Proposizione (*)

Sia $K(\alpha)$ un' estensione semplice di K e F/K un' altra estensione.

(a) Supponiamo che α sia trascendente su K.
Allora per ogni K-omomorfismo $\varphi: K(\alpha) \longrightarrow F$
$\varphi(\alpha)$ è trascendente su K, e la corrispondenza
$$\varphi \longmapsto \varphi(\alpha)$$
definisce una biezione
$$\{K\text{-omo } \varphi: K(\alpha) \to F\} \longleftrightarrow \{\beta \in F \mid \beta \text{ trasc. su } K\}$$
(b) Supponiamo α sia algebrico su K, $f(x) \in K[x]$ pol. min.
Per ogni K-omomorfismo $\varphi: K(\alpha) \longrightarrow F$
$\varphi(\alpha)$ è una radice di $f(x)$ in F, e la corrispondenza $\varphi \longmapsto \varphi(\alpha)$ definisce una biezione
$$\{K\text{ omo } \varphi: K(\alpha) \to F\} \longleftrightarrow \{\text{radici di } f \text{ in } F\}$$
In particolare il numero di K-omo $K(\alpha) \to F$ è uguale al # di radici di $f(x)$ in F (quindi $\leq \deg f$).

Dim.

a) Dire che α trascendente su K significa $K[x] \underset{K}{\simeq} K[\alpha]$. Quindi per ogni $\beta \in F$ esiste un unico K-omo di anelli $\varphi: K[\alpha] \longrightarrow F$ t.c. $\varphi(\alpha) = \beta$. φ si estende al campo dei quozienti $K(\alpha)$ $\Leftrightarrow$ elem. non nulli di $K[\alpha]$ sono mandati in elementi non nulli di F, $\Leftrightarrow$ $\varphi(\alpha)$

è trascendente su K. Quindi c'è corrisp. biunivoca tra

$$\left\{\begin{matrix} K\text{-omo} \\ K(\alpha) \to F \end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix} K \text{ omo} \\ K[\alpha] \to F \\ \text{t.c. } \varphi(\alpha) \text{ trascendente} \end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix} \text{elem.} \\ \text{trascendenti} \\ \text{di } F \end{matrix}\right\}$$

b) Sia α algebrico su K e $f(x) = \sum a_i X^i$ il suo polinomio minimo su K.

Sia $\varphi : K(\alpha) \longrightarrow F$ un K-omomorfismo.

Si ha

$$0 = \varphi\left(\sum a_i \alpha^i\right) = \sum a_i \varphi(\alpha)^i \Rightarrow \varphi(\alpha) \text{ è radice}$$

di $f(x)$ in F.

Viceversa se $\beta \in F$ è radice di $f(x)$, allora

$$K(\alpha) \simeq \frac{K[x]}{(f(x))} \simeq K(\beta)$$

$$\alpha \longmapsto \bar{x} \longmapsto \beta$$

fornisce un K-isom $K(\alpha) \longmapsto K(\beta)$ che corrisponde a un K-omo: $K(\alpha) \longrightarrow F$.

<u>Esempio</u>

Sia $\alpha = \sqrt[3]{2}$. $f(x) = x^3 - 2$ ha radici $\overset{\alpha_1}{\alpha}, \overset{\alpha_2}{\omega\alpha}, \overset{\alpha_3}{\omega^2\alpha}$

$\omega^2 + \omega + 1 = 0$

C'è un unico $\mathbb{Q}$-omom.

$$\mathbb{Q}(\alpha) \longrightarrow \mathbb{R} \qquad (\text{inclusione})$$

ci sono 3 $\mathbb{Q}$_ omom

$$\varphi_i : \mathbb{Q}(\alpha) \longrightarrow \mathbb{C}$$

$$f(\alpha) \longrightarrow f(\alpha_i)$$

<u>Esempio</u>

Sia $K = \mathbb{F}_p(X)$ e sia α una radice di $f(Y) = Y^p - X$. Quindi $\alpha^p = X$ e dunque

Ma $Y^p - X = X^p - \alpha^p = (X - \alpha)^p$

segue che in ogni estensione F di $K(\alpha)$ c'è un'unica radice di $f(Y)$. $\Leftrightarrow$ c'è un unico K- omom: $K(\alpha) \longrightarrow F$.

Generalizzazione della prop. precedente:

<u>Proposizione</u>

Sia $\varphi_0 : K \longrightarrow F$ omo di campi.

Sia $K(\alpha)/_K$ estensione semplice

a) α trascendente $\overset{su\,K}{\Rightarrow}$ $\exists$ biezione

$$\left\{ \begin{array}{l} \text{estensioni di } \varphi_0 \\ \text{a } K(\alpha) \end{array} \right\} \Longleftrightarrow \left\{ \begin{array}{l} \text{elementi} \\ \text{di } F \text{ trascendenti su } \varphi_0(K) \end{array} \right\}$$

$$\varphi \longmapsto \varphi(\alpha)$$

b) Se α è algebrico su K, la corrispondenza

$$\varphi \longmapsto \varphi(\alpha)$$

definisce una biezione

$$\left\{ \begin{array}{l} \text{Estensioni di} \\ \varphi_0 \text{ a } K(\alpha) \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{Radici di} \\ \varphi_0 f(x) \text{ in } F \end{array} \right\}$$

In particolare, il numero di estensioni di φ_0 a $K(\alpha)$ è uguale al numero di radici di $\varphi_0 f(x)$ in F.

(La dimostrazione è analoga alla precedente).

ESTENSIONI ALGEBRICHE

Abbiamo visto che α alg. su $K \iff K(\alpha)/K$ finita

E/K finita $\underset{\not\Leftarrow}{\Rightarrow}$ E/K algebrica

In particolare se E/K finita e $\alpha \in E$, allora

1) α algebrico su K
2) il grado di α su K divide $[E:K]$ (formula di moltiplicatività dei gradi).

