ARITMETICA 13 DIC 2017

Note Title 12/13/2017

Notazioni:

- $K \subseteq F$ campi.
- $\alpha \in F$ algebrico su K se $\exists f(x) \in K[x]$ NON NULLO tale che $f(\alpha)=0$.
- In questo caso i polinomi $f(x)$ tali che $f(\alpha)=0$ formano un ideale.
- Questo ideale è della forma $(g(x))$ quindi si può scegliere al suo interno un polinomio DI GRADO MINIMO e anche MONICO.
- Questo si dice polinomio minimo di α su K. $(\mu_\alpha(x))$
- Il polinomio minimo è IRRIDUCIBILE. $(\mu_\alpha(x) = f(x) = g(x)h(x) \Rightarrow 0 = f(\alpha) = g(\alpha)h(\alpha))$
- $\frac{K[x]}{(\mu_\alpha(x))}$ = è un campo.
- L'omomorfismo di sostituzione $g(x) \mapsto g(\alpha)$ dà un isomorfismo fra $\frac{K[x]}{(\mu_\alpha(x))}$ e $K(\alpha)$ = (il più piccolo sottocampo di F che contiene K e α).
- Supponiamo $\deg \mu_\alpha(x) = n$. Allora $\frac{K[x]}{(\mu_\alpha(x))}$ è uno spazio vettoriale su K di dimensione n, che ha come base possibile $\{\bar{1}, \bar{x}, \bar{x}^2, \dots, \bar{x}^{n-1}\}$.
- Tramite l'isomorfismo di sostituzione $X \mapsto \alpha$

si ottiene che $1, \alpha, \dots, \alpha^{n-1}$ è una base di $K(\alpha)$ come spazio vettoriale su K.

$$\deg \mu_\alpha(x) = \dim_K K(\alpha) = [K(\alpha):K].$$

Esempio standard: $K = \mathbb{Q}$, $F = \mathbb{C}$

$\alpha = \sqrt[3]{2}$

$X^3 - 2$ si annulla in α.

$\downarrow$

irriducibile $\rightarrow$ POL. MINIMO.

$$[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = 3.$$

Due passi successivi.

$K \subseteq E \subseteq F$

E è uno S.V. su K

$\rightarrow$ F è uno S.V. su E

F è uno S.V. su K

F | E | K

Prop. Se $[E:K] = m < \infty$ e $[F:E] = n < \infty$ allora $[F:K] = mn$

Dim. Sia $\{\alpha_1, \alpha_2, \dots, \alpha_m\}$ una base di E come S.V. su K.

Sia $\{\beta_1, \dots, \beta_n\}$ una base di F come S.V. su E.

Voglio dimostrare che $\{\alpha_j \beta_i\}_{j=1,\dots,m;\ i=1,\dots,n}$

è una base di F come s.v. su K.

(1) $\{\alpha_i \beta_j\}$ è un insieme di generatori.

Per (A) ogni elemento $x \in F$ si scrive nella forma

$$x = \sum_i e_i \beta_i \qquad \text{con } e_i \in E.$$

Per (B) ciascun e_i si scrive nella forma

$$e_i = \sum_{j=1}^{n} k_{ij} \alpha_j \qquad k_{ij} \in K$$

Sostituisco e ottengo

$$x = \sum_i e_i \beta_i = \sum_i \sum_j k_{ij} \alpha_j \beta_i .$$

$\Rightarrow x$ è comb. lineare degli $\alpha_j \beta_i$ con coeff. in K.

Resta da vedere che gli elementi $\alpha_j \beta_i$ sono linearmente indipendenti su K.

Siano $c_{ji} \in K$ tali che

$$\sum_{i,j} c_{ji} \alpha_j \beta_i = 0 .$$

Riscrivo l'equazione come

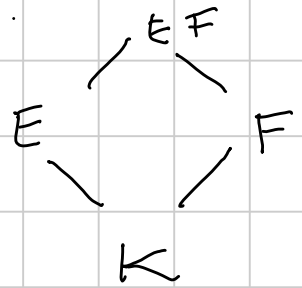
$$\sum_i \Big(\underbrace{\sum_j c_{ji} \alpha_j}_{\in E} \Big) \underbrace{\beta_i}_{\text{base di } F \text{ s.v. su } E} = 0$$

Questo implica che $\sum_j c_{ji} \alpha_j = 0 \quad \forall i$.

Siccome gli a_j sono una base di E come s.v. su K tutti i coefficienti c_{ij} sono $=0$ $\forall j$

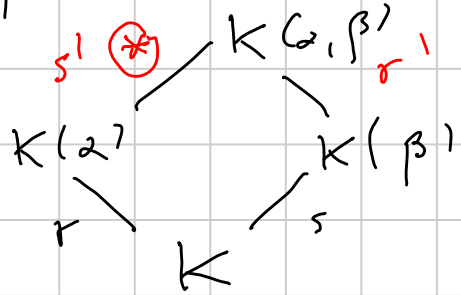
TUTTI $=0$ $\Rightarrow$ INDIPENDENZA LINEARE.

Grafici senza ordinamento totale dei campi.



EF è il più piccolo campo che contiene sia E che F.

Caso particolare:



$K(\alpha,\beta) = K(\alpha)(\beta) = K(\beta)(\alpha)$

$r = [K(\alpha):K]$ $\quad$ $s = [K(\beta):K]$

$s' = [K(\alpha,\beta):K(\alpha)]$ = grado del polinomio minimo di β su $K(\alpha)$.

