CAMPI : INTRODUZIONE

Note Title 12/7/2017

Complementi sugli anelli

Def. Siano A_1, A_2 anelli. Una funzione $f: A_1 \to A_2$ è detta OMOMORFISMO (DI ANELLI) se

- è un omomorfismo di gruppi additivi, ovvero

$$f(x+y) = f(x) + f(y) \qquad \forall x, y \in A_1$$

- rispetta il prodotto:

$$f(xy) = f(x)\, f(y) \qquad \forall x, y \in A_1$$

$$\left(\cdot \quad f(1_{A_1}) = 1_{A_2} \right)$$

Esempi (1) La riduzione modulo n:

$$\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$$

(2) La proiezione al quoziente: se I è un ideale di un anello A, $A \xrightarrow{\pi} A/I$ è un omomorfismo

(3) Sia A un anello (con unità). Allora c'è un omomorfismo

$$\begin{aligned} \mathbb{Z} &\xrightarrow{\varphi} A \\ n &\longmapsto \underbrace{1+1+\dots+1}_{n \text{ volte}} \\ -n &\longmapsto -(1+\dots+1) \end{aligned}$$

$$\varphi(n)\,\varphi(m) = \underbrace{(1+\dots+1)}_{n}\underbrace{(1+\dots+1)}_{m} = \underbrace{1+\dots+1}_{mn} = \varphi(mn)$$

(4) $\alpha \in \mathbb{C}$, $A_1 = \mathbb{Q}[x]$, $A_2 = \mathbb{C}$

$$\begin{aligned} \mathrm{val}_\alpha : \mathbb{Q}[x] &\longrightarrow \mathbb{C} \\ p(x) &\longmapsto p(\alpha) \end{aligned}$$

Più generalmente: $A[x] \longrightarrow A$, $p(x) \longmapsto p(\alpha)$ con $\alpha \in A$ fissato

o ancora, se $B \subseteq A$, $B[x] \longrightarrow A$, $p(x) \longmapsto p(\alpha)$

Oss Dato $f : A_1 \longrightarrow A_2$ omomorfismo,

$$\ker f = \{ a \in A, \mid f(a) = 0 \}$$

è un ideale di A,

PROP. Sia K un campo, $f(x) \in K[x]$,

$A = K[x]/(f(x))$. Un elemento $a \in A$,

che rappresentiamo come $p(x) + (f) = \overline{p(x)}$,

è:

(1) invertibile $\iff$ $(p(x), f(x)) = (1) = K[x]$

(2) divisore di 0 $\iff$ $(p(x), f(x)) \neq (1)$

(3) nilpotente $\iff$ $p(x)$ è divisibile per ognuno dei fattori irriducibili di $f(x)$

Dim (1) idea: identità di Bézout:

$\Leftarrow$ $\exists\, a(x), b(x)$ t.c. $a(x)p(x) + b(x)f(x) = 1$

Passando modulo $f(x)$, $\overline{a(x)} \cdot \overline{p(x)} = \overline{1}$

$\Rightarrow$ $\overline{a(x)} \cdot \overline{p(x)} = \overline{1}$ (esiste $\overline{a(x)}$ per ipotesi)

$\Rightarrow$ $a(x)\,p(x) - 1$ si scrive $b(x)\,f(x)$

$\Rightarrow$ $a(x)\,p(x) - b(x)\,f(x) = 1$

(2) $\boxed{\Rightarrow}$ Un div. di 0 non è invertibile

$\boxed{\Leftarrow}$ $f(x) = d(x)\,f_1(x)$ con $\deg d(x) > 0$

$p(x) = d(x) \cdot p_1(x)$

Allora $\overline{p(x)} \cdot \overline{f_1(x)} = \overline{d(x)} \cdot \overline{p_1(x)} \cdot \overline{f_1(x)}$

$= \overline{f(x)} \cdot \overline{p_1(x)}$

$= 0$

Inoltre $\overline{f_1(x)} \neq \bar{0}$ perché $\deg f_1(x) < \deg f(x)$

(3) $\overline{p(x)}$ nilpotente $\Leftrightarrow$ $\exists n$ $\overline{p(x)}^n = \bar{0}$

$\Leftrightarrow$ $\exists n$, $a(x)$ t.c. $p(x)^n = f(x)\,a(x)$

fatt. unica $\Leftarrow$ ogni fattore primo di $f(x)$ divide $p(x)$.

