Lezione 14 - 22/05/19

martedì 30 aprile 2019 15:10

Prop: Sia k campo, $f(x) \in k[x]$ irriducibile, L = c.d.s di $f(x)$ su k. Supponiamo che $f(x)$ non abbia radici multiple in L. Allora

$$\#\,Gal(L/k) = [L:k]$$

Lemma: Siano k_1/k, k_2/k normali, allora k_1k_2/k è normale e inoltre abbiamo una mappa iniettiva

$$\varphi: Gal(k_1k_2/k) \hookrightarrow Gal(k_1/k) \times Gal(k_2/k)$$

Dim: Basta considerare la restrizione. Dato $\psi \in Gal(k_1k_2/k) \longmapsto (\psi/_{k_1}, \psi/_{k_2})$ □

Def: Un polinomio $p(x) \in k[x]$ si dice SEPARABILE se $p(x)$ ha tutte radici distinte. Tutta la Teoria che sviluppiamo è per polinomi separabili, altrimenti ci sono delle patologie.

Qualche esempio:

(1) Sia E/k di grado p normale. Dato che gli unici gruppi con $\#$ p sono gli $\mathbb{Z}/p$ allora

$$Gal(E/k) \cong \mathbb{Z}/p$$

(2) Sia $f(x) \in k[x]$ di grado 3 e consideriamo E c.d.s su k di $f(x)$. Supponiamo $f(x)$ irriducibile. Allora

$$\#\,Gal(E/k) \begin{cases} \nearrow 3 \\ \rightarrow 6 \end{cases}$$

In particolare se $f(x) = x^3 + ax + b$ (sempre possibile farlo mediante la sostituzione)

$$x^3 + a_2x^2 + a_1x + a_0 \rightsquigarrow x = \overline{x} + a_2/3$$

allora detto $\Delta = -4a^3 - 27b^2$ vale che se

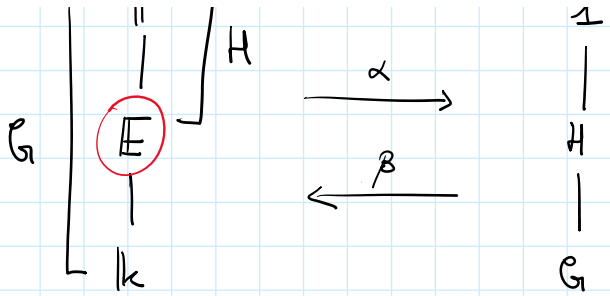
$$\sqrt{\Delta} \in k \Rightarrow |Gal(E/k)| = 3$$
$$\sqrt{\Delta} \notin k \Rightarrow \quad // \quad = 6$$

Teorema dell'elemento primitivo: Sia F/k un'estensione finita. Allora $\exists \gamma \in F$ tale che $F = k(\gamma)$.

Corrispondenza di Galois: Sia F/k una estensione finita di Galois con $G = Gal(F/k)$. Allora esiste una corrispondenza biunivoca

$$\{\text{Campi intermedi } E \text{ di } F/k\} \longleftrightarrow \{\text{sottogruppi } H \text{ di } G\}$$

$$\begin{bmatrix} F \\ | \\ \end{bmatrix} \quad H \qquad \xrightarrow{\alpha} \qquad \begin{matrix} 1 \\ | \end{matrix}$$

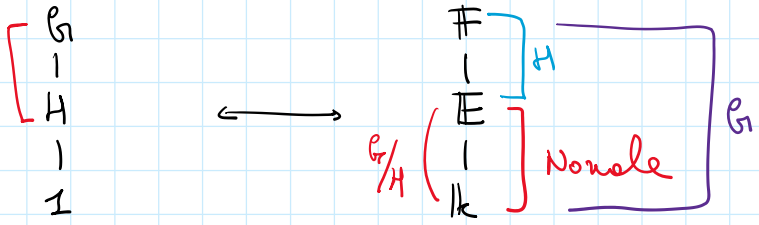


$$\alpha(\mathbb{E}) = Gal(\mathbb{F}/\mathbb{E}) \quad \text{(buona def per normalità)}$$

$$\beta(H) = Fix(H) = \{ x \in \mathbb{F} \mid \sigma(x) = x \ \forall \sigma \in H \}$$

Inoltre abbiamo il seguente importantissimo fatto:

$$H < G \text{ è normale} \iff \beta(H) = Fix(H) = \mathbb{E} \text{ è tale che } \mathbb{E}/k \text{ è normale}$$



E inoltre si ha che

$$Gal(\mathbb{E}/k) \simeq G/H$$

Esempio Campi finiti:
Consideriamo $\mathbb{F}_p$ campo finito e una sua estensione normale e separabile. Ho quindi $f(x) \in \mathbb{F}_p[x]$ irriducibile. Vale che il c.d.s. di $f(x)$ è proprio

$$\mathbb{F}_{p^n} \quad \text{con} \quad n = \deg f(x)$$

Inoltre è facile calcolare il gruppo di Galois di $\mathbb{F}_{p^n}/\mathbb{F}_p$. Si nota infatti facilmente che il morfismo di FROBENIUS

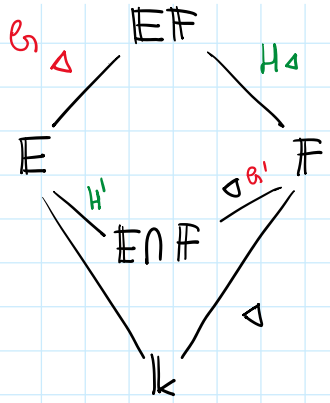
$$\Phi : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}, \quad x \longmapsto x^p$$

ha ordine esattamente n (altrimenti contraddirebbe il teorema di sottocampo ciclico) ed è automorfismo. Questo implica che

$$Gal(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \Phi \rangle \simeq \mathbb{Z}/n$$

LO SHIFT: Consideriamo la seguente torre di estensioni.

Con $\mathbb{F}/k$ normale, $\mathbb{E}/k$ qualunque.



Con F/k normale, E/k qualunque.

Allora EF/E normale (già visto)

$$\begin{aligned} Gal(EF/E) &\hookrightarrow Gal(F/k) \\ \varphi &\longmapsto \varphi|_F \end{aligned}$$

Inoltre detto $G = Gal(EF/E)$ vale che

$$G \cong Gal(F/E\cap F) = G'$$

Infine se EF/F normale e EF/E normale la mappa

$$\begin{aligned} Gal(EF/k) &\longrightarrow Gal(E/E\cap F) \times Gal(F/F\cap E) = G' \times H' \\ \varphi &\longmapsto (\varphi|_E, \varphi|_F) \end{aligned}$$

è un omomorfismo iniettivo e se $k = E\cap F$ (cioè $H\cap k = id$) allora è un isomorfismo di gruppi.

Radici Primitive: Sia $\Phi_n(x) = x^n - 1$. Allora $\exists\, \zeta_n \in \Gamma$ tale che

$$\Phi_n(\zeta_n) = 0 \quad \text{e} \quad \zeta_n^k - 1 \neq 0 \quad \forall k = 1, \dots, n-1$$

Tale ζ_n è detta RADICE n-ESIMA PRIMITIVA dell'unità. Vale che $\mathbb{Q}(\zeta_n)$ è il c.d.s. di $\Phi_n(x)$ e inoltre vale che

$$|Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = \varphi(n)$$