ALGEBA 1 - 19 DIC 2018

Note Title 12/19/2018

COMPLEMENTI

Risolubilità per radicali

Problema $f(x) \in \mathbb{Q}[x]$ $\deg f = n$

$\alpha_1, \dots, \alpha_n$ (eventualmente coincidenti) radici $\in \mathbb{C}$ di $f(x)$. Si possono scrivere $\alpha_1, \dots, \alpha_n$ "tramite radicali" ?

Es $\sqrt[3]{2+\sqrt[7]{5}}$ = espressione tramite radicali

$\sqrt[3]{1+i}$ "

Def. Un elemento $\alpha \in \mathbb{C}$ si dice esprimibile tramite radicali se appartiene ad un campo K tale che esiste una successione di sottocampi

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq K_2 \subseteq \dots \subseteq K_m = K$$

con $K_{i+1} = K_i(\sqrt[r]{a_i})$ $a_i \in K$.

$\sqrt[3]{2+\sqrt[7]{5}}$: $\mathbb{Q} = K_0 \subseteq K_1 = \mathbb{Q}(\sqrt[7]{5}) = K_2 = \mathbb{Q}(\sqrt[3]{2+\sqrt[7]{5}})$

Def 2 Un'equazione $f(x) = 0$ si dice risolubile per radicali se il campo di spezzamento di $f(x)$ è un campo del tipo precedente.

Esempio $f(x) = x^n - a$

2 radici: $\sqrt[n]{a}, \zeta_n\sqrt[n]{a}, \zeta_n^2\sqrt[n]{a}, \dots, \zeta_n^{n-1}\sqrt[n]{a}$.

$$\mathbb{Q} \subseteq \mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta_n, \sqrt[n]{a}) = K$$

$\zeta_n^n = 1$; $\sqrt[n]{a}^n = a$

$\zeta_n = \sqrt[n]{1}$

$\sqrt[m]{b}$

$$\underbrace{K \subseteq K(\zeta_n)}_{①} \underbrace{\subseteq K(\zeta_n, \sqrt[m]{b})}_{②}$$

In generale, ottengo una catena di estensioni di cui

① è di Galois abeliana

② è ciclica

$\| K'$

(Se il grado $[K(\zeta_n, \sqrt[m]{b}) : K(\zeta_n)]$ non è $= m$, comunque gli omomorfismi di K' che lasciano fisso K sono elementi di H.

$\varphi_i : \sqrt[m]{b} \mapsto \zeta^i\sqrt[m]{b}$

E gli i che intervengono sono un sottogruppo di $\mathbb{Z}/m\mathbb{Z}$

($\varphi_i \mapsto i$ è un omomorfismo iniettivo).

Oss Un'estensione abeliana finita F/E possiede una catena di sottoestensioni

$$F_0 = E \subseteq F_1 \subseteq \dots \subseteq F_s = F$$

dove F_{i+1}/F_i è ciclica

Conclusione Se $f(x)$ è risolubile per radicali, allora il suo c.d.s. K possiede una catena di sottocampi:

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \dots \subseteq K_n = K$$

dove K_{i+1}/K_i è ciclica

VICEVERSA? Supponiamo che le radici di $f(x)$ appartengano ad un campo del tipo descritto.

Se $\alpha \in K = K_n$

allora K_n/K_{n-1} è ciclica, per esempio di grado d

$$K_{n-1}(\alpha, \sqrt[d]{\beta})$$

$$K_{n-1}(\alpha) \qquad K_{n-1}(\sqrt[d]{\beta})$$

$$K_{n-1}$$

$\mathrm{Gal}(K_{n-1}(\alpha, \sqrt[d]{\beta})/K_{n-1}(\alpha)) \to \mathrm{Gal}(K_{n-1}(\sqrt[d]{\beta})/K_{n-1})$ come invertivo. ciclico

$\mathrm{Gal}(K_{n-1}(\alpha, \sqrt[d]{\beta})/K_{n-1}(\alpha))$ ciclica

PROBLEMA: SI PUÒ SCRIVERE QUESTA ESPRESSIONE TRAMITE UN RADICALE?

