

3) Ejemplo:  $0 \in S$

$$\frac{0}{0} = \frac{2}{6} \text{ pues } 0 \cdot b - 0a = 0.$$

por transitividad:

$$\frac{2}{6} = \frac{a}{a}, \forall a \in A, b, d \in \mathbb{Z}$$

$$S^{-1}A = \left\{ \frac{0}{0} \right\}.$$

Observe que:  $S^{-1}A$  es un anillo con:

$$\frac{a}{s} \cdot \frac{a'}{s'} = \frac{aa'}{ss'}.$$

$$\frac{a}{s} + \frac{a'}{s'} = \frac{as' + a's}{ss'}.$$

Ejercicio: Comprobar

• Existe un homomorfismo natural:  $\varphi: A \rightarrow S^{-1}A$ ; fijando  $s \in S$

(Si suponemos podemos escoger  $s=1$ )

dvs: No depende de la elección de  $s \in S$ .

$$\frac{sa}{s} = \frac{s'a}{s'} \text{ pues } sa \cdot s' - ss'a = 0 \text{ (comunitativo)}$$

$$\varphi(a+b) = \frac{s(a+b)}{s} = \frac{sa+sb}{s} = \frac{sa}{s} + \frac{sb}{s} = \varphi(a) + \varphi(b).$$

$$\varphi(ab) = \frac{sa \cdot sb}{s} = \frac{s^2ab}{s^2} = \left(\frac{sa}{s}\right)\left(\frac{sb}{s}\right) = \varphi(a)\varphi(b)$$

$$a \in \ker \varphi \iff \frac{sa}{s} = 0 \iff ss'(sa - 0) = 0 \iff ss' \mid s''a = 0$$

$$\text{pues si } \frac{sa}{s} = 0 \text{ si } s'' = s''s' \text{ cumple con } s''a = 0$$

$$\text{y si } s''a = 0 \Rightarrow \text{teniendo } s'' = s'''s, s''(s' - 0) = (s'''a)s' = 0$$

$$\therefore \frac{sa}{s} = 0.$$

En particular si  $S$  no contiene divisiones de cero, entonces  $\varphi$  es inyectivo. (pues  $S^{-1}a = 0 \Rightarrow a = 0$ )

Ejemplo:  $\mathbb{Z}/6\mathbb{Z} = A, S = \{\bar{3}\}$

$$\ker \varphi = \{\bar{0}, \bar{2}, \bar{4}\} \Rightarrow S^{-1}A = \left\{ \frac{\bar{0}}{\bar{3}}, \frac{\bar{1}}{\bar{3}} \right\}.$$

$$\text{Im } \varphi \cong \frac{A}{\ker \varphi} \cong \frac{\mathbb{Z}/6\mathbb{Z}}{\mathbb{Z}/2\mathbb{Z}} \cong \mathbb{Z}/2\mathbb{Z}$$

Ejemplo:  $A = \mathbb{D}$  dominio,  $S = D^{\neq 0}$

$$S^{-1}A = \left\{ \frac{a}{b} \mid a \in A, b \in A - \{0\} \right\} = \text{Umfld. (D)}$$

A anillo conmutativo.

$$S = \{a \in A \mid a \text{ no es divisor de cero}\}$$

$\Leftrightarrow ab \text{ es divisor de cero} \Leftrightarrow \text{factoconst. } (ab)c = 0$

$\Leftrightarrow b \text{ div. de cero.}$

$\Leftrightarrow b \neq 0 \text{ y } (2)(bc) = 0 \Rightarrow a \text{ divisor de cero.}$

O sea  $ab \text{ div. de cero} \Rightarrow a \text{ div. de cero o } b \text{ div. de cero.}$

$a, b \in S \Rightarrow ab \in S.$

$$S^{-1}A = \left\{ \frac{a}{b} \mid a \in A, b \in A \text{ no div. de cero} \right\}$$

$$\varphi: A \longrightarrow S^{-1}A$$

$\ker \varphi = \{0\}, A \subseteq S^{-1}A \leftarrow$  nula complemento de fracciones

(ambas, mas pregunta si se expresa

elementos de  $A - S \Rightarrow \ker \varphi \neq \{0\} \Rightarrow$

Ej:  $A = \mathbb{Z} \times \mathbb{Z}$ .

$$S = \{(c, d) \mid c, d \neq 0\}.$$

$$\frac{(a, b)}{(c, d)} \in S^{-1}A \Leftrightarrow c, d \neq 0 \Leftrightarrow \frac{a}{c} \in \mathbb{Z}, \frac{b}{d} \in \mathbb{Z}$$

$$Af: S^{-1}A \cong \mathbb{Z} \times \mathbb{Z}$$

$$\varphi: S^{-1}A \longrightarrow \mathbb{Z} \times \mathbb{Z}, \quad \varphi\left(\frac{(a, b)}{(c, d)}\right) = \left(\frac{a}{c}, \frac{b}{d}\right), \quad c, d \neq 0.$$

$$S: \frac{(a, b)}{(c, d)} = \frac{(a', b')}{(c', d')}$$

$$\hookrightarrow S^{\text{II}}: (a, b)(c', d') - (c, d)(a', b') = (0, 0)$$

no div. de cero.

$$\Leftrightarrow \begin{aligned} ac' - ca' &= 0 \Rightarrow \frac{a}{c} = \frac{a'}{c'} \\ bd' - db' &= 0 \Rightarrow \frac{b}{d} = \frac{b'}{d'} \end{aligned}$$

$$\Leftarrow \Psi\left(\frac{(a, b)}{(c, d)}\right) = \Psi\left(\frac{(a', b')}{(c', d')}\right) \text{ bién de finida e inyectiva}$$

Demostrarlo que falta.

Ejercicio:  $I^{-1}A = \frac{S}{S}$

Supongamos ahora que  $I \subseteq A$  ideal,  $A/I$  anillo, cociente  $= \{\bar{a}, a \in A\}$ .

$$S^{-1}I = \left\{ \frac{i}{s} : i \in I, s \in S \right\}$$

Aff:

$$S^{-1}I \in \text{ideal de } S^{-1}A \quad \text{ya que } s^{-1}i \in S^{-1}A \quad \forall s \in S, i \in I$$

$$\frac{1}{s} + \frac{1}{s'} = \frac{ss' + si}{ss'} \in S^{-1}A \quad \forall s, s' \in S, i \in I$$

$$\frac{i}{s} \cdot \frac{a}{s'} = \frac{ia}{ss'} \in S^{-1}I \quad \forall i \in I, a \in A, s, s' \in S$$

$$\bar{S} = S\bar{S}, S \in S^{\text{II}}. (\bar{S}\bar{S} = \bar{SS} \in S \Rightarrow \bar{S} \text{ conj. multiplicativo}).$$

Se define

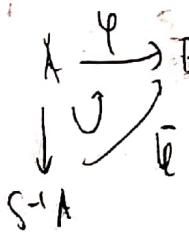
$$\bar{S}^{-1} = \{ \bar{s}^{-1} : s \in S \} \quad S^{-1}A / S^{-1}I \cong A / I$$

Prop:  $\bar{S}^{-1}(A/I) \cong S^{-1}A / S^{-1}I$

anillo de fracciones

Lema: Si  $\Psi: A \rightarrow B$  homomorfismo no tal que  $\Psi(s)$  invertible en  $B$  para

que  $S \subseteq \text{entres. p. de } A$ ,  $\Psi: S^{-1}A \rightarrow S^{-1}B$  sea p. inverso de  $\Psi$ .



Dew: Sea  $\bar{\Psi}\left(\frac{a}{s}\right) = \Psi(a) - \Psi(s)^{-1}a$

$$\frac{a}{s} = \frac{a'}{s'}, \text{ssi } S^{\text{II}}(as' - a's) = 0$$

$$\begin{aligned} \bar{\Psi}(S^{\text{II}})_b, (\Psi(a)\Psi(s) - \Psi(a)\Psi(s)^{-1}a) &= 0, \quad \Psi(a)\Psi(s)^{-1} = \Psi(a')\Psi(s')^{-1} \\ \Psi(a)\Psi(s)^{-1} &= \Psi(a')\Psi(s')^{-1} \end{aligned}$$

$$p: A \xrightarrow{a \mapsto \bar{a}} A/I$$

$$\downarrow$$

$$\bar{s}(A/I), \quad \frac{\bar{a}s}{s}$$

$$\bar{p}: S^{-1}A \xrightarrow{\bar{s}(A/I)}$$

$$\frac{a}{s} \mapsto \frac{\bar{a}}{\bar{s}} = \left( \frac{\bar{a}}{\bar{s}} \right)^{-1} = \left( \frac{\bar{a}}{\bar{s}} \right)$$

$$\text{Ker } \bar{p} = \left\{ \frac{a}{s} \mid \frac{\bar{a}}{\bar{s}} = 0 \right\}$$

$$\bar{s}^n(\bar{a} - \bar{a}) = 0 \Rightarrow \bar{s}^n a = 0 \Rightarrow s^n a \in I$$

$$\frac{a}{s} = \frac{a s^n}{s s^n} \in S^{-1}I \quad \therefore \text{ker } \bar{p} = S^{-1}I$$

Hipótesis:  $\tilde{p}: S^{-1}A/S^{-1}I \xrightarrow{\sim} S^{-1}(A/I)$  (Claramente sobreyectivo)

$$\therefore \tilde{p} \text{ es biyectivo: } \begin{aligned} \tilde{p}\left(\left(\frac{a}{s}\right)\left(\frac{b}{s'}\right)\right) &= \tilde{p}\left(\left(\frac{ab}{ss'}\right)\right) = \frac{\bar{a}\bar{b}}{\bar{s}\bar{s'}} = \frac{\bar{a} \cdot \bar{b}}{\bar{s} \cdot \bar{s'}} = \frac{a}{s} \cdot \frac{b}{s'} \\ &= \tilde{p}\left(\left(\frac{a}{s}\right)\right) \tilde{p}\left(\left(\frac{b}{s'}\right)\right) \end{aligned}$$

Ejemplos: Sea  $A = \mathbb{Z}_L$ ,  $I = n\mathbb{Z}_L$  donde  $(a, n) = 1$

$$S = \{1, a, a^2, \dots\}$$

$$\bar{S} = \{\bar{1}, \bar{a}, \bar{a}^2, \dots\}$$

$$\frac{S^{-1}\mathbb{Z}_L}{S^{-1}(n\mathbb{Z}_L)} \cong \frac{S^{-1}\mathbb{Z}_L}{nS^{-1}\mathbb{Z}_L} \cong \bar{S}^{-1}\left(\frac{\mathbb{Z}_L}{n\mathbb{Z}_L}\right)$$

$$\text{Pues } S^{-1}n\mathbb{Z}_L = \left\{ \frac{nb}{at} = n\left(\frac{b}{at}\right) \mid b \in \mathbb{Z}_L, t \in \mathbb{Z}_L \right\}$$

$$S^{-1}\mathbb{Z}_L = \mathbb{Z}_L[1/a] = \left\{ b/a^t \mid b \in \mathbb{Z}_L, t \geq 0 \right\}$$

obs: Los elementos de  $\bar{S}$  son invertibles en  $\mathbb{Z}_L/n\mathbb{Z}_L$ .

$$\text{Jugando: } \frac{S^{-1}\mathbb{Z}_L}{nS^{-1}\mathbb{Z}_L} \cong \bar{S}^{-1}\left(\frac{\mathbb{Z}_L}{n\mathbb{Z}_L}\right) \cong \mathbb{Z}_L/n\mathbb{Z}_L.$$

Agregara  $\mathbb{Z}_L$  elementos que son invertibles modulo  $n$  "nofecta" el cociente  $\mathbb{Z}_L/n\mathbb{Z}_L$ .

Ejemplo:  $A = \mathbb{Z}/\left[\frac{1}{2}\right] = S^{-1}\mathbb{Z}$ ,  $S = \{1, 2, 4, \dots\}$

en  $\mathbb{Z}/_6\mathbb{Z}$ .

$$\bar{S} = \{\bar{1}, \bar{2}, \bar{4}\}$$

$$\mathbb{Z}/_6A \cong \bar{S}^{-1}(\mathbb{Z}/_6\mathbb{Z}) = \left\{ \frac{\bar{0}}{\bar{1}}, \frac{\bar{1}}{\bar{1}}, \frac{\bar{2}}{\bar{1}} \right\}$$

$$\text{y como } \frac{\bar{3}}{\bar{1}} = \frac{\bar{0}}{\bar{1}}$$

$$\bar{S}^{-1}(\mathbb{Z}/_6\mathbb{Z}) \cong \bar{S}^{-1}(\mathbb{Z}/_3\mathbb{Z}) \cong \mathbb{Z}/_3\mathbb{Z} \cong \left\{ \bar{0}, \bar{1}, \bar{2} \right\}$$

Si uno recuerda t. ctiva del tensor:

$$\mathbb{Z}/_6\mathbb{Z} \cong \mathbb{Z}/_3\mathbb{Z} \times \mathbb{Z}/_2\mathbb{Z}$$

En general si  $n \in P_{\alpha}$

$$\mathbb{Z}/_n\mathbb{Z} \cong \prod_{\alpha \in P} \mathbb{Z}/_{P_{\alpha}}\mathbb{Z} \quad S^{-1}\mathbb{Z} = \mathbb{Z}[\frac{1}{m}]$$

$$\text{Si } m = p^{\alpha} n, \text{ en } \mathbb{Z}/_{p^{\alpha} n}\mathbb{Z} \quad \bar{p}^{\alpha} = \bar{0} \quad \frac{1}{m} = \frac{1}{p^{\alpha} n} = \frac{1}{p^{\alpha}} \cdot \frac{1}{n} = \frac{1}{\bar{p}^{\alpha}} \cdot \frac{1}{n}, \bar{0} \in S$$

$$S^{-1}(\mathbb{Z}/_{p^{\alpha} n}\mathbb{Z}) = \{\bar{0}\} \quad (\text{awlo})$$

Volviendo a lo anterior:

$$\text{Def: Si } a \in S \subseteq A^*, \text{ entonces } A \cong S^{-1}A$$

$$\psi: A \rightarrow S^{-1}A$$

que es una  $\psi(a) = \frac{a}{1}$  (no tiene dim. de  $\mathbb{Z}$ )

inyección (mantiene dim. de  $\mathbb{Z}$ )

$$\psi \text{ ep: pues } \frac{q}{s} = \psi(qs^{-1}) = \frac{qs^{-1}}{1} \quad \therefore \frac{q}{s} \in \text{Im } \psi$$

$$S^{-1}A \cong A \quad \text{ya que } \psi(A) = \left\{ \frac{a}{1} \mid a \in A \right\} = A$$

es decir  $S^{-1}A = A$

A anillo Comunitativo  $P \subseteq A$  ideal primo  $S_P = A/P = \{a \in A \mid a \notin P\}$

es multiplicativo.

$A_P = S_P^{-1}A = \left\{ \frac{a}{b} : a, b \in A, b \notin P \right\}$  Anillo Localizado en  $P$ ,  $\mathcal{U}(P)$ .

Problema. Resolver  $a^2 + b^2 = c^2$ ,  $a, b, c \in \mathbb{Z}$

$$(a+bi)(a-bi) = c^2$$

Sea  $\pi$  primo tal que  $\pi | (a+bi)$ , en  $\mathcal{U}(i)$ ,  $\pi | (a-bi)$   $\Rightarrow \frac{b}{\pi}$

Supongamos  $a, b, c$  son relativamente primos.

Asi:  $\pi | (2a)$ ,  $\pi | (2bi) \Rightarrow \pi | (2b)$  pero si  $\pi$  es impar.

$$\pi \in \mathcal{U}(i) \Rightarrow \pi = c + di$$

$$\text{Si } \pi | (2a) \Leftrightarrow 2a = \pi r \Leftrightarrow 2a = \overline{\pi} \bar{r} \Leftrightarrow \overline{\pi} | (2a)$$

Caso I: Supongamos que  $\pi$  y  $\bar{\pi}$  nos son asociados.

$\mathbb{Z} \ni N(\pi) = \pi \bar{\pi}$  divide a  $2a$

Juego:  $N(\pi) | 2a, 2b$ .

Caso II: Supongamos que  $\pi$  es asociado a  $\bar{\pi} \Rightarrow \pi = n\bar{\pi}$ ,  $n \in \mathbb{Z} \pm i$ .

$$\text{Si } \pi = \bar{\pi} \Rightarrow \pi \in \mathbb{R} \cap \mathcal{U}(i) = \mathbb{Z}.$$

$$\text{Si } \pi = -\bar{\pi} \Rightarrow \pi \in i\mathbb{R} \cap \mathcal{U}(i) = i\mathbb{Z}.$$

$$\text{Si } \pi = i\bar{\pi} \Rightarrow \pi = \lambda(1-i), \lambda \in \mathbb{Z} \text{ como es primo} \Rightarrow \pi \in \mathbb{Z}(1-i)$$

$$\text{y } N(\pi) = 2.$$

$$\text{Si } \pi = -i\bar{\pi} \Rightarrow \pi = \lambda(1+i), \lambda \in \mathbb{Z} \text{ como es primo} \Rightarrow \pi \in \mathbb{Z}(1+i)$$

$$\text{y } N(\pi) = 2. \text{ (Asociados al tercero pues } (1+i)^2 = (i)(1-i)).$$

S:  $a+bi$  y  $a-bi$  tienen un divisor primo común enteros:

1) Si  $\pi$  no es asociado a  $\pi$ :  $N(\pi) \mid a^2 - b^2$ .

2) Si  $\bar{\pi} = \pm \pi$ ;  $\pi$  es asociado a un primo de  $\mathbb{Z}$   $\Rightarrow \pi \mid a, b$ .

3) Si  $\bar{\pi} = \pm i\pi$   $\pi$  asociado a  $1+i$  ( $z = (1-i)(1+i)$ )

Entonces:  $\pi \mid 2a, 2b$  en  $\mathbb{Z}(i)$

$\pi$  no es asociado a  $(1+i)$   $\Rightarrow \pi + 2 \in \mathbb{Z}(i)$

$\pi \mid a, \pi \mid b$  en  $\mathbb{Z}(i)$

Si  $\pi \in \mathbb{Z}$ :  $\frac{a}{\pi} \in \mathbb{Z}(i)$ ,  $\frac{b}{\pi} \in \mathbb{Z}(i) \Rightarrow \frac{a}{\pi} \in \mathbb{Z} \Rightarrow \pi \mid a$  en  $\mathbb{Z}$ .

S:  $(a, b) = 1$  ( $a+bi, a-bi$ ) tiene cuadrados que dividen si y solo si  $a^2 - b^2$  es cuadrado.

Entonces  $at+bs=1$ ,  $t, s \in \mathbb{Z} \Rightarrow t, s \in \mathbb{Z}(i)$   $\Rightarrow \pi \mid a^2 - b^2$

y si  $\pi \mid a+bi$ ,  $\pi \mid a-bi \Rightarrow \pi \mid 2a, 2b$ , pero  $2at+2bs=2 \Rightarrow (2a, 2b)=2$   
 $\Rightarrow \pi \mid 2 \Rightarrow (a+bi, a-bi) \mid 2$ .

Caso I:  $(a+bi, a-bi)=1$ .

Sabemos que:  $(a+bi)(a-bi) = C^2$  tiene cuadrados que dividen si y solo si  $a^2 - b^2$  es cuadrado.

$\Rightarrow (a+bi) = (C+di)^2 \Rightarrow (a+bi) = i(C+di)$

$$\begin{cases} a = C^2 - d^2 \\ b = 2cd \end{cases} \quad \begin{cases} a = -2cd \\ b = -2C^2 + 2d^2 \end{cases}$$

Caso II:  $(a+bi, a-bi)=2$ .

