CRITERIO DI GALOIS PER LA RISOLUBILITÀ PER RADICALI

Sia F campo con $\operatorname{char} F = 0$ e $q(x) \in F[x]$ allora $q(x)$ è risolubile per radicali se e solo se G_q è risolubile

Dim. "$\Rightarrow$" Sia E campo di spezzamento di $q(x)$ allora per ipotesi esiste un campo $K \supseteq E$ con una torre di radicali di K su F

- $\operatorname{char} F = 0 \Rightarrow$ ogni polinomio è separabile quindi posso considerare la chiusura normale di K su F
  - la chiusura normale è un'estensione di Galois su F
  - per il Lemma 5 ha una torre di radici su F (con gli stessi esponenti della torre di K su F)

Concludendo: possiamo supporre che K sia un estensione di Galois (se così non fosse sostituiamo K con la sua chiusura normale)

- Sia $n = \text{m.c.m.}\{n_i\}$ dove gli n_i sono gli esponenti che compaiono nella torre di radici

- Sia z una radice n-esima dell'unità che genera tutte le altre radici ; in questo caso si dice che z è una radice primitiva.

[l'esistenza di una radice primitiva è dimostrata all'interno della dimostrazione del Lemma 1]

- consideriamo $K(z)$.
  Se K è il campo di spezzamento di $f(x)$ allora $K(z)$ è il campo di spezzamento di $f(x)(x^n-1)$
  $\Rightarrow K(z)$ è di Galois su F

- Se $K = F_r(d_r) \supseteq \dots \supseteq F_2 = F_1(d_1) \supseteq F_1 = F$ torre di radici su F allora posso costruire

$$K(z) = \overline{F}_{r+2} = \overline{F}_{r+1}(d_r) \supseteq \dots \supseteq \overline{F}_2(d_1) = \overline{F}_3 \supseteq \overline{F}_2 = F(z) \supseteq F = \overline{F}_1$$

torre di radici su F

[si osservi che $\overline{F}_i \supseteq F_{i-1}$]

- Per il Lemma 1 otteniamo che
  $\underbrace{F(z)}_{=\overline{F}_2}$ è abeliano su $\underbrace{F}_{=\overline{F}_1}$ (in particolare è est. di Galois)

[$F(z)$ è il campo ciclotomico di ordine n]

- Siccome $F(z) \subseteq \overline{F}_i$ per $i \geq 2$ allora
  $\overline{F}_i$ contiene tutte le radici n-esime dell'unità (che sono distinte)

- $\overline{F}_{i+1} = \overline{F}_i(d_{i-1})$ con $(d_{i-1})^{m_{i-1}} \in \overline{F}_{i-1} \subseteq \overline{F}_i$

  quindi d_{i-1} radice di
  $$x^{m_{i-1}} - (d_{i-1})^{m_{i-1}} \in \overline{F}_i[x]$$

- $m_{i-1} \mid n = m.c.m\{m_k\} \Rightarrow$

  $\Rightarrow \overline{F}_{i+1}$ contiene tutte le m_{i-1} radici m_{i-1}-esime dell'unità

  $\Rightarrow \overline{F}_{i+1}$ contiene d_{i-1} radici distinte di $x^{m_{i-1}} - (d_{i-1})^{m_{i-1}}$

per dimostrazione del Lemma 2 le radici di $x^{m_{i-1}} - (d_{i-1})^{m_{i-1}}$ si ottengono moltiplicando d_{i-1} con le m_{i-1} radici m_{i-1}-esime dell'unità

$\Rightarrow \overline{F}_{i+1}$ è il campo di spezzamento di $x^{n_{i-1}} - (\alpha_{i-1})^{n_{i-1}}$ su F_i

$\Rightarrow \overline{F}_{i+1}$ è un'estensione ciclica di $\overline{F}_i$ (ed in particolare e est di Galois)

Lemma 2

<u>Conclusione</u>: $\overline{F}_{i+1}$ estensione abeliana su $\overline{F}_i$ per ogni $i = 1, \dots, r+1$ $\left(Gal\left(\frac{\overline{F}_{i+1}}{\overline{F}_i}\right) \text{ è abeliano} \right)$

Definiamo $H_i = Gal\left(\frac{K(z)}{\overline{F}_i}\right)$

Per il teor. fond. della teoria di Galois

- $\overline{F}_{i+1} \supseteq \overline{F}_i \Rightarrow H_{i+1} \leq H_i$
- $\overline{F}_i = \mathrm{Inv}\left(Gal\left(\frac{K(z)}{\overline{F}_i}\right)\right) = \mathrm{Inv}(H_i)$

[Ricordo che per teor. fond. teoria di G.
Se L è un estensione di Galois di C
$H \lhd Gal(L/C) \Leftrightarrow \mathrm{Inv}(H)$ è normale su C
e se $H \lhd Gal(L/C)$ allora $Gal\left(\frac{\mathrm{Inv}\, H}{C}\right) \cong \frac{Gal(L/C)}{H}$]

Nel nostro caso

$H_{i+1} \lhd H_i = Gal\left(\frac{K(z)}{\overline{F}_i}\right) \Leftrightarrow \mathrm{Inv}\, H_{i+1} = \overline{F}_{i+1}$ è normale su $\overline{F}_i$

