PARTE TERZA
Teoria di Galois

Lezione 10

Prerequisiti: Lezione 4.

Il gruppo di Galois di un'estensione.

Sia F un campo, e sia K una sua estensione.

Definizione 10.1 Si dice *F-automorfismo* di K ogni automorfismo del campo K che lascia fissi gli elementi di F. Il gruppo degli F-automorfismi di K si dice *gruppo di Galois di K su F* e si denota con $G(K,F)$.

Più in generale, chiameremo *F-omomorfismo* ogni omomorfismo di campi tra estensioni di F che lascia fissi gli elementi di F (equivalentemente: ogni omomorfismo di campi che è anche un omomorfismo di F-spazi vettoriali).

Esempio 10.2

a) Calcoliamo $G(\mathbf{Q}(\sqrt{2}),\mathbf{Q})$. Sia φ un $\mathbf{Q}$-automorfismo di $\mathbf{Q}(\sqrt{2})$. Una base di $\mathbf{Q}(\sqrt{2})$ su $\mathbf{Q}$ è $\{1,\sqrt{2}\}$, quindi φ è univocamente determinato da $\varphi(\sqrt{2})$. Inoltre $2=\varphi(2)=(\varphi(\sqrt{2}))^2$, quindi $\varphi(\sqrt{2})=\sqrt{2}$ oppure $\varphi(\sqrt{2})=-\sqrt{2}$. Segue che φ è definito da

$$\varphi(a+b\sqrt{2})=a+b\sqrt{2} \quad (\forall a,b\in\mathbf{Q}) \quad \text{oppure} \quad \varphi(a+b\sqrt{2})=a-b\sqrt{2} \quad (\forall a,b\in\mathbf{Q}).$$

Nel primo caso φ è l'identità. Quindi $G(\mathbf{Q}(\sqrt{2}),\mathbf{Q})$ ha due elementi.

b) Calcoliamo $G(\mathbf{Q}(\sqrt[3]{2}),\mathbf{Q})$. Una base di $\mathbf{Q}(\sqrt[3]{2})$ su $\mathbf{Q}$ è $\{1,\sqrt[3]{2},\sqrt[3]{4}\}$. Sia φ un $\mathbf{Q}$-automorfismo di $\mathbf{Q}(\sqrt[3]{2})$. Esso è univocamente determinato da $\varphi(\sqrt[3]{2})$, che è, necessariamente, una radice cubica di 2, ed inoltre appartiene a $\mathbf{Q}(\sqrt[3]{2})$. Quindi $\varphi(\sqrt[3]{2})=\sqrt[3]{2}$. Ciò prova che $G(\mathbf{Q}(\sqrt[3]{2}),\mathbf{Q})$ è ridotto alla sola identità.

Nell'Esempio 10.2 a) ogni radice del polinomio x^2-2 viene inviata in una radice dello stesso polinomio, in b) avviene l'analogo per le radici del polinomio x^3-2. In generale, come abbiamo già osservato nella Lezione 4, se $f(x)\in F[x]$, e $\alpha_1,...,\alpha_n$ sono le sue radici (a due a due distinte) in una sua estensione, allora, posto $K=F(\alpha_1,...,\alpha_n)$, ogni $\varphi\in G(K,F)$ induce, per restrizione, una permutazione σ su $\{\alpha_1,...,\alpha_n\}$. D'altra parte, ogni permutazione σ siffatta determina univocamente φ. Possiamo scrivere, allora, $\varphi=\varphi_\sigma$, se $\varphi_{|\{\alpha_1,...,\alpha_n\}}=\sigma$.

Corollario 10.3 Sia $f(x)\in F[x]$ un polinomio non nullo di grado n. Sia K un suo campo di spezzamento su F. Allora $G(K,F)$ è isomorfo ad un sottogruppo di S_n.

Osservazione 10.4 Se il polinomio $f(x) \in F[x]$ è irriducibile su F, e K è un suo campo di spezzamento su F, allora il gruppo $G(K,F)$, secondo il Teorema di estensione degli isomorfismi (Corollario 4.5), agisce in maniera transitiva sulle radici di $f(x)$.

