ALGEBRA 1 — 4 DIC 2018

Note Title 12/4/2018

Problema: ricerca degli omomorfismi

$$\varphi: K(\alpha) \to \Omega$$

dove Ω è campo algebricamente chiuso contenente K e $\alpha \in \Omega$ è algebrico su K.

Nel caso particolare in cui $\varphi|_K = $ identità (inclusione) gli omomorfismi sono in corrispondenza biunivoca con le radici di $\mu_\alpha(x) =$ pol. min di α su K

$$K[x] \xrightarrow{f} \Omega$$

$$\searrow^{\pi} \quad \nearrow_{\varphi}$$

$$K[x]/(\mu_\alpha(x))$$

$x \mapsto \gamma$ radice di $\mu_\alpha(x)$

$$p(x) \xmapsto{f} p(\alpha)$$

e questo induce φ.

Nei casi classici (char $K = 0$ o K campo finito) il numero di radici distinte di $\mu_\alpha(x)$ (irriducibile) è uguale al grado di $\mu_\alpha(x)$ che è a sua volta uguale a $[K(\alpha):K]$.

In generale $\varphi(K) = K' \quad K' \cong K$

(stiamo considerando il caso $\varphi \not\equiv 0$).

In questo caso

$$K[x] \cong K'[x]$$

$$c_n x^n + \dots + c_0 \mapsto \varphi(c_n) x^n + \dots \to \varphi(c_0)$$

$$\mu_\alpha(x) \mapsto \mu'_\alpha(x)$$

irriducibile → inseparabile

Se voglio che $\ker \varphi \geq \mu_\alpha(x)$
devo mandare α in una radice di $\mu'_\alpha(x)$
Quindi, in particolare, ci sono tanti omomorfismi quante sono le radici distinte di $\mu'_\alpha(x)$.
("di solito" tanti quanto il grado di $\mu'_\alpha(x)$).

Generalizzazione:
Omomorfismi $\varphi : E \to \Omega$ tali che $\boxed{\varphi|_K = id.}$
dove E/K è un'estensione finita e
Ω è una chiusura algebrica di K.

In questo caso si ha comunque che l'estensione E/K è finitamente generata
(Per esempio, una base di E/K come S.V. è un insieme di generatori).

$$E = K(\alpha_1, \alpha_2, \dots, \alpha_m).$$

$$K = K_0 \subseteq K_1 = K(\alpha_1) \subseteq K_2 = K(\alpha_1)(\alpha_2) = K(\alpha_1, \alpha_2)$$
$$\subseteq \dots \dots \subseteq K_n = E = K(\alpha_1, \dots, \alpha_m)$$

Ad ogni passo ho aggiunto un solo elemento.

Sia $d_i = [K_i : K_{i-1}]$ $\quad i = 1, \dots, m.$

Allora:
- $\varphi|_K = Id.$ si "estende" in d_1 modi a K_1
- ogni omomorfismo $\psi : K_1 \to \Omega$

si "estende" in d_2 modi a K_2

...

- ogni omomorfismo $\lambda: K_{m-1} \to \Omega$ si "estende" in d_m modi a $K_m = E$

TOTALE: $d = d_2 \cdots d_m = [E:K]$ modi.

"TANTE ESTENSIONI QUANTO È IL GRADO"
(sottintendo che i pol irr. abbiano radici distinte)
fatto garantito nel caso $\mathrm{char}\, K = 0$
oppure K camp. finito).

ESEMPI

$K = \mathbb{Q} \qquad \Omega = \mathbb{C}$

① $E = \mathbb{Q}(\sqrt{2})$ $\qquad \varphi: E \to \mathbb{C}$, $\varphi|_{\mathbb{Q}} = id$.

$\sqrt{2} \mapsto \pm\sqrt{2}$

pol min è $X^2 - 2$

② $E = \mathbb{Q}(\sqrt[3]{2})$ ...

pol. min $= X^3 - 2$

$\sqrt[3]{2} \mapsto \begin{cases} \sqrt[3]{2} \\ \sqrt[3]{2}\,\zeta_3 \\ \sqrt[3]{2}\,\zeta_3^2 \end{cases}$ 3 omo.

③ $E = \mathbb{Q}(\zeta_p)$ $\quad p$ primo

pol min. $= \dfrac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1$

Le sue radici sono:

$$\zeta_p, \zeta_p^2, \dots, \zeta_p^{p-1}$$

sono: $\zeta_p \mapsto \zeta_p^i \quad 0 < i < p$.

