Appendice del teorema di Abel Ruffini

Teorema

1) Se $f(x) \in K[x]$ e $\deg f(x) \leq 4$ allora l'eq. $f(x)=0$ è risolubile per radicali.

2) In generale le equazioni di grado ≥ 5 non sono risolubili per radicali.

Dim.

Ricordiamo che il gruppo di Galois di $f(x)$ su K è isomorfo a un sottogruppo di permutazioni delle radici di $f(x)$.

Studiamo la risolubilità di S_n.

S_n ha un sottogruppo normale di indice 2, A_n

$$A_n \subseteq S_n$$

basta studiare la risolubilità di A_n.

Fatto: le classi di coniugio in S_n sono in corrispondenza biunivoca con i tipi delle permutazioni, cioè
Due permutazioni in S_n sono coniugate $\Leftrightarrow$ hanno la stessa struttura ciclica.

Teorema

A_n è risolubile per $n \leq 4$

Dim.

Basta provarlo per A_4.

Consideriamo il gruppo delle simmetrie di un rettangolo.

$$V_4 = \{(1), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \leq 4$$

è normale in S_4 (contiene tutte le permutazioni con la stessa struttura ciclica), quindi in A_4.

$|V_4| = 4 \qquad |A_4| = 12$

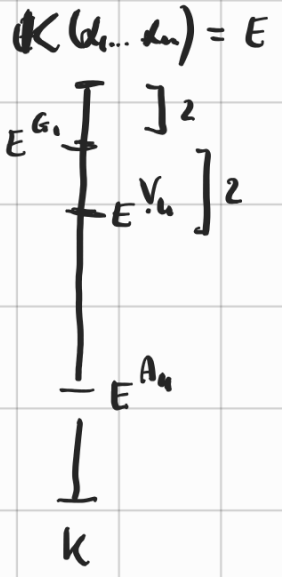
$$\{(1)\} \triangleleft V_4 \triangleleft A_4$$

$\{(1)\} \triangleleft V_4$: 4, abeliano, $\mathbb{Z}_2 \times \mathbb{Z}_2$

$V_4 \triangleleft A_4$: 3, ciclico

(tutti i gruppi di ordine 4 sono abeliani).

Quando se $f \in K[x]$ ha grado ≤ 4 si ottiene una successione di campi intermedi



ogni campo intermedio è ottenuto da quello immediatamente inferiore aggiungendo un radicale

ma questo dà la formula per le equazioni di quarto grado.

Definizione

Un gruppo si dice semplice se non ha sottogruppi normali non banali

Ovviamente ogni gruppo non abeliano semplice non è risolubile.

Teorema

A_n è semplice per $n \geq 5$.

In particolare: $f(x) \in K[x]$ ha grado n e ha gruppo di Galois S_n allora l'equazione $f(x) = 0$ non è risolubile per radicali.

Resta da dimostrare che tali polinomi esistono.

Teorema

Per ogni primo $p \geq 5$ esiste un polinomio $f(x)$ in $\mathbb{Q}[x]$ il cui gruppo di Galois è S_p

Ci serve il seguente

Lemma

Dato $p \geq 5$ esiste $f(x) \in \mathbb{Q}[x]$ (di grado p) con solo due radici cpx.

Dim Sia $k = p-2$

Scegliamo $c, a_1, \dots, a_k$ $(k > 1)$ numeri pari con

$c > 0$ $\quad a_1 < a_2 < \dots < a_k$ e $\sum a_i = 0$.

Consideriamo il polinomio

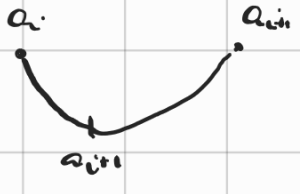
$$f(x) = (x^2 + c)(x - a_1) \cdots (x - a_k) + 2$$

$f(x)$ soddisfa il criterio di Eisenstein $\Rightarrow$ è irriduc. su $\mathbb{Q}$.

