Álgebra Moderna II: Marzo 27

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

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

$\Rightarrow$ Dominio euclidiano con respecto $\delta \Leftarrow$

$\forall \quad \beta = \alpha m + r \quad \delta(r) = \begin{cases} 0 \\ < \delta(\alpha) \end{cases}$

Consecuencias: (6) Todo ideal $I \neq 0$ en $\mathbb{Z}[i]$ es principal.

(7) si $I \neq 0$, entonces $\mathbb{Z}[i]/I$ finito

i.e. I tiene índice finito en $\mathbb{Z}[i]$

Dem:

$$0 \neq \alpha \in I, \quad \alpha \cdot \bar{\alpha} = a^2+b^2 = n > 0$$

$$\mathbb{Z}[i] \supset I \supset (n) = \{na+nbi \mid a,b \in \mathbb{Z}\}$$

índice finito n^2

$R/(n) = n^2$ clases laterales

entonces $\mathbb{Z}[i]/(\alpha)$ anillo finito

= EJER =

¿Cuál es su cardinalidad?

↳ si $I = (\alpha) \subseteq \mathbb{Z}[i]$, entonces

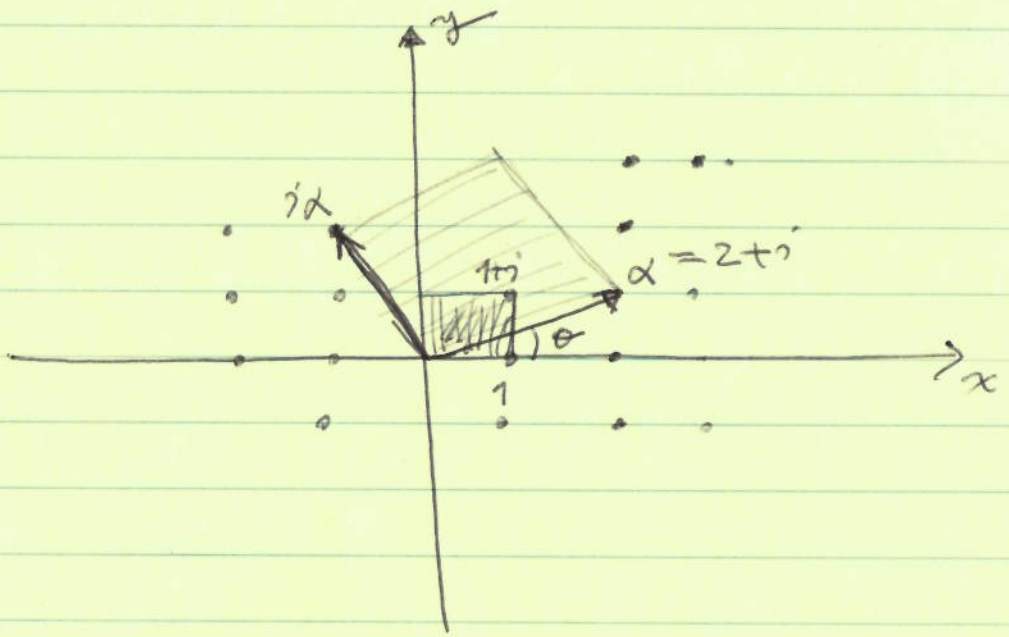
$$\# \mathbb{Z}[i]/(\alpha) = \delta(\alpha) = a^2 + b^2$$

NOTAR esta fórmula es cierta si $\alpha = n \in \mathbb{Z}$.

Argumento: si $\alpha = re^{i\theta} \in \mathbb{C}$.

$\Rightarrow \delta(\alpha) = r^2$

graficando $\alpha \cdot \mathbb{Z}[i]$: $\alpha a + b\alpha i$



escalar: r

rotar: θ

Índice r^2

(1') $I \neq 0$, entonces $\mathbb{Z}[i]/I$ es un anillo finito de cardinalidad $\delta(\alpha)$, donde $(\alpha) = I$.

(2) $\mathbb{Z}[i]$ tiene factorización única

i.e.

$$\alpha = u\, p_1 \cdots p_k$$

(u: Unidad; $p_1, \ldots, p_k$: Primos en $\mathbb{Z}[i]$)

OBSERVE: $p \in \mathbb{Z}[i]$ es primo en $\mathbb{Z}[i]$ sii $\mathbb{Z}[i]/(p)$ campo finito.

¿Cuáles son los unidades y primos de $\mathbb{Z}[i]$?

en $\mathbb{Z}$: Unidades $(\mathbb{Z}) = \langle \pm 1 \rangle$

primos: $2, 3, 5, 7, \ldots$

en $R = F[x]$: Unidades $R^* = F^*$

primos: $p(x) =$ irred mónico en F

$F = \mathbb{C}$, $p(x) = x - a$ $\quad a \in \mathbb{C}$

$F = \mathbb{R}$, $p(x) = \begin{cases} x - r \\ x^2 + rx + s \quad r^2 - 4s < 0 \end{cases}$

Primos & Unidades en $\mathbb{Z}[i] := R$

$$\left.\begin{array}{l} \delta : R \longrightarrow \mathbb{Z}_{\geq 0} \\ \alpha \longmapsto \alpha \cdot \bar{\alpha} = a^2 + b^2 \end{array}\right\} \text{No es homomorfismo}$$

Propiedad importante: $\delta(\alpha \cdot \beta) = \delta(\alpha) \cdot \delta(\beta)$

Afirmación: α es Unidad

$\Updownarrow$

$\delta(\alpha) = 1$

Argumento: $\Uparrow$ $\bar{\alpha}$ es inverso de α.

$\Downarrow$ dada $\alpha \in K$, existe $\beta \in K$ t.q.

$\alpha \cdot \beta = 1$. $\delta(\alpha) \cdot \delta(\beta) = 1 \Rightarrow$

$$\delta(\alpha) = \delta(\beta) = 1$$

$\blacksquare$

entonces, si

$\Rightarrow \alpha \in \mathbb{Z}[i]$ es Unidad

$$\delta(\alpha) = a^2 + b^2 = 1$$

$\Rightarrow$ Unidades $(\mathbb{Z}[i]) = \{1, -1, -i, i\}$.

Primos: si
en $\mathbb{Z}[i]$ $\pi \in R = \mathbb{Z}[i]$ es primo $\Rightarrow$

$R/(\pi)$ es un campo finito $\Rightarrow$

$\left| R/(\pi) \right| = p^n$ para algún $p \in \mathbb{Z}$ primo y $n \geq 1$.

en efecto,

$$\begin{array}{ccc} \mathbb{Z} & \hookrightarrow & R \\ \| & & \downarrow \\ \mathbb{Z} & \xrightarrow[i]{} & R/(\pi) \end{array}$$

$\left\{ \begin{matrix} \text{Núcleo} \\ \text{de } i \end{matrix} \right\} = (p) \leq \mathbb{Z}$

$\uparrow$ primo