Risolubilità per radicali.

Es: equazioni quadratiche $ax^2+bx+c=0$ $\quad a,b,c\in\mathbb{Q}$

$$x=\frac{-b\pm\sqrt{b^2-4ac}}{a} \qquad x\in\mathbb{Q}(\sqrt{\Delta})$$

(esistono formule risolutive per equazioni di 3° grado (formule di Cardano) e di 4° grado (Cartesio)).

Ad esempio l'equazione di 3° grado $x^3+ax+b=0$ ha come soluzioni

$$\alpha_1=\sqrt[3]{-\frac{b}{2}+\sqrt{\frac{b^2}{4}+\frac{a^3}{27}}}+\sqrt[3]{-\frac{b}{2}-\sqrt{\frac{b^2}{4}+\frac{a^3}{27}}}$$

$$\alpha_2=\omega(\qquad\qquad)+\omega^2(\qquad\qquad)$$

$$\alpha_3=(\;\ldots\;)+\omega(\;\ldots\;)$$

Nella formula risolutiva compaiono funzioni razionali di radicali di funzioni razionali di radicali ecc. ecc.

Diamo una formulazione precisa alla nostra idea di "equazione risolubile per radicali"

Def.

Sia $K\subseteq\overline{\mathbb{Q}}$, e $f(x)\in K[x]$.

L'equazione $f(x)=0$ si dice **risolubile per radicali** su K se esiste una successione di campi

$$K_0=K\subseteq K_1\subseteq\ldots\ldots\subseteq K_m$$

tale che K_m contiene tutte le radici di $f(x)$ e per $i = 0, \dots, m-1$, $K_{i+1} = K_i(\alpha_i)$ con $\alpha_i^{m_i} \in K_i$ $(m_i \in \mathbb{N})$

Quindi K_{i+1} è un'estensione radicale di K_i.

Dimostrazione del teorema di Abel-Ruffini

<u>Proposizione</u>

1) G risolubile $\Rightarrow$ ogni sottogruppo di G è risolubile

2) Dato un gruppo G e $H \triangleleft G$ allora

G risolubile $\Leftrightarrow$ H, G/H risolubile

3) G risolubile $\Leftrightarrow$ esiste una successione

$G = G'_0 \triangleright G'_1 \dots \triangleright G'_k = \{1\}$

t.c. $G'_{i+1} \triangleleft G'_i$ per $i = 0, \dots, k-1$ e G'_i / G'_{i+1} è ciclico per ogni i.

Dim.

1) A una catena $G_0 \triangleright G_1 \triangleright G_2 \dots \triangleright G_m$ corrisponde una catena $H_0 \triangleright H_1 \triangleright H_2 \dots \triangleright H_m$ con

$H_i = G_i \cap H$ per ogni i, quindi $H_0 = H$, $H_m = \{1\}$;

si ha $H_i \triangleleft H_{i+1}$ e $H_i / H_{i+1} \hookrightarrow G_i / G_{i+1}$ è abeliano

(infatti $H_i \cap G_{i+1} = H \cap G_{i+1} = H_{i+1}$).

2) Se G risolubile e $H \triangleleft G$ allora H risolubile (visto al punto 1) e alla catena

$G_0 = G \triangleright G_1 \triangleright G_2 \dots \triangleright G_n$

Facciamo corrispondere la catena

$\Gamma_0 \triangleright \Gamma_1 \triangleright \dots \triangleright \Gamma_n$

con $\Gamma_i = \dfrac{G_i H}{H}$ si ha $\dfrac{G_{i+1}H}{H} \triangleleft \dfrac{G_i H}{H}$

KH = minimo sottogruppo di G contenente G_i e H

$= \{k_1 h_1 k_2 h_2 \dots k_2 h_2\}$ in generale

$= \{kh \mid k \in K, h \in H$ se H è normale$\}$

Se $K \trianglelefteq G$ allora $\frac{KH}{H}$ normale in $\frac{G}{H}$

$$g k h g^{-1} = \underbrace{g k g^{-1}}_{\in K} \underbrace{g h g^{-1}}_{\in H}$$ quindi $\Gamma_{i+1} \trianglelefteq \Gamma_i$

Inoltre $\frac{\Gamma_i}{\Gamma_{i+1}} \simeq \frac{G_i H}{G_{i+1} H}$ e la mappa $\frac{G_i}{G_{i+1}} \longrightarrow \frac{G_i H}{G_{i+1} H}$

è un omom. suriettivo quindi $\frac{\Gamma_i}{\Gamma_{i+1}}$ è abeliano.

