17/08/20 **Proposición** R – DIP. $\pi \in R$ primo

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

(Ejemplo: $f \in k[x]$ irreducible $\Rightarrow k[x]/(f)$ es un campo.)

$\mathbb{Z}/(p)$ es un campo

Dem

$\bar{\alpha} \in R/(\pi) \iff \alpha \in R$ tq. $\pi \nmid \alpha$

$\bar{\alpha} \neq 0$

$(\pi, \alpha) = (\gamma)$ $\quad \gamma \mid \pi, \gamma \mid \alpha \Rightarrow \gamma \in R^\times \Rightarrow (\pi, \alpha) = R$

$\exists \beta, \alpha'$ tq $\quad \pi\beta + \alpha\alpha' = 1 \Rightarrow \alpha\alpha' \equiv 1 \pmod{\pi}$ ∎

Proposición $\forall \pi \in \mathbb{Z}[i]$ primo $\Rightarrow \mathbb{Z}[i]/(\pi)$ es un campo de $N(\pi)$ elementos.

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

2) $\mathbb{Z}[i]/(p) \simeq \mathbb{F}_{p^2}$

$p \equiv 3 \ (4)$

3) $p \equiv 1 \ (4)$ y $p = \pi\bar{\pi}$ $\quad \mathbb{Z}[i]/(\pi) \simeq \mathbb{F}_p$

Dem 1) $2 \equiv 0$, $i \equiv 1 \pmod{1+i}$

2), 3) $(p) = p\mathbb{Z} \oplus pi\mathbb{Z} \subset \mathbb{Z} \oplus i\mathbb{Z}$

$\mathbb{Z}[i]/(p) \simeq \mathbb{Z}/(p) \oplus i\cdot\mathbb{Z}/(p)$ como gpo abeliano.

$p \equiv 3 \ (4) \Rightarrow \simeq \mathbb{F}_{p^2}$ como anillo.

$p \equiv 1 \ (4) \Rightarrow \mathbb{Z}[i]/(p) \simeq \underbrace{\mathbb{Z}[i]/(\pi)}_{\simeq \mathbb{F}_p} \times \underbrace{\mathbb{Z}[i]/(\bar{\pi})}_{\simeq \mathbb{F}_p}$ ∎

§ **Enteros de Eisenstein** $\quad \mathbb{Q}(\sqrt{-3}) \simeq \mathbb{Q}(\zeta_3)$

$\mathbb{Z}[\zeta_3] = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$

$\sigma : a + b\zeta_3 \mapsto a + b\zeta_3^2$.

$N(\alpha) = \alpha \cdot \sigma(\alpha) = a^2 - ab + b^2$. – **norma** de $\mathbb{Q}(\zeta_3)/\mathbb{Q}$.

Se restringe a $\mathbb{Z}[\zeta_3] \to \mathbb{N}$

Lema 1) $\mathbb{Z}[\zeta_3]^\times = \{\alpha \mid N(\alpha) = 1\} = \{\pm 1, \pm\zeta_3, \pm\zeta_3^2\}$

2) Si $N(\pi) = p$ es un primo $\Rightarrow \pi$ es irreducible.

3) $\mathbb{Z}[\zeta_3]$ es un dominio euclidiano respecto a $N(a + b\zeta_3) = a^2 - ab + b^2$.

– ejercicio!

Proposición Sea $p \in \mathbb{Z}$ primo racional.

1) $p = 3 \Rightarrow 3 = -\zeta_3^2 (1-\zeta_3)^2$, donde $1-\zeta_3$ es primo en $\mathbb{Z}[\zeta_3]$

$\mathbb{Z}[\zeta_3]/(1-\zeta_3) \simeq \mathbb{F}_3$

2) $p \equiv 2 \ (3) \Rightarrow p$ es primo en $\mathbb{Z}[\zeta_3]$ y $\mathbb{Z}[\zeta_3]/(p) \simeq \mathbb{F}_{p^2}$

3) $p \equiv 1 \ (3) \Rightarrow p = \pi \cdot \bar{\pi}$ en $\mathbb{Z}[\zeta_3]$, donde $\pi, \bar{\pi}$ son primos no asociados

$\mathbb{Z}[\zeta_3]/(\pi) \simeq \mathbb{F}_p$.

