Lezioni del 15,18,20,22 aprile, III. Registro dettagliato

1 Corrispondenza di Galois

1.1 Estensioni normali.

Nel seguito si considerano solo estensioni finite di sottocampi di $\mathbb{C}$. Verranno messe in relazione la proprieta' che il campo maggiore abbia molti automorfismi che fissano il campo minore con la proprieta' che il campo maggiore sia campo di spezzamento di un polinomio sul campo minore.

Per ciascuna estensione F/K di campi, i $K-$automorfismi di F formano un gruppo rispetto alla composizione.

Per ogni polinomio monico $f(x)$ di grado $n > 0$ a coefficienti in $\mathbb{C}$, si e' detto "campo di spezzamento di $f(x)$" il sottocampo di $\mathbb{C}$ generato dalle radici di $f(x)$; piu' in generale, per ogni sottocampo K di $\mathbb{C}$, si dice "campo di spezzamento di $f(x)$ su K" il sottocampo di $\mathbb{C}$ generato dalle radici di $f(x)$ e da K (cosi' il "campo di spezzamento di $f(x)$" coincide col "campo di spezzamento di $f(x)$ su $\mathbb{Q}$").

Definizione 1. *Un'estensione F/K di campi si dice normale se e solo se gli elementi di F fissati da ogni $K-$automorfismo di F sono solo gli elementi di K.*

Per quanto visto in precedenza, in ciascuna estensione quadratica il campo maggiore possiede esattamente due automorfismi sul campo minore, e l'estensione e' normale; un esempio di un'estensione cubica non normale e' dato da $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Si e' anche visto che in ciascuna estensione quadratica il campo maggiore puo' essere visto come il campo di spezzamento di un polinomio sul campo minore.

Una caratterizzazione ed una proprieta' notevole delle estensioni normali sono date dai seguenti Teoremi, che non dimostriamo

Teorema 1. *Un'estensione F/K e' normale se e solo se F e' il campo di spezzamento di un polinomio su K.*

Teorema 2. *Se un'estensione F/K e' normale, allora ha un numero di $K-$automorfismi uguale al suo grado.*

1.2 Gruppo di Galois di un polinomio.

Siano f un polinomio monico a coefficienti in $\mathbb{C}$ ed F il campo di spezzamento di f. Per ogni campo K contenuto in F e contenente i coefficienti di f, il gruppo dei $K-$automorfismi di F si dice "gruppo di Galois di f su K" e si indica con $\mathcal{G}(F/K)$. Essendo F anche il campo di spezzamento di f su K, per i Teoremi di sopra si ha che l'estensione F/K e' normale, e che l'ordine del gruppo di Galois di f su K e' uguale al grado di F su K :

$$|\mathcal{G}(F/K)| = [F : K].$$

I gruppi di Galois di un polinomio si possono riguardare come gruppi di permutazioni sull'insieme delle radici del polinomio, nel senso specificato della seguente

Proposizione 1. *Sia $\mathcal{G}(F/K)$ il gruppo di Galois di un polinomio f su un campo K, sia A l'insieme delle radici di f, e sia $\mathcal{S}_A$ il gruppo simmetrico sull'insieme A. Allora*

-per ogni $\sigma \in \mathcal{G}(F/K)$, $\sigma(A) = A$;

-l'omomorfismo di restrizione $\mathcal{G}(F/K) \to \mathcal{S}_A$, $\sigma \mapsto \sigma|_A$, e' iniettivo.

Dim. Sia $f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ con $a_i \in \mathbb{C}$, e sia $A = \{\alpha_1, \ldots, \alpha_n\}$ l'insieme delle radici di f in $\mathbb{C}$. Il campo di spezzamento di f e' $F = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, il campo minimo di f e' $K_0 = \mathbb{Q}(a_1, \ldots, a_n)$, e si ha $K_0 \subset K \subset F$.

Sia $\sigma \in \mathcal{G}(F/K)$. Se $\alpha = \alpha_i$ e' una radice di f, cioe' se $\alpha^n + a_1\alpha^{n-1} + \cdots + a_{n-1}\alpha + a_n = 0$, allora applicando σ ed entrambi i membri si ottiene $\sigma(\alpha)^n + a_1\sigma(\alpha)^{n-1} + \cdots + a_{n-1}\sigma(\alpha) + a_n = 0$, cioe' $\sigma(\alpha)$ e' ancora una radice di f. Dunque $\sigma(A) = A$.

