Esempio

$$\mathbb{R}[i] = \{a+bi \mid a, b \in \mathbb{R}\}$$

$$\mathbb{R}(i) = \left\{\frac{a+bi}{c+di} \mid a,b,c,d \in \mathbb{R}\right\}$$

Si ha $\mathbb{R}[i] = \mathbb{R}(i)$ infatti

$$(a+bi)(x+yi) = 1$$

$$\begin{cases} ax - by = 1 \\ bx + ay = 0 \end{cases}$$ sistema lineare con

det $a^2+b^2 \neq 0$

(altrimenti $\left(\frac{a}{b}\right)^2 = -1$) $\Rightarrow$ $\exists!$ soluzione

È utile studiare le estensioni di campi utilizzando l'algebra lineare. Infatti se L/K è un'estensione allora possiamo vedere L come spazio vett. su K dove il prodotto di un vettore per uno scalare è dato dalla moltiplicazione in L.

$$K \times L \longrightarrow L$$
$$(\lambda, \alpha) \longmapsto \lambda\alpha$$

<u>Def.</u> Il **grado** dell'estensione L/K è $\dim_K(L)$.
e si indica $[L:K]$

<u>Esempio</u>

Sia $L = K(\alpha)$ un'estensione semplice.

- Se α è trascendente su K abbiamo visto che
  $\theta : K[x] \longrightarrow L$ è iniettiva

(osservo che θ è K-lineare)

$\Rightarrow$ L contiene un sottosp. di dim. infinita

$\Rightarrow$ $[L:K] = \infty$

- Se α è algebrico su K di grado n
  ogni elem di $K(\alpha)$ si scrive in modo unico come

  $a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$

  $\Rightarrow$ $(1, \alpha, \ldots, \alpha^{n-1})$ base di L/K $\Rightarrow n = [L:K]$.

E/K estensione **finita** se $[E:K]$ finita.

Quindi per un'estensione semplice

$K(\alpha)/K$ è
- finita se α algebrico su K
- infinita se α trascendente su K

Prop. Formula di moltiplicatività dei gradi

Sia $K \subseteq L \subseteq F$ una torre di estensioni.

Allora $[F:K] = [F:L][L:K]$

(con l'interpretaz. ovvia quando uno dei termini è ∞).

<u>Dim.</u>

Dimostriamo prima che

F/K finita $\Rightarrow$ F/L, L/K finite

$\Rightarrow$ F/K finita. ① Una base di F/K è un sistema di generatori di F/L $\Rightarrow$ F/L è f.g.

$\Rightarrow$ F/L finita.

② L/K è un sottosp. vett. di F/K $\Rightarrow$ è finita

$\Leftarrow$ Supponiamo $\alpha_1, \dots, \alpha_n$ base di F/L

$\beta_1, \dots, \beta_m$ base di L/K

Dico che $\alpha_i \beta_j$ è una base di F/K

Se $\gamma \in F$ $\quad \gamma = \sum a_i \alpha_i \quad a_i \in L$

$a_i = \sum b_{ij} \beta_j \qquad b_{ij} \in K$

$\gamma = \sum_{i,j} b_{ij} \alpha_i \beta_j \quad b_{ij} \in K \Rightarrow (\alpha_i \beta_j)_{ij}$ gen.

Sono l. i.: se

$$\sum_{i,j} b_{ij} \alpha_i \beta_j = 0 \Rightarrow \sum_i \Big(\overbrace{\sum_j b_{ij} \beta_j}^{\in L} \Big) \alpha_i = 0$$

(α_i) base di F/L $\Rightarrow$ $\forall i$ $\sum_j b_{ij}\beta_j = 0$
(β_j) base di L/K $\Rightarrow$ $b_{ij} = 0$ $\forall i, j$. ☒

Corollario

1) Ogni estensione finita è algebrica
2) Se L/K è finita e $\alpha \in L$ allora il grado di α su K divide $[L:K]$.

Dim.

Sia L/K finita e $\alpha \in L$

$$K \subseteq K(\alpha) \subseteq L \Rightarrow$$

$K(\alpha)/K$ finita $\Rightarrow$ α alg. su K.