$\Rightarrow 2 \mid a+bi \Rightarrow \frac{a+bi}{2} \in \mathbb{Z}(i) \Rightarrow \frac{a}{2}, \frac{b}{2} \in \mathbb{Z} \Rightarrow (a, b) \neq 2$ . (\*)

Caso III:  $(a+bi, a-bi) = (1+i)$

$a+bi = (1+i)(C+di)^2 \Rightarrow a+bi = (1+i)(1+i)(C+di)^2$

o bien  $a+bi = i(1+i)(C+di)^2$

$$\text{Entonces: } a+bi = (1+i)(c^2-d^2 + 2cdi)$$

$$a+bi = c^2-d^2 + 2cdi + (c^2-d^2)i - 2cd$$

$$\begin{cases} a = c^2-d^2-2cd \\ -b = c^2-d^2+2cd \end{cases} \Rightarrow a \equiv b \pmod{4}$$

$$\Rightarrow a, b \text{ impares} \Rightarrow \begin{cases} a^2 \equiv 1 \pmod{4} \\ b^2 \equiv 1 \pmod{4} \end{cases} \Rightarrow a^2+b^2 \equiv 2 \pmod{4}$$

otro lado:  $a+bi = (1+i)(c+di)^2$

$$a+ib = (1+i)(c-di)^2$$

$$a^2+b^2 = 2(c^2+d^2)^2 \quad (\neq)$$

Pregunta: ¿Los primos en  $\mathbb{Z}[i]$  se escriben como suma de cuadrados?

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

$$\text{en } \mathbb{Z}(i): p = (a+bi)(a-bi) \quad \text{dominio } \mathbb{F}_p[x] \xrightarrow{\text{Salvo s.}} \frac{\mathbb{F}_p[x]}{(x^2+1)} \xrightarrow{\text{Solución.}}$$

$p$  dejar de ser primo en  $\mathbb{Z}(i) \Leftrightarrow p \in \mathbb{Z}(i)$  no es dominio

$$p \text{ es primo en } \mathbb{Z}(i) \text{ si } \left(\frac{-1}{p}\right) = -1 \text{ si } p \equiv 3 \pmod{4}$$

Ej:  $5 = (2+i)(2-i) = 2^2 + 1^2$

obs:  $\pi$  es un primo de  $\mathbb{Z}(i)$  pero no es asociado a un primo en  $\mathbb{Z}$ .

entonces  $\pi$  divide  $N(\pi) = \pi\bar{\pi} \in \mathbb{Z}$ ,  $N(\pi) = p_1^{2n_1} p_2^{2n_2} \dots p_r^{2n_r}$

$\Rightarrow \pi | p_i$ , si hay d'or  $p_i \mid \pi$  es la fac. de  $N(\pi)$ .

$$\pi\bar{\pi} = (p_1 p_2 \dots p_r)^2$$

$$\pi\bar{\pi} = p_1^2 \dots p_r^2$$

entonces  $\pi$  es asociado a un primo de  $\mathbb{Z}$ . ( $\neq$ )

Luego  $N(\pi)$  es primo.

$$\text{En tal caso } p = \pi\bar{\pi}.$$

Por otro lado si  $N(q)$  es primo y  $\pi | q \Rightarrow \pi | N(q) \Rightarrow N(q) = N(\pi)N(v)$

$$\Rightarrow N(v) = 1 \Rightarrow N \in \{1, \pm i\} \therefore \pi \text{ primo (irreducible).}$$

Luego  $\exists \pi \in \mathbb{Z}_{>0}$  s.t.  $P \equiv 1(4)$  y si  $\pi \mid P$ ,  $\pi$  primo en  $\mathbb{Z}[i]$

$$\Rightarrow N(\pi) \mid N(P) = P^2$$

$$\text{Si } N(\pi) = \pi^2 \Rightarrow N\left(\frac{P}{\pi}\right) = 1 \Rightarrow P \mid \pi \text{ unidado} \Rightarrow P = u\pi.$$

$$\therefore N(\pi) = P$$

$$\therefore P = \pi\bar{\pi}. \quad (\text{no sociados})$$

$$\text{Si } P=2: \quad 2 = i(1+i)^2$$

Propuesta: (Vive numeros se escriben como suma de cuadrados?)

$$a^2 + b^2 = n = p_1^{d_1} \cdots p_r^{d_r} \in \mathbb{Z}_{>0}$$

$$\text{Si } p_j \equiv 3(4) \text{ entonces } p_j \mid (a^2 + b^2) \Rightarrow (a+ib)(a-ib)$$

$$\Rightarrow (p_j) \mid a+ib \text{ y } (p_j) \mid a-ib \Rightarrow p_j \mid (a+ib)(a-ib) = p_j(c-id).$$

$$\text{pero si: } a+ib = p_j(c+id) \text{ si } a-ib = p_j(c-id).$$

$$\text{Luego } p_j \nmid a+ib \text{ si } p_j \nmid a-ib.$$

$$\text{Si } t \text{ es maximal } \Rightarrow \alpha_j = 2t$$

$$\text{La potencia } \alpha_j \in \text{par para cada } p_j \equiv 3(4).$$

$$\text{Si: } n = 2^l \underbrace{p_1^{\alpha_1} \cdots p_s^{\alpha_s}}_{\equiv 1(4)} \underbrace{p_{s+1}^{\beta_{s+1}} \cdots p_r^{\beta_r}}_{\equiv 3(4)}$$

$$2 = N(1+i) \Rightarrow p_j = N(\pi_j), \quad j \in \{1, \dots, s\}$$

$$\text{Así } h = N\left(\underbrace{(1+i)^l \pi_1^{\alpha_1} \cdots \pi_s^{\alpha_s}}_{\text{a+ib}} \underbrace{p_{s+1}^{\beta_{s+1}} \cdots p_r^{\beta_r}}_{\text{a-ib}}\right)$$

$$\therefore h = N(a+ib) = a^2 + b^2 \text{ es suma de dos cuadrados.}$$

Proposición: Un número entero es suma de dos cuadrados si y sólo si para cada primo  $p=3(4)$ , plus la mayor potencia de  $p$  ( $v_p(n)$ ) es par.

$v_p(n)$  se dice valuación p-ádica de  $n$ .

Unidades: En  $\mathbb{Z}[\sqrt{2}]$  las fracciones no están sencillas como en  $\mathbb{Z}[i]$ .

$$\text{Si: Unidad } \Rightarrow N(u) = 1 = a^2 - 2b^2.$$

$$\text{Llego } 1+\sqrt{2} \text{ unidad } \Rightarrow (1+\sqrt{2})^n \text{ Unidad, } \forall n \in \mathbb{N}$$

∴ hay infinitas unidades.

$$a^2 - 2b^2 = 1$$

Ej: Encuentre las soluciones de

$$N(5+3\sqrt{2}) = ?$$

$$N((5+3\sqrt{2})(1+\sqrt{2})^n) = ? \rightarrow \text{tiene infinitas soluciones.}$$

$$\text{Si } h = e^{2\pi i} \quad m_h(x) = 1+x+x^2+x^3+x^4$$

$$\mathbb{Z}(n) \cong \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$$

$$\mathbb{Z}(n) \hookrightarrow \mathbb{C} \times \mathbb{C}$$

$$h \mapsto (h, h^2)$$

$$\text{pensemos en } \mathbb{U}(h) = \frac{u(x)}{(m_h(x))} \cong \frac{\mathbb{U}(x)}{(x^4 + \dots + 1)} \text{ es natural incrustar en el anillo de evaluaciones en } h^4.$$

$$\mathbb{U}(n) \hookrightarrow \mathbb{R}(n) \cong \frac{\mathbb{R}(x)}{(m_h(x))} \cong \frac{\mathbb{R}(x)}{(p_1(x)p_2(x))} \cong \frac{\mathbb{R}(x)}{(p_1(x))} \times \frac{\mathbb{R}(x)}{(p_2(x))} \cong \mathbb{C} \times \mathbb{C}$$

dónde

$$p_1(x) = x^4 - (h+h^4)x + 1$$

$$= x^4 - (2\cos(\frac{2\pi}{5}))x + 1. \text{ La norma la podemos definir como:}$$

$$N(z_1, z_2) = N(z_1)N(z_2)$$

Proposición: Sea  $\mathbb{S}$  el lóbulo de cuadrados.

Entonces  $K = \mathbb{Q}(\sqrt{S})$  enteros:

$$\mathcal{O}_K^* \cong \mathbb{Z} \times \mathbb{Z} \cong C_2 \times \mathbb{Z}.$$

Otras palabras existe  $h \in \mathcal{O}_K^*$  tal que

$$\mathcal{O}_K^* = \{ \pm h^n | n \in \mathbb{Z} \}.$$

Demostración: Basta ver que el rango de este grupo es 1.

Basta ver que:

1) existe  $h \in \mathcal{O}_K^*$  de orden infinito y puede suponerse  $h > 1$ .

2) Existe  $h$  que satisface (1) minimal.

3) Si  $h$  satisface (2) entonces toda unidad es  $u = \pm h^r$ ,  $r \in \mathbb{Z}$ .

Lema: Si  $n$  entero,  $n > 0$  existe  $\alpha \in \mathbb{R}$  irracional, existe  $p, q \in \mathbb{Z}$

tal que:  $\left| \alpha - \frac{p}{q} \right| < \frac{1}{(n+1)^q}$  con  $0 \leq p \leq n$ .

Notación: Si  $x \in \mathbb{R}$ ,  $(x) =$  parte entera,  $\{x\} =$  parte fraccionaria  $\in [0, 1[$ .

Tomé:  $\{0\}, \{x\}, \{2x\}, \dots, \{nx\}, 1 \in [0, 1[$

existen tres posibilidades:

$$1) |\{i\alpha\} - \{j\alpha\}| \leq \frac{1}{n+1}, 2) |\{i\alpha\} - 1| \leq \frac{1}{n+1}, 3) |\{i\alpha\} - 0| \leq \frac{1}{n+1}$$

$$1) |\{i\alpha\} - \{j\alpha\}| \leq \frac{1}{n+1} \Rightarrow |\alpha - \frac{p}{q}| \leq \frac{1}{(n+1)^q}.$$

$$2) |\{i\alpha\} - 1| \leq \frac{1}{n+1} \Rightarrow |\alpha - \frac{p}{q}| \leq \frac{1}{(n+1)^q}.$$

$$3) |\{i\alpha\}| \leq \frac{1}{n+1} \Rightarrow |\alpha - \frac{p}{q}| \leq \frac{1}{(n+1)^q}.$$

Corolario: Existen infinitos pares  $(p, q)$  enteros con  $|\alpha - \frac{p}{q}| \leq \frac{1}{q^2}$ .

Si  $d = \sqrt{d}$ .

Existen infinitos pares tales que:  $|\sqrt{d} - \frac{p}{q}| \leq \frac{1}{q^2}$   
pero si  $\frac{1}{q} < \sqrt{d}$ . (se cumple de donde  $q > \sqrt{d}$ ).  $|\frac{f\sqrt{d}}{q} - p| \leq \frac{1}{q}$

$$|p| \leq |\frac{f\sqrt{d}}{q}| + |\frac{f\sqrt{d}}{q} - p| \leq |\frac{f\sqrt{d}}{q}| + 1.$$
$$\leq \frac{1}{q} + 1.$$

$$|p^2 - f^2 d| \leq |p - q\sqrt{d}| |p + q\sqrt{d}| \leq \frac{1}{q} (2q\sqrt{d} + 1) \leq 2\sqrt{d} + \frac{1}{q} \leq 2\sqrt{d} + 1.$$

Hay un no finito de posibles valores de  $p^2 - f^2 d$ , luego para algún  $u$ :  
 $p^2 - f^2 d = u$ ; para infinitos valores de  $p$  y  $f$ .

Veamos:  $p + f\sqrt{d} \in \mathbb{Z}(\sqrt{d})$ .

$$\frac{p + f\sqrt{d}}{n} \in \frac{\mathbb{Z}(\sqrt{d})}{n} \cong \frac{\mathbb{Z}}{(n)} \oplus \frac{\mathbb{Z}}{(n)}\sqrt{d}, \text{ finito}$$

existen pares:  $(p, f)$ ,  $(p', f')$  tales que  
 $p \equiv p' \pmod{n}$  en otras palabras  $p + f\sqrt{d} \equiv p' + f'\sqrt{d} \pmod{n}$   
 $f \equiv f' \pmod{n}$ .

quedan los:  $h = \frac{p' + f'\sqrt{d}}{p + f\sqrt{d}} \in \mathbb{Q}(\sqrt{d})^*$  y  $N(h) = 1 = \frac{n}{n}$

$$\text{pero: } \frac{p' + f'\sqrt{d}}{p + f\sqrt{d}} = \frac{(p' + f'\sqrt{d})(p - f\sqrt{d})}{(p + f\sqrt{d})(p - f\sqrt{d})} = \frac{(p' + f'\sqrt{d})(p - f\sqrt{d})}{n}$$

$$\text{pero: } (p' + f'\sqrt{d})(p - f\sqrt{d}) \equiv (p + f\sqrt{d})(p - f\sqrt{d}) \pmod{n}$$

$$\equiv h(n) \equiv 0(n)$$

$$\therefore \frac{p' + f'\sqrt{d}}{p + f\sqrt{d}} \in \mathbb{Z}(\sqrt{d})^* \subseteq \mathbb{O}_k^*$$

Como sabemos si  $a+b\sqrt{d}, -a+b\sqrt{d}, a-b\sqrt{d}, -a-b\sqrt{d}$  son unidades es si

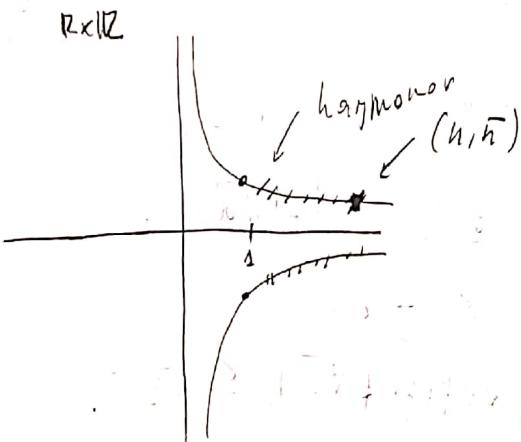
olganales.

Tomé  $u = a+b\sqrt{d}$ ,  $a, b > 0$ ,  $u > 1$ .

Recordemos que  $\mathbb{Q}(\sqrt{d}) \hookrightarrow \mathbb{R} \times \mathbb{R}$ ,  $\sqrt{d} \mapsto (\sqrt{d}, -\sqrt{d})$ .

con  $N(x,y) = N(x)N(y)$ .

Dectrode  $\mathbb{R} \times \mathbb{R}$ :



$$k = \mathcal{O}(\sqrt{a})$$

$$\Omega_k^* = \{ \lambda \in \mathbb{R} : \lambda > 0 \}$$

$$h = a + b\sqrt{a} \quad h \mapsto (h, \bar{h})$$

$$\bar{h} = a - b\sqrt{a}$$

$$\text{y como } h\bar{h} = \pm 1.$$

$(h, \bar{h})$  está en una de las hipérbolas.

pero  $\Omega_k^*$  es rectificado:  $\Omega_k = \mathbb{Z} \oplus \mathbb{Z}(\sqrt{a})$ .

Como se trata de un rectificado,  $\mathbb{Z} \oplus \mathbb{Z}(\frac{1+\sqrt{a}}{2})$ .

al restringirlo a  $\mathbb{N}_{\geq 1}$ , tam no finito de puntos, luego existe un mínimo. (que pueden ser dos si  $(h_1, h_2), (h_1, h_3)$  son mínimos en la coord.  $x$  ( $\Rightarrow h_2 = \bar{h}_1 = h_3$ )).

Sea  $\lambda \in \Omega_k^*$ ,  $\lambda = a + b\sqrt{a}$ ;  $N(\lambda) = \pm 1$ .

$$\{a + b\sqrt{a}, a - b\sqrt{a}, -a + b\sqrt{a}, -a - b\sqrt{a}\} = \{\lambda, -\lambda, \lambda^{-1}, -\lambda^{-1}\}.$$

podemos suponer,  $\lambda > 1$  (salvo cambiar por inverso).

en particular  $\lambda > h$ .

Como  $h > 1$ ,  $h^n \xrightarrow[h \rightarrow \infty]{} \infty$

Así existe  $n$  tal que:  $h^n \leq \lambda < h^{n+1}$   
 $1 \leq \lambda h^{-n} < h$ , no se puede dar más  $h$  minimal.

$$\therefore 1 = \lambda h^{-n}$$

$$\therefore \lambda = h^n$$

Obs:  $N(\pm h^r) = N(h)^r$

Si  $N(h) = 1 \Rightarrow N(h) = 1, \forall n \in \Omega_k^*$ .

Si  $N(h) = -1 \Rightarrow N(h) \in \{\pm 1\}, \forall n \in \Omega_k^*$ .

Suposiciones  $d \equiv 2, 3, (4)$

$$\mathcal{O}_K = \mathbb{Z}(\sqrt{d}).$$

$\mathcal{O}_K$  tiene unidad de norma  $-1$  si  $x^2 - dy^2 = -1$   
tiene soluciones enteras (no siempre)  
pero:  $x^2 - dy^2 = 1$  siempre tiene solución.

Ejemplo: 1)  $\mathbb{Z}(\sqrt{2})$ , tome  $u = 1 + \sqrt{2}$ .

$$N(1 + \sqrt{2}) = -1.$$

$(1 + \sqrt{2})$  es menor sol (unidad fundamental).

2)  $\mathbb{Z}(\sqrt{3})$ : Sol de  $x^2 - 3y^2 = -1$ .  
 $x^2 - 3y^2 = 1$ .

$2 + \sqrt{3}$  unidad fundamental.  $\Rightarrow N(u) = 1$ ,  $u \in \mathbb{Z}(\sqrt{3})^*$ .  
 $1 + \sqrt{3}$  no es unidad.

$\therefore x^2 - 3y^2 = -1$  no tiene solución entera

3) Queremos encontrar soluciones de  $4x^2 - 3y^2 = 1$ .

$4x^2 - 3y^2 = 1 = (2x)^2 - 3y^2 = 1$  (caso anterior, con coord. par).

$$5x^2 - 3y^2 = 2. \quad / \cdot 5$$

$$(5x)^2 - 15y^2 = 10$$

$$N(5x - y\sqrt{15}) = 10.$$

## Valores absolutos.

En un anillo  $K$  . . .  $f: K \rightarrow \mathbb{R}_{\geq 0}$  tal que:

$$1) f(0) = 0 \text{ si } a = 0$$

$$2) f(a \cdot b) = f(a) \cdot f(b)$$

$$3) f(a+b) \geq f(a) + f(b)$$

Ejemplo:

$$1) \text{ Si } K = \mathbb{R}, |a| = \begin{cases} a, & a > 0 \\ -a, & a < 0 \end{cases}$$

$$2) \text{ Si } K = \mathbb{C}, |z| = \sqrt{x^2 + y^2} \text{ si } z = x + iy.$$

$$3) \text{ Sea } p \in \mathbb{Z}, \text{ primo.}$$

$$N_p(n) = t \text{ si } p^t | n \text{ pero } p^{t+1} \nmid n.$$

$$V_p\left(\frac{m}{n}\right) = N_p(m) - N_p(n), m, n \neq 0.$$

Está bien definido pues si

$$\frac{m}{n} = \frac{r}{s} \Leftrightarrow ms = nr.$$

$$\text{Por lo tanto: } V_p(ms) = V_p(nr)$$

$$N_p(m) + V_p(s) = N_p(n) + V_p(r)$$

$$\text{Así: } N_p\left(\frac{m}{n}\right) = N_p(m) - N_p(n) = V_p(r) - V_p(s) = V_p\left(\frac{r}{s}\right).$$

Def: Si  $r \in \mathbb{Q}: |r|_p = p^{-V_p(r)}, |0|_p = 0.$

Es valor absoluto pues:

$$2) \text{ Si: } N_p\left(\frac{mr}{ns}\right) = N_p(m) + V_p(r) - V_p(n) - V_p(s) = N_p\left(\frac{m}{n}\right) + V_p\left(\frac{r}{s}\right)$$

$$\text{Así: } \left|\frac{mr}{ns}\right|_p = p^{-V_p\left(\frac{m}{n}\right) - V_p\left(\frac{r}{s}\right)} = p^{-V_p\left(\frac{m}{n}\right)} \cdot p^{-V_p\left(\frac{r}{s}\right)} = \left|\frac{m}{n}\right|_p \left|\frac{r}{s}\right|_p.$$

Proposición: Si  $\frac{m}{n}, \frac{r}{s} \in \mathbb{Q}$  entonces:

$$N_p\left(\frac{m+r}{n+s}\right) \geq \min\{N_p\left(\frac{m}{n}\right), V_p\left(\frac{r}{s}\right)\}.$$

$$\text{Lo puedes decir así: } \left(\frac{m+r}{n+s}\right)_p \leq \max\left\{\left|\frac{m}{n}\right|_p, \left|\frac{r}{s}\right|_p\right\} \leq \left|\frac{m}{n}\right|_p + \left|\frac{r}{s}\right|_p.$$

Caso I: Para enteros ( $h=s=1$ )

$$v_p(m+r) \geq \min \left\{ \frac{v_p(m)}{t}, \frac{v_p(r)}{n} \right\}.$$

$$m = p^t m_0, r = p^n r_0, t \leq n$$

$$\text{entonces: } m+n = p^t (m_0 + p^{n-t} r_0) \quad \therefore v_p(m+r) \geq t = \min \{ v_p(m), v_p(r) \}$$

Caso II:  $\frac{m}{n} + \frac{r}{s} = \frac{ms+nr}{ns}$ .

$$v_p\left(\frac{ms+nr}{ns}\right) = v_p(ms+nr) - v_p(ns)$$

$$\geq \min \{ v_p(ms), v_p(nr) \} - v_p(ns)$$

$$\geq \min \{ v_p(ms) - v_p(ns), v_p(nr) - v_p(ns) \}$$

$$\geq \min \{ v_p\left(\frac{m}{n}\right), v_p\left(\frac{r}{s}\right) \}.$$

( $K, p$  tienen con valor absoluto).