Per ogni $\sigma \in \mathcal{G}(F/K)$ e' dunque ben definita la restrizione $\sigma|_A : A \to A$, e l'applicazione $\mathcal{G}(F/K) \to \mathcal{S}_A$, $\sigma \mapsto \sigma|_A$, e' un omomorfismo di gruppi. Se $\sigma|_A = \mathrm{id}_A$ allora σ fissa $\mathbb{Q}$, fissa ogni radice $\alpha_1, \ldots, \alpha_n$ e dunque fissa $\mathbb{Q}(\alpha_1, \ldots, \alpha_n) = F$, cioe' $\sigma = \mathrm{id}_F$. L'omomorfismo di restrizione ad A ha cosi' nucleo ridotto all'unita', e dunque e' iniettivo.

Esempio Consideriamo il polinomio $f(x) = x^3 - 2$, col suo campo di spezzamento $F = \mathbb{Q}(\alpha, \beta, \gamma)$ generato dalle sue tre radici α, β, γ, ed il suo campo dei coefficienti $\mathbb{Q}$.

Per quanto gia' visto su questa estensione, e per i Teoremi del paragrafo precedente, il gruppo di Galois di f su $\mathbb{Q}$ ha ordine $|\mathcal{G}(F/\mathbb{Q})| = [F : \mathbb{Q}] = 6$.

Per il Teorema di sopra, ogni automorfismo del campo F trasforma in se' l'insieme $\{\alpha, \beta, \gamma\}$ delle tre radici di $f(x)$, e l'omomorfismo di restrizione $\mathcal{G}(F/\mathbb{Q}) \to S_{\{\alpha,\beta,\gamma\}}$ e' iniettivo. Essendo $|S_{\{\alpha,\beta,\gamma\}}| = 6$ si ha che l'omomorfismo di restrizione e' un isomorfismo e

$$\mathcal{G}(F/\mathbb{Q}) \simeq S_{\{\alpha,\beta,\gamma\}}.$$

Il gruppo di Galois di f su $\mathbb{Q}(\alpha)$ ha ordine $|\mathcal{G}(F/\mathbb{Q}(\alpha))| = [F : \mathbb{Q}(\alpha)] = 2$. L'omomorfismo di restrizione $\mathcal{G}(F/\mathbb{Q}(\alpha)) \to S_{\{\alpha,\beta,\gamma\}}$ e' iniettivo ed induce un isomorfismo

$$\mathcal{G}(F/\mathbb{Q}(\alpha)) \simeq S_{\{\beta,\gamma\}}.$$

Analogamente per i gruppi di Galois di f su $\mathbb{Q}(\beta)$ e su $\mathbb{Q}(\gamma)$.

1.3 Teorema fondamentale.

La struttura dell'estensione associata ad un polinomio e la struttura del suo gruppo di Galois sono in una corrispondenza naturale, nel senso descritto dal Teorema Fondamentale della teoria di Galois, che enunciamo di seguito senza dimostrazione. Queste corrispondenza mette in relazione i campi contenuti nel campo maggiore e contenenti il campo minore, in breve i "campi intermedi", dell'estensione, con i sottogruppi del gruppo di Galois dell'estensione

Teorema 3. *Siano f un polinomio monico non costante a coefficienti in $\mathbb{C}$, F il campo di spezzamento di f, K un campo contenente il campo dei coefficienti di f. Allora*

(1) per ogni campo L intermedio fra K ed F, l'estensione F/L e' normale; inotre, $|\mathcal{G}(F/L)| = [F : L]$;

(2) l'applicazione $L \mapsto \mathcal{G}(F/L)$ e' una biiezione dall'insieme dei campi intermedi fra K ed F all'insieme dei sottogruppi del gruppo $\mathcal{G}(F/K)$; inoltre, per ogni L_1, L_2 campi intermedi fra K ed F, si ha $L_1 \subseteq L_2$ se e solo e $\mathcal{G}(F/L_1) \supseteq \mathcal{G}(F/L_2)$;

(3) per ogni campo L intermedio fra K ed F, l'estensione L/K e' normale se e solo se $\mathcal{G}(F/L)$ e' un sottogruppo normale di $\mathcal{G}(F/K)$; inoltre, in tal caso si ha $\mathcal{G}(L/K) \simeq \mathcal{G}(F/K)/\mathcal{G}(F/L)$.