(Dim. classica: Teorema 90 di Hilbert)

$G = \mathrm{Gal}(\quad)$ ... ciclico

$G = \langle \sigma \rangle$ σ di ordine d

$F = K(\alpha, \sqrt[d]{\beta})$ $E = K(\alpha)$

σ è una funzione E-lineare

$\sigma : F \to E$

$\sigma^d = id$ pol. min. $X^d - 1$

autovalori: $1, \zeta_d, \zeta_d^2, \dots, \zeta_d^{n-1}$

In $\mathbb{C}$ esiste un autovettore per qualsiasi autovalore.

$$\sigma(v) = \zeta_d v$$

Questa equazione si può scrivere (tramite una base con coefficienti in E)

$\rightsquigarrow \exists$ un elemento che si scrive con coeff. in E

$v \in F$

(v = comb. lineare di una base di F/E con coeff in E)

$\beta \in E$ tale che $\sigma(\beta) = \zeta_d \beta$

(autovettore con autovalore ζ_d).

$$\sigma(\beta^d) = (\zeta_d \beta)^d = \zeta_d^d \beta^d = \beta^d$$

$\Rightarrow \beta^d$ è lasciato fisso da σ ($\forall \sigma \in \langle \sigma \rangle$)

$\beta^d \in E$.

β è radice di $X^d = c$ $\qquad \beta^2 = c$

$\Rightarrow \beta$ è un radicale

HO UN SE E SOLO SE:

EQ. RISOLUBILE PER RADICALI $\Leftrightarrow$

C'È UNA SUCCESSIONE DI ESTENSIONI CICLICHE COME PRIMA

FATTO Sia $f(x) \in \mathbb{Q}[x]$, $\deg f = n$

G = gruppo di Galois di $f(x)$

$G < S_n$.

Allora G è "quasi sempre" $= S_n$.

$n=2$ S_2 $\{e\} \subseteq S_2$

$n=3$ S_3 $\{e\} \subseteq A_3 \subseteq S_3$

$n=4$ S_4 $\{e\} \subseteq V_4 \subseteq A_4 \subseteq S_4$

$$V_4 = \{e, (12)(34), (13)(24), (14)(23)\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

$n=5$ $\{e\} \subseteq A_5 \subseteq S_5$

NIENTE DA FARE!!!

PERIODI GAUSSIANI

p primo $K = \mathbb{Q}(\zeta_p)$ $\zeta = \zeta_p$

$G = \mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ ciclico di ordine $p-1$

Sia $d \mid p-1$ $p-1 = ad$.

$\exists$ uno e un solo sottogruppo di G di ordine a $\rightarrow$ (Galois) $\exists$ uno e un solo sottocampo $2^\circ K$ di grado d

$G = \langle g \rangle$ $|H| = a$ $H = \langle g^d \rangle$

Consideriamo l'elemento

$$\gamma = \sum_{h \in H} \zeta^h$$

$H \hookrightarrow (\mathbb{Z}/p\mathbb{Z})^*$

$p=5 \quad a=2$

$\zeta+\zeta^4 = \zeta+\zeta^{-1}$

$p=7 \quad a=3$

$\zeta+\zeta^2+\zeta^4$.

Considero un "coniugato" di γ, cioè un elemento del tipo $\sigma(\gamma)$ dove $\sigma \in G$.

$$\sigma(\zeta) = \zeta^i$$

$$\sigma(\gamma) = \sum_{h \in H} \zeta^{ih} = \sum_{k \in iH} \zeta^k .$$

Ci sono d classi laterali

$\Rightarrow$ il n° di coniugati di γ è $\leq d$

In effetti $= d$.

Se ci fosse una coincidenza

$$\sum_{h \in H} \zeta^{ih} = \sum_{h \in H} \zeta^{jh} \qquad iH \neq jH$$

avrei $\sum_{h \in H} \zeta^{ih} - \sum \zeta^{jh} = 0$

cioè ζ radice del polinomio

$$\sum_{h \in H} X^{ih} - \sum_{h \in H} X^{jh} = f(X)$$

$1 \leq i, j \leq q-1 \qquad f(X) = X\, g(X)$

$\deg g < p-1$

pol. min di ζ : $X^{p-1} + X^{p-2} + \dots + X + 1 = \phi(X)$

$\downarrow$

$g \cdot d = p-1$

$\phi(X) \mid X\, g(X)$

$\Rightarrow \phi(X) \mid X \quad \cdot \quad \phi(X) \mid g(X)$

ASSURDO.

