INTERI DI GAUSS E ANELLI EUCLIDEI

Note Title 11/23/2018

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

e quindi UFD

Obiettivo Studiare i primi di $\mathbb{Z}[i]$

Norma
$$N : \mathbb{Z}[i] \longrightarrow \mathbb{Z}$$
$$a+bi \longmapsto a^2+b^2$$

Oss $|z_1 \cdot z_2|^2 = |z_1|^2 \cdot |z_2|^2 \quad \forall z_1, z_2 \in \mathbb{C}$

$$\Downarrow$$

$$N(z_1 \cdot z_2) = N(z_1) \cdot N(z_2) \quad \forall z_1, z_2 \in \mathbb{Z}[i]$$

$$\left(\begin{array}{ll} N : \mathbb{Q}(i)^\times \longrightarrow \mathbb{Q}^\times & \text{omomorf. gp} \\ \quad a+bi \longmapsto a^2+b^2 & \end{array} \right)$$

Oss $5 = (1+2i)(1-2i)$: 5 <u>non è primo in $\mathbb{Z}[i]$</u>

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

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

A livello di ideali: $(2) = (1+i)^2$

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

Dim Sia $u \in \mathbb{Z}[i]^\times$ e $u' \in \mathbb{Z}[i]^\times$ t.c.

$$u u' = 1$$

$$u = a + bi, \quad u' = a' + b'i$$

$$\underbrace{N(u)}_{\underbrace{(a^2+b^2)}_{1}} \underbrace{N(u')}_{\underbrace{((a')^2+(b')^2)}_{1}} = N(uu') = N(1) = 1$$

$\Rightarrow$ o a o b e' zero l'altro e' ± 1 $\Rightarrow u = \begin{matrix} \pm i \\ \pm 1 \end{matrix}$ $\square$

Oss 3 e' primo in $\mathbb{Z}[i]$? $\mathbb{Z}[i]$ UFD $\Rightarrow$

basta vedere se 3 e' irriducibile.

$$3 = (a+bi)(c+di)$$

$$\xrightarrow{N} \quad 9 = N(3) = \underbrace{N(a+bi)}_{\text{puo' essere solo } 1,\ 3,\ 9} N(c+di)$$

Se $N(a+bi) = 1 \Rightarrow a+bi =$ unità $\Rightarrow$ quella scritta sopra non e' una "vera" fattorizzazione

Se $N(a+bi) = 9 \Rightarrow N(c+di) = 1 \Rightarrow c+di =$ unità

Se $N(a+bi) = 3 \Rightarrow a^2+b^2 = 3 \Rightarrow$ assurdo.

Quindi 3 è irrid $\Rightarrow$ primo in $\mathbb{Z}[i]$.

Teorema Sia $p \in \mathbb{Z}$ un numero primo $(p>0)$

- Se $p=2 \Rightarrow 2 = -i(1+i)^2$ in $\mathbb{Z}[i]$,

  e $1+i$ è primo

- Se $p \equiv 1\ (4)$, esistono $a,b \in \mathbb{Z}$ t.c.

$$p = (a+bi)(a-bi)$$

  e $a+bi$, $a-bi$ sono primi in $\mathbb{Z}[i]$
  (inoltre $a+bi$, $a-bi$ non sono associati)

- Se $p \equiv 3\ (4)$, p è primo in $\mathbb{Z}[i]$

Oss Inoltre, questi sono tutti i primi di $\mathbb{Z}[i]$

Oss Sia $a+bi \in \mathbb{Z}[i]$ t.c. $N(a+bi) = p \in \mathbb{Z}$.

Allora $a+bi$ è primo in $\mathbb{Z}[i]$.
Se infatti $a+bi = (c+di)(e+fi)$

$$\Rightarrow \quad p = N(a+bi) = N(c+di)\,N(e+fi)$$

uno dei due è $+1$

$\Rightarrow$ o $c+di$ o $e+fi$ è un'unità.