$\Rightarrow L/K$ algebrica

Si ha

$$[L:K] = [L:K(\alpha)]\underbrace{[K(\alpha):K]}_{\text{grado di } \alpha \text{ su } K}$$

divide $[L:K]$. ☒

Oss. non è vero che L/K algebrica $\Rightarrow$ L/K finita.

Si vedrà che

$$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ algebrico}\}$$

è un campo, e $\overline{\mathbb{Q}}/\mathbb{Q}$ infinita (esistono estensioni alg. di ogni grado: $X^n - 2$ irrid. per ogni n).

OMOMORFISMI

Ricordiamo che se E, F sono campi ogni omomorfismo $E \longrightarrow F$ è iniettivo. (vengono anche detti <u>isomorfismi</u> o <u>immersioni</u>)

<u>Esempi</u>

Coniugio cpx

$$\sqrt{m} \longrightarrow \sqrt{m}$$

Un omomorfismo $\varphi: E \longrightarrow F$ induce un omomorfismo iniettivo di anelli

$$\tilde{\varphi}: E[x] \longrightarrow F[x]$$
$$f: \sum a_i x^i \longmapsto \sum f(a_i) x^i$$

(dim. per esercizio)

<u>Def.</u>

Sia $\varphi: E \longrightarrow F$ omom. di campi e E'/E. Se $\sigma: E' \longrightarrow F$ è tale che $\sigma|_E = \varphi$, si dice che σ **estende** φ a E'.

Campo di numeri = <u>estensione finita</u> di $\mathbb{Q}$.

Oss L'unico omom. $\mathbb{Q} \longrightarrow \mathbb{Q}$ è l'identità
" $\mathbb{F}_p \longrightarrow \mathbb{F}_p$ "

Def: Siano $E/_K$, $F/_K$ estensioni.
Un omomorfismo
$\varphi: E \longrightarrow F$ si dice K-omomorfismo
se $\varphi|_K = id$, cioè se φ è K-lineare.

Per quanto visto:
- se $car(E) = car(F) = 0$ allora
ogni omom. $E \longrightarrow F$ è un $\mathbb{Q}$-omomorfismo
- se $car(E) = car(F) = p$ allora
ogni omom $E \longrightarrow F$ è un $\mathbb{F}_p$-omomorfismo
(se $\exists$ omom. $E \longrightarrow F$ allora $car(E) = car(F)$)

Prop.
Siano E, F campi e $\sigma, \tau: E \longrightarrow F$ omom.
Allora l'insieme
$K = \{ \alpha \in E \mid \sigma(\alpha) = \tau(\alpha) \}$ è un sottocampo
di E.
In particolare, se $E \subseteq F$ e $\sigma: E \longrightarrow F$ omo

allora $\{\alpha \in E \mid \sigma(\alpha) = \alpha\}$ è un campo, detto campo fissato da σ, E^{σ}

Dim.

Si ha $\alpha, \beta \in K$

$\alpha - \beta \in K$ infatti $\sigma(\alpha-\beta) = \sigma(\alpha) - \sigma(\beta) =$
$\varepsilon(\alpha) - \varepsilon(\beta) = \varepsilon(\alpha-\beta)$

$\alpha\beta \in K$ ⇝ $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta) = \dots$

$\alpha^{-1} \in K$ ⇝ $\sigma(\alpha^{-1}) = \sigma(\alpha)^{-1} = .$

Per la seconda affermazione, si consideri
$\varepsilon = i$ inclusione $E \longrightarrow F$ $(i(e) = e)$.

Oss.

Se $\sigma : E \longrightarrow F$ omomorfismo, allora $\sigma(E)$ è sottocampo di F.

Prop E/K estensione di campi e $\sigma : E \longrightarrow F$ omo, $\Rightarrow$ $\sigma(E)/\sigma(K)$ estensione. Inoltre

$$[\sigma(E) : \sigma(K)] = [E : K]$$

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

$$\{K\text{-omo } \varphi: K(\alpha) \to F\} \leftrightarrow \{\beta \in F \mid \beta \text{ trasc. su } K\}$$

(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

$$\{K\text{ omo } \varphi: K(\alpha) \to F\} \leftrightarrow \{\text{radici di } f \text{ in } F\}$$

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.

(da concludere)