D'ora in avanti ci occuperemo soltanto di estensioni algebriche di $\mathbb{Q}$ (contenute in $\overline{\mathbb{Q}}$)

Teorema

Siano $K \subseteq E$ $[E:K]=n$.

e sia $\varphi: K \longrightarrow \overline{\mathbb{Q}}$ un omom.

Allora φ si estende ad E in esattamente n modi distinti.

Dim.

Se E/K è semplice, deriva dal teorema visto

(*)

sugli omomorfismi da estensioni semplici.

Infatti per il lemma se $E = K(\alpha)$ e il polinomio minimo di α su K è $f(x)$ di grado n, allora $\varphi f(x)$ ha esattamente n radici distinte in $\overline{\mathbb{Q}}$, ognuna delle quali corrisponde a un'estensione di φ a $K(\alpha)$.

Se E/K non è semplice, (induzione sul grado) sia $\alpha \in E \setminus K$ e consideriamo l'estensione intermedia $F = K(\alpha)$.

Per il teorema $(*')$ φ si estende a F in $[K(\alpha) : K]$ modi distinti: $\tilde{\varphi}_1, \dots, \tilde{\varphi}_r$ $\quad r = [K(\alpha) : K]$

Per ipotesi induttiva ogni $\tilde{\varphi}_i$ si estende a E in $[E : K(\alpha)]$ modi distinti $\tilde{\varphi}_{ij}$, $j = 1, \dots, s$
$s = [E : K(\alpha)]$.

I $\tilde{\varphi}_{ij}$ sono tutti distinti:

$i \neq i' \Rightarrow \tilde{\varphi}_{ij} \neq \tilde{\varphi}_{i'j'}$ su $K(\alpha)$

$i = i'$ e $j \neq j' \Rightarrow \tilde{\varphi}_{ij} \neq \tilde{\varphi}_{ij'}$ su E

Inoltre ogni estensione $\hat{\varphi}$ di φ coincide con qualche $\tilde{\varphi}_{ij}$: su $K(\alpha)$ deve essere qualche

$\tilde{\varphi}_i$ e su E deve coincidere con qualche $\tilde{\varphi}_{ij}$.

<u>Corollario</u>

Sia E/K estensione finita $[E:K]=n$

$a \in E$, m = grado di a su K

$f(x)$ polinomio minimo di a su K.

$a = a_1, a_2, \dots, a_m$ le radici di $f(x)$

$\sigma_1, \dots, \sigma_n$ gli n K-omomorfismi $E \to \mathbb{C}$.

Allora gli elementi $\sigma_1(a), \dots, \sigma_n(a)$ sono esattam. le radici $a_1, \dots, a_m$ ognuna contata $\frac{n}{m}$ volte.

<u>Dim.</u>

Si ha $m = [K(a):K] \mid [E:K] = n$

inoltre $\sigma_1, \dots, \sigma_n$ estendono K-omom. $\overbrace{K(a) \to \mathbb{C}}^{\varphi_1 \dots \varphi_m}$

e ognuno di questi è esteso da esattamente $\frac{n}{m}$ tra i σ_i. Per il teorema (*) i φ_i corrispondono biunivocamente alle radici di $f(x)$.

Possiamo assumere $\varphi_i(a) = a_i$.

Quindi $\sigma(a) = a_i$ per gli $\frac{n}{m}$ omom. che estendono φ_i. ∎

LA CORRISPONDENZA DI GALOIS

Sia E/K finita di grado m.

Sappiamo che ci sono m K-omom. $E \to \mathbb{C}$.

Poniamo $\mathcal{J}(E/K) = \{K\text{-omom. } E \to \mathbb{C}\}$

Sia F un campo intermedio: $K \subseteq F \subseteq E$

Allora si ha ovviamente $\mathcal{J}(E/F) \subseteq \mathcal{J}(E/K)$

Quindi abbiamo una corrispondenza

$$\left\{ \begin{matrix} \text{campi intermedi} \\ K \subseteq F \subseteq E \end{matrix} \right\} \longleftrightarrow \left\{ \begin{matrix} \text{sottoinsiemi di} \\ \mathcal{J}(E/K) \end{matrix} \right\}$$

$$F \longmapsto \mathcal{J}(E/F)$$

Viceversa se $T \subseteq \mathcal{J}(E/K)$

uno può costruire $\{\alpha \in E \mid t(\alpha) = \alpha \ \forall t \in T\} = E^T$.

campo fissato da T

Si verifica facilmente che E^T è un campo e che $K \subseteq E^T \subseteq E$.

