ARITMETICA 14 DIC 2017

Note Title 12/14/2017

[Complementi sulle estensioni algebriche e sui polinomi irriducibili.

Ricordiamo che, se $f(X) \in \mathbb{Q}[X]$ con $\deg f = n$ allora esiste una fattorizzazione

$$f(X) = c\,(X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n)$$

in $\mathbb{C}[X]$.

Se K è un campo qualsiasi, esiste (TEO. DIFFICILE) un campo Ω (algebricamente chiuso) tale che, se $f(X) \in K[X]$ (con $\deg f = n$) allora esiste una fattorizzazione

$$f(X) = c\,(X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n)$$

in $\Omega[X]$.

Molteplicità di una radice.

Def. Una radice α di $f(X)$ ha molteplicità m se

$$(X-\alpha)^m \mid f(X) \quad \text{ma} \quad (X-\alpha)^{m+1} \nmid f(X)$$

Con questa definizione, posso riscrivere la fattorizzazione di $f(X)$ (in $\mathbb{C}[X]$ o in $\Omega[X]$) nella forma

$$f(X) = c\,(X-\alpha_1)^{m_1}(X-\alpha_2)^{m_2}\cdots(X-\alpha_k)^{m_k}$$

dove $m_1, \dots, m_k$ sono le molteplicità delle radici $\alpha_1, \dots, \alpha_k$.
Abbiamo che, se $\deg f = n$, allora

$$n = m_1 + m_2 + \dots + m_k.$$

<u>Def.</u> Una radice α di un polinomio $f(X)$ si dice una radice MULTIPLA se la sua molteplicità m è > 1.
Se invece $m = 1$, α si dice una radice SEMPLICE.

CRITERIO DELLA DERIVATA

<u>Prop.</u> Sia $f(X) \in K[X]$ e sia $\alpha \in \Omega$ una radice di $f(X)$.
(Caso principale: $K = \mathbb{Q}$, $\Omega = \mathbb{C}$)
Allora
α è una radice MULTIPLA di $f(X) \iff f'(\alpha) = 0$
dove $f'(X)$ è la derivata di $f(X)$.

<u>Dim.</u> m = molteplicità della radice α

$$f(X) = (X-\alpha)^m g(X)$$

con $\boxed{g(\alpha) \neq 0}$

$$f'(X) = m(X-\alpha)^{m-1} g(X) + (X-\alpha)^m g'(X)$$

$$f'(\alpha) = m(X-\alpha)^{m-1} g(X) + 0.$$

$\boxed{g(\alpha) \neq 0}$

Quindi $f'(\alpha)=0 \iff m-1>0$ ossia $m>1$
(α radice multipla).

<u>Teo</u>. Sia $f(X) \in \mathbb{Q}[X]$ un polinomio IRRIDUCIBILE.
Allora $f(X)$ ha tutte radici <u>semplici</u>.
(cioè, se $\deg f = n$, f ha n radici DISTINTE).

<u>Dim.</u> Supponiamo, per assurdo, che α sia una radice MULTIPLA di $f(X)$
Criterio della derivata $\Rightarrow$ α è radice anche di $f'(X)$

Quindi α è radice di $(f(X), f'(X))$

Sto usando implicitamente Ruffini
$X-\alpha \mid f(X)$ $\quad$ $X-\alpha \mid f'(X)$

Questo ha grado $<$ $\deg f(X)$.
perché se $\deg f(X)=n$, allora $\deg f'(X)=n-1$.

$f(X) = a_n X^n + \dots$ $\quad$ $f'(X) = n a_n X^{n-1}$
$a_n \neq 0$ $\quad$ $\boxed{n a_n \neq 0}$

Siccome $f(X)$ è irriducibile, allora
$f(X) = \text{cost} \cdot \mu_\alpha(X)$ (pol. minimo di α su K).
e quindi non ci sono polinomi di grado $<$ $\deg f(X)$
che si annullano in α.
Se avessimo $X-\alpha \mid f'(X)$ avremmo
un polinomio di grado $<$ $\deg f$ che si annulla
in α. VIETATO.

Si può generalizzare?

$\mathbb{Q} \to K$?

Sì, se $\operatorname{char} K = 0$. In particolare,

sì, se $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$.

CAMPI FINITI

<u>Esempi:</u> $\mathbb{Z}/p\mathbb{Z}$ con p primo.

(Invece, se m NON E' un numero primo, allora $\mathbb{Z}/m\mathbb{Z}$ NON E' un campo).

Esistono altri campi finiti al di fuori di questi?

Supponiamo che F sia un campo finito.

$0 \in F$, $1 \in F$.

$\langle 1 \rangle$ = sottogruppo additivo generato da 1.

