

$$\alpha = \sum_{i=-n}^{\infty} a_i \pi^i \quad \{ \pi_i / i \in \mathbb{Z}_1 \}$$

$$v_K(\pi_i) = i$$

$$\alpha = \sum_{i=-n}^{\infty} a_i \pi^i \quad \text{única}$$

$$\beta = \sum_i a_i \pi^i, \quad i = er+t, \quad 0 \leq t < e$$

$$\pi_i = \pi_K \pi_L^t$$

$$\beta = \sum_{t=0}^{e-1} \left( \sum_r a_{er+t} \pi_K^r \right) \pi_L^t$$

$$\beta_t \in K$$

$$\beta = \sum_{t=0}^{e-1} \beta_t \pi_L^t, \quad \deg \beta = e$$

$$[L : K] = e$$

Caso general.  $f = [F_L : F_K]$

grado residual

$e$ : índice de ramificación

$$F_L = F_K[c], \quad p(x) = \text{med}_{c, F_K}(x)$$

$$p(x) = \text{med}_{g^e, K}(x), \quad g \in O_L$$

$$E = K[x]$$

$$[E : K] = [F_L : F_K]$$

$$e \mid \begin{cases} L \\ E \end{cases} \quad \text{totalmente ramificada}$$

$$F_E = F_L \quad f \mid \begin{cases} L \\ K \end{cases} \quad \text{no ramificada.}$$

$$[L:K] = fe$$

( $K$  local)

$K$  global

$K_{\wp}$  lugar en  $K \rightarrow K_{\wp}$  completado

$L/K$  extensión

$$L \otimes_K K_{\wp} \cong L_{P_1} \times \dots \times L_{P_r}$$

$P_1, \dots, P_r$  lugares sobre  $\wp$ .

$$[L:K] = \dim_K L = \sum_{i=1}^r \dim_{K_{\wp}} L_{P_i} = \sum_{i=1}^r [L_{P_i}:K_{\wp}]$$

$$= \sum_{i=1}^r e(L_{P_i}/K_{\wp}) f(L_{P_i}/K_{\wp})$$

$$n = \sum_{i=1}^r e_i f_i$$

Cuando  $L/K$  es Galoisiana  $\Rightarrow n = \text{ref.}$

$$\overline{\mathbb{Z}_2}^{x^2} = L + \mathfrak{O}_L \mathbb{Z}_2 \quad , \quad \mathfrak{O}_L(\sqrt{3})/\mathfrak{O}_L \cong K$$

$\mathfrak{O}_L$   
 $\mathbb{Z}_2$

$$x^2 = 3 \quad \mathfrak{O}_L = \mathbb{Z}_2[\sqrt{3}]$$

$$\beta \in \mathfrak{O}_L = b_1 + b_2 \sqrt{3}$$

$$\sqrt{3} \equiv 1 \pmod{m_{\wp}} \quad \overline{b_1 + b_2 \sqrt{3}} = \overline{b_1 + b_3} \in \mathbb{F}_2$$

$\mathbb{F}_L = \mathbb{F}_2$  totalmente ramificada

$$\text{ch}\left(\mathfrak{O}_{\wp}/m_{\wp}\right) = 2 \rightarrow \text{en característica 2 la raíz cuadrada es única}$$

$\mathbb{Q}(\sqrt{5})/\mathbb{Q}_2$  no ramificada

$$\mathcal{O}_L = \mathbb{Z}_2 \left[ \underbrace{\frac{1+\sqrt{5}}{2}}_{=\beta} \right]$$

$$\beta = \frac{1+\sqrt{5}}{2}, \quad (\underbrace{2\beta - 1}_{=5})^2 = 5$$

$$4\beta^2 - 4\beta + 1 = 5$$

$$\beta^2 - \beta - 1 = 0$$

$$\bar{p} \in \mathcal{O}_L/m_L, \quad \bar{p} \notin \mathbb{Z}_2/2\mathbb{Z}_2 \cong \mathbb{F}_2$$

$$\therefore F_L \neq F_2$$

En  $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$  2 es un primo ramificado

en  $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$  2 es un primo inerte

En  $\mathbb{Q}(\sqrt{-7})/\mathbb{Q}$  2 es descompuesto.

$$\mathbb{Q}(\sqrt{D})/\mathbb{Q}$$

$L/k$  totalmente ramificada,  $[L:k] = e$

$$v_L(\pi_k) = e$$

$$m_{\alpha, k}(x) = x^e + a_{e-1}x^{e-1} + \dots + a_1x + a_0$$

$$\pi_L \equiv 0 \pmod{m_L}$$

puede probarse que cada  $a_i \equiv 0 \pmod{m_K}$ .

$$\pi_L^e + a_{e-1}\pi_L^{e-1} + \dots + a_1\pi_L + a_0$$

$$v_L(\pi_L^e) < v_L(a_i \pi_L^i)$$

" " " "

$$v_L(\pi_L^e) \doteq e = v_L(a_0)$$

$$\therefore v_k(a_0) = 1$$

$A = \{x \in \mathbb{C}^p : \sum_{k=1}^{\infty} \frac{|x|^k}{(k!)^2} < \infty\} \quad (p \neq 2)$ . Determinar A.

$$\sum_{k=1}^{\infty} \frac{|x|^k}{(k!)^2} < \infty \iff \left\| \frac{x^k}{(k!)^2} \right\|_p \xrightarrow{k \rightarrow \infty} 0 \iff \lim_{k \rightarrow \infty} \left( \frac{|x|^k}{(k!)^2} \right) \rightarrow 0.$$

$$v_p \left( \frac{|x|^k}{(k!)^2} \right) = v_p(|x|^k) - v_p((k!)^2) = k v_p(x) - 2 v_p((k!))$$

$$v_p((k!)) = \sum_{i=1}^{\infty} \left[ \frac{k}{p^i} \right] \leq \sum_{i=1}^{\infty} \frac{k}{p^i} = k \sum_{i=1}^{\infty} \frac{1}{p^i} = k \left( \frac{1}{p} + \frac{1}{p^2} + \dots \right)$$

$$= k \frac{1/p}{1 - 1/p} = k \frac{1}{1-p}$$

$$\therefore v_p \left( \frac{|x|^k}{(k!)^2} \right) = v_p(|x|^k) - v_p((k!)^2) \geq v_p(|x|^k) - 2k \frac{1}{1-p}$$

$$\therefore v_p \left( \frac{|x|^k}{(k!)^2} \right) \geq k \left( v_p(x) - \frac{2}{1-p} \right)$$

$$v_p \left( \frac{|x|^k}{(k!)^2} \right) \xrightarrow{k \rightarrow \infty} 0 \iff v_p(x) - \frac{2}{1-p} \geq 0$$

$$\iff v_p(x) \geq \frac{2}{1-p}$$

$$v_p(x) \geq \frac{2}{1-p} \iff -\frac{2}{1-p} > -v_p(x) \iff p^{-\frac{2}{1-p}} > p^{-v_p(x)} = \|x\|_p$$

$$\therefore \|x\|_p \leq p^{-\frac{2}{1-p}} \quad (x \in B(0, p^{-\frac{2}{1-p}}))$$

$\sum_{k=0}^{\infty} \binom{1/2}{k} 3^k$  converges en  $\text{Cl}_3$ .

$$\sum_{k=0}^{\infty} \binom{1/2}{k} 3^k < \infty \text{ en } \text{Cl}_3 \iff \left| \binom{1/2}{k} 3^k \right|_3 \xrightarrow{k \rightarrow \infty} 0$$

$$\iff v_3 \left( \binom{1/2}{k} 3^k \right) \xrightarrow{k \rightarrow \infty} -\infty$$

$$v_3 \left( \binom{1/2}{k} 3^k \right) = v_3 \left( \binom{1/2}{k} \right) + v_3 (3^k) = v_3 \left( \binom{1/2}{k} \right) + k v_3^1 (3)$$

$$= v_3 \left( \binom{1/2}{k} \right) - k$$

$$\left| \binom{1/2}{k} \right|_3 = \dots$$

$$\binom{1/2}{k} = \frac{\frac{1}{2}(1-\frac{1}{2})(2-\frac{1}{2}) \cdots (k-1-\frac{1}{2})}{k!}$$

$$\left| \binom{1/2}{k} \right|_3 = \frac{| \frac{1}{2} |_3 | 1 - \frac{1}{2} |_3 | 2 - \frac{1}{2} |_3 \cdots | k - 1 - \frac{1}{2} |_3}{| k! |_3}$$

$$\leq \frac{1}{| k! |_3} = \left| \frac{1}{k!} \right|_3 = 3^{-v_3(\frac{1}{k!})} = 3^{v_3(k!)}$$

$$\therefore \left| \binom{1/2}{k} \right|_3 \leq 3^{v_3(k!)} \iff 3^{-v_3 \left( \binom{1/2}{k} \right)} \leq 3^{v_3(k!)}$$

$$\therefore -v_3 \left( \binom{1/2}{k} \right) \leq v_3(k!)$$

$$\Rightarrow v_3 \left( \binom{1/2}{k} \right) \geq -v_3(k!)$$

$$\therefore v_3 \left( \binom{1/2}{k} 3^k \right) = v_3 \left( \binom{1/2}{k} \right) - k \geq -v_3(k!) - k$$

$$v_3(k!) \leq k \frac{1}{1-3} = -\frac{1}{2}k \implies -v_3(k!) \geq \frac{1}{2}k$$

$$\therefore v_3\left(\binom{1/2}{k} 3^k\right) \geq \frac{1}{2}k - k = k\left(\frac{1}{2} - 1\right) = -\frac{1}{2}k \xrightarrow{k \rightarrow \infty} -\infty$$

Por la fórmula binomial:  $(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$

$$\therefore \sum_{k=0}^{\infty} \binom{1/2}{k} 3^k = (1+3)^{1/2} = 4^{1/2} \in \mathcal{O}_p = \mathcal{O}_3$$

Así  $\sum_{k=0}^{\infty} \binom{1/2}{k} 3^k$  converge a 2

Supongamos que  $\sum_{k=0}^{\infty} \binom{1/2}{k} 3^k = 2$

$$\Leftrightarrow \left| \sum_{k=0}^{\infty} \binom{1/2}{k} 3^k - 2 \right|_3 = 0 \quad ; \quad 3 \left| \left( \sum_{k=0}^{\infty} \binom{1/2}{k} 3^k - 2 \right) \right|$$

$$3 \mid \left( \binom{1/2}{k} 3^k - 2 \right) \quad \forall k \geq 1 \quad \Rightarrow \quad 3 \mid 1 - 2 = -1 \quad (\Leftarrow)$$

Como  $(\mathcal{O}_p, 1 \cdot \|\cdot\|_3)$  es un espacio métrico, las sucesiones convergentes tienen único límite

$$\therefore \sum_{k=0}^{\infty} \binom{1/2}{k} 3^k = 2$$

$$\sum_{k=0}^{\infty} \binom{1/2}{k} 3^k \neq 2 \quad \rightarrow \quad \sum_{k=0}^{\infty} \binom{1/2}{k} 3^k = -2$$

Problema Encuentra todos los enteros  $n$  tales que la ecuación  $x^2 - n$  tiene raíces en  $\mathbb{Q}_5$ ; justifíquelo.

$n=0$  (caso trivial)

$n \neq 0$ .

$$\mathbb{Q}_5[x] \ni f(x) = x^2 - n = (x - \sqrt{n})(x + \sqrt{n})$$

$$\Rightarrow \frac{\mathbb{Q}_5[x]}{(f)} \cong \frac{\mathbb{Q}_5[x]}{(x - \sqrt{n})} \times \frac{\mathbb{Q}_5[x]}{(x + \sqrt{n})} \cong \mathbb{Q}_5 \times \mathbb{Q}_5$$

$$\frac{\mathbb{Q}_5[x]}{(f)} \cong \frac{\mathbb{Q}[x]}{(f)} \times \mathbb{Q}_5$$

Si  $n$  es  $\square$  en  $\mathbb{Q}$   $\Rightarrow n$  es  $\square$  en  $\mathbb{Q}_5$  (???)

Caso II.  $f$  irreducible en  $\mathbb{Q}[x]$

$f(x) = x^2 - n$  tiene raíces en  $\mathbb{Q}_5 \Leftrightarrow$  se descompone en  $\mathbb{Q}(\sqrt{n})$

$$f(x) = x^2 - n ; f(x_0) = 0 \text{ para algún } x_0 \in \mathbb{Q}_5$$

$$|x_0^2 - n|_5 = 0$$

$$x_0^2 - n \equiv 0 \pmod{5^t} \text{ para } t \in \mathbb{N} \text{ ya que } |x_0^2 - n|_5 \leq 5^{-t}$$

$$\therefore x_0^2 \equiv n \pmod{5} \Rightarrow \left( \frac{n}{5} \right) = 1$$

$$\left( \frac{n}{5} \right) = n^{\frac{5-1}{2}} \pmod{5} \Rightarrow n^2 \left( \frac{n}{5} \right) \equiv n^2 \pmod{5}$$

$$\text{Condición } n^2 \equiv 1 \pmod{5} \Leftrightarrow n^2 - 1 \equiv 0 \pmod{5}$$

Como característica  $\neq 2$

$$n = \frac{\pm \sqrt{4}}{2} = \pm 1$$

-4-

$$\therefore \begin{aligned} n &\equiv 1 \pmod{5} \\ n &\equiv 4 \pmod{5} \end{aligned}$$

$$\begin{aligned} n &= 1 + 5t \\ n &= 4 + 5t \end{aligned}$$

$t \in \mathbb{Z}$

Encotrar primos ramificados, inertes y descompuestos de  $\mathbb{Q}(\sqrt{55})/\mathbb{Q}$ .

$$\mathbb{Q}(\sqrt{55}) = \frac{\mathbb{Q}[x]}{(f)} \quad ; \quad f(x) = x^2 - 55$$

$$f'(x) = 2x.$$

$$\boxed{p=2} \quad \mathbb{Q}(\sqrt{55}) \otimes_{\mathbb{Q}} \mathbb{Q}_2 = \mathbb{Q}_2(\sqrt{55})$$

$$\text{Pero } K \subset L \Rightarrow \mathbb{F}_K \subset \mathbb{F}_L, \text{ donde}$$

$$\therefore \text{char}(\mathbb{Q}_8/m_8) = 2$$

$$\text{en clau 2 la raíz cuadrada es única : } 55 \equiv 1 \pmod{m_8}$$

$$\therefore \sqrt{55} \equiv 1 \pmod{m_8}$$

$$\beta \in \mathbb{Q}_8 = \mathbb{Z}_2[\sqrt{55}] \iff \beta = a_1 + a_2\sqrt{55}$$

$$\text{mod } m_8 : \overline{\beta} = \overline{a_1 + a_2\sqrt{55}} = \overline{a_1} + \overline{a_2}\sqrt{55} = \overline{a_1} + \overline{a_2} = \overline{a_1 + a_2} \in \mathbb{F}_K$$

$$\therefore \mathbb{F}_L = \mathbb{F}_K \quad (2 \hookrightarrow \text{ramificado}).$$

$$\underline{\text{observación}} \quad 55 \equiv 3(4) \Rightarrow \mathbb{Q}_4 = \mathbb{Z}_4[\sqrt{55}]$$

Faltan los primos no ramificados.

$p \in \mathbb{Z}$  primo no ramificado  $\iff f(x)$  tiene raíces  $\neq$ 's en  $\mathbb{Q}_p$ .

Sup. que  $\exists x_0 \in \mathbb{Q}_p : f(x_0) = 0$  (en  $\mathbb{Q}_p$ )

$$\iff x_0^2 - 55 = 0$$

$$\therefore |x_0^2 - 55|_p = 0 \iff |x_0^2 - 55|_p \leq \left(\frac{1}{p}\right)^t \quad \forall t \in \mathbb{N}$$

$$\iff x_0^2 \equiv 55 \pmod{p^t} \quad \forall t \in \mathbb{N}.$$

Estudiar  $f(x) \equiv 0 \pmod{p} \iff x_0^2 - 55 \equiv 0 \pmod{p} \iff \left(\frac{55}{p}\right) \equiv 1 \pmod{p}$

$$\left(\frac{55}{p}\right) = \left(\frac{5}{p}\right)\left(\frac{11}{p}\right)$$

$p=2$

$$\underline{p=3}: \left(\frac{5}{p}\right) = \left(\frac{2}{p}\right) \equiv -1, \quad \left(\frac{11}{p}\right) \equiv \left(\frac{2}{p}\right) \equiv -1 \pmod{p}$$

$$\therefore \left(\frac{55}{p}\right) \equiv 1$$

~~$$p=5: \left(\frac{5}{5}\right) \equiv \left(\frac{1}{5}\right) \equiv 1, \quad \left(\frac{11}{5}\right) = \left(\frac{1}{5}\right) \equiv 1, \quad \left(\frac{55}{5}\right) \equiv 1$$~~

~~$$p=7: \left(\frac{5}{7}\right) \equiv (-1)^{\frac{5-1}{2} \cdot \frac{7-1}{2}} \equiv (-1)^{2 \cdot 3} \equiv 1, \quad \left(\frac{11}{7}\right) = \left(\frac{4}{7}\right) = \left(\frac{2}{7}\right)^2 \equiv 1$$~~

~~$$p \neq 11: \therefore \left(\frac{55}{7}\right) = 1$$~~

~~$$p=11: \left(\frac{5}{11}\right) = (-1)^{\frac{5-1}{2} \cdot \frac{11-1}{2}} \left(\frac{11}{5}\right) = \left(\frac{1}{5}\right) = 1, \quad \left(\frac{11}{11}\right) = \left(\frac{0}{11}\right) = 0$$~~

~~$$p > 11: \left(\frac{55}{p}\right) = \left(\frac{5}{p}\right)\left(\frac{11}{p}\right) = (-1)^{\frac{5-1}{2} \cdot \frac{p-1}{2}} (-1)^{\frac{11-1}{2} \cdot \frac{p-1}{2}} \left(\frac{p}{5}\right)\left(\frac{p}{11}\right)$$~~

$$= (-1)^{\frac{5(p-1)}{2}} \left(\frac{p}{5}\right)\left(\frac{p}{11}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{5}\right)\left(\frac{p}{11}\right) (*)$$

Todos los primos  $p$  que cumplen  $(*)=1$

Son compuestos!!

Un poco complicada la combinación para que dé  $1^0 - 1$ .

$$L = \mathbb{Q}(\sqrt{55})$$

$p$  primo y go lugar en  $L$  que extiende al valor absoluto primitivo.

$$|\sqrt{55}|_p^2 = |55|_p = |55|_p = |5|_p |11|_p$$

$$|5|_p = p^{-v_p(5)}, \quad |11|_p = p^{-v_p(11)}$$

$$|55|_p = p^{-v_p(55)} = p^{-v_p(5) - v_p(11)} = p^{-v_p(5)} p^{-v_p(11)}$$

$$\text{para } p=5 : |55|_p = |55|_5 = \frac{1}{5} \Rightarrow |\sqrt{55}|_{\mathbb{F}_5} = \frac{1}{\sqrt{5}} \notin 5^{\mathbb{Z}}$$

implica que el índice de ramificación  $[\mathbb{L}_{\mathfrak{f}}^*: \mathbb{Q}_5^*]$   
no puede ser 1 (es 2).

$$\therefore [\mathbb{F}_L : \mathbb{F}_K] = 1 \quad (\text{5 es ramificado})$$

$$p=11 : |55|_{11} = \frac{1}{11} \Rightarrow |\sqrt{55}|_{\mathbb{F}_5} = \frac{1}{\sqrt{11}} \notin 11^{\mathbb{Z}} \quad (11 \text{ es ramificado})$$

(y lugar sobre 11)

Hasta el momento: 2, 5, 11 son ramificados.