Quindi si ha anche una corrispondenza nella direzione $\longleftarrow$ e valgono

1) $T \subseteq \mathcal{J}(E/E^T)$ 2) $F = E^{\mathcal{J}(E/F)}$

1) vale per def. di E^T

2) Si ha ovviamente $F \subseteq E^{\mathcal{J}(E/F)}$

Viceversa, ricordiamo che $|\mathcal{J}(E/F)| = [E:F]$.

Si ha $[E:F] = [E:E^{\mathcal{G}(E/F)}][E^{\mathcal{G}(E/F)}:F]$

$\Rightarrow [E:F] \leq [E:E^{\mathcal{G}(E/F)}]$

Per la 1

$$\mathcal{G}(E/F) \subseteq \mathcal{G}\left(E/E^{\mathcal{G}(E/F)}\right)$$

Quindi $[E:E^{\mathcal{G}(E/F)}] \geq [E:F]$

$$\Rightarrow [E:E^{\mathcal{G}(E/F)}] = [E:F] \Rightarrow F = E^{\mathcal{G}(E/F)}.$$

Quindi otteniamo la seguente

<u>Proposizione</u>

La corrispondenza

$$F \rightsquigarrow \mathcal{G}(E/F)$$

è una corrispondenza <u>iniettiva</u> tra i campi intermedi $K \subseteq F \subseteq E$ e i sottoinsiemi di $\mathcal{G}(E/K)$.

<u>Oss.</u>

Non possiamo aspettarci suriettività. Infatti

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

<u>Per es.</u>

$\mathbb{Q}(\sqrt[5]{2})/\mathbb{Q}$ non ha campi intermedi non banali.

<u>Corollario</u>: esiste solo un numero finito di campi intermedi F tra K e E.

(Infatti il # di sottoinsiemi di un insieme finito è finito).

Corollario Teorema dell'elemento primitivo

Ogni estensione finita di campi di numeri è semplice.

Dim.

Sia E/K finita. Sappiamo che è f.g., quindi
$$E = K(\alpha_1, \dots, \alpha_n).$$

Per induzione, basta provare che un'estensione generata da due elementi è semplice.

Sia $E = K(\alpha_1, \alpha_2)$

Per ogni intero h consideriamo il campo
$$E_h = K(\alpha_1 + h\alpha_2)$$

Si ha $K \subseteq E_h \subseteq E$, quindi

$\exists\, h, k$ interi t.c. $\alpha_1 + k\alpha_2 \in K(\alpha_1 + h\alpha_2)$

$\Rightarrow \alpha_1 + k\alpha_2 - \alpha_1 - h\alpha_2 = (k-h)\alpha_2 \in K(\alpha_1 + h\alpha_2)$

$\Rightarrow \alpha_2 ; \alpha_1 \in K(\alpha_1 + h\alpha_2) \Rightarrow K(\alpha_1 + h\alpha_2) = K(\alpha_1, \alpha_2)$. ∎

Esercizio

Trovare un elemento primitivo per

$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$, $\quad \mathbb{Q}(\sqrt[3]{2}, \sqrt{5})$, $\quad \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{5})$

Estensioni di Galois

Domanda: quali sono i sottoinsiemi di $S(E/K)$ che corrispondono ai campi intermedi?

$\emptyset$ no

id $\rightsquigarrow$ K

$\mathcal{J}(E/K) \rightsquigarrow E$

$|\mathcal{J}(E/F)|$ deve dividere $|\mathcal{J}(E/K)|$

Daremo una risposta completa nel caso di particolari estensioni E/K dette "di Galois".

Def.

Un'estensione E/K si dice di Galois se ogni $\varphi \in \mathcal{J}(E/K)$ ha immagine in E: $\varphi(E) \subseteq E$.

Oss.

Se $\varphi(E) = E$ φ è un endomorfismo K-lineare iniettivo di E $\Rightarrow$ è un automorfismo se E/K è finito.

Gli automorfismi si possono comporre e invertire $\rightsquigarrow$ formano un gruppo.

Def.

Sia E/K un'estensione. Il gruppo dei K-automorfismi di E si dice gruppo di Galois di E su K e si denota con $Gal(E/K)$

E/K di Galois $\iff$ $Gal(E/K) = \mathcal{G}(E/K)$.

Esempio

$\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ è di Galois, $\dfrac{\mathbb{Q}(\sqrt[3]{2})}{\mathbb{Q}}$ no

Oss.

Se E/K è di Galois e $K \subseteq F \subseteq E$ allora E/F è Galois.

Invece non è detto che F/K sia Galois.

Esempio

$E = \mathbb{Q}(\sqrt[3]{2}, \omega)$ $\quad \omega^2+\omega+1=0$ è di Galois su $\mathbb{Q}$

ma $F = \mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ non è Galois.