Quindi $[\mathbb{Q}(\sum_{h \in H} \zeta^h) : \mathbb{Q}] = d$

(ci sono d automorfismi distinti).

Caso particolare $d = 2$.

$\alpha = \gamma = \sum_{h \in Q} \zeta^h \qquad \beta = \sigma(\gamma) = \sum_{h \notin Q} \zeta^h$

Q quadrati

Pol. min su $\mathbb{Q}$ è $(X-\alpha)(X-\beta)$

$= X^2 - (\alpha+\beta)X + \alpha\beta$

$\alpha + \beta = \sum_{h \neq 0} \zeta^h = -1$

$\alpha\beta = \sum_{h \in Q} \sum_{k \notin Q} \zeta^{h+k}$

CONGRUENZA di p mod 4.

$p \equiv 1 \pmod 4$ quadrato x^2

$= 1 - x^2$ quadrato

-1 è un quadrato)

$p \equiv 3 \pmod 4$ $\quad x^2$ quadrato $\to -x^2$ non è un quadrato.

Nel caso $p \equiv 1 \pmod 4$ $\quad h+k \not\equiv 0$ sempre $\pmod p$

Nel caso $p \equiv 3 \pmod 4$ $\quad h+k \equiv 0$ $\pmod p$

esattamente $\frac{p-1}{2}$ volte

(una per ogni valore di h)

$p \equiv 1 \pmod 4 \longrightarrow \alpha\beta$ = somma di potenze di ζ tutte con esponente $\not\equiv 0 \ (p)$

$a_1\zeta^1 + a_2\zeta^2 + \dots + a_{p-1}\zeta^{p-1} \in \mathbb{Q}$

$\Rightarrow a_1 = a_2 = \dots = a_{p-1} = r \in \mathbb{Q}$

$(a_1 X + a_2 X^2 + \dots + a_{p-1} X^{p-1} - r$ è un multiplo del polinomio di ζ)

$\left(\frac{p-1}{2}\right)^2$ prodotti ognuno ζ^i compare $\frac{p-1}{4}$ volte.

$\zeta^{p-1} + \zeta^{p-2} + \dots + \zeta = -1$

$Q \cdot (\text{non } \mathbb{Q})$

Pol min $\quad X^2 + X - \frac{p-1}{4}$

$(\alpha + \beta = -1)$

$\Delta = 1 + 4\frac{(p-1)}{4} = p$

$\mathbb{Q}(\sqrt{p})$.

$p \equiv 3 \pmod 4$ $\quad \frac{p-1}{2}$ volte $h+k \equiv 0 \ (p=11)$

$\downarrow$

contribuisce con $\frac{p-1}{2}$ volte $\underline{1}$

Restano

$$\left(\frac{p-1}{2}\right)^2 - \left(\frac{p-1}{2}\right) \quad \text{per } h \neq k \quad \zeta^{h+k} \neq 1$$

11

$$\left(\frac{p-1}{2}\right)\left(\frac{p-3}{2}\right)$$

Come prima, questi si dividono in gruppi ciascuno dei quali ha $p-1$ termini

Quindi questi contribuiscono con

$\frac{p-3}{4}$ volte il valore -1.

TOTALE: $\frac{p-1}{2} - \frac{p-3}{4} = \frac{2p-2-p+3}{4} = \frac{p+1}{4}$.

Pol min

$$X^2 + X + \frac{p+1}{4}$$

$$\Delta = -1 - 4\left(\frac{p+1}{4}\right) = -p$$

$$\mathbb{Q}(\sqrt{-p}).$$

Es $\quad G(5_9) \qquad H < (\mathbb{Z}/9\mathbb{Z})^*$

$$H = \{1, 4, 7\}$$

$$\gamma = \zeta + \zeta^4 + \zeta^7 = \zeta(1 + \zeta^3 + \zeta^6) = 0.$$