ANELLI DI FRAZIONI, PID, UFD, ...

Note Title 11/21/2018

Massimali di $\mathbb{Z}[x]$

$I \subset \mathbb{Z}[x]$ ideale massimale

Tesi: $I = (p, f(x))$ t.c. p primo
$\overline{f(x)} \in \mathbb{F}_p[x]$ sia irriducibile

Oss 1: $I \cap \mathbb{Z}$ = ideale di $\mathbb{Z}$, primo

$a, b \in \mathbb{Z}$ t.c. $ab \in I \cap \mathbb{Z} \Rightarrow ab \in I$

I max $\Longrightarrow$ I primo $\Rightarrow a \in I$ o $b \in I \Rightarrow$ $a \in I \cap \mathbb{Z}$ o $b \in I \cap \mathbb{Z}$

Due casi: (i) $I \cap \mathbb{Z} = (p)$ p primo

(ii) $I \cap \mathbb{Z} = (0)$

Caso (i) $I \neq (p)\cdot\mathbb{Z}[x]$, perché

$$\frac{\mathbb{Z}[x]}{(p)\,\mathbb{Z}[x]} \simeq \mathbb{F}_p[x]$$ NON È UN CAMPO

$\{I$ ideali di $\mathbb{Z}[x]$ contenenti $(p)\} \longleftrightarrow \{$ ideali di $\mathbb{F}_p[x]\}$

$I \longleftrightarrow \overline{I}$

I massimale $\Rightarrow$ $\overline{I}$ massimale

$\parallel$

$(\overline{f(x)})$ con $\overline{f(x)}$ irriducibile

(perché $\overline{I}$ massimale)

Tramite la corrispondenza, $I = (p, f(x))$

Caso (ii) Vogliamo ricavare un assurdo.

Vogliamo vedere che $I = (f(x))$ con $f(x)$

primitivo ($\gcd(\text{coeff}) = 1$) ed irriducibile in $\mathbb{Q}[x]$

$$\begin{array}{ccc} \mathbb{Z}[x] & \hookrightarrow & \mathbb{Q}[x] = S^{-1}\mathbb{Z}[x] \\ I & \longrightarrow & S^{-1}I = (g(x)) \end{array}$$

$$S = \{ n \in \mathbb{Z},\ n \neq 0 \}$$

$S^{-1}I \neq \mathbb{Q}[x]$, perché se $1 \in S^{-1}I$, allora

$$1 = \frac{i}{n} \quad \text{con } i \in I,\ n \in S \Rightarrow i = n \in \mathbb{Z},$$

ma abbiamo supposto $I \cap \mathbb{Z} = (0)$

Scegliamo $g(x)$ = generatore di $S^{-1}I$ come un polinomio a coeff. interi primitivo

$g(x)$ irriducibile ($S^{-1}I$ max)

Adesso vogliamo vedere che $I = (g(x))$

Sia $i \in I$. Allora $i \in S^{-1}I \Rightarrow i = g(x)\,q(x)$

per qualche $q(x) \in \mathbb{Q}[x]$. Ma $i(x)$ è a coeff. interi, $g(x)$ pure $\Rightarrow$ $q(x) \in \mathbb{Z}[x]$

lemma di Gauss

Allora I non è massimale: se $g(x) = c_n x^n + \dots + c_0$, scegliamo p primo che NON DIVIDA c_n. Allora

- $I \subsetneq (g(x), p)$ $\subseteq$ ovvio, sono diversi perché $p \notin I$
- $(g(x), p) \neq \mathbb{Z}[x]$

$$\frac{\mathbb{Z}[x]}{(p, g(x))} \simeq \frac{\mathbb{F}_p[x]}{(\overline{g(x)})} \neq \text{anello banale}$$

