ESERCITAZIONE 18 - 11 - 2020

· Interpolazione col TCR

Siano $a_1 < a_2 < \dots < a_n \in \mathbb{Q}$, [devono essere DISTINTI]
$b_1, b_2, \dots, b_n \in \mathbb{Q}$

Allora $\exists$ un unico polinomio $p \in \mathbb{Q}[x]$ di grado $\leq n-1$ t.c.

$$p(a_i) = b_i \quad \forall i = 1, \dots, n$$

OSS: $p_1, p_2 \in \mathbb{Q}[x]$ di grado qualsiasi t.c. $p_1(a_i) = b_i$
$p_2(a_i) = b_i$

Allora $p_2 - p_1 \in \mathbb{Q}[x]$ si annulla in $x = a_1, \dots, a_n$

$\Rightarrow$ Per Ruffini $p_2 - p_1$ è div. per $(x - a_i)$ $\forall i$

Inoltre tali $(x - a_i)$ sono tutti coprimi (evidentemente)

$$\Rightarrow \prod (x - a_i) \mid p_2 - p_1$$

$\Rightarrow$ Pensare ai pol. p tali che $p(a_i) = b_i$ è come considerare le classi di resto mod $\prod (x - a_i)$

$$\text{Sia } A := \frac{\mathbb{Q}[x]}{\left(\prod (x - a_i)\right)} = \frac{\mathbb{Q}[x]}{(q)}, \qquad \prod (x-a_i) = q$$

Per definizione $(q) = \prod I_i$ dove $I_i := (x - a_i)$

$$\Rightarrow A = \frac{\mathbb{Q}[x]}{I_1 \cdots I_n}$$

Inoltre $I_i + I_j = (x - a_i, x - a_j) = (x - a_i, (x - a_i) - (x - a_j))$

$$= (x-a_i,\ \underbrace{a_i-a_j}_{\substack{\text{se } i\neq j \\ \text{questo } \in \mathbb{Q}^\times}}) = (1)$$

Per il TCR segue che

$$A = \frac{\mathbb{Q}[x]}{(q)} = \frac{\mathbb{Q}[x]}{I_1 \cdots I_n} \simeq \prod_{i=1}^{n} \frac{\mathbb{Q}[x]}{I_j}$$

$$\frac{\mathbb{Q}[x]}{(q)} \updownarrow \{\text{pol di grado} \leq n-1\}$$

$$\prod_{i=1}^{n} \frac{\mathbb{Q}[x]}{I_j} \cong \prod_{i=1}^{n} \mathbb{Q}(a_i) \cong \prod_{i=1}^{n} \mathbb{Q}$$

Oss $\frac{\mathbb{Q}[x]}{(q)} \xrightarrow{\Psi} \prod \frac{\mathbb{Q}[x]}{(x-a_i)} \xrightarrow{\pi\varphi_i} \prod \mathbb{Q}$

Dunque la classe di un polinomio r in $\frac{\mathbb{Q}[x]}{(q)}$ viene mandata in:

$$r+(q) \longmapsto (r+(x-a_1), \dots, r+(x-a_n))$$

$$\downarrow$$

$$(r(a_1), \dots, r(a_n))$$

Siccome questa composizione è un isomorfismo, dato $(b_1, \dots, b_n) \in \mathbb{Q}^n$ esiste un'unica classe $r+(q)$ t.c.

$$(r(a_1), \dots, r(a_n)) = (\Psi \circ \pi\varphi_i)(r+(q)) = (b_1, \dots, b_n)$$

Segue la tesi perché ogni classe mod. (q) contiene uno e un solo pol. di grado $\leq n-1$. $\blacksquare$

Radicali di ideali

A comm., $I, J \triangleleft A$

1) $IJ \subseteq I \cap J$

2) $\sqrt{\sqrt{I}} = \sqrt{I}$

3) $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$

OSS: $IJ = \{ i_1 j_1 + \dots + i_n j_n : i_1, \dots, i_n \in I, j_1, \dots, j_n \in J \}$

