Complementi

Note Title 20/12/2018

Teorema fondam. dell'algebra

- $f(x) \in \mathbb{R}[x]$ deg $f(x) \geq 3$ $\boxed{\text{dispari}}$ $\Rightarrow$ $f(x)$ riducibile

  teorema dei valori intermedi, primo input analitico

- $\mathbb{C}$ non ha estens. quadratiche

  $$x^2 + ax + b = 0$$

  $$\mathbb{C} \ni \frac{-a \pm \sqrt{a^2 - 4b}}{2}$$

  in $\mathbb{C}$ riesco ad estrarre radici quadrate

- Per assurdo $\mathbb{C}$ non alg. chiuso

Galois gruppo G

$$\begin{array}{l} K \\ | \\ F \\ | \leftarrow \text{finita} \\ \mathbb{C} \\ |\,2 \\ \mathbb{R} \end{array} \qquad K \overset{2^a}{\text{---}} K^{P_2} \overset{d \text{ dispari}}{\text{---}} \mathbb{R}$$

$G > P_2$ un 2-Sylow

d dispari $\Longrightarrow K^{P_2} = \mathbb{R}$

il polinomio minimo di un generatore ha grado dispari, quindi è di grado 1 (deve essere irriducibile)

L'unica ext. quadratica di $\mathbb{R}$ è $\mathbb{C}$

$$\frac{\mathbb{R}[x]}{(x^2+ax+b)} \simeq \mathbb{C}$$

$$P_2 \underbrace{> H_m >}_{2} \underbrace{H_{m-1} \supset}_{2} \dots \supset H_0 = \{e\}$$

Via teoria di Galois otteniamo una catena di estensioni

$$K \underset{2}{\supset} K^{H_1} \underset{2}{\supset} K^{H_2} \supset \dots \supset K^{H_n} \underset{2}{\supset} K^{P_2} = \mathbb{R}$$

Da $\mathbb{C}$ a K si passa con ext quadratiche $\Rightarrow K = \mathbb{C}$

Il teorema delle funzioni simmetriche

$a+b+c \qquad a^2b+b^2c+c^2a+ab^2+bc^2+ca^2$

$$f(x_1, \dots, x_n) = f(x_{\sigma(1)}, \dots, x_{\sigma(n)}) \quad \forall \sigma \in S_n$$

Esempi
- $x_1^k + \dots + x_n^k$
- funzioni simm. elementari

$a+b+c, \quad ab+bc+ca, \quad abc$

$$e_i = \sum_{\substack{|I|=i \\ I \subseteq \{1,\dots,n\}}} \prod_{j \in I} x_j$$

In 4 variabili,

$$\begin{aligned} a+b+c+d &= e_1 \\ ab+ac+ad+bc+bd+cd &= e_2 \\ abc+abd+acd+bcd &= e_3 \\ abcd &= e_4 \end{aligned}$$

$$(x-x_1)\cdots(x-x_n) = x^n - e_1x^{n-1} + e_2x^{n-2} - \dots + (-1)^n e_n$$

Teo Sia $f(x_1, \dots, x_n) \in K(x_1, \dots, x_n)$ simmetrica

$\exists\, g \in K(e_1, \dots, e_n)$ t.c. $f(x_1, \dots, x_n) = g(e_1, \dots, e_n)$

Esempio $a^2b + a^2c + \dots + cb^2 = (a+b+c)(ab+bc+ca) - 3abc$

$= e_1e_2 - 3e_3$

Dim

$$\left[\begin{array}{c} K(x_1, \dots, x_n) \circlearrowleft S_n \\ | \\ K(x_1, \dots, x_n)^{S_n} \\ | \\ K(e_1, \dots, e_n) \end{array}\right]$$

Galois grado $n!$ — grado $\le n!$

$$(t-x_1)\dots(t-x_n) = t^n - e_{n-1}t^{n-1} + \dots \pm e_n t^n$$

Siccome $K(x_1, \dots, x_n)$ = campo di spezzamento del polinomio qui sopra, ottengo $[K(x_1, \dots, x_n) : K(e_1, \dots, e_n)] \leq (\deg)! = n!$

$\mathbb{Q}(\alpha,\beta) = \mathbb{Q}(\alpha+\beta)$ se $\deg(\alpha)$, $\deg \beta$ coprimi

$$\begin{tikzcd} & \mathbb{Q}(\alpha,\beta) & \\ \mathbb{Q}(\alpha) \arrow[ur, dash, "n"] & & \mathbb{Q}(\beta) \arrow[ul, dash, "m"'] \\ & \mathbb{Q} \arrow[ul, dash, "m"] \arrow[ur, dash, "n"'] & \end{tikzcd}$$