Dem

1) $N(1-\zeta_3) = 3 \Rightarrow 1-\zeta_3$ primo.

2) $p \equiv 2 \ (3)$ $\quad a^2 - ab + b^2 \not\equiv 2 \ (3) \Rightarrow$ no hay elts de norma p

$\Rightarrow p$ es irreducible (= primo).

3) $p \equiv 1 \ (3)$. Reciprocidad cuadrática: $\left(\frac{-3}{p}\right) = +1$.

$\Leftrightarrow \exists \, a \in \mathbb{Z}$ t.q. $a^2 \equiv -3 \ (p)$

$p \mid (a^2+3) = (a+\sqrt{-3})(a-\sqrt{-3})$

$= (a+1+2\zeta_3)(a-1-2\zeta_3)$

no son divisibles por p

$\Rightarrow p$ no es primo. $\quad p = \pi \cdot \bar{\pi}$ (similar a $\mathbb{Z}[i]$)

Proposición $p \equiv 1 \ (3) \Rightarrow 4p = u^2 + 27v^2$ para $u, v \in \mathbb{Z}$,

Además, u y v están bien definidos salvo ± 1.

Dem $p \equiv 1 \ (3) \Rightarrow p = \pi \cdot \bar{\pi}$ en $\mathbb{Z}[\zeta_3]$, $\pi = a + b\zeta_3$ primo.

Ejercicio Entre los asociados de π uno cumple

$a \equiv 2, \ b \equiv 0 \ (3)$.

$p = N(\pi) = a^2 - ab + b^2 \qquad 4p = (2a-b)^2 + 3b^2$

$= u^2 + 27v^2 \quad | \quad u = 2a-b, \ v = b/3.$

Factorización única en $\mathbb{Z}[\zeta_3] \Rightarrow u$ y v están bien definidos

Ejemplo

$$4 \cdot 7 = 7^2 + 27 \cdot 1^2$$
$$4 \cdot 13 = 5^2 + 27 \cdot 1^2$$
$$4 \cdot 19 = 7^2 + 27 \cdot 1^2$$
$$4 \cdot 31 = 4^2 + 27 \cdot 2^2 \quad \text{etc.}$$

§ **Reciprocidad cúbica**

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \cdot \left(\frac{q}{p}\right) - \text{rec. cuadrática}$$

Lema $\pi \in \mathbb{Z}[\zeta_3]$ primo de Eisenstein, $\pi \nmid (1-\zeta_3)$

$\Rightarrow \forall \alpha \in \mathbb{Z}[\zeta_3]$ tq. $\pi \nmid \alpha$

$$\alpha^{\frac{N(\pi)-1}{3}} \equiv 1, \zeta_3, \zeta_3^2 \pmod{\pi}$$

no son congruentes.

Dem $3 \mid (N(\pi)-1)$: de hecho, $N(\pi) = p$, $p \equiv 1 \ (3)$ ó $N(\pi) = p^2$, $p \equiv 2 \ (3)$

Ahora, $\mathbb{Z}[\zeta_3]/(\pi)$ es un campo de $N(\pi)$ elementos.

$$\alpha^{N(\pi)-1} \equiv 1 \Rightarrow \alpha^{\frac{N(\pi)-1}{3}} \text{ es una raíz cúbica módulo } \pi$$

$\Rightarrow$ es congruente a $1, \zeta_3, \zeta_3^2$. ∎

Def $\pi \nmid (1-\zeta_3)$, $\pi \nmid \alpha \Rightarrow$ **el símbolo de residuo cúbico**.