Definición:  $\{a_n\}_{n \in \mathbb{N}} \in K$  diremos que  $a_n$  converge a  $a \in K$  si

$$\text{si } p(a_n - a) \xrightarrow[n \rightarrow \infty]{} 0$$

Ejemplo:  $a_n = 1 + p + \dots + p^n$  converge a  $a = \frac{1}{1-p}$ .

$$a_n = \frac{p^{n+1} - 1}{p - 1}$$

$$a_n - a = \frac{p^{n+1}}{p-1}$$

$$|a_n - a| = \frac{|p|_p^{n+1}}{|(p-1)|_p} = \frac{\left(\frac{1}{p}\right)^{n+1}}{1} \xrightarrow{n \rightarrow \infty} 0.$$

$$\therefore a_n = 1 + p + \dots + p^n \xrightarrow{n \rightarrow \infty} \frac{1}{1-p}.$$

$$\left\{ \left( \frac{1}{2} \right)^n, \left( \frac{1}{3} \right)^n, \left( \frac{1}{4} \right)^n \right\} \text{ son conjuntos de límites}$$

$$\left\{ \left( \frac{1}{2} \right)^n, \left( \frac{1}{3} \right)^n, \left( \frac{1}{4} \right)^n, \dots \right\} \text{ son conjuntos de límites}$$

## Sucesiones de Cauchy:

{ $a_n$ }  $\in \mathbb{N}$  se dice de Cauchy si:

$$\forall \varepsilon > 0 \exists N \in \mathbb{N} : n, m > N \Rightarrow f(a_n - a_m) < \varepsilon.$$

Toda sucesión convergente es de Cauchy:

Dem: Si { $a_n$ }  $\in \mathbb{N}$ ,  $a_n \rightarrow a$   $\exists N \geq 1$  tal que  $n > N \Rightarrow f(a_n - a) < \varepsilon/2$ .  
 $\forall m > N \Rightarrow f(a_n - a) < \varepsilon/2 \Rightarrow f(a_n - a_m) \leq f(a_n - a) + f(a - a_m) < \varepsilon/2$ .

Def:  $K$  se dice completo si toda sucesión de Cauchy converge.

Hecho: Todo cuerpo con valor absoluto se puede "completar".  
(pd:  $\tilde{K}$ -cuerpo).

Def:  $\mathbb{K}_p$  se define como el complemento de  $\mathbb{K}$  con respecto a  $\mathbb{K}_p$ .

$\mathbb{K}_p = \text{cls}_{\mathbb{K}_p}(\mathbb{K})$ . (Closura topológica). ( $\mathbb{K} \subseteq \mathbb{K}_p \subseteq \mathbb{K}_p$ )

Prop:  $\mathbb{K}_p$  es un anillo.

Sean  $a, b \in \mathbb{K}_p \Rightarrow a_n \rightarrow a, b_n \rightarrow b$ ,  $a, b \in \mathbb{K}$ ,  $f(a_n - a) \xrightarrow{n \rightarrow \infty} 0$ ,  $f(b_n - b) \xrightarrow{n \rightarrow \infty} 0$ .

entonces:

Dem: ¿Los mapas el producto son continuos.

$$\text{Si } a_n \rightarrow a, b_n \rightarrow b \Rightarrow a_n + b_n \rightarrow a + b \quad \text{y} \quad a_n b_n \rightarrow a b.$$

$$0 \leq f(a + b - a_n - b_n) \leq f(a - a_n) + f(b - b_n) \rightarrow 0 \quad \therefore a_n + b_n \rightarrow a + b.$$

$$\begin{aligned} 0 &\leq f(a b - a_n b_n) = f(a b - a_n b + a_n b - a_n b_n) \leq f(b) f(a - a_n) + f(a_n) f(b - b_n) \\ &\leq f(b) f(a - a_n) + (f(a) + f(a_n - a)) f(b - b_n) \rightarrow 0. \end{aligned}$$

$$\therefore a_n b_n \rightarrow a b.$$

$$\text{Si } a_n, b_n \in \mathbb{Z}_p : \begin{array}{l} a_n + b_n \in \mathbb{Z}_p \text{ y } a_n + b_n \rightarrow a+b \\ a_n b_n \in \mathbb{Z}_p \text{ y } a_n b_n \rightarrow ab \end{array}$$

$$\therefore a+b, ab \in \mathbb{Z}_p$$

Proposición: Si  $p+n$  entonces  $\frac{1}{n} \in \mathbb{Z}_p$ .

Dem: Si  $p+n \Rightarrow \bar{n} \in (\mathbb{Z}/p\mathbb{Z})^*$ ,  $\forall t \in \mathbb{Z}_{>0}$ .

Asi  $\exists a_t \in \mathbb{Z} : n a_t \equiv 1 \pmod{p}$ , con  $a_t$  único módulo  $p$ .

$$\text{Si } r > t \Rightarrow a_r \equiv a_t \pmod{p}$$

$$a_r - a_t = p^t b_{r,t} \quad p | b_{r,t} \quad \text{pues } |b_{r,t}|_p = p^{-v_p(b)} \leq 1.$$

$\therefore \{a_t\}_t$  es Cauchy  $\Rightarrow a_t$  converge en  $\mathbb{K}_p$ .

$$n a_t \equiv 1 \pmod{p} \Rightarrow |n a_t - 1| = p^{-t} \xrightarrow[t \rightarrow \infty]{} 0$$

$\therefore a_t \xrightarrow[t \rightarrow \infty]{} 1$ .   
  $\therefore a_t \xrightarrow[t \rightarrow \infty]{} 1$  y como  $a_t \in \mathbb{Z} \Rightarrow \frac{1}{n} \in \mathbb{Z}_p$ . (el límite está en la clausura).

Si  $\frac{h}{m} \in \mathbb{K}_p$ ,  $\frac{h}{m} = p_1^{x_1} \cdots p_r^{x_r} a \in \mathbb{Z}$ .

$$p = p_1 \quad \left| \frac{h}{m} \right|_p = p^{-|a|}$$

$$\left| \frac{h}{m} \right|_p \leq 1 \text{ si } p \nmid m$$

Corolario:

Si  $a \in \mathbb{K}$   $\} \Rightarrow a \in \mathbb{Z}_p$  pues  $a = \frac{n}{m} \in \mathbb{Z}_p$ .

$$|a|_p \leq 1 \quad a = \frac{1}{m} \cdot n \in \mathbb{Z}_p$$

$$\left( \frac{1}{m} \right)_p \leq 1 \quad \left( \frac{1}{m} \right)_p = \frac{1}{m} \in \mathbb{Z}_p$$

Sig a  $a \in \mathbb{K}_p$ ,  $|a|_p \leq 1$ .

entonces existe  $a_n \rightarrow a$  ( $a_n \in \mathbb{K}$ ,  $a_n \in \mathbb{K}$ ) y  $a_n$  alg.

Afirmación:  $|a_n|_p \leq 1$ ,  $n \gg 1$ ,  $a_n \in K$

Luego:  $a_n \in \mathbb{Z}_p$ ,  $n \gg 1 \Rightarrow a \in \mathbb{Z}_p$ .

✓.  $\therefore \mathbb{Z}_p = \{a \in \mathbb{K}_p \mid |a|_p \leq 1\}$ .

Lema: (principio de dominancia)

Sea  $K$  un cuerpo que satisface la desigualdad triangular fuerte.

Si  $f(x) < f(y)$  entonces:  $|f(x+y)| = f(y)$ .

Demostración:  $f(x+y) \leq \max \{f(x), f(y)\} = f(y)$

Si  $f(x+y) < f(y)$  entonces:  $f(y) \leq \max \{f(-x), f(x+y)\}$   
 $= \max \{f(x), f(x+y)\} < f(y)$  ( $\neq$ )

$\therefore f(x+y) = f(y)$ .

Ejercicio: Si  $x_1, \dots, x_n \in K$  y  $f(x_i) < f(x_1) \quad \forall i \in \{2, \dots, n\}$

entonces:  $f(x_1 + \dots + x_n) = f(x_1)$

Lema:  $K$  satisface des. triangular fuerte.

$f(a_n + b_n) \leq \max \{f(a_n), f(b_n)\}$ .

Aplicando límite:  $f(a+b) \leq \max \{f(a), f(b)\}$ .

Dem: Si  $a_n \rightarrow a \Rightarrow f(a_n - a) \rightarrow 0$ , si  $|a_n|_p > 1$ ,  $|a|_p \leq 1$

entonces:  $|a_n - a|_p = |a_n|_p > 1$  ( $\neq$ )

Sea  $p \in \mathbb{Z}_p$ . <sup>primos en  $\mathbb{Z}$</sup>

Afirmación:  $p\mathbb{Z}_p$  ideal de  $\mathbb{Z}_p$ .

$$\begin{cases} p \notin \mathbb{Z}_p^* \\ \text{mas } (\frac{1}{p})_p = 1 \\ \Rightarrow \frac{1}{p} \notin \mathbb{Z}_p \end{cases}$$

$$\mathbb{Z} \hookrightarrow \mathbb{Z}, \hookrightarrow \mathbb{Z}/p\mathbb{Z}$$

$\mathbb{Z}_p/\mathbb{Z}_p$ .

Tenemos una función bien definida:

$$\mathbb{Z}/p\mathbb{Z} \xrightarrow{\Psi} \mathbb{Z}/p\mathbb{Z}$$

están

Si:  $p+n, \frac{1}{n} \in \mathbb{Z}_p^* \Rightarrow \frac{1}{n} \not\equiv 0 \pmod{p\mathbb{Z}_p} \quad | \quad n \equiv 0 \pmod{p\mathbb{Z}_p}$ .

$\therefore \text{Ker } \Psi = \{0\} \therefore \text{inyectiva}$

Sea  $\bar{a} \in \mathbb{Z}/p\mathbb{Z}$ ,  $a_n \in \mathbb{Z}$  con  $|a_n - a|_p < \frac{1}{p}$ .

Sea  $b = \frac{a_n - a}{p} \in \mathbb{Z}_p$ .

$$|b| = \frac{|a_n - a|_p}{|p|_p} \cdot \frac{|H_p|}{|H_p|} = 1 \Rightarrow b \in \mathbb{Z}_p.$$

$$a_n - a = pb$$

$$a_n \equiv a \pmod{p\mathbb{Z}_p} \quad \therefore \bar{a}_n = \bar{a}.$$

$\therefore \mathbb{Z}_p/\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$ . (Anillo)  $\rightarrow p\mathbb{Z}_p$  es ideal de  $\mathbb{Z}_p$ .

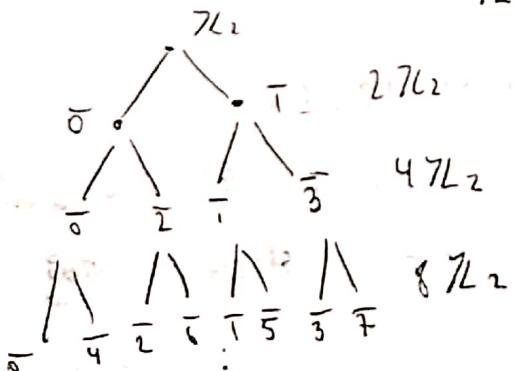
Ejercicio: Por el mismo argumento, probar que:  $\mathbb{Z}/p^t\mathbb{Z}_p \cong \mathbb{Z}/p^t\mathbb{Z}$ .

para  $p=2$

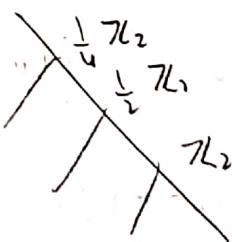
$\mathbb{Z}_2$

$$\mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}_2/\mathbb{Z} \cong \{0, 1\}$$

$$\mathbb{Z}_2 = (2\mathbb{Z}_2) \cup (2\mathbb{Z}_2 + 1)$$



$\mathbb{Z}_2$  "Conjunto de Caminos"



$$\mathbb{Z}/p^t \mathbb{Z} \cong \mathbb{Z}/p^t \mathbb{Z}.$$

Dem:  $\mathbb{Z} \hookrightarrow \mathbb{Z}/p^t \mathbb{Z} \hookrightarrow \mathbb{Z}/p^t \mathbb{Z}/p^t \mathbb{Z} \quad | \quad \mathbb{Z}/p^t \mathbb{Z} \hookrightarrow \mathbb{Z} \hookrightarrow \mathbb{Z}/p^t \mathbb{Z}$ .  
 $\mathbb{Z}/p^t \mathbb{Z} \xrightarrow{\Psi} \mathbb{Z}/p^t \mathbb{Z}$ ,  $\Psi$  bien definida.

Primero demostremos que  $\Psi$  inyectiva.

Lema: Si  $p^t + h$  enton  $\Leftrightarrow \frac{1}{n} \in \mathbb{Z}/p^t \mathbb{Z}$ .

Dem: Si  $p^t + h \Rightarrow \frac{1}{n} \in (\mathbb{Z}/p^t \mathbb{Z})^*$

$$\Rightarrow n \cdot a_n \equiv 1(p^n), a_n \text{ unico modulo } p^n.$$

luego si  $n > u$ :  $a_n \equiv a_n(p^n) \Rightarrow |a_n - a_u|_p < p^{-u}$

$\therefore \{a_n\}_{n \in \mathbb{N}}$  es de Cauchy.

$\therefore \{a_n\}_{n \in \mathbb{N}}$  es de Cauchy.

$$\therefore |1 - n a_n| < p^{-u} \Rightarrow \lim_{n \rightarrow \infty} n a_n = 1 \Rightarrow a_u \xrightarrow[n \rightarrow \infty]{} \frac{1}{n} \text{ y } a_u \in \mathbb{Z}$$

$\therefore \frac{1}{n} \in \mathbb{Z}/p^t \mathbb{Z}$  y  $\in \text{inv} \text{ pues } n \in \mathbb{Z}/p^t \mathbb{Z}$ .

$$\therefore \frac{1}{n} \in (\mathbb{Z}/p^t \mathbb{Z})^* \Rightarrow n \in (\mathbb{Z}/p^t \mathbb{Z})^*$$

$$\rightarrow n \neq 0 \text{ (mud } p^t \mathbb{Z}) \quad \therefore \text{ker } \Psi = \{0\}.$$

Escribimos: Sea  $\bar{a} \in \frac{\mathbb{Z}}{p^t \mathbb{Z}} \Rightarrow a \in \mathbb{Z}/p^t \mathbb{Z} \Rightarrow \exists a_n \in \mathbb{Z}: a_n \xrightarrow[n \rightarrow \infty]{} a$ .

$$\therefore |a_n - a|_p < \frac{1}{p^t} \text{ cierto } n \in \mathbb{N}.$$

$$\text{Sea } b = \frac{a_n - a}{p^t} \in \mathbb{W}/p^t \mathbb{W}$$

$$\text{as: } |b| = \frac{|a_n - a|}{|p^t|} < \frac{1/p^t}{1/p^t} = 1. \quad \therefore b \in \mathbb{Z}/p^t \mathbb{Z}.$$

$$\text{y } a_n - a \equiv 0 \pmod{p^t \mathbb{Z}}$$

$$a_n \equiv a \pmod{p^t \mathbb{Z}}$$

$$\therefore \exists a_n \in \mathbb{Z} \text{ tal que: } \bar{a}_n = \bar{a}.$$

$$\therefore \mathbb{Z}/p^t \mathbb{Z} \cong \mathbb{Z}/p^t \mathbb{Z}.$$

soc. constante:

bien de pares  $\in \mathbb{Z} \hookrightarrow \mathbb{Z}_p$ .

pd:  $\mathbb{Z}_p$  es ideal de  $\mathbb{Z}_p$ .  $P$  permite en  $\mathbb{Z}$ .

Sea  $a, b \in P \subset \mathbb{Z}_p \Rightarrow$  Janibn:  $\begin{array}{l} a \mapsto a \\ b \mapsto b \end{array}$

$$\therefore P(a_n + b_n) \rightarrow P(x \pm b), a_n + b_n \in \mathbb{Z}$$

$$\therefore P a_n \cdot P b_n \rightarrow P^2(ab), a_n b_n \in \mathbb{Z}$$

$\therefore P \mathbb{Z}_p$  subanillo de  $\mathbb{Z}_p$ .

Sea  $c \in P \Rightarrow \exists c_n \in \mathbb{Z}: c_n \mapsto c$

$$\therefore P(a_n c_n) \rightarrow P(xc), a_n c_n \in \mathbb{Z}$$

$\therefore P \mathbb{Z}_p$  ideal de  $\mathbb{Z}_p$ .

$\mathbb{Q}_p$  es anillo:  $\mathbb{Q}_p \subseteq \mathbb{Z}_p \Rightarrow$   $\mathbb{Q}_p$  es ideal de  $\mathbb{Z}_p$ .

$\mathbb{Z}_p$  tiene solo ideales triviales.

$\mathbb{Z}_p$  es anillo.

$$\begin{aligned}\ker \varphi &= \left\{ c+id \mid n | (c+id)(x+bi) \right\} \quad , \quad n = (a+bi)(a-bi) \\ &= \left\{ c+di \mid (x+ib)(x-bi) \mid (c+id)(x+ib) \right\} \\ &= \left( x-ib \right) \quad \text{Se } A = \frac{\mathbb{Z}(i)}{(n)}\end{aligned}$$

$$\begin{aligned}\therefore \left| \frac{\mathbb{Z}(i)}{(n)} \right| &= |A| = \left| \frac{A}{\text{Im } \varphi} \right| \cdot |\text{Im } \varphi| \\ &= \left| \frac{\mathbb{Z}(i)/(n)}{(x+bi)(b)} \right| \cdot |\text{Im } \varphi| \\ &= \left| \frac{\mathbb{Z}(i)}{(x+ib)} \right| \cdot |\text{Im } \varphi| \quad \text{Im } \varphi \cong \mathbb{Z}(i)/\ker \varphi \\ h^2 &= \left| \frac{\mathbb{Z}(i)}{(x+ib)} \right| \cdot \left| \frac{\mathbb{Z}(i)}{(x-bi)} \right| = \left| \frac{\mathbb{Z}(i)}{(x+ib)} \right|^2 \\ \therefore h &= \left| \frac{\mathbb{Z}(i)}{(x+ib)} \right|.\end{aligned}$$

- Problema:  $\bar{n} \subseteq \partial K$ ,  $[K : \mathbb{Q}] = 2$   
 $\bar{n} = \mathbb{Z} + h \partial K$ ,  $\bar{n}$   $\mathbb{Z}$ -módulo de rango 2.

