Teorema

Sia E/K un'estensione finita di grado n e sia $\mathcal{G}(E/K) = \{\sigma_1, \dots, \sigma_n\}$. Allora

1) $E = \sigma_1(E)\,\sigma_2(E) \dots \sigma_n(E)/K$ è di Galois

2) Ogni estensione F/E di Galois su K contiene E'.

3) $\mathrm{Gal}(E'/K)$ è (canonicamente) isomorfo a un sottogruppo transitivo di S_n

(Un sottogruppo H di S_n è transitivo se l'azione di H su $\{1,\dots,n\}$ è transitiva, cioè $\forall i,j \ \exists \sigma \in H$ t.c. $\sigma(i)=j$)

L'estensione E'/K si dice chiusura di Galois di E/K: è la più piccola estensione di Galois di K contenente E.

Dim.

1) Sia $\varphi \in \mathrm{Gal}(E'/K)$. $\forall j$ si ha $\varphi|_{\sigma_j(E)} \in \mathrm{Hom}_K(\sigma_j(E), E')$ e $\varphi \circ \sigma_j \in \mathrm{Gal}(E/K)$

$\varphi(\sigma_j(E)) = \sigma_i(E) \subseteq E'$. ($\varphi \circ \sigma_j = \sigma_i$)

Poiché E' è generato su K dai $\sigma_j(E)$, si ha $\varphi(E') \subseteq E'$

$\Rightarrow E'/K$ è Galois.

2) Sia $E \subseteq F$ e F/K di Galois. $\forall \varphi \in \mathrm{Gal}(F/K)$ si ha $\varphi|_E = \sigma_i$ per qualche i, quindi $\sigma_i(E) \subseteq F$. Segue $E' \subseteq F$.

3) Per ogni $\varphi \in \mathrm{Gal}(E'/K)$ si ha $\varphi \circ \sigma_i = \sigma_j$

Quindi φ induce una funzione $\tilde{\varphi}$ sull'insieme $\{\sigma_1,\dots,\sigma_n\}$

$\tilde{\varphi}$ è biiettiva: se $\tilde{\varphi}(\sigma_i) = \tilde{\varphi}(\sigma_{i'})$ allora $\varphi \circ \sigma_i = \varphi \circ \sigma_{i'}$ ma φ iniettiva $\Rightarrow \sigma_i = \sigma_{i'} \Rightarrow \tilde{\varphi} \in \mathrm{Sym}(\{\sigma_1,\dots,\sigma_n\})$

La corrispondenza

$\varphi \longmapsto \tilde{\varphi}$ è iniettiva:

se $\varphi \circ \sigma_i = \sigma_i$ per ogni i allora φ è l'identità su ogni $\sigma_i(E)$

Quindi c'è un omom iniettivo

$\Phi: Gal\left(\frac{E'}{K}\right) \to Sym\left(\mathcal{I}\left(\frac{E}{K}\right)\right) \simeq S_n$

Dati $\sigma_i, \sigma_j \in \mathcal{I}\left(\frac{E}{K}\right)$, essi si estendono a $\varphi_i, \varphi_j \in Gal\left(\frac{E'}{K}\right)$

e $\varphi_j \circ \varphi_i^{-1} \circ \sigma_i = \sigma_j$ ma l'immagine di Ω è un sgp transitivo di S_n.

(Guardiamo se ciò già visto delle estensioni semplici)

Oss.

1) Sia $f(x) \in K[x]$ e E/K finita.

Sia L/K il campo di spezzamento di $f(x)$ su K.

Il campo di spezzamento di $f(x)$ su E è $L \cdot E$.

2) Siano $f(x), g(x) \in K[x]$

L = campo di spezzamento di $f(x)$ su K

F = " " $g(x)$ su K

Il campo di spezzamento di $f(x)g(x)$ su K è il composto $L \cdot F$

Il seguente teorema dà informazioni sulle proprietà galoisiane del composto:

Teorema

Siano E/K, F/K due estensioni, con E/K di Galois. Allora

1) EF/F è di Galois e $Gal\left(\frac{EF}{F}\right)$ è isom. a un sottogruppo di $Gal\left(\frac{E}{K}\right)$.

