Corso:Algebra IV I1/Risoluzione di radicali/Equazione risolubile per radicali

1 Criterio di risolubilità

Definizione 3.6

Sia K un campo e $f(x)$ un polinomio non costante in $K[x]$. Allora si dice che l'equazione $f(x) = 0$ è *risolubile per radicali* se, detto M un campo di spezzamento per $f(x)$ su K , allora M è contenuto in un'estensione radicale di K , cioè esiste un campo E con $E \supseteq M \supseteq K$ e tale che l'estensione $E \supseteq K$ è radicale.

Definizione 3.7

Nelle ipotesi precedenti, si definisce *gruppo di Galois del polinomio* $f(x)$ il gruppo di Galois di M su K .

Si parla di gruppo di Galois di un polinomio come gruppo di permutazioni delle radici di $f(x)$: in altre parole, se $\Omega = \{\alpha_1, \dots, \alpha_n\}$ è l'insieme delle radici di $f(x)$, posso considerare la mappa $\phi\colon \mathcal{G}(M/K) \to S_n$ che a g associa $g_{|\Omega}$. Il gruppo di Galois del polinomio è quindi isomorfo a un sottogruppo di S_n .

Dai teoremi precedenti discende il seguente

Teorema 3.4 (criterio di risolubilità per radicali)

Sia K è un campo di caratteristica 0, e $f(x) \in K[x]$ un polinomio non costante. Se l'equazione $f(x) = 0$ è risolubile per radicali, allora il gruppo $\mathcal{G}(M/K)$ con M campo di spezzameno di f su K è risolubile.

2 Polinomi con gruppo di Galois non risolubile

Esistono polinomi che hanno un gruppo di Galois non risolubile.

Proposizione 3.3

Sia p un numero primo, $f(x)$ un polinomio a coefficienti razionali, monico, irriducibile di grado p con esattamente due radici complesse non reali. Allora il gruppo di Galois di $f(x)$ è tutto S_p .

Dimostrazione

Sia M un campo di spezzamento di $f(x)$ su $\mathbb{Q}$, e $\alpha \in M$ una radice di $f(x)$, allora posso considerare $M \supseteq \mathbb{Q}(\alpha) \supseteq \mathbb{Q}$.

Osservo che $|\mathbb{Q}(\alpha) : \mathbb{Q}| = p$ perché $f(x)$ è polinomio minimo di ogni sua radice. In particolare, $p \mid |M : \mathbb{Q}| = o(\mathcal{G}(M/\mathbb{Q}))$, e quindi in $\mathcal{G}(M/\mathbb{Q})$ c'è un elemento di ordine p .

Sappiamo che il coniugio sui complessi induce un automorfismo di M su $\mathbb{Q}$ che scambia le due radici complesse e fissa le altre.

Per le osservazioni precedenti, posso pensare al gruppo di Galois di $f(x)$ come a un sottogruppo di S_p .

A meno di riordinare le radici, l'automorfismo indotto dal coniugio può essere pensato come la trasposizione $\sigma = (1, 2)$.

Supponiamo che l'elemento di ordine p in $\mathcal{G}(M/\mathbb{Q})$ di cui abbiamo mostrato l'esistenza sia $\tau = (i_1, i_2, \ldots, i_p)$.

Allora anche le potenze di τ stanno nel gruppo, e a meno di scambiare le potenze posso supporre $\tau = (1, 2, \ldots, p)$.

Mostro che S_p è generato da σ e τ : piu' in generale S_n e' generato da $\sigma = (1, 2)$ e $\tau = (1, 2, \ldots, n)$, infatti osservo che

$$
\begin{gathered}
(1,2) \in H = \langle \sigma, \tau \rangle \\
(1,2,\ldots,n)^{(1,2)} = (2,1,\ldots,n) \in H \\
(1,2)^{(2,1,\ldots,n)} = (1,3) \in H \\
(2,1,3,\ldots,n)^{(1,3)} = (2,3,1,\ldots,n) \in H \\
(1,3)^{(2,3,1,\ldots,n)} = (4,1) = (1,4) \in H
\end{gathered}
$$

e procedendo in questo modo ottengo che tutte le trasposizioni della forma $(1, i)$ stanno in H , per $i = 2, \ldots, n$.

Per quanto già dimostrato, S_p non è risolubile per $p \geq 5$.

Esempio 3.6 (Esempio concreto)

Il polinomio $f(x) = x^5 - 6x + 3 \in \mathbb{Q}[x]$ ha due radici complesse non reali ed è irriducibile su $\mathbb{Q}$, monico e di grado p , allora per la proposizione precedente il suo gruppo di Galois è S_5 che non è risolubile.

3 Fonti per testo e immagini; autori; licenze

3.1 Testo

- **Corso:Algebra IV I1/Risoluzione di radicali/Equazione risolubile per radicali**
  Fonte: https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Risoluzione_di_radicali/Equazione_risolubile_per_radicali?oldid=48276 *Contributori:* Toma.luca95, Irene, ScimmiaSpaziale e Mmontrasio

3.2 Immagini

3.3 Licenza dell'opera