1) $\forall i \in I, j \in J$ la propr. di ass. di I e J dà che

$$i \cdot j \in I \quad e \quad i \cdot j \in J \implies ij \in I \cap J$$

Essendo $I \cap J$ ideale segue che la somma dei vari add. sta in $I \cap J$

2) $\sqrt{I} = \{ a \in A : \exists n \geq 1 \text{ intero t.c. } a^n \in I \}$

OSS: $I_1 \subseteq I_2 \implies \sqrt{I_1} \subseteq \sqrt{I_2}$

Infatti se $a^n \in I$ per qualche n, allora $a^n \in I_2$

OSS 2: $I \subseteq \sqrt{I}$: infatti se $a = a^1 \in I$ una potenza di a appartiene ad $I \implies a \in \sqrt{I}$

$$\implies \sqrt{I} \subseteq \sqrt{\sqrt{I}}$$

Viceversa: $a \in \sqrt{\sqrt{I}}$ se $\exists n > 0$ t.c. $a^n \in \sqrt{I}$, cioè

$$\exists m > 0 \text{ t.c. } (a^n)^m = a^{nm} \in I$$

Ma allora $a \in \sqrt{I}$ e quindi $\sqrt{I} = \sqrt{\sqrt{I}}$. $\blacksquare$

3) $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$

$IJ \subseteq I \cap J \Rightarrow \sqrt{IJ} \subseteq \sqrt{I \cap J}$

Viceversa, se $a \in \sqrt{I \cap J}$ allora $\exists n$ t.c. $a^n \in I \cap J$.

Tesi: $\exists m$ t.c. $a^m \in IJ$

Basta prendere $m = 2n$:

$$a^{2n} = \underset{I \cap J \subseteq I}{\underset{\cap}{a^n}} \cdot \underset{I \cap J \subseteq J}{\underset{\cap}{a^n}} \in I \cdot J$$

- $\dfrac{\mathbb{Q}[x,y]}{(xy-1)}$ è un dominio

1ª Strada: $\mathbb{Q}[x,y]$ è UFD; $(xy-1)$ è primo $\Leftrightarrow$ $xy-1$ è el. primo $\overset{UFD}{\Longleftrightarrow}$ $xy-1$ irriducibile e questo si vede subito con i gradi

2ª Strada: in $A = \dfrac{\mathbb{Q}[x,y]}{(xy-1)}$ si ha $\bar{x} \cdot \bar{y} = \bar{1}$, cioè $\bar{x}$ è invertibile in A.

$\rightsquigarrow$ Forse $A \simeq S^{-1}\mathbb{Q}[x]$ con $S = \{x^i : i \geq 0\}$

PROPRIETÀ UNIVERSALE DELLA LOCALIZZAZIONE

Sia $\varphi : A \to B$, $S \subseteq A$ parte molt. Se $\underbrace{\varphi(S) \subseteq B^\times}_{\text{ogni el. di } S \text{ viene mandato in un invertibile di } B}$ allora φ si estende univocamente ad una $\psi : S^{-1}A \to B$ t.c.

$$\begin{tikzcd}
A \arrow[rr, "\varphi"] \arrow[dr, "a \mapsto \frac{a}{1}"'] & & B \\
& S^{-1}A \arrow[ur, dashed, "\exists!\psi"'] &
\end{tikzcd}$$

commuta.

DIM Se ψ esiste, è unica.

Infatti $\varphi = \psi \circ \iota$ mi dice che $\forall a \in A$: $\psi\left(\frac{a}{1}\right) = \varphi(a)$.

Inoltre

$$1_B = \psi(1) = \psi\left(\frac{s}{s}\right) = \psi(s) \cdot \psi\left(\frac{1}{s}\right) \Rightarrow \psi\left(\frac{1}{s}\right) = \psi(s)^{-1} = \varphi(s)^{-1}$$

Dunque $\psi\left(\frac{a}{s}\right) = \varphi(a)\varphi(s)^{-1}$.

Tale mappa è ben definita, omomorfismo di anelli.

BUONA DEF Siano $\frac{a}{s}, \frac{a'}{s'}$ t.c. $as' = a's$. Allora

$$\psi\left(\frac{a}{s}\right) = \varphi(a)\varphi(s)^{-1} \; ; \; \psi\left(\frac{a'}{s'}\right) = \varphi(a')\varphi(s')^{-1}$$

$$\Rightarrow \varphi(a)\varphi(s)^{-1} \overset{?}{=} \varphi(a')\varphi(s')^{-1}$$

$$\Leftrightarrow \underbrace{\varphi(a)\varphi(s')}_{\varphi(as')} = \underbrace{\varphi(a')\varphi(s)}_{\varphi(a's)}$$

$$\varphi(as') \overset{\checkmark}{=} \varphi(a's)$$

OMOMORFISMO Non mi va

Tornando a $\dfrac{\mathbb{Q}[x,y]}{(xy-1)} \simeq S^{-1}\mathbb{Q}[x]$

$$\begin{aligned} \alpha : \mathbb{Q}[x,y] &\longrightarrow S^{-1}\mathbb{Q}[x] \\ p(x,y) &\longmapsto p\left(x, \tfrac{1}{x}\right) \end{aligned}$$