Sia $g(x) = (x^2 + c)(x - a_1) \cdots (x - a_k)$

Per $i = 1, \dots, k-1$ si ha $a_i < a_i + 1 < a_{i+1}$

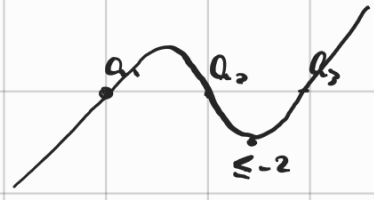
quindi

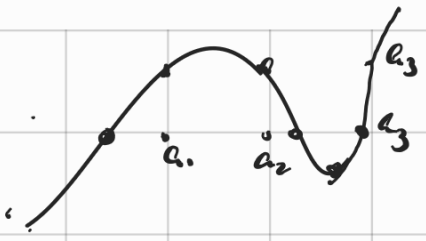


$|g(a_i + 1)|$ è un intero pari diverso da 1 $\Rightarrow \geq 2$

In part. $\quad g(a_i + 1) \leq -2$

Quindi tutti i minimi relativi della funzione $f(x)$ sono ≤ 0

$g(x)$ 

$f(x)$ 

in ogni intervallo $[a_i, a_{i+1}]$ con i pari, $g(x)$ assume valore -2 in due punti distinti.

$\Rightarrow f(x)$ ha almeno k radici reali.

Se avesse altre radici reali, tutte le radici sarebbero reali.

$$f(x) = (x^2 + c)(x - a_1) \dots (x - a_k) + 2$$

$$= x^{k+2} + \underbrace{\qquad}_{\text{il termine di grado } k+1 \text{ è } 0 \text{ perché } \sum a_i = 0} + \left(c + \sum_{i \neq j} a_i a_j\right) x^k + \dots$$

se $\alpha_1, \dots \alpha_{k+2}$ sono le radici di $f(x)$

allora $\sum \alpha_i = 0$ $\qquad \sum_{i \neq j} \alpha_i \alpha_j = c + \sum_{i \neq j} a_i a_j$

Quindi

$$\sum_{i<j} \alpha_i \alpha_j = \frac{1}{2}\left(\left(\sum \alpha_i\right)^2 - \sum \alpha_i^2\right) = -\frac{1}{2}\left(\sum \alpha_i^2\right)$$

($\sum \alpha_i = 0$)

Se tutte le radici sono reali $\sum_{i<j} \alpha_i \alpha_j < 0$.

Scegliendo c abbastanza grande in modo che $c + \sum_{i,j} a_i a_j > 0$ il polinomio $f(x)$ deve avere una (e quindi esattamente due) radici complesse. ∎

Dim. del teorema

Sia $p \geq 5$ e sia $f(x) \in \mathbb{Q}[x]$ un polinomio di grado p con esattamente due radici complesse.

Sia α una sua radice, quindi $[\mathbb{Q}(\alpha) : \mathbb{Q}] = p$

Sia $E/\mathbb{Q}$ il campo di decomposizione di $f(x)$, quindi $p \mid [E : \mathbb{Q}]$.

Sia $G = Gal(E/\mathbb{Q})$ $\Rightarrow$ $G \leq S_p$, $p \mid |G|$.

Per il teorema di Cauchy, G contiene un elemento di periodo p $\Rightarrow$ G contiene un ciclo σ di lunghezza p.

Possiamo anche assumere che $1, 2$ corrispondano alle due radici complesse. Il coniugio complesso τ induce un automorfismo di E che fissa j, $j = 3, \dots, p$ e inverte 1 e 2 $\Rightarrow$ $\tau = (1\ 2)$

Esiste i t.c. $\sigma^i(1) = 2$ e σ^i è un ciclo di lunghezza p $\Rightarrow$ possiamo assumere $\sigma = (1\ 2 \dots p)$

Quindi G contiene $(1\ 2 \dots p)$ e $(1\ 2)$

Proviamo che ogni trasposizione è in G.

$\sigma \tau \sigma^{-1} = (1\ 2 \dots p)(1\ 2)(p \dots 1) = (2\ 3)$

e analogamente $\sigma (i\ i+1) \sigma^{-1} = (i+1, i+2)$

$\Rightarrow$ $(i, i+1) \in G$ per ogni i.

Inoltre $(2\ 3)(1\ 2)(2\ 3) = (1\ 3)$

$(3\ 4)(1\ 3)(3\ 4) = (1\ 4)$

$(i\ i+1)(1\ i)(i\ i+1) = (1\ i+1) \rightsquigarrow (1,j) \in G$

e $(1\ j)(1\ i)(1\ j) = (i\ j)$

Quindi G contiene tutte le trasposizioni $\rightsquigarrow G = S_n$. ☐

È possibile dimostrare che per ogni n esiste un polinomio di grado n in $\mathbb{Q}[x]$ che ha gruppo di Galois S_n o A_n. (da fatto il "generico" polinomio di grado n in $\mathbb{Q}[x]$ ha gruppo di Galois S_n).