Para  $p > 11$ ,  $f$  tiene raíces distintas (módulo  $p$ ) ya que  
 $f, f'$  son relativamente primos

$\therefore \forall p > 11$ ,  $p$  es un primo no ramificado. (?)

$p > 11$ ; Se sabe que  $\mathbb{F}_K \subset \mathbb{F}_L$ , pero además  $\text{char}(\mathbb{F}_L) = p$ .

$$p=7 : 55 \equiv 6 \pmod{m_{f,g}}$$

$$\left(\frac{6}{7}\right) = \left(\frac{3}{7}\right) \left(\frac{2}{7}\right) = -1 \cdot 1 = -1$$

$p$  valores absolutos no arquimediano en  $\mathbb{Q}(i)$ .

Sean  $\pi_1, \pi_2$  primos  $\neq$ 's en  $\mathbb{Z}[i]$ . Probar que  $p(\pi_1)$  y  $p(\pi_2)$  no pueden ser menores que 1 simultáneamente.

— o —

$p(\alpha) = |N_{L/K}(\alpha)|_p$ , donde  $L = \mathbb{Q}(i)$ ,  $K = \mathbb{Q}$ .  
 $p \in \mathbb{Z}$  primo.

$\pi_1, \pi_2 \in \mathbb{Z}[i]$  primos  $\iff a_1\pi_1 + a_2\pi_2 = 1$ ,  $a_i \in \mathbb{Z}[i]$

$$1 = p(1) = p(a_1\pi_1 + a_2\pi_2) \leq \max_{i \in \{1, 2\}} \{p(a_1\pi_1), p(a_2\pi_2)\}$$
$$1 \leq \max \{p(a_1)p(\pi_1), p(a_2)p(\pi_2)\}$$

Supongamos que  $p(\pi_1), p(\pi_2) < 1$

Tenemos  $L_{\mathbb{Z}_p} = \mathbb{Q}_p(i)$ ,  $O_p = \mathbb{Z}_p[i]$

como  $\mathbb{Z}[i] \hookrightarrow \mathbb{Z}_p[i]$  :  $p(a_i) \leq 1$

$$\therefore p(a_i\pi_i) < 1 \quad \forall i = 1, 2 \iff$$

---

Toda sucesión en  $\mathbb{Z}_p$  tiene una subsecuencia convergente.

$(a_n)_{n \in \mathbb{N}}$  suc en  $\mathbb{Z}_p$ :  $|a_n|_p \leq 1 \quad \forall n$ .

$$\therefore a_n \in B[0, 1] \quad \forall n.$$

Tenemos que demostrar que  $B[0, 1]$  es compacto en  $(\mathbb{Q}_p, |\cdot|_p)$  (espacio métrico)

Af.  $B[0, 1]$  ~~es~~ cerrado. (No debe ser muy difícil)

Clase 24 Junio TN

(1)

## Distribución de primos

Función Zeta:  $\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z}$  convergente si  $\operatorname{Re}(z) > 1$   
divergente si  $z = 1$

$$\zeta(z) = \prod_{p \text{ primo}} \left(1 - \frac{1}{p^z}\right)^{-1}$$

$$B_p(\zeta, x) = (1-x)^{-1} = 1 + x + x^2 + \dots$$

$$\log B_p(\zeta, x) = -\log(1-x)$$

$$\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \dots$$

$$\log B_p(\zeta, x) = x - \cancel{\frac{1}{2}x^2} + \cancel{\frac{1}{3}x^3} = x - \frac{x^2}{2} + \frac{x^3}{3} - \dots$$

$$\log \zeta(z) = \sum_{p \text{ primo}} \log B_p(\zeta, \frac{1}{p^z})$$

$$= \sum_{p \text{ primo}} \left( \frac{1}{p^z} + \frac{1}{p^{2z}} + \frac{1}{p^{3z}} + \dots \right)$$

$$\sum_{n \geq 2} \frac{1}{n^t} \leq \int_1^{\infty} \frac{1}{x^t} dt = \frac{x^{-t+1}}{1-t} \Big|_1^{\infty} = \frac{1}{t-1}$$

$$\sum_{p \text{ primo}} \left( \sum_{j=2}^{\infty} \frac{1}{j p^{jt}} \right) \leq \sum_{j=2}^{\infty} \left( \frac{1}{j} \sum_{p \text{ primo}} \frac{1}{p^j} \right)$$

$$\leq \sum_{j=2}^{\infty} \frac{1}{j} \sum_{n \geq 2} \frac{1}{n^j} \leq \sum_{j=2}^{\infty} \frac{1}{j(j-1)} = 1$$

Luego para cada  $z$ ,  $\log \zeta(z)$  converge si  $\sum'_{p \text{ primo}} \frac{1}{p^z}$  converge.

Para  $z=1$ ,  $\sum'_{p \text{ primo}} \frac{1}{p}$  diverge, pues  $\sum_{n=1}^{\infty} \frac{1}{n}$  diverge.

En particular,

- 1) Hay infinitos primos
- 2) para cada  $t < 1$  y  $\varepsilon > 0$  hay un  $n$  tal que  $p_n \leftarrow n\text{-ésimo primo}$ .

satisface  $p_n < \varepsilon^{n^t}$ .

Si no,  $p_n \geq \varepsilon^{n^t}$

$$\sum_{n=1}^{\infty} \frac{1}{p_n} \leq \sum_{n=1}^{\infty} \frac{1}{\varepsilon^{n^t}}$$

↑                      ↓  
div                  conv

$(\rightarrow \leftarrow)$

Fijemos  $n$  y consideremos

$\chi : (\mathbb{Z}/n\mathbb{Z})^* \rightarrow \mathbb{C}^*$  homomorfismo. (caracter).

$$\sum_{a \in (\mathbb{Z}/n\mathbb{Z})^*} \chi(a) = \begin{cases} \phi(n) & \text{si } \chi \equiv 1 \\ 0 & \text{si no} \end{cases}$$

$\chi \neq 1$ ,  $\exists b$  con  $\chi(b) \neq 1$

$$\sum_a \chi(a) = \sum_a \chi(ab) = \sum_a \chi(a) \chi(b)$$

$$(1 - \chi(b)) \sum_a \chi(a) = 0 \quad \therefore \quad \sum_a \chi(a) = 0$$

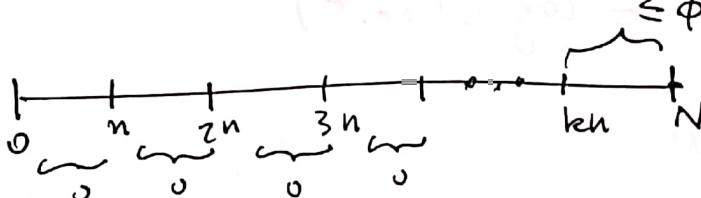
(2)

Ahora definimos la L-función como

$$L(\chi, z) = \sum_{(a,n)=1} \frac{\chi(a)}{a^z}$$

$$\left[ \begin{array}{l} \chi_0(\bar{a}) = 1 \\ \text{fa con} \\ (n,a) = 1 \end{array} \right] \quad \text{obr: si } \chi \neq \chi_0, \quad \sum_{a \leq N} \chi(a) \text{ es acotado}$$

$$\left| \sum_{a \leq N} \chi(a) \right| \leq \phi(n) \quad |\chi(\bar{a})| = 1$$



$z \in \mathbb{R}, z \geq 1$        $\left\{ \sum_a \chi(a) \right\}_a \leftarrow \text{sumas parciales acotadas}$

$$\frac{1}{a^z} \rightarrow 0 \text{ uniformemente}$$

$\therefore L(\chi, z)$  unif. convergente.

$$L(\chi_0, z) = \sum_{(a,n)=1} \frac{1}{a^z}$$

$$\chi_0(a) = \begin{cases} 1, & (n,a)=1 \\ 0, & (n,a) \neq 1 \end{cases} \leftarrow \text{función multiplicativa.}$$

$$L(\chi_0, z) = \prod_{p \text{ primo}} B_p(\chi_0, \frac{1}{p^z})$$

$$B_p(\chi_0, x) = \begin{cases} 1 + x + x^2 + \dots & \text{si } p \nmid n \\ 1 & \text{si } p \mid n. \end{cases}$$

$$\begin{aligned}\therefore L(x_0, z) &= \prod_{\substack{p \text{ primo} \\ p \neq n}} \left(1 - \frac{1}{p^z}\right)^{-1} \\ &= \left[ \prod_{p \neq n} \left(1 - \frac{1}{p^z}\right) \right] \zeta(z)\end{aligned}$$

Ejercicio. Si  $p_1, \dots, p_r$  son primos y  $T = \{n \mid q \nmid n \forall q \neq p_1, \dots, p_r\}$  entonces  $\sum_{n \in T} \frac{1}{n}$  converge.

$$\sum'_{\substack{p \text{ primo} \\ p \neq n}} \frac{\chi_0(p)}{p^z} + g(z) = \log L(x_0, z)$$

así que

$$z=1, \quad \sum'_{p \neq n} \frac{\chi_0(p)}{p^z} \text{ diverge.}$$

así que

$$\sum'_{p \neq n} \frac{1}{p^z}$$

Razonando del mismo modo con  $x \neq x_0$  y  $\sum'_{p \neq n} \frac{\chi(p)}{p^z}$ .

Usando:

Hecho:  $L(x, 1) \neq 0$

$\log L(x, z)$  converge en una vecindad de  $z=1$ .

$$\therefore \sum'_{p \neq n} \frac{\chi(p)}{p^z} \text{ converge.}$$

(3)

Sea  $\bar{b} \in (\mathbb{Z}/n\mathbb{Z})^*$  fija.  $\bar{c} \in (\mathbb{Z}/n\mathbb{Z})^*$

Si en invierto ( $\bar{b}\bar{c} = \bar{1}$  en  $(\mathbb{Z}/n\mathbb{Z})^*$ )

Lema. Si  $\bar{b} \neq \bar{1}$  existe  $\chi : (\mathbb{Z}/n\mathbb{Z})^* \rightarrow \mathbb{C}^*$  tal que  $\chi(\bar{b}) \neq 1$

$$(\mathbb{Z}/n\mathbb{Z})^* \cong \prod_{l=1}^r C_{d_l}$$

$$\bar{b} \mapsto (\bar{b}_1, \dots, \bar{b}_r) \text{ s.t. } \begin{cases} \bar{b}_l \neq \bar{1} \\ b_j \neq 0 \end{cases}$$

$$\chi : \prod_{l=1}^r C_{d_l} \rightarrow \mathbb{C}^*$$

$$\chi(\bar{a}_1, \dots, \bar{a}_r) = e^{2\pi i \left( \frac{a_1}{d_1} + \dots + \frac{a_r}{d_r} \right)}$$

$$e^{2\pi i \left( \frac{b_1}{d_1} \right)} \neq 1$$

Sea  $G = \{ \chi : (\mathbb{Z}/n\mathbb{Z})^* \rightarrow \mathbb{C}^*, \text{ character} \}$

prop:  $\sum_{\chi \in G} \chi(\bar{b}) = \begin{cases} |G| \text{ si } \bar{b} = \bar{1} \\ 0 \text{ si no} \end{cases}$

$\bar{b} \neq \bar{1} \Rightarrow \exists \chi, \text{ con } \chi(\bar{b}) \neq 1$

$$\sum_{\chi \in G} \chi(\bar{b}) = \sum_{\chi \in G} (\chi \chi_1)(\bar{b}) = \chi_1(\bar{b}) \sum_{\chi \in G} \chi(\bar{b})$$

$$\therefore (1 - \chi_1(\bar{b})) \sum_{\chi \in G} \chi(\bar{b}) = 0$$

$$\therefore \sum_{\chi \in G} \chi(\bar{b}) = 0.$$

Sea  $\bar{b} \in (\mathbb{Z}/n\mathbb{Z})^*$  fijo,  $\bar{c} = \bar{b}^{-1}$

$$\begin{aligned} \sum_{\substack{p \leq x \\ p \equiv b \pmod{n}}} \frac{1}{p} &= \sum_{p \leq x} \frac{1}{p} \left( \frac{1}{|G|} \sum_{\chi \in G} \chi(\bar{p}\bar{c}) \right) \\ &= \frac{1}{|G|} \sum_{\chi \in G} \chi(\bar{c}) \left( \sum_{p \leq x} \frac{\chi(\bar{p})}{p} \right) \end{aligned}$$

Converge si  $\sum_{p \leq x} \frac{1}{p}$  convergente

luego NO converge

Teorema de Dirichlet sobre primos en progresión aritmética.

Si  $\bar{b} \in (\mathbb{Z}/n\mathbb{Z})^*$  (i.e.,  $(n, b) = 1$ )

entonces existen infinitos primos  $p$  con  $p \equiv b \pmod{n}$

"hay  $\infty$  primos  $p = \{an + b \mid a \in \mathbb{Z}_4\}$ ".

Se puede demostrar que

$$\frac{\sum_{\substack{p \leq x \\ p \equiv b \pmod{n}}} \frac{1}{p}}{\sum_{p \leq x} \frac{1}{p}} \xrightarrow{x \rightarrow \infty} \frac{1}{\phi(n)}$$

Más difícil.

$$\frac{\sum_{\substack{p \leq x \\ p \equiv b \pmod{n}}} 1}{\sum_{p \leq x} 1} \xrightarrow{x \rightarrow \infty} \frac{1}{\phi(n)}$$

Fin! ↴

## Teoría de Números. Guía 6

Junio 20 de 2010

A. Probar que si una función  $\rho : K \rightarrow [0, \infty]$  definida en un cuerpo  $K$ , satisface las tres condiciones siguientes:

- (a)  $\rho(x) = 0$  si y sólo si  $x = 0$ .
- (b)  $\rho(ab) = \rho(a)\rho(b)$ .
- (c)  $\rho(u) \leq 1$  implica  $\rho(1+u) \leq 1$ .

Entonces  $\rho$  es un valor absoluto y satisface la desigualdad triangular fuerte

$$\rho(a+b) \leq \max\{\rho(a), \rho(b)\}.$$

B. Probar que si  $\rho$  es un valor absoluto en un cuerpo  $K$ , entonces para todo  $x$  en  $K$  se tiene  $\rho(-x) = \rho(x)$ .

3. Determine cuales de las siguientes sucesiones convergen en la norma  $p$ -ádica indicada y calcule el límite si este es el caso.

- (a)  $a_n = 2^n$  con  $p = 2$ .
- (b)  $a_n = 2^{-n}$  con  $p = 2$ .
- (c)  $a_n = 1 + 2 + 2^2 + \dots + 2^n$  con  $p = 2$ .
- (d)  $a_n = 1 + 4^n$  con  $p = 2$ .

~~(e)~~  $a_n = 4^n$  con  $p = 3$ .  $\|a_n\|_3 = \|4^n\|_3 = \frac{1}{2}$

C. Determine cuales de las siguientes series convergen en el cuerpo  $\mathbb{Q}_p$  con el valor indicado de  $p$ .

~~(a)~~  $1 + 2 + 4 + \dots + 2^n + \dots$  con  $p = 2$ . Con  $n \frac{1}{2-1} = 1$

~~(b)~~  $1 + 2 + 4 + \dots + 2^n + \dots$  con  $p = 3$ .

~~(c)~~  $\sum_{i=1}^{\infty} \frac{2^n}{n}$  con  $p = 2$ .

$\|2^n\|_3 \xrightarrow[n \rightarrow \infty]{} 0$  pero  $\|2^n\|_3 = 1$ .

pues:  $2^n \leq n$

$\left\| \frac{2^n}{n} \right\|_2 \xrightarrow[n \rightarrow \infty]{} 0$ .  $\lim_{n \rightarrow \infty} \frac{2^n}{n} = 0 \Rightarrow -\log_2 \left\| \frac{2^n}{n} \right\|_2 = -\log_2 0 = \infty$

$\Rightarrow -\log_2 n - \log_2 \left\| \frac{2^n}{n} \right\|_2 \leq \log_2 n + \log_2 \frac{2^n}{n} \xrightarrow[n \rightarrow \infty]{} -\infty \therefore \text{Converge}$

Problema 7. f. n a en  $\mathbb{K}$  en pue  $f(n) \geq 1 \quad \forall n \in \mathbb{N}$ .

probar para  $p \in \text{pot. de un } \mathbb{N} \times \text{usual o el trivial } p(r) = 1, \forall r \in \mathbb{R}$ .

Demostración: Si  $p(n) = 1 \quad (\forall n \in \mathbb{N}) \Rightarrow p\left(\frac{m}{n}\right) = \frac{p(m)}{p(n)} = 1, \forall m, n \in \mathbb{N}$ .

Si  $p(n) > 1, \exists p_i \in \mathbb{P}, n_i \in \mathbb{N} \quad \prod p(p_i)^{n_i} > 1$

$\Rightarrow \exists p_i \in \mathbb{P} \quad p(p_i) > 1$ .

Sea  $m \in \mathbb{N}$  primo,  $m = \sum_{i=0}^t a_i p^i, a_i \in \{1, \dots, p-1\}, D = \max \{p(a_i)\}_{i=1}^t$ .

$$m^t \leq p^n \leq m^{t+1} \quad p(m^r) \leq \sum_{i=0}^t a_i p(p)^i \leq (t+1) \prod p(p)^{t+1}, p(p) = \frac{\ln p}{\ln m}$$

$$p(m) \leq \sqrt[t+1]{(t+1) \prod p(m)} \xrightarrow[r \rightarrow \infty]{} \alpha_n(p, m)$$

$$\text{Luego: } \log p(p) \leq \log \alpha_n + \frac{1}{r} \log p(m)$$

$$\leq \log \alpha_n + \frac{\log p}{\log m} \log p(m), \quad \text{Si } r \rightarrow \infty$$

$$\log p(p) \leq \frac{\log p}{\log m} \log p(m) \Rightarrow \frac{\log p(p)}{\log p(m)} \leq \frac{\log p}{\log m} \quad \text{Por limite fin}$$

completar ordenar.

$$\therefore \frac{\log p(p)}{\log p(m)} = \frac{\log p}{\log m}, \quad \text{Sea } \lambda = \frac{\log p}{\log m}$$

$$\therefore p(p) = p^\lambda \quad \text{pd: } \lambda < 1.$$

$$\therefore p(n) = n^\lambda.$$

Problema 8. pd:  $\sum_{k=1}^{\infty} \frac{x^k}{k}$  converge  $\forall x \in B(0,1)$ . pd: cada condición para k es completa.

$$\text{Sea } x_n = \sum_{k=1}^n \frac{x^k}{k} \Rightarrow p(x_n - x_m) \leq \max_{m+1 \leq k \leq n} \left\{ p\left(\frac{x^k}{k}\right) \right\}$$

~~(a)~~  $\sum_{n=1}^{\infty} \frac{3^n}{n!}$  con  $p = 3$ .

~~(b)~~  $\sum_{k=0}^{\infty} p^k \binom{1/2}{k}$  con  $p \neq 2$ .

~~(c)~~  $\sum_{k=0}^{\infty} 2^k \binom{1/2}{k}$  con  $p = 2$ .

