Teoría de Números: 31 agosto 2018
Clase pasada: ideales maximales

Hoy: Enteros gaussianos: $\mathbb{Z}[i]$

Algoritmo de la división en $\mathbb{Z}[i]$

$A, B \in \mathbb{Z}[i]$

si intentamos dividir: $B/A = \frac{B\bar{A}}{A\bar{A}} = \frac{B\bar{A}}{\text{entero posit.}}$

entonces $B = A\omega$ con

$\omega \in \mathbb{Q}[i]$ i.e. $\omega = \alpha + \beta i$ $\alpha, \beta \in \mathbb{Q}$.

$\alpha = \alpha_0 + r_0$ $\qquad \alpha_0, \beta_0 \in \mathbb{Z}$ &

$\beta = \beta_0 + s_0$ $\qquad -1/2 \leq r_0, s_0 < \frac{1}{2}$

Por lo tanto

$$B = A\underbrace{(\alpha_0 + \beta_0 i)}_{m} + \underbrace{A(r_0 + s_0 i)}_{R}$$

$$= Am + R$$

Afirmación: $\delta(R) \leq \frac{1}{2}\delta(A)$

Demostración:

$$\delta(R) = \delta(A)(r_0^2 + s_0^2)$$
$$\leq \delta(A)\left(\frac{1}{4} + \frac{1}{4}\right) = \frac{1}{2}\delta(A)$$

$\boxed{\equiv}$

COROLARIO: $\mathbb{Z}[i]$ es Dominio de ideales principales.

Demostración: EJER.

Pregunta: si $I \leq \mathbb{Z}[i]$ ideal

¿Qué campos aparecen como $\mathbb{Z}[i]/I$? ¿o anillos?

EJEMPLO: $R = \mathbb{Z}[i]$ $\quad I = (2+i)$

$R/I = \overline{R} \longleftarrow$ ¿Qué anillo es este?

1) Identifiquemos $I \cap \mathbb{Z}$

$\hookrightarrow$ observamos $5 \in I \cap \mathbb{Z}$

Claro $5 = (2+i)(2-i)$

$\Rightarrow I \cap \mathbb{Z} \supseteq 5 \cdot \mathbb{Z}$

$\Rightarrow I \cap \mathbb{Z}$ es $\cong \mathbb{Z}$ ó $5 \cdot \mathbb{Z}$

2) si $(2+i)(a+bi) \in \mathbb{Z}$

$\Rightarrow -2b = a$

$\Rightarrow 2(-2b) - b = -5b \in 5\mathbb{Z}$

$\Rightarrow I \cap \mathbb{Z} \cong 5\mathbb{Z}$

Se sigue que el homomorfismo canónico $i: \mathbb{Z} \hookrightarrow \overline{R}$

tiene kernel $5\mathbb{Z}$ e imagen $\mathbb{Z}/5\mathbb{Z}$

Por lo tanto $\overline{R}$ es un espacio vectorial sobre $\mathbb{Z}/5$

Más aún, el morfismo canónico es suprayectivo

$i: \mathbb{Z} \longrightarrow \overline{R}$ EJER

$\Rightarrow \boxed{\overline{R} \cong \mathbb{Z}/5}$

<u>OBSERVACIÓN</u>: $(2+3i) = I$ $\qquad$ $\underbrace{\overline{R} = \mathbb{Z}[i]/_I}$

¿Qué anillo es?

1) $(2+3i)(2-3i) = 4+9 = 13$

$\Rightarrow \quad 13 \cdot \mathbb{Z} \subseteq I$

2) si $(2+3i)(a+bi) \in \mathbb{Z} \Rightarrow 2b+3a = 0$

$\Rightarrow 2a-3b = 2a+3a-b$

$= +5a-b$

$\Rightarrow 5a+\frac{3}{2}a \approx 13a \in 13\mathbb{Z}$

$\Rightarrow I \cap \mathbb{Z} \cong 13\mathbb{Z}$

$\Rightarrow \boxed{\overline{R} = \mathbb{Z}/13}$

$$\mathbb{Z}[i] \longrightarrow \mathbb{Z}[i]/_I$$
$$i \longmapsto f(i)$$

$f^2(i) = -1$

$\Rightarrow f(i)$ tiene orden 4 en $\left(\mathbb{Z}[i]/_I\right)^* \overset{\text{si}}{=} (\mathbb{Z}/p)^*$

$\Rightarrow \boxed{p \equiv 1 \pmod 4}$