

Teoría de Números

Desarrollo tarea #2
por Marco Godoy V.¹



- **Problema 1.** Calcule el máximo común divisor de 1701 y 2240.

- *Desarrollo.* Tenemos por algoritmo de la división

$$\begin{aligned}2240 &= 1701 \cdot 1 + 539 \\1701 &= 539 \cdot 3 + 84 \\539 &= 84 \cdot 6 + 35 \\84 &= 35 \cdot 2 + 14 \\35 &= 14 \cdot 2 + 7 \\14 &= 7 \cdot 2 + 0\end{aligned}$$

$$\therefore \quad mcd(1701, 2240) = 7$$

$$\begin{array}{c|c} & 12 \\ 1 & | 12 \\ 2 & | 12 \\ 3 & | 11 \\ 4 & | 12 \\ 5 & | 12 \end{array}$$

- **Problema 2.** Resuelva el sistema siguiente:

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

- *Desarrollo.* Con un poco de álgebra vemos que el sistema se puede dejar de la forma equivalente

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

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

$$\begin{cases} x \equiv 4(7) \\ x \equiv 9(11) \\ x \equiv 1(23) \end{cases} \quad \begin{cases} x \equiv 4(11) \\ x \equiv 9(17) \\ x \equiv 22(23) \end{cases}$$

Primero buscamos las soluciones de $\begin{cases} x \equiv 4(7) \\ x \equiv 9(11) \\ x \equiv 1(23) \end{cases}$. Como

$$1 = 7 \cdot 8 + 11 \cdot (-5)$$

¹Dirección de e-mail: marco.godoy@ug.uchile.cl

entonces la solución de $\begin{cases} x \equiv 4(7) \\ x \equiv 9(11) \end{cases}$ módulo $7 \cdot 11$ es la siguiente

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

$$\therefore x \equiv 53 \pmod{7 \cdot 11}$$

Ahora pasamos al siguiente sistema $\begin{cases} x \equiv 53(7 \cdot 11) \\ x \equiv 1(23) \end{cases}$. Ocupando el algoritmo de la división, 1 se escribe como combinación lineal entera de 23 y 77 ($77 = 7 \cdot 11$):

$$\begin{aligned} 77 &= 23 \cdot 3 + 8 \\ 23 &= 8 \cdot 2 + 7 \\ 8 &= 7 \cdot 1 + 1 \end{aligned}$$

\Rightarrow

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

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

La solución de $\begin{cases} x \equiv 53(7 \cdot 11) \\ x \equiv 1(23) \end{cases}$ módulo $7 \cdot 11 \cdot 23$ es

$$\begin{aligned} x &\equiv 77 \cdot 3 \cdot 1 + 23 \cdot (-10) \cdot 53 \\ &\equiv 77 \cdot 3 - 23 \cdot 53 \cdot 10 \\ &\equiv 231 - 12190 \\ &\equiv -11959 \\ &\equiv -10626 - 1333 \\ &\equiv -1771 \cdot 6 - 1333 \\ &\equiv -1333 \\ &\equiv 438 \end{aligned}$$

$$\therefore x \equiv 438 \pmod{7 \cdot 11 \cdot 23}$$

Como $\begin{cases} x \equiv 4(7) \\ x \equiv 9(11) \end{cases}$ implica $x \equiv 53(7 \cdot 11)$, entonces sólo falta resolver

$$\begin{cases} x \equiv 53(7 \cdot 11) \\ x \equiv 22(23) \end{cases}$$

Por el cálculo anterior, inmediatamente tenemos su solución, módulo $7 \cdot 11 \cdot 23$:

$$\begin{aligned} x &\equiv 77 \cdot 3 \cdot 22 + 23 \cdot (-10) \cdot 53 \\ &\equiv 5082 - 12190 \\ &\equiv -7108 \\ &\equiv -7084 - 24 \\ &\equiv -1771 \cdot 4 - 24 \\ &\equiv -24 \\ &\equiv 1747 \end{aligned}$$



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

Por lo tanto, las soluciones del sistema son

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

- **Problema 3.** Demuestre que si $\eta = e^{2\pi i/5}$, entonces $\eta^2 + 1$ es una unidad y $\eta + 3$ es un primo en $\mathbb{Z}[\eta]$. Recuerde que el polinomio irreducible de η es $(x^5 - 1)/(x - 1)$.