7. Probar que  $K$  es un cuerpo con un valor absoluto  $\rho$  que satisface la desigualdad triangular fuerte y si definimos

$$B(a; r) = \{x \in K \mid \rho(x - a) < r\},$$

entonces para cada punto  $b \in B(a; r)$  se tiene  $B(a; r) = B(b; r)$ .

8. Sea  $\rho$  un valor absoluto en  $\mathbb{Q}$  y sea  $p$  un primo tal que  $\rho(p) < 1$ .

(a) Probar que  $\rho$  es acotada en  $\mathbb{Z}$  (sugerencia: escribir cada entero en base  $p$ ).

(b) Probar que  $\rho$  es acotada por 1 en  $\mathbb{Z}$  (sugerencia: si  $\rho(n) > 1$  probar que existe  $m$  con  $\rho(m)$  arbitrariamente grande).

(c) Probar que si  $n$  no es divisible por  $p$  se tiene  $\rho(n) = 1$  (sugerencia  $nt + ps = 1$ ).

(d) Concluir que  $\rho$  es una potencia del valor absoluto  $p$ -ádico.

9. Sea  $\rho$  un valor absoluto en  $\mathbb{Q}$  en el que cada entero  $n$  satisface  $\rho(n) \geq 1$ . Probar que  $\rho$  es una potencia del valor absoluto usual o el trivial donde  $\rho(r) = 1$  para cada  $r$  en  $\mathbb{Q} - \{0\}$  (sugerencia: Si  $m$  y  $n$  son enteros positivos, escribir cada potencia  $m^r$  y usar la desigualdad triangular).

8. Sea un cuerpo  $K$  que contiene a  $\mathbb{Q}_p$  y que es completo con respecto a un valor absoluto  $\rho$  que extiende el de  $\mathbb{Q}_p$ . Probar que la serie

$$\log_p(1+x) = \sum_{k=1}^{\infty} \frac{x^k}{k}, \quad k \in \mathbb{N} \subseteq \mathcal{K}_p$$

$$\rho(k) = p^{-\nu_p(k)} \leq 1$$

converge para cada  $x$  en  $B(0; 1)$ . Probar que si  $x \in B(0; p^{-1/(p-1)})$  entonces  $\rho[\log_p(1+x)] = \rho(x)$ .

$$\rho(x) \leq p^{1/(p-1)} \Rightarrow N_p(x) \geq \frac{1}{p-1}$$

8. Sean  $K$  y  $\rho$  como en el problema precedente. Probar que la serie

$$\exp_p(x) = \sum_{k=0}^n \frac{x^k}{k!}$$

converge para cada  $x$  en  $B(0; p^{-1/(p-1)})$ .

$$\begin{aligned} & \rho(\exp_p(1+x)) \\ &= \rho\left(\sum_{k=1}^n \frac{x^k}{k}\right) \\ &\leq \max_{1 \leq k \leq n} \left\{ \rho\left(\frac{x^k}{k}\right) \right\} \end{aligned}$$

Problema 1. Basta probar que:  $\frac{p(x^n)}{p(n!)} \xrightarrow[n \rightarrow \infty]{} 0$

$$\text{Esto si } \underset{n \rightarrow \infty}{\underset{\approx 0}{\lim}} n \log p(x) - \log p(n!) \xrightarrow[n \rightarrow \infty]{} -\infty$$

pero: si  $n = p_1^{d_1} \cdots p_m^{d_m}$   
 $\Rightarrow n! = p_1^{d_1} \cdots p_m^{d_m} \Rightarrow \|n\|_p = d \quad \text{pero} \quad p^d \leq n$   
 $\alpha \log p \leq \log n \Rightarrow -\log p(n!) = -\log p^{d_m} = \alpha \log p \leq \log n$

$$\therefore n \log p(x) + \log n \xrightarrow[n \rightarrow \infty]{} -\infty.$$

Problema 2. Basta ver que  $\frac{p(x^n)}{p(n!)} \xrightarrow[n \rightarrow \infty]{} 0$  pol:  $n \log p(x) - \log p(n!) \xrightarrow[n \rightarrow \infty]{} -\infty$

si  $0 \leq k \leq n$  (cuando)  $n^k$  se divide por  $p_1^{p_1}, \dots, p_m^{p_m}, \quad p^k \leq n$

$$\left( \frac{n}{p_1} \right), \left( \frac{n}{p_2} \right), \dots, \left( \frac{n}{p_m} \right)$$

$$\Rightarrow n_p(n!) = \sum_{i=1}^k \left[ \frac{n}{p_i} \right], \quad \text{pero si} \quad p^k \leq n \Rightarrow k \leq \frac{\log n}{\log p}$$

$$-\log p(n!) = -\log p^{-k} = \alpha \log p \leq \sum_{i=1}^k \left[ \frac{n}{p_i} \right] \cdot \log p$$

$$\text{Luego} \quad n \log p(x) - \log p(n!) \leq \underbrace{n \log p(x)}_{> 0} + \left( \sum_{i=1}^k \left[ \frac{n}{p_i} \right] \right) \log p$$

$$\leq n \log p(x) + \left( \sum_{i=1}^k \left( \frac{n}{p_i} \right) \cdot 1 \right) \log p$$

$$\leq n \log p(x) + n \left( \sum_{i=1}^k \frac{1}{p_i} \right) \log p$$

$$\leq n \frac{1}{p-1} \log p + n \left( \sum_{i=1}^k \frac{1}{p_i} \right) \log p$$

$$\leq n \log p \left( \frac{-\left(\frac{1}{p}\right)^{k-1}}{p-1} \right)$$

$$\text{Si } p < \frac{1}{p-1}$$

$$\sum a_i = \frac{\frac{1}{p} - \left(\frac{1}{p}\right)^k}{1 - \frac{1}{p} \left(\frac{1}{p}\right)^k} = \frac{1}{p-1}$$

## Teoría de Números

problema 1. Si la función  $p: K \rightarrow [0, \infty[$  del cuerpo  $K$  satisface:

$$(a) p(x) = 0 \text{ si } x = 0$$

$$(b) p(ab) = p(a)p(b)$$

$$(c) p(a) \leq 1 \Rightarrow p(1+a) \leq 1$$

entonces  $p \in \mathbb{N}_2$  cumple con la desigualdad triangular fuerte.

Demonstración: Sea  $a, b \in K$ . S.P.G.:  $p(a) \leq p(b)$  p.d.:  $p(a+b) \leq p(b)$ .

Dem: observe que  $p\left(\frac{a}{b}\right) = \frac{p(a)}{p(b)}$

$$\Rightarrow p\left(\frac{a}{b}\right) \leq 1 \Rightarrow p\left(1 + \frac{a}{b}\right) \leq 1 \Rightarrow p(b+a) \leq p(b)$$

$$\therefore p(a+b) \leq \max\{p(a), p(b)\}$$

$$\therefore p(a+b) \leq \max\{p(a), p(b)\} \leq p(a) + p(b) \quad \therefore p \in \mathbb{N}_2.$$

problema 2. Probar que si  $p \in \mathbb{N}_2$  en  $K \Rightarrow \forall x \in K : p(-x) = p(x)$ .

Demonstración: Demostraremos que  $p(-1) = 1$ .

en efecto:  $p(1) = p(-1)^2$ , pero  $p(1) = p(1)^2 \Rightarrow p(1) = 0 \text{ o } p(1) = 1$ .

$$\Rightarrow p(1) = 1 \Rightarrow 1 = p(-1)^2 \Rightarrow p(-1) = 1.$$

$$\therefore p(-x) = p(-1) p(x) = p(x).$$

problema 3. Det. cuales de los sigts. succ. conv. en la norma  $\|\cdot\|_2$  indicada

Calcule su límite

$$(a) a_n = 2^n, \text{ con } p = 2.$$

p.d.:  $a_n \xrightarrow[n \rightarrow \infty]{} \infty$   $\|a_n\|_2 = 2^{-n} \xrightarrow{n \rightarrow \infty} 0$ .

$$(b) a_n = 2^{-n}, p = 2.$$

p.d.:  $a_n$  no converge pues  $\|a_n\|_2 = 2^n \xrightarrow{n \rightarrow \infty} \infty$

$$(c) a_n = 1 + 2 + \dots + 2^n, p = 2.$$

p.d.:  $a_n \xrightarrow[n \rightarrow \infty]{} \infty$ ,  $a_n = 1 + 2 + \dots + 2^n = \frac{2^{n+1} - 1}{2 - 1} = 2^{n+1} - 1$

$$\|a_n\|_2 = 2^{-(n+1)} \xrightarrow{n \rightarrow \infty} 0$$

$$(d) a_n = 1 + 4^n, p = 2.$$

p.d.:  $a_n \xrightarrow[n \rightarrow \infty]{} \infty$ ,  $\|a_n\|_2 = 2^{-2n} \xrightarrow{n \rightarrow \infty} 0$ .

$$(e) a_n = 4^n, p = 3 \text{ Basta ver que es de Cauchy: } \|a_n - a_m\|_3 = \|4^n - 4^m\|_3,$$

$$\text{Si: } 3 \equiv 0 \equiv 4^n - 4^m \quad \exists k \in \mathbb{N} \text{ tal que } 4^k \mid 4^n - 4^m$$

problema 5. K cuerpo con n.z. p. gesatstue der. trian. fuerte

$$\text{y def: } B(a,r) = \{x \in K : p(x-a) < r\}$$

$$\text{Se } a, b \in B(a,r) : B(a,r) = B(b,r).$$

$$\underline{\text{Demostacion:}} \quad \text{Si } c \in B(b,r) \Rightarrow p(c-b) < r, \text{ pero } p(b-a) < r$$

$$\Rightarrow p(c-a) \leq \max\{p(c-b), p(b-a)\} < r$$

$$\therefore c \in B(a,r)$$

$$\therefore B(b,r) \subseteq B(a,r)$$

$$\text{Sea } c \in B(a,r) \Rightarrow p(a-c) < r, \text{ pero } p(b-a) < r$$

$$\Rightarrow p(c-b) \leq \max\{p(a-c), p(b-a)\} < r$$

$$\therefore c \in B(b,r)$$

$$\therefore B(b,r) \supseteq B(a,r) \quad \therefore B(b,r) = B(a,r).$$

problema 6. p v.a en K y p primo:  $p(p) < 1$ .

(a) Probar que  $p$  es acotada en  $\mathbb{Z}$

$$\text{Dem: Si } n \in \mathbb{Z} \Rightarrow n^r = a_0 + a_1 p + \dots + a_{p-1} p^{p-1}, \quad a_i \in \{0, \dots, p-1\}$$

$$\begin{aligned} \text{Luego } p(n) &\leq \sum_{i=0}^{p-1} p(a_i) p(p)^i, \quad n = \max\{p(a_i)\}_{i=1}^{p-1} \\ &\leq \sum_{i=1}^{p-1} p(a_i) \leq (t+1) M. \Rightarrow p(n) \leq (t+1) M^{\frac{1}{r}} \xrightarrow[r \rightarrow \infty]{} 1 \\ &\therefore p(n) \leq 1. \end{aligned}$$

(b) Probar que  $p$  acotada por len  $\mathbb{Z}$ .

$$\text{Si } p(n) > 1 \Rightarrow n^r \text{ estaria } \underset{r \rightarrow \infty}{\rightarrow} \infty \quad \therefore n^r \in \mathbb{Z} \quad \therefore p \text{ acotada en } \mathbb{Z}$$

$\therefore p$  acotada por len  $\mathbb{Z}$

(c) Probar que si  $p+n \Rightarrow p(n)=1$ .

$$\text{Si } p+n \Rightarrow (p+n) = 1 \Rightarrow \exists s, t \in \mathbb{Z} : s p + n t = 1, \quad \text{Si } p(n) < 1$$

$$\therefore p(n) = 1 = p(s p + t n) \leq \max\{p(s)p(t), p(t)p(n)\} < \max\{p(s), p(t)\} \quad \times$$

$$\therefore p(n)=1. \quad \text{Este piso si } \mathbb{Z} \text{ acotado: Si } p(a) \leq p(b) \Rightarrow p\left(\frac{a+b}{2}\right) \leq 1$$

$$\therefore p(a+b) \leq p(b) \quad p\left(\frac{a+b}{2}\right) \leq p(b). \quad \therefore \text{cumple dico. D. fuerte}$$

(d) Si:  $p \notin \mathbb{Z}$ . del N.A p-ndico.

$$\text{Sea } \frac{a}{b} \in \mathbb{Q}, b \neq 0 \quad (a, b) = 1. \quad p(a) = p\left(\frac{a_1}{p_1} \dots \frac{a_n}{p_n}\right)^{d_n} = \frac{p(a)}{p_1^{d_1} \dots p_n^{d_n}}, \quad \text{Sea } C = \frac{\log p(a)}{\log p}$$

$$\Rightarrow p(a) = \left(\frac{1}{p}\right)^{-C} = \left(\left(\frac{1}{p}\right)^{\log(a/b)}\right)^C = \|a/b\|_p^C \Rightarrow p\left(\frac{a}{b}\right) = \left\|\frac{a}{b}\right\|_p^C.$$

problema 3) Sabemos que:  $\rho(Lip(\lambda+x)) = \rho\left(\sum_{n=1}^{\infty} \frac{x^n}{n}\right)$

para por principio de dominancia paracádicas:

$$\text{pd: } \rho(x) \geq \rho\left(\frac{x^n}{n}\right), \forall n \geq 2 \quad \text{rel: } v_p(x) \leq v_p\left(\frac{x^n}{n}\right)$$

$$\text{Dem: } v_p\left(\frac{x^n}{n}\right) = n v_p(x) - v_p(n)$$

$$\text{pd: } n \geq p^{v_p(n)} \Rightarrow \frac{\log n}{\log p} \geq v_p(n)$$

$$\forall x \in B(0: p^{-\frac{1}{p-1}}) \Rightarrow v_p(x) > \frac{1}{p-1}$$

problema 4.  $\ell_{x, p}(x) = \sum_{k=0}^{\infty} \frac{x^k}{k!}$  converge

$$\text{equivalentemente: } k v_p(x) - v_p(k!) \xrightarrow[k \rightarrow \infty]{} \infty$$

$$\text{Dem: } v_p\left(\frac{x^k}{k!}\right) \xrightarrow[k \rightarrow \infty]{} 0 \quad \text{Dem: } v_p(k!) = \sum_{i=1}^{\infty} \left[\frac{k}{p^i}\right] \leq \sum_{i=1}^{\infty} \left(\frac{k}{p^i}\right) = k \frac{1-p^{-k}}{p-1} \xrightarrow[k \rightarrow \infty]{} \infty$$

$$\therefore k v_p(x) - v_p(k!) \geq k v_p(x) - k \frac{1-p^{-k}}{p-1} = k \left(v_p(x) - \frac{1}{p-1}\right) \xrightarrow[k \rightarrow \infty]{} \infty$$

$\therefore$  converge  $\forall x \in B(0: p^{-\frac{1}{p-1}})$

problema 4. Queremos que  $\sum_{k=1}^{\infty} \frac{x^k}{(k!)^2}$  converja en  $U_3$ .

H) esto sucede si:  $\left\| \frac{x^k}{(k!)^2} \right\|_3 \xrightarrow[k \rightarrow \infty]{} 0$  equivalentemente:

$$k v_3(x) - v_3((k!)^2) = k v_3(x) - 2 v_3((k!)) \xrightarrow[k \rightarrow \infty]{} \infty$$

Dem: Sabemos que:  $v_3((k!)) \leq \sum_{i=1}^{\infty} \left[\frac{k}{3^i}\right] \leq \sum_{i=1}^{\infty} \left(\frac{k}{3^i}\right) = k \frac{1}{3-1} = \frac{k}{2}$

$$\text{y la aproximación es óptima pues: } \sum_{i=1}^n \left[\frac{k}{3^i}\right] / \sum_{i=1}^n \left(\frac{k}{3^i}\right) \xrightarrow[k \rightarrow \infty]{} 1. \quad (*)$$

$$\text{Supong: } k v_3(x) - 2 v_3((k!)) \geq k v_3(x) - 2 \frac{k}{2} = k(v_3(x)-1)$$

$\therefore$  J) dice converge  $\forall x \in B(0, 3^{-1})$ . (óptima  $p=3$ )

Dem: Solucion que destaca que: s:  $x \in B(0, 3^{-1}) \Rightarrow v_3(x) > 1$

$$k v_3(x) - 2 v_3((k!)) \geq k \underbrace{(v_3(x)-1)}_{> 0} \xrightarrow[k \rightarrow \infty]{} \infty$$

problem 4d. (Converge en  $\mathbb{K}_3$ :  $\sum_{i=1}^{\infty} \frac{3^n}{n!}$  ?)

Basta demostrar que  $\left\| \frac{3^n}{n!} \right\|_3 \xrightarrow{n \rightarrow \infty} 0$  (entonces  $\|x\|_3 = \left(\frac{1}{3}\right)^{V_p(x)}$ )

$$\text{obtenemos: } V_3\left(\frac{3^n}{n!}\right) = n \cdot V_3(n!) \xrightarrow{n \rightarrow \infty} \infty$$

$$\text{pero: } V_3(n!) = \sum_{i=1}^n \left(\frac{n}{3^i}\right) \leq \sum_{i=1}^n \left(\frac{n}{2^i}\right) = \frac{n}{2}$$

$$\therefore V_3\left(\frac{3^n}{n!}\right) \geq n - \frac{n}{2} = \frac{n}{2} \xrightarrow{n \rightarrow \infty} \infty \quad \therefore \text{Converge en } \mathbb{K}_3.$$

problem 4e. (Converge en  $\mathbb{K}_p$ :  $\sum_{k=0}^{\infty} p^k \binom{1/2}{k}$ )

$$\text{donde: } \binom{1/2}{k} = \frac{f^{(k)}(0)}{k!}, \quad f(x) = \sqrt{x+1}, \quad f'(x) = \frac{1}{2}(x+1)^{-1/2}, \quad f''(x) = -\frac{1}{4}(x+1)^{-3/2}$$

$$f'''(x) = +\frac{3}{8}(x+1)^{-5/2}$$

$$\text{pd: } f^k(x) = -(-1)^k \frac{1 \cdot 3 \cdots (2k-3)(x+1)^{-2k-1}}{2^k}$$

$$\text{Denn: } f^{k+1}(x) = -(-1)^{k+1} \frac{1 \cdot 3 \cdots (2k-3)(2k-1)(x+1)^{-2k-2}}$$

$$\text{Luego: } \binom{1/2}{k} = \frac{(-1)^{k+1} 1 \cdot 3 \cdots (2k-3)}{k! 2^k} \quad \forall k \geq 2 \quad p \neq 2.$$

$$\text{pd: } \left\| p^k \binom{1/2}{k} \right\|_p \xrightarrow{k \rightarrow \infty} 0 \Leftrightarrow V_p\left(p^k \binom{1/2}{k}\right) \xrightarrow{k \rightarrow \infty} 0 \Leftrightarrow k - V_p\left(\binom{1/2}{k}\right) \xrightarrow{k \rightarrow \infty} \infty$$

$$\Leftrightarrow k - V_p\left(\frac{(-1)^{k+1} 1 \cdot 3 \cdots (2k-3)}{k! 2^k}\right)$$

$$\Leftrightarrow k - V_p(1 \cdot 3 \cdots (2k-3)) + V_p(k!) \xrightarrow{k \rightarrow \infty} \infty$$

$$\text{pero: } V_p(k!) = \sum_{i=1}^{\infty} \left[ \frac{k}{p^i} \right] \Rightarrow \frac{k}{p} \leq V_p(k!)$$

$$\begin{aligned} V_p(1 \cdot 3 \cdots (2k-3)) &= V_p((2k-3)!) - V_p(2^k (k-1)!) & kp(p-1) + k(p-1) + (k-1)p - (2k-3)p \\ &= V_p((2k-3)!) - V_p(\underline{(k-1)!}) &= k(p^2 + p - 1 + p - 2p) \end{aligned}$$

$$\Rightarrow -V_p(1 \cdot 3 \cdots (2k-3)) = V_p((k-1)!) - V_p((2k-3)!)$$

$$\text{Luego: } V_p\left(f^k\left(\binom{1/2}{k}\right)\right) \geq k + \frac{k}{p} + \frac{k-1}{p} - \sum_{i=1}^{\infty} \left[ \frac{2^{k-1}}{p^i} \right] \leq \frac{k-1}{p} - \left(2^{k-3}\right) \frac{1}{p-1} \quad \frac{1 - (1/p)^k}{1 - 1/p}$$

$$= \frac{k(p^2 - 1) + 4p}{p(p-1)} \xrightarrow{k \rightarrow \infty} \infty.$$

problema 4

Si  $p(\pi_1), p(\pi_2) < 1$  entonces: Como  $(\pi_1, \pi_2) = \mathbb{Z}(i)$   
 $\Rightarrow \exists a, b \in \mathbb{Z}(i): 2\pi_1 + b\pi_2 = 1$ . Si  $a, b \in \mathbb{Z}(i) \Rightarrow p(a), p(b) \leq 1$ .