Dim Teorema • $p = 2 = -i(1+i)^2$, e

$N(1+i) = 1^2 + 1^2 = 2$ è primo $\Rightarrow$ $1+i$ è primo

• $p \equiv 3 \pmod 4$. Voglio dim che p è irrid. in $\mathbb{Z}[i]$:

$$p = (a+bi)(c+di)$$
$$\Downarrow \text{ norma}$$
$$p^2 = (a^2+b^2)(c^2+d^2)$$

Se $a^2+b^2 = 1$ o $c^2+d^2 = 1$ $\Rightarrow$ $\begin{matrix} a+bi \\ c+di \end{matrix}$ è unità OK

Se $a^2+b^2 = c^2+d^2 = p$

* se $p \mid a \Rightarrow p \mid (a^2+b^2) - a^2 \Rightarrow p \mid b$
$\Rightarrow p^2 \mid a^2+b^2 = p$, assurdo

* se $p \nmid a \Rightarrow a^2+b^2 \equiv 0 \ (p)$
$\Rightarrow 1 + \left(b/a\right)^2 \equiv 0 \ (p)$
$\Rightarrow \left(b/a\right)^2 \equiv -1 \ (p)$,

assurdo perché -1 non è $\square$ mod p.

[Criterio di Eulero: $x \not\equiv 0 (p)$ è quadrato mod p

$\iff \quad x^{\frac{p-1}{2}} \equiv 1 \mod p \,]$

- $p \equiv 1 \pmod 4$: scegliamo $x \in \mathbb{Z}$ t.c.

$$x^2+1 \equiv 0 \pmod p$$

$$\implies p \mid x^2+1 = (x+i)(x-i)$$

Osserviamo che (in $\mathbb{Z}[i]$) $p \nmid x+i$:

$$x+i = p\cdot(a+bi) = pa+pbi$$

parte immag $\implies 1 = pb \implies$ assurdo

divide un prodotto senza dividere i fattori

Quindi p non e' primo! Quindi non e' irriducibile (siamo in un UFD), e dunque

$$p = \underbrace{(a+bi)(c+di)}_{\text{non unità}}$$

$$p^2 = N(p) = \underbrace{(a^2+b^2)}_{p}\underbrace{(c^2+d^2)}_{p}$$

perché $1\cdot p^2$ e $p^2\cdot 1$ sono escluse

Più precisamente: $p = a^2+b^2 = (a+bi)(a-bi)$

Inoltre: * $a+bi$, $a-bi$ sono primi, perché la loro norma è $a^2+b^2=p$

$$* \quad \frac{a+bi}{a-bi} = \frac{(a+bi)^2}{p} = \frac{(a^2-b^2)+2abi}{p}$$

e questo non è nemmeno in $\mathbb{Z}[i]$: guardando la parte immag., se il rapporto $\in \mathbb{Z}[i]$ si ha

$$p \mid 2ab \Rightarrow p \mid ab \Rightarrow \begin{array}{c} p\mid a \\ \text{o} \\ p \mid b \end{array} \quad \text{e} \quad p = a^2+b^2$$

$$\Rightarrow p \mid a,\ p \mid b \Rightarrow p^2 \mid a^2+b^2 = p, \text{ assurdo.}$$

Secondo approccio ai primi $\equiv 1 \pmod 4$

Basta verificare che $\frac{\mathbb{Z}[i]}{(p)}$ non è un campo

In effetti, il polinomio x^2+1 ha 4 radici in questo quoziente: $\bar{i}$, $\overline{-i}$, le classi di $\pm n \in \mathbb{Z}$ dove $n^2+1 \equiv 0 \pmod p$ $\square$

Corollario Sia $p \equiv 1\ (4)$. Allora $p = a^2+b^2$ in modo unico a meno di $a \longleftrightarrow b$, $a \to -a$, $b \to -b$.