In (1) ogni omomorfismo ha la proprietà
$\varphi(E) = E$

$$a + b\sqrt{2} \mapsto a \pm b\sqrt{2} \in \mathbb{Q}(\sqrt{2}) = E$$

$\subseteq \Rightarrow =$

(spazi vettoriali della stessa dimensione)

In (2) no $\quad \exists$ è un omomorfismo che manda $\mathbb{Q}(\sqrt[3]{2})$ in $\mathbb{Q}(\sqrt[3]{2}\zeta_3)$

$\cap$ $\quad$ $\cap$

$\mathbb{R}$ $\quad$ ~~$\mathbb{R}$~~

In (3) di nuovo sì

$$\zeta_p \mapsto \zeta_p^i \in \mathbb{Q}(\zeta_p)$$

$\subseteq \Rightarrow =$.

Def. Notazioni come sopra. Un'estensione finita E/k si dice NORMALE se per ogni omomorfismo $\varphi : E \to \Omega$ con $\varphi|_k = id$ si ha $\varphi(E) \subseteq E$ $(\varphi(E) = E)$.

Proprietà delle estensioni normali

(1) E_1/k normale, E_2/k normale $\Rightarrow$
E_1E_2/k normale, $E_1 \cap E_2/k$ normale

Dim. Se $\forall \varphi \quad \varphi(E_1) \subseteq E_1, \quad \varphi(E_2) \subseteq E_2$

si ha $\varphi(E_1E_2) \subseteq E_1E_2$ e $\varphi(E_1 \cap E_2) \subseteq E_1 \cap E_2$
(basta vederlo i generatori)

② Torri $K \subseteq E \subseteq F$

E' vero che E/K normale + F/E normale $\Leftrightarrow$ F/K normale ?

NO F/K normale $\Rightarrow$ F/E normale VERO

Ip. tesi: $\forall \varphi : F \to \Omega$ t.c. $\varphi|_K = id$ si ha $\varphi(F) \subseteq F$

Tesi: $\forall \varphi : F \to \Omega$ t.c $\varphi|_E = id$. si ha $\varphi(F) \subseteq F$

$\varphi|_E = id \Rightarrow \varphi|_K = id$.

F/K normale $\Rightarrow E/K$ normale FALSO

Esempio $K = \mathbb{Q}$ $E = \mathbb{Q}(\sqrt[3]{2})$ $F = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$

E/K non normale (visto prima)

normale basta vedere le immag. nei generatori

$\sqrt[3]{2} \mapsto \sqrt[3]{2}\zeta_3^i$ $\zeta_3 \mapsto \zeta_3^j$ $\in F$.

cds di $X^3 - 2$

E/K normale + F/E normale $\Rightarrow F/K$ normale FALSO.

Oss Ogni estensione di grado 2 è normale

$[B : A] = 2$ $B = A(\alpha)$

α radice di un pol di 2° grado $\in A[X]$.

Se α' è l'altra radice allora $\alpha + \alpha' \in A$

$\alpha\alpha' \in A$ $\quad$ $\alpha' \in A(\alpha) = B$

$\alpha \mapsto \begin{cases} \alpha \\ \alpha' \end{cases}$ $\quad$ In ogni caso l'immagine appartiene a $B = A(\alpha)$.

Esempio $\quad K = \mathbb{Q} \quad E = \mathbb{Q}(\sqrt{2}) \quad F = \mathbb{Q}(\sqrt[4]{2})$

$\deg = 1$

pol min. $= X^4 - 2$

radici $\quad \pm\sqrt[4]{2}, \pm\sqrt[4]{2}\, i$

$\Rightarrow$ esiste un omomorfismo

$$\varphi : \mathbb{Q}(\sqrt[4]{2}) \longrightarrow \mathbb{Q}(\sqrt[4]{2}\, i)$$

$\cap$ $\quad$ $\cap$

$\mathbb{R}$ $\quad$ $\mathbb{R}$

NON NORMALE.

Prop. 1 $\quad$ Se $f(x) \in K[x]$ e E è il campo di spezzamento di $f(x)$, allora E/K è un'estensione normale

(Ogni campo di spezzamento è un'estensione normale)

Dim $\quad$ Siano $\alpha_1, \dots, \alpha_n$ le radici di $f(x)$ (che generano E).

Per ogni omomorfismo $\varphi : E \to \Omega$ tale che $\varphi|_K = \mathrm{id}$

$\varphi(\alpha_i) = \alpha_j$ "altra radice di $f(x)$"

$\varphi(E) \subseteq E$

Prop. 2 $\quad$ Se E/K è normale, allora E è il campo di spezzamento di un polinomio $f(x) \in K[x]$

Dim. Supponiamo che $E = K(\alpha_1, \dots, \alpha_m)$ con $f_i(X) = \mu_{\alpha_i}(X)$ (f_i i min.)