Oss. $(2x+1, 2) = (1)$

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

$$\mathbb{Q}[x,x^{-1}] = \left\{ \sum_{j=-r}^{k} c_j x^j \;\middle|\; c_j \in \mathbb{Q} \right\}$$

$$A = \mathbb{Q}[x] \qquad S = \{ x^k \mid k \in \mathbb{N} \}$$

$$S^{-1}A = \left\{ \frac{p(x)}{x^k} \;\middle|\; p(x) \in \mathbb{Q}[x],\ k \in \mathbb{N} \right\} = \mathbb{Q}[x,x^{-1}]$$

$$S^{-1}A = \{ (s,a) \mid s \in S,\ a \in A \} / \sim$$

$$(s_1,a_1) \sim (s_2,a_2) \iff a_1 s_2 = a_2 s_1$$

$$\Phi : S^{-1}A \longrightarrow \mathbb{Q}[x,y]/(xy-1)$$

$$(x^k, a(x)) \longmapsto [y^k a(x)]$$

$$"x^{-k} a(x)" \longmapsto y^k a(x) = (x^{-1})^k a(x)$$

$$(x^{k_1}, a_1(x)) \sim (x^{k_2}, a_2(x)) \iff x^{k_1} a_2(x) = x^{k_2} a_1(x)$$

$$\downarrow \qquad\qquad \downarrow$$

$$[y^{k_1} a_1(x)] \qquad [y^{k_2} a_2(x)]$$

Se $k_1 > k_2 \Rightarrow x^{k_1-k_2} a_2(x) = a_1(x)$

$$[y^{k_1} a_1(x)] = [y^{k_1} x^{k_1-k_2} a_2(x)] =$$

$$= \left[y^{k_2} \cdot \left(y^{k_1-k_2} x^{k_1-k_2} \right) a_2(x) \right]$$

$$= \left[y^{k_2} \ (xy)^{k_1-k_2} \ a_2(x) \right]$$

$$= \left[y^{k_2} \ a_2(x) \right]$$

Iniettività: se $\frac{p(x)}{x^k} \in$ nucleo, allora anche $x^k \cdot \frac{p(x)}{x^k} \in$ nucleo, cioè $p(x) \in \ker$.

$$\Phi(p(x)) = [p(x)] = [0]$$

$$\Rightarrow p(x) \in (xy-1)$$

$$\Rightarrow p(x) = (xy-1) \cdot q(x,y)$$

$$\Rightarrow \underbrace{\deg_y p(x)}_{0} = \underbrace{\deg_y (xy-1)}_{1} + \underbrace{\deg_y q(x,y)}_{-1\,?}$$

assurdo

Def. $r(x,y) = \sum_{i,j} c_{ij} x^i y^j =$

$$= \sum_{j=0}^{N} \left(\sum_i c_{ij} x^i \right) y^j$$

$$\deg_y r(x,y) = \max \left\{ j \text{ t.c. } \sum_i c_{ij} x^i \neq 0 \right\}$$

Surgettività: $\Phi\left(c\frac{X^a}{X^b}\right) = [cY^bX^a]$

Φ è un isomorfismo!

$$\mathbb{Q}[x,y]/_{(xy-1)} \simeq S^{-1}A \quad \text{(dominio)}$$

$\Rightarrow (xy-1)$ è ideale primo.

Localizzazioni di $\mathbb{Z}$

$S_1 = \mathbb{Z} \setminus 2\mathbb{Z}$ $\qquad$ $S_2 = \{n \mid (n,6)=1\}$

$S_3 = \{2^n \mid n \geq 0\}$

Descrivere gli ideali primi di $S_i^{-1}\mathbb{Z}$.

$$\left\{\begin{array}{l}\text{ideali primi di}\\ \mathbb{Z} \text{ che non intersecano } S\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{ideali primi di}\\ S^{-1}\mathbb{Z}\end{array}\right\}$$

S_1: (p) con p primo dispari, $p \in (p) \cap S$

Gli unici ideali primi di $S_1^{-1}\mathbb{Z}$ sono (0) e (2)

Caso speciale della seguente costruzione: A dominio, $P \subset A$ ideale primo, $S = A \setminus P$ ⌟

Tutti gli ideali di $S_1^{-1}\mathbb{Z}$: sono generati da un numero pari.

$(6) \subsetneq (18) \subsetneq (2)$

in $S_1^{-1}\mathbb{Z}$

Gli ideali di $S_1^{-1}\mathbb{Z}$ sono (0), (2), (2^2), (2^3), ...