2) Se anche F/K è di Galois allora EF/K è Galois e

$Gal\left(\frac{EF}{K}\right)$ è isomorfo a un sottogruppo di $Gal\left(\frac{E}{K}\right) \times Gal\left(\frac{F}{K}\right)$, tale che ognuna delle proiezioni su due fattori è suriettiva. (es $K \hookrightarrow K \times K$).

Dim.

1) Sia $\varphi \in \mathcal{G}\left(\frac{EF}{F}\right)$. Allora $\varphi|_E \in \mathcal{G}\left(\frac{E}{K}\right) \Rightarrow \varphi(E) \subseteq E$

$\Rightarrow \varphi(EF) \subseteq EF$ perché φ è l'identità su F.

La funzione $Gal\left(\frac{EF}{F}\right) \longrightarrow Gal\left(\frac{E}{K}\right)$

$\varphi \longmapsto \varphi|_E$

è un omom. di gruppi, iniettivo: se $\varphi|_E = id_E$ allora $\varphi = id_{EF} \Rightarrow \ker Res_E = id_{EF}$.

2) Supponiamo anche F/K Galois.

$$Gal\left(\frac{EF}{K}\right) \longrightarrow Gal\left(\frac{E}{K}\right) \times Gal\left(\frac{F}{K}\right)$$

è il prodotto di due restrizioni $\Rightarrow$ è un omomorfismo e ognuna delle due proiezioni è suriettiva (Thm (**)) è iniettivo: se $\varphi \in Gal\left(\frac{EF}{K}\right)$ è l'identità su E e su F, allora è l'identità su EF. ∎

Corollario

Il composto di estensioni abeliane è un'estensione ab.

Corollario

Se E/K, F/K sono di Galois e $\left([E:K], [F:K]\right) \overset{m}{=} \overset{n}{=} 1$ allora

$$\mathrm{Gal}\left(\frac{EF}{K}\right) \simeq \mathrm{Gal}\left(\frac{E}{K}\right) \times \mathrm{Gal}\left(\frac{F}{K}\right).$$

Dim.

l'ordine dell'immagine è un divisore di nm divisibile per n e per $m \Rightarrow$ è nm se n, m coprimi.

Oss. Le considerazioni fatte si generalizzano al caso del composto di più estensioni.

ESTENSIONI RADICALI

Sia K un campo di numeri, $b \in K$ e $m \in \mathbb{N}$.

Consideriamo il polinomio $f(x) = x^m - b$

Se α è una radice, le radici hanno la forma

$\alpha, \omega\alpha, \dots, \omega^{m-1}\alpha$ con ω radice (primitiva) m-esima dell'unità

Quindi il campo di spezzamento di $f(x)$ su K è $K(\alpha, \omega)$.

Studiamo prima il caso in cui $\omega \in K$.

In questo caso il campo di spezzamento di $f(x)$ su K è $K(\alpha)$.

Un'estensione E/K si dice ciclica se è di Galois e $\mathrm{Gal}(E/K)$ è un gruppo ciclico.

Teorema

Supponiamo $\mu_m \subseteq K$.

Un'estensione E/K di grado un divisore di m è ciclica $\iff E = K(\alpha)$ con $\alpha^m \in K$ (estensione radicale).

Dim.

$\Leftarrow$ no $E = K(\alpha)$, $\alpha^m = b \in K$.

Per hp. $\omega \in K$ quindi $\omega^i\alpha \in E$ per ogni i e E è campo di spezzam. di $f(x)$ su K.