Noi sappiamo che $\overline{F}_{i+1}$ è di Galois (quindi normale) su $\overline{F}_i$ e quindi otteniamo $H_{i+1} \triangleleft H_i$

Inoltre

$$Gal\left(\frac{\overline{F}_{i+1}}{\overline{F}_i}\right) = Gal\left(\frac{Inv\, H_{i+1}}{F_i}\right) \cong \frac{Gal\left(\frac{K(z)}{F_i}\right)}{H_{i+1}} = \frac{H_i}{H_{i+1}}$$

Sappiamo che $Gal\left(\frac{\overline{F}_{i+1}}{\overline{F}_i}\right)$ è abeliano

e quindi H_i / H_{i+1} abeliano per $i = 1 \dots r+1$

Otteniamo una serie subnormale

$$\{1\} = H_{r+2} \triangleleft H_{r+1} \triangleleft \dots \triangleleft H_2 \triangleleft H_1 = Gal\left(\frac{K(z)}{F}\right)$$

tale che H_i / H_{i+1} è abeliano

$\Longrightarrow Gal\left(\frac{K(z)}{F}\right)$ è risolubile

- Considero infine $K(z) \supseteq E \supseteq F$

E è normale su F perchè è un campo di spezzamento di un polinomio

Considero quindi:

$$E = \mathrm{Inv}\left(\mathrm{Gal}\left(\frac{K(z)}{E}\right)\right)$$

e nuovamente per teor. fond. teoria di Galois

$$E \text{ è normale su } F \Rightarrow \mathrm{Gal}\left(\frac{K(z)}{E}\right) \triangleleft \mathrm{Gal}\left(\frac{K(z)}{F}\right)$$

e vale che:

$$\mathrm{Gal}\left(\frac{E}{F}\right) \cong \frac{\mathrm{Gal}\left(\frac{K(z)}{F}\right)}{\mathrm{Gal}\left(\frac{K(z)}{E}\right)}$$

Siccome $\mathrm{Gal}\left(\frac{K(z)}{F}\right)$ è risolubile anche $\mathrm{Gal}\left(E/F\right)$ è risolubile

" $\Leftarrow$ "

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

In questo caso l'ipotesi è che $\mathrm{Gal}(E/F)$ è risolubile

Sia $n = |\mathrm{Gal}(E/F)| = [E:F]$

(char $F \Rightarrow q$ separabile $\Rightarrow E$ est di Galois su F)

Definiamo $F_1 = F$, $F_2 = F(z)$ dove z è una radice n-esima primitiva dell'unità e $K = E(z)$

Possiamo porre $E = F(r_1, \dots, r_k)$

dove r_i sono le radici di $q(x)$

Quindi $K = F(r_1, \dots, r_k)(z) = F(z)(r_1, \dots, r_k)$

ottenendo K campo di spezzamento

di $q(x)$ su $F_2 = F(z)$

Lemma 4 $\Longrightarrow$ $\begin{cases} Gal\left(\frac{K}{F_2}\right) \text{ è isomorfo ad un} \\ \text{sottogruppo di } Gal\left(\frac{E}{F}\right) \end{cases}$

$\Longrightarrow Gal\left(K/F_2\right)$ è risolubile

$\Longrightarrow Gal\left(K/F_2\right)$ ha una serie di composizione

$H_2 = Gal\left(K/F_2\right) \triangleright H_3 \triangleright \dots \triangleright H_{r+1} = \{1\}$

con H_i / H_{i+1} ciclico $i = 2, \dots, r$

$\Longrightarrow$ esiste una catena di sottocampi

teor
fond
teoria di G

$$\begin{array}{ccccccc} F_2 & \subseteq & F_3 & \subseteq & \dots \subseteq F_r & \subseteq & F_{r+1} = K \\ \shortparallel & & \shortparallel & & \shortparallel & & \\ Inv\,H_2 & & Inv\,H_3 & & Inv\,H_r & & Inv(H_{r+1}) \end{array}$$

tali che $H_i = Gal\left(\frac{K}{F_i}\right)$

Sempre per teor. fond. teoria di Galois

$$H_{i+1} \lhd H_i \Rightarrow F_{i+1} \text{ estensione normale su } F_i$$

e $Gal\left(\frac{F_{i+1}}{F_i}\right) \cong \frac{H_i}{H_{i+1}}$ ciclico di ordine p_i primo

Osserviamo detto che $Gal\left(\frac{K}{F_2}\right)$ isomorfo a sottogruppo di $Gal\left(\frac{E}{F}\right)$ allora

$$\left|Gal\left(\frac{K}{F_2}\right)\right| \,\Big|\, \left|Gal\left(E/F\right)\right| = n \qquad e \ p_i \mid n$$

Siccome $F_i \supseteq F_2 = F(z)$ con z radice n-esima primitiva dell'unità allora F_i contiene tutte le radici p_i-esime dell'unità

Lemma 3 $\Rightarrow$ $F_{i+1} = F_i(d_i)$ con $d_i^{p_i} \in F_i$

Costruisco

$$F = F_1 \subseteq F_2 = F_1(z) \subseteq F_3 = F_2(d_2) \subseteq \ldots\ldots \subseteq F_{r+1} = K$$

(con $z^n = 1 \in F$)

torre di radici di K su F; inoltre $E \subseteq K$ per costruzione

$$\Longrightarrow$$

$q(x)$ è risolubile per radicali