Esempio Consideriamo il polinomio $f(x) = x^3 - 2$, col suo campo di spezzamento $F = \mathbb{Q}(\alpha, \beta, \gamma)$ generato dalle sue tre radici α, β, γ, ed il suo campo dei coefficienti $K = \mathbb{Q}$. Abbiamo visto che la restrizione di $K-$automorfismi dal campo F all'inisieme $\{\alpha, \beta, \gamma\}$ delle radici e' un isomorfismo $\mathcal{G}(F/K) \simeq S_{\{\alpha,\beta,\gamma\}}$.

Ora: i sottogruppi propri di $S_{\{\alpha,\beta,\gamma\}}$ sono

- tre sottogruppi di ordine 2, generati rispettivamente dai tre scambi $(\alpha\beta), (\alpha\gamma), (\beta\gamma)$, non normali;

- un sottogruppo di ordine 3, generato da $(\alpha\beta\gamma)$, che e' normale.

Per il Teorema Fondamentale, i campi intermedi propri dell'estensione F/K sono

- tre campi intermedi A, B, C che sono campi minori di tre estensioni normali F/A, F/B, F/C di grado 2, e sono campi maggiori di tre estensioni non normali A/K, B/K, C/K di grado 3;

- un campo intermedio D che e' campo minore di un'estensione normale F/D di grado 3, ed e' campo maggiore di un'estensione normale D/K di grado 2.

Si lascia come esercizio di determinare esplicitamente questi campi intermedi.

1.4 Cenni alla risolubilita' per radicali delle equazioni algebriche

All'origine della Teoria di Galois sta il problema classico della risolubilita' per radicali delle equazioni algebriche, nella forma fine riguardante ciascuna singola equazione. Tramite la corrispondenza di Galois, la proprieta' della risolubilita' per radicali di un'equazione algebrica $p(x) = 0$, espresssa da una proprieta' dell'estensione associata al polinomio $p(x)$, viene provata essere equivalente ad una proprieta' del gruppo di Galois associato al polinomio. Precisamente:

- si dice che l'equazione $p(x) = 0$ e' risolubile per radicali se e solo se ciascuna soluzione dell'equazione e' esprimibile a partire dai coefficienti di $p(x)$ mediante un numero finito di operazioni di addizione, sottrazione, prodotto, quoziente e dell'operazione di scelta di una radice; questa proprieta' si traduce nella seguente proprieta' dell'estensione F/K associata al polinomio $p(x)$: esiste una catena finita di campi $K_0 = K$, $K_1 = K(\alpha_1)$, $K_2 = K_1(\alpha_2)$, ..., $K_m = K_{m-1}(\alpha_m)$ che termina con un campo K_m contenente F, tale che per ciascun $i = 1, 2, \ldots, m$ esiste una potenza di α_i che appartine al campo K_{i-1}.

- si dice che un gruppo G e' risolubile se e solo se esiste una catena finita di sottogruppi $\{u\} = G_0 \subset G_1 \subset G_2 \subset \cdots \subset G_m = G$ tale che per ciascun $i = 1, 2, \ldots, m$ il gruppo G_{i-1} sia normale nel gruppo G_i ed il gruppo quoziente G_i/G_{i-1} sia abeliano.

Il Teorema di Galois afferma che per ciascun polinomio $p(x)$ a coefficienti in $\mathbb{C}$, l'equazione $p(x) = 0$ e' risolubile per radicali se e solo se il gruppo di Galois di $p(x)$ e' risolubile. In particolare:

- dal fatto che il "generico" polinomio di grado n abbia gruppo di Galois uguale al gruppo simmetrico S_n e che il gruppo S_n sia risolubile se e solo se $n \leq 4$, segue l'esistenza di "formule risolutive" delle equazioni algebriche di grado $n \leq 4$ ed il Teorema di Ruffini-Abel sulla non esistenza di "formule risolutive" per le equazioni di grado $n \geq 5$;

- dal fatto che per ogni n esistano dei polinomi di grado n aventi come gruppo di Galois S_n segue che per ogni $n \geq 5$ esistono delle singole equazioni algebriche non risolubili per radicali nemmeno con un metodo "ad hoc".