Ogni $\sigma \in \mathrm{Gal}(E/K)$ è caratterizzato da $\alpha \mapsto \omega^i\alpha$

Poniamo $\theta : Gal\left(\frac{E}{K}\right) \longrightarrow \mu_m$

$\sigma \longmapsto \frac{\sigma(\alpha)}{\alpha}$

θ non dipende dalla radice α scelta, infatti se $\alpha' = \omega^i \alpha$ allora $\frac{\sigma(\alpha')}{\alpha'} = \frac{\sigma(\omega^i \alpha)}{\omega^i \alpha} = \frac{\sigma(\alpha)}{\alpha}$

θ è un omomorfismo.

$$\theta(\sigma\tau) = \frac{\sigma\tau(\alpha)}{\alpha} = \frac{\sigma(\tau(\alpha))}{\tau(\alpha)} \frac{\tau(\alpha)}{\alpha} = \theta(\sigma)\theta(\tau)$$

θ iniettiva:

$$\frac{\sigma(\alpha)}{\alpha} = 1 \Rightarrow \sigma(\alpha) = \alpha \Rightarrow \sigma = id_E.$$

$\Rightarrow Gal\left(\frac{E}{K}\right)$ è ciclico di ordine un divisore di m.

Vogliamo dimostrare il viceversa:

se $\mu_m \subseteq K$ e $Gal\left(\frac{E}{K}\right)$ è ciclico di ordine un divisore di m allora $E = K(\alpha)$ con $\alpha^m \in K$.

Sia $Gal\left(\frac{E}{K}\right) = \langle \sigma \rangle$ ciclico di ordine $n \mid m$.

Le radici n-esime dell'unità $\{1, \eta, \dots, \eta^{n-1}\}$ stanno in K

$\forall \gamma \in E$, la risolvente di Lagrange di γ è

$$\alpha = \gamma + \eta\sigma(\gamma) + \eta^2\sigma^2(\gamma) + \dots + \eta^{n-1}\sigma^{n-1}(\gamma) = \sum_{i=0}^{n-1} \eta^i \sigma^i(\gamma) \in E$$

Si ha $\sigma(\alpha) = \eta^{-1}\alpha$, quindi $\sigma^i(\alpha) = \eta^{-i}\alpha$

SUPPONIAMO $\alpha \neq 0$

$\Rightarrow \alpha, \sigma(\alpha), \dots, \sigma^{n-1}(\alpha)$ sono tutti distinti

$\Rightarrow [K(\alpha) : K] = n \Rightarrow E = K(\alpha)$

Inoltre $\alpha^n \in K$. Infatti $\forall \sigma \in Gal\left(\frac{E}{K}\right)$

$$\sigma(\alpha^m) = \sigma(\alpha)^m = \eta^{-m}\alpha^m = \alpha^m \quad \forall \sigma \in Gal\left(\tfrac{E}{K}\right)$$

$\Rightarrow \alpha^m \in E^{Gal(E/K)} = K.$

Quindi se $\alpha \neq 0$, posto $\alpha^m = b$ hoviamo che $E = K(\alpha)$, il polinomio minimo di α su K è $X^m - b$ e $\alpha^m = b^{\frac{m}{m}} \in K$.

Resta da dimostrare che data E/K ciclica di ordine un divisore di m, esiste $\gamma \in E/K$ t.c. la (Δ) sua risolvente di Lagrange è non nulla.

Dimostreremo un enunciato più forte:

Se E/K finita e $\mathcal{G}\left(\tfrac{E}{K}\right) = \{\sigma_1, \dots, \sigma_m\}$ allora $\sigma_1, \dots, \sigma_m$ sono $\mathbb{C}$-linearmente indipendenti (nel $\mathbb{C}$-sp. vett. delle funzioni da $E \longrightarrow \mathbb{C}$):

se $\lambda_1\sigma_1(\gamma) + \dots + \lambda_m\sigma_m(\gamma) = 0 \quad \forall \gamma \in E$ allora

$\lambda_1 = \lambda_2 = \dots = \lambda_m = 0.$