$\alpha_1, \dots, \alpha_m$ = coniugati di α

$\beta_1, \dots, \beta_n$ = ——————— β

Oss Su $\mathbb{C}$ c'è un ordinamento compatibile con la somma: "lessicografico"

$$a_1+ib_1 < a_2+ib_2 \iff \begin{cases} \text{o} & a_1 < a_2 \\ \text{o} & a_1 = a_2 \text{ e } b_1 < b_2 \end{cases}$$

$$a_3+ib_3 \leq a_4+ib_4$$

Consideriamo l'insieme finito $\left\{ \alpha_i + \beta_j \;\middle|\; \begin{matrix} i=1,\dots,m \\ j=1,\dots,n \end{matrix} \right\}$

Diciamo che il massimo di questo insieme sia $\alpha_k+\beta_\ell$, dove $\alpha_k = \max\{\alpha_i\}$, $\beta_\ell = \max\{\beta_j\}$

$$\text{Galois}\left[\begin{tikzcd} K \arrow[d, dash] \\ \mathbb{Q}(\alpha,\beta) \arrow[d, dash] \\ \mathbb{Q}(\alpha+\beta) \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd}\right.$$

$$\left.\begin{matrix} \mathbb{Q}(\alpha,\beta) \\ \\ \mathbb{Q} \end{matrix}\right] mn$$

Le radici del polinomio minimo di $\alpha+\beta$ sono i $\sigma(\alpha+\beta)$ al variare di $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$

alcuni degli $\alpha_i+\beta_j$

Certamente $\forall i \; \forall j$ trovo σ t.c. $\sigma(\alpha) = \alpha_i$, $\sigma(\beta) = \beta_j$

$\llcorner$ ci sono $m \cdot n$ omomorfismi $\neq 0$ di $\mathbb{Q}(\alpha,\beta)$ in $\mathbb{C}$

(questo dipende da $[\mathbb{Q}(\alpha,\beta) : \mathbb{Q}(\alpha)] = [\mathbb{Q}(\beta):\mathbb{Q}]$)

Osserviamo che $\sigma(\alpha_k+\beta_\ell) = \alpha_i+\beta_j$ e per

$\sigma \neq id$ se avessi $\alpha_i+\beta_j = \alpha_k+\beta_\ell \geq \alpha_i+\beta_j$

otterrei un assurdo.

$\Rightarrow$ $\alpha_k+\beta_\ell$ non e' fissato da alcun σ

$\Rightarrow$ $[\mathbb{Q}(\alpha_k+\beta_\ell):\mathbb{Q}] = m\cdot n$

$\Rightarrow$ $[\mathbb{Q}(\alpha+\beta):\mathbb{Q}] = mn$

Rivediamo i punti chiave della dimostrazione:

① Il max di $\alpha_i+\beta_j$ e' $\max\{\alpha_i\}+\max\{\beta_j\}$, questo garantisce $\sigma(\alpha_k+\beta_\ell)\neq\alpha_k+\beta_\ell$ se $\sigma\neq id$, perché se $\sigma\neq id$ allora o $\sigma(\alpha_k)<\alpha_k$ o $\sigma(\beta_\ell)<\beta_\ell$, o entrambi, e quindi $\sigma(\alpha_k)+\sigma(\beta_\ell)<\alpha_k+\beta_\ell$

② $\sigma(\alpha_k+\beta_\ell)\neq\tau(\alpha_k+\beta_\ell)$ se $\sigma\neq\tau$, perché se fossero uguali otterrei $\tau^{-1}\sigma(\alpha_k+\beta_\ell)=\alpha_k+\beta_\ell$, quindi $\tau^{-1}\sigma=id \Rightarrow \tau=\sigma$.

③ I coniugati di $\alpha_k+\beta_\ell$ sono TUTTI (e soli) gli $\alpha_i+\beta_j$ (perché ogni σ produce un coniug. diverso)

④ Questo implica $[\mathbb{Q}(\alpha_k+\beta_\ell):\mathbb{Q}]=mn$ ed inoltre

$[\mathbb{Q}(\alpha+\beta):\mathbb{Q}]=[\mathbb{Q}(\alpha_k+\beta_\ell):\mathbb{Q}]$, perché

$\alpha+\beta$ e $\alpha_k+\beta_\ell$ coniugati, quindi hanno lo stesso grado su $\mathbb{Q}$.

