Lezione 12

Prerequisiti: Lezioni 5, 10, 11.

Teorema Fondamentale della Teoria di Galois.

Osservazione 12.1 Sia F un campo, e sia K una sua estensione. Allora è facile vedere che

a) per ogni campo intermedio L tra F e K, $G(K,L)$ è un sottogruppo di $G(K,F)$;
b) per ogni sottogruppo H di $G(K,F)$, $F \subset K_H \subset K$;
c) più in generale, dati due sottogruppi $H,\ H'$ di $G(K,F)$, con $H \subset H'$, allora $K_{H'} \subset K_H$.

Fatta questa premessa, possiamo dare il seguente enunciato:

Teorema 12.2 Sia K un'estensione galoisiana del campo F, e sia $G = G(K,F)$. Allora

a) per ogni campo intermedio L tra F e K, si ha $K_{G(K,L)} = L$;
b) per ogni sottogruppo H di G, si ha $G(K,K_H) = H$;

Inoltre, un sottogruppo H di G è normale se e solo se K_H è un'estensione normale di F. Equivalentemente, un campo intermedio L tra F e K è un'estensione normale di F se e solo se $G(K,L) \lhd G(K,F)$.

Nota L'ultima parte dell'enunciato giustifica il termine "normale" attribuito alle estensioni di campo considerate.

Si osservi che le condizioni a) e b) si possono parafrasare come segue. Considerati gli insiemi

$$\mathsf{L} = \{L \text{ campo} \mid F \subset L \subset K\}$$

$$\mathsf{H} = \{H \text{ sottogruppo di } G\}$$

le applicazioni

$$\begin{aligned} \varphi : \mathsf{L} &\to \mathsf{H} \\ L &\mapsto G(K,L) \end{aligned}$$

e

$$\begin{aligned} \psi : \mathsf{H} &\to \mathsf{L} \\ H &\mapsto K_H \end{aligned}$$

sono una l'inversa dell'altra.

Dimostrazione: Sia L un campo intermedio tra F e K. Allora, in virtù dell'Osservazione 11.9, K è un'estensione galoisiana di L. La parte a) dell'enunciato segue allora dal Teorema 11.7 (a) $\Rightarrow$ c)).

Sia $H < G(K,F)$. Per provare b), osserviamo preliminarmente che $H < G(K,K_H)$: è facile verificarlo, dal momento che ogni *F*-automorfismo di *K* appartenente ad *H*, naturalmente, per definizione di campo fisso, fissa gli elementi di K_H . Inoltre, per il Teorema 11.7, essendo *K* un'estensione galoisiana di K_H, si ha $|G(K,K_H)| = [K:K_H]$. Quindi basta provare che, posto $|H| = n$, $n \geq [K:K_H]$. Sia $H = \{\sigma_1,...,\sigma_n\}$. Supponiamo per assurdo che $n < [K:K_H]$. Esistono allora *n* + 1 elementi $\alpha_1,...,\alpha_{n+1}$ di *K* linearmente indipendenti su K_H. Consideriamo la matrice seguente, a *n* righe ed *n* + 1 colonne e coefficienti in *K*:

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

Le sue colonne, naturalmente, sono linearmente dipendenti su *K*. Sia *k* il minimo numero intero positivo tale che, a meno di permutazioni, le prime *k* colonne di questa matrice sono linearmente dipendenti. Allora esistono coefficienti $c_1,...,c_k \in K$ non tutti nulli tali che

$$\sum_{i=1}^{k} c_i \sigma_j(\alpha_i) = 0 \quad \text{per ogni } j = 1,...,n. \tag{1}$$

Data la minimalità di *k*, $c_i \neq 0$ per ogni $i = 1,...,k$. Quindi, a meno di moltiplicazione per c_1^{-1}, possiamo supporre che sia $c_1 = 1$. Sia $\tau \in H$. Allora $H = \{\tau\sigma_1,...,\tau\sigma_n\}$, quindi, applicando τ su entrambi i membri di (1) si ottiene

$$\sum_{i=1}^{k} \tau(c_i)\sigma_j(\alpha_i) = 0 \quad \text{per ogni } j = 1,...,n. \tag{2}$$

