ALGEBRA 1 — 30 NOV 2018

Note Title 11/30/2018

Estensioni di campi.

$K \subseteq F$ campi.

$\alpha \in F$

- α algebrico su K : $\exists\, f(x) \in K[x]$ $f \neq 0$ tale che $f(\alpha) = 0$.
- α trascendente su K : $\forall\, f(x) \in K[x]$ $f \neq 0$ $f(\alpha) \neq 0$.

In alternativa, possiamo considerare

$$\phi : K[x] \to F \qquad \text{OMOMORFISMO}.$$
$$f(x) \mapsto f(\alpha)$$

α algebrico $\iff$ $\ker \phi \neq \{0\}$.

L'immagine di ϕ è $K[\alpha] \subseteq F$
dove $K[\alpha] = \{f(\alpha) \mid f \in K[x]\}$.

$K[\alpha]$ è un dominio d'integrità. $(\subseteq F)$

$\ker \phi = (\mu_\alpha(x))$

$$K[x]/(\mu_\alpha(x)) \hookrightarrow K[\alpha]$$

$(\mu_\alpha(x))$ è un ideale PRIMO. $\neq 0$

$(\mu_\alpha(x))$ è un ideale MASSIMALE

$K[x]/(\mu_\alpha(x))$ è un campo $\Rightarrow K(\alpha)$ è un campo.

Notazione $K[\alpha] = K(\alpha)$

$K[\alpha]$: MIN. SOTTOANELLO di F che contiene K e α

$K(\alpha)$: MINIMO SOTTOCAMPO di F che contiene K e α.

$[K(\alpha) : K] = d$ (grado dell'estensione
$=$ dim $K(\alpha)$ come spazio vettoriale su K)
$=$ deg $\mu_\alpha(x)$ (c'è una base data da
$1, \alpha, \dots, \alpha^{d-1}$)

Teo (senza dimostrazione) Per ogni campo K esiste un campo algebricamente chiuso che lo contiene

Es. $K = \mathbb{R}$: Tesi fondam. $\mathbb{C} \supseteq \mathbb{R}$.

"Dim": Sia $f(x) \in \mathbb{C}[x]$ deg $f > 0$.

Considero la funzione

$$\phi : \mathbb{C} \to \mathbb{R}_+ = \{x \in \mathbb{R} \mid x \geq 0\}$$
$$\alpha \mapsto |f(\alpha)|$$

ϕ è continua

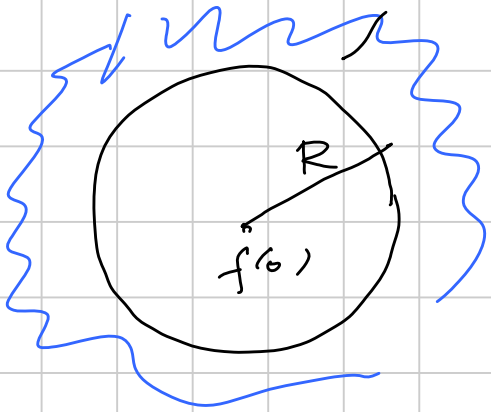
Dimostriamo che ϕ ha un minimo.

$f(x) = c_n z^n + \dots$

Poniamo $|z| = R$

Per $R \to +\infty$ $\quad |f(z)| = |c_n| R^n + O(R^{n-1})$

$\to +\infty$



I valori nella zona blu sono "grandi".

$R > |f(0)|$.

Quindi $\inf_{z \in \mathbb{C}} |f(z)| = \inf_{|z| \le R} |f(z)| = \min_{|z| \le R} |f(z)|$

Vogliamo vedere che $\min = 0$.

Supponiamo per assurdo di no.

Normalizziamo:

① posso supporre (a meno di traslazione) che il min sia $|f(0)|$

② posso supporre (a meno di moltiplicare per una costante) che $|f(0)| = 1$.

$$f(z) = 1 + c_k z^k + c_{k+1} z^{k+1} + \dots$$

$$\boxed{c_k \neq 0}.$$

Si sa risolvere $c_k z^k = -1$

Sol.: w

$c_k w^k = -1$

$t \in \mathbb{R}_+$

$c_k (tw)^k = -t^k$.

$f(tw) = 1 - t^k + o(t^{k+1})$

< 1

ASSURDO.

