ALGEBRA 1 - 11 DIC 2018

Note Title 12/11/2018

Nota preliminare Tutte le estensioni algebriche F/K che consideriamo sono separabili (i polinomi minimi su K degli elementi $\alpha \in F$ hanno radici distinte).

Teorema dell'elemento primitivo

Sia F/K un'estensione finita.
Allora esiste un elemento $\gamma \in F$ tale che $F = K(\gamma)$.
(Ogni estensione finita separabile è semplice).

Dim. 1° caso: K infinito.
Certamente $F = K(\alpha_1, \alpha_2, \dots, \alpha_m)$.
Osserviamo che è sufficiente dimostrare che un'estensione del tipo $K(\alpha, \beta)$ si può scrivere nella forma $K(\gamma)$.
(Sostituisco α_1, α_2 con β_2; β_2, α_3 con β_3 ... fino ad arrivare ad un solo elemento).

Supponiamo $[K(\alpha,\beta) : K] = n$
Cerco γ della forma $\gamma = \alpha + c\beta$ con $\in K$
$\gamma \in K(\alpha, \beta)$. Per avere $K(\alpha,\beta) = K(\gamma)$ basta vedere che γ ha grado n su K.

Ci sono n omomorfismi distinti $\sigma_1, \dots, \sigma_n$.
(che lasciano fisso K)

$$\varphi_i : K(\alpha, \beta) \to \overline{K} \quad (\Omega)$$

Non coincidono sia su α che su β.

Allora i polinomi $\sigma_i(\alpha) + X\sigma_i(\beta)$ sono distinti.

Se $f(X) = \prod_{i<j} \left(\sigma_i(\alpha) + X\sigma_i(\beta) - \sigma_j(\alpha) - X\sigma_j(\beta)\right)$

allora $f(X) \not\equiv 0$.

$\exists c \in K$ che non è una radice $f(c) \neq 0$.

$X \to c$ $\quad \sigma_i(\alpha) + c\sigma_i(\beta) = \sigma_i(\alpha + c\beta)$

sono tutti distinti.

$K(\alpha + c\beta)$ ha n omomorfismi distinti.

$[K(\alpha + c\beta) : K] \geq n$

(di fatto $= n$).

Con questo c, $\gamma = \alpha + c\beta$ è l'elemento cercato.

2° caso K finito. $\quad K = \mathbb{F}_{p^a} \quad F = \mathbb{F}_{p^?}$

(a|b)

F^* è ciclico $= \langle \gamma \rangle \qquad F = K(\gamma)$.

Lemma 1 F/K algebrica

Se $\exists n \geq 1$ tale che $\forall \alpha \in F$ si ha $[K(\alpha) : K] \leq n$,

allora $[F : K] \leq n$.

Dim Sia $\alpha \in F$ tale che $[K(\alpha) : K] = m \leq n$ con m massimale. Allora $F = K(\alpha)$. Infatti, se $\exists \beta \in F$ $\beta \notin K(\alpha)$, il campo $K(\alpha, \beta)$ contiene strettamente $K(\alpha)$

Teo. el. prim. $\Rightarrow K(\alpha, \beta) = K(\gamma)$

$[K(\gamma):K] > m$ assurdo .

$\otimes$ K è un campo .

Lemma 2 (lemma di Artin)

F campo , G un gruppo finito di automorfismi di F ($|G| = n$). Sia $K^{\otimes} = \text{Fix}\, G = F^G$ l'insieme dei punti fissi di G, cioè $\{x \in F \mid \sigma(x) = x \ \forall \sigma \in G\}$.

Allora :

- F/K è un'estensione di Galois (normale + sep.)
- $[F:K] = n = |G|$
- $G = \text{Gal}(F/K)$.

Dim. $G = \{\sigma_1, \sigma_2, \dots, \sigma_n\}$.

Sia $\alpha \in F$. Considero solo $\sigma_1, \dots, \sigma_m$ (con $m \leq n$) dove $\sigma_1(\alpha), \dots, \sigma_m(\alpha)$ sono distinti (ed m è massimo possibile)

Considero il polinomio

$$f(X) = \prod_{i=1}^{m} (X - \sigma_i(\alpha))$$

Se $\tau \in G$, allora $\{\tau\sigma_1(\alpha), \dots, \tau\sigma_m(\alpha)\}$ è una permutazione di $\{\sigma_1(\alpha), \dots, \sigma_m(\alpha)\}$.

$$f(X) = X^m + c_{m-1}X^{m-1} + \dots + c_0$$

$$\tau f(X) = X^m + \tau(c_{m-1})X^{m-1} + \dots + \tau(c_0)$$

$$= \prod_{i=1}^{m} (X - \tau\sigma_i(\alpha)) = \prod_{i=1}^{m} (X - \sigma_i(\alpha))$$

$$= f(X)$$

$\tau(c_i) = c_i \ \forall i$.