- *Demostración.* Es evidente que $\eta^2 + 1$ es unidad en $\mathbb{Z}[\eta]$ ssi $(\eta^2 + 1) = \mathbb{Z}[\eta]$. Así bastaría demostrar que $\mathbb{Z}[\eta]/(\eta^2 + 1)$ es el anillo trivial $\{0\}$.

En efecto

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

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

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

Ahora para demostrar que $\eta + 3$ es primo en $\mathbb{Z}[\eta]$ es necesario y suficiente demostrar que $(\eta + 3)$ es un ideal primo, o dicho en otras palabras, $\mathbb{Z}[\eta]/(\eta + 3)$ es dominio de integridad.

$$\begin{aligned}
 \frac{\mathbb{Z}[\eta]}{(\eta + 3)} &\cong \frac{\mathbb{Z}[x]}{\left(\frac{x^5 - 1}{x - 1}, x + 3\right)} \\
 &\cong \frac{\mathbb{Z}[-3]}{\left(\frac{(-3)^5 - 1}{-3 - 1}, (-3) + 3\right)} \quad (\text{evaluación en } x = -3, \text{raíz de } x + 3 \in \mathbb{Z}[x] \text{ irreducible}) \\
 &\cong \frac{\mathbb{Z}[i]}{\left(\frac{-3^5 - 1}{-3 - 1}, 0\right)} \\
 &\cong \frac{\mathbb{Z}[i]}{\left(\frac{3^5 + 1}{3 + 1}\right)} \quad \text{Z, no } \mathbb{Z}[i] \\
 &\cong \frac{\mathbb{Z}[i]}{(3^4 - 3^3 + 3^2 - 3 + 1)} \\
 &\cong \frac{\mathbb{Z}[i]}{(61)} \\
 &\cong \mathbb{F}_{61} \quad (\text{Cuerpo (dominio de integridad) con 61 elementos})
 \end{aligned}$$

$$\therefore \mathbb{Z}[\eta]/(\eta + 3) \cong \mathbb{F}_{61}$$

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

- **Problema 4.** Determine cuantas soluciones tiene la ecuación $x^{50} = 1$ en el anillo $\mathbb{Z}/1296\mathbb{Z}$. Justifique. Observe que $1296 = 6^4$.

- *Desarrollo.* Como $6^4 = 2^4 \cdot 3^4$, el teorema chino de los restos dice que resolver la ecuación $x^{50} \equiv 1 \pmod{6^4}$ es equivalente a resolver el sistema

$$\begin{cases} x^{50} \equiv 1(2^4) \\ x^{50} \equiv 1(3^4) \end{cases}$$

Primero afirmamos que las ecuaciones $x^{50} \equiv 1(3^4)$ y $x^{50} \equiv 1(2^4)$ comparten el mismo número de soluciones. En efecto, si x_0 es solución de $x^{50} \equiv 1(3^4)$ entonces obviamente $x_0^{50} \equiv 1(3)$ ($x_0^{50} = 1 + 3 \cdot 3^3y$, $y \in \mathbb{Z}$). Ahora para tener las soluciones de $x^{50} \equiv 1(3)$, veamos que se cumple $x^2 \equiv 1(3)$ (Fermat), en particular $x^{48} \equiv 1(3)$; luego $x^{50} \equiv x^2 \equiv 1(3)$. Las soluciones de $x^2 \equiv 1(3)$ son $x_0 \equiv 1, 2(3)$. Aplicando el lema de Hensel a cada una de estas soluciones, tenemos que existen dos soluciones, congruentes a 1 y 2 módulo 3 respectivamente, para $x^{50} \equiv 1(3^4)$.