$\blacksquare$

Corollario K campo, $f(x) \in K[x]$ $K[x]/(f(x))$ è un campo $\Leftrightarrow$ $f(x)$ è irriducibile

CAMPI

DEF Un anello K è detto **CAMPO** se è commutativo e $K^\times = K \setminus \{0\}$

(ovvero: $(K,+)$ gruppo abeliano,

$(K^\times, \cdot)$ ——————,

proprietà distributiva)

CARATTERISTICA K campo. Esiste un omomorf. di anelli

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\varphi} & K \\ 1 & \longmapsto & 1 \end{array}$$

$\ker(\varphi)$ $\begin{cases} (0) & \text{char}(K) = 0 \\ m\mathbb{Z} \quad m>0 & \text{char}(K) = m > 0 \end{cases}$

- $\text{char}(K) = 0 \Rightarrow \mathbb{Z} \subseteq K \overset{K \text{ campo}}{\Longrightarrow} \mathbb{Q} \subseteq K$

$K = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \dots$

- $\text{char}(K) = m > 0$: allora m è un numero primo.

Se per assurdo $m = ab$ con $a, b > 1$,

allora $\varphi(ab) = 0 \iff \varphi(a)\varphi(b) = 0$

$\Rightarrow \varphi(a)=0 \ \vee \ \varphi(b)=0$, perché K non ha divisori di zero non banali

$\Rightarrow a \in \ker\varphi$ oppure $b \in \ker\varphi = (m)$, assurdo perché $m > a, b$

Esempio $\mathrm{char}(K) \neq 6$: se vale

$$1+1+1+1+1+1=0$$

$$(1+1)(1+1+1)=0$$

quindi $\mathrm{char}(K)=2$ o $\mathrm{char}(K)=3$

Se $\mathrm{char}(K)=p$, allora $K \supseteq \mathbb{Z}/p\mathbb{Z}$

DEF $\mathbb{Z}/p\mathbb{Z}$ pensato come campo si denota $\mathbb{F}_p$

ESTENSIONI

Dati due campi F_1, F_2 con $F_1 \subseteq F_2$ si dice che F_2 è una ESTENSIONE di F_1

(con $x +_{F_1} y = x +_{F_2} y \quad \forall x, y \in F_1$

$$x \cdot_{F_1} y = x \cdot_{F_2} y \quad \forall x, y \in F_1 \Big)$$

Esempi $\mathbb{Q} \subseteq \mathbb{R}$, $\mathbb{R} \subseteq \mathbb{C}$

Oss Se $F_1 \subseteq F_2$ è un'estensione di campi, F_2 è uno spazio vettoriale su F_1.

Dim: $(F_2, +)$ è un gruppo additivo; c'è un prodotto per scalare $F_1 \times F_2 \longrightarrow F_2$ dato dalla struttura di campo. ∎

DEF Il GRADO di F_2 su F_1 ($F_1 \subseteq F_2$ est. di campi) è $\dim_{F_1}(F_2)$ come spazi vett.

Questo numero si denota $[F_2 : F_1] = \dim_{F_1}(F_2)$

Esempio $[\mathbb{C} : \mathbb{R}] = 2$ $\quad \mathbb{C} \simeq \mathbb{R}^2$ come S.V.

$$[\mathbb{C} : \mathbb{Q}] = +\infty$$

Esempio aritmetico

$$\mathbb{Q}(\sqrt{2}) = \{ a + b\sqrt{2} \mid a, b \in \mathbb{Q} \}$$

$\mathbb{Q}(\sqrt{2})$ è un anello (sotto anello di $\mathbb{R}$)

- $(\mathbb{Q}(\sqrt{2}), +)$ è un grp. abeliano: OK
- $\mathbb{Q}(\sqrt{2}) \times \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{R}$ ha img contenuta in $\mathbb{Q}(\sqrt{2})$

$$(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd) + \sqrt{2}(bc+ad)$$

- distrib.: OK

In realtà è anche un campo: devo fare vedere che ci sono gli inversi.

$$\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})} = \frac{a-b\sqrt{2}}{a^2-2b^2}$$

Siamo a posto purché $a^2-2b^2 \neq 0$: in effetti $a^2 = 2b^2$ con a, b razionali implica $a = b = 0$ (infatti: se $b=0 \Rightarrow a=0$; altrimenti $(a/b)^2 = 2$, ma $\sqrt{2} \notin \mathbb{Q}$).

$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ (base: $1, \sqrt{2}$)

Elementi algebrici e trascendenti

Sia $F_1 \subseteq F_2$ un'estensione di campi, $\alpha \in F_2$.

Dato $\alpha \in F_2$ posso definire $F_1(\alpha)$ = il più piccolo sottocampo di F_2 che contiene sia F_1 che α (= intersezione di tutti i sottocampi di F_2 contenenti α ed F_1)

(1) Può succedere che $F_1(\alpha) = F_2$

(2) se $K_1, K_2 \subseteq F_2$ sono campi t.c.

$F_1 \subseteq K_1, K_2$ e $\alpha \in K_1, K_2$, allora

$K_1 \cap K_2$ è un campo che contiene F_1 e α

Per vedere che $K_1 \cap K_2$ è un campo:

$$x, y \in K_1 \cap K_2 \overset{?}{\Longrightarrow} x+y \in K_1 \cap K_2$$

$$\left.\begin{array}{l} K_1 \text{ campo} \Rightarrow x+y \in K_1 \\ K_2 \text{ —} \Rightarrow x+y \in K_2 \end{array}\right\} \Rightarrow x+y \in K_1 \cap K_2$$

etc...