Luego:  $p(1) = p(2\pi_1 + b\pi_2) = \max \{ p(2)p(\pi_1), p(b)p(\pi_2) \} = 1$ .   
 Luego  $1 < \max \{ p(a), p(b) \} \leq 1 \quad (*)$    
 Luego  $1 < \max \{ p(a), p(b) \} \leq 1 \quad (*)$    
 $\Rightarrow p(a) = p(\underbrace{a+i\bar{a}}_{\in \mathbb{Z}}) \parallel_p \leq 1$ .

## Teoría de Números.

### Prueba 3

Julio 17 de 2012

Escoja 4 de los cinco problemas siguientes:

1. Probar que la serie

$$\sum_{n=1}^{\infty} n!$$

es convergente en  $\mathbb{Z}_p$  para cada primo  $p$ .

$$\begin{aligned} \sum_{k=1}^{\infty} \sum_{n=1}^{\infty} \frac{(p^n)^m}{m} &= \sum_{m=1}^{\infty} \sum_{n=2}^{k+1} (p^n)^m \\ &= \sum_{m=1}^{\infty} \frac{p^{(k+1)m} - p^2}{p^m - 1} \end{aligned}$$

2. Probar que si  $K$  es un cuerpo con un valor absoluto  $\rho$  que satisface la desigualdad triangular fuerte y si definimos

$$B(a; r) = \{x \in K \mid \rho(x - a) < r\},$$

entonces para cada punto  $b \in B(a; r)$  se tiene  $B(a; r) = B(b; r)$ .

3. Probar que toda sucesión en  $\mathbb{Z}_p$  tiene una subsucesión convergente.

4. Sea  $\rho$  un valor absoluto no arquimediano definido en el cuerpo  $\mathbb{Q}(i)$ . Sean  $\pi_1$  y  $\pi_2$  dos primos distintos en  $\mathbb{Z}[i]$ . Probar que  $\rho(\pi_1)$  y  $\rho(\pi_2)$  no pueden ser menores que 1 simultáneamente.

5. Probar que, para cada primo  $p$ , la serie

$$\sum_{n=2}^{\infty} \log_p(1 + p^n) = \sum_{n=2}^{\infty} \left( \sum_{m=1}^{\infty} \frac{(p^n)^m}{m} \right)$$

es convergente, donde

$$x_k = \sum_{n=1}^k n!$$

$$\log_p(1 + x) = \sum_{n=1}^{\infty} \frac{x^n}{n}$$

bien definido:

Definición:  $x_k = \sum_{n=1}^k n!$   $\log_p(1 + x) = \sum_{n=1}^{\infty} \frac{x^n}{n}$ , si  $x \in B(0, 1)$ , pero  $p^n \in B(0, 1)$ .  $\parallel p^n \parallel = p^{-n} \in B(0, 1)$

y  $k \rightarrow \infty \Rightarrow x \in \mathbb{Z}_p$

problema 1: Baste demostrar que  $(x_k) \in$  de Cauchy pues como  $\mathbb{Z}_p = B(0, 1)$  es completo  $\Rightarrow x_k$  converge  $\mathbb{Z}_p$

Como  $\log_p(1 + x) = \sum_{n=1}^{\infty} \frac{x^n}{n}$  es no-arquimediano

Y esto si:  $\lim_{k \rightarrow \infty} \parallel k! \parallel_p = 0$

Y esto tiene que: si  $k \geq p^l$ , la mayor potencia que divide en la cota

entonces  $\left[ \frac{n}{p} \right] = n$  de elementos entre 0 y  $n$  son divisibles por  $p$

$\therefore \left[ \frac{n}{p} \right] = n^0 \parallel p \parallel^l \text{ (de } k, p^l \Rightarrow \frac{\log k}{\log p} > l \Rightarrow -l \geq -\frac{\log k}{\log p} \text{)}$

AMBR

$$\text{Luego: } N_p(k!) = \sum_{i=1}^k \left[ \frac{k}{p^i} \right] \geq \sum_{i=1}^k \frac{\frac{k}{p^i} - 1}{\frac{p-1}{p} - 1} \cdot k$$

$$\geq \frac{k \cdot \left( 1 - \left( \frac{1}{p} \right)^{k-1} \right) \cdot \log p}{(p-1)} \xrightarrow[k \rightarrow \infty]{} \infty$$

$$y K - 2 \log K = \log e^K - 2 \log K = \log \left( \frac{e^K}{K^2} \right) \xrightarrow[K \rightarrow \infty]{} \infty$$

$$\therefore N_p(k!) \xrightarrow[K \rightarrow \infty]{} \infty \quad \because \sum_{n=1}^{\infty} n! \text{ converge en } \mathbb{K}_p.$$

Problema 5. Para probar que  $\sum_{n=2}^{\infty} \log_p (1+p^n)$  converge, basta demostrar que es de Cauchy esd:  $X_k = \sum_{n=2}^k \log_p (1+p^n)$ . Si  $k, m; k > m$ :  $\|X_k - X_m\|_p = \left\| \sum_{n=m+1}^k \log_p (1+p^n) \right\|_p$

$$\leq \left\| \log_p (1+p^{m+1}) \right\|_p \quad \text{pd: } N_p(\log_p(1+p^{m+1})) \xrightarrow[m \rightarrow \infty]{} 0 \quad \Rightarrow \left\| \log_p (1+p^{m+1}) \right\|_p \xrightarrow[m \rightarrow \infty]{} 0$$

Más:  $\left\| \log_p (1+p^n) \right\|_p = \left\| \sum_{m=1}^{\infty} \frac{p^{nm}}{m} \right\|_p \leq \left\| \sum_{m=1}^{\infty} \frac{p^{(n-1)m}}{m} \right\|_p \leq \left\| \log_p (1+p^{n-1}) \right\|_p$

$$\left\| p^{-1} \right\|_p \left\| \sum_{m=1}^{\infty} \frac{p^m}{m} \right\|_p = p^{-1} \left\| \sum_{m=1}^{\infty} \frac{p^m}{m} \right\|_p$$

Demonstración:  $N_p(\log_p(1+p^{m+1})) = \lim_{k \rightarrow m} \left\| \sum_{n=2}^k \frac{p^{nm}}{n} \right\|_p$

Lemma: Si  $\|a_i\| \leq \|a_n\|, \forall n \geq 2$

Prueba: Sea  $\left\| \sum_{n=2}^{\infty} a_n \right\|_p \leq \|a_n\|_p$  si  $k > m$   $\left\| \sum_{n=m+1}^{\infty} a_n \right\|_p \leq \|a_n\|_p \leq \|a_m\|_p$

Aclaración:  $\left\| p^{m+1} \right\|_p \geq \left\| \frac{p^{nm}}{n} \right\|_p \quad \forall n \geq 2 \quad \text{pd: } N_p\left(\frac{p^{nm}}{n}\right) \geq N_p(p^m) = m$

Más:  $N_p\left(\frac{p^{nm}}{n}\right) = nm - N_p(n) > nm - n = n(n-1) \geq m, \forall n \geq 2$

Por lo tanto:  $N_p\left(\frac{p^{nm}}{n}\right) < n$

$\therefore \left\| \log_p (1+p^{m+1}) \right\|_p \leq \left\| p^{m+1} \right\|_p \xrightarrow[m \rightarrow \infty]{} 0$

$\sum_{n=2}^{\infty} \log_p (1+p^n)$  converge en  $\mathbb{K}_p$ .

Aclaración:

$$n, m \in \mathbb{N} \geq 2$$

$$\frac{(n-1)m}{m} \geq \frac{n}{n-1}, \quad \text{si } n \geq 2, \text{ más } m \in \mathbb{N}.$$

# Teoría de Números

## Closure ???

$$\Lambda \subseteq \mathbb{Q}^2, \quad \Lambda \subseteq \mathbb{Z}^2$$

Observación. Si  $\Lambda$  es un reticulado y  $L \subseteq \Lambda$  satisface  $aL \subseteq L$  para algún  $a \in \mathbb{Z}$ , entonces  $L$  es reticulado

Dem.  $\Lambda \subseteq \mathbb{Z}^2 \Rightarrow \Lambda \cong \mathbb{Z}^2$

$$\begin{aligned}\Lambda &\subseteq \mathbb{Z} \\ \Lambda &= \langle 0 \rangle\end{aligned}$$

$$\varphi: \mathbb{Z}^3 \hookrightarrow \mathbb{Z}^2 ?$$

$$e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad e_3 = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

$\varphi(e_1), \varphi(e_2), \varphi(e_3)$  linealmente independientes en  $\mathbb{Z}^2$ .  
 $\Rightarrow$  linealmente independientes en  $\mathbb{Q}^2$ .

Sea  $K$  un cuerpo de números. Un reticulado en  $K^n$  es un  $\mathbb{Q}_K$ -módulo submódulo  $\Lambda$  de  $K^n$  tal que existen  $\alpha$  y  $\beta$  en  $K^*$  tales que

$$\beta \mathcal{O}_K^n \subseteq \Lambda \subseteq \alpha \mathcal{O}_K^n$$

Proposición 1. Si  $\Lambda, \Lambda'$  son reticulados en  $\mathbb{Q}^2$ , entonces  $\Lambda_p = \Lambda'_p$  para ~~esta~~ casi todo  $p$ .

Proposición 2. Si  $\Lambda_p = \Lambda'_p$  para todo  $p$ , entonces  $\Lambda = \Lambda'$

Proposición 3. Si  $\{\Lambda(p)\}_{p \in \Pi_f(\mathbb{Q})}$  es una familia de reticulados  $\Lambda(p)$  en  $\mathbb{Q}_p^2$ , y  $\Lambda(p) = \Lambda'_p$  para casi todo  $p$  y algún reticulado  $\Lambda'$  fijo,

entonces existe un reticulado  $\Lambda$  con  $\Lambda_p = \Lambda(p) \nmid p$ .

Hecho.  $\mathcal{O}_K$  es un reticulado

Hecho. Estos resultados se extienden a  $\mathbb{Z}^n$ .

Sea  $\Lambda$  un reticulado en  $K^n \cong \mathbb{Q}^{[K:\mathbb{Q}]} = \mathbb{Z}^n$

$$\text{y } \mathcal{O}_K^n \cong \mathbb{Z}^n$$

$\alpha \in K \Rightarrow \alpha \mathcal{O}_K$  es reticulado

Basta ver que en  $r, s \in \mathbb{Q}$  tales que  $r\mathcal{O}_K \subseteq \alpha \mathcal{O}_K \subseteq s\mathcal{O}_K$

Si  $\alpha$  es algebraico, existe  $n \in \mathbb{Z}$  tal que  $n\alpha$  es entero

$$n\alpha \mathcal{O}_K \subseteq \mathcal{O}_K$$

$$\alpha \mathcal{O}_K \subseteq n^{-1}\mathcal{O}_K$$

mostrar entero

$$\Rightarrow \alpha^{-1}\mathcal{O}_K \subseteq m^{-1}\mathcal{O}_K$$

$$\Rightarrow \mathcal{O}_K \subseteq \alpha m^{-1}\mathcal{O}_K$$

$$\Rightarrow m\mathcal{O}_K \subseteq \alpha \mathcal{O}_K$$

Observación.  $\Lambda$  net en  $K^n$

$\Lambda'$  net en  $K^m$

$\Lambda \times \Lambda'$  net en  $K^{n+m}$

$$(\alpha \mathcal{O}_K)^n = \alpha^n \mathcal{O}_K^n \subseteq \Lambda \subseteq \beta \mathcal{O}_K^n$$

$$\alpha^m \mathcal{O}_K^m \subseteq \Lambda' \subseteq \beta' \mathcal{O}_K^m$$

(3)

Basta ver que dados  $\alpha, \alpha' \in K$  existe  $\alpha'' \in K$  con

$$\alpha''\mathcal{O}_K \subseteq \alpha\mathcal{O}_K$$

$$\alpha''\mathcal{O}_K \subseteq \alpha'\mathcal{O}_K$$

$\exists n, m$  tales que  $n\alpha^{-1}, m(\alpha')^{-1}$  son enteros

$n\alpha^{-1}, nm(\alpha')^{-1}$  son enteros

$$nm\alpha^{-1}\mathcal{O}_K \subseteq \mathcal{O}_K$$

$$nm\mathcal{O}_K \subseteq \alpha'\mathcal{O}_K$$

Similamente  $nm\mathcal{O}_K \subseteq \alpha\mathcal{O}_K$

$$\alpha''\mathcal{O}_K^n \times \alpha''\mathcal{O}_K^m \subseteq \Lambda \times \Lambda'$$

$$\alpha''(\mathcal{O}_K^n \times \mathcal{O}_K^m) \subseteq \Lambda \times \Lambda'$$

□

Si  $\mathfrak{f}$  es un lugar en  $K$  (no arquimediano),  $K_{\mathfrak{f}}$  completado  $\mathfrak{f}$ -ádico

( $\mathcal{O}_{\mathfrak{f}}$  anillo de enteros sobre de  $K_{\mathfrak{f}}$ )

$p_{\mathfrak{f}}$  valor absoluto en  $K$

$$p_{\mathfrak{f}}|_{\mathbb{Q}} = 1 \circ |_p \quad " \mathfrak{f} \text{ es un lugar sobre } p "$$

$$K_p = K \otimes_{\mathbb{Z}} \mathcal{O}_p$$

$$K = (\mathbb{Z}[t])/(f)$$

$$K_p = (\mathcal{O}_p[t])/(f), \quad f = f_1 \dots f_r$$

$$K_p = \frac{\mathcal{O}_p[t]}{(f_1)} \times \dots \times \frac{\mathcal{O}_p[t]}{(f_r)}$$

$$K_p = K_{\mathfrak{f}_1} \times \dots \times K_{\mathfrak{f}_r}$$

Λ  $\mathbb{Z}_l$ -reticulado en  $K^n \cong \mathbb{Q}^N$

$\Lambda_p$   $\mathbb{Z}_l$ -reticulado en  $K_p^n \cong \mathbb{Q}_p^N$

$\Lambda_p$   $\mathbb{Z}_l$ -reticulado en  $K_p^n \cong K_{g_1}^n \times \cdots \times K_{g_r}^n$

$$\mathcal{O}_p = \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_{\mathfrak{p}}$$

Se puede probar que

$$\mathcal{O}_p = \mathcal{O}_{g_1} \times \mathcal{O}_{g_2} \times \cdots \times \mathcal{O}_{g_r}$$

$\mathcal{O}_p$  contiene a  $P_i = (1, 0, \dots, 0)$ , etc (idempotentes)

Λ es  $\mathcal{O}_K$ -reticulado

$$\mathcal{O}_K \Lambda \subseteq \Lambda$$

$$\Lambda_p \supseteq P, \Lambda_p \subseteq P, K^n = K_{g_1}^n$$

$$\Lambda_p = P_1 \Lambda_p \times P_2 \Lambda_p \times \cdots \times P_r \Lambda_p$$

$P_i \Lambda_p$  reticulado en  $K_{g_i}^n$

$$P_i \Lambda_p = \Lambda_{g_i} \leftarrow \text{completado en } g_i$$

Λ  $\mathcal{O}_K$ -reticulado  $\Rightarrow \Lambda_{g_i}$   $\mathcal{O}_{g_i}$ -reticulado ( $g_i \in \Pi_p(K)$ )

Proposición.  $\Lambda, \Lambda'$  reticulados en  $K^n$ ,

$$\Lambda_g = \Lambda_{g'} \text{ para } \cancel{\text{esta}} \text{ casi todo } g$$

Proposición. Si  $\Lambda_g = \Lambda_{g'}$  para todo  $g \Rightarrow \Lambda = \Lambda'$

Proposición. Sea  $I \subseteq \mathcal{O}_K$  ideal ( $K/\mathbb{Q}$  cuadrática) entonces existen  $\alpha, \beta \in \mathcal{O}_K$  tales que  $I = (\alpha, \beta)$

Observación.  $I$  ideal,  $\alpha \in I$

$$\alpha \mathcal{O}_K \subseteq I \subseteq \mathcal{O}_K \\ \Rightarrow I \text{ es reticulado}$$

$$J = \alpha \mathcal{O}_K, J \subseteq I$$

$$f \in \Pi_p(K)$$

$$J_f = \alpha \mathcal{O}_f \subseteq I_f$$

además  $J_f = I_f$  para casi todo  $f$ .

Sean  $f_1, \dots, f_s$  los lugares donde  $J_{f_i} \neq I_f$

Sea  $\pi_i \in \mathcal{O}_{f_i}$  parámetro uniformizante

$$I_{f_i} = (\pi_i^{t_i}) \supseteq J_{f_i} = (\alpha)$$

$$v_{f_i}(\alpha) \geq t_i$$

Sean  $\sigma_j, \dots, \sigma_l$  los lugares donde  $J_{\sigma_j} = I_{\sigma_j}$  y  $I_{\sigma_j} \neq \mathcal{O}_{\sigma_j}$

Escogemos  $\beta \in \mathcal{O}_K$  tal que  $v_{f_i}(\beta) = t_i, i = 1, \dots, s$

$$v_{\sigma_j}(\beta) \geq v_{\sigma_j}(\alpha), j = 1, \dots, l$$

Afirmación.  $I = (\alpha, \beta)$

Sea  $I' = (\alpha, \beta)$ . Basta ver que  $I_f = I'_f \forall f$

Si  $f = f_i$ :

$$I_{f_i} = (\pi_i^{t_i}) = (\beta)$$

$$I'_{f_i} = (\alpha) + (\beta) = I_{f_i}$$

Si  $f = \phi_j$ :  $I_{\phi_j} = J_{\phi_j} = (\alpha)$

$$I'_{\phi_j} = (\alpha) + (\beta) = (\alpha) = I_{\phi_j}$$

Si  $f$  es cualesquier otro lugar:

$$(\alpha) = J_f = I_f = \mathcal{O}_f$$

$$I'_{\phi} = (\alpha) + (\beta) = \mathcal{O}_{\phi} = I_{\phi}$$

Ejercicio 1. Probar que  $\alpha \in K$  es un entero si y sólo si  $P_f(\alpha) \leq 1$  para todo  $f \in T\mathcal{O}_f(K)$

$I \subseteq \mathcal{O}_K$  ideal

$I_f$  para cada  $f$

$$I_f = (\pi_f)^{v_f(I)}$$

$I \subseteq \mathcal{O}_K$  ideal

$I_f$  para cada  $f$   
 $I_f = (\pi_f)^{v_f(I)}$

$I_f = \mathcal{O}_f \quad \forall f \quad v_f(I) = 0$

$m(f) \subseteq \mathcal{O}_K$  ideal

$m(f)_f = (\pi_f)$

$m(f)_\vartheta = \mathcal{O}_\vartheta \quad \vartheta = f$

$m(f)$  ideal maximal.