$\mathbb{F}_p$: Posso prendere $\bigcup_{n \geq 1} \mathbb{F}_{p^n} = \Omega$ (*)

(*) denota un campo algebricamente chiuso (è un campo).

Alg. chiuso:

$f(x) \in \Omega[x]$ $\quad d = \deg f > 0$

$f(x) \in \mathbb{F}_{p^n}[x]$ $\quad$ per n opportuno

Se $f(x) = f_1(x) \cdots f_r(x)$ è la sua fattorizzazione, con $\deg f_i = d_i$.

Una radice di $f_i(x)$ (= radice di f) appartiene $\mathbb{F}_{p^{n d_i}} \subseteq \Omega$.

Differenza fra i due casi:

- $\mathbb{C}$ non è algebrico su $\mathbb{Q}$ (CARDINALITÀ)
- Ω è algebrico su $\mathbb{F}_p$. (OVVIO)

Al posto di $\mathbb{C}$ stesso si prende

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

Estensioni finite ed estensioni algebriche.

Def 1 Un'estensione di campi $K \subseteq F$ (oppure F/K) si dice FINITA se $[F:K]$ è finito.

Def 2 Un'estensione di campi F/K si dice algebrica se ogni elemento di F è algebrico su K.

Proposizione 1 FINITA $\Rightarrow$ ALGEBRICA

$[F:K]=n$ $\quad \alpha \in F$

$1, \alpha, \alpha^2, \dots, \alpha^n$ sono

$n+1$ vettori $\rightarrow$ linearmente dipendenti su K.

$c_0 + c_1\alpha + \dots + c_n\alpha^n = 0$ $\quad c_i$ non tutti nulli

Proposizione 2 $K \subseteq F \subseteq E$ $\quad F/K, E/F$ finite

$\Rightarrow [E:K]$ è finito (1) (2)

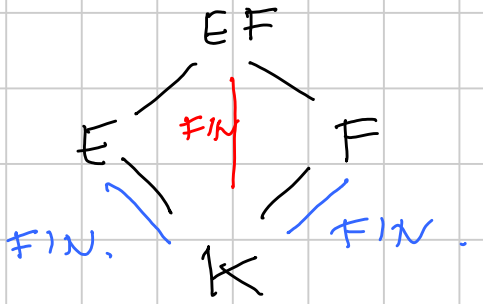
(3) $[E:K] = [E:F][F:K]$

Base (1) $\alpha_1, \dots, \alpha_n$

Base (2) $\beta_1, \dots, \beta_m$

$\Rightarrow$ Base (3) $\{\alpha_i \beta_j\}$.

Proposizione 3



$EF = E(F) = F(E)$

"composto" dei due

FIN + FIN $\Rightarrow$ FIN.

$[EF:F] \leq [E:K]$

Proposizione 4 Perché F/K sia algebrica è sufficiente che F sia generato su K da un insieme di elementi algebrici su K

$S = \{\alpha_i\}_{i \in I}$ $\quad K[S]$ polinomi negli α_i

$F = K(S)$

monomio $\quad c\,\alpha_{i_1}^{h_1} \cdots \alpha_{i_r}^{h_r}$

polinomio = somma di monomi

Basta vedere che somma e prodotto di elementi algebrici su K sono algebrici su K

$\alpha, \beta \qquad \alpha+\beta, \alpha\cdot\beta \in K(\alpha,\beta)$

composto di estensioni finite $\Rightarrow$ est. finita

$\Rightarrow$ est. algebrica.

Proposizione 5 $\quad K \subseteq E \subseteq F \quad E/K$ alg. + F/E alg.

$\Rightarrow F/K$ alg.

"Traccia di dim": $\quad \alpha \in F$ è algebrico su E

$\exists\, c_n, c_{n-1}, \dots, c_0 \in E$ non tutti nulli tali che

$c_n \alpha^n + c_{n-1}\alpha^{n-1} + \dots + c_0 = 0$.

Basta considerare il sottocamp. di E definito da

$E_0 = K(c_n, c_{n-1}, \dots c_0)$

$\to E_0/K$ è finita perché composto di est. finite.