Viceversa, se H e $\frac{G}{H}$ sono risolubili, siano

$$\frac{G}{H} = \Gamma_0 \supseteq \Gamma_1 \supseteq \dots \supseteq \Gamma_k = \{1\}$$
$$H = H_0 \supseteq H_1 \supseteq \dots \supseteq H_k = \{1\}$$

catene che danno la risolubilità.

Per $i = 1 \dots k$ sia G_i la controimmagine di Γ_i attraverso la proiezione $G \longrightarrow \frac{G}{H}$ e consideriamo

$$G_0 = G \supseteq G_1 \dots \supseteq G_k = H = H_0 \supseteq H_1 \dots \supseteq H_2 = \{1\}$$

È facile verificare che $G_{i+1} \triangleleft G_i$ e $\frac{G_i}{G_{i+1}} \simeq \frac{\Gamma_i}{\Gamma_{i+1}}$ da cui la risolubilità di G.

iii) Sia $G_i \triangleright G_{i+1}$ con $\frac{G_i}{G_{i+1}}$ abeliano

Sia H sottogruppo normale massimale proprio di G_i contenente G_{i+1}, quindi

$$G_i \triangleright H \triangleright G_{i+1}$$

Si ha $\frac{G}{G_{i+1}} \longrightarrow \frac{G}{H} \Rightarrow \frac{G}{H}$ abeliano finito e non contiene sottogruppi propri $\Rightarrow G/H$ è ciclico di ordine un numero primo.

Iterando l'argomento possiamo raffinare ogni passo della catena $G_i \triangleright G_{i+1}$ a una successione in cui ogni quoziente successivo è ciclico di ordine primo. ☒

Lemma

Sia E/K Galois e sia ξ r.p. n-esima di 1.
Allora $\mathrm{Gal}(E/K)$ risolubile $\Leftrightarrow$ $\mathrm{Gal}(E(\xi)/K(\xi))$ risolubile.

Dim.

Sappiamo $\mathrm{Gal}(E(\xi)/K(\xi))$ è isom. a un sottogruppo di $\mathrm{Gal}(E/K)$. Questo prova $\boxed{\Rightarrow}$

Viceversa, supponiamo $\mathrm{Gal}(E(\xi)/K(\xi))$ risolubile.

si ha

$$\mathrm{Gal}(K(\xi)/K) \simeq \mathrm{Gal}(E(\xi)/K) \big/ \mathrm{Gal}(E(\xi)/K(\xi))$$

$$\begin{tikzcd}[column sep=small]
 & E(\xi) \arrow[dl, dash, "ab"'] \arrow[dr, dash] & \\
E \arrow[dr, dash] & & K(\xi) \arrow[dl, dash, "ab"] \\
 & K &
\end{tikzcd}$$

$$\mathrm{Gal}(E/K) \simeq \mathrm{Gal}(E(\xi)/K) \big/ \mathrm{Gal}(E(\xi)/E)$$

I gruppi $\mathrm{Gal}(E(\xi)/E)$ e $\mathrm{Gal}(K(\xi)/K)$ abeliani e quindi risolubili.

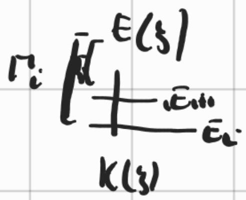
Segue che $Gal\left(E(\xi)/K\right)$ è risolubile e essendo $Gal\left(E(\xi)/E\right)$ risolubile abbiamo $Gal\left(E/K\right)$ risolubile.
(Applicazione iterata del punto (iii) della prop preced.)

