Ancora $\mathbb{Z}[i]$ e PID / euclidei

Note Title 11/28/2018

Primi in $\mathbb{Z}[i]$

I primi in $\mathbb{Z}[i]$ sono:

- gli $a+bi$ con $a^2+b^2=2$ o $a^2+b^2=p\equiv 1\ (4)$
- $p\equiv 3\ (4)$

Dim. Sia $a+bi\in\mathbb{Z}[i]$ primo. Allora

$$a+bi \mid a^2+b^2 = p_1^{e_1}\cdots p_k^{e_k}$$

$$\Rightarrow \exists j \text{ t.c. } a+bi \mid p_j$$

① $p_j=2 \Rightarrow a+bi \mid -i(1+i)^2$

$$\Rightarrow a+bi \mid 1+i \Rightarrow (a+bi)=(1+i)$$
$$(\Leftrightarrow a^2+b^2=2)$$

② $p_j\equiv 1\ (4) \Rightarrow a+bi \mid \underbrace{(c+di)(c-di)}_{c^2+d^2=p_j}$.

$$\Rightarrow a+bi \mid c+di \text{ o } a+bi \mid c-di$$

$$\Rightarrow a+bi \text{ associato a } c+di \text{ o } c-di$$

③ $p_j\equiv 3(4) \Rightarrow a+bi \mid p_j \Rightarrow (a+bi)=(p_j)$

p_j primo in $\mathbb{Z}[i]$ $\square$

$\mathbb{Z}[i]/(a+bi)$ ha a^2+b^2 elementi

L'altra volta: l'abbiamo mostrato supponendo che $a+bi$ fosse primo.

- $\mathbb{Z}[i]/(1+i) \simeq \mathbb{F}_2$

$$\frac{\mathbb{Z}[x]}{(x^2+1,\ x+1)} \simeq \frac{\mathbb{Z}[x]}{(x^2+1,\ x+1,\ x^2+x,\ x-1,\ 2)} \simeq$$

$$\simeq \frac{\mathbb{Z}[x]}{(x+1,\ 2)} \simeq \frac{\mathbb{F}_2[x]}{(x+1)} \simeq \mathbb{F}_2$$

- $\mathbb{Z}[i]/(p)$ con $p \equiv 3\ (4)$: ha p^2
- $\mathbb{Z}[i]/(a+bi)$ con $a^2+b^2 = p \equiv 1\ (4)$: fatto

$$\left|\mathbb{Z}[i]/(a+bi)\right| = \left|\mathbb{Z}[i]/(a-bi)\right|$$

$$\mathbb{Z}[i]/(a^2+b^2) \overset{TCR}{\simeq} \mathbb{Z}[i]/(a+bi) \times \mathbb{Z}[i]/(a-bi)$$

Due ingredienti:

(i) $(a+bi) = (u \cdot \underbrace{p_1^{e_1} \cdots p_k^{e_k}}_{\text{primi negli interi di Gauss}}) =$

$$= (p_1)^{e_1} \cdot \ldots \cdot (p_k)^{e_k}$$

$$\frac{\mathbb{Z}[i]}{a+bi} = \frac{\mathbb{Z}[i]}{\prod (p_j)^{e_j}} \overset{TCR}{\simeq} \prod \frac{\mathbb{Z}[i]}{(p_j)^{e_j}}$$

(ii) $$\left| \mathbb{Z}[i] / (p_j)^{e_j} \right| = \left| \frac{\mathbb{Z}[i]}{(p_j)} \right|^{e_j}$$

(i): si è visto che $I + J = (1) \Rightarrow I^n + J^m = (1)$

Vorrei vedere che $(p_i) \neq (p_j) \Rightarrow (p_i) + (p_j) = (1)$

$$(p_i) + (p_j) = (p_i, p_j)$$

Due modi: * il mcd tra p_i e p_j è (1)

* (p_i) primo $\neq (0) \Rightarrow$ è massimale

$(1) = (p_i) + (p_j) \supsetneq (p_i)$

per massimalità

Possiamo allora applicare il TCR:

$$\mathbb{Z}[i] / \prod (p_j)^{e_j} \simeq \prod \mathbb{Z}[i] / (p_j)^{e_j}$$

(ii) Sia $A = PID$ e $I = (p)$ un ideale $\neq (0)$

$$\Phi : \begin{array}{ccccc} A & \longrightarrow & A & \longrightarrow & A/I^2 \\ x & \longmapsto & px & \longmapsto & \overline{px} \end{array}$$

omomorfismo DI GRUPPI ABELIANI

immagine $\Phi = I/I^2$

$$\ker \Phi = \{x : px \in (p^2)\} =$$
$$= \{x : p^2 \mid px\} = \{x : p \mid x\} = I$$