Demo::  $\pi: K \rightarrow K/\mathbb{Q} \cong \mathbb{Q}$  Cerrado grupo abeliano  
 $\pi(h) = h \pi(\partial K)$ .

$$\begin{aligned}\text{Problema}: \quad B &= \frac{\mathbb{Z}(x, x^{-1})}{(x - 2x^{-1})} \cong \frac{\mathbb{Z}(x, x^{-1})}{(x^2 - 2)} \cong \frac{\mathbb{Z}(x)}{(x^2 - 2)} [x^{-1}] \\ &\cong \mathbb{Z}(\sqrt{2}) [(N_1)^{-1}] \quad \text{localizado de un DFU, es DFU.}\end{aligned}$$

$\therefore B \in \text{DFU.}$

Lema: Todo localización de un DFU es DFU.

Encuentre los primos p de  $\mathbb{Z}(w)$

$$\frac{\mathbb{Z}(w)}{(p)} \cong \frac{\mathbb{Z}(x)}{(x^2+x+1, p)} \cong \frac{\mathbb{F}_p[x]}{(x^2+x+1)} \quad \text{DI sc., } x^2+x+1 \text{ no tiene raíces.}$$

$$\frac{\mathbb{F}_2[x]}{(x^2+x+1)} \cong \mathbb{F}_4 \Rightarrow 2 \text{ es primo.} \\ \text{Si } p \neq 2, \quad x = \frac{-1 \pm \sqrt{-7}}{2} \quad \therefore p \text{ no es cuadrado.}$$

$$\left(\frac{-3}{p}\right) = -1, \quad p \equiv 1(4), \quad p \equiv -1(4)$$

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = 1, \quad p \equiv 1(4) \Rightarrow p \equiv 1( \text{mod } 3).$$

$$\left(\frac{-3}{p}\right) \equiv +\left(\frac{p}{3}\right), \quad \left(\frac{p}{3}\right) = -1 \Rightarrow p \equiv 2( \text{mod } 3).$$

Lema: Si  $A \cong A_1 \times A_2$ ,  $I \subseteq A$ ,  $I_1 \subseteq A_1$ ,  $I_2 \subseteq A_2$  ideales correspondientes a  $I$   
 $\Rightarrow \frac{I}{I} \cong \frac{A_1}{I_1} \times \frac{A_2}{I_2}$ .

Problema:  $3x^2 - 7y^2 = 60$  encontrar sus soluciones enteras. (infinitas)

$$3x^2 - 7y^2 = 60$$

$$N(3x - y\sqrt{21}) = 60 \text{ en } \mathbb{Z}(\sqrt{21}).$$

$$N(6 - \sqrt{21}) = 60 \text{ en } \mathbb{Z}(\sqrt{21}).$$

$$(6 - \sqrt{21})(2 + b\sqrt{21}) \in [0, 60] \text{ normal}$$

$$x^2 - 7y^2 = 7 \text{ enteras.} \quad \mathbb{Z}(\sqrt{2}) \in \text{DIP.}$$

$$N(x - y\sqrt{2}) = 7$$

$$\therefore x = 3 \quad \text{o} \quad x = 3 \\ y = -1 \quad \quad \quad y = 1$$

$$7 = (3 - \sqrt{2})(3 + \sqrt{2})$$

$$\text{todas las soluciones} = \left\{ \begin{array}{l} (3 - \sqrt{2})h_1 \\ (3 + \sqrt{2})h_1 \end{array} \right\}, \quad h_1, h_1' = \pm h_0, h_0 = 14\sqrt{2}.$$

Problema: Encuentre todas las soluciones de  $x^2 + y^2 = 20$ .

$$(x+iy)(x-iy) = 20 = 2^2 \cdot 5 \\ = -(1+i)^4 (2+i)(2-i)$$

$$(x+iy) = (2+i)(1+i)^2 \\ (x-iy) = (2-i)(1-i)^2$$

Si tenemos:  $x^2 + y^2 = 65$

$$(x+iy)(x-iy) = (2+i)(2-i)(3+2i)(3-2i)$$

$$x+iy = (2+i)(3+2i) \quad x+iy = (2+i)(3-2i) \\ = (4+7i) \quad = (8-i)$$

Problema: Encuentre las soluciones enteras de

$$x^2 + 2y^2 = 49$$

Demo: Como sabemos,  $\mathbb{Z}(\sqrt{-2})$  es D. Euclídeo  $\Rightarrow \mathbb{Z}(\sqrt{-2})$  es D.F.U.

$$(x-\sqrt{-2}y)(x+\sqrt{-2}y) = 49 = 7^2$$

Pero en  $\mathbb{Z}(\sqrt{-2})$ :  $7 \in \mathbb{Z}$  irreducible pues

$$7 = \alpha\beta \Rightarrow N(\alpha\beta) = N(\alpha)N(\beta)$$

$\therefore N(\alpha) \in \{1, 7, 49\} \Rightarrow$  Si  $N(\alpha) = 7 \Rightarrow x^2 + 2y^2 \Rightarrow x$  impar  $\Rightarrow x=1 \therefore b=2y^2 (\#)$ .

$\therefore \alpha \in \mathbb{Z}(\sqrt{-2})^* \text{ o } \beta \in \mathbb{Z}(\sqrt{-2})^*$ .

Luego:  $x - \sqrt{-2}y = 7 \Rightarrow \begin{cases} x = 7 \\ y = 0 \end{cases}$  Es la única solución!

Problema: Demuestre que la ecuación  $x^2 + 2y^2 = \pm 3$  tiene infinitas soluciones.

Esto es equivalente a:  $N(x + \sqrt{-2}y) = (x - \sqrt{-2}y)(x + \sqrt{-2}y) = \pm 3$  (no irred):

Pero  $\mathbb{Z}(\sqrt{-2}) \in SDE \Rightarrow \mathbb{Z}(\sqrt{-2})^* \in DFU$ :

$\therefore 4 - 3\sqrt{-2} \in S$  solución,  $4 + 3\sqrt{-2}$  es solución -

Como  $(1+\sqrt{2})$  es unida al fundamental, las sol. son:

$$(1+\sqrt{2})^{2n}(4-3\sqrt{-2}), n \in \mathbb{Z}, n \neq 0$$

$\therefore$  Hay infinitas soluciones.

- Problemas :
- 1) ¿Es  $\mathbb{Z}(\sqrt{3})$  D.Euclídea? ✓
  - 2) ¿Cómo son los primos en  $\mathbb{Z}(\sqrt{3})$ ? 2i) Unidades.
  - 3) - ¿Cuáles son las soluciones de  $x^2 + xy + y^2 = z^2$ ? ✓
    - Los elementos p primos  $p = x^2 + xy + y^2$  ✓
    - Los enteros n =  $x^2 + xy + y^2$ . ✓
  - 4) Encuentre las soluciones de  $13 \cdot 5 \cdot 4 = x^2 + y^2$  enteras. ✓

Solución 4 : Queremos que:  $x^2 + y^2 = 13 \cdot 5 \cdot 4$

$$\text{D.F.T. } (x+iy)(x-iy) = \underbrace{(3+2i)(3-2i)}_{\text{irred}} \underbrace{(2+i)(2-i)}_{\text{unidad}} \underbrace{(1+i)^4}_{i^2}$$

Luego:

$$x+iy = (3+2i)(2-i)(1+i)^2 \quad \text{otro conjugado}$$

$$x+iy = (3+2i)(2+i)(1+i) \quad \text{y otro}$$

$$x+iy = 2i(8-i) = (16i+2)$$

$$x+iy = 2i(4+i) = (8i-14)$$

$$\therefore (x,y) \in \{(2,16), (-2,16), (16,-2), (-2,-16), (-16,-2), (-16,2), (2,-16), (14,2), (2,14), (-2,14), (14,-2), (-2,-14), (14,-2), (2,-14), (-14,2)\}$$

Solución 3 La norma:  $N(a+b\sqrt{3}) = |a^2 - 3b^2|$

$$\text{Sea } \alpha, \beta \in \mathbb{Z}(\sqrt{3}). \quad \alpha^{-1} \in \mathbb{Z}(\sqrt{3}), \quad \alpha^{-1} = s+t\sqrt{3}$$

entonces existen  $p, q \in \mathbb{Z}$ :  $|p-s| \leq \frac{1}{2}, |q-t| \leq \frac{1}{2}$ .

$$\text{Sea } \theta = p+q\sqrt{3}, \quad M = \beta((s-p)+(t-q)\sqrt{3}).$$

$$\text{entonces: } 1) \quad \beta\theta + M = \beta(p+q\sqrt{3}) + \beta((s-p)+(t-q)\sqrt{3}) = \beta(s+t\sqrt{3}) = d \quad (\text{d} \mid r = d).$$

$$2) \quad M \in \mathbb{Z}(\sqrt{3}) \quad \Rightarrow \quad 0 \leq (t-q)^2 \leq \frac{1}{4}, \quad \frac{3}{4} \leq 3(t-q)^2 \leq 0 \quad \forall t, q \in \mathbb{Z}$$

$$\text{todas las raíces de } N(M) = N(M)((s-p)^2 + 3(t-q)^2) \leq \frac{1}{4}N(\beta)$$

$\therefore \mathbb{Z}(\sqrt{3})$  es D euclídeo.

2) Los primos en  $\mathbb{Z}(\sqrt{3})$

Sea  $p \in \mathbb{Z}$  primo, este es primo en  $\mathbb{Z}(\sqrt{3})$  si

$$\frac{\mathbb{Z}(\sqrt{3})}{(p)} \cong \frac{\mathbb{Z}(x)}{(p, x^2 - 3)} \cong \frac{\mathbb{F}_p[x]}{(x^2 - 3)} \in \text{D.E.}$$

$$\text{Esto es } \left(\frac{3}{p}\right) = -1.$$

$$\text{Pero: } \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = -1 \text{ si } p \equiv 2 \pmod{3}, p \neq 3.$$

2i) Unidades:  $a + b\sqrt{3} \in \mathbb{Z}(\sqrt{3})^*$  si  $a^2 - 3b^2 = \pm 1$ .  $a + b\sqrt{3} > 1$ .

- Encuentramos  $a + b\sqrt{3}$  mínimo tal que

$$\text{tome } 2 + \sqrt{3} > 1 \quad (2 - \sqrt{3})(2 + \sqrt{3}) = 4 - 3 = 1 \quad a + b\sqrt{3} > 1.$$

$b=0$  no,  $a=1$  no,  $a=0$  no.  $a^2 - 3b^2 = -1$  no tiene solución.

$$\therefore M = \left(2 + \sqrt{3}\right)^n \quad (\text{haga } N(u) = 1 \text{ si } a^2 - 3b^2 = -1)$$

3) i) Las soluciones de  $z^2 = x^2 + xy + y^2$ :  $z^2 = (x + (\frac{1+\sqrt{3}}{2})y)(x + (\frac{1-\sqrt{3}}{2})y)$

Con  $(x, y) = 1$ : D.F.U.  $= \pi \mid (x + (\frac{1-\sqrt{3}}{2})y), \pi \mid (x + (\frac{1+\sqrt{3}}{2})y)$

Si:  $\pi$  primo en  $\mathbb{Z}(\omega)$  es tal que

$$\pi \mid 2x+y, \pi \mid \sqrt{-3}y.$$

Como  $(x, y) = 1 \Rightarrow \exists s, t \in \mathbb{Z}: sx+ty=1$ .

$$\mathbb{Z}(\omega)^* = \left\{ \pm 1, \pm \frac{1+\sqrt{-3}}{2}, \pm \frac{1-\sqrt{-3}}{2} \right\}.$$

$$\pi \mid 2x + (\frac{1-\sqrt{-3}}{2})y$$

$$\pi \mid 2 = \underbrace{\left(1 - \frac{\sqrt{-3}}{2}\right)}_{u} \left(1 + \sqrt{-3}\right)$$

$$\pi \mid$$

$$\therefore \pi \mid 2\sqrt{-3}.$$

$$2\sqrt{-3} = \underbrace{\left(1 - \frac{\sqrt{-3}}{2}\right)}_2 \left(1 + \sqrt{-3}\right) \sqrt{-3} = 2(2w-1).$$

$$\text{irredssi } \frac{\mathbb{Z}(\omega)}{(2)} \cong \frac{\mathbb{F}_2[x]}{(x^2 + x + 1)} \text{ Cuest po } \checkmark$$

Pd: 2,  $2w-1$  irred en  $\mathbb{Z}(\omega)$ .

$$N(2) = 4, \text{ pero: } x^2 + xy + y^2 = 2$$

$$N(\sqrt{-3}) = N(2w-1) = 8-2+4 \in 3, \text{ primo} \Rightarrow 2w-1 \text{ irred.}$$

Lênhgo:  $\pi = 2w - 1$ .

$$\text{vì } \pi = 2: 21x + \left(\frac{1+\sqrt{3}}{2}\right)y$$

$$\therefore 2(a+b\left(\frac{1+\sqrt{3}}{2}\right)) = x + \left(\frac{1+\sqrt{3}}{2}\right)y$$

$$\Rightarrow \begin{cases} 2a = x \\ 2b = y \end{cases} \Rightarrow 21xy \quad (\text{*})$$

$$\therefore \pi = 2w - 1 \Leftrightarrow t(x+w\bar{y}, x+\bar{w}y) = 1.$$

Ánh ảnh, s:  $\rho \nmid 2 \Rightarrow \rho \nmid \frac{x+w\bar{y}}{\pi} \text{ và } \rho \nmid \frac{x+\bar{w}y}{\pi}$

$$\therefore \rho^2 \nmid \frac{x+w\bar{y}}{\pi}, \text{ s: } \rho \nmid 2^2$$

$$\therefore x+w\bar{y} = \frac{\pi}{\rho^2} \in \mathbb{Z}(\omega)$$

$$x+\bar{w}y = \frac{\pi}{\rho^2}$$

$$\text{s: } \pi = 2w - 1 \Leftrightarrow x + xy + y^2 = 3(\omega)^{12} \in 2^2 \Rightarrow 3 \nmid 2^2 \text{ và } \pi \nmid 2^2.$$

$$\therefore 3 \nmid x+w\bar{y} \Rightarrow 3 \nmid x, 3 \nmid y \quad (\text{*}).$$

Lênhgo  $\pi = 1$  (Unidiv). ASL:  $x + \left(\frac{1+\sqrt{3}}{2}\right)y = (c + (1+\sqrt{3})d)^2$

$$\begin{aligned} &= c^2 + (1+\sqrt{3})cd + \frac{1}{4}(-2+2\sqrt{-3})d^2 \\ &= c^2 + (1+\sqrt{3})cd - \frac{1}{2}(1-\sqrt{-3})d^2 \\ \therefore \begin{cases} x = c^2 - d^2 & (c, d \in \mathbb{Z}) \\ y = 2cd + d^2 \end{cases} \quad \pi = c^2 - d^2 + 2cd(1+\sqrt{3}) + d^2\left(1+\frac{\sqrt{-3}}{2}\right) \end{aligned}$$

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

$$4 - 2\sqrt{-3} = 4 - 2\sqrt{-3} = 4 - 2\sqrt{-3} =$$

$$4 - 2\sqrt{-3} = 4 - 2\sqrt{-3} = 4 - 2\sqrt{-3} =$$

$$4 - 2\sqrt{-3} = 4 - 2\sqrt{-3} = 4 - 2\sqrt{-3} =$$

$$4 - 2\sqrt{-3} = 4 - 2\sqrt{-3} = 4 - 2\sqrt{-3} =$$

$$4 - 2\sqrt{-3} = 4 - 2\sqrt{-3} = 4 - 2\sqrt{-3} =$$

$$4 - 2\sqrt{-3} = 4 - 2\sqrt{-3} = 4 - 2\sqrt{-3} =$$

$$4 - 2\sqrt{-3} = 4 - 2\sqrt{-3} = 4 - 2\sqrt{-3} =$$

$$4 - 2\sqrt{-3} = 4 - 2\sqrt{-3} = 4 - 2\sqrt{-3} =$$

$$4 - 2\sqrt{-3} = 4 - 2\sqrt{-3} = 4 - 2\sqrt{-3} =$$

4) En algunos casos tenemos  $f(a+b) \leq \max\{f(a), f(b)\}$   
(dos triángulos fuerte).

" $(K, p)$ "  $\Rightarrow$   $K$  se dice arquimediano si cumple 4) y no arquimediano en caso contrario.  
 $(\mathbb{R}, \mathbb{C}$  son arquimedianos)

Para cualquier anillo:  $\varphi: \mathbb{Z} \rightarrow A$

$$\begin{aligned} l_2 &\mapsto l_A \\ n &\mapsto l_A + \dots + l_A \end{aligned}$$

Se define:  $\mathbb{Z}_A = \varphi(\mathbb{Z})$ .

Lema: Si  $\mathbb{Z}_K \subseteq K$  es acotado por  $p$  entonces  $\mathbb{Z}_K \subseteq B[0_K; 1_K] = \{b \in K : |p(b)| \leq 1\}$

Demonstración: Sean  $n \in \mathbb{Z}_K \subseteq B[0_K, r]$

$$|p(n_K)|^t = |p(n_K^t)| \leq r.$$

Así  $|p(n_K)| \leq r^{1/t} \xrightarrow[t \rightarrow \infty]{} 1$

$\therefore |p(n_K)| \leq 1$

Luego  $n_K \in B[0_K, 1]$ .

Proposición:  $(K, p)$  es no arquimediano si  $\mathbb{Z}_K$  es acotado.

Dem: Si  $g(2) = p(1_K + 1_K) \leq \max\{p(1_K), p(1_K)\} = p(1_K)$

$p(3_K) \leq \max\{p(2_K), p(1_K)\} = p(1_K)$

per inducción:  $p(n_K) \leq p(1_K)$  y como  $p(-1_K) = p(1_K) \Rightarrow p(-n_K) \leq p(1_K)$ .

$\therefore \mathbb{Z}_K$  acotado.

Si  $\mathbb{Z}_K$  es acotado  $p(n_K) \leq 1, \forall n \in \mathbb{Z}$  pd:  $p(a+b) \leq \max\{p(a), p(b)\}$

Basta demostrarlo si  $b = 1_K$   $p(a) \leq 1_K$

En general si  $p(a) \leq p(b)$

$$(p(\frac{a}{b}) \leq 1)$$

entonces:  $p(a+1_K) = p(b) (p(\frac{a}{b} + 1)) \leq p(b) \max\{p(\frac{a}{b}), 1\} \leq \max\{p(a), p(b)\}$ .

$$\begin{aligned} \text{Pd: } & p(x) \leq 1 \\ & p(x+1) \leq 1. \end{aligned}$$

$$\begin{aligned} \text{Peso: } & p(x+1)^n = p((x+1)^n) = p\left(\sum_{k=0}^n \binom{n}{k} x^k\right) \\ & \text{Coeficiente de } x^n \text{ en la suma} \leq \sum_{k=0}^n \binom{n}{k} p(x)^k \\ & \leq \sum_{k=0}^n 1 = n+1. \end{aligned}$$

$$\begin{aligned} \forall n \in \mathbb{N}: & \\ \therefore & p(x+1) \leq \sqrt[n+1]{n+1}, \text{ si } n \rightarrow \infty: & \square \\ \therefore & p(x+1) \leq 1. \end{aligned}$$

Corolario: Si  $\deg K > 0 \Rightarrow (K, f)$  es no-aritmético.

Ejemplo:  $\mathbb{F}_p[x]$  dominio Euclídeo

$f \in \mathbb{F}_p[x]$ , polinomio irreducible.