$$\alpha^{\frac{N(\pi)-1}{3}} \equiv \left(\frac{\alpha}{\pi}\right)_3 \pmod{\pi}$$

$$\left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 \cdot \left(\frac{\beta}{\pi}\right)_3$$

$\alpha \equiv \beta \ (\pi) \Rightarrow \left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3$

$$\left(\frac{\cdot}{\pi}\right)_3 : \left(\mathbb{Z}[\zeta_3]/(\pi)\right)^\times \longrightarrow \{1, \zeta_3, \zeta_3^2\}$$ homomorfismo

Lema $\left(\frac{\alpha}{\pi}\right)_3 = 1 \iff x^3 \equiv \alpha \ (\pi)$ tiene solución en $\mathbb{Z}[\zeta_3]$.

Dem Ejercicio, use que $(\mathbb{Z}[\zeta_3]/(\pi))^\times$ es cíclico. ∎

Def Digamos que primo $\pi \in \mathbb{Z}[\zeta_3]$ es **primario** si $\pi \equiv 2 \ (3)$

(Si $N(\pi) = p \equiv 1 \ (3) \Rightarrow$ entre $\pi' = \zeta_6^r \pi \sim \pi$ precisamente uno es primario)

Teorema (Reciprocidad cúbica) Si π_1, π_2 primarios, $N(\pi_1) \neq N(\pi_2)$, entonces

$$\left(\frac{\pi_1}{\pi_2}\right)_3 = \left(\frac{\pi_2}{\pi_1}\right)_3.$$

(Ref: Ireland-Rosen)

Teorema: Un primo racional p tiene forma $x^2 + 27y^2$

$\iff$ $p \equiv 1 \ (3)$ y 2 es un cubo mód p ($x^3 \equiv 2 \ (p)$ para $x \in \mathbb{Z}$)

(**Nota**: $p \equiv 2 \ (3)$ $x \mapsto x^3$ es un automorfismo $\mathbb{F}_p^\times$ $\Rightarrow$ todo $y \in \mathbb{F}_p^\times$ es un cubo)

Lema Para π primario, $N(\pi) = p \equiv 1 \ (3)$, $x^3 \equiv 2 \ (\pi)$ tiene solución en $\mathbb{Z}[\zeta_3] \iff \pi \equiv 1 \ (2)$.

Dem

$$\left(\frac{2}{\pi}\right)_3 = \left(\frac{\pi}{2}\right)_3 \equiv \pi^{\frac{N(2)-1}{3}} = \pi \pmod 2$$

∎

Dem. del teorema Suponganos $p \equiv 1 \ (3)$ y 2 es un cubo mód p.

$x^3 \equiv 2 \ (p)$ tiene solución $\Rightarrow$ $x^3 \equiv 2 \ (\pi)$ tiene solución en $\mathbb{Z}[\zeta_3]$

$\pi \mid p$

$\pi = a + b\zeta_3$ Podemos asumir $\pi \equiv 2\ (3)$ (primario)

$\pi \equiv 1\ (2)$ por el lema.

$a \equiv 2,\ b \equiv 0\ (3) \iff \pi \equiv 2\ (3)$

$a \equiv 1,\ b \equiv 0\ (2) \iff \pi \equiv 1\ (2)$

$N(\pi) = p = a^2 - ab + b^2$

$4p = (2a - b)^2 + 3b^2$ $\qquad x = \frac{2a-b}{2},\ y = \frac{b}{6}$

$p = x^2 + 27y^2$.

Viceversa, si $p = x^2 + 27y^2$, entonces $p \equiv 1\ (3)$

Cambiando el signo de x, asumamos que

$x \equiv 2\ (3)$.

$p = \pi \cdot \overline{\pi}$, donde $\pi = x + 3\sqrt{-3}\cdot y$

$= x + 3y + 6y\cdot\zeta_3$

$N(\pi) = N(\overline{\pi}) = p$, $\pi \equiv 2\ (3) \Rightarrow$ es primario.