$(2^k d_1) = (2^k d_2)$

$(2^h) \neq (2^k)$ se $h \neq k$

$\left\{ 2^h \frac{a}{b} \mid b \text{ dispari} \right\}$ $\left\{ 2^k \frac{c}{d} \text{ con } d \text{ dispari} \right\}$

Se (per esempio) $h > k$, vorrei vedere che $(2^h) \subsetneq (2^k)$

Infatti se $2^k \in (2^h)$ avrei $2^k = \frac{2^h a}{b}$ b dispari

$\Rightarrow 2^h \mid b \cdot 2^k \Rightarrow k \geq h$, assurdo.

- $S_2^{-1}\mathbb{Z}$: ideali primi: (0), (2), (3)

  tutti gli ideali: (0), $(2^a 3^b)$

- $S_3^{-1}\mathbb{Z}$: ideali primi (0) e (p) per $p \neq 2$

  $\| $

  $\{$numeri raz. con denom. potenza di $2\}$

  se $(p) \cap S_3 \neq \emptyset \Rightarrow p = 2$

A PID $\Rightarrow S^{-1}A$ PID, A UFD $\Rightarrow S^{-1}A$ UFD

Oss. Il viceversa non vale: per esempio $A = \mathbb{Q}[x,y]$,

$S = A \setminus \{0\} \Rightarrow S^{-1}A$ campo (quindi UFD e PID), ma A non è PID: (x,y) non è principale

Caso dei PID $I \subset S^{-1}A$, allora $I = S^{-1}J$ per qualche J ideale di $A \xrightarrow[A \text{ PID}]{} J = (j)$ e

$S^{-1}J = I = (j)$

$\left\{ \frac{a}{s} \mid a \in J, s \in S \right\} = \left\{ \frac{jb}{s} \mid b \in A, s \in S \right\}$

$= \left\{ j \cdot \frac{b}{s} \mid \frac{b}{s} \in S^{-1}A \right\}$

Caso degli UFD

A UFD, $S \subseteq A$ parte moltiplicativa

$\mathcal{U} = \{ p \in A \text{ irriid. t.c. } \exists s \in S \; p \mid s \}$

$\mathcal{P} = \{ p \in A \text{ irriid t.c. } p \notin \mathcal{U} \}$

Lemma $p \in A$ irriid diventa invertibile in $S^{-1}A \iff p \in \mathcal{U}$

Dim. $\Leftarrow$ $p \in \mathcal{U} \rightsquigarrow \exists s \in S \; \exists x \in A$ t.c. $s = px$

Allora $\frac{x}{s} \in S^{-1}A$ e si ha $p \cdot \frac{x}{s} = \frac{s}{s} = 1$

$\Longrightarrow$ $p \cdot \frac{x}{s} = 1 \Rightarrow s = p \cdot x$ (con $s \in S$) $\square$

Lemma $p \subset A$ irrid resta irrid. in $S^{-1}A \Leftrightarrow p \in \mathfrak{P}$

Prendiamo $\frac{a}{s} \in S^{-1}A$. Scrivo la fatt. di $a \in A$.

$$a = \underbrace{p_1^{e_1} \cdots p_r^{e_r}}_{\in \mathcal{U}} \underbrace{q_1^{f_1} \cdots q_s^{e_s}}_{\in \mathfrak{P}} \cdot u \quad \llcorner \in A^\times$$

$$\frac{a}{s} = \left(\frac{u}{s} \cdot p_1^{e_1} \cdots p_r^{e_r}\right) q_1^{f_1} \cdots q_s^{e_s} \cdot \underbrace{t_1^{g_1} \cdots t_v^{g_v}}_{\in \mathfrak{P}}$$

$$= \frac{n}{s'}$$

Eliminando i denominatori:

$$u s' q_1^{e} \cdots q_s^{e_s} = n s \, t_1^{g_1} \cdots t_v^{g_v}.$$

$$t_1 \mid u s' q_1^{e_1} \cdots q_s^{e_s} \overset{t_1 \in \mathfrak{P}}{\Longrightarrow} t_1 \mid q_1^{e_1} \cdots q_s^{e_s}$$

$$q_1 \mid n s \, t_1^{g_1} \cdots t_v^{g_v}$$

Bisogna escludere che $q_1 \mid n$. Ma se succede:

$$\frac{n}{s} \cdot \frac{n''}{s''} = 1 \Rightarrow q_1 \mid n n'' = s s'' \in S$$

e questo è assurdo perché q, non divide alcun elemento di S. Da qui si conclude come ogni dim. di fattorizzazione unica.