OSS: $\alpha(xy-1) = x\frac{1}{x} - 1 = 0 \Rightarrow (xy-1) \subseteq \operatorname{Ker}\alpha$

$$\begin{tikzcd} \mathbb{Q}[x,y] \arrow[rr] \arrow[dr] & & S^{-1}\mathbb{Q}[x] \\ & \dfrac{\mathbb{Q}[x,y]}{(xy-1)} \arrow[ur, "\bar{\alpha}"'] & \end{tikzcd}$$

$\bar{\alpha}(\bar{x}) = \alpha(x) = x$

$\bar{\alpha}(\bar{y}) = \alpha(y) = \frac{1}{x}$

$*\quad \beta : \mathbb{Q}[x] \longrightarrow \mathbb{Q}[x,y] \longrightarrow \mathbb{Q}[x,y]/(xy-1)$

$$p \longmapsto p \longmapsto p + (xy-1)$$

è omo. Inoltre $\beta(x^n)$ è invertibile, e il suo inverso è $\overline{y}^n$: $\beta(x^n) = x^n + (xy-1) = \overline{x}^n$

Dunque $\overline{x}^n \cdot \overline{y}^n = (\overline{x}\,\overline{y})^n = 1$

Per la proprietà univ. della localizzazione
$\exists!\ \overline{\beta} : S^{-1}\mathbb{Q}[x] \to \dfrac{\mathbb{Q}[x,y]}{(xy-1)}$

⌜ che posso applicare perché $\overline{x}^n$ è inv. in $\dfrac{\mathbb{Q}[x,y]}{(xy-1)}$ ⌟

t.c.

$$\begin{tikzcd}
\mathbb{Q}[x] \arrow[rr] \arrow[dr] & & \mathbb{Q}[x,y]/(xy-1) \\
& S^{-1}\mathbb{Q}[x] \arrow[ur, "\overline{\beta}"'] &
\end{tikzcd}$$

OSS: $\overline{\beta}(x) = \beta(x) = \overline{x}$

$$\overline{\beta}\left(\tfrac{1}{x}\right) = \beta(x)^{-1} = \overline{x}^{-1} = \overline{y}$$

REMAINDER: $\overline{\alpha}(\overline{x}) = x \quad , \quad \overline{\alpha}(\overline{y}) = \frac{1}{x}$

$$\begin{tikzcd}
\dfrac{\mathbb{Q}[x,y]}{(xy-1)} \arrow[r, bend left, "\overline{\alpha}"] & S^{-1}\mathbb{Q}[x] \arrow[l, bend left, "\overline{\beta}"]
\end{tikzcd}$$

Siccome $S^{-1}\mathbb{Q}[x]$ è generato da $x, \frac{1}{x}, \mathbb{Q}$ e analogamente

$$\frac{\mathbb{Q}[x,y]}{(xy-1)} \quad \text{è generato da } \bar{x}, \bar{y}, \mathbb{Q}.$$

$\Rightarrow$ Per verificare che $\bar{\alpha} \circ \bar{\beta} = id$, $\bar{\beta} \circ \bar{\alpha} = id$ basta farlo sui generatori

$$\begin{aligned} &\bar{\alpha} \circ \bar{\beta}(a) = a \quad \forall a \in \mathbb{Q} \\ &\bar{\alpha} \circ \bar{\beta}(x) = \bar{\alpha}(\bar{x}) = x \\ &\bar{\alpha} \circ \bar{\beta}\left(\tfrac{1}{x}\right) = \bar{\alpha}(\bar{y}) = \tfrac{1}{x} \end{aligned} \qquad \left\{ \begin{aligned} &\bar{\beta} \circ \bar{\alpha}(a) = a \quad \forall a \in \mathbb{Q} \\ &\bar{\beta} \circ \bar{\alpha}(\bar{x}) = \bar{\beta}(x) = \bar{x} \\ &\bar{\beta} \circ \bar{\alpha}(\bar{y}) = \bar{\beta}\left(\tfrac{1}{x}\right) = \bar{y} \end{aligned} \right.$$

$\Rightarrow$ $\bar{\alpha}$ e $\bar{\beta}$ sono isomorfismi e dunque

$$\frac{\mathbb{Q}[x,y]}{(xy-1)} \simeq S^{-1}\mathbb{Q}[x].$$

In particolare $\frac{\mathbb{Q}[x,y]}{(xy-1)} \simeq S^{-1}\mathbb{Q}[x]$ è un dominio in quanto localizzazione di un dominio, e quindi $(xy-1)$ è primo.

