Lezione 13 - 17/05/19

martedì 30 aprile 2019 15:10

Def: Un CAMPO è un anello commutativo con identità in cui ogni el $\neq 0$ è invertibile.

Oss: Gli unici campi finiti sono della forma $\#p^n$ con p primo $n \in \mathbb{N}$

Def: Sia $\mathbb{k}$ campo e $\mathbb{F}$ campo. $\mathbb{k} \subseteq \mathbb{F}$ è detta ESTENSIONE DI CAMPI. Un elemento $\alpha \in \mathbb{F}$ tale che $\exists p(x) \in \mathbb{k}[x]$ t.c. $p(\alpha) = 0$ si dice ALGEBRICO. Un elemento non algebrico si dice TRASCENDENTE

Oss: $\mathbb{k}[x]$ è un PID. Se considero

$$\begin{aligned} v_\alpha : \mathbb{k}[x] &\longrightarrow \mathbb{k}[\alpha] \subseteq \mathbb{F} \\ p(x) &\longmapsto p(\alpha) \end{aligned}$$

v_α è di anelli e prende il nome di VALUTAZIONE IN α.

Oss: Se α è algebrico, allora $\ker v_\alpha = (\mu_\alpha(x))$ con $\mu_\alpha(x)$ primo (dunque irriducibile) $\mu_\alpha(x)$ prende il nome di POLINOMIO MINIMO DI α e per il primo teorema di omomorfismo si ha che $\mathbb{k}[x]/(\mu_\alpha(x)) \cong \mathbb{k}[\alpha]$ ma $\mathbb{k}[\alpha]$ è anche campo e dunque $\mathbb{k}[\alpha] = \mathbb{k}(\alpha)$.

Oss: Dato un campo $\mathbb{k}$ esiste sempre Ω chiusura algebrica di $\mathbb{k}$. (No dim da dispense)

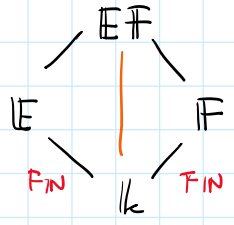
Def: Sia $\mathbb{k} \subseteq \mathbb{F}$ estensione. $\mathbb{k} \subseteq \mathbb{F}$ si dice FINITA se $[\mathbb{F} : \mathbb{k}] = \dim_{\mathbb{k}} \mathbb{F}$ è finita come spazio vettoriale

Def: Una estensione $\mathbb{k} \subseteq \mathbb{F}$ si dice ALGEBRICA se $\forall \alpha \in \mathbb{F}$, α è algebrico su $\mathbb{k}$.

Oss: Finita $\Rightarrow$ Algebrica in quanto sia $\alpha \in \mathbb{F} \Rightarrow 1, \alpha, \dots, \alpha^n$ con $n = \dim_{\mathbb{k}} \mathbb{F}$ sono linearmente dipendenti

Oss: Se $\mathbb{k} \subseteq \mathbb{F}$, $\mathbb{F} \subseteq \mathbb{L}$ finite, allora $\mathbb{k} \subseteq \mathbb{L}$ finita.
Basta considerare $[\mathbb{L} : \mathbb{k}] = [\mathbb{L} : \mathbb{F}] \cdot [\mathbb{F} : \mathbb{k}] < +\infty$.

Oss: Se ho la seguente torre:



con $EF = E(F) = F(E) =$ il più piccolo campo che contiene E e F

allora $\mathbb{k} \subseteq EF$ finita in quanto

$$[EF : F] \leq [E : \mathbb{k}]$$

Prop: Sia $\mathbb{k} \subseteq E$, $E \subseteq \mathbb{F}$ algebriche. Allora $\mathbb{k} \subseteq \mathbb{F}$ algebrica

Dim: Sia $\alpha \in \mathbb{F} \Rightarrow \exists p(x) \in E[x]$ t.c. $p(\alpha) = 0$ con $p(x) = \sum_{i=0}^{n} e_i x^i$ ed $e_i \in E$.
Adesso e_i algebrici su $\mathbb{k}$ $\forall i$. Dunque

$\mathbb{k} \subseteq \mathbb{k}(e_0, \_, e_n) \subseteq \mathbb{k}(e_0, \_, e_n)(\alpha)$ è algebrica

Ovviamente abbiamo $\mathbb{k} \subseteq \mathbb{k}(e_1 \_ e_n, \alpha)$ finita $\Rightarrow$ Algebrica e dunque α algebrico su $\mathbb{k}$.

□

Oss: Dato $\mathbb{k}$ un campo e Ω una sua chiusura algebrica abbiamo gli omomorfismi

$$f: \mathbb{k} \longrightarrow \Omega$$

di campi. Osserviamo che un omomorfismo di campi o è 0 oppure è iniettivo in quanto gli unici ideali sono $\{0\}$ e $\mathbb{k}$.

Cerchiamo di dire chi sono gli omomorfismi di campi

$$\varphi: \mathbb{k}(\alpha) \longrightarrow \Omega$$

con α algebrico su $\mathbb{k}$ tale che $\varphi|_{\mathbb{k}} = id_{\mathbb{k}}$.

Questi sono in bigezione naturale con le radici γ di $\mu_\alpha(x)$. Infatti se $\varphi|_{\mathbb{k}} = id|_{\mathbb{k}}$ allora

$\tilde{\varphi}: \mathbb{k}[x] \longrightarrow \mathbb{k}[x]$ manda $\mu_\alpha(x) \longmapsto \mu_\alpha(\alpha)$ e di conseguenza φ manda le radici in radici.

Il viceversa è ovvio.