1° teo omomorf: $A/I \simeq I/I^2$

$$A/I \simeq \frac{A/I^2}{I/I^2} \Rightarrow |A/I| = \frac{|A/I^2|}{|I/I^2|}$$

$$\Rightarrow |A/I^2| = |A/I| \cdot |I/I^2|$$
$$= |A/I|^2.$$

In generale: $\Phi_k : A \longrightarrow A \longrightarrow A/I^{k+1}$

$$x \longmapsto p^k x \longmapsto \overline{p^k x}$$

$$\left.\begin{array}{l} \mathrm{im}\ \Phi_k : \ I^k/I^{k+1} \\ \ker \Phi_k : \ I \end{array}\right\} \Rightarrow A/I \simeq I^k/I^{k+1}$$

E ora per induzione:

$$A/I^k \simeq \frac{A/I^{k+1}}{I^k/I^{k+1}} \Rightarrow |A/I^{k+1}| = |A/I^k| \cdot |I^k/I^{k+1}|$$
$$= |A/I|^k \cdot |A/I|$$

Conclusione: se $a+bi = u \cdot p_1^{e_1} \cdots p_k^{e_k}$, allora

$$\left| \frac{\mathbb{Z}[i]}{(a+bi)} \right| \overset{(i)}{\simeq} \prod_{j=1}^{k} \left| \frac{\mathbb{Z}[i]}{p_j^{e_j}} \right| \overset{(ii)}{=\!=} \prod_{j=1}^{k} \left| \frac{\mathbb{Z}[i]}{(p_j)} \right|^{e_j}$$

$$\underset{\text{volta}}{\overset{\text{altra}}{=}} \prod_{j=1}^{k} N(p_j)^{e_j} = N\left(\prod p_j^{e_j}\right) = N(a+bi).$$

$\square$

Somme di quadrati $\quad 65 = a^2+b^2 \quad a,b \in \mathbb{Z}$

$$(2+i)(2-i)(3+2i)(3-2i) = 5 \cdot 13 = 65 = (a+bi)(a-bi)$$

$\boxed{2+i \mid a+bi}$ $\qquad a+bi = (2+i)(c+di)$

a meno di cambiare $b \mapsto -b$, posso assumerlo $\qquad a-bi = (2-i)(c-di)$

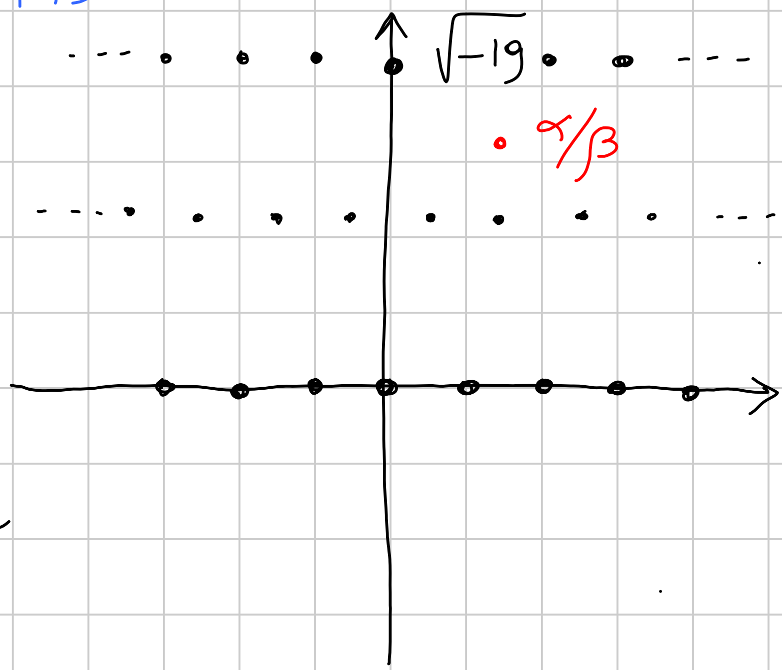
Due casi: • $3+2i \mid a+bi \Rightarrow (a+bi) = (2+i)(3+2i) \cdot u$

$(2+i)(3+2i) = 4+7i \qquad 65 = 16+49$

• $3-2i \mid a+bi$

$(2+i)(3-2i) = 8-i \qquad 65 = 8^2+1$

$A = \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ è un PID



$$\omega := \frac{1+\sqrt{-19}}{2}$$

I ideale di A

β = elemento di norma minima in $I \setminus \{0\}$

Vorrei dimostrare $I = (\beta)$

Per assurdo: sia $\alpha \in I \setminus (\beta)$.