Definición:  $\mathfrak{f}_f : \mathbb{F}_p[x] \rightarrow \mathbb{R}$

Si  $p(x) = f(x) + h(x)$ , con  $f \neq h$ .

entonces  $v_f(p) = t$  y  $\mathfrak{f}_f(p) = c^{-v_f(p)}$ ,  $c < 1$ . (Función  $v$ . absoluta en  $(\mathbb{F}_p[x])$ ).

obtenemos:  $v_\infty(p) = -2f$

En ambos casos:  $v_f(p+h) \geq \min(v_f(p), v_f(h))$

$2(p+h) \leq \max(2p, 2h)$

$\mathfrak{f}_\infty(p) = c^{v_\infty(p)} = c^{2p}$ ,  $c < 1$ .

Subejemplo:  $f(x) \in S$ ,  $f(x) = x^n f_0(x)$ ,  $f_0(0) \neq 0$

$$\Rightarrow \nu_x(f) = n.$$

Entonces:  $\rho_x(f-p) < \varepsilon$

$$\nu_x(f-p) < \varepsilon$$

$$\nu_x(f-p) > \frac{\log \varepsilon}{\log c}$$

$\therefore$  algo converge a cero cuando su evaluación tiene a infinito.

$\therefore f_n \xrightarrow{p_x} f$ ssi  $\nu_x(f_n - f) \rightarrow 0$

$\therefore f_n \xrightarrow{p_x} f$ ssi  $\forall M > 0 \exists N > 0$  tal que  $n > N \Rightarrow \nu_x(f - f_n) \geq M$

equivalentemente:  $\forall M \mid f - f_n = a_m x^m + \dots$

equivalentemente:  $f \equiv f_n \pmod{x^M}$

Si  $f(x) = a_0 + a_1 x + \dots$   $b_m = a_m$  paramétricamente en  $\mathbb{F}_p$ .

$$f_n(x) = b_0 + b_1 x + \dots$$

$\therefore f(x) = a_0 + a_1 x + \dots + a_n x^n + \dots$  anillo de series de potencias.

En este caso el complemento es:  $\mathbb{F}_p[[x]]$  anillo de series de potencias.

y el complemento de  $\text{Quot}(\mathbb{F}_p[[x]])$  es  $\text{Quot}(\mathbb{F}_p[[x]])^\perp$

$$f_p = 1 = a_0 b_0 + (a_1 b_0 + a_0 b_1) x + \dots$$

$$\begin{aligned} f(x) &= a_0 + a_1 x + \dots + a_n x^n + \dots \\ p(x) &= b_0 + b_1 x + \dots + b_n x^n + \dots \end{aligned}$$

$$\text{Luego } a_0 b_0 = 1 \quad (\text{av invertible})$$

$$b_0 = a_0^{-1}$$

$$b_1 = a_0^{-1} (-a_1 b_0)$$

$$b_2 = a_0^{-1} (-a_1 b_1 - a_2 b_0)$$

entonces  $f(x) = x^n (a_0 + a_1 x + \dots + a_n x^n) \in \mathbb{F}_p[[x]]^\perp$

$$\frac{1}{f} = \frac{1}{x^n} \cdot f^{-1} \in \mathbb{F}_p[[x]] = \frac{b_n}{x^n} + \frac{b_{n+1}}{x^{n+1}} + \dots + b_1 x + \dots$$

Serie de Laurent.

$\text{Woot}(\mathbb{F}_p((x))) = \mathbb{F}_p((x))$  sellano cuerpos de series de Laurent.

- Hecho:  $(\tilde{\mathbb{F}}_p(x))_{\infty} \cong \mathbb{F}_p((x^{-1}))$ .
- $(\tilde{\mathbb{F}}_p(x))_x \cong \mathbb{F}_p((x))$ .

Kno argui mediano, completo.

$$\mathcal{O}_K = \{a \in K : |p(a)| \leq 1\}$$

$$m_K = \{a \in K : p(a) < 1\}$$

Afirmación:  $\forall a, b \in \mathcal{O}_K, |p(a)|, |p(b)| \leq 1$

$$|p(a+b)| \leq \max\{|p(a)|, |p(b)|\} \leq 1$$
$$|p(ab)| \leq |p(a)| |p(b)| \leq 1$$

∴  $\mathcal{O}_K$  anillo de Enteros de  $K$

$$\text{Si } |p(a)| < 1 \Rightarrow |p(a \cdot b)| = |p(a)| |p(b)| < |p(b)| \leq 1$$

$\therefore m_K$  es ideal [ideal maximal de  $\mathcal{O}_K$ ]

Es maximal pues:  $\forall I \subset \mathcal{O}_K, I \neq m_K \Rightarrow a \in I \cap (\mathcal{O}_K \setminus m_K) \Rightarrow |p(a)| = 1$

$$\text{Sea } I \subset \mathcal{O}_K, I \neq m_K \Rightarrow a \in I \cap (\mathcal{O}_K \setminus m_K) \Rightarrow |p(a)| = 1$$

$$\text{Luego } a^{-1} \in \mathcal{O}_K (|p(a^{-1})| = 1) = \{1\}$$

$$\therefore a \in \mathcal{O}_K^* \Rightarrow I = \mathcal{O}_K$$

$m_K$  es el único ideal maximal de  $\mathcal{O}_K$ .

$\mathcal{O}_K/m_K$ : Cuerpo residual de  $K$ .

\* para  $\mathbb{F}_p \hookrightarrow \mathbb{F}_p$  (Demostrar)

$$\mathbb{F}_p((x)) \hookrightarrow \mathbb{F}_p$$

Ejercicio: Si  $K = \mathbb{F}_p((x))$ ,  $\mathcal{O}_K = \mathbb{F}_p[[x]]$ ,  $m_K = x \mathbb{F}_p[[x]]$ .

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

Diremos que  $p$  es discreto si  $p(k^*)$  es discreto en  $\mathbb{R}_{>0}$ .

obs:  $p(k^*)$  es Subgrupo de  $\mathbb{R}_{>0} \cong \mathbb{R}$

$p(k^*)$  cíclico,  $p(k^*) = C^\mathbb{Z}$ ,  $c \in (0, 1)$

Si  $c=1$ :  $p(k^*)=\{1\}$ . (valor absoluto trivial).

Si  $p$  es discreto y no trivial, existe  $\pi \in k$ -tal que:  $p(\pi) = c$ ,  $\pi$  se dice un parámetro uniformizante.

E particular: 1)  $\pi \in m_k$  ( $p(\pi) = c < 1$ )

2)  $a \in m_k$  ( $p(a) \leq p(\pi)$ )

Luego:  $p\left(\frac{a}{\pi}\right) \leq 1 \Rightarrow \frac{a}{\pi} \in \mathbb{O}_k \Rightarrow a \in \mathbb{O}_k \cdot \pi = (\pi) \Rightarrow m_k = (\pi)$

Si  $a \in k \Rightarrow p(a) = c^t$ ,  $t \in \mathbb{Z}$

$$p(a) = p(\pi)^t$$

$$p\left(\frac{a}{\pi^t}\right) = 1 \text{, Sea } n = \frac{a}{\pi^t} \in \mathbb{O}_k^*$$

$$\therefore a = n\pi^t \quad n \in \mathbb{O}_k^*$$

Sea  $S \subseteq \mathbb{O}_k$  un conjunto de representantes de  $\mathbb{O}_k / m_k$

Con  $s \in S$ .

Si  $a \in \mathbb{O}_k$ ,  $\exists s_0 \in S$  con  $a \equiv s_0 \pmod{m_k}$

Así  $a = s_0 + \pi a_1$ ,  $a_1 \in \mathbb{O}_k$

$$a_1 = s_1 + \pi a_2$$

$$a = s_0 + \pi s_1 + \pi^2 s_2$$

Repetiendo esto  $n$ -veces:

Luego:

$$a = s_0 + \pi s_1 + \pi^2 s_2 + \dots + \pi^n s_n$$

Más generalmente si  $a = n\pi^t$ ,  $t \in \mathbb{Z}$ ,  $n \in \mathbb{O}_k^*$ .

$a = \pi^t (s_0 + \pi s_1 + \dots + \pi^n s_n)$ ,  $t \in \mathbb{Z}$  (puede ser negativo)

$$\begin{aligned} \mathbb{Z}_p &= \{a_0 + a_1 p + \dots \mid a_i \in \{1, \dots, p-1\}\}, \\ \mathbb{Q}_p &= \{a_n p^n + \dots \mid a_i \in \{1, \dots, p-1\} \text{ in } \mathbb{Z}, a_n \neq 0\} \cup \{0\}. \end{aligned}$$

Motivo: en  $(\mathbb{F}(x))_\infty$  el parámetro un fijo es  $\pi = \frac{1}{x}$ , luego:

$$(\mathbb{F}_p(x))_\infty = \mathbb{F}_p\left(\frac{1}{x}\right)$$

valores absolutos en  $(\mathbb{F}_p(x))_\infty$

### 1) $f$ primos medios

$\mathbb{Z}$  no acotado

$\Rightarrow$  existe primo con  $p(p) > 1$ .

Sea  $f$  otro primo.

$$pt \leq p^t < p^{t+1} \Rightarrow t \log p \leq n \log p \leq (t+1) \log p - 1$$

$$\Rightarrow p^n = a_0 p^t + a_{t+1} p^{t+1} + \dots + a_0 \quad \{a_i \in \{0, \dots, p-1\}\}$$

$$M = \max \{p(1), \dots, p(f-1)\}$$

$$\begin{aligned} \Rightarrow p(p^n) &\leq \sum_{i=0}^{t-1} p(a_i)^{p^i} M^{p^{t-i}} \\ &\leq (t+1) M \max \{1, p(f)^t\} \end{aligned}$$

$$\text{Caso I: } p(f) \leq 1 \Rightarrow p(p^n) \leq (t+1) M \leq \left(n \frac{\log p}{\log f} + 1\right) M$$

$$\Rightarrow p(p^n) \leq \sqrt[n]{\left(n \frac{\log p}{\log f} + 1\right) M} \rightarrow 1 \quad n \rightarrow \infty$$

$$\text{Caso II: } p(f) > 1:$$

$$\begin{aligned} \Rightarrow p(p^n) &\leq (t+1) M p(f)^t \\ \Rightarrow p(p^n) &\leq \sqrt[n]{\left(n \frac{\log p}{\log f} + 1\right) M} p(f)^{t/n} \\ &\leq \sqrt[n]{n} p(f)^{t/n} \end{aligned}$$

$$\begin{aligned} \Rightarrow p(p^n) &\rightarrow 1 \quad n \rightarrow \infty \\ \text{Por lo tanto:} \quad & \end{aligned}$$

$$\log^2 p(f) \leq \log \sqrt[n]{n} p(f)^{t/n} + \frac{t}{n} \log p(f).$$

$$\log(p(p)) \leq \frac{\log p}{\log f} \log(p(f)) + \log q_n(p|f).$$

$$\Rightarrow \log(p(p)) \leq \frac{\log p}{\log f} \log(p(f))$$

$$\frac{\log(p(p))}{\log(p(f))} \leq \frac{\log p}{\log f}$$

Ahora:  $\frac{\log p(f)}{\log(p(p))} \leq \frac{\log f}{\log p}$

$$\frac{\log(p(p))}{\log(p(f))} = \frac{\log p}{\log f} \Rightarrow \frac{\log(p(p))}{\log p} = \frac{\log(p(f))}{\log f} = \lambda$$

$$p(p) = p^\lambda \\ p(n) = n^\lambda. \quad (\text{ejercicio } \lambda < 1). \quad (\text{equivale a } 1.1)$$

los no argumentos:

entonces  $p$  acotado:  $p(p) \leq 1, \forall p \text{ primo}$

Supongamos que  $\exists p, f$  primos con:  $p(p), p(f) < 1$ .

Si  $p, f$  primos distintos:  $\exists S_p, S_f \in \mathbb{Z}$  s.t.  $S_p p + S_f f = 1$

$$\Rightarrow p(1) \leq \max \left\{ p(p)p(f), q(p)p(f) \right\} \\ \leq \max \{ 1, p(p)p(f) \}. < 1 (*) \quad (p(1)=1)$$

Dos alternativas: i)  $p(1) = 1 \quad \forall p \text{ primo}$ .

ii)  $\exists n \text{ ab. trivial.}$

ii) Si  $\exists n \text{ primo}$  con  $p(p) < 1, p(p) = c$

$$\Rightarrow n = p_1^{d_1} \cdots p_r^{d_r}, \quad (p_i = p_i)$$

entonces  $g(n) = p(p_1)^{d_1} = c^{d_1} \quad \therefore p(n) = c^{v_p(n)}$

$$\text{con } c = \left(\frac{1}{p}\right)^\lambda, \quad \lambda = \frac{\log c}{\log \frac{1}{p}} > 0. \quad \therefore p(n) = \left(\frac{1}{p}\right)^{v_p(n)} = |n|^{\lambda}.$$

Definición:

Si  $K$  es un cuerpo, una clase de eq. de valores absolutos

Se denotará, un loparenk.

$\Pi(K)$  ← loparesenk.

$$\Pi(K) = \{ p \mid p \text{ primo} \} \cup \{\infty\}$$

↑  
 no-nfp  
 p-dicho

↑  
 ref. val. ab. usual

Def.  $p, p'$  son equivalentes si:  $\exists \lambda > 0$  tal que:

$$|f(a)| = |f(a')|^{\lambda} \quad \forall a \in K^*$$

obs: Si  $f \sim g$  toda soc. de Cauchy para  $f$  es soc. de Cauchy para  $g$ .

$$\text{Si } \exists N: |f(a_n - a_m)| < \varepsilon \Rightarrow |f(a_n - a_m)| < \varepsilon^N$$

obs:  $p^n \rightarrow 0$  Si  $p = \lim p_n$  entonces:  $p = 1$   $|f|_p = \lim_{n \rightarrow \infty} |f(p_n)|$ .

Prop: Si  $p \neq p'$  (entonces existen soc. pue convergen a 0 pero no en  $p'$ ).

Dem:  $\exists z \in K^*$  con:

$$\frac{\log |f(z)|}{\log |f'(z)|} \neq \frac{\log |f(b)|}{\log |f'(b)|} \Rightarrow \frac{\log |f(z)|}{\log |f(b)|} + \frac{\log |f'(z)|}{\log |f'(b)|}$$

Supongamos  $\exists \frac{m}{n} \in \mathbb{Q}: \frac{\log |f(z)|}{\log |f(b)|} < \frac{m}{n} < \frac{\log |f'(z)|}{\log |f'(b)|}$ .

$$n \log |f(z)| < m \log |f(b)|$$

$$\log |f(\frac{z^n}{b^m})| < 0 \Rightarrow f(\frac{z^n}{b^m}) < 1$$

$$m \log |f'(b)| < n \log |f'(z)|$$

$$a < \log |f'(\frac{z^n}{b^m})|$$

$\exists c$  con  $|f(c)| < 1$ ,  $|f'(c)| > 1$ .

entonces  $c^n \xrightarrow[n \rightarrow \infty]{} 0$  pero  $c^m \xrightarrow[m \rightarrow \infty]{} 0$  y  $|f(c)| > 1$ ,  $|f'(c)| < 1$ .

$\Rightarrow c^{-n} \xrightarrow[n \rightarrow \infty]{} 0$  pero  $(\frac{1}{c})^m \xrightarrow[m \rightarrow \infty]{} 0$ .

Queremos que  $\lim_{n \rightarrow \infty} f(d_n) = 1$ .

$$\text{Sea } d_n = \frac{c^n}{c^n + c^{-n}}, \quad e_n = \frac{c^{-n}}{c^n + c^{-n}}, \quad d_n + e_n = 1$$

$$0 \leq f(d_n) \leq \frac{f(c^n)}{f(c^n) - f(c^{-n})} \xrightarrow{n \rightarrow \infty} 0. \quad \begin{aligned} & \lim_{n \rightarrow \infty} f(e_n) \xrightarrow{n \rightarrow \infty} 0 \\ & f'(c^n) \leq f'(d_n) \leq \frac{f'(e_n)}{f'(c^n) - f'(c^{-n})} \end{aligned}$$

$$\therefore \lim_{n \rightarrow \infty} f'(d_n) \xrightarrow{n \rightarrow \infty} 1.$$

$$\therefore e_n = 1 - d_n \quad \therefore e_n \rightarrow 0 \quad d_n \rightarrow 1.$$

Sean  $y_1, y_2 \in K$ ,  $d_n = f(y_n)$

$$\text{Luego } d_n \xrightarrow[p]{} y \quad y \xrightarrow[p']{} f(y).$$

Proposición: Si  $f, f'$  son val. ab. no equivalentes en  $K$ , entonces  $\Delta_K = \{f(z_i) | z_i \in K\}$ .

Es densa en  $(K, p) \times (K, p')$ .

Tercera Aproximación del Límite: Si  $p_1, \dots, p_n$  son val. ab. no equivalentes en  $K$

(ninguno es equivalente) existen  $a_1, \dots, a_n \in K$  tales que para  $b_k \xrightarrow[p]{} a_i$

$$\text{que: } b_k \xrightarrow[p]{} a_i.$$

Entorno de Números: V. A en  $\mathbb{K}(ii)$ .

Si  $p$  v. ab. en  $\mathbb{K}(ii) \Rightarrow p$  es un n. en  $\mathbb{K}$ .

Si  $p$  es v. ab. en  $\mathbb{K}(ii)$ ,  $\bar{p}$  también lo es con:

$$\bar{p}(z) = p(\bar{z}).$$

caso -  $f(z) = 1/z \Rightarrow p|_K = 00$ .

Sea  $p$  primo. Dos casos: Si  $p = \overline{\pi\pi}$ ,  $\pi$  primo en  $\mathbb{K}(ii)$

ssi  $\nexists$  es cuadrado en  $\mathbb{F}_p$ .  $x^2+1$  tiene raíces en  $\mathbb{F}_p$

$$f(x) = x^2 + 1, \quad f'(x) = 2x$$

P#2. Problema de Hensel:

$$x^2 + 1 = 0 \text{ tiene sol. sobre } \mathbb{Z}/p\mathbb{Z}, \forall p.$$

Sea  $a \in \mathbb{Z}$  tal que:  $a^2 \equiv -1 \pmod{p} \mathbb{Z}$ .

$$\text{con } a_{n-1} \equiv a_n \pmod{p^{n-1}\mathbb{Z}}.$$

entonces  $\{a_n\}_{n \in \mathbb{N}}$  suc. de Cauchy en  $\mathbb{Z}/p\mathbb{Z} \Rightarrow a_n \rightarrow a$  con  $a^2 = -1$  en  $\mathbb{K}_p$

entonces  $\mathbb{K}(i) \hookrightarrow \mathbb{K}_p$

$$i \mapsto a$$

$$p_1 \leftarrow 11, \quad p_1 \nmid p_2 \quad (\text{llave } x \mapsto a - i)$$

$$p_2$$

En cambio si  $x^2 + 1 = 0$  no tiene soluciones en  $\mathbb{F}_p$ , no tiene soluciones en  $\mathbb{K}_p$

Así  $\mathbb{K}_p(i)$  es extensión cuadrática (de  $\mathbb{K}_p$ ).

Afirmación: Si  $K$  es cuerpo completo y  $L/K$  extensión finita

existe una única extensión del valor absoluto de  $K$  a  $L$ .

Demo:

(más adelante)

$\mathbb{K}_p(i)$  tiene unív. val. ab. absoluto que extiende el de  $\mathbb{K}_p$ .

y  $\mathbb{K}(i) \hookrightarrow \mathbb{K}_p(i)$ . Luego existe  $v, v'$  en  $\mathbb{K}(i)$  que extiende el val. abs.  $p$ -ádico.

Si  $p=2$ :  $f(x) = x^2 + 1$  tiene sol. en  $\mathbb{K}_2$ ?

pol. de Eisenstein en  $\mathbb{Z}$ ,

tonce  $p(x) = f(x-1) = (x-1)^2 + 1 = x^2 - 2x + 2$ .

en  $\mathbb{Z}_2$   $\therefore$  p divide a  $p(x)$  (no tiene raíces)

$\mathbb{K}(i) \hookrightarrow \mathbb{K}_2(x)$ .  $\mathbb{K}(i)/\mathbb{K}$  ext cuadrática

existe un v. abs. que extiende el v. abs.  $2$ -ádico.