~ o ~ o ~ o ~

INTERI DI GAUSS

$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ è un ED.

($\Rightarrow$ PID, UFD)

$$\mathbb{Z}[i]^{\times} = \{\pm 1, \pm i\}$$

- Classificare i primi di $\mathbb{Z}[i]$

Introduciamo la norma $N : \mathbb{Z}[i] \longrightarrow \mathbb{N}$

$$a + bi \longmapsto a^2 + b^2$$

OSS: N è moltiplicativa: $\forall x, y \in \mathbb{Z}[i]$: $N(xy) = N(x)N(y)$

① Sia $p \in \mathbb{Z}$ primo $\equiv 3\ (4)$. Mostriamo che è primo in $\mathbb{Z}[i]$

Siccome $\mathbb{Z}[i]$ è UFD, basta mostrare che p è irriducibile.

Sia $p = (a+bi)(c+di)$ e mostriamo che

$$a+bi \in \mathbb{Z}[i]^\times \quad \vee \quad c+di \in \mathbb{Z}[i]^\times$$

$$p^2 = N(p) = (a^2+b^2)(c^2+d^2)$$

$$\Rightarrow a^2+b^2 \mid p^2 \Rightarrow a^2+b^2 \in \{1; p; p^2\}$$

- $a^2+b^2=1$ Allora essendo $a, b \in \mathbb{Z}$ si ha che
$$(a=0 \text{ e } b=\pm 1) \vee (a=\pm 1 \text{ e } b=0)$$
$$\Rightarrow a+bi \in \mathbb{Z}[i]$$

- $a^2+b^2=p^2$ Allora $c^2+d^2=1 \Rightarrow c+di \in \mathbb{Z}[i]$

- $a^2+b^2=p$ Se $p \mid b$ allora $p \mid a^2 \Rightarrow p \mid a$
dunque $p^2 \mid a^2$, $p^2 \mid b^2 \Rightarrow p^2 \mid a^2+b^2 = p$. ASSURDO

Ma se $p \nmid b$ trovo

$\to$ b è inv. perché $p \nmid b$

$$a^2+b^2 \equiv 0\ (p) \iff a^2 \equiv -b^2\ (p)$$
$$\iff \frac{a^2}{b^2} = \left(\frac{a}{b}\right)^2 \equiv -1\ (p)$$

cioè -1 è un quadrato mod p.

CRITERIO DI EULERO: $a \not\equiv 0\ (p)$ è un quadrato mod p sse $a^{\frac{p-1}{2}} \equiv 1\ (p)$.

DIM $\mathbb{F}_p^\times$ è ciclico $\rightsquigarrow$ $\mathbb{F}_p^\times \cong \mathbb{Z}/_{(p-1)}\mathbb{Z}$.

I quadrati sono le soluzioni di

$$\frac{p-1}{2} \cdot a \equiv 0 \quad (p-1)$$

Dunque in notazione esponenziale se e solo se

$$a^{\frac{p-1}{2}} \equiv 1 \quad (p)$$

$\blacksquare$

OSS: -1 è un quadrato mod p sse $(-1)^{\frac{p-1}{2}} \equiv 1 \ (p)$

Se $p \equiv 3 \ (4) \iff p = 4k+3$, allora

$$(-1)^{2k+1} = -1 \not\equiv 1 \ (p)$$

Dunque $N(a+bi) \neq p \neq N(c+bi)$

Questo mostra che p è irriducibile e quindi primo. $\blacksquare$

② Se $p \equiv 1 \ (4)$, come si fattorizza p in irr. in $\mathbb{Z}[i]$?

ES: $5 = (2+i)(2-i) = 4 - i^2 = 4+1 = 5$

$13 = (3+2i)(3-2i)$

$17 = (4+i)(4-i)$

CONGETTURA: $p = (a+bi)(a-bi)$ irr.