Oss. $|\underbrace{p\alpha + q\beta}_{\in I}| < |\beta| \Rightarrow p\alpha + q\beta = 0 \qquad p, q \in A$

Consideriamo $\frac{\alpha}{\beta} \in \mathbb{Q}(\sqrt{-19})$. Posso scegliere $r \in A$

t.c. $\operatorname{Imm}\left(\frac{\alpha}{\beta} - r\right) \in \left[-\frac{\sqrt{19}}{4}, \frac{\sqrt{19}}{4}\right]$

multiplo di ω

$\exists\, n \in \mathbb{Z}$ t.c. $\operatorname{Re}\left(\frac{\alpha}{\beta} - r - n\right) \in \left[-\frac{1}{2}, \frac{1}{2}\right]$

$$\operatorname{Im}\left(\frac{\alpha}{\beta} - r - n\right) \in \left[-\frac{\sqrt{19}}{4}, \frac{\sqrt{19}}{4}\right]$$

Se $\left|\frac{\alpha}{\beta}-r-n\right|<1 \Rightarrow \underbrace{\left|\alpha-(r+n)\beta\right|}_{0}<|\beta| \Rightarrow \alpha\in(\beta)$

$\boxed{\text{Caso 1}}$ $\operatorname{Im}\left(\frac{\alpha}{\beta}-r-n\right)\in\left(-\frac{\sqrt{3}}{2},\frac{\sqrt{3}}{2}\right)$

$$\left|\frac{\alpha}{\beta}-r-n\right|^2=\operatorname{Im}^2+\operatorname{Re}^2<\frac{3}{4}+\frac{1}{4}=1$$

$$\Rightarrow \left|\alpha-(r+n)\beta\right|<|\beta| \Rightarrow \alpha=(r+n)\beta\in(\beta)$$

$\boxed{\text{Caso 2}}$ $\operatorname{Im}\left(\frac{\alpha}{\beta}-r-n\right)\in\left[-\frac{\sqrt{19}}{4},-\frac{\sqrt{3}}{2}\right]\cup\left[\frac{\sqrt{3}}{2},\frac{\sqrt{19}}{4}\right]$

Considero $2\frac{\alpha}{\beta}-2r-2n-\omega$, la cui parte imm. sta in $\left[\sqrt{3}-\frac{\sqrt{19}}{2},\ 0\right]$.

$$\frac{\sqrt{19}}{2}-\sqrt{3}\leq\frac{\sqrt{27}}{2}-\sqrt{3}=\frac{1}{2}\sqrt{3}$$

A meno di spostarlo di un altro intero, ho che

$$\frac{2\alpha}{\beta}-2r-\omega-m\in\left[-\frac{1}{2},\frac{1}{2}\right]\times\left[-\frac{\sqrt{3}}{2},0\right]$$

$$\Rightarrow \left|\frac{2\alpha}{\beta}-2r-\omega-m\right|<1$$

$$\Rightarrow \left|2\alpha-(2r+\omega+m)\beta\right|<|\beta|$$

$\cap$ I, quindi è 0

$$I\ni\alpha=r\cdot\beta+\frac{\omega+m}{2}\cdot\beta \quad \left(\frac{\omega-1+(m+1)}{2}\right)\beta$$

Per differenza, $\frac{\omega}{2}\beta$ o $\frac{\omega-1}{2}\beta \in I$

$\omega^2 - \omega + 5 = 0$ $\qquad\qquad$ $\omega\overline{\omega} = 5$

$$\frac{1+\sqrt{-19}}{2} \cdot \frac{1-\sqrt{-19}}{2} = 5$$

Se $\frac{\omega}{2}\beta \in I \Rightarrow \overline{\omega} \cdot \frac{\omega}{2}\beta \in I \Rightarrow 5/2\, \beta \in I$

$\Rightarrow I \ni 5/2\, \beta - 2\beta = \beta/2$, ma questo

è assurdo perché $|\beta/2| < |\beta|$

Se $\frac{\omega-1}{2}\beta = -\frac{\overline{\omega}}{2}\beta \in I \Rightarrow \frac{\omega\overline{\omega}}{2}\beta \in I$

$\Rightarrow 5/2\, \beta \in I$, come prima si arriva ad un assurdo

L'unica ipotesi di assurdo fatta era $\alpha \in I \setminus (\beta)$,

quindi $I = (\beta)$. $\square$

Esercizi vari

A anello; se $A[x]$ è un PID, A è campo.