Scanned with CamScanner

Lema de Hensel:

Si  $f(a) \equiv 0 \pmod{p^r}$  y  $f'(a) \equiv 0 \pmod{p^r} \Rightarrow \exists b \in \mathbb{Z}/p^{2r}\mathbb{Z}$

$f(b) \equiv 0 \pmod{p^r}$  y  $b \equiv a \pmod{p^r}$ .

Ingrediente fundamental:  $f(x+y) \equiv f(x) + y f'(x) \pmod{y^2}$

Lema de Hensel p-ádico: Sea  $K$  cuerpo completo y divisor primo.

y sea  $f \in \mathcal{O}_K[[x]]$  tal que existe  $a$  con:  $|f(a)| < 1$

$$|f'(a)|^2 > |f(a)|$$

Entonces  $b \in \mathcal{O}_K$  con  $f(b) = 0$ .

Demonstración: Se define:  $a_0 = a$ ,  $a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}$

Afirmación:  $\{a_n\}$  converge a una solución.

Obs: Basta probar que:  $a_{n+1} - a_n \xrightarrow{n \rightarrow \infty} 0$ .

$$\text{Pues } |a_{n+1} - a_n| \leq \sum_{i=n}^{n+1} |a_{i+1} - a_i| \leq \max_{i=n}^{n+1} |a_{i+1} - a_i|.$$

Equivientemente:  $\sum b_i$  c.v. si  $b_i \rightarrow 0$

$$a_{n+1} - a_n = \frac{f(a_n)}{f'(a_n)} \quad \text{Por otro lado: } f(a_{n+1}) = f(a_n) - \frac{f(a_n)}{f'(a_n)} \\ = f(a_n) - \frac{f(a_n)}{f'(a_n)} f'(a_n) + p_n \in \left( \frac{f(a_n)}{f'(a_n)} \right)^2 \\ = p_n, \quad p_n \in \left( \frac{f(a_n)}{f'(a_n)} \right)^2$$

$$\text{y } f'(a_{n+1}) = f'(a_n) - \frac{f(a_n)}{f'(a_n)} f''(a_n) + h_n, \quad h_n \in \left( \frac{f(a_n)}{f'(a_n)} \right)^2$$

$$= f'(a_n) + h_n, \quad h_n \in \left( \frac{f(a_n)}{f'(a_n)} \right)^2$$

Por inducción probamos que: Sea  $\lambda = \frac{|f(a)|}{|f'(a)|} < |f'(a)|$

Por inducción:

$$1) |f(a_n)| \leq \lambda^n |f(a)|^2$$

$$2) |f'(a_n)| = |f'(a)|$$

$$\text{del anterior: } |f(a_{n+1})| \leq \frac{|f(a_n)|^2}{|f'(a_n)|^2} \leq \frac{\lambda^{2n} |f(a)|^4}{|f'(a_n)|^2} \leq \lambda^{2n} |f(a)|^2 \leq \lambda^{n+1} |f(a)|$$

y por la otra propiedad:

$$|f'(a_{n+1}) - f'(a_n)| \leq \left| \frac{f(a_n)}{f'(a_n)} \right| = \frac{|f(a_n)|}{|f'(a_n)|} \cdot |f'(a_n)|$$
$$< \lambda^n |f'(a_n)| \leq |f''(a_n)|$$

∴  $|f'(a_{n+1})| = |f'(a_n)|$ . (principio de dominancia).

Luego  $|a_{n+1} - a_n| = \frac{|f(a_n)|}{|f'(a_n)|} < \lambda^n |f'(a_n)| \xrightarrow{n \rightarrow \infty} 0$

∴  $|a_{n+1} - a_n| \xrightarrow{n \rightarrow \infty} 0$

Luego  $\{a_n\}_{n \in \mathbb{N}}$  es convergente. ∴  $a_n \rightarrow \bar{a}$ .  
 $f(a_n) \rightarrow f(\bar{a})$  [polinomio continuo]. Ejercicio.

Por otro lado:  $|f(a_n)| \xrightarrow{n \rightarrow \infty} 0$  ∵  $f(\bar{a}) = 0$ .

Además:  $|a - a_0| = 0$   
 $|a - a_1| = |a_0 - a_1| = \frac{|f(a_0)|}{|f'(a_0)|} < |f'(a_0)|$

$$|a - a_2| \leq \max\{|a - a_1|, |a_1 - a_2|\} < |f'(a_0)| \quad [\text{Principio de Dominancia}]$$

Por inducción:  $|a - a_n| < |f'(a_0)|$

Tomando el límite:  $|a - \bar{a}| \leq |f'(a_0)| = |f'(a)| < 1$

Ejemplo:  $a \in \mathbb{O}_K$ ,  $f \in \mathcal{O}_K[x]$ ,  $f(a) \equiv 0 \pmod{\pi}$   
 $K$  discreto,  $m_K = (\pi)$ .

$$f(a) \equiv 0 \pmod{\pi}$$

$$f'(a) \not\equiv 0 \pmod{\pi}$$

$$|f'(a)| = 1, |f(a_n)| \leq |\pi| < 1.$$

$$\exists \bar{a} \in \mathbb{O}_K^* \text{ s.t. } |a - \bar{a}| < 1, a \equiv \bar{a} \pmod{\pi}$$

$$\text{con } f(\bar{a}) = 0 \pmod{\pi^r} \quad \forall r$$

Ejemplo 2:  $K = \mathbb{Z}_2$ ,  $f(x) = x^2 - b$  en  $\mathbb{Z}_2$

$$f'(x) = 2x, b \in \mathbb{Z}_2 = \{0, 1\}$$

tenemos  $x^2 \equiv b \pmod{2}$  sea solución de esta.

Como  $|b| = 1$ ,  $|a| = 1$ ,  $|f'(a)| = 2$ .

si  $|f(a)| = |a^2 - b| < 4$ ,  $\exists \bar{a} \in \mathbb{Z}_2$  con  $\bar{a}^2 = b$ .

En particular, si  $b \equiv 1 \pmod{8}$  entonces es cuadrado en  $\mathbb{Z}_2$ .

Más generalmente:

Ejercicio: Tezema de los cuadrados latentes

Si  $K$  es completo, no infinito, existe  $a$  con  $|a^2 - b| > 4$ ,

entonces  $b$  es un cuadrado en  $\mathbb{Z}_K$ .

Ejemplo: Si  $b$  es cuadrado módulo 9, para si módulo 4.

Si  $K$  es distinto, ( $m_K = (\pi)$ ) entonces toda unidad  $\Delta$  tal que:

$\exists a \in \mathbb{Z}_K$  con  $|a^2 - \Delta| = 14$  pero no es un cuadrado se dice

Unidad de defecto cuadrático minimal.

Ejemplo: Sea  $f \in K[x]$  cuadrático,  $f(x) = ax^2 + bx + c$  con  $|a|, |b|, |c| \leq M$ .

Dividiendo:  $p(x) = \frac{a}{b}x^2 + x + \frac{c}{b} \in \mathbb{Z}_K[x], |\frac{a}{b}| \leq 5, |\frac{c}{b}| \leq 1$ .

$p(x) \equiv x \pmod{m_K}$

Asi:  $p(0) \equiv 0 \pmod{m_K}$ ,  $|p(0)| \leq 1$ ,  $|p(0)| \geq 1$ . (porque  $p(0) \neq 0$ )

$\therefore p$  tiene raíz en  $\mathbb{Z}_K$   $\therefore f$  tiene raíz en  $\mathbb{Z}_K$ .

Esto es lo que queríamos probar.

Todos los cuadráticos tienen raíz.

Sea  $L/k$  extensión cuadrática. Sea  $x \in L$

prop:  $x$  entero sobre  $k$  si y sólo si  $N_{L/k}(x) \in \mathcal{O}_k$ .

Dem: Caso I -  $x \notin k$

$$m_x(x) = x^2 + bx + c$$

$$N_{L/k}(x) = c - b^2$$

$x$  entero  $\Rightarrow N_{L/k}(x) = 0$ .

Si  $N_{L/k}(x) \in \mathcal{O}_k$ , si  $b \in \mathcal{O}_k$   $m_x$  tiene raíces en  $k$ . ( $\neq$ )

Caso II :  $x \in k \Rightarrow N_{L/k}(x) = x^2$

Corolario:  $N_{L/k}(x) \in \mathcal{O}_k \Rightarrow N_{L/k}(x+y) \in \mathcal{O}_k$

Si  $(k, p)$  completo, definimos  $\rho_L : L \rightarrow \mathbb{R}$  tal que  $\rho_L(\alpha) = \rho_k(N_{L/k}(\alpha))$

Dem:  $\rho_L(\alpha \beta) = \rho_L(\alpha) \rho_L(\beta)$ .

pd:  $\rho_L(\alpha + \beta) \leq \max\{\rho_L(\alpha), \rho_L(\beta)\}$

Sig:  $\rho_L(\alpha) \leq \rho_L(\beta)$

$$\rho_L(\alpha + \beta) = \rho_L(\beta) \rho_L(1 + \frac{\alpha}{\beta}) \leq \rho_L(\beta)$$

Por lo tanto  $\rho_L(\frac{\alpha}{\beta}) \leq 1 \Rightarrow \rho_L(1 + \frac{\alpha}{\beta}) \leq 1$

Si  $\rho_L$  es un valor absoluto no trivialmente.

Si  $D$  no es cuadrado, en  $\mathbb{Q}_p$ , de forma que  $(\mathbb{Q}_p(\sqrt{D})/\mathbb{Q}_p)$  es cuadrática, existe  $y, z$  en  $\mathbb{Q}_p(\sqrt{D})$  que contiene a 1.

Único.

Es único porque si  $\rho$  extiende a  $\rho_k$  entonces

$$\text{antilog } \sqrt{D} \xrightarrow{\rho} \text{antilog } \sqrt{D}$$

$$\Rightarrow \frac{a_n}{b_n} \xrightarrow[p_k \rightarrow 0]{} 0 \Rightarrow p_k \approx 1/p$$

∴ Evidente.

Aproximación fuerte en  $\mathbb{Z}$

Sean  $p_1, \dots, p_r$  primos distintos y sean  $d_1, \dots, d_n$

con  $x_i \in \mathbb{Z}$  para  $i > 0$ .

Entonces existe  $\alpha \in \mathbb{Q}$  tal que  $|d_i - \alpha|_p < \varepsilon$   $\forall i \in \{1, \dots, n\}$

equivalente, existe  $\alpha \in \mathbb{Q}$  tal que: 1)  $|d_i - \alpha|_p < \varepsilon$ ,  $\forall i \in \{1, \dots, n\}$

2)  $|\alpha|_p \leq 1$ ,  $\forall p \neq p_1, \dots, p_r$

Ejercicio. Si  $\alpha \in \mathbb{Q}$ :  $\prod_p |\alpha|_p \cdot |\alpha|_{\infty} = 1$ .

Demostración: Basta tomar  $n_i$  tales:

$$\left(\frac{1}{p_i}\right)^{n_i} < \varepsilon$$

$\alpha \in \mathbb{Q}$  tal que:

Basta encontrar  $\alpha \equiv x_i \pmod{p_i^{n_i}}$

y aplicar TCR.

Sean  $p_1, \dots, p_r$  primos en  $\mathbb{Z}$  y  $\alpha \in \mathbb{Q}$ ,  $\varepsilon > 0$ , entonces existe

$\alpha \in \mathbb{Q}$  tal que:

1)  $|x_i - \alpha| < \varepsilon$ ,  $i \in \{1, \dots, r\}$

2)  $|\alpha|_p \leq 1$ ,  $\forall p \neq p_i$ ,  $i \in \{1, \dots, r\}$ .

Demostración: Observemos que  $\alpha \in \mathbb{Q}$  si y solo si  $\alpha = \sum_i x_i p_i^{n_i}$  para  $x_i \in \mathbb{Z}$ ,  $n_i \geq 0$ . Si  $\alpha = \sum_i x_i p_i^{n_i}$  para  $x_i \in \mathbb{Z}$ ,  $n_i \geq 0$  y  $\alpha \in \mathbb{Q}$ .

$\exists h \in \mathbb{Z}$  tal que:  $\alpha x_i \in \mathbb{Z}_{(p_i)}$ ,  $i \in \{1, \dots, r\}$  ( $\alpha = \sum_i x_i p_i^{n_i}$ ).

Por TCR:  $\exists \beta \in \mathbb{Z}$  tal que: 1)  $|\alpha - \beta|_p \leq \varepsilon |h|_p$ , 2)  $|\beta|_p \leq \varepsilon$ , para  $p \neq p_i$ ,  $i \in \{1, \dots, r\}$

Sea  $\alpha = \beta/n \in \mathbb{Q}$

$$1) |\alpha - x_i|_{p_i} = \frac{1}{|n|_{p_i}} |\beta - n\alpha|_{p_i} \leq \frac{1}{|n|_{p_i}} \varepsilon |n|_{p_i} = \varepsilon.$$

$$2) |\alpha|_p = \frac{|\beta|_p}{|n|_p} = |\beta|_p \text{, i.e. } |n|_p = 1 \text{ y } \exists \text{ que } n = \prod p_i^{s_i}$$

Sea  $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$  extensión cuadrática.

Entonces  $D_K = \{a+bh \mid a, b \in \mathbb{Z}\}$ , donde  $K = \begin{cases} \sqrt{D}, & D \equiv 2, 3 \pmod{4} \\ \frac{1+\sqrt{D}}{2}, & D \equiv 1 \pmod{4} \end{cases}$

y  $K = \{a+bh \mid a, b \in \mathbb{Q}\}$ .

¿Existe topo de Aprox. en  $K$ ?

Resposta: Topo de Aprox. fuerte en  $K$ :

Sean  $p_1, \dots, p_n \in \Pi f(K)$  ( $\Pi f(K) = \{f\} \cup \text{parentesis sobre algun p_i\}$ )

y sea  $\varepsilon \in K$ ,  $\varepsilon > 0$ .

Entonces existe  $\alpha \in K$  tal que:

$$1) |\alpha - x_i|_{p_i} < \varepsilon \quad \forall i \in \{1, \dots, n\}$$

$$2) |\alpha|_p \leq 1, \quad p \in \Pi^+(K), \quad p \neq p_1, \dots, p_n.$$

Demonstración:  $\tilde{K}_p = K \otimes \mathbb{Q}_p = \{a + b\tilde{h} \mid a, b \in \mathbb{Q}_p\}$

$\mathbb{Q}_p$ -álgebra,  $\tilde{h}^2 = D\tilde{h}$ .

$$K \cong \frac{\mathbb{Q}(x)}{(x^2-D)}$$

$$\tilde{K}_p \cong \frac{\mathbb{Q}(x)}{(x-D)} \otimes \mathbb{Q}_p \cong \frac{\mathbb{Q}(x) \otimes \mathbb{Q}_p}{(x-D) \otimes \mathbb{Q}_p}$$

$$\approx \frac{U_p(x)}{(x^2 - D)} \quad \left\{ \begin{array}{l} \text{en general} \quad w \leq v, w_0 \leq v_0 \\ \frac{v}{w} \otimes \frac{v_0}{w_0} = \frac{v \otimes v_0}{w \otimes v_0 + v \otimes w_0} \end{array} \right.$$

Caso I: 1) Es cuadrado en  $U_p$ :

$$\frac{U_p(x)}{(x^2 - D)} \approx \frac{U_p(x)}{(x - \sqrt{D})} \times \frac{U_p(x)}{(x + \sqrt{D})} \cong U_p \times U_p \cong k_p \times k_p$$

$$\begin{matrix} \tilde{h} = (1, 1) \\ \tilde{h} = (h, \bar{h}) \end{matrix}$$

$$a + b h \mapsto (a + b h, a + b \bar{h}) \quad (\text{Aprox. encarta componente})$$

Caso II:  $D$  no es cuadrado en  $U_p$ :

$$\frac{U_p(x)}{(x^2 - D)} \cong k_p \quad (p \text{ unico lugar sobre } p)$$

Demonstración de TAF en  $K$ :

$$p_1, \dots, p_r \in \Pi_f(K) \text{ entanobre } p_1, \dots, p_s \in \Pi_f(U).$$

Algunos lugares si fueran necesarios, podemos suponer que todos los lugares sobre  $p_i$  estan sobre  $p_1, \dots, p_r$

$$\text{Si: } p \notin p_1, \dots, p_r, |d_{p_i} - d_p|_p \leq \epsilon \Rightarrow |d_{p_i} - d_p|_p \leq 1.$$

$$\text{Entonces: } d_i = a_i + b_i h = (a_i + b_i h, a_i + b_i \bar{h}) \text{ pues } k_p \cong k_{p_1} \times k_{p_2}$$

$$\text{Si: } |a_i - a_{p_i}|_p \leq \epsilon, |b_i - b_{p_i}|_p \leq \epsilon \quad |U_p \cong k_{p_1} \times k_{p_2}|_p$$

$$|(a_i + b_i h) - (a_{p_i} + b_{p_i} h)|_{p_1} \leq \max \{ |a_i - a_{p_i}|_p, |b_i - b_{p_i}|_p \} \leq \epsilon.$$

$$|(a_i + b_i h) - (a_{p_i} + b_{p_i} h)|_{p_2} = |(a_i + b_i h) - (a_{p_i} + b_{p_i} h)|_p \leq \max \{ |a_i - a_{p_i}|_p, |b_i - b_{p_i}|_p \} \leq \epsilon$$

$$\text{Pues } |N(h)|_p = |h|_p \leq 1.$$

Caso II:  $W_p(\sqrt{D}) = K_p$ , el único lugar sobre  $P$ .

$$\left\| (a_i + b_i)h - (a + bh) \right\|_p = \left\| (a_{i-1} + (b_i - b)h) \right\|_p \\ = \left\| N_{K_p/K_{p'}}((a_{i-1} + (b_i - b)h)) \right\|_p$$

Por la continuidad de polinomios (Norma de los polinomios)  
Esto es cierto si  $|a_{i-1}|_p, |b_i - b|_p \leq \varepsilon_i$  algún  $\varepsilon_i$ .

Proposición: Si  $T$  es unión en  $O_F$  entonces existe  $\alpha, \beta$   
 $\in O_F$  tales que:  $T = (\alpha, \beta)$ .

Un par de conceptos previos:  $U^2 \subset e.v$  de dim 2.