⑤ Ne segue $[\mathbb{Q}(\alpha+\beta):\mathbb{Q}]=mn=[\mathbb{Q}(\alpha,\beta):\mathbb{Q}]$, che combinato con $\mathbb{Q}(\alpha+\beta)\subseteq\mathbb{Q}(\alpha,\beta)$ da' l'uguaglianza voluta

Teorema della progressione aritmetica di Dirichlet

$a, b \in \mathbb{Z}$ con $(a, b) = 1$ $\quad a \neq 0$

Allora l'insieme $\{ma + b, \; m \in \mathbb{Z}\}$ contiene infiniti numeri primi

Dim per $b = 1$

Supponiamo p primo, c intero, $\begin{cases} c^a \equiv 1 \; (p) \\ c^k \not\equiv 1 \; (p) & 0 < k < a \end{cases}$

$\Rightarrow \operatorname{ord}_p(c) = a \Rightarrow a \mid p-1$

Mi basta dim che $\exists$ infiniti p per cui esiste c di ordine esattamente a

Considero $x^a - 1 = \prod_{r \mid a} \Phi_r(x)$, dove Φ_r e' il polin. minimo delle radici r-esime di 1 $\quad$ deg $\varphi(r)$

$$\left(a = \sum_{r \mid a} \varphi(r) \right)$$

Cerco radici di $\Phi_a(x)$ che non siano radici di $\prod_{k<a} (x^k - 1) =: q(x)$

$$(\Phi_a(x), q(x)) = 1 \Longrightarrow \Phi_a(x) \underset{\mathbb{Q}[x]}{\underset{\cup}{u(x)}} + q(x) \underset{\mathbb{Q}[x]}{\underset{\cup}{v(x)}} = 1$$

$$\Rightarrow \Phi_a \cdot \underset{\mathbb{Z}[x]}{\underset{\cap}{U}} + q(x) \cdot \underset{\mathbb{Z}[x]}{\underset{\cap}{V(x)}} = A \in \mathbb{Z}$$

Esistono infiniti primi modulo i quali $\Phi_a(x)$ abbia una radice, chiamiamola c

$$\overbrace{\Phi_a(c) \cdot U(c)}^{0} + q(c) \, V(c) \equiv A \mod p$$

se $p \nmid A$, allora $p \nmid q(c)$

Riassumendo:
- esistono infinite coppie $(p, c \bmod p)$ t.c.
$$\Phi_a(c) \equiv 0 \mod p$$
- la congruenza qui sopra implica che per ogni tale coppia si abbia $q(c)\, V(c) \equiv A\ (p)$
- Scartando i p che dividono A, ho ancora ∞ coppie t.c. $\Phi_a(c) \equiv 0\ (p)$, $q(c) \not\equiv 0\ (p)$
- $c^a \equiv 1\ (p)$: infatti $x^a - 1 = \Phi_a(x) \cdot s(x)$
$$\Rightarrow \quad c^a - 1 \equiv \Phi_a(c)\, s(c) \equiv 0\ (p)$$

e d'altro canto $\quad 0 \not\equiv q(c) = \prod_{k<a} (c^k - 1) \quad (p)$

$\Rightarrow$ FINE! $\square$

Esempio $\quad 3K+1 \qquad \Phi_3(x) = x^2 + x + 1$

$q(x) = x - 1 \qquad (x^2+x+1) - (x-1)\cdot(x+2) = 3 = A$

Quindi devo scartare il primo 3, e poi voglio primi modulo i quali Φ_3 abbia radici. Il modo più semplice è quello di guardare i fattori primi di $\Phi_3(n)$ al variare di $n \in \mathbb{Z}$.

da scartare

$\Phi_3(2) = 7 \equiv 1\ (3)$, $\Phi_3(3) = 13 \equiv 1\ (3)$, $\Phi_3(4) = 21 = 3 \cdot 7$,

$\Phi_3(5) = 31 \equiv 1\ (3)$, $\Phi_3(6) = 43 \equiv 1\ (3)$, ...

Problema inverso di Galois per gruppi abeliani

$G \simeq G_{p_1} \times \dots \times G_{p_k}$ gruppo abeliano finito.

Vorrei trovare un polinomio il cui campo di spezz. abbia gruppo di Galois G.