$K \subseteq E_0 \subseteq E_0(\alpha)$ finita $\Rightarrow$ algebrica.

finita

Ricordiamo che i polinomi irriducibili $\in \mathbb{Q}[X]$ oppure a $\mathbb{F}_p[X]$ hanno radici distinte.

(criterio della derivata)

Per $\mathbb{Q}$ o in generale per un camp. di caratteristica zero $\quad \deg f = n \quad \deg f' = n-1$

Per $\mathbb{F}_p$ o anche per $\mathbb{F}_{p^k}$, tutto torna come prima se $\deg f' < \deg f$.

Resta il caso $f' = 0$.
Però questo succede soltanto se $f(x)$ è della forma

$$f(x) = c_n x^{np} + c_{n-1} x^{(n-1)p} + \dots + c_0$$

(cioè compaiono solo monomi di grado multiplo di p).

Se $f(x) \in \mathbb{F}_p[x]$ ho $c_i = c_i^p$

$$f(x) = c_n^p x^{np} + \dots + c_0^p$$
$$= (c_n x^n + \dots + c_0)^p$$

NON IRRIDUCIBILE

In generale, $f(x) \in \mathbb{F}_{p^k}[x]$
osservo che

$$\phi : \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$$
$$\alpha \mapsto \alpha^p$$

è un isomorfismo. (in particolare è surjettivo)
Avrò comunque $e_i = d_i^p$

$$f(x) = d_n^p x^{pn} + \dots + d_0^p$$
$$= (d_n x^n + \dots + d_0)^p$$

NON IRRIDUCIBILE

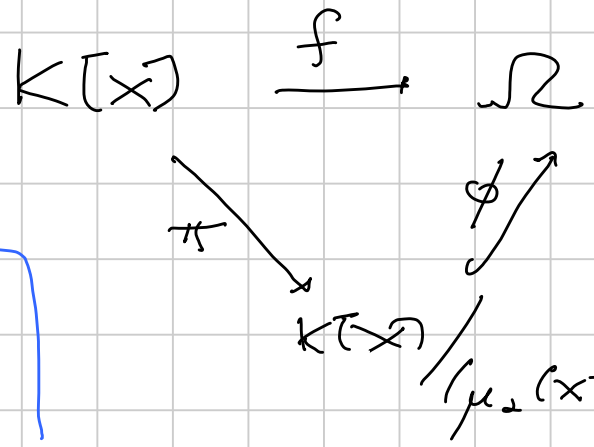
OMOMORFISMI DA $K(\alpha) \to \Omega$
dove Ω è algebricamente chiuso contenente K e $\alpha \in \Omega$ è algebrico su K.

Abbiamo $K(\alpha) \cong K[x] / (\mu_\alpha(x))$

OSS. BANALE Un omomorfismo definito in un campo è o nullo o iniettivo.
(Gli ideali sono $\{0\}$ e il campo stesso).

Gli omomorfismi interessanti sono quelli iniettivi.

Teorema.



Voglio che
$\ker f = (\mu_\alpha(x))$.

Considerando dapprima il caso $K = \mathbb{Q}$.
In questo caso abbiamo $f|_{\mathbb{Q}} =$ identità (inclusione).

Se $f(X) = \gamma$, allora
per ogni polinomio $p(X)$ si ha
$$f(p(x)) = p(\gamma)$$
$$p(X) = c_n X^n + c_{n-1} X^{n-1} + \dots + c_0$$
$$f(p(x)) = f(c_n) f(x)^n + f(c_{n-1}) f(x)^{n-1} + \dots + f(c_0)$$
$$= c_n f(x)^n + c_{n-1} f(x)^{n-1} + \dots + c_0$$
$$= c_n \gamma^n + c_{n-1} \gamma^{n-1} + \dots + c_0$$
$$= p(\gamma).$$

Voglio che $\mu_\alpha(X) \in \ker f$
$$f(\mu_\alpha(x)) = \mu_\alpha(\gamma) = 0.$$
(Condizione sufficiente per avere $f \not\equiv 0$)

Ci sono tante possibilità per γ quante è $\deg \mu_\alpha(x)$

2° caso K qualsiasi, ma considero solo gli automorfismi f tali che $f|_K = \mathrm{Id}_K$.

Se $x \mapsto y$
ci sono di nuovo tante possibilità per y quante è $\deg \mu_x(X)$.