

Approfondimento:

Studiamo ora i polinomi del tipo $x^n - 1$ e $x^n - a$, si ha:

- F_n è estensione di Galois di F e $\text{Gal}(F_n/F)$ è abeliano.

$\varphi \in \text{Gal}(F_n/F) \Rightarrow \varphi(z_n)$ è generatore di $G_n(F)$ che è ciclico con n elementi (i generatori del GRUPPO $\mathbb{Z}/n\mathbb{Z}$ sono gli elementi invertibili dell'ANELLO $\mathbb{Z}/n\mathbb{Z}$)

\Rightarrow si ottiene un omomorfismo iniettivo
 $\text{Gal}(F_n/F) \rightarrow U(\mathbb{Z}/n\mathbb{Z})$

Considereremo sempre, d'ora in poi, campi con caratteristica 0 (se non detto altrimenti).

Def. (Estensione per radicali):

Si dice che K è **ESTENSIONE PER RADICALI** di F se $\exists E_1, \dots, E_{m-1}$ campi intermedi di K t.c.

$$1) F = E_0 \subseteq E_1 \subseteq \dots \subseteq E_{m-1} \subseteq E_m := K$$

$$2) E_i = E_{i-1}(b_i) \text{ con } b_i^{m_i} \in E_{i-1} \quad \forall i = 1, \dots, m$$

Lemme:

K estensione per radicali di $F \Rightarrow \exists$ estensione di K che è estensione per radicali di F ed è Galois su F

Dim.:

Induzione su $[K:F]$:

Ovvio se $[K:F]=1$. Sia $[K:F]>1$. Allora wlog possiamo supporre $E_{m-1} \not\subseteq K \Rightarrow E = E_{m-1}$ soddisfa l'ipotesi induktiva ($[E:F] < [K:F]$)
 $\Rightarrow \exists E'$ estensione di E che è Galois su F ed estensione per radicali di F
 $\Rightarrow \exists b \in E$ t.c. $K = E(b)$ e $b^m \in E$
Sia $g(x) = \prod_{\gamma \in \text{Gal}(E'/F)} (x^m - \gamma(b^m)) \Rightarrow g(x)$ è invariante per $\gamma \in \text{Gal}(E'/F) \Rightarrow g(x) \in F[x]$
Se K' è CRC di $g(x)$ su E' , $b \in K' \Rightarrow K = E(b) \subseteq K'$
 \Rightarrow le radici di $g(x)$ sono tutte radicali
 $\Rightarrow K'$ è estensione per radicali di K e, quindi, anche di F . Per costruzione E' è Galois su F , quindi è CRC di $f(x) \in F[x]$
 $\Rightarrow K'$ è CRC di $f(x)g(x)$ su F

q.e.d.

Def. (Polinomio risolubile per radicali):

$f(x) \in F[x]$ è RisOLUBILE PER RADICALI se $\exists F \subseteq K$ estensione per radicali t.c. $f(x)$ si fattorizza completamente in $K[x]$. Se K è CRC di f su F , diremo $\text{Gal}(f/F) = \text{Gal}(K/F)$

N.B.

Ricordiamo che un gruppo G è risolubile se \exists

$$\{1\} = N_0 \trianglelefteq \dots \trianglelefteq N_{m-1} \trianglelefteq N_m = G$$

t.c. N_i/N_{i-1} è abeliano.

Si ha che, se G è risolubile, lo è anche ogni suo sottogruppo. Inoltre, dato $N \trianglelefteq G$, G è risolubile se e solo se lo sono N e G/N .

Lemma:

Sia K estensione di Galois di F . Vale la seguente:
Esiste una catena di campi intermedii $F = E_0 \subseteq \dots \subseteq E_{m-1} \subseteq E_m = K$ t.c. $\text{Gal}(E_i/E_{i-1})$ è Galois su E_{i-1} e $\text{Gal}(E_i/E_{i-1})$ è risolubile $\Leftrightarrow \text{Gal}(K/F)$ è risolubile

Dimo.:

dal Teorema Fondamentale della Teoria di Galois

q.e.d.

Teorema:

Sia K estensione di Galois di F ed E campo intermedio Galois su F . Allora $\text{Gal}(K/F)$ è risolubile se e solo se lo sono $\text{Gal}(E/F)$ e $\text{Gal}(K/E)$
 $(\text{Gal}(E/F) \cong \frac{\text{Gal}(K/F)}{\text{Gal}(K/E)})$

Dimo.:

dalla Teoria sui Gruppi risolubili.

q.e.d.

Teorema (di Galois):

Sia $f(x) \in F[x]$. Sono equivalenti le seguenti:

- 1) f risolubile per radicali
- 2) $\text{Gal}(f/F)$ è risolubile

Dim.:

1) \Rightarrow 2):

$\exists F \subseteq K$ t.c.:

1) f si scomponga completamente in K

2) K estensione per radicali di F

3) K Galois su F

$\Rightarrow F = E_0 \subseteq \dots \subseteq E_{m-1} \subseteq E_m = K$ con

$$E_i = E_{i-1}(b_i), b_i^{n_i} \in E_{i-1}$$

Sia K' CRC di $f \Rightarrow K' \subseteq K$. $\text{Gal}(K/F)$ è risolubile perché $\text{Gal}(K'/F)$ ne è un quoziente

2) \Rightarrow 1):

$\text{Gal}(f/F)$ risolubile. Supponiamo che F contenga le radici di 1. \Rightarrow Sia:

$$\{1\} = H_0 \trianglelefteq \dots \trianglelefteq H_{m-1} \trianglelefteq H_m = \text{Gal}(f/F) \text{ con}$$

H_i/H_{i-1} abeliano

\Rightarrow assumiamo WLOG H_i/H_{i-1} ciclico. Mostriamo che se K Galois su F , $\text{Gal}(K/F)$ è ciclico di ordine n e F contiene le radici n -esime di 1 allora K è estensione per radicali di F :

K è estensione primitiva di F : $K = F(\zeta)$.