$= \{ k \cdot 1 \mid k \in \mathbb{Z} \}$

$\cong \begin{cases} \mathbb{Z} & \text{NO (INFINITO)} \\ \mathbb{Z}/m\mathbb{Z} \end{cases}$

m <u>deve essere primo</u> perché altrimenti già in $\mathbb{Z}/m\mathbb{Z} \subseteq F$ ci sono divisori di zero (non banali).

Quindi $F \supseteq \mathbb{Z}/p\mathbb{Z}$ (con p primo).

$\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$

F è uno spazio vettoriale su $\mathbb{F}_p$.

F finito $\Rightarrow$ F ha una base su $\mathbb{F}_p$ composta da un numero finito di elementi

$\mathcal{B} = \{ \alpha_1, \dots, \alpha_n \}$ base

$$F = \{ c_1\alpha_1 + c_2\alpha_2 + \dots + c_n\alpha_n \mid c_i \in \mathbb{F}_p \}$$

$$|F| = p^n.$$

Dato p primo e $n \geq 1$, esiste un campo con p^n elementi?

$\boxed{\mathbb{F}_p \subseteq \Omega}$ algebricamente chiuso
(Ω contiene le radici dei poli $\in \mathbb{F}_p[x]$).

$$f(X) = X^{p^n} - X \qquad \deg f = p^n.$$

n° di radici di $f(X) \leq p^n$.

$\boxed{\text{Le radici sono tutte distinte}}$ (criterio della derivata):

$$f'(X) = \underset{\overset{\shortparallel}{0}}{p^n} X^{p^n - 1} - 1 = -1$$

$f'(X)$ NON HA RADICI

$\Rightarrow$ nessuna radice comune fra $f(X)$ e $f'(X)$

Le radici $F = \{\alpha_1, \alpha_2, \dots, \alpha_{p^n}\}$ sono un insieme di p^n elementi.

Queste radici formano un CAMPO.

$+$ $\quad 0 \in F$

$\alpha \in F, \beta \in F \Rightarrow \alpha + \beta \in F$

$(\alpha^{p^n} - \alpha = 0 \Rightarrow \alpha^{p^n} = \alpha, \quad \beta^{p^n} = \beta$

$$(\alpha+\beta)^{p^n} = \alpha^{p^n}+\beta^{p^n} = \alpha+\beta$$

$$(-\alpha)^{p^n} = -\alpha^{p^n} = -\alpha \qquad (p=2 \quad -1=1)$$

$\alpha \in F$, $\beta \in F \Rightarrow \alpha\beta \in F$

$\alpha^{p^n}=\alpha \quad \beta^{p^n}=\beta \Rightarrow (\alpha\beta)^{p^n} = \alpha\beta.$

$\alpha \neq 0$, $\alpha \in F \Rightarrow \alpha^{-1} \in F$

$\alpha^{p^n}=\alpha \Rightarrow (\alpha^{-1})^{p^n} = \alpha^{-p^n} = (\alpha^{p^n})^{-1}$
$= \alpha^{-1}.$

<u>Prop</u> Fissato Ω algebricamente chiuso tale che $\mathbb{F}_p \subset \Omega$, esiste un solo campo F con $\mathbb{F}_p \subseteq F \subseteq \Omega$ con p^n elementi.

<u>Dim.</u> Se $|F| = p^n$ allora $F = \{0\} \cup F^*$ dove $|F^*| = p^n - 1$.

0 è radice del polinomio x

se $\alpha \in F^*$, allora $\alpha^{p^n-1} = 1$, cioè α è radice di $X^{p^n-1}-1$

$\Rightarrow$ tutti gli elementi di F sono radici del pol

$$x(x^{p^n-1}-1) = x^{p^n} - x.$$

Quindi la costruzione fatta è l'unica possibile

<u>Notazione</u> L'UNICO CAMPO con p^n elementi si denota con $\mathbb{F}_{p^n}$.

<u>Attenzione</u>: Se $n > 1$, $\mathbb{F}_{p^n} \neq \mathbb{Z}/p^n\mathbb{Z}$.

Struttura di $\mathbb{F}_{p^n}$ rispetto a $+$.

($\mathbb{F}_{p^n}$ è s.v. su $\mathbb{F}_p$ di dimensione n)

$$\mathbb{F}_{p^n} \underset{+}{\cong} \mathbb{F}_p^n \cong (\mathbb{Z}/p\mathbb{Z})^n$$

Struttura di $\mathbb{F}_{p^n}^*$ rispetto a $\odot$.

Risultato: $\mathbb{F}_{p^n}^*$ è CICLICO, $\forall p, \forall n$

$$\Downarrow$$

$(\mathbb{Z}/p\mathbb{Z})^*$ è CICLICO $\quad (n=1)$