I coefficienti di $f(X)$ sono lasciati fissi da tutto G, e quindi appartengono a $K = \mathrm{Fix}(G)$.

$$f(x) \in K[x]$$

α è radice di un polinomio $\in K[x]$ di grado $m \leq n$

Lemma 1 $\Longrightarrow$ $[F:K] \leq n$.

F/K normale? sì (τ manda α in qualche $\sigma_i(\alpha) \in F$; $\tau(F) \subseteq F$)

Quindi c'è $\mathrm{Gal}(F/K)$

Ma $\sigma_1, \dots, \sigma_n \in \mathrm{Gal}(F/K)$

$$G \leq \mathrm{Gal}(F/K).$$

$$n = |G| \leq |\mathrm{Gal}(F/K)| = [F:K] \leq n.$$

e quindi ho uguaglianza dappertutto.

CORRISPONDENZA DI GALOIS

IPOTESI: F/K finita di Galois con $G = \mathrm{Gal}(F/K)$

Campi intermedi di F/K Sottogruppi H di G

$\alpha(E) = \mathrm{Gal}(F/E) = H$

$\beta(H) = \mathrm{Fix}(H) = F^H$ (è un'estensione intermedia)

Teorema (Corrispondenza di Galois) Le funzioni α e β definiscono una corrispondenza biunivoca fra le estensioni intermedie e i sottogruppi di G.

Oss Esistono un n° finito di estensioni intermedie.

Dim Facciamo vedere che $\beta\circ\alpha = id$ e $\alpha\circ\beta = id$

$\boxed{\beta\circ\alpha}$ $E \xrightarrow{\alpha} H = Gal(F/E) \xrightarrow{\beta} Fix\, H$

$(\overset{?}{=} E)$

$\beta\circ\alpha(E) \supseteq E$ ovvio per definizione

Viceversa, sia $|H| = h$. Allora H è un gruppo di automorfismi di F

Lemma di Artin $\Rightarrow [F : Fix\, H] = h$.

Ma anche $[F:E] = |H| = h$

$E \subseteq Fix\, H$ ed hanno lo stesso grado

$\Longrightarrow$ sono uguali.

(Se $[F:K] = n$ $[F:E] = h$ $[E/K] = \frac{n}{h}$).

$\boxed{\alpha\circ\beta}$ $H \xrightarrow{\beta} Fix\, H = E \xrightarrow{\alpha} Gal(F/E)$

$(|H| = h)$.

$H \subseteq Gal(F/E)$ ovvio, per definizione

Viceversa, $[F:E] = h$ (Lemma di Artin)