Ejercicio 2.  $I \subseteq \mathcal{O}_K$  es ideal si  $I_f \subseteq \mathcal{O}_f$  ideal  $\forall f$ .

Ejercicio 3.  $I, J \subseteq \mathcal{O}_K$  ideales  $\Rightarrow (IJ)_f = I_f J_f$

$$I' = \prod_{f \in I_f(K)} m(f)^{v_f(I)}$$

$$I'_\vartheta = m(\vartheta)^{v_\vartheta(I)} = (\pi_\vartheta)^{v_\vartheta(I)} = I_\vartheta$$

$$\therefore I' = I$$

■

$$I_1 \times I_2 \cong \mathcal{O}_K \times I_1 I_2$$

$$\{\alpha_f\}_f \quad \alpha \sim \alpha_f \quad ; \quad I_f = (\alpha_f) \quad , \quad I = (\alpha).$$

( f( ) )

Teoría de Números  
Desarrollo Tarea 4  
Marco Godoy V.

60

1	20
2	20
3	10

Problema 1. Determine cuántas extensiones del valor absoluto usual existen en el cuerpo  $L = \mathbb{Q}(\sqrt[3]{2})$ . Repita la pregunta si el valor absoluto usual se reemplaza por el valor absoluto 2-ádico o 5-ádico.

Demonstración

Caso I: valor absoluto usual.

El polinomio irreducible de  $L$  es  $p(x) = x^3 - 2 \in \mathbb{Q}[x]$  y  $\mathbb{R}$  es el completado de  $\mathbb{Q}$  con el valor absoluto usual.

Hacemos la extensión de escalares de  $L$  sobre  $\mathbb{R}$  y vemos cómo se comporta  $p(x)$  en esta extensión.

$$L \otimes_{\mathbb{Q}} \mathbb{Q}_{\infty} = L \otimes_{\mathbb{Q}} \mathbb{R} \cong \frac{\mathbb{Q}[x]}{(p(x))} \otimes \mathbb{R} \cong \frac{\mathbb{R}[x]}{(p(x))}$$

$$\cong \frac{\mathbb{R}[x]}{(x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4})} \quad (\sqrt[3]{2} \in \mathbb{R} \text{ es raíz de } p(x))$$

$$\cong \frac{\mathbb{R}[x]}{(x - \sqrt[3]{2})} \times \frac{\mathbb{R}[x]}{(x^2 + \sqrt[3]{2}x + \sqrt[3]{4})} \quad (\text{Teo. cloro de los nros})$$

$$\cong \mathbb{R} \times \frac{\mathbb{R}[x]}{(x^2 + \sqrt[3]{2}x + \sqrt[3]{4})}$$

Como el discriminante de la ecuación  $x^2 + \sqrt[3]{2}x + \sqrt[3]{4} = 0$  es negativo, sus raíces son complejas conjugadas,

$$\text{así } \frac{\mathbb{R}[x]}{(x^2 + \sqrt[3]{2}x + \sqrt[3]{4})} \cong \mathbb{C}$$

$$\therefore L \otimes_{\mathbb{Q}} \mathbb{Q}_\infty \cong \mathbb{R} \times \mathbb{C}$$

Se concluye que hay dos extensiones del valor absoluto usual, una real y una compleja.

Caso II : Valor absoluto 2-ádico .

Recordemos que  $[L : \mathbb{Q}] = ef$ , donde  $e$  es el índice de ramificación y  $f$  es el grado residual de la extensión.

Si  $\wp$  es un lugar sobre 2 , entonces

$$|\sqrt[3]{2}|_\wp^3 = |(\sqrt[3]{2})^3|_\wp = |2|_\wp = |2|_2 = \frac{1}{2}$$

$$\therefore |\sqrt[3]{2}|_\wp = \sqrt[3]{\frac{1}{2}}$$

Notemos que  $\sqrt[3]{\frac{1}{2}} \notin 2^{\mathbb{Z}}$ . Así  $\sqrt[3]{\frac{1}{2}} = |\sqrt[3]{2}|_\wp \in |L^*|_\wp$

pero  $|\sqrt[3]{2}|_\wp \notin |\mathbb{Q}^*|_2$ ,

$$\therefore [|\mathbb{L}^*|_\wp : |\mathbb{Q}^*|_2] = e \neq 1$$

Como  $[L : \mathbb{Q}] = 3$ , entonces  $f = 1$  (el grado residual es 1).

~~Entonces~~ se tiene que 2 es ramificado en la extensión  $L/\mathbb{Q}$ , o sea,  $|\cdot|_2$  se extiende de manera finita en  $L$ .

Caso III : Valor absoluto 5-ádico.

Tenemos que  $p(x) = x^3 - 2$ ,  $p'(x) = 3x^2$ . Ahora si  $\alpha \in \mathbb{Q}_5$  es raíz de  $p(x)$ , entonces

$$\alpha^3 - 2 = 0, \quad |\alpha^3 - 2|_5 = 0$$

pero en particular  $|\alpha^3 - 2|_5 \leq \frac{1}{5^t}, \forall t \in \mathbb{N}$ . La última desigualdad es equivalente a que

$$\alpha^3 - 2 \equiv 0 \pmod{5^t} \quad \forall t \in \mathbb{N}.$$

En particular  $\alpha^3 - 2 \equiv 0 \pmod{5}$ . Así, basta estudiar las raíces de  $p(x)$  módulo 5.

Los distintos cubos de  $\mathbb{F}_5$  son los siguientes

$$\begin{array}{lll} 0^3 \equiv 0 & 2^3 \equiv 3 & 4^3 \equiv 4 \\ 1^3 \equiv 1 & 3^3 \equiv 2 & \end{array}$$

Se sigue que  $\alpha^3 - 2 \equiv \alpha^3 + 3 \equiv 0 \pmod{5} \iff \alpha \equiv 3$ .

Como  $p'(3) \not\equiv 0 \pmod{5}$ ,  $p(x)$  no tiene raíces dobles (ni siquiera tiene más raíces que no sea 3); por el lema de Hensel levantamos a una única raíz de  $p(x)$  en  $\mathbb{Q}_5$ .

Así

$$\mathbb{L} \otimes_{\mathbb{Q}} \mathbb{Q}_5 \cong \mathbb{Q}_5 \times \mathbb{L}_{\sqrt[3]{2}}$$

Con esto,  $|\cdot|_5$  se extiende a dos valores absolutos de  $\mathbb{Q}(\sqrt[3]{2})$ .

Problema 2. Considere el reticulado  $\Lambda$  generado por los vectores  $(1, 2, 3)$ ,  $(4, 4, 5)$  y  $(1, 6, 8)$ . Determine los primos tales que  $\Lambda_p \neq \mathbb{Z}_p^3$ .

Demonstración

Tenemos  $\Lambda = (1, 2, 3) \mathbb{Z} \oplus (4, 4, 5) \mathbb{Z} \oplus (1, 6, 8) \mathbb{Z}$ . Si  $B = \{\hat{e}_1, \hat{e}_2, \hat{e}_3\}$  es la base canónica de  $\mathbb{Q}^3$ , buscamos un homomorfismo de  $\mathbb{Z}$  módulos  $T$  tal que

$$T(\hat{e}_1) = (1, 2, 3)$$

$$T(\hat{e}_2) = (4, 4, 5)$$

$$T(\hat{e}_3) = (1, 6, 8)$$

Inmediatamente,  $A = [T]_B = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 4 & 6 \\ 3 & 5 & 8 \end{pmatrix}$ . Con un pequeño cálculo obtenemos  $\det A = 2 \neq 0$  ( $A$  es invertible).  $A^{-1}$  es

$$A^{-1} = \frac{1}{2} \begin{pmatrix} 2 & -3 & 2 \\ 2 & 5 & -4 \\ -2 & -2 & 2 \end{pmatrix}$$

No olvidar que  $\Lambda = T\Lambda_0$ , con  $\Lambda_0 = \hat{e}_1 \mathbb{Z} \oplus \hat{e}_2 \mathbb{Z} \oplus \hat{e}_3 \mathbb{Z} = \mathbb{Z}^3$ . También  $A \in M_{3 \times 3}(\mathbb{Q})^*$ . Por lo visto en clases,  $\Lambda_p = \Lambda_0 p$  para casi todo  $p$  salvo en número finito. También

$\Lambda_p = T\Lambda_0 p = \Lambda_0 p$ , donde en ese caso  $A \in M_{3 \times 3}(\mathbb{Z}_p)^*$  (para casi todo  $p$ ) (Hecho:  $A \in M_{3 \times 3}(\mathbb{Q})^* \Rightarrow A \in M_{3 \times 3}(\mathbb{Z}_p)^*$  casi todo  $p$ ).

Para que  $A^{-1} \in M_{3 \times 3}(\mathbb{Z}_p)$ , cada coeficiente de esta matriz debe pertenecer a  $\mathbb{Z}_p$ ; teniendo así una condición necesaria y suficiente la cual es  $p \times 2$

$\left( \frac{m}{n} \in \text{el.} : \left| \frac{m}{n} \right|_p \leq 1 \Leftrightarrow p \times n \right)$

Se concluye que  $A_p \neq \mathbb{Z}_p^3$  siempre y cuando  $p = 2$ .

Problema 3. Sean  $W \subseteq V$  espacios vectoriales de dimensión finita. Sea  $\Lambda$  un reticulado en  $V$ , y sea  $M$  un reticulado en  $W$ . Probar que  $M_p \subseteq \Lambda_p$  para todo  $p$  salvo un número finito.

Demonstración. Si  $W \subseteq V$ , entonces  $M$  se puede identificar con un reticulado de  $V$ . Siendo así,

(de rango no maximal)

$M, \Lambda$  reticulados de  $V$

$\therefore M + \Lambda$  reticulado de  $V$

A continuación,  $(M + \Lambda)_p = \Lambda_p$  para casi todo  $p$ ; pero en un ese caso,  $\Lambda_p = (M + \Lambda)_p = M_p + \Lambda_p$

cuidado! con la definición de reticulado dada en  
clases  $M$  no es un ret. de  $V$ ,  
pues  $\alpha O_K \subseteq M$  no se cumple. Es un ret. de

subespacio  
de  $V$ .

$$\therefore \Lambda_p = M_p + \Lambda_p$$

$$\therefore M_p \subseteq \Lambda_p \quad (\text{para casi todo } p)$$

Anexo.  $M + \Lambda$  es un reticulado de  $K$ .

En efecto, existen  $\alpha, \alpha' \in \mathcal{O}_K$ ,  $\beta, \beta' \in \mathcal{O}_K$  tales que

$$\alpha \mathcal{O}_K \subseteq \Lambda \subseteq \beta \mathcal{O}_K$$

$$\alpha' \mathcal{O}_K \subseteq M \subseteq \beta' \mathcal{O}_K$$

?  $\alpha \mathcal{O}_K^n \subseteq \Lambda$ ?

$\Lambda \subseteq V \cong K^n$  !!

pero existen  $\alpha'', \beta'' \in \mathcal{O}_K$  tales que

$$\alpha'' \mathcal{O}_K \subseteq \alpha \mathcal{O}_K ;$$

$$\alpha'' \mathcal{O}_K \subseteq \alpha' \mathcal{O}_K$$

$$\beta \in \mathcal{O}_K \subseteq \beta'' \mathcal{O}_K$$

$$\beta' \in \mathcal{O}_K \subseteq \beta'' \mathcal{O}_K$$

$$\therefore \alpha''\mathcal{O}_K \subseteq \Lambda \subseteq \beta''\mathcal{O}_K$$

$$\alpha''\mathcal{O}_K \subseteq M \subseteq \beta''\mathcal{O}_K$$

$$\therefore \alpha''(\mathcal{O}_K + \mathcal{O}_K) \subseteq \Lambda + M \subseteq \beta''(\mathcal{O}_K + \mathcal{O}_K)$$

Así  $\alpha''\mathcal{O}_K \subseteq \Lambda + M \subseteq \beta''\mathcal{O}_K$ .

Como  $\Lambda, M$  son  $\mathcal{O}_K$ -módulos de  $V$ ,  $\Lambda + M$  es un  $\mathcal{O}_K$ -módulo de  $V$ .

$\therefore \Lambda + M$  es un reticulado.

Teoría de Números  
Desarrollo prueba 1  
María Godoy V

70

Problema 1

$$2240 = 1701 \cdot 1 + 539$$

$$1701 = 539 \cdot 3 + 84$$

$$539 = 84 \cdot 6 + 35$$

$$84 = 35 \cdot 2 + 14$$

$$35 = 14 \cdot 2 + 7$$

$$14 = 7 \cdot 2 + 0$$

	15
2	15
3	15
4	-
5	15

$$\therefore \text{mcd}(2240, 1701) = 7$$

SGS, Galerías  
@Gmail.com

## Problema 2.

$$\begin{cases} x \equiv 4 \pmod{7} \\ 3x+5 \equiv -1 \pmod{11} \\ x^2 \equiv 1 \pmod{23} \end{cases} \rightarrow \begin{cases} x \equiv 4 \pmod{7} \\ 3x \equiv 10-5 \pmod{11} \\ x^2 \equiv 1 \pmod{23} \end{cases}$$

$$\rightarrow \begin{cases} x \equiv 4 \pmod{7} \\ 3x \equiv 5 \pmod{11} \\ x^2 \equiv 1 \pmod{23} \end{cases} \xrightarrow{3^{-1} \equiv 4 \pmod{11}} \begin{cases} x \equiv 4 \pmod{7} \\ x \equiv 20 \pmod{11} \\ x^2 \equiv 1 \pmod{23} \end{cases}$$

$$\rightarrow \begin{cases} x \equiv 4 \pmod{7} \\ x \equiv 9 \pmod{11} \\ x^2 \equiv 1 \pmod{23} \end{cases}$$

Como  $x^2 - 1 = (x-1)(x+1)$ , entonces en módulo 23,  $x_1 \equiv 1$ ,  $x_2 \equiv 22$  son soluciones de  $x^2 \equiv 1 \pmod{23}$

Debemos estudiar los sistemas

$$\begin{cases} x \equiv 4 \pmod{7} \\ x \equiv 9 \pmod{11} \\ x \equiv 1 \pmod{23} \end{cases} \quad \begin{cases} x \equiv 4 \pmod{7} \\ x \equiv 9 \pmod{11} \\ x \equiv 22 \pmod{23} \end{cases}$$

Primero estudiamos las soluciones de

$$\begin{cases} x \equiv 4 \pmod{7} \\ x \equiv 9 \pmod{11} \\ x \equiv 1 \pmod{23} \end{cases}$$

$$\begin{cases} x \equiv 4 \pmod{7} \\ x \equiv 9 \pmod{11} \end{cases} : \text{ como } 1 = 7 \cdot 8 + 11 \cdot (-5)$$

$$\begin{aligned} \Rightarrow x &\equiv 7 \cdot 8 \cdot 9 + 11 \cdot (-5) \cdot 4 \pmod{7 \cdot 11} \\ &= 7 \cdot 72 - 11 \cdot 20 \\ &= \cancel{7 \cdot 66} + 7 \cdot 6 - \cancel{11 \cdot 14} - 11 \cdot 6 \quad (\text{mod } 7 \cdot 11) \\ &\equiv 7 \cdot 6 - 11 \cdot 6 \\ &= 42 - 66 \\ &= -24 \\ x &\equiv 53 \pmod{7 \cdot 11} \end{aligned}$$

$$\begin{cases} X \equiv 53 \pmod{7 \cdot 11} \\ X \equiv 1 \pmod{23} \end{cases}$$

Daremos algoritmo de la división ~~por el menor~~ (23, 77)

$$77 = 23 \cdot 3 + 8$$

$$23 = 8 \cdot 2 + 7$$

$$8 = 7 \cdot 1 + 1$$

$$\begin{aligned} \Rightarrow 1 &= 8 - 7 \cdot 1 \\ &= 8 - (23 - 8 \cdot 2) = 8 - 23 + 8 \cdot 2 = 8 \cdot 3 - 23 \\ &= (77 - 23 \cdot 3) \cdot 3 - 23 \\ &= 77 \cdot 3 - 23 \cdot 9 - 23 = 77 \cdot 3 - 23 \cdot 10 \end{aligned}$$

$$\therefore 1 = 77 \cdot 3 + 23 \cdot (-10)$$

Por teorema chino de los restos:

$$X \equiv 77 \cdot 3 \cdot 1 + 23 \cdot (-10) \cdot 53 \pmod{7 \cdot 11 \cdot 23}$$

$$\equiv 77 \cdot 3 - 23 \cdot 53 \cdot 10 \pmod{7 \cdot 11 \cdot 23}$$

$$\equiv 231 - 12190 \pmod{7 \cdot 11 \cdot 23}$$

$$\equiv -11959 \pmod{7 \cdot 11 \cdot 23}$$

$$\equiv -10626 - 1333 \pmod{7 \cdot 11 \cdot 23}$$

$$\equiv -17716 - 1333 \pmod{7 \cdot 11 \cdot 23}$$

$$\equiv -1333$$

$$X \equiv 438 \pmod{7 \cdot 11 \cdot 23}$$

$$\overline{7 \cdot 11 \cdot 23 = 1771}$$

✓

5

$$\text{Com} \begin{cases} x \equiv 4 \pmod{7} \\ x \equiv 9 \pmod{11} \end{cases} \Rightarrow x \equiv 53 \pmod{77}$$

$$\text{Ahora sólo falta resolver} \quad \begin{cases} x \equiv 53 \pmod{11 \cdot 7} \\ x \equiv 22 \pmod{23} \end{cases}$$

Por el cálculo anterior, inmediatamente tenemos que:

$$x \equiv 77 \cdot 3 \cdot 22 + 23 \cdot (-10) \cdot 53 \pmod{7 \cdot 11 \cdot 23}$$

$$x \equiv 5082 - 12190 \pmod{7 \cdot 11 \cdot 23}$$

$$x \equiv -7108 \pmod{7 \cdot 11 \cdot 23}$$

$$x \equiv -7084 - 24$$

$$\equiv -1771 \cdot 4 - 24$$

$$\equiv -24 \pmod{7 \cdot 11 \cdot 23}$$

$$\equiv 1747 \pmod{7 \cdot 11 \cdot 23}$$

Por lo tanto, las soluciones del sistema son

$$\begin{cases} x \equiv 438 \pmod{7 \cdot 11 \cdot 23} \\ x \equiv 1747 \pmod{7 \cdot 11 \cdot 23} \end{cases}$$