$s = [K(\beta):K]$ = grado del polinomio minimo di β su K. $\quad$ $\mu_{\alpha,K}(x)$

Certamente so che $\mu_{\beta,K}(x) \in K(\alpha)[x]$ in quanto $K \subseteq K(\alpha)$

Quindi $\mu_{\beta,K}(x)$ è UN MULTIPLO di $\mu_{\beta,K(\alpha)}(x)$.

Ne segue che

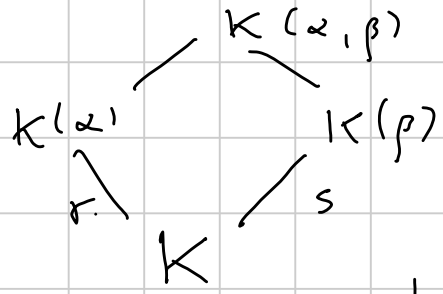
$$\deg \mu_{\beta, K(\alpha)}(x) \leq \deg \mu_{\beta, K}(x).$$

Quindi $\boxed{s' \leq s}$

Simmetricamente $\boxed{r' \leq r}$.

$$s'r = r's = [K(\alpha,\beta) : K]$$

Oss. Se $(r,s) = 1$, allora $r' = r$ $s' = s$.



Infatti so che $r \mid [K(\alpha,\beta) : K]$

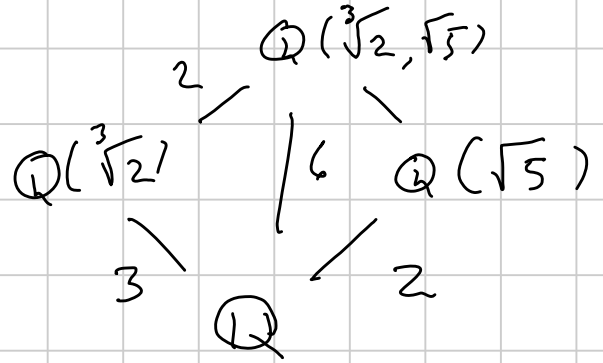
$s \mid [K(\alpha,\beta) : K]$

$$\Rightarrow rs \mid [K(\alpha,\beta) : K] = sr' = s'r$$

$s' \leq s$ $r' \leq r$

$$\Rightarrow sr' = rs = s'r$$

$$\Rightarrow s' = s \quad r' = r.$$



CAMPO DI SPEZZAMENTO DI UN POLINOMIO

$K \subseteq \Omega$ (algebricamente chiuso)

Caso cruciale: $\mathbb{Q} \subseteq \mathbb{C}$

$f(x) \in K[x]$ ($\mathbb{Q}[x]$) $\quad \deg f = n$

$f(x) = c(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n)$ in $\Omega[x]$ ($\mathbb{C}[x]$)

Def. Il campo di spezzamento di $f(x)$ su K è il campo

$$K(\alpha_1, \alpha_2, \dots, \alpha_n)$$

(Si può pensare di "aggiungere" le radici una alla volta:

$K \subseteq K(\alpha_1) \subseteq K(\alpha_1,\alpha_2) \subseteq \dots \subseteq K(\alpha_1,\alpha_2,\dots,\alpha_n)$

$K_0 \subseteq K_1 \subseteq K_2 \subseteq K_n$

e so che $K_i = K_{i-1}(\alpha_i)$)

Voglio studiare $[K(\alpha_1,\dots,\alpha_n) : K] = D$

In particolare, voglio confrontare questo grado con $n!$

(1) $D \leq n!$

(Induzione su n)

Caso iniziale: $n = 1$ $\quad f(x) = c(x-\alpha)$

$[K(\alpha) : K] = 1$.

Passaggio induttivo:

- $[K(\alpha_1) : K] \leq n$. $\quad \mu_{\alpha_1}(x) \mid f(x)$

Siccome $\alpha_1 \in K(\alpha_1)$

per il teorema di Ruffini ho

$$f(x) = (x-\alpha_1)\, g(x) \quad \text{in } K(\alpha_1)[x]$$

GRADI: $\quad n \qquad 1 \qquad n-1$

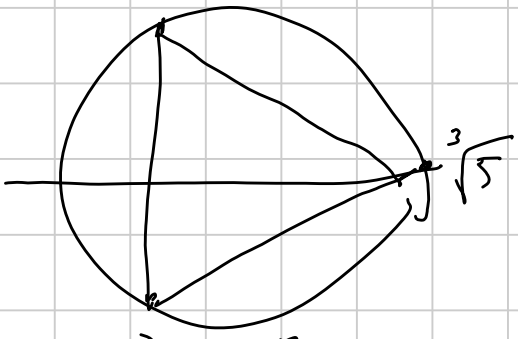
$$K \subseteq K(\alpha_1) \subseteq \dots \subseteq K(\alpha_1, \dots, \alpha_n)$$

GRADI $\quad \leq n \qquad \leq (n-1)!$

PRODOTTO: $\quad \leq n!$

Esempio $\quad f(x) = x^3 - 5 \in \mathbb{Q}[x]$

Radici: $\quad \alpha_1 = \sqrt[3]{5} \quad \alpha_2 = \sqrt[3]{5}\,\zeta_3, \quad \alpha_3 = \sqrt[3]{5}\,\zeta_3^2$



$[\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) : \mathbb{Q}]$

$$\mathbb{Q} \subseteq \mathbb{Q}(\alpha_1) \subseteq \mathbb{Q}(\alpha_1, \alpha_2) \subseteq \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$$

$\downarrow$

3

$\mathbb{Q}(\alpha_1) \subseteq \mathbb{R}$

$\alpha_2 \notin \mathbb{R} \qquad \alpha_3 \notin \mathbb{R}$