Algebra n. 3 - NOTE ALLA LEZIONE 12

Premessa

Data un'estensione di campi $F \subset K$, e dato un campo intermedio L, separabilità e normalità si trasmettono dalla prima estensione alle due estensioni intermedie come segue:

$$\overbrace{F \subset \underbrace{L \subset K}_{\text{separabile}}}^{\text{separabile}} \qquad \overbrace{\underbrace{F \subset L}_{\text{separabile}} \subset K}^{\text{separabile}}$$

$$\overbrace{F \subset \underbrace{L \subset K}_{\text{normale}}}^{\text{normale}} \qquad \overbrace{\underbrace{F \subset L}_{?} \subset K}^{\text{normale}}$$

Quindi, in sintesi:

$$\overbrace{F \subset \underbrace{L \subset K}_{\text{galoisiana}}}^{\text{galoisiana}} \qquad \overbrace{\underbrace{F \subset L}_{?} \subset K}^{\text{galoisiana}}$$

Teorema 12.2

L'enunciato si può riassumere nel seguente schema, che mette in evidenza il doppio passaggio dall'ambito dei **campi intermedi di un'estensione galoisiana** $F \subset K$ all'ambito dei **sottogruppi del relativo gruppo di Galois** $G(K,F)$ e viceversa.

Campi intermedi Sottogruppi

$$\begin{tikzcd}
L \arrow[r, "\varphi"] \arrow[d, equal] & G(K,L) \arrow[dl, "\psi"] \\
K_{G(K,L)} &
\end{tikzcd}$$

Campi intermedi Sottogruppi

$$\begin{tikzcd}
K_H \arrow[dr, "\varphi"'] & H \arrow[l, "\psi"'] \arrow[d, equal] \\
& G(K,K_H)
\end{tikzcd}$$

Entrambi i passaggi si concludono con il ritorno al punto di partenza.

Dimostrazione del **Teorema 12.2**:

Le colonne della matrice

$$\begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_{n+1}) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_{n+1}) \\ \vdots & \vdots & \vdots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_{n+1}) \end{pmatrix}$$

sono $n+1$ elementi del *K*-spazio vettoriale K^n, e quindi sono linearmente dipendenti su *K*. Pertanto esistono coefficienti $c_1,...,c_n \in K$ non tutti nulli tali che

$$\sum_{i=1}^{n+1} c_i \begin{pmatrix} \sigma_1(\alpha_i) \\ \sigma_2(\alpha_i) \\ \vdots \\ \sigma_n(\alpha_i) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

ossia tali da dare luogo al seguente sistema di uguaglianze indicizzato su $j = 1,...,n$ (indici delle righe):

$$\sum_{i=1}^{n+1} c_i \sigma_j(\alpha_i) = 0.$$

Se *k* è la più piccola cardinalità degli insiemi di colonne linearmente dipendenti, si può supporre, a meno di riordinare le colonne, che sia riferita all'insieme delle prime *k* colonne. In tal caso si ha un sistema di uguaglianze del tipo precedente ove le somme, però, vengono effettuate sugli indici *i* compresi fra 1 e *k*:

$$\sum_{i=1}^{k} c_i \sigma_j(\alpha_i) = 0.$$

Ora, applicando a ciascuna di queste uguaglianze l'elemento τ di *H*, in virtù della conservazione della somma e del prodotto, si ottiene il seguente sistema:

$$\sum_{i=1}^{k} \tau(c_i)\tau\sigma_j(\alpha_i) = 0, \qquad (j = 1,...,n).$$

Si osservi che, al variare di *j*, l'elemento $\tau\sigma_j$ varia in tutto *H*. Dunque il sistema può essere riscritto nella forma seguente, nella quale cambia solo l'ordine delle uguaglianze:

$$\sum_{i=1}^{k} \tau(c_i)\sigma_j(\alpha_i) = 0, \qquad (j = 1,...,n).$$

Dimostrazione del **Teorema 12.5**:

Poiché K è un'estensione normale di F, ed L è un campo intermedio fra F e K, K è anche un'estensione normale di L. Pertanto è il campo di spezzamento su L di un certo polinomio. In virtù del Teorema 4.4, ogni (F-)automorfismo di L si estende dunque ad un (F-)automorfismo di K. In altri termini: ogni elemento di $G(L,F)$ si può ottenere mediante la restrizione ad L di un opportuno elemento di $G(K,F)$. Ciò spiega la surgettività di $\gamma_{G(K,L)}$.