### Problema 3

$$\eta = e^{\frac{2\pi i}{5}} \text{ raiz de } \frac{x^5 - 1}{x - 1}$$

Pd:  $\eta^2 + 1$  es una unidad en  $\mathbb{Z}[\eta]$

Dem. Es evidente que  $\eta^2 + 1$  unidad en  $\mathbb{Z}[\eta]$  si

$$(\eta^2 + 1) = \mathbb{Z}[\eta]$$

Luego bastaría demostrar que  $\mathbb{Z}[\eta]/(\eta^2 + 1)$  es el anillo trivial

$\{0\}$ . En efecto

$$\begin{aligned} \mathbb{Z}[\eta]/(\eta^2 + 1) &\cong \frac{\mathbb{Z}[x]}{\left(\frac{x^5 - 1}{x - 1}, x^2 + 1\right)} \\ &\cong \frac{\mathbb{Z}[i]}{\left(\frac{i^5 - 1}{i - 1}, 0\right)} \quad \left( \begin{array}{l} \text{evaluando en } x=i, \text{ ya que es} \\ \text{raiz de } x^2 + 1 \end{array} \right) \\ &\cong \frac{\mathbb{Z}[i]}{\left(\frac{i^5 - 1}{i - 1}, 0\right)} \quad x^2 + 1 \text{ irreducible en } \mathbb{Z}[x] \end{aligned}$$

$$\text{Como } i^5 = i \Rightarrow \frac{\mathbb{Z}[i]}{\left(\frac{i^5 - 1}{i - 1}, 0\right)} \cong \frac{\mathbb{Z}[i]}{\left(\frac{i - 1}{i - 1}, 0\right)} \cong \frac{\mathbb{Z}[i]}{(1, 0)} \cong \frac{\mathbb{Z}[i]}{(1)} \cong \frac{\mathbb{Z}[i]}{\mathbb{Z}[i]}$$

$$\therefore \mathbb{Z}[\eta]/(\eta^2 + 1) \cong \{0\}$$

$\therefore \eta^2 + 1$  unidad (invertible) en  $\mathbb{Z}[\eta]$

Pd:  $\eta+3$  es primo en  $\mathbb{Z}[\eta]$

Dem. Se sabe que

$$\begin{aligned}\eta+3 \text{ es primo en } \mathbb{Z}[\eta] &\Leftrightarrow (\eta+3) \text{ es primo (ideal)} \\ &\quad \text{en } \mathbb{Z}[\eta] \\ &\Leftrightarrow \mathbb{Z}[\eta]/(\eta+3) \text{ dominio de integridad}\end{aligned}$$

$$\begin{aligned}\mathbb{Z}[\eta]/(\eta+3) &\cong \frac{\mathbb{Z}[x]}{\left(\frac{x^5-1}{x-1}, x+3\right)} \\ &\cong \frac{\mathbb{Z}[-3]}{\left(\frac{(-3)^5-1}{-3-1}, 0\right)} \quad (\text{evaluando en } x=-3) \\ &\cong \frac{\mathbb{Z}}{\left(\frac{-3^5-1}{-3-1}\right)} \\ &\cong \frac{\mathbb{Z}}{\left(\frac{3^5+1}{3+1}\right)}\end{aligned}$$

$$\text{Como } 3^5+1 = (3+1)(3^4-3^3+3^2-3+1)$$

$$\begin{aligned}\Rightarrow 3^4-3^3+3^2-3+1 &= 81-27+9-3+1 \\ &= 54+6+1 \\ &= 61 \quad (\text{primo en } \mathbb{Z})\end{aligned}$$

$$\therefore \frac{\mathbb{Z}}{\left(\frac{3^5+1}{3+1}\right)} \cong \frac{\mathbb{Z}}{(61)} \cong \mathbb{F}_{61} \quad (\text{cuerpo, en particular dominio de integridad})$$

$\therefore$  Se concluye que  $\eta+3$  es primo en  $\mathbb{Z}[\eta]$

### Problema 5

Encuentre el inverso de la clase  $\overline{1+i}$  en  $\frac{\mathbb{Z}[i]}{(2+i)}$

### Desarrollo

Primero veamos que

$$\frac{\mathbb{Z}[i]}{(2+i)} \cong \frac{\mathbb{Z}[x]}{(x^2+1, 2+x)} \cong \frac{\mathbb{Z}[-2]}{(-2)^2+1, 0} = \frac{\mathbb{Z}}{(4+1)} = \frac{\mathbb{Z}}{(5)} \cong \frac{\mathbb{Z}_5}{5\mathbb{Z}_5} \cong \mathbb{F}_5$$

Como  $\mathbb{F}_5$  ( $\cong \mathbb{Z}/5\mathbb{Z}$ ) es el cuerpo con 5 elementos, entonces

$$\forall x \in \mathbb{F}_5^*: \quad \bar{x}^4 = \bar{1} \quad \text{En efecto}$$

$$\begin{aligned} \mathbb{F}_5^* &= \{1, 2, 3, 4\} \quad : \quad 1^4 \equiv 1 \pmod{5} \\ 2^4 &\equiv 16 \equiv 1 \pmod{5} \\ 3^4 &\equiv 81 \equiv 1 \pmod{5} \\ 4^4 &\equiv 256 \equiv 1 \pmod{5} \end{aligned}$$

Entonces  $\overline{1+i}$  debe tener orden 4 en  $\left(\frac{\mathbb{Z}[i]}{(2+i)}\right)^*$ . Es decir,  $\overline{1+i}^{-1} = (\overline{1+i})^3$ .

Comprobemos de que es así:

$$\begin{aligned} (1+i)^3 &= 1 + 3i + 3i^2 + i^3 \\ &= 1 + 3i - 3 - i \\ &= -2 + 2i \end{aligned}$$

$$\begin{aligned} (i+1)^4 &= (-2+2i)(i+1) \quad \checkmark \\ &= -2i - 2 + 2i^2 + 2i \\ &= -2 - 2 = -4 \\ &= 1 - 5 \quad , \text{ pero } 5 = (2-i)(2+i) \end{aligned}$$

$$\begin{aligned} \therefore (i+1)^4 &= 1 - (2-i)(2+i) \\ &\equiv 1 \pmod{(2+i)} \end{aligned}$$

Teoría de Números  
 Desarrollo prueba 2  
 Marco Godoy V.

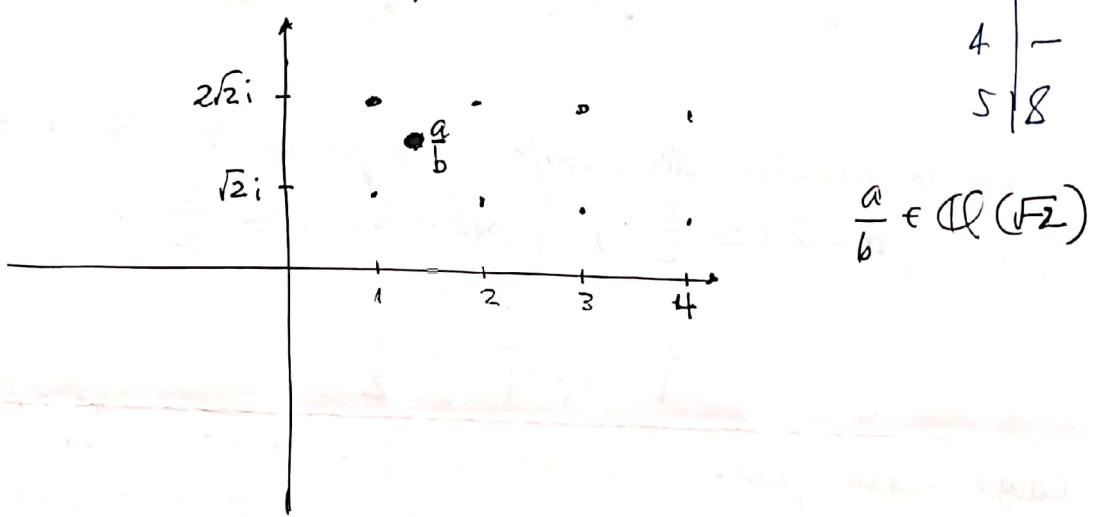
4,1

Problema 2

Por demostrar que  $\mathbb{Z}[\sqrt{-2}]$  es un DFU.

Dem. Recordando que  $\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} / a, b \in \mathbb{Z}\}$

Ubicamos estos puntos en el plano complejo  $\mathbb{C}$



donde la norma cuadrática  $N$  viene dada por  $N(a+b\sqrt{-2}) = a^2+2b^2$

Ahora supongamos que tenemos  $a, b \in \mathbb{Z}[\sqrt{-2}]$ , con  $b \neq 0$ , la idea es demostrar que existen  $q, r \in \mathbb{Z}[\sqrt{-2}]$  tales que

$a = bq + r$ , donde  $\tilde{N}(r) \leq \tilde{N}(b)$  o  $r=0$ ; donde  $\tilde{N}$  corresponde al "algoritmo de euclides" respectivo

$$\tilde{N}(a+b\sqrt{-2}) = |a^2+2b^2| = a^2+2b^2$$

Primero descartamos el caso  $b=0$

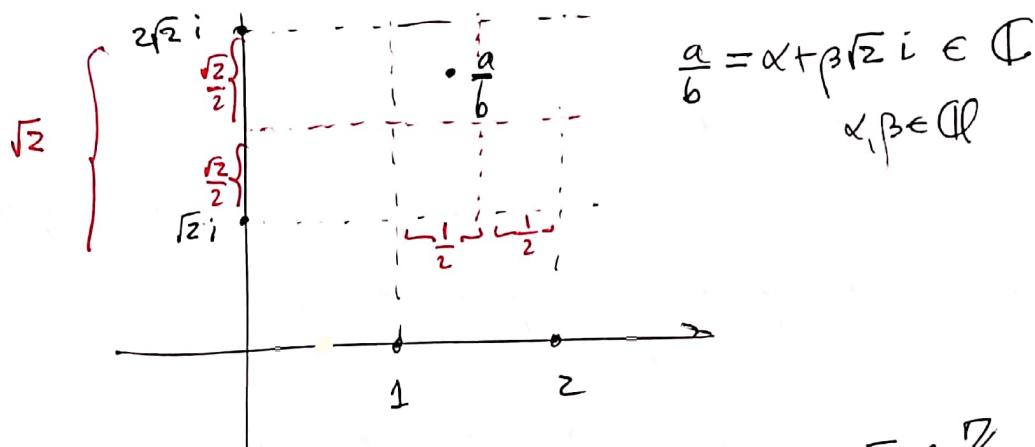
Para demostrar la existencia de  $q, r \in \mathbb{Z}[\sqrt{-2}]$ , primero veamos que  $\frac{a}{b} \in \mathbb{Q}(\sqrt{-2})$  (ver figura). Podemos luego suponer que

$$\frac{a}{b} = \alpha + \beta\sqrt{-2} ; \quad \alpha, \beta \in \mathbb{Q}$$

El caso trivial es que  $\alpha, \beta \in \mathbb{Z}$ , con lo cual se tiene que  $\alpha = \alpha + \beta\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$  y  $a = b\alpha$ . Luego basta tomar

$f = \sigma$  y  $r = 0$  y se cumple lo pedido.

El caso importante es cuando  $\alpha, \beta \in \mathbb{Q}$  no enteros simultáneamente.  
Pero en ese caso ubicamos  $\frac{a}{b}$  en el plano complejo



Dada la geometría del dibujo, siempre existen  $\bar{\alpha}, \bar{\beta} \in \mathbb{Z}$  tales que  $|\alpha - \bar{\alpha}| \leq \frac{1}{2}$ ,  $|\beta\sqrt{2} - \bar{\beta}\sqrt{2}| \leq \frac{\sqrt{2}}{2}$ ,

$$\therefore \begin{cases} |\alpha - \bar{\alpha}| \leq \frac{1}{2} \\ |\beta - \bar{\beta}| \leq \frac{1}{2} \end{cases}$$

Luego nuestro primer candidato es  $q = \bar{\alpha} + \bar{\beta}\sqrt{2} \in \mathbb{Z}[\sqrt{-2}]$ .

Por otro lado,  $\frac{a}{b} - q = (\alpha - \bar{\alpha}) + (\beta - \bar{\beta})\sqrt{-2} \in \mathbb{Q}(\sqrt{-2})$

pero  $\frac{a}{b} - q = \frac{a - bq}{b} = \frac{r}{b}$ , donde  $r = a - bq \in \mathbb{Z}[\sqrt{-2}]$ ,

ya que  $a, b, q \in \mathbb{Z}[\sqrt{-2}]$ . Ahora es fácil ver que

$$r = b\left(\frac{a}{b} - q\right)$$

y el resto sale por la multiplicidad de  $\tilde{N}$  (ya que  $N$  también es multiplicativa. O sea

$$\begin{aligned} \tilde{N}(r) &= \tilde{N}\left(b\left(\frac{a}{b} - q\right)\right) = \tilde{N}(b)\tilde{N}\left(\frac{a}{b} - q\right) \\ &= \tilde{N}(b)\tilde{N}\left((\alpha - \bar{\alpha}) + (\beta - \bar{\beta})\sqrt{-2}\right) \\ &= \tilde{N}(b) \left[ (\alpha - \bar{\alpha})^2 + 2(\beta - \bar{\beta})^2 \right] \\ &\leq \tilde{N}(b) \left[ \frac{1}{4} + 2 \cdot \frac{1}{4} \right] = \tilde{N}(b) \left[ \frac{1}{4} + \frac{1}{2} \right] \\ &\leq \frac{3}{4} \tilde{N}(b) \leq \tilde{N}(b) \end{aligned}$$

Por lo tanto, como  $r = a - bq$

$$a = bq + r$$

donde  $r, q \in \mathbb{Z}[\sqrt{-d}]$  y  $\tilde{N}(r) \leq \tilde{N}(b)$

□

### Problema 3

$\alpha$  raíz de  $x^3+x+2$ . Debemos encontrar  $m$  tal que

$$\mathbb{Z}[\alpha]/(\alpha^3+x+2) \cong \mathbb{Z}/m\mathbb{Z}.$$

Desarrollo: Evidente que  $x^3+x+2$  irreducible en  $\mathbb{Z}[x]$  (~~No tiene~~ (Discriminante negativo, no tiene raíces en  $\mathbb{R}$ ). Luego trabajamos mediante cocientes:

$$\begin{aligned} \frac{\mathbb{Z}[\alpha]}{(\alpha^3+x+2)} &\cong \frac{\mathbb{Z}[x]}{(x^3+x+2, x^2+5)} \cong \frac{\mathbb{Z}[\sqrt{-5}]}{((\sqrt{-5})^3 + \sqrt{-5} + 2, 0)} \\ &\quad \text{evaluación en } x = \sqrt{-5}, \text{ ya que } x^2+5 \text{ irreducible en } \mathbb{Z}[x] \\ &\cong \frac{\mathbb{Z}[\sqrt{-5}]}{(-5\sqrt{-5} + \sqrt{-5} + 2)} \cong \frac{\mathbb{Z}[\sqrt{-5}]}{(-4\sqrt{-5} + 2)} = \frac{\mathbb{Z}[\sqrt{-5}]}{(4\sqrt{-5} - 2)} \\ &\cong \frac{\mathbb{Z}[x]}{(x^2+5, 4x-2)} \cong \frac{\mathbb{Z}[\frac{1}{2}]}{(\frac{1}{4} + 5, 0)} \cong \frac{\mathbb{Z}[\frac{1}{2}]}{(\frac{21}{4})} \quad \text{8/15} \\ &\quad \text{evaluando en } x = \frac{1}{2}, \text{ ya que } 4x-2 \text{ irreducible en } \mathbb{Z}[x] \quad \text{no es irreducible es una función no es un isomorfismo.} \end{aligned}$$

Ahora, por localización,  $\frac{\mathbb{Z}[\frac{1}{2}]}{(\frac{21}{4})} \cong \left(\mathbb{Z}_{(21)}\right) \left[\frac{1}{2}\right]$

Como 2 es coprimo con 21, el inverso de 2 en  $\mathbb{Z}_{(21)}$  ya existe, luego el anillo  $\left(\mathbb{Z}_{(21)}\right) \left[\frac{1}{2}\right]$  no se altera por agregar este elemento

$$\therefore \frac{\mathbb{Z}[\frac{1}{2}]}{(\frac{21}{4})} \cong \frac{\mathbb{Z}}{21\mathbb{Z}}$$

Por lo tanto,  $m = 21$

#### Problema 4

Por demostrar que la ecuación  $2x^2 - 3y^2 = 1$  tiene infinitas soluciones enteras.

#### Problema 5

Pd:  $\alpha$  un entero algebraico. Probar que todo ideal primo de  $\mathbb{Z}[\alpha]$  distinto de  $(0)$  es maximal.

Dem. Primero probaremos que todo ideal no nulo  $I$  de  $\mathbb{Z}[\alpha]$  contiene un  $n \in \mathbb{Z}$  distinto de  $0$ .

Dem. Dm. Si tuviéramos el caso en que ningún entero  $a \in \mathbb{Z}$  está en  $I$  ( $a \neq 0$ ) entonces tenemos que  $0 \notin I$  o  $0 \in I$  simultáneamente. El primer caso nos daría que  $I = (0)$  y el cual descartamos. En el segundo caso la única opción es que  $\alpha \in I$ , pero como  $I$  es ideal de  $\mathbb{Z}[\alpha]$

$$\alpha^n \in I \quad \forall n \geq 0$$

$$a\alpha \in I, \text{ con } a \in \mathbb{Z}$$

luego la combinación lineal  $a_n\alpha^n + \dots + a_1\alpha + a_0 \in I$ , pero  $a_n\alpha^n + \dots + a_1\alpha = -a_0 \in I$  y ( $a_0 \neq 0$ )  
 (Si  $a_0 = 0 \Rightarrow \alpha = 0$  y  $\mathbb{Z}[\alpha] = \mathbb{Z}$ )

$\therefore I$  ideal no nulo de  $\mathbb{Z}[\alpha]$  admite un elemento ~~entero~~ no nulo de  $\mathbb{Z}$ .



8/15

Por demostrar que si  $I$  es primo, entonces  $I$  es maximal en  $\mathbb{Z}[\alpha]$  ( $I \neq (0)$ )

Lo anterior es equivalente a demostrar que  $\mathbb{Z}[\alpha]/I$  es cuerpo, es decir,  $\forall \bar{p} \in \mathbb{Z}[\alpha]/I$ , existe  $\bar{q} \in \mathbb{Z}[\alpha]/I$  tal que  $\bar{p}\bar{q} = \bar{1} \pmod{I} \Leftrightarrow pq - 1 \in I$

Si no fuera cuerpo, existiría  $p \in \mathbb{Z}[\alpha]$  tal que para todos  $q \in \mathbb{Z}[\alpha] : pq - 1 \notin I$ . Ahora sea  $m \in \mathbb{Z}$  tal que  $m \in \mathbb{Z}[\alpha]$ . Como  $I$  es ideal

$$m(pq - 1) \in I$$

pero  $m(pq - 1) = mpq - m$  ??