Oss.

Sia $K \subseteq E \subseteq F$ torre di estensioni, e $\alpha \in F$.

Se α è algebrico su K allora α è algebrico su E (infatti $K[x] \subseteq E[x]$). Sia $f(x) \in K[x]$ il polinomio minimo di α su K.

$f(x)$ può essere riducibile in $E[x]$

In generale il pol. minimo g di α su E divide il pol. minimo di α su K.

Esempio: 1) se $\alpha \in E \setminus K$

1 $g(x) = x - \alpha$ ha grado 1
$f(x)$ " > 1 (perché $\alpha \notin K$)

2) $x^4 - 2$ è irrid su $\mathbb{Q}$ (Eisenstein)

$\Rightarrow$ è il polinomio minimo di
$\pm\sqrt[4]{2}$, $\pm i\sqrt[4]{2}$

Su $\mathbb{Q}(\sqrt{2})$ si fattorizza come
$(X^2-\sqrt{2})(X^2+\sqrt{2})$
Su $\mathbb{Q}(\sqrt[4]{2})$ si fattorizza come
$(X-\sqrt[4]{2})(X+\sqrt[4]{2})(X^2+\sqrt{2})$

Se $\alpha = i\sqrt[4]{2}$
Il pol. minimo di α su $\mathbb{Q}$ è X^4-2
" " di α su $\mathbb{Q}(\sqrt[4]{2})$ è $X^2+\sqrt{2}$

Estensioni algebriche finitamente generate

Prop.
Sia K campo, e $\alpha_1, \dots, \alpha_n$ algebrici su K
Allora l'estensione $K(\alpha_1 \dots \alpha_n)/K$ è finita e
$$[K(\alpha_1,\dots,\alpha_n):K] \leq \prod_{i=1}^{n} [K(\alpha_i):K]$$

Dim.
Consideriamo la torre

$$K \subseteq K(\alpha_1) \subseteq K(\alpha_1,\alpha_2) \subseteq \dots \subseteq K(\alpha_1 \dots \alpha_n)$$
Ogni gradino della torre è un'estensione semplice e $[K(\alpha_1 \dots \alpha_{i+1}) : K(\alpha_1 \dots \alpha_i)] \leq [K(\alpha_{i+1}):K]$
Il risultato segue per la formula di molt. dei gradi.

Viceversa

Prop. Ogni estensione L/K finita è f.g., cioè esistono $\alpha_1, \dots, \alpha_n$ t.c. $L = K(\alpha_1, \dots, \alpha_n)$.

Dim.

Si prenda per es. una base di L come K. sp. vett.

Osservazione:

Se L/K f.g. come sp. vett. $\Rightarrow$ f.g. come campo

$\not\Leftarrow$

(per es. est. trascendenti)

Corollario

1) Se $K \subseteq E \subseteq F$ e E/K, F/E algebriche allora F/K algebrica.

2) Sia E/K un'estensione e

$$E^0 = \{\alpha \in E \mid \alpha \text{ algebrico su } K\}$$

Allora E^0 è un campo.

(In particolare $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ algebrico}\}$ è un campo

Dim.

1) Se $\alpha \in F$ si ha $g(\alpha) = 0$ per un $g(x) \in E[x]$ non nullo, $g(x) = \sum_{i=0}^{m} b_i X^i$, $b_i \in E$

In particolare α è algebrico su $\tilde{E} = K(b_1, \dots, b_m)$
est. algebrica f.g. $\Rightarrow$ finita.
Ne segue che

$$[\tilde{E}(\alpha):K] = \underbrace{[\tilde{E}(\alpha):\tilde{E}]}_{\substack{\text{finita} \\ \text{(semplice e} \\ \text{algebrica)}}} \underbrace{[\tilde{E}:K]}_{\substack{\text{finita} \\ \text{(f.g + algebrica)}}} < \infty$$

$\Rightarrow \alpha$ algebrico su K.

2) Siano $\alpha, \beta \in E^\circ$
allora $\alpha + \beta,\ \alpha\beta,\ \alpha^{-1} \in \underbrace{K(\alpha,\beta)}_{\text{finita}}$

$\Rightarrow \alpha+\beta, \alpha\beta, \alpha^{-1}$ sono algebrici su K.

<u>Definizione</u>
Sia K un campo. Un'estensione E/K si dice
chiusura algebrica di K se
1) E/K è algebrica
2) E è algebricamente chiuso: ogni polinomio non costante in $E[x]$ ha una radice in E.

Sia $K \subseteq E$ e E algebricamente chiuso
allora $E^\circ = \{\alpha \in E \mid \text{algebrico su } K\}$ è una

chiusura algebrica di K.

Si dimostra che
1) Ogni campo ha una chiusura algebrica
2) Due chiusure algebriche di K sono K-isomorfe

Parleremo quindi della chiusura algebrica $\overline{K}$ di K.

In particolare $\overline{\mathbb{Q}}$ è la chiusura algebrica di $\mathbb{Q}$

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

<u>Lemma</u>

Se $f(x) \in K[x]$ è irrid., allora $f(x)$ ha radici distinte in $\overline{\mathbb{Q}}$.

<u>Dim.</u>

Altrimenti $MCD(f(x), f'(x)) \neq 1 \Rightarrow f(x) \mid f'(x)$
$\Rightarrow f'(x) = 0$ perché $f(x)$ irrid.

Ma se $f(x) = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0 \quad a_n \neq 0$

$f'(x) = n a_n X^{n-1} + \ldots + a_1 = 0 \Rightarrow n a_n = 0 \Rightarrow$ assurdo. ∎