Esempio 12.6

a) Il campo $\mathbb{Q}(\sqrt{2},\sqrt{3})$ è l'insieme delle combinazioni lineari razionali di $1,\sqrt{2},\sqrt{3},\sqrt{6}$. Consideriamo le loro immagini rispetto ad ognuno degli automorfismi elencati. Nel determinarle, teniamo conto dell'azione delle corrispondenti permutazioni sulle radici $\sqrt{2},-\sqrt{2},\sqrt{3},-\sqrt{3}$, e della conservazione del prodotto:

	1	$\sqrt{2}$	$\sqrt{3}$	$\sqrt{6}$
$\varphi_{(12)}$	1	$-\sqrt{2}$	$\sqrt{3}$	$-\sqrt{6}$
$\varphi_{(34)}$	1	$\sqrt{2}$	$-\sqrt{3}$	$-\sqrt{6}$
$\varphi_{(12)(34)}$	1	$-\sqrt{2}$	$-\sqrt{3}$	$\sqrt{6}$

Ad essere lasciate fisse sono le combinazioni lineari in cui i coefficienti degli elementi della base che vengono "mossi" sono nulli. Così, ad esempio, per $H_2=\{\mathrm{id},\phi_{(12)}\}$,

$$K_{H_2}=\left\{a+b\sqrt{3}\,\middle|\,a,b\in\mathbb{Q}\right\}=\mathbb{Q}(\sqrt{3}).$$

b) Diamo un esempio di procedimento per la determinazione degli elementi di una delle righe della tabella.

σ	1	ω	$\sqrt[3]{2}$	$\omega\sqrt[3]{2}$	$\sqrt[3]{4}$	$\omega\sqrt[3]{4}$
id	1	ω	$\sqrt[3]{2}$	$\omega\sqrt[3]{2}$	$\sqrt[3]{4}$	$\omega\sqrt[3]{4}$
(12)	1	$-1-\omega$	$\omega\sqrt[3]{2}$	$\sqrt[3]{2}$	$(-1-\omega)\sqrt[3]{4}$	$\omega\sqrt[3]{4}$
(13)	1	$-1-\omega$	$(-1-\omega)\sqrt[3]{2}$	$\omega\sqrt[3]{2}$	$\omega\sqrt[3]{4}$	$\sqrt[3]{4}$
[illegible]	1	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

La permutazione (12) scambia tra loro le radici $\sqrt[3]{2}$ e $\omega\sqrt[3]{2}$. Possiamo così compilare subito due delle caselle. Per le restanti basta, anzitutto, ricordare che $\omega^{-1}=\omega^2=-1-\omega$, e quindi applicare la conservazione del prodotto da parte di $\varphi_{(12)}$:

$$\sqrt[3]{4}=(\sqrt[3]{2})^2\mapsto(\omega\sqrt[3]{2})^2=(-1-\omega)\sqrt[3]{4}$$

$$\omega=\frac{\omega\sqrt[3]{2}}{\sqrt[3]{2}}\mapsto\frac{\sqrt[3]{2}}{\omega\sqrt[3]{2}}=\omega^{-1}=\omega^2=-1-\omega$$

$$\omega\sqrt[3]{4}\mapsto=\omega^4\sqrt[3]{4}=\omega\sqrt[3]{4}$$

Veniamo ora al campo fissato da H_2. Evidentemente $K_{H_2} \supset \mathbb{Q}(\omega\sqrt[3]{4})$. Proviamo l'uguaglianza. Poniamo $K = \mathbb{Q}(\omega, \sqrt[3]{2})$. Da un lato, per il teorema di moltiplicazione dei gradi per le estensioni finite successive, si ha:

$$[K : \mathbb{Q}(\omega\sqrt[3]{4})] = \frac{[K : \mathbb{Q}]}{[\mathbb{Q}(\omega\sqrt[3]{4}) : \mathbb{Q}]} = \frac{6}{3} = 2$$

Dall'altro, si ha anche

$$[K : \mathbb{Q}(\omega\sqrt[3]{4})] = [K : K_{H_2}][K_{H_2} : \mathbb{Q}(\omega\sqrt[3]{4})],$$

ove, per il Teorema Fondamentale della Teoria di Galois, applicato all'estensione galoisiana $\mathbb{Q} \subset K$,

$$[K : K_{H_2}] = \left|G(K, K_{H_2})\right| = |H_2| = 2.$$

Ne consegue che $[K_{H_2} : \mathbb{Q}(\omega\sqrt[3]{4})] = 1$, da cui l'uguaglianza voluta.

Infine: passando in rassegna l'elenco dei campi intermedi trovati, potrebbe, a prima vista, stupire l'assenza del campo $\mathbb{Q}(\sqrt[3]{4})$. In realtà questo coincide con $\mathbb{Q}(\sqrt[3]{2})$, presente nella lista. Infatti:

$\mathbb{Q}(\sqrt[3]{4}) \subset \mathbb{Q}(\sqrt[3]{2})$, e, d'altra parte, vale l'inclusione opposta, poiché $\sqrt[3]{2} = \frac{1}{2}(\sqrt[3]{4})^2$.