(1) p non è primo in $\mathbb{Z}[i] \iff p \equiv 1 \ (4)$

Se $p \equiv 1 \ (4)$ allora -1 è un quadr. mod p, in quanto

$$(-1)^{\frac{p-1}{2}} \equiv (-1)^{\frac{(4k+1)-1}{2}} = (-1)^{2k} \equiv 1 \quad (p)$$

Ciò significa che $\exists\, n \in \mathbb{Z}$ t.c. $n^2 \equiv -1 \ (p)$, ovvero

$$p \mid n^2+1.$$

In $\mathbb{Z}[i]$ allora

$$\underbrace{p \mid n^2+1}_{} = (n+i)(n-i)$$

$(n^2+1) = p \cdot a$
con $a \in \mathbb{Z} \subseteq \mathbb{Z}[i]$

Se p fosse primo, allora $p \mid n+i$ oppure $p \mid n-i$

$$\Updownarrow \qquad\qquad\qquad \Updownarrow$$

$$n+i = p(x+iy) = px + ipy \qquad n-i = p(x+iy) = px+ipy$$

Dunque in particolare $\pm 1 = py$, ma ciò è assurdo poiché p non è invertibile in $\mathbb{Z}$.

<u>OSS</u>: in un UFD primi = irrid.
Se voglio mostrare che qualcosa è primo, mostro che è <u>IRR</u> poiché è una condizione più debole,
se voglio mostrare che qualcosa è non primo, mostro che NON VALE LA PRIMALITÀ.

DIM 2:
Se p fosse primo allora $B := \dfrac{\mathbb{Z}[i]}{(p)}$ sarebbe un dominio
In B le classi

$$\bar{n}, \ -\bar{n}, \ \bar{i}, \ -\bar{i}$$

$[n^2 \equiv -1 \ (p)$
come primo $]$

sono tutte distinte
$\Rightarrow$ in B il polinomio t^2+1 ha almeno 4 radici (in quanto $n^2 \equiv -1$) ma questo è assurdo poiché abbiamo supposto che B fosse un dominio $\blacksquare$

Quindi p non è irriducibile:

$$p = (a+bi)(c+di)$$

con $a+bi$, $c+di \notin \mathbb{Z}[i]^\times$.
Prendendo le norme

$$p^2 = (a^2+b^2)(c^2+d^2)$$

da cui per quanto detto prima $a^2+b^2 = c^2+d^2 = p$.

$$\Rightarrow p = a^2+b^2 = (a+bi)(a-bi)$$

Resta da capire se $a+bi$, $a-bi$ trovati ora sono irriducibili

Infatti se fossero riducibili avrei

$$a \pm bi = (u+vi)(w+zi)$$

$$\Rightarrow N(a \pm bi) = N(u+vi)N(w+zi)$$

$a^2+b^2 = p \Rightarrow$ uno tra $u+vi$ e $w+zi$ è un'unità. $\blacksquare$

Ultimo primo da guardare: $p=2$.
In $\mathbb{Z}[i]$ si ha $2 = (1+i)(1-i) = -i(1+i)^2$

$$\Rightarrow 1+i \sim 1-i$$

FATTO: se $N(a+bi) = a^2+b^2$ è un primo in $\mathbb{Z}$, allora $a+bi$ è primo in $\mathbb{Z}[i]$.

DIM Già fatta

PROBLEMA: sono tutti? PROSSIMA LEZIONE

Quozienti $\mathbb{Z}[i]/P$ con $P = (p)$, $p \in \mathbb{Z}[i]$ primo

① Se $p \equiv 3 \ (4)$, descrivere $\frac{\mathbb{Z}[i]}{(p)} =: B$.

B è finito: un insieme di rappr. è

$$\{ \bar{a} + \bar{b}\bar{i} : 0 \leq a, b < p-1 \}$$

OSS $p \mid x+iy \iff x+iy = p(u+vi)$

$$\iff x+iy = pu + vpi$$

$$\iff p \mid x \wedge p \mid y$$

$\Rightarrow$ Segue quindi che gli el. $\bar{a}+\bar{b}\bar{i}$ sono tutti distinti poiché certamente $\bar{a}-\bar{a'}$, $\bar{b}-\bar{b'}$ sono $\neq 0$ (e quindi non div. per p) ogni qualvolta $\bar{a}+\bar{b}\bar{i} \neq \bar{a'} - \bar{b'}\bar{i}$.

Inoltre B è dominio ((p) è primo in $\mathbb{Z}[i]$)

$\Rightarrow B$ è un $\boxed{\text{campo!}}$