Ahora nos falta encontrar el número de soluciones de $x^{50} \equiv 1(2^4)$. Como $(\mathbb{Z}/2^4\mathbb{Z})^*$ es el producto directo de dos grupos cíclicos, uno de orden 2 y uno orden $2^2 = 4$. Entonces

$$(\mathbb{Z}/2^4\mathbb{Z})^* \cong (\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^*$$

Luego basta saber el número de soluciones del sistema

$$\begin{cases} x^{50} \equiv 1(3) \\ x^{50} \equiv 1(5) \end{cases}$$

Antes, no olvidemos que $x^2 \equiv 1(3)$, $x^4 \equiv 1(5)$ (y con ello $x^{48} \equiv 1(5)$), quedando el sistema anterior reducido a uno de forma más simple:

$$\begin{cases} x^2 \equiv 1(3) \\ x^2 \equiv 1(5) \end{cases}$$

En resumen, como $x^2 \equiv 1(5)$ tiene dos soluciones, $x^2 \equiv 1(3)$ tiene dos soluciones y $x^{50} \equiv 1(3^4)$ tiene 2 soluciones, entonces por el teorema chino de los restos, $x^{50} \equiv 1(6^4)$ tiene 8 soluciones.

- **Problema 5.** Encuentre el inverso de la clase $\overline{1+i}$ en el anillo cociente $\mathbb{Z}[i]/(2+i)$.

- *Desarrollo.* Primero veamos que

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

Como \mathbb{F}_5 es el cuerpo con 5 elementos, entonces para todo $x \in \mathbb{F}_5^*$, $x^4 = 1$. Entonces queda claro que $\overline{1+i}$ debe tener orden 4 en $(\mathbb{Z}[i]/(2+i))^*$, es decir, $\overline{1+i}^{-1} = \overline{1+i}^3$. Comprobemos que efectivamente esto es cierto:

$$\begin{aligned}(1+i)^3 &= 1 + 3i + 3i^2 + i^3 \\&= 1 + 3i - 3 - i \\&= -2 + 2i \\(1+i)^4 &= (-2+2i)(1+i) \\&= -2 - 2i + 2i + 2i^2 \\&= -2 - 2 \\&= -4 \\&= 1 - 5 \\&= 1 - (2-i)(2+i) \\&\equiv 1 \quad (\text{mod } (2+i))\end{aligned}$$

$$\therefore (1+i)^4 \equiv 1 \quad (\text{mod } (2+i))$$

Se concluye que el inverso de $\overline{1+i}$ en $(\mathbb{Z}[i]/(2+i))$ es $\overline{1+i}^3 = \overline{-2+2i}$.



$$X^{50} \equiv 1 \quad (1296)$$

$$1296 = 6^4$$

$$\boxed{X^{50} = 1(6)}$$

$$\mathbb{Z}_{(6)} = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5} \}$$

$$\text{Immediato } X_1 = 1 \quad : \quad X_1^{50} \equiv 1 \quad (6)$$

$$50 = 5^2 \cdot 2$$

$$\begin{aligned} \left\{ \begin{array}{l} X^{50} \equiv 1 \quad (2) \\ X^{50} \equiv 1 \quad (3) \end{array} \right. & \iff \left(X^2 \right)^{25} \equiv 1 \quad (2) \Rightarrow X^{25} \equiv 1 \quad (2) \\ & \iff \left(X^3 \right)^{16} \cdot X^2 \equiv 1 \quad (3) \quad \left| \begin{array}{l} X^{24} \cdot X \equiv 1 \quad (2) \\ ((X^2)^2)^8 \cdot X \equiv 1 \quad (2) \end{array} \right. \\ & \quad X^{16} \cdot X^2 \equiv 1 \quad (3) \\ & \quad X^{18} \equiv 1 \quad (3) \quad \left| \begin{array}{l} X^3 \cdot X \equiv 1 \quad (2) \\ X^4 \equiv 1 \quad (2) \end{array} \right. \\ & \quad X^6 \equiv 1 \quad (3) \\ & \quad X^2 \equiv 1 \quad (3) \quad \left| \begin{array}{l} X \equiv 1 \quad (2) \\ X \equiv 5 \quad (2) \end{array} \right. \end{aligned}$$

