Oss. Galois = "normale" in caratteristica 0.

Definizione

Sia K un campo di numeri e $f(x) \in K[x]$.

Siano $\alpha_1, \dots, \alpha_n$ le radici di $f(x)$ in $\overline{\mathbb{Q}}$.

Il campo $K(\alpha_1, \dots, \alpha_n)$ si dice campo di spezzamento di $f(x)$ su K.

Il suo gruppo di Galois (su K) si dice gruppo di Galois del polinomio $f(x)$ su K.

<u>Oss.</u> $\mathbb{Q}(\sqrt{2})$ è campo di spezzamento su $\mathbb{Q}$ di X^2-2

$\mathbb{Q}(\sqrt[3]{2}, \omega)$ " " X^3-2

Se ζ radice primitiva n-esima di 1

$\mathbb{Q}(\zeta)$ è campo di spezzamento su $\mathbb{Q}$ di X^n-1.

<u>Teorema</u> Sia $f(x) \in K[x]$, $E = K(\alpha_1 \dots \alpha_n)$ suo campo di spezzam. su K

1) E/K è un'estensione di Galois

2) Ogni K-automorfismo di E permuta tra loro le radici $\alpha_1, \dots, \alpha_n$

3) $Gal(E/K)$ è isomorfo al gruppo di permutazioni indotto su $\{\alpha_1 - \alpha_n\}$

4) Se $f(x)$ è irriducibile in $K[x]$ l'azione di $Gal(E/K)$ su $\alpha_1, \dots, \alpha_n$ è transitiva (cioè $\forall i,j \ \exists \sigma \in Gal(E/K) \ \sigma(\alpha_i) = \alpha_j$)

<u>Dim.</u>

1) Sia $\sigma \in \mathcal{I}(E/K)$. Per ogni $i = 1 \dots n$ si ha

$0 = \sigma(f(\alpha_i)) = f(\sigma(\alpha_i))$

Quindi $\sigma(\alpha_i) = \alpha_j$ per qualche j.

Siccome σ manda $\{\alpha_1 \dots \alpha_n\}$ in se stesso ed è K-lineare, σ è un K-automorfismo.

2) Per quanto visto al punto 1, σ

induce una biezione da $\{\alpha_1, \dots \alpha_n\}$ in se stesso.

3)
Sia $\theta : Gal\left(E/K\right) \longrightarrow S_n = Symm\{\alpha_1, \dots \alpha_n\}$

$\sigma \longmapsto \sigma|_{\{\alpha_1, \dots \alpha_n\}}$

è iniettiva: se σ è l'identità su $\alpha_1 \dots \alpha_n$ allora è l'identità su $E = K(\alpha_1 \dots \alpha_n)$ perché ogni elem. di E si esprime come funzione razionale a coeff. in K negli α_i.

4) Siano α_i, α_j radici di $f(x)$
esiste un K-omom (prop $*$)
$K(\alpha_i) \longrightarrow \mathbb{C}$ che manda $\alpha_i \longrightarrow \alpha_j$
Per il teorema di sollevamento, questo si solleva a un K-automorfismo $E \longrightarrow E$ (perché E è di Galois).

Oss.: se $f(x) = f_1(x)^{e_1} \dots f_m(x)^{e_m}$ è riducibile (f_i irrid.)
l'azione di $Gal\left(E/K\right)$ ha come orbite le radici di ogni $f_i(x)$

Viceversa, si consideri l'azione di $Gal(E/K)$ sull'insieme $\{\alpha_1, \dots, \alpha_n\}$ delle radici di $f(x)$

Tale insieme si decompone nell'unione disgiunta delle sue orbite. Sia $\{\beta_1, \dots \beta_k\}$ una tale orbita. Allora il polinomio $g(x) = \prod_{i=1}^{k} (x - \beta_i)$ è un fattore irriducibile di $f(x)$.

Infatti $\forall \sigma \in Gal(E/K)$, $(\sigma g)(x) = g(x) \Rightarrow$ i coeff. di $g(x) \in E^{G(E/K)} = K$

$\Rightarrow g(x) \in K[x]$

$\Rightarrow g(x) \mid f(x)$

$g(x)$ è irriducibile, altrimenti avrebbe un fattore irriducibile $h(x)$ e la sua orbita si decomporrebbe ulteriormente.

Abbiamo quindi mostrato che ogni campo di spezzamento è un'estensione di Galois.

Vale anche l'inverso

Prop.

Se E/K è un'estensione di Galois $\Rightarrow \exists f(x) \in K[x]$ irriducibile t.c. E è il campo di spezzamento di $f(x)$ su K.

Dim.

E/K semplice $\Rightarrow$ $E = K(\alpha)$

Se $f(x)$ pol. minimo di α su K e

$\alpha_1 = \alpha, \alpha_2, \dots \alpha_n$ radici di $f(x)$ in $\mathbb{C}$

sappiamo che $\forall i$ $\exists \sigma \in G(E/K)$ t.c. $\sigma(\alpha) = \alpha_i$

ma E/K Galois $\Rightarrow$ σ automorfismo $\Rightarrow$ $\alpha_i \in E$.

$\Rightarrow E = K(\alpha_1, \dots, \alpha_n)$. $\blacksquare$

Oss. Nel caso precedente si ha

$$[E : K] = n = \text{grado di } f(x).$$

In generale se E è campo di spezzam. di $f(x)$ su K si ha $Gal(E/K) \subseteq S_n$ $\quad n = \deg f(x)$

$$[E : K] = |Gal(E/K)| \leq |Sym(\alpha_1 \dots \alpha_n)| = n!$$

Esempio

per $f(x) = x^4 - 2$ (su $\mathbb{Q}$) si ha

$E = \mathbb{Q}(\pm \sqrt[4]{2}, \pm i\sqrt[4]{2})$ ha grado 8 su $\mathbb{Q}$

$= \mathbb{Q}(\sqrt[4]{2}, i)$

Abbiamo visto che

estensioni di Galois = campi di spezzamento.

Ma la stessa estensione può essere campo di spezzamento di diversi polinomi.

Se E/K Galois, i sottoinsiemi $\mathcal{G}(E/F)$ di $\mathcal{G}(E/K) = Gal(E/K)$ corrispondenti ai campi intermedi sono descrivibili in termini della struttura di gruppo di $Gal(E/K)$.

<u>Teorema</u> CORRISPONDENZA DI GALOIS

Sia E/K un'estensione di Galois.

1) la corrispondenza
$$F \longmapsto Gal(E/F)$$
definisce una biezione
$$\left\{\begin{matrix}\text{campi intermedi} \\ K \subseteq F \subseteq E\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{sottogruppi} \\ \text{di } Gal(E/K)\end{matrix}\right\}$$

2) Dato un campo intermedio F
$$F/K \text{ è Galois} \iff Gal(E/F) \triangleleft Gal(E/K)$$
↳ sottogruppo normale

e la restrizione $\sigma \longmapsto \sigma|_F$ induce un epimorfismo
$$Gal(E/K) \longrightarrow Gal(F/K)$$
il cui nucleo è $Gal(E/F)$..

Quindi (Teorema di isomorfismo)
$$Gal(E/K) \big/ Gal(E/F) \simeq Gal(F/K).$$

3) Per un campo intermedio F qualsiasi, gli elementi di $\mathcal{I}(F/K)$ corrispondono biunivocamente ai laterali sinistri di $Gal(E/F)$ in $Gal(E/K)$.
↳ ($\neq$ Procesi)