Radici di f_1 : $\alpha_1 = \alpha_1^{(1)}, \alpha_1^{(2)}, \dots, \alpha_1^{(d_1)}$

Radici di f_m : $\alpha_m = \alpha_m^{(1)}, \alpha_m^{(2)}, \dots, \alpha_m^{(d_m)}$

Siccome E/K è normale, tutti gli $\alpha_i^{(j)}$ appartengono ad E. (α_i può essere mandato in ogni indice di $f_i(X)$ e questo indice deve appartenere ad E, perché E/K è normale

Ho anche $E = K(\alpha_i^{(j)})$
e quindi E/K è il camp. di spezzamento di $f = f_1 \cdot f_2 \cdots f_m$

Supponiamo E/K normale
($\forall \varphi : E \to \Omega \quad \varphi(E) \subseteq E$)

Conseguenza: Se $\varphi, \psi : E \to \Omega$ sono due omomorfismi (con $\varphi|_K = \psi|_K = id$) allora li posso COMPORRE.
($A \xrightarrow{f} B \xrightarrow{g} C$)

Teo. Gli omomorfismi $\varphi : E \to K$ formano un GRUPPO, detto gruppo di GALOIS dell'estensione ($Gal(E/K)$)

Negli esempi precedenti: $(K = \mathbb{Q})$

(1) $E = \mathbb{Q}(\sqrt{2})$: $\mathrm{Gal}(E/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$.

(2) E = c.d.s. di $X^3 - 2$ $\quad [E:\mathbb{Q}] = 6$

$\mathrm{Gal}(E/\mathbb{Q}) \cong S_3$ (v. dopo)

(3) $E = \mathbb{Q}(\zeta_p)$, $\mathrm{Gal}(E/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^*$

$\bar{i} \in (\mathbb{Z}/p\mathbb{Z})^* \leftrightarrow \zeta_p \mapsto \zeta_p^i$

Prop. Sia $f(X) \in K[X]$ un polinomio di grado n e sia E il c.d.s. di $f(X)$.
Allora $\mathrm{Gal}(E/K) < S_n$.

Dim. $E = K(\alpha_1, \dots, \alpha_n)$ $(\alpha_i =$ radici del polinomio, eventualmente ripetute)
In ogni caso $\varphi : E \to \Omega$ deve permutare le radici. Siano $\alpha_1, \dots, \alpha_k$ $(k \le n)$ le radici distinte.
Ogni φ deve permutare $\alpha_1, \dots, \alpha_k$

$\varphi|_{\{\alpha_1,\dots,\alpha_k\}} \in S_k$

$\varphi \xrightarrow{f} \varphi|_{\{\alpha_1,\dots,\alpha_k\}}$

$\mathrm{Gal}(E/K) \xrightarrow{f} S_k$

f è un omomorfismo INIETTIVO.
(Siccome $\alpha_1, \dots, \alpha_k$ generano E, una funzione che è l'identità su $\alpha_1, \dots, \alpha_k$ è l'identità ovunque).

Quando $Gal(E/K) \leq S_k \leq S_n$. (Es. 2)

Esempio con polinomi di grado 3.

f riducibile (si spezza come prodotto di polinomi di grado $2+1$, $1+1+1$)

ci riconduciamo ai casi di grado 1 e 2

f irriducibile Radici α, β, γ.

E = c.d.r. di f

$$K \subseteq K(\alpha) \subseteq K(\alpha,\beta) \subseteq K(\alpha,\beta,\gamma)$$

grado 3

divisore di $3! = 6$

$$3 \mid [E:K] \mid 6$$

$$\mathbb{Z}/3\mathbb{Z} \cong A_3 \leq Gal(E/K) \leq S_3$$

Caso $f(X) \in \mathbb{Q}[X]$

$f(X) = X^3 - a$ (supp. irriducibile)

$\mathbb{Q}(\sqrt[3]{a})$ è reale e ha grado 3.

c.d.s non è reale

$\Rightarrow Gal(E/\mathbb{Q}) \cong S_3$

$f(X) = X^3 + X + 1$

$f'(X) = 3X^2 + 1$ ha soluzioni positive

$\Rightarrow$ come funzione della variabile reale x è CRESCENTE.

$\Rightarrow$ 1 radice reale + 2 complesse coniugate

$\Rightarrow$ $\mathrm{Gal}(E/\mathbb{Q}) \cong S_3$.

Esercizio Se $\alpha = \zeta_7 + \zeta_7^{-1}$
$\mathbb{Q}(\alpha)/\mathbb{Q}$ è normale e il gruppo di Galois è isomorfo a $\mathbb{Z}/3\mathbb{Z}$.