Si può generalizzare: Sia $\mathbb{k} \subseteq \mathbb{E}$ finita. Allora $\mathbb{E} = \mathbb{k}(\alpha_1, \_, \alpha_n)$ dove posso pensare l'estensione fatta per passi

$$\mathbb{k} \subseteq \mathbb{k}(\alpha_1) \subseteq \mathbb{k}(\alpha_1, \alpha_2) \subseteq \_\_\_ \subseteq \mathbb{k}(\alpha_1 \_\_ \alpha_{n-1}) \subseteq \mathbb{k}(\alpha_1 \_\_ \alpha_n) = \mathbb{E}$$

Anche in questo caso considero i morfismi $\varphi: \mathbb{E} \longrightarrow \Omega$ tali che $\varphi|_{\mathbb{k}} = id_{\mathbb{k}}$.

Pensando alle estensioni passo per passo se ne deduce che i φ accettati sono tanti quanti

$[\mathbb{E}:\mathbb{k}]$ in quanto ad ogni passo ho tante φ quante le radici "distinte"

Def: Una estensione $\mathbb{k} \subseteq \mathbb{E}$ si dice NORMALE se $\forall \varphi: \mathbb{E} \longrightarrow \Omega$ tale che $\varphi|_{\mathbb{k}} = id_{\mathbb{k}}$ vale che $\varphi(\mathbb{E}) \subseteq \mathbb{E}$ $(\varphi(\mathbb{E}) = \mathbb{E})$.

Esempi:

① $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$ è normale. Ho solo $\varphi_1: \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{C}$ $\sqrt{2} \longmapsto -\sqrt{2}$
$\varphi_0: \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{C}$ $\varphi_0 = id$

e fanno la cosa giusta

② $\mathbb{Q}(\sqrt[3]{2}) \supseteq \mathbb{Q}$ NON è normale. Ho $\varphi_0: \mathbb{Q}(\sqrt[3]{2}) \longrightarrow \mathbb{C}$ id
$\varphi_1: \mathbb{Q}(\sqrt[3]{2}) \longrightarrow \mathbb{C}$ $\varphi_1(\sqrt[3]{2}) = \sqrt[3]{2}\,\omega$
$\varphi_2: \mathbb{Q}(\sqrt[3]{2}) \longrightarrow \mathbb{C}$ $\varphi_2(\sqrt[3]{2}) = \sqrt[3]{2}\,\omega^2$

e non è vero che $\varphi_i(\mathbb{Q}(\sqrt[3]{2})) = \mathbb{Q}(\sqrt[3]{2})$

$\varphi_1 : \mathbb{Q}(\sqrt[3]{2}) \longrightarrow \mathbb{Q} \quad \varphi_1(\sqrt[3]{2}) = \sqrt[3]{2}\,\omega$

$\varphi_2 : \mathbb{Q}(\sqrt[3]{2}) \longrightarrow \mathbb{C} \quad \varphi_2(\sqrt[3]{2}) = \sqrt[3]{2}\,\omega^2$

e non è vero che $\varphi(\mathbb{Q}(\sqrt[3]{2})) = \mathbb{Q}(\sqrt[3]{2})$

Proposizione: Se $k \subseteq E_1$ e $k \subseteq E_2$ normali allora $k \subseteq E_1E_2$ e $k \subseteq E_1 \cap E_2$ normali.

Dim: basta guardare i generatori. Se $\varphi(E_1) = E_1$ e $\varphi(E_2) = E_2 \Rightarrow \varphi(E_1 E_2) = E_1E_2$ e analogamente $\varphi(E_1 \cap E_2) = E_1 \cap E_2$

Teorema: Sia $f(x) \in k[x]$ e sia E il campo di spezzamento di $f(x)$ su k. Allora $k \subseteq E$ è normale. Viceversa se $k \subseteq E$ è normale $\exists f(x) \in k[x]$ tale che E è il suo campo di spezzamento

Dim: Sia $\varphi : E \longrightarrow \Omega$ tale che $\varphi|_k = id_k \Rightarrow \varphi(f(x)) = f(x)$ cioè φ manda le radici di f in radici di f. Ma E le contiene tutte $\Rightarrow \varphi(E) = E$.
Viceversa $k \subseteq E$ normale considero $E = k(\alpha_1, \dots, \alpha_n)$ e considero $\mu_{\alpha_i}(x)$ polinomio minimo di α_i e chiamo $f_i = \mu_{\alpha_i}$. Considero $\alpha_i^{(j)}$ le radici di f_i al variare di j tra 1 e $\deg(f_i(x))$. Per normalità vale che

$$E = k(\alpha_i^{(j)})_{i,j}$$

e dunque E = campo di spezzamento di $F = f_1 \cdot f_2 \cdot \dots \cdot f_n$. ▫

Def: Sia E/k una estensione normale. Definiamo

$$Aut(E/k) = Gal(E/k) = \{\varphi : E \longrightarrow \Omega \mid \varphi|_k = id|_k\}$$

Dove se $\varphi, \psi \in Gal(E/k)$ allora $\varphi \circ \psi$ e $\psi \circ \varphi \in Gal(E/k)$. Inoltre $id_E \in Gal(E/k)$ e se $\varphi \in Gal(E/k) \Rightarrow \varphi^{-1} \in Gal(E/k)$.
Il gruppo $Gal(E/k)$ prende il nome di GRUPPO DI GALOIS

Oss: Sia E/k normale e sia $f(x) \in k[x]$ il pol. di cui E è cds. Allora

$$Gal(E/k) < S_n \qquad \deg(f(x)) = n$$

Infatti $Gal(E/k)$ sono le permutazioni delle radici di $f(x)$ che sono poi automorfismi.
Dunque $Gal(E/k)$ è sottogruppo di un gruppo di permutazioni