Inoltre

- ogni gruppo risolubile è un gruppo di Galois su $\mathbb{Q}$
- non so se ogni gruppo finito è un gruppo di Galois su $\mathbb{Q}$. (Cayley $\rightsquigarrow$ è un gruppo di G. su un campo di numeri).

COMPLEMENTI SULLE PERMUTAZIONI

Prop. Due permutazioni in S_n sono coniugate $\Leftrightarrow$ hanno la stessa struttura ciclica (tipo)

Dim.

Basta provarlo per i cicli

$$\sigma\,(i_1 \dots i_k)\,\sigma^{-1} : \sigma(i_j) \longrightarrow \sigma(i_{j+1}) \quad (\text{mod } k)$$

$$: \ell \longmapsto \ell$$

$$\text{se } \ell \notin \{\sigma(i_1), \dots \sigma(i_{j+1})\}$$

Quindi

$$\sigma\circ(i_1 \dots i_k)\circ\sigma^{-1} = (\sigma(i_1), \dots, \sigma(i_k))$$

Se due permutazioni hanno lo stesso tipo

$\tau_1 = (c_1 \dots c_2)$ - - — — (cicli disgiunti)

$\tau_2 = (c'_1 \dots c'_2)$ - - - — —

Posto $\sigma(c_i) = c'_i$ troviamo $\sigma\tau_1\sigma^{-1} = \tau_2$. ∎

Conseguenza: se $H \leq S_n$

$H \lhd S_n \Leftrightarrow$ per ogni tipo, o H non contiene alcuna permutazione di quel tipo, o le contiene tutte.

Prop.

A_n è generato dai 3-cicli

Dim. (Induzione sul # di elementi mossi da σ)

Sia $\sigma \in A_n$ | Se $\sigma \neq (1)$ σ opera su almeno 3 elementi a, b, c. Supponiamo $b = \sigma(a) \neq a$, $c \neq a, b$

Consideriamo $\gamma = (b\ a\ c)\sigma$

è poi $\gamma(a) = a \Rightarrow$ è generato da 3-cicli.

Teorema

A_n è semplice per $n \geq 5$

Dim.

Sia $H \triangleleft A_n$ H non banale, $n \geq 5$

Per la proposizione precedente, basta provare che H contiene un 3-ciclo.

Sia $\sigma \in H$ tale che l'insieme $\{k \mid \sigma(k) \neq k\}$ ha cardinalità minima m_0.

Se $\sigma = c_1 \dots c_r$ è lo scrittura di σ come prodotto di cicli disgiunti, tutti i c_i devono avere la stessa lunghezza (altrimenti una potenza di σ non nulla coinvolgerebbe un numero di elementi $< m_0$.

$\sigma' = c_1 c_2^{-1} \dots c_k^{-1} \in H$ (ha lo stesso tipo di σ).

$\Rightarrow c_1^2 \in H \rightsquigarrow$ 2 possibilità

① σ è un ciclo

② $c_1 \dots c_2$ sono 2 cicli

Se σ è un ciclo $(a_1\ a_2 \dots a_k)$

$\tau = (a_2\ a_1 \dots a_k) \in H$

$\sigma\tau$ fissa a_1, a_2 ma $\sigma\tau = 1$ $\tau = \sigma^{-1}$

ma σ è un 2-ciclo (NO) o un 3 ciclo OK.

Se σ è prodotto di 2 cicli

$\sigma = (a_1\ a_2)(a_3\ a_4) \dots$

$\tau = (a_1\ a_3)(a_2\ a_4) \dots$

$\sigma\tau = (a_1\ a_2)(a_3\ a_4)(a_1\ a_3)(a_2\ a_4) = (a_1\ a_4)(a_2\ a_3)$

Sia $b \in \{a_1\ a_2\ a_3\ a_4\}$

$\nu = (a_1\ b)(a_2\ a_3) \in H$

$\nu\sigma = (a_1\ a_4)(a_1\ b) = (a_1\ b\ a_4) \in H.$ ∎