In un PID, i primi $\neq (0)$ sono massimali

$\varphi : A \longrightarrow B$ omom. di anelli, A PID
B dominio d'integr.
φ suriettivo.

Allora o φ è un iso, o B è un campo

Guardo $\ker \varphi$ $\begin{cases} (0) \Rightarrow \varphi \text{ è iso} \\ \text{è primo} \neq (0) \quad (\text{primo perché } A/\ker\varphi \simeq B \text{ dominio}) \end{cases}$

Se dimostro che primo $\neq (0) \Rightarrow$ massimale ho che B è un campo.

$\mathfrak{p} \subseteq \mathfrak{m}$
$\|\quad\|$
$(p) \quad (m) \Rightarrow p \in (m)$, p irriducibile

$p = m \cdot a$
se unità $\Downarrow$ $m = (1)$
se unità $\mathfrak{p} = \mathfrak{m}$

Interi di Gauss

$$\mathbb{Z}[i] = \{ a+bi \mid a,b \in \mathbb{Z} \}$$

$$A = \frac{\mathbb{Z}[x]}{(x^2+1)} \overset{?}{\simeq} \mathbb{Z}[i]$$

$$\Phi : \mathbb{Z}[x] \longrightarrow \mathbb{Z}[i]$$

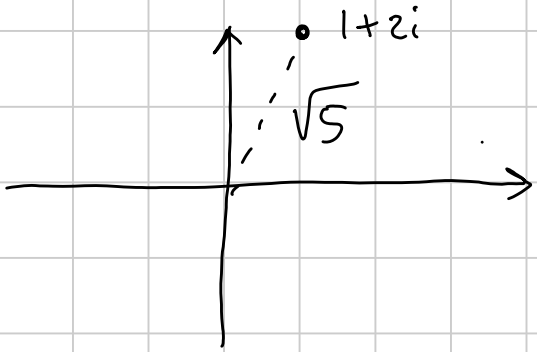
$$x \longmapsto i$$

$$p(x) \longmapsto p(i)$$

$$\ker \Phi = \ker \left(\begin{array}{ccc} \mathbb{Q}[x] & \longrightarrow & \mathbb{Q}[i] \\ p(x) & \longmapsto & p(i) \end{array} \right) \cap \mathbb{Z}[x]$$

$$\ker \Phi = (x^2+1) \qquad \mathbb{Z}[x] = (x^2+1)$$

$$\overset{1^\circ \text{ teo}}{\underset{\text{iso}}{\Longrightarrow}} \frac{\mathbb{Z}[x]}{(x^2+1)} \simeq \mathbb{Z}[i]$$



$$I = (5) \qquad J = (1+2i)$$

$$J : I = \{ a \in \mathbb{Z}[i] \text{ t.c. } aI \subseteq J \} = \mathbb{Z}[i]$$

$$\| (1+2i) \| = \sqrt{5} \rightsquigarrow (1+2i)(1-2i) = 5$$

$$5 \in J$$

$$I : J = (5) : (1+2i) = \big((1+2i)(1-2i) \big) : (1+2i)$$

$$\| \{ a+bi \text{ t.c. } (a+bi)(1+2i) \in (5) \}$$

$$(a-2b)+(2a+b)i \in (5)$$

$$\begin{cases} a \equiv 2b \ (5) \\ 2a \equiv -b \ (5) \end{cases} \iff a \equiv 2b \ (5)$$

$$I : J = \{ (2b+5k) + bi \mid b, k \in \mathbb{Z} \} =$$

$$= \{ b(2+i) + 5k \mid b, k \in \mathbb{Z} \} \supseteq (5, 2+i)$$

$$(2+i) = ((2+i)(2-i), 2+i)$$

$$I : J = (2+i) = (1-2i)$$

differiscono per un fattore $i \in \mathbb{Z}[i]^\times$

□