$m(pq + 1)$



$$\text{Una aplicación: } \left( \frac{1}{p} \right) = (-1)^{\frac{p-1}{2}} \quad \begin{cases} 1, & p \equiv 1(4) \\ -1, & p \equiv 3(4) \end{cases}$$

Otro desarrollo similar:  $\frac{1}{p} \equiv 1 \pmod{4}$  si y sólo si  $1 \pmod{4(pn)}^2 \equiv 1 \pmod{4(p-1)}$ .

$$\text{Definición: } \left( \frac{2}{p} \right) = (-1)^{\frac{p-1}{8}}.$$

Calcular en  $\mathbb{Z}[i] \cong \mathbb{Z} \oplus i\mathbb{Z}$ .

$$\frac{\mathbb{Z}(i)}{p} \cong \frac{\mathbb{Z}/p\mathbb{Z}}{\text{parte real}} \oplus \frac{i(\mathbb{Z}/p\mathbb{Z})}{\text{parte imaginaria}}$$

$$\text{por: } \frac{\mathbb{Z} \oplus i\mathbb{Z}}{(p)} \cong \frac{\mathbb{Z} \oplus \mathbb{Z}i}{p\mathbb{Z} \oplus ip\mathbb{Z}} \cong \frac{\mathbb{Z}/p\mathbb{Z}}{\text{parte real}} \oplus \frac{i(\mathbb{Z}/p\mathbb{Z})}{\text{parte imaginaria}}$$

$$\text{obs: 1) } 2 = (-i)(ii)^2 \quad 2^{\frac{p-1}{2}} \equiv (-i)^{\frac{p-1}{2}} (ii)^{p-1}, \quad 2^{\frac{p-1}{2}} (ii) \equiv (-i)^{\frac{p-1}{2}} (ii)^p \equiv (-i)^{\frac{p-1}{2}} (ii^p).$$

Hagamos calcular:

$$(\text{caso I: } p \equiv 1(8)) \quad 2^{\frac{p-1}{2}} (ii) \equiv ii \pmod{p}$$

$$\text{así: } 2^{\frac{p-1}{2}} \equiv 1 \pmod{p} \quad (\text{teniendo parte real})$$

$$(\text{caso II: } p \equiv 5(8)): \text{evidentemente } (-i)^{\frac{p-1}{2}} = -1, \quad i^p = i$$

$$\text{Así: } 2^{\frac{p-1}{2}} (ii) \equiv - (ii)$$

$$2^{\frac{p-1}{2}} \equiv -1$$

$$(\text{caso III: } p \equiv 3(8)): \text{evidentemente } (-i)^{\frac{p-1}{2}} = i, \quad i^p = -i$$

$$\text{Así: } 2^{\frac{p-1}{2}} (ii) \equiv -i(i) = -i^2$$

$$2^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

Caso IV:  $p \in \mathbb{P}(8)$ ,  $(-1)^{\frac{p-1}{8}} = i$

$$\text{Entonces: } 2^{\frac{p-1}{2}}(1+i) = i(1-i) = 1+i$$

$$\text{Luego: } 2^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

$$\text{y como: } \left(\frac{2}{p}\right) := (-1)^{\frac{p-1}{8}} = \begin{cases} 1, & \text{s. } p \in \mathbb{P}(8) \\ -1, & \text{s. } p \in \mathbb{S}(8) \end{cases}$$

Línea terminar.

entendiendo en los cuadrados  $\left(\frac{p}{q}\right)$  para  $p$  primo impar,

Proposición: Si  $q_1, q_2$  son primos: Regla de Reciprocidad Cuadrática.

$$\left(\frac{q_1 q_2}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q_1-1}{2}} \left(\frac{q_1}{p}\right)$$

$$\text{Un poco más: } \left(\frac{q_1 q_2}{q_1 q_2}\right) = (-1)^{\frac{q_1-1}{2} \cdot \frac{q_2-1}{2}} \left(\frac{q_2}{q_1 q_2}\right) = \left(\frac{q_2}{q_1}\right) = \left(\frac{q_1}{q_2}\right)$$
$$= \left(\frac{2}{q_1}\right) \left(\frac{2}{q_2}\right) = (-1) \left(\frac{2}{q_2}\right) = (-1)^{\frac{q_2-1}{2} \cdot \frac{3}{2}} \left(\frac{2}{q_2}\right)$$
$$= -(-1) \left(\frac{1}{q_2}\right) = \left(\frac{1}{q_2}\right) = (-1)^{\frac{q_2-1}{2}} = -1$$

•  $q_3$  no es cuadrado modulo  $q_1$  o bien:

$$x^2 \equiv q_3 \pmod{q_1}$$

DJS: Supongamos que planteamos resolver:

$$x^2 \equiv 17 \pmod{31 \cdot 11}$$

$$\text{Como: } \mathbb{Z}_{341\mathbb{Z}} \cong \mathbb{Z}_{31\mathbb{Z}} \oplus \mathbb{Z}_{11\mathbb{Z}}$$

y además  $\mathbb{Z}_{341\mathbb{Z}} \rightarrow \mathbb{Z}_{11\mathbb{Z}}$  es un isom. coductivo.

$$\bar{a} = a + 341\mathbb{Z} \mapsto a + 11\mathbb{Z}$$

Es suficiente resolver:  $\begin{cases} x^2 \equiv 17 \pmod{31} \\ x^2 \equiv 17 \pmod{11} \end{cases}$

Demonstración: (ley X.1.iii)

$\Gamma \subseteq \mathbb{Z}$  finito  $A = \prod_{a \in \Gamma} a$ .

$$\Phi = \left\{ n \in \mathbb{N} \mid \text{lcm} \left( \frac{n-1}{2}, \text{lcm}(a, p) \right) = 1 \right\}.$$

$$\Psi = \left\{ n \in \mathbb{N} \mid \text{lcm}(p, n) = 1 \right\}.$$

$$X = \left\{ q \ell \mid 1 \leq \ell \leq \frac{p-1}{2} \right\}.$$

ds:  $\Psi = \Phi \cup X$  pues:  $\Phi = \{ n \in \Psi \mid \ell + n \}$ ,  $X = \{ n \in \Psi \mid \ell \in X \}$

$$\Rightarrow \Phi \cap X = \emptyset$$

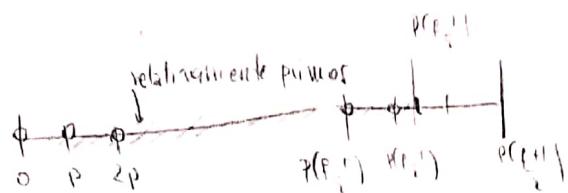
$$A \nmid A_X = \prod_{a \in \Gamma} a \cdot \prod_{a \in X} a = \prod_{a \in \Gamma \cup X} a = \prod_{a \in \Psi} a = A \cdot p$$

para cada  $t$ :  $\Psi_t = \{ n \in \mathbb{N} \mid 1 \leq n \leq \frac{p-1}{2} \}$ .

$$\Psi_t^1 = \{ n \in \mathbb{N} \mid 1 \leq n \leq \frac{p-1}{2} \}.$$

$$\Psi = \bigcup_{t=0}^{\frac{p-1}{2}} \Psi_t \cup \Psi_{\frac{p-1}{2}}^1.$$

$$A \Psi = \left( \prod_{a=0}^{\frac{p-1}{2}} A \Psi_a \right) A \Psi_{\frac{p-1}{2}}^1$$



Lema:  $(-1)^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ .

ksi  $A \Psi_t \equiv -1 \pmod{p}$ , pues  $A \Psi_t = (p|1)(p|1) \dots (p|1) \equiv (-1)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

$$\lambda \Psi \equiv (-1)^{\frac{p-1}{2}} A \Psi_{\frac{p-1}{2}}^1 \equiv (-1)^{\frac{p-1}{2}} \left( \frac{p-1}{2} \right) !.$$

$$A_X \equiv \left( \frac{p-1}{2} \right) ! \equiv \left( \frac{q}{p} \right) \left( \frac{p-1}{2} \right) !.$$

$$A \Psi = A_X A_\Psi, \text{ así } (-1)^{\frac{p-1}{2}} \left( \frac{p-1}{2} \right) ! \equiv \left( \frac{q}{p} \right) \left( \frac{p-1}{2} \right) ! A_\Psi \pmod{p}$$

$$A \not\equiv (-1)^{\frac{p-1}{2}} \left( \frac{q}{p} \right) (\text{mod } p)$$

Parámetros:

$$A \not\equiv (-1)^{\frac{p-1}{2}} \left( \frac{p}{q} \right) (\text{mod } q)$$

Case I:  $A \not\equiv 1 \pmod{p}$ ,  $A \not\equiv 1 \pmod{q}$

$$\Rightarrow A \not\equiv 1 \pmod{pq}$$

Case II:  $A \not\equiv -1 \pmod{p}$ ,  $A \not\equiv -1 \pmod{q}$

$$\Rightarrow A \not\equiv -1 \pmod{pq}$$

Cases III y IV:  $A \not\equiv 1 \pmod{p}$  o  $A \not\equiv -1 \pmod{p}$   
 $A \not\equiv 1 \pmod{q}$  o  $A \not\equiv -1 \pmod{q}$

el sistema da una solución de  $K^2 \equiv 1 \pmod{pq}$  gracias a la L.

Ejemplo:  $A \not\equiv \pm 1 \pmod{pq}$  si  
 $(-1)^{\frac{p-1}{2}} (-1)^{\frac{q-1}{2}} = \left( \frac{p}{q} \right) \left( \frac{q}{p} \right)$

pd:  $A \not\equiv \pm 1$  si  $(p \equiv f \equiv 1 \pmod{4})$ .

$$(-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{q-1}{2}} = \left\{ \begin{array}{l} 1, \text{ si } p \equiv f \equiv 1 \pmod{4} \\ -1, \text{ si no.} \end{array} \right.$$

Debrafmeridion  $(-1)^{\frac{p-1}{2}} (-1)^{\frac{q-1}{2}} = \left( \frac{p}{q} \right) \left( \frac{q}{p} \right)$  es  $(-1)^{\frac{p-1}{2}} (-1)^{\frac{q-1}{2}} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$

Dcm. debrafmeridion: Sean  $\Phi$ , entonces existen únicas

Def: Si  $\in \Phi$  definimos  $w \in \Phi$  tal que:  $w^2 \equiv 1 \pmod{pq}$

Existe un único elemento en  $\{w, -w\}$  que cumple que

$$w = (w^{-1})^2 = \{w^2, -w^2\}.$$

Sea  $\Delta = \{x \in \Phi \mid W = \langle x \rangle\}$

$A\phi \in \mathbb{Z}A\Delta \pmod{p\mathbb{Z}}$ , mas  $A\phi = \underbrace{u_1 u_2 \dots}_{\pm 1} \in A\Delta$

Caso:  $p \equiv \pm 1 \pmod{4}$

No existen  $W \equiv \pm 1 \pmod{p\mathbb{Z}}$  con  $\begin{cases} K \equiv 1 \pmod{p} \\ K \equiv -1 \pmod{4} \end{cases}$

$$\text{Pues } \mathcal{U}/p\mathbb{Z} \cong \mathcal{U}/p\mathbb{Z} \times \mathcal{U}/p\mathbb{Z}_{(-1,1)}^{\pm 1} \times K_{(1,-1)}$$

Si  $W \equiv 1 \pmod{p\mathbb{Z}} \Leftrightarrow \begin{cases} W \equiv 1 \pmod{p} \\ W \equiv -1 \pmod{4} \end{cases}$

Caso  $p \equiv \pm 1 \pmod{4}$ :  $\mathcal{U}/p\mathbb{Z}$  tiene soluciones:

$$\Delta = \{1, \pm k, \pm l, \pm kl\}$$

$$\text{Así: } Ax = \pm kl \equiv \pm 1 \pmod{p\mathbb{Z}}$$

Si  $p \not\equiv 1 \pmod{4}$  o  $p \not\equiv -1 \pmod{4}$ :

cuando  $(1, k, l)$  tienen soluciones  $\Rightarrow \Delta = \{1, \pm k, \pm l\}$

$$Ax \equiv \pm k \pmod{p\mathbb{Z}}$$

$$\not\equiv \pm 1 \pmod{p\mathbb{Z}}$$

Ejemplo: 143 es un cuadrado módulo 181.

$$\left(\frac{143}{181}\right) = \left(\frac{3}{181}\right) \left(\frac{92}{181}\right)^{-1} = \left(\frac{3}{181}\right) \cdot \left(\frac{181}{3}\right) \cdot \left(\frac{1}{3}\right) = 1$$

$$A \not\equiv (-1)^{\frac{p-1}{2}} \left(\frac{q}{p}\right) (\text{mod } p)$$

por simetría:

$$A \not\equiv (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) (\text{mod } q)$$

Caso I:  $A \not\equiv 1 (\text{mod } p)$ ;  $B \not\equiv 1 (\text{mod } q)$

$$\Rightarrow A \not\equiv 1 (\text{mod } pq)$$

Caso II:  $A \not\equiv 1 (\text{mod } p)$ ,  $B \not\equiv -1 (\text{mod } q)$

$$\Rightarrow B \not\equiv -1 (\text{mod } pq)$$

Casos III y IV:  $A \not\equiv 1 (\text{mod } p)$  o  $A \not\equiv -1 (\text{mod } p)$   
 $B \not\equiv 1 (\text{mod } q)$  o  $B \not\equiv -1 (\text{mod } q)$

el sistema de ecuaciones de  $K^* \equiv \{(pq)\}$  tiene sol. ( $m=1$ ).

luego:  $A \not\equiv \pm 1 (\text{mod } pq)$   
 $(-1)^{\frac{p-1}{2}} (-1)^{\frac{q-1}{2}} = \left(\frac{p}{q}\right) \left(\frac{q}{p}\right)$

pd:  $A \not\equiv \pm 1$  si  $p \neq q \in \{1, 4\}$ .

$$(-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{q-1}{2}} = \begin{cases} 1, & \text{si } p \neq q \in \{1, 4\} \\ -1, & \text{si no.} \end{cases}$$

definición  $(-1)^{\frac{p-1}{2}} (-1)^{\frac{q-1}{2}} = \left(\frac{p}{q}\right) \left(\frac{q}{p}\right)$  si  $(-1)^{\frac{p-1}{2}} (-1)^{\frac{q-1}{2}} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$

Dm. de brañmercia: Sean  $\Phi$ , entonces existe un único

Def: Si  $w \in \Phi$  definimos  $w \in \Phi$  tal que:  $w^{-1} \in \Phi$

Existe un único elemento en  $\{c_1, c_2\}$  que está en  $\Phi$

$$w = (w^{-1})^* = \{w^{-1}, -w^{-1}\}.$$

Quellenwert für:  $\left(-\frac{1}{n}\right) = (-1)^{\frac{n^2-1}{2}}$

$$\left(-\frac{1}{n}\right) = \prod_{i=1}^v \left(-\frac{1}{p_i}\right)^{d_i} = \prod_{i=1}^v (-1)^{\frac{p_i-1}{2} \cdot d_i}$$
$$= (-1)^{\sum_{i=1}^v d_i \left(\frac{p_i-1}{2}\right)}$$

Prop. Si  $a$  y  $b$  non impares :  $\frac{ab-1}{2} \equiv \frac{a-1}{2} + \frac{b-1}{2} \pmod{2}$

$$\text{Dem: } a = 2t+1, b = 2s+1$$

$$\frac{(2t+1)(2s+1)-1}{2} = \frac{4ts+2(t+s)}{2} = 2ts + t+s \equiv t+s \pmod{2}$$

$$\text{Aplicando esto repetidamente: } \prod_{i=1}^k \frac{p_i^{d_i}-1}{2} \equiv \sum_{i=1}^k d_i \left( \frac{p_i-1}{2} \right)$$

$$\left( \frac{a^2-1}{2} \equiv \frac{a^2-1}{2}, \frac{a-1}{2} \equiv 3 \left( \frac{a-1}{2} \right) \right)$$

$$\therefore \left( \frac{1}{n} \right) = (-1)^{\frac{n-1}{2}}$$

$$\text{y } \left( \frac{1}{n} \right) = \prod_{i=1}^k \left( \frac{2}{p_i} \right)^{d_i} = \prod_{i=1}^k (-1)^{\frac{p_i-1}{2} d_i} = (-1)^{\sum_{i=1}^k d_i \left( \frac{p_i-1}{2} \right)}$$

Proposición: Si  $a$  y  $b$  compuestos.

$$\frac{a^2b^2-1}{8} \equiv \frac{a^2-1}{8}, \frac{b^2-1}{8} \pmod{2}$$

$$\begin{aligned} a^2 = 8t+1 &\Rightarrow \frac{a^2b^2-1}{8} = \frac{64ts+8t+s}{8} \quad 8t+s+8 \equiv 1+8 \pmod{2} \\ b^2 = 8s+1 & \end{aligned}$$

$$\therefore \left( \frac{1}{n} \right) = (-1)^{\frac{\sum p_i d_i - 1}{8}} = (-1)^{\frac{n-1}{8}}$$

Si  $p$  es primo:

$$\left( \frac{p}{n} \right) = \prod_{i=1}^r \left( \frac{p}{p_i} \right)^{d_i}$$

$$\left( \frac{p}{q} \right) = \prod_{i=1}^r \left( \frac{p_i}{q} \right)^{d_i}$$

$$\begin{aligned} \text{as: } \left( \frac{p}{n} \right) \left( \frac{q}{n} \right) &= \prod_{i=1}^r \left( \frac{p}{p_i} \right)^{d_i} \left( \frac{q}{p_i} \right)^{d_i} \\ &= \prod_{i=1}^r \left[ (-1)^{\frac{p-1}{2}} \cdot \frac{q-1}{2} \right]^{d_i} \\ &= (-1)^{\frac{p-1}{2} \sum_{i=1}^r d_i \cdot \frac{q-1}{2}} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \end{aligned}$$

$$\left( \frac{m}{n} \right) = \prod_{i=1}^s \left( \frac{b_i}{n} \right)^{\beta_i}$$

$$\begin{aligned} \left( \frac{m}{n} \right) \left( \frac{w}{n} \right) &= \prod_{i=1}^s \left( \frac{b_i}{n} \right)^{\beta_i} \prod_{i=1}^s \left( \frac{c_i}{n} \right)^{\gamma_i} \\ &= \prod_{i=1}^s \left[ \left( \frac{b_i}{n} \right) \left( \frac{c_i}{n} \right) \right]^{\beta_i} \\ &= \prod_{i=1}^s \left[ (-1)^{\frac{b_i-1}{2}} \frac{b_i-1}{2} \right]^{\beta_i} \cdot (-1)^{\frac{w-1}{2} \sum_{i=1}^s \beta_i \cdot \frac{c_i-1}{2}} = (-1)^{\frac{w-1}{2} \cdot \frac{m-1}{2}} \end{aligned}$$

obs:  $\left( \frac{m}{n} \right) = 1$  significa que  $x \in n\mathbb{Z}$  tiene solución.

(ii) Suposición:  $x \in n\mathbb{Z}$  tiene solución ssi  $\left( \frac{m}{n} \right) = 1 \forall p \mid n$ .

$$\begin{aligned} \text{ejemplo: } \left( \frac{111}{147} \right) &= \left( \frac{111}{147} \right) = \left( \frac{34}{147} \right) = \left( \frac{2}{147} \right) \left( \frac{11}{147} \right) = (-1)^{\frac{11-1}{2}} \left( \frac{1}{147} \right) \\ &= -\left( \frac{12}{147} \right) = \left( \frac{11}{147} \right) = -\left( \frac{1}{11} \right) = -(-1)^{\frac{11-1}{2}} \left( \frac{3}{11} \right) = \left( \frac{3}{11} \right) \\ &= (-1) \left( \frac{11}{3} \right) = (-1) \left( \frac{2}{3} \right) = 1 \end{aligned}$$

Para que estos sea 1:  $\left( \frac{m}{n} \right) \left( \frac{w}{n} \right) = (-1)^{\frac{n-1}{2} \cdot \frac{m-1}{2}}$   $n, w$  impares rel. primos.