$$\text{Tenemos: } X^{\varphi(6)} \equiv 1 \quad (6) \quad \varphi(6) = \underline{\underline{4}} \quad (1, 5)$$

$$X^2 \equiv 1 \quad (6)$$

$$X^{50} \equiv 1 \quad (6) \Leftrightarrow X^{25} \equiv 1 \quad (6) \Leftrightarrow \left\{ \begin{array}{l} X^{25} \equiv 1 \quad (2) \\ X^{25} \equiv 1 \quad (3) \end{array} \right.$$

$$X^{25} = X^{24} \cdot X \Rightarrow X^{25} \equiv (X^3)^8 \cdot X \quad (3)$$

$$\equiv X^8 \cdot X \quad (3)$$

$$\equiv X^9 \quad (3)$$

$$\equiv X \quad (3)$$

$$x^{50} \equiv 1 \pmod{6^4}, \quad 6^4 = 2^4 \cdot 3^4$$

Debemos resolver el sistema

$$\begin{cases} x^{50} \equiv 1 \pmod{2^4} \\ x^{50} \equiv 1 \pmod{3^4} \end{cases}$$

Buxamos soluciones de $x^{50} \equiv 1 \pmod{2}$, $x^{50} \equiv 1 \pmod{3}$

$$x^{50} \equiv 1 \pmod{2} \Leftrightarrow x^{25} \equiv 1 \pmod{2}$$

$$\Leftrightarrow (x^3)^{13} \cdot x \equiv 1 \pmod{2}$$

$$x^3 \cdot x \equiv 1 \pmod{2}$$

$$x^4 \equiv 1 \pmod{2}$$

$$x \equiv 1 \pmod{2}$$

$$x^{50} \equiv 1 \pmod{3} \Leftrightarrow (x^3)^{16} \cdot x^2 \equiv 1 \pmod{3}$$

$$x^{16} \cdot x^2 \equiv 1 \pmod{3}$$

$$x^{18} \equiv 1 \pmod{3}$$

$$x^9 \cdot x^9 \equiv 1 \pmod{3}$$

$$x^2 \equiv 1 \pmod{3}$$

Resolvemos el sistema

$$\begin{cases} x \equiv 1 \pmod{2} \\ x^2 \equiv 1 \pmod{3} \end{cases}$$

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 1 \pmod{3} \end{cases}$$

$$x_1 \equiv 1 \pmod{6}$$

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \end{cases}$$

$$x_2 \equiv 5 \pmod{6}$$

$$\begin{cases} x^{50} \equiv 1 \pmod{2^4} \\ x^{50} \equiv 1 \pmod{3^4} \end{cases}$$

Por la estructura de $\mathbb{Z}_4/\langle r \rangle$ tenemos que estudiar los invertibles modulo $2^4, 3^4$ simultáneamente

como $(\mathbb{Z}_4/\langle r \rangle)^*$ ciclico de orden $\varphi(3^4) = 3^3(3-1) = 27 \cdot 2 = 54$

Debemos descartar los múltiplos de 3

\bar{u} invertible en $\mathbb{Z}_4/\langle r \rangle \iff \text{mcd}(u, 2^4) = 1$

Debemos descartar todos los potencias de 2 los múltiplos de 2

Quedan múltiplos de 5, 7, 11, 13, 17, 19

1:

5: 5 ~~10~~ 15 ~~20~~ 25 ~~30~~ 35 ~~40~~ 45 ~~50~~ 55 ~~60~~ 65 ~~70~~ ~~75~~ ~~80~~

