

Álgebra Moderna II : ~~17~~ ABRIL LUNES, 18 ABRIL

Repaso:

Primos en $\mathbb{Z}[i]$:

$p \equiv 1 \pmod{4} \rightsquigarrow 2$ primos
 π y π'

$p \equiv 3 \pmod{4} \rightsquigarrow 1$ primo

$$\pi \cdot \pi' = p \quad \pi = a + bi \quad \&$$

$$a^2 + b^2 = p$$

(FERMAT)

¿ Existe una fórmula para "a" y "b" ?

Próximas
clases :

Estudiaremos anillos análogos
a $\mathbb{Z}[i]$ y sus elementos primos.

↳ Ej: $\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} \mid a, b \in \mathbb{Z}\}$

1) $S(a + b\sqrt{-2}) = a^2 + 2b^2$

Norma euclidiana.

Eg: $\mathbb{Z}[\sqrt{5}]$ ¡ No tiene factorización

Única!

$$6 = 3 \cdot 2 = (1 + \sqrt{5})(1 - \sqrt{5})$$

↑ ↑ ↗ ↘
elementos primos
en $\mathbb{Z}[\sqrt{5}]$.

Eg: $\mathbb{Z}[\sqrt{-3}]$

No es euclidiano, pues

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$$

2 es irreducible pero no es primo

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d}\} \cong \mathbb{Z}[x] / (x^2 - d) \quad \begin{array}{l} \text{con} \\ \text{no} \\ \text{cuadrado} \end{array} d$$

→ No es, del todo, anillo análogo
a $\mathbb{Z}[i]$. ←

↳ Eg: $f(x) = x^2 + x + 1$

raíces: $\alpha = \frac{-1 \pm \sqrt{-3}}{2}$

$$R = \mathbb{Z}[x] / (f(x)) = \mathbb{Z} + \mathbb{Z}\alpha \cong \mathbb{Z} + \mathbb{Z}\sqrt{-3}$$

\uparrow
 $2\alpha + 1 = \pm\sqrt{-3}$

Ambos anillos (R y $\mathbb{Z} + \mathbb{Z}\sqrt{-3}$) son dominios enteros con el mismo campo de fracciones: $\mathbb{Q}[\sqrt{-3}]$.

¡Sin embargo R es euclidiano!

= EJER =

= FIGURA =

Enteros algebraicos: $\alpha \in \mathbb{C}$

α es raíz de un polinomio mónico $f(x) \in \mathbb{Z}[x]$

Ej: * $m \in \mathbb{Z}$ es un entero algebraico: $f(x) = x - m$

* \sqrt{d} con $d \in \mathbb{Z}$. pues $f(x) = x^2 - d$

* $\alpha = \frac{-1 \pm \sqrt{-3}}{2}$; $f(x) = x^2 + x + 1$