## Enteros Algebricos

de  $\mathbb{Q}$  o entero algebraico es aquella que cumple  
 $x^n + a_{n-1}x^{n-1} + \dots + a_0 \in \mathbb{Z}$

Entonces  $\mathbb{Z}[d] = \underbrace{\mathbb{Z} \oplus \mathbb{Z} d \oplus \dots \oplus \mathbb{Z} d^{n-1}}_{\mathbb{Z}}$

$$d^n = -a_{n-1}d^{n-1} - \dots - a_0 \in \mathbb{Z}$$

$$\begin{aligned} \text{as } d, d^2, \dots, d^n \in \mathbb{Z} \\ \text{y } a_{n-1}, a_{n-2}, \dots, a_0 \in \mathbb{Z} \end{aligned}$$

Por inducción:  $d^n \in \mathbb{Z}$  (señalado)

Ejemplo:  $\mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2} \mid a, b \in \mathbb{Z}\} \text{ s.t. } t^2-2=0$

$$\mathbb{Z}[\sqrt{-2}] = \{a+b\sqrt{-2} \mid a, b \in \mathbb{Z}\} \text{ s.t. } t^2-2=0$$

$$\mathbb{Z}[\sqrt[3]{2}] = \{a+b\sqrt[3]{2}+c\sqrt[3]{4} \mid a, b, c \in \mathbb{Z}\} \text{ s.t. } t^3-2=0$$

Si no son enteros algebraicos. Si  $w = \frac{1}{\sqrt{2}} \Rightarrow 2w^2-1=0 \Rightarrow t^2-\frac{1}{2}=0$

$\Rightarrow \frac{1}{\sqrt{2}}$  no es entero algebraico.

Aquí  $\mathbb{Z}\left[\frac{1}{\sqrt{2}}\right] = \{a+b\frac{1}{\sqrt{2}} \mid a, b \in \mathbb{Z}\}$

$$\text{donde } \mathbb{Z}(z) = \{a, b \mid \text{s.t. } z \in \mathbb{Z}(z)\}$$

Preguntas:

Es dos un primo en  $\mathbb{Z}(\sqrt{2})$

$$\mathbb{Z}(z) \cong \frac{\mathbb{Z}[x]}{(f(x))}$$

$$\frac{\mathbb{Z}(z)}{(2)} \cong \frac{\mathbb{Z}(x)}{(2x)} \cong \frac{\mathbb{Z}_2[x]}{(f(x))} \text{ no es dominio.}$$

Si  $x+1 \neq 0$  en  $\mathbb{F}_2[x]$  (pues  $0 - x^2 + 1 = (x+1)^2$  en  $\mathbb{F}_2[x]$ )

$$\text{Por consiguiente } \frac{\mathbb{F}_2[x]}{(x^2+1)} \cong \frac{\mathbb{F}_2[x]}{(x+1)^2} \cong \frac{\mathbb{F}_2[x]}{y^2} \cong \mathbb{F}_2 \oplus \mathbb{F}_2[y].$$

Preguntar  
¿ $\mathbb{Z}_{(1+i)}$  es primo en  $\mathbb{Z}[i]?$

$$\frac{\mathbb{Z}(1+i)}{(1+i)} \cong \frac{\mathbb{Z}(1)}{(1+i, 1+i)} \cong \frac{\mathbb{Z}(1)}{(1+i)} \cong \frac{\mathbb{Z}}{(2)} \cong \mathbb{F}_2 \quad \text{Dado que}$$

$\lim_{x \rightarrow 1+i} \Rightarrow (1+i)$  es primo.

Otro caso:  $\mathbb{Z}(\sqrt{-3})$ :

$$\frac{\mathbb{Z}(\sqrt{-3})}{(3)} \cong \frac{\mathbb{Z}(x)}{(3, x^2+1)} \cong \frac{\mathbb{F}_3[x]}{x^2+1} \cong \frac{\mathbb{F}_3[x]}{x-1} \times \frac{\mathbb{F}_3[x]}{x+1} \cong \mathbb{F}_3 \times \mathbb{F}_3$$

Ast:  $\Phi: \mathbb{Z}(\sqrt{-3}) \rightarrow \mathbb{F}_3 \times \mathbb{F}_3$

$$\ker \Phi = (3)$$

$$\text{Im } \Phi_1 = (3, \sqrt{-3}-1) \quad \{ \text{ideales maximales.}$$

$$\text{Im } \Phi_2 = (3, \sqrt{-3}+1)$$

$$(3) = (3, \sqrt{-3}-1) \cap (3, \sqrt{-3}+1)$$

$\mathbb{Z}(\sqrt{-3})$  es de los

1  
11

1  
3

1  
Descompuesto

$\mathbb{Z}(1+i)$  (1+i)

1  
 $\mathbb{Z}$   
(2)

Primo  
ramificado

$$(x, y, z) = \alpha(a, b, 0) + \beta(a+1, b+1, 0) + \gamma(1, a, 1)$$

$$\Rightarrow \begin{cases} x = \alpha a + \beta a + \beta + \gamma = \alpha a + (a+1)\beta + \gamma \\ y = \alpha b + \beta b + \beta + \gamma a = b\alpha + (b+1)\beta + a\gamma \\ z = \gamma \end{cases}$$

$$\Rightarrow \begin{cases} x = \alpha a + \beta a + \beta + z \\ y = \alpha b + \beta b + \beta + za \end{cases}$$

$$\begin{aligned} x - y &= \alpha(a-b) + \beta(a-b) + z(1-a) \\ &= (\alpha + \beta)(a-b) + z(1-a) \end{aligned} \quad \left. \begin{array}{l} bx = ab\alpha + b(a+1)\beta + bz \\ -ay = -ab\alpha - a(b+1)\beta - a^2z \\ \hline \beta [b(a+1) - a(b+1)] \\ = bx - ay + z(a^2 - b) \end{array} \right\}$$

~~suppose~~

$$\begin{cases} x = a\alpha + (a+1)\beta + z \\ y = b\alpha + (b+1)\beta + az \end{cases}$$



• Given formula  
• Given formula  
• Given formula

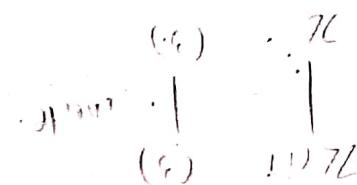
W.L.C.S. d.g. d.

$$t - z = 9.9176$$

$$y - z = 2.9176$$

$$n - z = 1.9176$$

Table



$$L1 \cdot E1 = \frac{1.9176}{1.9176} = \frac{(a)Z}{(a)Z} = \frac{(b)}{(b)Z} = \frac{1.9176}{1.9176}$$

Teoría de Números  
Desarrollo Puebla 3  
Marco Godoy V.

(2,8)

1	-
3	3
3	3
4	-
5	12
6	-

## Problema 2

Por demostrar que toda sucesión en  $\mathbb{Z}_p$  tiene una subsucesión convergente.

Dem. Sea  $(a_n)_{n \in \mathbb{N}}$  sucesión en  $\mathbb{Z}_p$ .

$$|a_n|_p \leq 1 \quad \forall n \in \mathbb{N}$$

$$|a_n|_p \leq 1 \iff a_n \in B[0, 1]$$

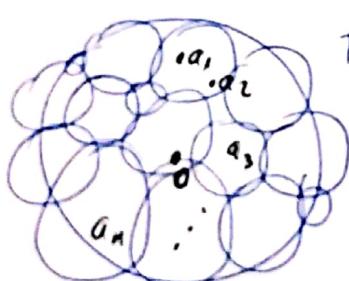
Como  $(\mathbb{Q}_p, | \cdot |_p)$  es un espacio métrico, sólo basta demostrar que  $B[0, 1] = \mathbb{Z}_p$  es compacto en  $(\mathbb{Q}_p, | \cdot |_p)$ . ✓

Sea  $\mathcal{A} = \{A_i\}_{i \in I}$  un abanimiento de  $B[0, 1]$ , es decir,

~~B[0,1]~~

$$B[0, 1] \subseteq \bigcup_{i \in I} A_i = \bigcup \mathcal{A}$$

$\Rightarrow \exists i_0 \in I$  tal que  $A_{i_0}$  contiene infinitos términos de la sucesión



$B[0, 1]$

¿Por qué? (los un  
abamiento finito?)

$\mathcal{A} = \{A_i\}_{i \in I}$  abanicado.

si  $A_{i_0}$  contiene infinitos términos,  
no significa que los contiene todos salvo  
unos <sup>finitos</sup> puntos de la sucesión!

Sea  $\{a_{n_1}, a_{n_2}, \dots, a_{n_k}\}$  los términos de la sucesión que no están en  $\mathbb{Z} \setminus A_{i_0}$ , y  $A_{n_1}, A_{n_2}, \dots, A_{n_k} \in \mathcal{A}$  tq  $B[0, 1]$  no es el conjunto de punto de la sucesión!

$$a_{n_j} \in A_{n_j} \quad \forall j = 1, \dots, k$$

Luego  $\mathcal{A}_0 = \{A_{n_1}, A_{n_2}, \dots, A_{n_k}, A_{i_0}\} \subset \mathcal{A}$  es un subabamiento finito de  $B[0, 1]$ : etc.

$$B[0, 1] \subset \bigcup \mathcal{A}_0$$

$\therefore B[0,1]$  es compacto.

$\therefore (a_n)_{n \in \mathbb{N}}$  admite una subsecuencia convergente  
en  $B[0,1] = \mathbb{Z}_p$ .

## Problema ② ③

¿Para qué primos  $p$  se cumple que el anillo de enteros del cuerpo  $\mathbb{Q}_p(\sqrt{5})$  es  $\mathbb{Z}_p[\sqrt{5}]$ ?

Sea  $\mathfrak{o}$  un lugar sobre  $p$  ( $\frac{8}{1}$ ).  $\mathcal{O}_{\mathfrak{o}}$  el anillo de enteros de  $L_{\mathfrak{o}}$ , donde  $L = \mathbb{Q}(\sqrt{5})$ . El valor absoluto de  $L$  es  $P_{\mathfrak{o}}$  y ~~se sabe~~  $L_{\mathfrak{o}}$  es el completado de  $L$  por  $P_{\mathfrak{o}}$ .

Primero notemos que  $\mathbb{Z}_p[\sqrt{5}] \subset \mathcal{O}_{\mathfrak{o}}$ , ya que

$$x \in \mathbb{Z}_p[\sqrt{5}] : x = x_1 + \sqrt{5}x_2, \quad x_1, x_2 \in \mathbb{Z}_p$$

$$P_{\mathfrak{o}}(x) = |N_{L/\mathbb{Q}}(x)|_p = |x_1^2 - 5x_2^2|_p \quad (k = \mathbb{Q}).$$

$$\leq \max \{|x_1|_p, |5x_2|_p\}$$

$$\text{Pero } |x_1|_p, |x_2|_p \leq 1 \quad \text{y} \quad |5|_p = \begin{cases} 1 & p=5 \\ \frac{1}{5} & p \neq 5 \end{cases}$$

$$\therefore P_{\mathfrak{o}}(x) \leq 1 \quad \forall x \in \mathbb{Z}_p[\sqrt{5}]$$

$$\text{Por otro lado, } \mathcal{O}_L = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right] \quad (5 \equiv 1 \pmod{4}).$$

~~El diagrama siguiente explica mejor la situación, si  $\delta = \frac{1+\sqrt{5}}{2}$~~

$$\Rightarrow \delta^2 - \delta - 1 = 0.$$

Observemos el diagrama siguiente

$$\mathcal{O}_L \supset \mathcal{O}_K = \mathbb{Z}$$

$$\cap \quad \cap$$

$$\mathcal{O}_{\mathfrak{o}} \supset \mathcal{O}_p = \mathbb{Z}_p$$

$$\cap \quad \cap$$

$$L_{\mathfrak{o}} \supset \mathbb{Q}_p$$

sabiendo esto, es fácil llegar a la conclusión, es para  $p \neq 2$ .

Luego queremos que  $8 \notin \mathbb{O}_p$ , pero esto es equivalente a encontrar los primos  $p$  tales que

$$x^2 - x - 1 \equiv 0 \pmod{p} \quad \text{no tiene solución.}$$

No olvidar que  $\frac{8}{p}$  (Si  $x^2 - x - 1 \equiv 0 \pmod{p}$ ) tuviera solución, entonces por Hensel puedo levantar a una solución en  $\mathbb{O}_p$

Para  $p=2$ ,  $x^2 - x - 1 \equiv 0 \pmod{2}$  no tiene solución (fácil).

Para  $p > 2$ , ~~basta estudiar el símbolo del Jacobiano~~ podemos ocupar la fórmula clásica de ecuaciones cuadráticas

$$x^2 - x - 1 = 0 \iff x = \frac{1 \pm \sqrt{5}}{2}$$

$\Rightarrow (x^2 - x - 1 \equiv 0 \pmod{p})$  sin solución  $\iff 5$  no es ~~-~~ mudiado

$$\iff \left(\frac{5}{p}\right) = -1$$

$$\underline{p=3}: \quad \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1 \quad \left(1^2 \equiv 1(3), 2^2 \equiv 1(3), 0^2 \equiv 0(3)\right)$$

$$\underline{p=5}: \quad X$$

$$\underline{p > 5}: \quad \left(\frac{5}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{p-1}{2}} \left(\frac{p}{5}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{5}\right)$$

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

$$\text{Ahora: } 0^2 \equiv 0, 1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 4, 4^2 \equiv 1 \pmod{5}$$

$\therefore 0, 1, 4$  son  $\square$  modulo 5 ;  $2, 3$  no son  $\square$  modulo 5

$$\therefore p \equiv 2, 3 \pmod{5}$$

~~Conclusión~~ Los primos que sirven son los que son congruentes a 2 y/o 3 módulo 5. También sirve el 2 y el 3.

### Problema 5

$p$  primo mayor que 2

(a) Por demostrar que  $\exp_p(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$  convergente para todo  $x \in p\mathbb{Z}_p$ .

#### Demarcación

Observación:  $x \in p\mathbb{Z}_p \Leftrightarrow x = p^y, y \in \mathbb{Z}_p$ .

$$\exp_p(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!} < \infty \Leftrightarrow \left| \frac{x^n}{n!} \right|_p \xrightarrow{n \rightarrow \infty} 0$$

$$\Leftrightarrow v_p\left(\frac{x^n}{n!}\right) \xrightarrow{n \rightarrow \infty} \infty$$

$$v_p\left(\frac{x^n}{n!}\right) = v_p(x^n) - v_p(n!) \quad , \text{ donde}$$

$$v_p(n!) = \sum_{i=1}^{\infty} \left[ \frac{n}{p^i} \right] \leq \sum_{i=1}^{\infty} \frac{n}{p^i} = n \sum_{i=1}^{\infty} \frac{1}{p^i} = n \left( \frac{1}{1-p} - 1 \right)$$

$$= n \frac{\frac{1}{p}}{1-p} = \frac{n}{p-1}$$

$$\therefore v_p\left(\frac{x^n}{n!}\right) = n v_p(x) - n \frac{p}{1-p} = n \left( v_p(x) - \frac{p}{1-p} \right)$$

$$\therefore v_p\left(\frac{x^n}{n!}\right) \xrightarrow{n \rightarrow \infty} \infty \Leftrightarrow v_p(x) - \frac{p}{1-p} > 0$$

$$\Leftrightarrow v_p(x) > \frac{p}{1-p}$$

pero  $v_p(x) > \frac{p}{1-p}$  es lo mismo que  $-\frac{p}{1-p} > -v_p(x)$

$$\Rightarrow p^{-\frac{p}{1-p}} > p^{-v_p(x)} = |x|_p \quad \therefore x \in B(0, p^{-\frac{p}{1-p}})$$

Luego basta demostrar que

$$\forall x \in p\mathbb{Z}_p : |x|_p < p^{-\frac{p}{1-p}}$$

$$x \in p\mathbb{Z}_p : x = py, y \in \mathbb{Z}_p$$

$$|x|_p = |py|_p = |p|_p |y|_p < p^{-1},$$

$$\text{pero como } p > 2 : p^{\frac{p}{p-1}} \geq 1$$

$$\therefore \frac{1}{p^{\frac{p}{p-1}}} \leq p \quad (\Rightarrow p^{\frac{p}{p-1}-p} \leq p)$$

$$\therefore p^{-1} \leq p^{-\frac{p}{1-p}}$$

$$\therefore \forall x \in p\mathbb{Z}_p : |x|_p < p^{-\frac{p}{1-p}}$$

(b) Probar que  $\sum_{n=1}^{\infty} (\exp_p(p^n) - 1)$  es convergente.

Dem.

$$\sum_{n=1}^{\infty} (\exp_p(p^n) - 1) < \infty \iff \exp_p(p^n) - 1 \xrightarrow{n \rightarrow \infty} 0$$
$$\iff |\exp_p(p^n) - 1|_p \xrightarrow{n \rightarrow \infty} 0$$

$$\iff v_p(\exp_p(p^n) - 1) \xrightarrow{n \rightarrow \infty} \infty$$

Por otro lado:

$$\exp_p(x) - 1 = \sum_{k=1}^{\infty} \frac{x^k}{k!}$$

$$\Rightarrow \exp_p(p^n) - 1 = \sum_{k=1}^{\infty} \frac{p^{nk}}{k!}$$

$$\Rightarrow v_p(\exp_p(p^n) - 1) = v_p \left( \sum_{k=1}^{\infty} \frac{p^{nk}}{k!} \right)$$

obs.  $n!$  crece mucho más rápido que  $p^{nk}$  cuando  $n$  crece indefinidamente

Parcialmente tenemos

$$v_p\left(\sum_{k=1}^j \frac{p^{nk}}{k!}\right) \geq \min_{k=1}^j \left\{ v_p\left(\frac{p^{nk}}{k!}\right) \right\} = v_p\left(\frac{p^{nj}}{j!}\right)$$

$$v_p\left(\sum_{k=1}^j \frac{p^{nk}}{k!}\right) \geq v_p\left(\frac{p^{nj}}{j!}\right) = v_p(p^{nj}) - v_p(j!)$$

$$= nj v_p(p) - v_p(j!)$$

$$= nj - v_p(j!)$$

$$\geq nj - j \underbrace{\frac{p}{1-p}}_{p-1} \quad \left( \text{por resultado en (a)} \right) \quad v(j!) \leq j \frac{p}{1-p}$$

$$= j \left(n - \frac{p}{1-p}\right)$$

cuando  $j \rightarrow \infty$ ,  $\cancel{v_p\left(\sum_{k=1}^j \frac{p^{nk}}{k!}\right)}$   $j \left(n - \frac{p}{1-p}\right) \xrightarrow{j, n \rightarrow \infty} \infty$

(cuando  $n > \frac{p}{1-p}$ , sea suficientemente grande)

$$\therefore v_p\left(\sum_{k=1}^{\infty} \frac{p^{nk}}{k!}\right) \xrightarrow{n \rightarrow \infty} \infty$$

$\therefore \sum_{n=1}^{\infty} (\exp_p(p^n) - 1)$  converge.