$\lambda \subseteq U^2$  se dice reticulado si existe base  $\{v_1, v_2\}$  de  $U^2$  con

$$\lambda = \mathbb{Z}v_1 \oplus \mathbb{Z}v_2$$

Ej:  $\Lambda_0 = \mathbb{Z}e_1 + \mathbb{Z}e_2$  (tiny & sobre  $\Rightarrow$  T invertible).

$$\Lambda = T\Lambda_0 \quad T(e_1) = v_1, \quad T(e_2) = v_2$$

Como  $U^2 \subseteq W_p$  ( $T$  es unión en  $O_F$ )

$$\Lambda \mapsto \Lambda_p, \quad (\text{Clas } \Lambda = \Lambda_p)$$

$$\Lambda_p = \mathbb{Z}_p v_1 \oplus \mathbb{Z}_p v_2$$

$$T\Lambda_0 = \Lambda_0 \cap T\mathbb{Z}^2 = \mathbb{Z}^2$$

$$T\Lambda_0 = S\Lambda_0 \quad \text{ssi } S^{-1}T \in M_2(\mathbb{Z})^*$$

$$\Lambda = T\Lambda_0 \Rightarrow \Lambda_p = T\Lambda_0 p, \quad \Lambda_0 p = \mathbb{Z}^2 - \{(0,0)\}$$

$$T\Lambda_0 p = S\Lambda_0 p \quad \text{ssi } S^{-1}T \in M_2(\mathbb{Z}_p)^*$$

Si

Segundas Derivadas:

$f: \Omega \subseteq \mathbb{R}^m \rightarrow \mathbb{R}^n$ , abierto,  $\vec{x}_0 \in \Omega$

$$D^2 f(\vec{x}_0)(\vec{u}, \vec{v}) = D(D f(\vec{x}_0) \vec{u}) \vec{v}.$$

Ejemplo:  $f: \Omega \subseteq \mathbb{R}^3 \rightarrow \mathbb{R}$

$$H_f = \begin{pmatrix} \frac{\partial^2 f}{\partial x^2} & \frac{\partial^2 f}{\partial y \partial x} & \frac{\partial^2 f}{\partial z \partial x} \\ \frac{\partial^2 f}{\partial x \partial y} & \frac{\partial^2 f}{\partial y^2} & \frac{\partial^2 f}{\partial z \partial y} \\ \frac{\partial^2 f}{\partial x \partial z} & \frac{\partial^2 f}{\partial y \partial z} & \frac{\partial^2 f}{\partial z^2} \end{pmatrix}.$$

Demostre que:

$$\begin{aligned} & \left\{ D_f(x_0 + h_1, y_0 + h_2, z_0 + h_3) - D f(x_0, y_0, z_0) \right\} \vec{w} = \left( \frac{\partial f}{\partial x}(x_0 + h_1, y_0 + h_2, z_0 + h_3) - \frac{\partial f}{\partial x}(x_0, y_0, z_0) \right. \\ & \quad \left. + \frac{\partial^2 f}{\partial y \partial x}(x_0 + \vec{h}) - \frac{\partial^2 f}{\partial y \partial x}(x_0) \right) \vec{w}. \\ & = \left( \left( \frac{\partial^2 f}{\partial x^2} \frac{\partial^2 f}{\partial y \partial x} \frac{\partial^2 f}{\partial z \partial x} \right) \begin{pmatrix} h_1 \\ h_2 \\ h_3 \end{pmatrix} + R_1(\vec{h}) \right), \left( \frac{\partial^2 f}{\partial x \partial y} \frac{\partial^2 f}{\partial y^2} \frac{\partial^2 f}{\partial z \partial y} \right) \begin{pmatrix} h_1 \\ h_2 \\ h_3 \end{pmatrix} + R_2(\vec{h}), \left( \frac{\partial^2 f}{\partial x \partial z} \frac{\partial^2 f}{\partial y \partial z} \frac{\partial^2 f}{\partial z^2} \right) \begin{pmatrix} h_1 \\ h_2 \\ h_3 \end{pmatrix} + R_3(\vec{h}) \right) \vec{w} \\ & = \left( (f_{xx}h_1 + f_{xy}h_2 + f_{xz}h_3 + r_1(\vec{h})), f_{xy}h_1 + f_{yy}h_2 + f_{yz}h_3 + r_2(\vec{h}), f_{xz}h_1 + f_{yz}h_2 + f_{zz}h_3 + r_3(\vec{h})) \right) \vec{w} \\ & = \left( (f_{xx}h_1 + f_{xy}h_2 + f_{xz}h_3 + r_1(\vec{h})), f_{xy}h_1 + f_{yy}h_2 + f_{yz}h_3, f_{xz}h_1 + f_{yz}h_2 + f_{zz}h_3 \right) \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix} + r_1(\vec{h})w_1 + r_2(\vec{h})w_2 + r_3(\vec{h})w_3 \\ & = w_1 f_{xx}h_1 + w_1 f_{xy}h_2 + w_1 f_{xz}h_3 + w_2 f_{xy}h_1 + w_2 f_{yy}h_2 + w_2 f_{yz}h_3 + w_2 f_{xz}h_1 + w_2 f_{yz}h_2 + w_3 f_{xz}h_1 + w_3 f_{yz}h_2 + w_3 f_{zz}h_3 + R(\vec{h}, \vec{w}) \\ & = (w_1, w_2, w_3) \begin{pmatrix} f_{xx} & f_{xy} & f_{xz} \\ f_{xy} & f_{yy} & f_{yz} \\ f_{xz} & f_{yz} & f_{zz} \end{pmatrix} \begin{pmatrix} h_1 \\ h_2 \\ h_3 \end{pmatrix} + R(\vec{h}, \vec{w}) \\ & = D^2 f(x_0, y_0, z_0)(\vec{h}, \vec{w}) + R(\vec{h}, \vec{w}), \lim_{\vec{h} \rightarrow 0} \frac{R(\vec{h}, \vec{w})}{\|\vec{h}\|} = 0 \end{aligned}$$

$\left| \frac{n}{m} \right|_p \leq 1$  ( $\frac{n}{m}$  entero si lo es p-adicamente)

ssi.  $p \nmid m \wedge p \Rightarrow m = \pm 1$ ,

$U \in \mathcal{D}_2(\mathbb{Z})$ :  $U \in \mathcal{D}_2(\mathbb{Z})^*$  ssi.  $U \in \mathcal{D}_2(\mathbb{Z}_p)^*$   $\forall p$ .

I).  $\Lambda = \Lambda'$ , ssi.  $\Lambda_p = \Lambda'_p \quad \forall p$ .

obs:  $U \in \mathcal{D}_2(\mathbb{Z})^* \Rightarrow U \in \mathcal{D}_2(\mathbb{Z}_p)^*$  casi todo p.

II):  $\Lambda, \Lambda'$  ret  $\Rightarrow \Lambda_p = \Lambda'_p$ , casi todo p.

Dado: Si para cada  $p$  tomamos un reticulado  $\Lambda_p \subseteq U_p$  tales fu:

$\Lambda(p) = \Lambda_p$  para casi todo p entonces existe

un reticulado tal que  $(\Lambda \subseteq \mathbb{Z}^2)$ ,  $\Lambda_p = \Lambda(p) \cap U_p$ .

Existen  $n \in \mathbb{Z}$ :  $n\Lambda(p) \subseteq \Lambda_p$   
 $\Lambda(p) \subseteq n\Lambda_p$ .

podemos suponer

obs: Si  $p_1, \dots, p_n$  son primos  $v(p_i) \in U(p_i)$ ,  $\varepsilon > 0$  podemos escoger

$n \in \mathbb{Z}^2$  con:  $|n - v(p_i)|_{p_i} < \varepsilon \quad i \in \{1, \dots, n\}$   
 $|n|_p \leq 1 \quad \forall p \neq p_1, \dots, p_n$ .

donde  $|a, b|_p = \max\{|a|_p, |b|_p\}$ .

$\Lambda(p_i) = \mathbb{Z} v_1(p_i) \oplus \mathbb{Z} v_2(p_i) \quad |v_1(p_i)|_p \in \mathbb{Z}_{p_i}^2$   
 $|v_2(p_i)|_p \in \mathbb{Z}_{p_i}^2$

Encuentramos  $N_1, N_2 \in \mathbb{Z}^2$  que apret  $v_1(p_i), v_2(p_i)$  en cada  $p_i$ .

obs:  $\mathbb{Z}_p$  es abierto en  $U_p$

$\Lambda(p_i)$  aben  $U(p_i)$ .

$\Lambda(p_i) = \mathbb{Z}_{p_i} v_1(p_i) \oplus \mathbb{Z}_{p_i} v_2(p_i) \quad |v_1(p_i)|_p \sim N_1(p_i)$   
 $|v_2(p_i)|_p \sim N_2(p_i)$

$\{ \mathcal{D}_2(\mathbb{Z}_p)^* \text{ es abierto} \}$

(donde  $p_1, \dots, p_n$  con  $\Lambda(p_i) \neq \Lambda_{p_i}$ ).

$$\Lambda' = \mathbb{Z} v_1 \oplus \mathbb{Z} v_2$$

$$\Lambda'_p = \Lambda(p_i) \quad i=1, \dots, h$$

$$\Lambda'_p \subseteq \Lambda_{op} \text{ todo } p \neq p_1, \dots, p_n$$

$p_1, \dots, p_m$  lógicos con  $\Lambda(p_i) \subset \Lambda_{op}$

Repetiendo el proceso encontramos  $\Lambda''$  con

$$\Lambda''_{p_i} = \Lambda(p_i), \quad i=1, \dots, n$$

$$\Lambda''_{p_j} \subseteq \Lambda(p_j) \quad j=1, \dots, m$$

Tomando  $\Lambda = \Lambda' + \Lambda''$  (menos reticulados que contiene  $\Lambda'$ ,  $\Lambda''$ )

$$\Lambda_p = \Lambda'_p + \Lambda''_{p_i}$$

Ejercicio: Comprobar caso a caso  $\Lambda_p = \Lambda(p) \neq p$ .

$L/K$  t. ramificada

$$[L:K] = e$$

$$N_L(\pi_K) = \pi$$

$$\text{irr}_{\alpha_K}(x) = x^e + a_{e-1}x^{e-1} + \dots + a_0$$

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

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

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

$$N_L(\pi_L^e) < N_L(a_0)$$

$$N_L(\pi_L^e) = e = N_L(a_0)$$

$\therefore N_L(a_0) = 1$ . (pol. de Eisenstein).

Pimos:

$L/K$  extensión cuadrática, si  $\sigma \in K$  y  $\pi$  es parámetro uniformizante de  $K$

$$\alpha = \sum_{i=-m}^{\infty} a_i \pi^i$$

$$\pi \sigma_L = m_L$$

i) Si  $\pi$  es uniformizante en  $L$ :

entonces

$$\sigma_K / \pi \sigma_K \leq \sigma_L / \pi \sigma_L$$

$$(\text{cuerpo}) \quad \mathbb{F}_K \subseteq \mathbb{F}_L$$

$$\mathbb{F}_K = \{\overline{a_0} = \overline{0}, \overline{a_1}, \dots, \overline{a_n}\}, \quad \mathbb{F}_L = \{\overline{b_0} = \overline{0}, \overline{b_1}, \dots, \overline{b_t}\}$$

Así si

$\alpha \in K$ :

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

$$\left| \begin{array}{l} \beta \in L \\ \beta = \sum_{i=-n}^{\infty} b_i \pi^i \end{array} \right. \text{ irreducible}$$

función:  $\mathbb{F}_L = \mathbb{F}_K[C]$ , con  $C = \overline{b_j}$  sol. p.  $j$ .

$$\tilde{P}(x) = \text{Im}[C(x)] \in \mathbb{F}_K[x]$$

$$\tilde{P}'(b_j) = 0 \text{ en } \mathbb{F}_L$$

$\tilde{P}'(b_j) \neq 0$  (si fuese cero)

$$p(b_j) = 0 \text{ en } \mathcal{O}_L$$

$$p(b_j)' \neq 0 \text{ en } \mathcal{O}_L$$

Por lo tanto:

$$\exists M \text{ raiz de } p(x) = 0 \text{ en } \mathcal{O}_L, M \equiv b_j \left( \frac{\sigma}{M} = c \right)$$

Si  $\bar{p}(x)$  irred  $\Rightarrow p(x)$  irred en  $\mathcal{O}_L$  (teorema de Gauss)

(en el cuerpo) (en el anillo de enteros)

$$\text{Así, si } E := K[M], [E : K] = \frac{[E : \bar{p}]}{[\bar{p} : K]} = [\mathbb{F}_L : \mathbb{F}_K]$$

Podemos suponer:

$$\{b_0, \dots, b_t\}, b_i = h_i(M), \text{ con } 2h_i < 2p, h_i \text{ concavas en } \{\bar{a}_0, \dots, \bar{a}_r\}$$

$$\Rightarrow p \in L \Rightarrow \sum_{i=-n}^{\infty} h_i(M) \pi^i = f(M), f \text{ polinomio}$$

$\therefore E = L$  (pues  $L \subseteq E$  por lo anterior y  $r(M)$  tiene coef. en  $K \subseteq L \cap M \cap L \therefore E \subseteq L$ )

$$\therefore [L : K] = [\mathbb{F}_L : \mathbb{F}_K]$$

2) Supongamos  $\mathbb{F}_L = \mathbb{F}_K$ ,  $\pi_L$  un factorante en  $L$ ,  $\pi_K$  unitario.

$\therefore \pi_K \in L$   $\leftarrow$  índice de ramificación

$$\therefore \pi_K = n \pi_L^e \quad \text{Algun } e > 1 \quad (\text{s: } c=1 \Rightarrow L = K \text{?} \text{ (*)})$$

$$\text{Sea } p(x) = \text{irr}_{\mathbb{F}_L, K}(x)$$

$$\text{Si } d \in K \text{ enton } \alpha = \sum_{i=-n}^{\infty} a_i \pi_L^i = \sum_i a_i \pi_K^i \quad \checkmark \text{ notación}$$

$$\text{y si } \beta \in L \text{ entonces } \beta = \sum_{i=-n}^{\infty} b_i \pi_L^i$$

$$\text{digamos } \pi_i = \pi_K^r \pi_L^t, \text{ con } 0 \leq t \leq e$$

$$\text{Así: } \beta = \sum_{t=0}^{e-1} \left( \sum_{r=0}^e (b_r \pi_K^r \pi_L^t) \right) \pi_L^t = \sum_{t=0}^{e-1} \beta_t \pi_L^t$$

$$\therefore 2p = e / (\text{lon } \beta \text{ dividido entre } \beta_t \text{ para } t = 0, \dots, e-1)$$

$\begin{cases} L \\ K \end{cases}$  ramificadas  $\Rightarrow$  Si  $F_L = F_K$  la extensión es t-ramificada.  
 $L$  ramificada  $\Rightarrow$  Si  $F_L \neq F_K$  no ramificada.

Ejemplo:  $L = \mathbb{Q}(x)$  y  $K = \mathbb{Q}(x^2)$   
 $L/K$  es una extensión de cuadrática.  
 $L/K$  es una extensión de cuadrática.  
 $L/K$  es una extensión de cuadrática.

Entonces  $L \subseteq K$  es la interfaz de  $L$

obs: si  $N$  es reticulado y  $L \subseteq K$  es la interfaz de  $L$  es reticulado.

para algún  $a \in L$  entonces  $\sigma(a) = a$

$$\begin{aligned}
 & \text{1) } N \cong \mathbb{Z}^2 \\
 & \text{2) } N \hookrightarrow \mathbb{Z}^2 \Rightarrow N \cong \mathbb{Z}^2 \text{ o } N \cong \langle 1, \sigma \rangle \\
 & \text{3) } N \cong \langle 1, \sigma \rangle \Rightarrow \Psi: \mathbb{Z}^3 \rightarrow \mathbb{Z}^2 \text{ la trastación}
 \end{aligned}$$

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

dónde  $\Psi(a) = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \Psi(b) = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$  y definimos  $\Psi: \mathbb{Z}^2 \rightarrow \mathbb{Z}^3$

$$\Psi \circ \Psi = \text{id}_{\mathbb{Z}^2}$$

$$\text{Sea } N = \ker \Psi, v \in \mathbb{Z}^3, v - \Psi(u) \in N$$

$$\text{pues: } \Psi(v - \Psi(u)) = \Psi(v) - \underbrace{\Psi(\Psi(u))}_{\text{id}} = 0$$

$$\therefore v = \underbrace{(v - \Psi(u))}_{N} + \underbrace{\Psi(u)}_{\in \text{Im } \Psi}, w \in N \cap \text{Im } \Psi \Rightarrow w = \Psi(u) \Rightarrow \Psi(w) = 0 \Rightarrow u = 0$$

$\Rightarrow w = 0 \therefore \mathbb{Z}^3 = \ker \Psi \oplus \text{Im } \Psi$   
 si  $\Psi$  inyectiva  $\Rightarrow \text{Im } \Psi = \mathbb{Z}^3 \Rightarrow \mathbb{Z}^3$  gen. por dos elementos. ( $\mathbb{Z}^3$  es finitamente generado por 2 elementos).

$$(\mathbb{Z}^3)^* \cong (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/3\mathbb{Z} \cong (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/3\mathbb{Z}$$

Si  $\psi: \mathbb{Z}^3 \hookrightarrow \mathbb{Z}^2$

$e_1, e_2, e_3$  son l.i. en  $\mathbb{Z}^2 \Rightarrow$  linealmente indep. en  $\mathbb{Z}^2$

Nueva definición:

Sea  $K$  un cuerpo de números reticulado en  $K^n$  es un  $\mathbb{Z}$ -submódulo  $\Lambda$  de  $K^n$  tal que existen  $\alpha, \beta \in K^*$  tales que:

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

Proposición 1: Si  $\Lambda$  y  $\Lambda'$  son reticulados en  $K^n$ , entonces  $\Lambda_p = \Lambda'_p$  para casi todos  $p$ .

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

Proposición 3: Si  $\{\Lambda(p)\}_{p \in \text{Primes}}$  es una familia de reticulados de  $N(p)$  en  $(\mathbb{Z}/p\mathbb{Z})^n = A(p) = \Lambda'(p)$  para casi todos  $p$  y el reticulado  $\Lambda'$  fijo,

entonces existen reticulados  $\Lambda$  con  $\Lambda_p = \Lambda(p)$  para todos  $p$ .

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

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

Sea  $\Lambda$  un reticulado en  $K^n \cong (\mathbb{Z}/n\mathbb{Z})^n = N$

Además lo anterior:  $\mathcal{O}_K^n \cong \mathbb{Z}^n$

Si  $\mathcal{O}_K$  reticulado pol:  $\mathcal{O}_K$  reticulado  $\Rightarrow \mathcal{O}_K^n$  reticulado

Bastarán que existan  $\alpha, \beta \in \mathbb{Z}$  tales que:  $\beta \mathcal{O}_K \subseteq \alpha \mathcal{O}_K \subseteq \mathcal{O}_K$

Ejercicio: Si  $\alpha$  es algebraico  $\exists n \in \mathbb{N}^*$ :  $n\alpha \in \mathbb{Z}$

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

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

Si  $m \in \mathbb{Z}$  entero  $\Rightarrow \mathcal{O}_K \subseteq m\mathcal{O}_K \Rightarrow m\mathcal{O}_K \subseteq \alpha \mathcal{O}_K$

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

obs:  $\Lambda$  ret en  $K^n$  y  $\Lambda'$  ret en  $K^m$   $\Rightarrow \Lambda \times \Lambda'$  es ret en  $K^{n+m}$ .

$$\text{Si } \Lambda \text{ ret en } K^n \Rightarrow \alpha \in \Lambda \subseteq \beta \in K^n$$

$$\Lambda' \text{ || } \Rightarrow \alpha' \in \Lambda' \subseteq \beta' \in K^m$$

Bastarán pedir dos  $\alpha, \alpha' \in K$  existe  $\alpha'' \in K$  con  $\alpha'' \in \alpha \in \alpha'$   $\alpha'' \in \alpha' \in K$

Existen  $n, m \in \mathbb{N}^*$  tales que  $\alpha \in \alpha' \in \dots \in \alpha^n \in \alpha^{n+m} \in \alpha^{n+m+1} \in K$   
también  $n, m \in \mathbb{N}^*$  tales que  $\alpha' \in \alpha'' \in \dots \in \alpha'^m \in \alpha'^{n+m} \in \alpha'^{n+m+1} \in K$

Entonces  $\alpha^n \in \alpha'^m \in K$  similitamente:  $n \in \alpha \subseteq \alpha' \subseteq K$ .

$\therefore n \in \alpha \subseteq \alpha' \subseteq K$

$$\text{Si: } \alpha'' \in \alpha^n \times \alpha'^m \subseteq \Lambda \times \Lambda' \subseteq \Lambda \times \Lambda'$$

$$\alpha'' \in (\alpha \times \alpha') \subseteq \Lambda \times \Lambda'$$

Por lo tanto  $\alpha'' \in \Lambda \times \Lambda'$  es completo,  $\mathcal{P}$  es nulo de

Si  $\mathcal{P}$  es uniformemente  $K$ -p.  $\mathcal{P}$  es completo,  $\mathcal{P}$  es nulo de

uniforme de  $K$ .  $\mathcal{P}$  es nulo absoluto en  $K \Rightarrow \int_{\mathcal{P}} f = \int_{\mathcal{P}} g$

Resumir la parte sobre  $\mathcal{P}$ .

$$K_p = K \otimes_{\mathbb{Q}} \mathbb{Q}_p, K = \frac{\mathbb{Q}(t)}{(f)}, K_p = \frac{\mathbb{Q}_p[t]}{(f)}, f = f_1 \dots, f_r$$

$$K_p \cong \frac{\mathbb{Q}_p(t)}{(f_1)} \times \dots \times \frac{\mathbb{Q}_p(t)}{(f_r)}$$

$$\cong K_{p_1} \times \dots \times K_{p_r}$$

Si  $\Lambda$  es reticulado en  $K^n$ ,  $\Lambda \subseteq \Lambda'$  es reticulado en  $K_p^n \cong \mathbb{Q}_p^N$

Apesar de que  $K_p^n \cong K_{p_1}^n \times \dots \times K_{p_r}^n$   $\Lambda$  es reticulado en  $K_p^n$ .