Sia $z_n \in F$ radice primitiva di 1. Consideriamo

$$\alpha = \sum_{i=0}^{n-1} z_n^{-i} \zeta^i(b) \text{ dove } \text{Gal}(K/F) = \langle \zeta \rangle$$

$$\Rightarrow \zeta(\alpha) = \sum_{i=0}^{n-1} z_n^{-i} \zeta^{i+1}(b) = \sum_{i=0}^{n-1} z_n^{-i+1} \zeta^i(b) = z_n \alpha$$

$$\Rightarrow \zeta^n(\alpha) = z_n^n \alpha \quad (\text{induzione})$$

$$\Rightarrow \varphi^0(a) \varphi^1(a) \dots \varphi^{n-1}(a) = z_n^0 \dots z_n^{n-1} a^n = c$$

$$\Rightarrow \varphi(c) = c \Rightarrow \varphi^k(c) = c \Rightarrow c \in F$$

$\Rightarrow z_n^0 \dots z_n^{n-1} = \pm 1 \Rightarrow F(a)$ è estensione per radicali di F ed è Galois su F (contiene le radici di $x^n - a$). Quindi $\text{Gal}(K/F(a))$ è ciclico. Per induzione, si esaurisce K estendendo per radicali

q.e.d.

Teorema:

Tutti i polinomi con $\deg \leq 4$ sono risolubili per radicali

Lemme:

Se $f(x) \in F[x]$ ha $\deg = n$, allora $\text{Gal}(f/F)$ è isomorfa ad un sottogruppo di S_n

Dim. (Lemma):

$X = \{b_1, \dots, b_n\}$ insieme delle radici di $f(x)$ nel CRC K .

(distinte) $\Rightarrow |X| \leq n \Rightarrow f(x) = a_0 + \dots + a_n x^n$, sia

$$\begin{aligned} & \varphi \in \text{Gal}(f/F), b \in X \Rightarrow f(\varphi(b)) = a_0 + \dots + a_n \varphi(b)^n \\ &= \varphi(a_0) + \dots + \varphi(a_n b^n) \end{aligned}$$

$\Rightarrow \varphi(b)$ definisce $\hat{\varphi}: X \rightarrow X$ iniettiva, quindi suriettiva

$\Rightarrow \hat{\varphi} \in S_X$ ed è omomorfismo da $\text{Gal}(f/F)$ in S_X

$\Rightarrow \text{Gal}(f/F)$ è isomorfa ad un sottogruppo di S_X

$\Rightarrow S_4 \cong S_m \wedge S_m$ è isomorfo ad un sottogruppo
di S_n

q.e.d.

Dim. (Teorema):

S_4 è risolubile:

$\{()\} \trianglelefteq V = \{(), (12)(34), (13)(24), (14), (23)\} \trianglelefteq A_4 \trianglelefteq S_4$
con V abeliano, $|A_4/V| = 3 \Rightarrow A_4/V$ abeliano,
 $|S_4/A_4| = 2 \Rightarrow S_4/A_4$ è abeliano.

q.e.d.

N.B.

$x^m - 1, x^m - a$ sono risolubili per radicali $\forall n, \forall a$
Esempio:

$f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$ è irriducibile per Eisenstein
Consideriamo $f(x) = x^5 - 4x + 2$ su \mathbb{R} :

$\Rightarrow f'(x) = 5x^4 - 4$, max in $-\sqrt[4]{\frac{4}{5}}$, minimo in $\sqrt[4]{\frac{4}{5}}$
 $\Rightarrow f(-\sqrt[4]{\frac{4}{5}}) > 0, f(\sqrt[4]{\frac{4}{5}}) < 0 \Rightarrow f$ ha 3 radici reali
e 2 immaginarie pure b, \bar{b}

$\Rightarrow [\mathbb{Q}(b) : \mathbb{Q}] = 5$, K CRC di f su \mathbb{Q} :

$\text{Gal}(K/F) = \text{Gal}(f/F)$ ha ordine $[K : \mathbb{Q}]$

$\Rightarrow 5 | [K : \mathbb{Q}] = |\text{Gal}(K/F)|$

\Rightarrow per Cauchy, $\text{Gal}(f/F)$ ha un elemento di
ordine 5

Il coniugio in \mathbb{C} ($\in K \subseteq \mathbb{C}$) induce un automorfismo

di K (che fissa \mathbb{Q}), quindi un elemento di $\text{Gal}(\mathbb{F}/\mathbb{F})$ ha ordine 2. Perciò $\text{Gal}(\mathbb{F}/\mathbb{F})$ è isomorfa ad un sottogruppo H di S_5 t.c. H contiene un ciclo di lunghezza 5 e una trasposizione.

Supponiamo wlog che $(12345) \in H$, $(1i) \in H$ con $i \in \{1, \dots, 5\}$, allora $H = S_5$

Tuttavia S_n non è risolubile per $n > 5$!!!

Infatti A_n è un gruppo semplice per $n > 5$ (non ha sottogruppi non triviali non banali) e non è abeliano:

$$(123)(234) = (12)(34), \quad (234)(123) = (13)(24)$$

N.B.

A_5 è semplice (dall'equazione delle classi):
nessuna unione di classi del coniugio $(1, 12, 12, 20, 15)$
ha come ordine un divisore di 60