Esempio $\mathbb{Q} \subseteq \mathbb{R}$, $\alpha = \sqrt{2} \in \mathbb{R}$, $\mathbb{Q}(\sqrt{2})$ è il campo visto sopra

$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \Rightarrow a \in \mathbb{Q}(\sqrt{2}) \quad \forall a \in \mathbb{Q}$

$\sqrt{2} \in \mathbb{Q}(\sqrt{2}) \Rightarrow b\sqrt{2} \in \mathbb{Q}(\sqrt{2}) \quad \forall b \in \mathbb{Q}$

$\Downarrow$

$a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2}) \quad \forall a, b \in \mathbb{Q}$

$[\mathbb{Q}(\pi) : \mathbb{Q}] = +\infty$ (dim. tardo 1800)

DEF Sia $F_1 \subseteq F_2$ un'estensione di campi.

Un elemento $\alpha \in F_2$ si dice ALGEBRICO su F_1 se esiste un polinomio non nullo $f(x) \in F_1[x]$ t.c. $f(\alpha) = 0$. Se un tale polinomio non esiste, α si dice TRASCENDENTE

Es. $\mathbb{Q} \subseteq \mathbb{R}$: $1 + \sqrt{3}$ è algebrico, π è trasc.

POLINOMIO MINIMO $F_1 \subseteq F_2$ est. di campi, $\alpha \in F_2$. C'è un omomorfismo di anelli

$$\begin{aligned} \text{val}_\alpha : F_1[x] &\longrightarrow F_2 \\ p(x) &\longmapsto p(\alpha) \end{aligned}$$

Se $\ker(\text{val}_\alpha) = (0)$, vuol dire che non

ci sono polinomi ($\neq 0$) che si annullano in α, quindi α è trascendente

Nel caso $\ker V_\alpha \neq (0)$ $\Rightarrow$ $\ker V_\alpha = (f)$

I generatori di $\ker(V_\alpha)$ sono i polinomi di grado minimo contenuti in V_α

$\ker V_\alpha$ è un ideale di $F_1[X]$
ogni ideale è generato da un singolo elemento

Tra tutti gli f possibili, prendiamo quello

MONICO (= coeff di grado max uguale a 1):

si chiama il POLINOMIO MINIMO di α

Lo denotiamo $f_\alpha(x)$

Esempio $f_{\sqrt{2}}(x) = x^2 - 2$

$$V_{\sqrt{2}} : \mathbb{Q}[x] \longrightarrow \mathbb{R}$$
$$p(x) \longmapsto p(\sqrt{2})$$

$\ker V_{\sqrt{2}}$ NON CONTIENE polinomi di grado 1

contiene $3x^2 - 6$ di grado 2

Siccome $3x^2 - 6$ è di grado minimo in

$\ker(v_4)$, si ha $\ker(v_\alpha) = (3x^2 - 6)$

Rinormalizzando il coeff. di testa, $f_{\sqrt{2}}(x) = x^2 - 2$

Esempio Sia $f(x) = x^3 - x - 1$.

Sia $\alpha \in \mathbb{R}$ una radice di questo polinomio.

Vorrei dim che f è il polinomio minimo di α su $\mathbb{Q}$ $\quad (\mathbb{Q} \subseteq \mathbb{R},\ \alpha \in \mathbb{R})$

$$\begin{aligned} \mathrm{val}_\alpha : \mathbb{Q}[x] &\longrightarrow \mathbb{R} \\ p(x) &\longmapsto p(\alpha) \end{aligned}$$

(1) $\ker(\mathrm{val}_\alpha) \ni f(x)$ $\quad f(\alpha) = 0$ per definiz.

(2) $\ker(\mathrm{val}_\alpha) = (g)$ (con g di grado minimo)

(3) $g \mid f$ in $\mathbb{Q}[x]$, perché $f \in \ker v_4 = (g)$

(4) f è irriducibile : $x^3 - x - 1$ in $\mathbb{Q}[x]$

[$x^3 - x - 1$ irrid. in $\mathbb{Z}[x]$: modulo 2]

(5) (3) + (4) $\Rightarrow$ $f = g \cdot u$ con $u \in \mathbb{Q}^\times$

(6) $(f) = (g) = \ker V_\alpha$, f è monico $\Rightarrow f =$ pol. min di α

DEF Grado: sia $F_1 \subseteq F_2$ un'estensione di campi, $\alpha \in F_2$ algebrico su F_1.

Grado di $\alpha = \deg(f_\alpha(x))$ $\left(= [F_1(\alpha) : F_1] \right)$