Sottraendo (2) da (1) si ricava

$$\sum_{i=2}^{k} (c_i - \tau(c_i))\sigma_j(\alpha_i) = 0 \quad \text{per ogni } j = 1,...,n. \tag{3}$$

Per minimalità si deduce che $c_i - \tau(c_i) = 0$ per ogni $i = 1,...,k$. Data l'arbitrarietà di $\tau \in H$, segue che $c_i \in K_H$ per ogni $i = 1,...,k$. Ma allora la (1) si può riscrivere nella forma

$$\sigma_j\left(\sum_{i=1}^{k} c_i\alpha_i\right) = 0 \quad \text{per ogni } j = 1,...,n.$$

Poiché i σ_j sono automorfismi, segue che

$$\sum_{i=1}^{k} c_i\alpha_i = 0,$$

che contraddice la supposta lineare indipendenza di $\alpha_1,...,\alpha_{n+1}$ su K_H. Ciò completa la dimostrazione di b).
Proviamo ora l'ultima parte dell'enunciato.
Supponiamo dapprima che $H \lhd G(K,F)$. Sia $\alpha \in K_H$, e sia β una sua radice coniugata su *F*. Per la forma forte del Teorema di estensione degli isomorfismi (Teorema 4.6) esiste $\varphi \in G(K,F)$ tale che $\varphi(\alpha) = \beta$. Per ogni $\tau \in H$ si ha $\tau(\beta) = \varphi\varphi^{-1}\tau\varphi(\alpha)$. In virtù della normalità di *H*, si ha $\varphi^{-1}\tau\varphi \in H$, quindi $\varphi^{-1}\tau\varphi(\alpha) = \alpha$. Pertanto, $\tau(\beta) = \varphi(\alpha) = \beta$, cioè, data l'arbitrarietà di τ, $\beta \in K_H$. Dunque K_H è un'estensione normale di *F*.
Viceversa, supponiamo che K_H sia un'estensione normale di *F*; segue che K_H è il campo di spezzamento di un polinomio $f(x) \in F[x]$ in virtù del Teorema 11.4. Sia $\sigma \in G(K,F)$. Allora anche $\sigma(K_H)$ è un campo di spezzamento di $f(x) \in F[x]$ contenuto in *K*. Segue, in base alla Proposizione 4.7, che $\sigma(K_H) = K_H$. Possiamo allora considerare l'applicazione

$$\gamma_H : G(K,F) \to G(K_H,F)$$
$$\sigma \mapsto \sigma_{|K_H}$$

che è, evidentemente, un omomorfismo di gruppi. Si ha, tenendo anche conto di b),

$$\mathrm{Ker}\gamma_H = G(K,K_H) = H .$$

Ciò prova che $H \lhd G(K,F)$. □

Da questo teorema, tenendo conto della sua riformulazione contenuta nella nota, segue subito:

Corollario 12.3 Se *K* è un'estensione galoisiana di *F*, tra *F* e *K* esiste solo un numero finito di campi intermedi.

Osservazione 12.4 In base all'Osservazione 5.8 a), ogni campo intermedio *L* tra *F* e *K* è un'estensione separabile di *F*. Quindi *L* è normale su *F* se e solo se è una sua estensione galoisiana.

Teorema 12.5 Sia *K* un'estensione galoisiana del campo *F*, e sia $G = G(K,F)$. Allora per ogni campo intermedio *L* tra *F* e *K*,

a) $[K:L] = |G(K,L)|$, e $[L:F] = (G(K,F) : G(K,L))$
b) se *L* è un'estensione normale di *F*, allora $G(L,F) \cong G(K,F)/G(K,L)$

Dimostrazione: Essendo, in base all'Osservazione 11.9, *K* un'estensione galoisiana di *L*, allora, in virtù del Teorema 11.7, $[K:L] = |G(K,L)|$, e, inoltre, per il Teorema di Lagrange, e per il teorema di moltiplicazione dei gradi per le estensioni successive,

$$(G(K,F) : G(K,L)) = \frac{|G(K,F)|}{|G(K,L)|} = \frac{[K:F]}{[K:L]} = [L:F] .$$