Sea  $\mathcal{O}_p = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathbb{Z}_p$  Se puede probar que  $\mathcal{O}_p = \mathcal{O}_{p_1} \times \dots \times \mathcal{O}_{p_r}$

Si  $\Lambda$  es  $\mathcal{O}_p$  reticulado  $\mathcal{O}_p \Lambda \subseteq \Lambda$

$$\Lambda \supseteq P_1 \Lambda \subseteq P_1 K^n = K_{p_1}^n \text{ (reticulado)} \Rightarrow \Lambda \subseteq \mathcal{O}_{p_1}$$

$$\Lambda = P_1 \Lambda \times \dots \times P_r \Lambda = (\mathbb{Z}_{p_1})^r = \mathbb{Z}^r$$

donde  $P_i \Lambda$  es reticulado en  $K^n$ .

p.  $\Lambda_p = \Lambda_{p_i} \leftarrow$  completando en  $p_i$ .

$$\bar{\Lambda}_{\sigma_K \text{ ret}} \xrightarrow{\text{aciso}} \{\Lambda_p, \text{Optimalizado}\}_{p \in \Pi_f(k)}$$

prop1:  $\lambda, \lambda' \in \mathbb{K}^n$ ,  $\lambda_p = \lambda_p'$  para casi todos  $p$ .

prop2:  $\exists \lambda_p = \lambda'_p \forall p$   $\Rightarrow \lambda = \lambda'$

prop3: Si para cada  $p \in \Pi_f(k)$  se tiene un reticulado  $\Lambda(p)$  con  $\Lambda(p) = \Lambda_p$  para casi todos  $p$  y un reticulado fijo  $\lambda'$ ,

entonces existe un reticulado  $\Lambda$  con  $\Lambda(p) = \Lambda(p)$ ,  $\forall p \in \Pi_f(k)$ .

Prop: Sea  $I$  un ideal de  $\sigma_K$  ( $K/\mathbb{Q}$  ext cuadrática).

entonces existen  $\alpha, \beta \in \sigma_K$  tales que  $I = (\alpha, \beta)$ .

Defin: otras;  $I$  es ideal,  $\alpha \in I$ ,  $\alpha \in \sigma_K \subset I \subset \sigma_K \Rightarrow I$  reticulado.

Sea  $J = \alpha \sigma_K \cap \sigma_K \Pi_f(k)$ , así  $J_p = \alpha \sigma_p \subset I_p$ .

ademas  $J_p = I_p$  para casi todos  $p$ . Sean  $p_1, \dots, p_s$  dupares donde:

$$J_{p_i} \subsetneq J_p$$

Sea  $\pi_i \in \sigma_{p_i}$  parametriza uniformemente.

$$I_{p_i} = (\pi_i, \pi_i) \quad J_{p_i} = (\alpha)$$

así:  $v_{p_i}(\alpha) > t_i$

Sean  $q_1, \dots, q_s$  dupares donde  $J_{q_j} = I_{q_j}$ ,  $I_{q_j} \neq \sigma_{q_j}$ .

Escogemos  $\beta \in K$  tal que:  $v_{p_i}(\beta) = t_i$ ,  $i = 1, \dots, s$

$$v_{q_j}(\beta) > v_{q_j}(\alpha), \quad j = 1, \dots, l$$

Afirmación:  $I = (\alpha, \beta)$

Sea  $I' = (\alpha, \beta)$  basta ver que:  $I_p = I'_{p_i}$ ,  $\forall p$ .

Si  $p = p_i \Rightarrow I'_{p_i} = (\pi_i, \pi_i) = (\beta)$

$$I'_{p_i} = (\alpha, \beta) = (\beta) = I_{p_i}$$

Si:  $p = \mathfrak{q}_j$

$$I_{\mathfrak{q}_j} = \mathfrak{q}_j = (\alpha)$$

$$I'_{\mathfrak{q}_j} = (\alpha) + (\beta) = (\alpha) = I_{\mathfrak{q}_j}$$

Si:  $p$  es en otro lugar:

$$(\alpha) = I_p = I_R = \mathcal{O}_R$$

$$I'_{\mathfrak{p}} = (\alpha) + (\beta) = \mathcal{O}_R = I_R$$

Ejercicio: 1) Dibujar que  $\mathfrak{p} \in K$  es un entero ssi  $\mathfrak{p}_p(\alpha) \leq 1$  para todo lugar

$\mathfrak{p} \in \prod_{\mathfrak{f} \in K}$  ideal,  $I_{\mathfrak{p}}$  paracaido  $\mathfrak{p}$  basta considerar

$$\underline{\text{obs}}: \quad I \subseteq \mathcal{O}_{\mathfrak{K}} \text{ ideal}, \quad I_{\mathfrak{p}} = (\prod_{\mathfrak{f} \in \mathfrak{K}} \mathfrak{m}_{\mathfrak{f}})^{v_{\mathfrak{f}}(I)}$$

$$\mathfrak{m}(\mathfrak{p}) \subseteq \mathcal{O}_{\mathfrak{K}} \text{ ideal}$$

$$\mathfrak{m}(\mathfrak{p})_{\mathfrak{p}} = (\mathfrak{p})$$

$$\mathfrak{m}(\mathfrak{p})_{\mathfrak{f}} = \mathfrak{O}_{\mathfrak{f}} \text{ si } \mathfrak{f} \neq \mathfrak{p} \text{ y } \mathfrak{m}(\mathfrak{p}) \text{ es ideal maximal.}$$

2)  $I \subseteq \mathcal{O}_{\mathfrak{K}}$  es ideal ssi  $I_{\mathfrak{p}} \subseteq \mathcal{O}_{\mathfrak{p}}$  ideal  $\forall \mathfrak{p}$ .

3)  $I, J$  ideales,  $I, J \subseteq \mathcal{O}_{\mathfrak{K}}$  enteros

$$(IJ)_{\mathfrak{p}} = I_{\mathfrak{p}} J_{\mathfrak{p}}$$

$$\text{Aví definimos: } I' = \prod_{\mathfrak{f} \in \prod_{\mathfrak{f} \in K}} \mathfrak{m}(\mathfrak{f})^{v_{\mathfrak{f}}(I)} = (\prod_{\mathfrak{f} \in K} \mathfrak{m}_{\mathfrak{f}})^{v_{\mathfrak{f}}(I)} = I^{\#}$$

$$I'_{\mathfrak{p}} = \mathfrak{m}(\mathfrak{f})^{v_{\mathfrak{f}}(I)} = (\mathfrak{p})$$

Entonces  $I' = I$ . Esto es lo que queríamos.

Por tanto  $I' = I$  es el ideal de los enteros de  $\mathcal{O}_{\mathfrak{K}}$ .

Entonces  $I' = I$  es el ideal de los enteros de  $\mathcal{O}_{\mathfrak{K}}$ .

Entonces  $I' = I$  es el ideal de los enteros de  $\mathcal{O}_{\mathfrak{K}}$ .

Entonces  $I' = I$  es el ideal de los enteros de  $\mathcal{O}_{\mathfrak{K}}$ .

Entonces  $I' = I$  es el ideal de los enteros de  $\mathcal{O}_{\mathfrak{K}}$ .

Lema: Sean  $K$  un cuerpo de números y sean  $I, J$  ideales en  $\mathcal{O}_K$  tales que para cada lugar finito  $\mathfrak{p}$ ,  $I_{\mathfrak{p}} \oplus J_{\mathfrak{p}}$  es  $\mathcal{O}_{\mathfrak{p}}$ .

Entonces  $I + J = \mathcal{O}_K$

Dem:  $(I + J)_{\mathfrak{p}} \stackrel{(*)}{=} I_{\mathfrak{p}} + J_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}$

Luego  $I + J = \mathcal{O}_K$

(\*) Se cumple pues  $I + J$  es el menor ideal que contiene a  $I$  y  $J$  tanto local como globalmente.

Lema: Si  $p_1, \dots, p_r, q_1, \dots, q_s$  son lugares distintos y tomamos  $x_i \in \mathcal{O}_{p_i}^*$ ,  $\alpha_j \in m_{q_j}$ ,  $\beta_i \in m_{p_i}$ ,  $\beta_j \in \mathcal{O}_{q_j}^*$  satisface  $\alpha_i x_i + \beta_j x_j = 1$  si y solo si existe  $\gamma \in \mathcal{O}_K$  tal que  $\alpha_i - \gamma p_i \in \mathcal{O}_{p_i}^*$  y  $\beta_j - \gamma q_j \in \mathcal{O}_{q_j}^*$ .

Entonces existe  $\gamma \in \mathcal{O}_K$  tal que  $\alpha_i - \gamma p_i \in \mathcal{O}_{p_i}^*$  y  $\beta_j - \gamma q_j \in \mathcal{O}_{q_j}^*$ .

$$1) |\alpha - \gamma p_i|_{p_i} < \varepsilon, |\alpha - \gamma p_i|_{q_j} < \varepsilon$$

$$2) |\beta - \gamma q_j|_{p_i} < \varepsilon, |\beta - \gamma q_j|_{q_j} < \varepsilon$$

$$3) (\alpha) + (\beta) = 1$$

Supongamos  $\varepsilon \in (0, 1)$ :

Dem: Se usa el teorema de aproximación para encontrar  $\alpha$  que cumple 1.

que cumple 2.

Luego se usa el teo. de aproximación para encontrar  $\beta$  que cumple 2 de modo que  $|\beta - 1|_{p_i} < 1 \quad \forall i \neq p_i, q_j$  donde  $|\alpha|_{p_i} < 1$ . ← exigencias.

$$\text{Si } p_i = p_j: (\alpha)_{p_i} + (\beta)_{p_i} = (\alpha_i)_{p_i} + (\beta)_{p_i} = (1)_{p_i}.$$

$$\text{Si } p_i \neq p_j, q_j: (\alpha)_{p_i} + (\beta)_{p_i} = (\alpha)_{q_j} + (\beta)_{q_j} = (1)_{q_j}.$$

$$\text{Si } p_i \neq q_j, p_i: |\alpha|_{p_i} = |\beta|_{p_i} \Rightarrow |\alpha|_{p_i} = |\beta|_{p_i} < 1$$

$$\Rightarrow |\beta|_{p_i} = |1|_{p_i} \Rightarrow (\beta)_{p_i} = \mathcal{O}_{p_i} = (1)_{p_i} \therefore (\alpha)_{p_i} + (\beta)_{p_i} = 1.$$

$$\text{Si } \alpha \neq \beta_1, \beta_2 \quad (\alpha)_{\beta} = 1$$

$$(\alpha)_{\beta} + (\beta)_{\beta} = (1)_{\beta} + (\beta)_{\beta} = (1)_{\beta}$$

$$\text{Luego: } (\alpha) + (\beta) = (1)$$

Definimos  $SL_n(k) = \{ \pi \in M_n(k) \mid \det \pi = 1 \}$

Hecho: Este grupo es generado por las matrices elementales.

$$\text{Si } n=2: \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}. \quad SL_2(\sigma_k) = SL_2(k) \cap M_2(\sigma_k)$$

(grado pues  $\pi^{-1} = \frac{1}{\det \pi} \text{adj} \pi = \text{adj} \pi$  tiene coef. enteros)

Tercera parte Aproximación para  $SL_n(k)$ :

Sean  $\alpha_1, \dots, \alpha_r \in \Pi(k)$ .

$A_i \in SL_n(k\alpha_i)$ ,  $i=1, \dots, r$ . Si  $\epsilon > 0$ .

Entonces existe  $\lambda \in SL_n(k)$  tal que:

$$1) |A - A_i|_{\alpha_i} < \epsilon$$

$$2) A \in SL_n(\sigma_k), \alpha \neq \alpha_1, \dots, \alpha_r$$

Demostración:  $n=2$ . Basta aproximar los generadores.

Sin pérdida de generalidad:  $\alpha_i$  es una matriz elemental y  $A_i = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Caso 1:  $A_1 = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$ ,  $A_2 = \dots = A_r = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Basta aproximar  $\lambda$  usando el T.T. de Aprox. fuerte en  $k$ .

Basta aproximar  $\lambda$  usando el T.T. de Aprox. fuerte en  $k$  ( $i=2, \dots, r$ ) sobre cuerpos distintos.

$$A = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$$

Caso 2:  $A_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ ,  $A_2 = \dots = A_r = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Buscamos  $\alpha$  en  $k$ :  $|\alpha|_{\alpha_1} < \epsilon$ ,  $|\alpha - 1|_{\alpha_1} < \epsilon$ ,  $|\alpha|_{\alpha_i} < \epsilon$  para  $i=2, \dots, r$ ,  $(\alpha) + (1) = (1)$ .

$$\text{entonces } (\alpha^i) + (\beta^i) = 1$$

$$\exists s, t : \alpha^i t + \beta^i s = 1.$$

$$A = \begin{pmatrix} \alpha & \beta \\ -\beta s & \alpha t \end{pmatrix}, \det A = 1$$

Entonces en  $\mathbb{R}^2$ :  $\alpha \approx 0, \beta \approx 1$  ( $\alpha^i t + \beta^i s \approx 1$ )

$$A \sim \begin{pmatrix} 0 & 1 \\ -s & t \end{pmatrix}$$

$$\text{Caso I: } 1 = \alpha^i t + \beta^i s \approx s \Rightarrow A \sim \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

$$\text{En } A \sim \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ pues } 1 = \alpha^i t + \beta^i s \text{ nt.}$$

$$\underline{\text{Caso III}}. \quad A_1 = \begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix}, \quad A_2 = \dots = A_r = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \quad \text{si } e \in \mathbb{O}^*$$

$$|\alpha - u|_{\mathbb{R}^2} < \varepsilon, \quad |\beta|_{\mathbb{R}^2} \leq \varepsilon.$$

$$i \neq 1 \quad |\alpha - 1|_{\mathbb{R}^2} < \varepsilon, \quad |\beta|_{\mathbb{R}^2} < \varepsilon$$

$$(\alpha) + (\beta) = 1 \quad \text{entonces: } \alpha^i t + \beta^i s = 1.$$

$$A = \begin{pmatrix} \alpha & \beta \\ -\beta s & \alpha t \end{pmatrix} \sim \begin{pmatrix} u & 0 \\ 0 & ut \end{pmatrix}, \quad \text{pero: } \frac{u^i t}{ut - u^{-1}} \approx 1$$

$$\text{en } \mathbb{R}^2: \quad A \sim \begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\text{en } \mathbb{R}^2: \quad A \sim \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ pues } t \in \mathbb{R}.$$

Cualquier  $\lambda \in \mathbb{K} \setminus \mathbb{R}$ :  $\alpha = \lambda \pi t, t \in \mathbb{R}$ ,  $\pi$  uniformizante.

$$\underline{\text{Caso IV}}. \quad A_1 = \begin{pmatrix} \pi & 0 \\ 0 & \pi^{-1} \end{pmatrix}, \quad A_2 = \dots = A_r = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \text{si } e \in \mathbb{O}^*$$

$$\text{pero: } \begin{pmatrix} \pi & 0 \\ 0 & \pi^{-1} \end{pmatrix} = \begin{pmatrix} \pi & 0 \\ \pi^{-1} & \pi^{-1} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} \pi & 0 \\ \pi & \pi^{-1} \end{pmatrix}$$

$$\text{Si: } \lambda = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} \pi & 0 \\ \pi & \pi^{-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} \pi & -\pi^{-1} \\ \pi & 0 \end{pmatrix} \begin{pmatrix} 1 & \pi^{-2} \\ 0 & 1 \end{pmatrix}$$

$$\text{Si: } \beta \neq 0 \text{ y } \beta \neq 1 \text{ (ya que: } \beta = 1 \Rightarrow \lambda = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ y } \beta = 0 \Rightarrow \lambda = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix})$$

$$\Rightarrow |\beta|_{\mathbb{R}^2} = 1 \text{ (ya que: } \beta = 1 \Rightarrow \lambda = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ y } \beta = 0 \Rightarrow \lambda = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix})$$

$$\begin{pmatrix} \pi & 0 \\ 0 & \pi^{-1} \end{pmatrix} \sim \begin{pmatrix} \pi & 0 \\ \pi^{-1} & \pi \end{pmatrix} \sim \begin{pmatrix} 1+\pi & 1 \\ \pi^{-1} & \pi^{-1} \end{pmatrix}$$

$$\sim \begin{pmatrix} 1+\pi & 1 \\ 0 & \pi^{-1} - (1+\pi)^{-1}\pi^{-1} \end{pmatrix} \sim \begin{pmatrix} 1+\pi & 1 \\ 0 & (1+\pi)^{-1} \end{pmatrix}$$

$$\sim \begin{pmatrix} 1+\pi & 0 \\ 0 & (1+\pi)^{-1} \end{pmatrix} \quad \text{(cae en el caso III.)}$$

↑ unidimensional

$$= \pi \begin{pmatrix} 1 & \frac{1}{1+\pi} \\ 0 & 1 \end{pmatrix}$$

$$= \frac{1}{\pi+1}$$

$$(1+\pi) = 1 \text{ (Luego } 1+\pi \in \sigma_{\mathcal{P}}^+)$$

Ejemplo:  $I \subseteq \mathcal{O}_K$  ideal.  $I \subseteq K$  ideal-fraccionario. ( $\alpha I$  ideal en  $\mathcal{O}_K$  algun  $\alpha \in \mathcal{O}_K$ )

$$I = \prod_{P \in \mathcal{P}(K)} M(P)^{\alpha_P} \quad \text{M(P) ideal maximal correspondiente a P}$$

$$M(P) = \begin{cases} (\pi), & \text{si } P = \pi, \\ (1), & \text{si no} \end{cases}$$

$$\Lambda = I \times J \text{ reticulado en } K^2, \quad I, J \text{ ideales.} \quad \mathcal{O}_K' = \left\{ \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \alpha, \beta \in \mathcal{O}_K \right\}.$$

$$\text{Localmente } \Lambda_{P_i} = A_i \mathcal{O}_{P_i}^2, \quad A_i = \begin{pmatrix} \alpha_i & 0 \\ 0 & \beta_i \end{pmatrix}, \quad \begin{array}{l} I_{P_i} = (\alpha_i) \\ J_{P_i} = (\beta_i) \end{array} \quad \begin{array}{l} \text{lugares donde} \\ \Lambda_{P_i} + \mathcal{O}_K' \end{array}$$

(de hecho  $\alpha_i = \pi_{P_i} \alpha_i$ ,  $\beta_i = \pi_{P_i} \beta_i$ )

$$\text{Sea } B_i = \begin{pmatrix} \alpha_i^{-1} & 0 \\ 0 & \beta_i \end{pmatrix}, \quad \det B_i = 1.$$

Sea B una matriz que sea:

$$1) |B - B_i|_P < \varepsilon, \quad i = 1, \dots, r$$

$$2) B \in SL_2(\mathcal{O}_K), \quad \text{si } P \neq P_1, \dots, P_r$$

$$\text{entonces se:} \quad \Lambda' = B \Lambda$$

obs: 1)  $\Lambda' \cong \Lambda$  como  $\mathcal{O}_K$ -módulo.

2) Si  $B \in SL_2(\mathcal{O}_K)$  (ojo: si  $P \neq P_1, \dots, P_r$ )

$$\Lambda_P = B \Lambda_P = B \mathcal{O}_{P^2} = \mathcal{O}_{P^2}.$$

3) Si  $\varepsilon < 1$ .  $\Lambda'_P = B \Lambda_P = B_i \Lambda_{P_i} \quad \text{falta explicación.}$

(\*)