \alpha_1) = \alpha_1 + \alpha_2 + \alpha_3 = 0 \end{aligned} \quad \left\{ \begin{array}{l} \text{le tre} \\ \text{risolventi} \end{array} \right.$$

Ora cerco di esprimere z_1^3 e z_2^3 in termini di $p, q, D = \sqrt{d}$

$$\begin{aligned} z_1^3 &= \alpha_1^3 + \alpha_2^3 + \alpha_3^3 + 3\omega(\alpha_1^2 \alpha_2 + \alpha_1^2 \alpha_3 + \alpha_1 \alpha_3^2) \\ &\quad + 3\omega^2(\alpha_1 \alpha_2^2 + \alpha_1^2 \alpha_3 + \alpha_2 \alpha_3^2) + 6\alpha_1 \alpha_2 \alpha_3 \end{aligned}$$

per z_2^3 si scambia il ruolo di ω e ω^2

$$\begin{aligned} D = \sqrt{d} &= (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_1 - \alpha_3) \\ &= (\alpha_1^2 \alpha_2 + \alpha_1 \alpha_3^2 + \alpha_2^2 \alpha_3) - (\alpha_1 \alpha_2^2 + \alpha_2 \alpha_3^2 + \alpha_3 \alpha_1^2) \end{aligned}$$

- poniamo $\mu = x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1 + x_1 x_2^2 + x_2 x_3^2 + x_3 x_1^2$
- sappiamo che $w + w^2 = -1$ $w - w^2 = \sqrt{-3}$

Da cui

$$\begin{aligned} z_1^3 &= \sum x_i^3 + 3w \left(\frac{\mu + \sqrt{d}}{2} \right) + 3w^2 \left(\frac{\mu - \sqrt{d}}{2} \right) + 6x_1 x_2 x_3 \\ &= \sum x_i^3 + \frac{3\mu}{2} + \frac{3}{2} \sqrt{-3} \sqrt{d} + 6x_1 x_2 x_3 \end{aligned}$$

Inoltre

$$\bullet \text{ da } x^3 - px + q = (x - x_1)(x - x_2)(x - x_3)$$

$$\text{ottengo } q = -x_1 x_2 x_3$$

$$\begin{aligned} \bullet \quad 0 &= (x_1 + x_2 + x_3) \cdot (x_1 x_2 + x_2 x_3 + x_1 x_3) = \\ &= \mu + 3x_1 x_2 x_3 \Rightarrow \mu = 3q \end{aligned}$$

$$\bullet \quad 0 = (x_1 + x_2 + x_3)^2 = \sum_{i=1}^3 x_i^3 + 3\mu + 6x_1 x_2 x_3$$

$$\Rightarrow \sum_{i=1}^3 x_i^3 = -3q$$

da cui ottengo:

$$z_1^3 = -3q - \frac{9}{2}q + \frac{3}{2}\sqrt{-3}\sqrt{d} - 6q$$

$$= -\frac{27}{2}q + \frac{3}{2}\sqrt{-3d} \rightarrow \text{Fisso una radice quadrata di } \sqrt{-3d}$$

analogamente

$$z_2^3 = -\frac{27}{2}q - \frac{3}{2}\sqrt{-3d}$$

$$\text{Quindi: } z_1 = \sqrt[3]{-\frac{27}{2}q + \frac{3}{2}\sqrt{-3d}} \quad z_2 = \sqrt[3]{-\frac{27}{2}q - \frac{3}{2}\sqrt{-3d}} \quad (*)$$

$$\text{con } d = -4p^3 - 27q^2$$

Concludo:

$$z_1 + z_2 = x_1 + \omega x_2 + \omega^2 x_3 + x_1 + \omega^2 x_2 + \omega x_3$$

$$= 2x_1 - x_2 - x_3 = 3x_1$$

$$\nearrow x_1 + x_2 + x_3 = 0$$

$$\Rightarrow \boxed{x_1 = \frac{z_1 + z_2}{3}} \quad [\text{char } F \neq 3]$$

$$\omega^2 z_1 + \omega z_2 = \omega^2 x_1 + x_2 + \omega x_3 + \omega x_1 + x_2 + \omega^2 x_3$$

$$= 2x_2 - x_1 - x_3 = 3x_2$$

$$\Rightarrow \boxed{x_2 = \frac{\omega^2 z_1 + \omega z_2}{3}}$$

$$\omega^2 z_2 + \omega z_1 = \omega^2 x_1 + \omega x_2 + x_3 + \omega x_1 + \omega^2 x_2 + x_3$$

$$= 2x_3 - x_2 - x_1 = 3x_3$$

$$\Rightarrow \boxed{x_3 = \frac{\omega^2 z_2 + \omega z_1}{3}}$$

Utilizzando (*) ottengo le formule risolventi
per $x^3 + px + q$ e poi per $q(x)$