Dim. Sia $a^2+b^2 = c^2+d^2 \Rightarrow \underbrace{(a+bi)}_{N=p}\underbrace{(a-bi)}_{N=p} = \underbrace{(c+di)}_{N=p}\underbrace{(c-di)}_{N=p}$

$a+bi$ primo $\Rightarrow$ $a+bi \mid c+di$ oppure
$a+bi \mid c-di$

$\Rightarrow$ a meno di cambiare b in $-b$, $a+bi \mid c+di$

e $c+di$ primo $\Rightarrow$ $\dfrac{c+di}{a+bi} \in \{1, -1, i, -i\}$

Se per esempio $\dfrac{c+di}{a+bi} = i \Rightarrow c+di = -b+ai$

$\Rightarrow d = a, \; c = -b$

eccetera. $\square$

Quozienti di $\mathbb{Z}[i]$

$$\left|\frac{\mathbb{Z}[i]}{(n)}\right| = n^2,$$ perché come insieme

$$\frac{\mathbb{Z}[i]}{(n)} = \left\{ a+bi \;\middle|\; a,b \in \mathbb{Z}/_{n\mathbb{Z}} \right\}$$

Teorema $$\left|\frac{\mathbb{Z}[i]}{(a+bi)}\right| = a^2+b^2 \quad \text{se} \quad a+bi \neq 0$$

Filosofia

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

- $$\frac{\mathbb{Z}[i]}{(a+bi)} \simeq \frac{\mathbb{Z}[i]}{(a-bi)}$$

Questo sarà vero solo sotto opportune ipotesi!

Combinando questi fatti: $$\left|\frac{\mathbb{Z}[i]}{(a+bi)}\right|^2 = \left|\frac{\mathbb{Z}[i]}{(a^2+b^2)}\right| = (a^2+b^2)^2$$

Dimostrazione Sia $\varphi: \mathbb{Z}[i] \longrightarrow \mathbb{Z}[i]$.
$$x+yi \longmapsto x-yi$$

È un automorfismo di $\mathbb{Z}[i]$ (verifica immediata)

Il nucleo di $\mathbb{Z}[i] \xrightarrow{\varphi} \mathbb{Z}[i] \longrightarrow \dfrac{\mathbb{Z}[i]}{(a-bi)}$ è

$$\varphi^{-1}\big((a-bi)\big) = (a+bi)$$

1° teo isom. $\Longrightarrow \dfrac{\mathbb{Z}[i]}{(a+bi)} \simeq \dfrac{\mathbb{Z}[i]}{(a-bi)}$

Cerchiamo di capire se valga

$$\frac{\mathbb{Z}[i]}{\big((a+bi)(a-bi)\big)} \simeq \frac{\mathbb{Z}[i]}{(a+bi)} \times \frac{\mathbb{Z}[i]}{(a-bi)}$$

Sarebbe un TCR se gli ideali $(a+bi)$ e $(a-bi)$ fossero primi fra loro

<u>Caso facile</u>: $a+bi$ è primo, e non è associato ad $1+i$

Vorrei verificare l'ipotesi del Teo Cinese del Resto:

$$(a+bi) + (a-bi) = (1)$$

$\llcorner$ ideale primo $\neq 0$ $\xRightarrow{\text{PID}}$ è massimale

Due casi: o $(a+bi, a-bi) = (a+bi)$

o $(a+bi, a-bi) = (1)$

Il primo caso è impossibile, perché per simmetria si avrebbe $(a+bi) = (a+bi, a-bi) = (a-bi)$

$\Rightarrow$ $a+bi$ associato ad $a-bi$, che non è vero.

Dimostrato fino ad ora: sia $p \equiv 1 \ (4)$,

$$p = (a+bi)(a-bi) \Longrightarrow (a+bi) + (a-bi) = (1)$$

$$\xrightarrow{TCR} \frac{\mathbb{Z}[i]}{((a+bi)(a-bi))} \simeq \frac{\mathbb{Z}[i]}{(a+bi)} \times \frac{\mathbb{Z}[i]}{(a-bi)} \simeq \left(\frac{\mathbb{Z}[i]}{(a+bi)}\right)^2$$

cardinalità p^2: è $\frac{\mathbb{Z}[i]}{(p)}$

$$\Rightarrow \left|\frac{\mathbb{Z}[i]}{(a+bi)}\right| = p$$

$$\mathbb{Z}[i]/(1+i) \simeq \frac{\overbrace{\mathbb{Z}[i]/(2)}^{4 \text{ elementi}}}{\underbrace{(1+i)/(2)}_{2 \text{ elementi}}} \simeq \mathbb{Z}/2\mathbb{Z}$$