Dimostrazione del teorema di Abel-Ruffini

Sia E il campo di spezzamento di $f(x)$ su K
Supponiamo $Gal\left(E/K\right)$ risolubile e sia $m = \left|Gal\left(E/K\right)\right|$
Sia ξ radice primitiva dell'unità.
Per il lemma precedente $\Gamma = Gal\left(E(\xi)/K(\xi)\right)$ è risolubile ed è un sottogruppo di $Gal\left(E/K\right)$.
Sia $\Gamma = \Gamma_0 \supseteq \Gamma_1 \dots \supseteq \Gamma_n = \{1\}$ catena che dà la risolubilità di Γ e t.c. Γ_i/Γ_{i+1} ciclico di ordine m_i. Ovviamente $m_i | m$
Corrispondentem. si ha una successione di campi intermedi

$$E(\xi) = E_n \supseteq E_{n-1} \dots \supseteq E_0 = K(\xi) \qquad E_i = E^{\Gamma_i}$$

si ha E_{i+1}/E_i Galois e $Gal\left(\frac{E_{i+1}}{E_i}\right) = \Gamma_i/\Gamma_{i+1}$



Perché $m_i | m$ e E_i contiene tutte le radici m-esime di 1
Si ha $E_{i+1} = E_i(\alpha_i)$ con $\alpha_i^{m_i} \in E_i$ e la successione di campi $K \subseteq K(\xi) \subseteq E_0 \subseteq E_1 \dots \subseteq E_n = E(\xi)$

dà la risolubilità per radicali dell'equazione $f(x)=0$.

Viceversa supponiamo che l'equazione $f(x)=0$ sia risolubile per radicali: esiste una successione di campi

$K_0 = K \subseteq K_1 \subseteq \dots \subseteq K_s$ con $K_{i+1} = K_i(\alpha_i)$, $\alpha_i^{m_i} \in K_i$

e K_s contiene le radici di $f(x)$.

Sia $m = \text{mcm}(m_i)$ e ξ una radice primitiva m-esima dell'unità. Poniamo $K_i' = K_i(\xi)$ e una catena di estensioni $K \subseteq K_0' \subseteq K_1' \dots \subseteq K_s'$ e ancora $K_{i+1}' = K_i'(\alpha_i)$ con $\alpha_i^{m_i} \in K_i'$, e le radici di $f(x)$ stanno in K_s'.

Sia E il campo di spezzamento di E su K. $\Rightarrow E \subseteq K_s'$

Per il lemma precedente

$$Gal\left(E/K\right) \text{ risolubile} \Leftrightarrow Gal\left(E(\xi)/K(\xi)\right) \text{ risolubile.}$$

Abbiamo $K(\xi) \subseteq E(\xi) \subseteq K_s'$

se fosse $K_s'/K(\xi)$ Galois basta provare $Gal\left(K_s'/K(\xi)\right)$ risolubile per ottenere $Gal\left(E(\xi)/K(\xi)\right)$ risolubile.

Supponiamo $K_s'/K(\xi)$ Galois. Segue K_s'/K_i Galois per ogni i e anche K_{i+1}'/K_i' Galois (sono est. radicali e K_i' contiene le radici m_i-esime dell'unità). Posto $\Gamma_i = Gal\left(K_s'/K_i\right)$ si ha $\Gamma_{i+1} \triangleleft \Gamma_i$ e $\Gamma_i/\Gamma_{i+1} = Gal\left(K_{i+1}'/K_i'\right)$ ciclico.

$\Rightarrow Gal\left(K_s'/K(\xi)\right)$ risolubile.

Se $K_s'/K(\xi)$ sia $\{\sigma_1, \dots, \sigma_t\} = \mathcal{G}\left(K_s'/K(\xi)\right)$

e allunghiamo la catena

$$K'_s \subseteq K'_s(\sigma_1(\alpha_0)) \subseteq K'_s(\sigma_1(\alpha_0), \sigma_1(\alpha_1), \dots) \subseteq \dots$$
$$K'_s(\sigma_1(\alpha_0), \dots, \sigma_1(\alpha_{s-1}), \sigma_2(\alpha_0) \dots)$$

Precisamente poniamo

$$K'_{hs+i+1} = K'_{hs+i}(\sigma_h(\alpha_0)) \quad \text{per } i < s.$$

Se $\tilde{K}$ è l'ultimo campo della catena, $\tilde{K} = K'_{ts+t}$.

$\tilde{K}$ si ottiene estraendo successivi radicali di indice uno degli m_i.

Inoltre $\tilde{K} = \sigma_1(K'_s) \dots \sigma_t(K'_s)$

perché $K'_s = K'(\alpha_0, \dots \alpha_{s-1})$, quindi $\tilde{K}$ è la chiusura di Galois di K'_s su K'. $\boxtimes$