$A \subseteq A[x]$ e $A[x]$ dominio $\Rightarrow$ A dominio.

$$\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$$

$$(\text{se } f(x) \neq 0,\ g(x) \neq 0)$$

$$\left[A = \mathbb{Z}/4\mathbb{Z}, \quad (1+2x)(1-2x) = 1\right]$$

Sia $a \in A \setminus \{0\}$. Considero l'ideale $(a, x) = \underset{\underset{b}{\parallel}}{\overset{\overset{(1)}{\parallel}}{(p(x))}}$

Cosa so su $p(x)$? Che è di grado 0, perché divide a, ed inoltre $b \mid x$ in $A[x]$, cioè

$$x = b \cdot (cx + d) \qquad \begin{cases} 1 = b \cdot c \\ d = 0 \end{cases}$$

$$\Rightarrow b \in A^{\times} \Rightarrow (b) = (1) \Rightarrow 1 \in (a, x)$$

$$\Rightarrow 1 = a \cdot q_1(x) + x \cdot q_2(x)$$

$$\Rightarrow 1 = a \cdot q_1(0) + 0 \cdot q_2(x)$$

$\Rightarrow$ a invertibile con inverso $q_1(0)$

PER FAVORE:

$$\boxed{\text{non avere radici} \not\Rightarrow \text{irriducibile}}$$

Fattorizziamo il pol. $x^4+x^2y^2+y^4$ in $\mathbb{Q}[x,y]$.

Idea 1 Ricondursi ad un $\square$:

$$(x^2+y^2)^2 - x^2y^2 = (x^2+y^2+xy)(x^2+y^2-xy)$$

Idea 2 $y^4\left(\left(\frac{x}{y}\right)^4+\left(\frac{x}{y}\right)^2+1\right)$ $\quad t := x/y$

$$\frac{(t^2)^3-1}{t^2-1} = t^4+t^2+1 = (t^2+1)^2-t^2$$

$$= (t^2+t+1)(t^2-t+1)$$

$$x^4+x^2y^2+y^4 = y^4\cdot\left[\left(\frac{x}{y}\right)^2+\left(\frac{x}{y}\right)+1\right]\left[\left(\frac{x}{y}\right)^2-\left(\frac{x}{y}\right)+1\right]$$

$$= [x^2+xy+y^2][x^2-xy+y^2].$$

Domanda: $\underbrace{x^2+xy+y^2}_{s(x,y)}$ e' irriducibile?

Se si fattorizzasse, $s(x,y) = a(x,y)\,b(x,y)$,

$$\deg_x a(x,y) + \deg_x b(x,y) = 2$$

I gradi possono essere soltanto $1+1$ o $0+2$, $2+0$

Sia $a(x,y) = c_2(y)\,x^2 + c_1(y)\,x + c_0(y)$

$b(x,y) = b(y) = \text{cost.}$

$$\begin{cases} b(y)\,c_0(y) = y^2 \\ b(y)\,c_1(y) = y \\ b(y)\,c_2(y) = 1 \end{cases} \longrightarrow \quad \left\{ \; b(y) = \text{cost} \right.$$

$\Rightarrow$ "finta fattorizzazione", b è unità

Sia $a(x,y) = c_1(y)\,x + c_2(y)$

$b(x,y) = d_1(y)\,x + d_2(y)$

$$\begin{cases} c_2(y)\,d_2(y) = y^2 \\ c_2(y) + d_2(y) = y \\ c_1(y)\,d_1(y) = 1 \end{cases} \underset{\text{WLOG}}{\Longrightarrow} \quad c_1(y) = d_1(y) = 1$$

$c_2(y) = ky \qquad d_2(y) = \frac{1}{k}\,y$

$k + \frac{1}{k} = 1$ e questa non ha soluz. raz.

[ovviamente la sostituzione $t = x/y$ conduce a una soluzione più facile]