Idea per concludere (lo faremo la settimana prossima):

$$a+bi = p_1^{e_1} \cdots p_k^{e_k} \cdot u$$

$$\frac{\mathbb{Z}[i]}{(a+bi)} \simeq \prod_{i=1}^{k} \frac{\mathbb{Z}[i]}{(p_i^{e_i})}$$

1. $p_i^{e_i} + p_j^{e_j} = (1)$ se $i \neq j$

2. $\left| \frac{\mathbb{Z}[i]}{p_i^{e_i}} \right| = N(p_i)^{e_i}$

PID $\not\Rightarrow$ EUCLIDEO

$$
\begin{tikzcd}
\text{Euclideo} \arrow[r, Rightarrow] & \text{PID} \arrow[r, Rightarrow] \arrow[l, bend left, "\times"] & \text{UFD} \arrow[l, bend left, "\times"]
\end{tikzcd}
$$

$\mathbb{Q}[x,y]$

(x,y) non è principale

Esempio $A = \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right] \simeq \dfrac{\mathbb{Z}[x]}{(x^2-x+5)}$

$$\mathbb{Q}(\sqrt{-19}) \supseteq \left\{ a + b\frac{1+\sqrt{-19}}{2} \;\middle|\; a,b \in \mathbb{Z} \right\}$$

Qualche verifica:

$$\frac{1+\sqrt{-19}}{2} \cdot \frac{1+\sqrt{-19}}{2} = \frac{-18+2\sqrt{-19}}{4} = \frac{-9+\sqrt{-19}}{2}$$

$$x^2 - x + 5 = 0 \qquad \frac{1 \pm \sqrt{1-20}}{2} = \frac{1 \pm \sqrt{-19}}{2}$$

Teorema A non è un anello euclideo (ma è PID)

Dim. Sia per assurdo $d : A \setminus \{0\} \to \mathbb{N}$ una funzione grado

(Dati $x \in A$ e $a \in A$, $\exists\, q \in A$ $\exists\, r \in A$ t.c.

$$x = aq + r, \quad \text{e} \quad r = 0 \quad \text{o} \quad d(r) < d(a))$$

Prendiamo $x \in A$ un elemento di grado minimo TOLTI 0 e A^*

Facciamo la divisione con resto:

$$y = x \cdot q + r \qquad r = 0 \text{ oppure } d(r) < d(x)$$
$$\Downarrow$$
$$r \in A^\times$$

Determiniamo allora $A^\times$.

Come prima, esiste $N : A \longrightarrow \mathbb{Z}$

$$a + b\,\frac{1+\sqrt{-19}}{2} \longmapsto \left|\left(a + b\,\frac{1+\sqrt{-19}}{2}\right)\right|^2$$

e le unità hanno $N = +1$

$$\underbrace{N\left(a + b\,\frac{1+\sqrt{-19}}{2}\right)}_{1} = \left(a + \frac{b}{2}\right)^2 + \left(\frac{b}{2}\sqrt{19}\right)^2$$

$$= a^2 + ab + 5b^2$$
$$= (a^2 + ab + b^2) + 4b^2 \geq 4b^2$$

Unica soluz (disuguaglianze): $b = 0$, $a = \pm 1$

Quanto sopra $\Rightarrow \{0, 1, -1\} \twoheadrightarrow A/(x)$

$\Rightarrow |A/(x)| \leq 3 \Rightarrow A/(x) \in \{\mathbb{F}_2, \mathbb{F}_3\}$

Contraddizione: il polinomio $x^2 - x + 5$ ha una radice in A, ma non ha radici

né in $\mathbb{F}_2$ né in $\mathbb{F}_3$ $\big(X^2 - X + 5 \equiv$
$\equiv X^2 + 2X + 2$
$\equiv (X+1)^2 + 1 \ (3) \big)$

Assurdo $\Rightarrow$ x non esiste $\Rightarrow$ d non esiste.

Abbiamo così mostrato che A non è euclideo. La

prossima volta vedremo che è un PID.