Basta realizzare $G_{p_1}, G_{p_2}, \dots, G_{p_k}$:

$$\begin{tikzcd}
 & K = K(\alpha) \arrow[dl, no head] \arrow[dr, no head] & \\
K_{p_1} \arrow[dr, no head, "G_{p_1}"'] & & K_{p_2} \arrow[dl, no head, "G_{p_2}"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

$Gal(K/\mathbb{Q}) \hookrightarrow G_{p_1} \times G_{p_2}$

cardinalità $[K:\mathbb{Q}] = [K_{p_1}:\mathbb{Q}] \cdot [K_{p_2}:\mathbb{Q}]$
$= \# G_{p_1} \cdot \# G_{p_2}$

Basta prendere il polin. minimo di α.

Ci siamo così ridotti al caso $G =$ p-gruppo.

Studiamo $G_p = \mathbb{Z}/p^{a_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{a_r}\mathbb{Z}$

Cominciamo a realizzare $\mathbb{Z}/p^{a_1}\mathbb{Z}$.

Esempio: $\mathbb{Z}/4\mathbb{Z}$

$$\begin{tikzcd}
\mathbb{Q}(\zeta_{13}) \arrow[d, no head, "\mathbb{Z}/12\mathbb{Z}"'] \arrow[r, no head] & \mathbb{Q}(\zeta_{13})^H \arrow[dl, no head, "4"] \\
\mathbb{Q} &
\end{tikzcd}$$

$|H| = 3$

4, gp di Galois $\mathbb{Z}/12\mathbb{Z} \,/ H \simeq \mathbb{Z}/4\mathbb{Z}$

Notare che $H \triangleleft \mathbb{Z}/12\mathbb{Z}$!

In generale: realizzare $\mathbb{Z}/d\mathbb{Z}$

$$\begin{tikzcd}[row sep=large]
\mathbb{Q}(\zeta_q) \arrow[dd, dash, bend right=60, "\mathbb{Z}/(q-1)\mathbb{Z}"'] \arrow[dr, dash] \arrow[dd, dash] & \\
& \mathbb{Q}(\zeta_q)^H \arrow[dl, dash, "\text{Galois con gp } \mathbb{Z}/d\mathbb{Z}"] \\
\mathbb{Q} &
\end{tikzcd}$$

Sia d un divisore di $q-1$. $\mathbb{Z}/(q-1)\mathbb{Z}$ c'è un sottogruppo di indice d, chiamiamolo H, ovviamente normale

Realizzare $\mathbb{Z}/p^{a_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{a_r}\mathbb{Z}$

Per ogni $\mathbb{Z}/p^{a_i}\mathbb{Z}$ scegliamo un primo $q_i \equiv 1 \pmod{p^{a_i}}$ e dentro $\mathbb{Q}(\zeta_{q_i})$ prendiamo il sottocampo che abbia grado p^{a_i} su $\mathbb{Q}$, chiamiamolo K_i

$K := K_1 \dots K_r$ $\qquad\qquad$ $\mathrm{Gal}(K/\mathbb{Q}) \hookrightarrow \prod \mathrm{Gal}(K_i/\mathbb{Q})$

$$\begin{tikzcd}
& K_1K_2 \arrow[dl, dash] \arrow[dr, dash] & \\
K_1 \arrow[dr, dash, "p^{a_1}"'] & & K_2 \arrow[dl, dash, "p^{a_2}"] \\
& \mathbb{Q} &
\end{tikzcd}$$

ed inoltre si ha

$$[K_1K_2 : \mathbb{Q}] = [K_1K_2 : K_2][K_2 : \mathbb{Q}]$$

$$= [K_1 : K_1 \cap K_2][K_2 : \mathbb{Q}]$$

$\hookrightarrow$ è $\mathbb{Q}$? Sì, $\subseteq \mathbb{Q}(\zeta_{q_1}) \cap \mathbb{Q}(\zeta_{q_2}) = \mathbb{Q}$

$$= [K_1 : \mathbb{Q}][K_2 : \mathbb{Q}].$$

Ne segue (per induz. su r) che $[K_1 \dots K_r : \mathbb{Q}] =$

$$= [K_1 : \mathbb{Q}] \dots [K_r : \mathbb{Q}] = \#\mathrm{Gal}(K_1/\mathbb{Q}) \dots \#\mathrm{Gal}(K_r/\mathbb{Q})$$

e quindi $\mathrm{Gal}(K/\mathbb{Q}) \hookrightarrow \prod_{i=1}^{r} \mathrm{Gal}(K_i/\mathbb{Q})$ è un isomorfismo per questioni di cardinalità.