Ciò prova a). Sapendo che $K_{G(K,L)} = L$, consideriamo ora, come nella dimostrazione del Teorema 12.2, l'omomorfismo di gruppi

$$\gamma_{G(K,L)} : G(K,F) \to G(L,F)$$
$$\sigma \mapsto \sigma_{|L}$$

Si ha $\mathrm{Ker}\gamma_{G(K,L)} = G(K,L)$. Inoltre $\gamma_{G(K,L)}$ è suriettivo in virtù del Teorema 4.4. Quindi, per il Teorema fondamentale di omomorfismo per gruppi, resta indotto un isomorfismo $G(L,F) \cong {G(K,F)}/{G(K,L)}$. Ciò prova b). □

Nota Gli enunciati dei Teorema 12.2 e 12.5 formano il cosiddetto *Teorema fondamentale della Teoria di Galois.*

Esempio 12.6 Il Teorema 12.2 può essere utile per determinare i campi intermedi (normali) tra un campo *F* ed una sua estensione galoisiana *K* tramite i sottogruppi (normali) del gruppo di Galois di *K* su *F*. Riprendiamo l'Esempio 11.11.

a) Sia $F = \mathbf{Q}$, $K = \mathbf{Q}(\sqrt{2},\sqrt{3})$. Allora $G(K,F) \cong \{\mathrm{id},(12),(34),(12)(34)\}$, ove ogni $\varphi \in G(K,F)$ è associato alla permutazione che induce sulle radici $\sqrt{2},-\sqrt{2},\sqrt{3},-\sqrt{3},$ prese in quest'ordine. Quindi i sottogruppi di $G(K,F)$ sono, con i simboli introdotti nella Lezione 10, i seguenti:

$$H_1 = \{\mathrm{id}\}, \quad H_2 = \{\mathrm{id},\varphi_{(12)}\}, \quad H_3 = \{\mathrm{id},\varphi_{(34)}\}, \quad H_4 = \{\mathrm{id},\varphi_{(12)(34)}\}, \quad H_5 = G(K,F)$$

Sapendo che una base di *K* su $\mathbf{Q}$ è formata da $1,\sqrt{2},\sqrt{3},\sqrt{6}$, i relativi campi fissi sono

$$K_{H_1} = \mathbf{Q}(\sqrt{2},\sqrt{3}), \quad K_{H_2} = \mathbf{Q}(\sqrt{3}), \quad K_{H_3} = \mathbf{Q}(\sqrt{2}), \quad K_{H_4} = \mathbf{Q}(\sqrt{6}), \quad K_{H_5} = \mathbf{Q}.$$

Questi sono dunque i campi intermedi tra $\mathbf{Q}$ e $\mathbf{Q}(\sqrt{2},\sqrt{3})$.

b) Sia ora $F = \mathbf{Q}$, $K = \mathbf{Q}(\omega,\sqrt[3]{2})$, dove ω è una radice primitiva cubica dell'unità. Allora $G(K,F) \cong S_3$. La corrispondenza qui è basata sulle permutazioni delle radici $\sqrt[3]{2},\omega\sqrt[3]{2},\omega^2\sqrt[3]{2}$, che possiamo prendere in quest'ordine. I sottogruppi di $G(K,F)$ sono dunque

$$H_1 = \{\mathrm{id}\}, \; H_2 = \{\mathrm{id},\varphi_{(12)}\}, \; H_3 = \{\mathrm{id},\varphi_{(13)}\}, \; H_4 = \{\mathrm{id},\varphi_{(23)}\}, H_5 = \{\mathrm{id},\varphi_{(123)},\varphi_{(132)}\}, \; H_6 = G(K,F)$$

Una base di $\mathbf{Q}(\omega,\sqrt[3]{2})$ su $\mathbf{Q}$ è formata dagli elementi $1,\omega,\sqrt[3]{2},\omega\sqrt[3]{2},\sqrt[3]{4},\omega\sqrt[3]{4}$.
La seguente tabella mostra come vengono trasformati gli elementi della base da ogni automorfismo φ_σ, ossia sottoponendo le radici $\sqrt[3]{2},\omega\sqrt[3]{2},\omega^2\sqrt[3]{2}$ ad ogni permutazione σ:

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	$-1-\omega$	$(-1-\omega)\sqrt[3]{2}$	$\omega\sqrt[3]{2}$	$\omega\sqrt[3]{4}$	$\sqrt[3]{4}$
(23)	1	$-1-\omega$	$\sqrt[3]{2}$	$(-1-\omega)\sqrt[3]{2}$	$\sqrt[3]{4}$	$(-1-\omega)\sqrt[3]{4}$
(123)	1	ω	$\omega\sqrt[3]{2}$	$(-1-\omega)\sqrt[3]{2}$	$(-1-\omega)\sqrt[3]{4}$	$\sqrt[3]{4}$
(132)	1	ω	$(-1-\omega)\sqrt[3]{2}$	$\sqrt[3]{2}$	$\omega\sqrt[3]{4}$	$(-1-\omega)\sqrt[3]{4}$

Quindi i campi intermedi sono:

$$K_{H_1} = \mathbf{Q}(\omega, \sqrt[3]{2}),\ K_{H_2} = \mathbf{Q}(\omega\sqrt[3]{4}),\ K_{H_3} = \mathbf{Q}(\omega\sqrt[3]{2}),\ K_{H_4} = \mathbf{Q}(\sqrt[3]{2}),\ K_{H_5} = \mathbf{Q}(\omega),\ K_{H_6} = \mathbf{Q}.$$

Si noti che tra questi campi, le sole estensioni normali di **Q** sono K_{H_1}, K_{H_5}, K_{H_6}, che corrispondono ai sottogruppi normali di S_3.

Nell'Esempio 12.6 a), invece, tutti campi intermedi trovati sono normali su **Q**. Ciò segue da una proprietà generale, che è immediata conseguenza del Teorema 12.2:

Corollario 12.8 Se $G(K,F)$ è abeliano, allora ogni campo intermedio tra F e K è normale su F.

In base all'Osservazione 11.2 c), due elementi di un'estensione normale K di un campo F sono radici coniugate su F se e solo esiste un elemento del gruppo di Galois di K su F che trasforma uno nell'altro. Conoscendo un elemento α algebrico su F, ed un'estensione normale L di F contenente α, una volta determinato il gruppo $G(L,F)$, si possono così determinare tutte le radici coniugate di α su F, (che sono gli elementi $\varphi(\alpha)$, al variare di φ in $G(L,F)$), e, di conseguenza, si può scrivere il polinomio minimo di α su F.

Esercizio 12.9 Determinare il polinomio minimo di $1+\sqrt[3]{2}$ su **Q**.

Svolgimento: Si ha $\mathbf{Q}(1+\sqrt[3]{2}) = \mathbf{Q}(\sqrt[3]{2})$, che è contenuto in $\mathbf{Q}(\sqrt[3]{2},\omega)$, un'estensione galoisiana di **Q**. Dall'Esempio 11.11 b) sappiamo che $G(\mathbf{Q}(\sqrt[3]{2},\omega),\mathbf{Q}) \cong S_3$, quindi i **Q**-automorfismi di $\mathbf{Q}(\sqrt[3]{2},\omega)$ inducono sulle radici $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$ tutte le possibili permutazioni. Le radici coniugate di $1+\sqrt[3]{2}$ su **Q** sono dunque (oltre a $1+\sqrt[3]{2}$), $\varphi_{(12)}(1+\sqrt[3]{2}) = 1+\omega\sqrt[3]{2}$ e $\varphi_{(13)}(1+\sqrt[3]{2}) = 1+\omega^2\sqrt[3]{2}$. Il polinomio minimo di $1+\sqrt[3]{2}$ su **Q** è quindi

$$f(x) = (x-1-\sqrt[3]{2})(x-1-\omega\sqrt[3]{2})(x-1-\omega^2\sqrt[3]{2}) = x^3 - 3x^2 + 3x - 3.$$

Nota Utilizzando il Teorema Fondamentale della Teoria di Galois, è possibile dimostrare il Teorema Fondamentale dell'Algebra. Una dimostrazione si trova, ad esempio, in [PC], Teorema 7.4.2.