Esempio 10.5 $\mathbf{Q}(\sqrt{2})$ è un campo di spezzamento di x^2-2 su $\mathbf{Q}$, in cui esso ha due radici distinte. Come stabilito nell'Esempio 10.2 a), $G(\mathbf{Q}(\sqrt{2}),\mathbf{Q}) \cong S_2$.

In generale, però, l'isomorfismo sussiste con un sottogruppo proprio di S_n, come mostra il prossimo

Esempio 10.6 Sia $f(x)=(x^2-2)(x^2-3)$, il suo campo di spezzamento su $\mathbf{Q}$ è $\mathbf{Q}(\sqrt{2},\sqrt{3})$ (vedi anche Osservazione 4.9) in cui ha quattro radici distinte: $\sqrt{2},-\sqrt{2},\sqrt{3},-\sqrt{3}$. Nessun $\mathbf{Q}$-automorfismo di $\mathbf{Q}(\sqrt{2},\sqrt{3})$ scambia $\sqrt{2}$ e $\sqrt{3}$. Quindi $G(\mathbf{Q}(\sqrt{2},\sqrt{3}),\mathbf{Q})$ è isomorfo ad un sottogruppo proprio di S_4. Lo determineremo più avanti.

Intanto diamo un primo risultato generale sull'ordine di $G(K{:}F)$.

Teorema 10.7 Se K è un'estensione finita di F, allora

$$\left|G(K,F)\right| \le [K:F].$$

Dimostrazione: Sia $n=[K:F]$, e siano $u_1,\ldots, u_n$ gli elementi di una base di K su F. Supponiamo per assurdo che esistano $n+1$ F-automorfismi di K distinti $\sigma_1,..,\sigma_{n+1}$. Il seguente sistema di n equazioni in $n+1$ incognite $x_1,\ldots,x_{n+1}$ a coefficienti in K ha una soluzione non banale $(a_1,\cdots,a_{n+1})$.

$$\begin{cases} \sigma_1(u_1)x_1 + \sigma_2(u_1)x_2 + \cdots + \sigma_{n+1}(u_1)x_{n+1} = 0 \\ \quad\vdots \qquad\qquad \vdots \qquad\quad \vdots \qquad\qquad \vdots \qquad\quad \vdots \\ \sigma_1(u_n)x_1 + \sigma_2(u_n)x_2 + \cdots + \sigma_{n+1}(u_n)x_{n+1} = 0 \end{cases}$$

Ma allora, per ogni $i=1,\ldots,n$,

$$a_1\sigma_1(u_i)+a_2\sigma_2(u_i)+\cdots+a_{n+1}\sigma_{n+1}(u_i)=0,$$

e, quindi, $a_1\sigma_1+a_2\sigma_2+\cdots+a_{n+1}\sigma_{n+1}$ è l'applicazione nulla. Ma ciò contraddice il Lemma di Dedekind (Teorema 6.6). □

Nell'Esempio 10.2 a), la disuguaglianza del Teorema 10.7 è, in realtà, un'uguaglianza. L'Esempio 10.2 b) mostra però che tale disuguaglianza, in generale, è stretta.

È immediato verificare la seguente:

Proposizione 10.8 Sia G un gruppo di automorfismi del campo K. L'insieme degli elementi di K che vengono lasciati fissi da ogni elemento di G è un sottocampo di K. Esso viene detto *campo fisso* di G, ed è denotato K_G.

Osservazione 10.9 Dalla Definizione 10.1 segue, evidentemente,

$$F \subset K_{G(K,F)}.$$

Nell'Esempio 10.2 a) vale l'uguaglianza. In generale, però, l'inclusione è stretta. Il controesempio è fornito, ancora una volta, dall'Esempio 10.2 b): infatti $\mathbf{Q} \neq K_{G(\mathbf{Q}(\sqrt[3]{2},\mathbf{Q})} = \mathbf{Q}(\sqrt[3]{2})$.

Nella prossima lezione capiremo cosa distingua l'estensione $\mathbf{Q}(\sqrt{2})$ dall'estensione $\mathbf{Q}(\sqrt[3]{2})$ di $\mathbf{Q}$.