$\pi \equiv x + y\ (2)$, x e y tienen diferente paridad

$\Rightarrow \pi \equiv 1\ (2) \Longrightarrow x^3 \equiv 2\ (\pi)$

Lema tiene solución en $\mathbb{Z}[\zeta_3]$

$\mathbb{Z}[\zeta_3]/(\pi) \simeq \mathbb{F}_p \Rightarrow x^3 = 2$ tiene solución en $\mathbb{F}_p$ ∎

Ejemplo $\qquad p = x^2 + 27y^2$

$31 = 2^2 + 27\cdot 1^2 \qquad 2 \equiv 4^3\ (31)$

$43 = 4^2 + 27\cdot 1^2 \qquad 2 \equiv 20^3\ (43)$

$109 = 1^2 + 27\cdot 2^2 \qquad 2 \equiv 57^3\ (109)$

Ejemplo $\left(\frac{5}{\pi}\right)_3 = ?$ Para cuáles $\pi \in \mathbb{Z}[\zeta_3]$

$x^3 \equiv 5 \ (\pi)$ tiene solución

$x^3 \equiv 5 (\pi)$ tiene sol. $\iff$ $x^3 \equiv 5 (\pi')$ tiene sol.

$\pi' \sim \pi$.

Podemos asumir que π es primario ($\pi \equiv 2 \ (3)$)

$$\left(\frac{5}{\pi}\right)_3 = \left(\frac{\pi}{5}\right)_3$$

cuáles son los cubos mód 5 ?!

$\mathbb{Z}[\zeta_3]/(5) \simeq \mathbb{F}_{25}$. tiene $\frac{25-1}{3} = 8$ cubos.

Se puede ver que son

$$\begin{cases} 1, 2, 3, 4, \\ 1+2\zeta_3, \ 2+4\zeta_3, \ 3+\zeta_3, \ 4+3\zeta_3. \end{cases}$$

•) Si $p \equiv 2 \ (3)$ primo racional

$$\Rightarrow \left(\frac{p}{5}\right)_3 = \left(\frac{5}{p}\right)_3$$

(no es interesante, $(\mathbb{F}_p^\times)^3 = \mathbb{F}_p^\times$)

•) Si $p \equiv 1 \ (3)$ primo racional

$p = \pi \cdot \bar{\pi}$

por ejemplo, $p = 7 = \pi \cdot \bar{\pi}$, donde $\pi = -1-3\zeta_3$.

$\equiv 2 \ (3)$.

$\pi \equiv 4 + 2\zeta_3 \ (5)$

$\Rightarrow$ $x^3 \equiv 5 \ (\pi)$ no tiene sol. $\Rightarrow$ $x^3 \equiv 5 \ (p)$ tampoco.

Los cubos mód 7 son ± 1

5 no es un cubo mód 7.

Ahora $p = 13 = \pi \cdot \bar{\pi}$, $\pi = -4-3\zeta_3$

$\equiv 2 \ (3)$

$\pi \equiv 1+2\zeta_3 \ (5)$ $\Rightarrow$ $x^3 \equiv 5 \ (\pi)$ tiene sol.

$x^3 \equiv 5 \ (p)$ tiene sol.

$7^3 \equiv 5 \pmod{13}$

Elementos vs. ideales primos

- elementos primos
  $\pi \neq 0$, $\pi \notin R^\times$ t.q. $\pi \mid \alpha\beta \Rightarrow \pi \mid \alpha$ ó $\pi \mid \beta$.
- ideales primos
  $\mathfrak{p} \subset R$, $\mathfrak{p} \neq R$, t.q. $\alpha\beta \in \mathfrak{p} \Rightarrow \alpha \in \mathfrak{p}$ ó $\beta \in \mathfrak{p}$

Para $\pi \neq 0$. (!)
π es primo $\iff$ (π) primo.

Nuevo horario: $13^{00} - 14^{30}$