e $|Gal(F/E)| = [F:E] = h$

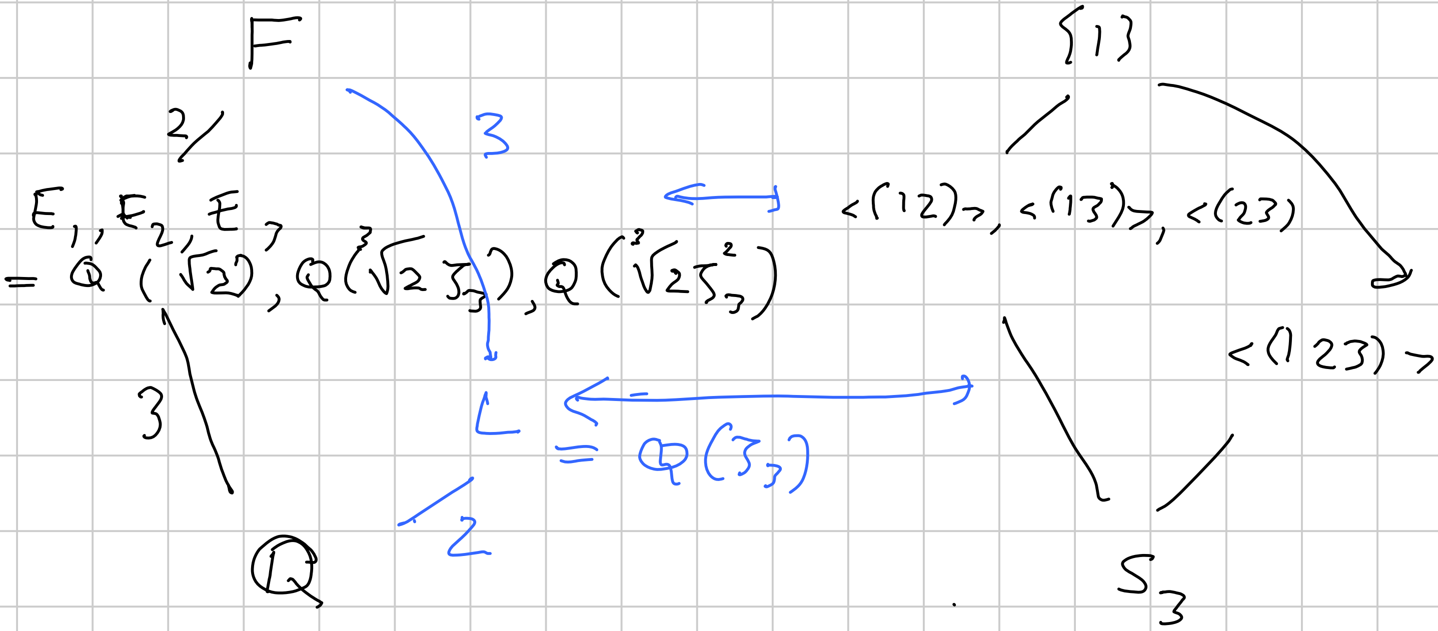
H e $Gal(F/E)$ hanno lo stesso ordine,

$\Longrightarrow$ sono uguali

Esempio $K = \mathbb{Q}$ $F =$ camp. di spezzament di $X^3 - 2$

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

$$\mathrm{Gal}(F/\mathbb{Q}) \cong S_3$$



Supponiamo $E_1 \leftrightarrow H_1$ $E_2 \leftrightarrow H_2$.

$$E_1E_2 \leftrightarrow H_1 \cap H_2$$

$$E_1 \cap E_2 \leftrightarrow <H_1, H_2>$$

$$E \leftrightarrow H$$

Abbiamo inoltre E/K normale $\iff H \lhd G$.

Dim. Sia $\sigma \in G = \mathrm{Gal}(F/K)$

e poniamo $\sigma(E) = E'$

$E \leftrightarrow H$ $E' \leftrightarrow H'$

dove $H' = \sigma H \sigma^{-1}$

Infatti: Se $\tau \in H$ e $x' \in E'$

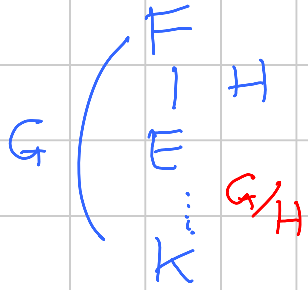
$$\sigma\tau\sigma^{-1}(x') = \sigma\tau(x) \qquad \sigma(x)=x'$$
$$= \sigma(x) = x'$$

e si conclude facilmente.

Conclusione: $\sigma(E)=E$ $\forall\sigma$ e quindi $H'=H$ $\forall\sigma$
cioè $H \triangleleft G$

oppure $\sigma(E)\neq E$ per qualche σ e quindi
$H'\neq H$ " " $H \ntriangleleft G$.

Supponiamo adesso E/K normale
e quindi $H \triangleleft G$



<u>Prop.</u> $Gal(E/K) \cong G/H$

<u>Dim.</u> $G \xrightarrow{\lambda} Gal(E/K)$

$\lambda(\sigma) = \sigma|_E$ (ben definita perché E/K normale)

λ è un omomorfismo surgettivo.
(tutti gli omomorfismi si estendono).

$$\ker\lambda = \{\sigma\in G \mid \sigma|_E = id\} = H = Gal(F/E).$$

GRUPPI DI GALOIS DI ESTENSIONI DI CAMPI FINITI.

Caso $\quad K = \mathbb{F}_p \qquad F = \mathbb{F}_{p^n}$.

La funzione $\phi(x) = x^p$ è un automorfismo di F (che lascia fisso K : Fermat)

$$(x+y)^p = x^p + y^p \qquad (xy)^p = x^p y^p .$$

$\phi \in Gal(\mathbb{F}_{p^n}/\mathbb{F}_p) = G$

ord $\phi = ?$

$\phi^2(x) = x^{p^2} \qquad x \to x^p \to (x^p)^p = x^{p^2}$

$\phi^k(x) = x^{p^k}$.

Quand $\phi^k = id$? $\qquad x^{p^k} = x \quad \forall x$

al più p^k soluzioni

$G = \langle \phi \rangle \qquad \Rightarrow k \geq n$. ($k = n$?)

Caso generale $\quad \mathbb{F}_{p^a} \subseteq \mathbb{F}_{p^b} \qquad b = an$.

Gli elementi del gruppo di Galois devono lasciare fisso $\mathbb{F}_{p^a}$.

$\phi_a(x) = x^{p^a} \qquad x^{p^a} = x \quad \forall x \in \mathbb{F}_{p^a}$

Per ottenere $\phi^k = id$ devo avere

$$x^{p^{ak}} = x \quad \forall x \in \mathbb{F}_{p^b}$$

$$k \geq n .$$

$G = \langle \phi_a \rangle$.