7: 7 ~~14~~ 21 28 ~~35~~ 42 49 56 63 ~~70~~ 77

11: 11 22 ~~33~~ 44 ~~55~~ 66 ~~77~~

13: 13 26 39 52 ~~65~~ 78

∴ 1, 5, 25, 35, 55, 65, 7, 49, 77, 11, 13,

Además los primos

17, 19, 23, 29, 31, 37, 41, 43, 47, 51, 53, 57, 59, 61, 67, 71, 73,

~~79~~

~~79~~

$$\varphi(6^4) = \varphi(2^4)\varphi(3^4) = \varphi(2^4)3^3(3-1)$$

$$\varphi(6^4) = 6^3 \varphi(6) = 6^3$$

$$1296 = 6^4 = 2^4 3^4$$

$$\mathbb{Z}/1296\mathbb{Z}^* = \mathbb{Z}/6^4\mathbb{Z}^* \cong \mathbb{Z}/2^4\mathbb{Z}^* \times \mathbb{Z}/3^4\mathbb{Z}^*$$

invertibles en $\mathbb{Z}/3^4\mathbb{Z}$

~~1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 24, 25, 26, 28, 29, 31,~~
~~32, 34, 35, 37, 38, 40, 41, 43, 44, 46, 47, 49, 50, 52, 53, 55, 56, 57,~~
~~58, 59, 61, 62, 64, 67, 68, 70, 71, 73, 74, 76, 77, 79, 80~~

En rojo se descartan los que son múltiplos de 2 (i.e. no $\in (\mathbb{Z}/2^4\mathbb{Z})^*$)

~~1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43~~
~~47, 49, 53, 55, 57, 59, 61, 67, 71, 73, 77, 79~~

$$(\mathbb{Z}/8\mathbb{Z})^* = \{1, 3, 5, 7\}$$

$$x^n \equiv 1 \pmod{p^t} \Rightarrow x \in (\mathbb{Z}/p^t\mathbb{Z})^*$$

Sup. x nilpotente: $\exists m \in \mathbb{N}, x^m \equiv 0 \pmod{p^t}$

$$x^n \equiv 1 \pmod{p^t} \Rightarrow (x^n)^m \equiv 1 \pmod{p^t} \Rightarrow (x^m)^n \equiv 1 \pmod{p^t}$$

$$\Rightarrow 0 \equiv 1 \pmod{p^t} \text{ (Contradic)}$$

$$\mathbb{Z}/2^4\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

$$\cong C_2 \times C_2^2$$

$$\cong (\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^*$$

$$\Rightarrow x^{50} \equiv 1 (2^4) \Leftrightarrow \begin{cases} x^{50} \equiv 1 (3) \\ x^{50} \equiv 1 (5) \end{cases}$$

$d = (50, 2^2) = (50, 4) = 2$, hay 4 soluciones

luego

$$x^{50} \equiv 1 (3) \Rightarrow x^{48} x^2 \equiv 1 (3)$$

$$\Rightarrow x^6 x^{18} \equiv 1 (3)$$

$$\Rightarrow x^{48} x^2 \equiv 1 (3)$$

$$x^{48} \equiv 1 (3)$$

$$x^{12} x^{12} x^{12} x^{12} \equiv 1 (3)$$

$$x^4 x^4 x^4 x^4 \equiv 1 (3)$$

$$x^2 \equiv 1 (3)$$

$$x^2 \equiv 1 (3)$$

$$x^{48} \equiv 1 (3)$$

$$\therefore x^{50} \equiv x^2 \equiv 1 (3)$$

$$\text{Ahora } x^{50} \equiv 1 (5)$$

$$x^4 \equiv 1 (5)$$

$$x^{48} \equiv 1 (5)$$

$$x^2 \equiv 1 (5)$$

$$\therefore \begin{cases} x^2 \equiv 1 (3) \rightarrow x = 1, 2 \\ x^2 \equiv 1 (5) \rightarrow x = 1, 4, \end{cases}$$

$x = 1, 2, 4$ soluciones

$x^{50} \equiv 1 (3^4)$ soluble $\Leftrightarrow x^{50} \equiv 1 (3)$ (mismas # soluciones)

$x=1, 2$ piven, $2^2 \equiv 1 (3)$
 $2^5 \equiv 1 (3)$

$$\mathbb{Z}/6\mathbb{Z}^* \cong \mathbb{Z}/2\mathbb{Z}^* \times \mathbb{Z}/3\mathbb{Z}^*$$

$$\cong (\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^* \times (\mathbb{Z}/3\mathbb{Z})^*$$

$$(8) \not\in \mathbb{Z}^*$$

$$(8) \not\in \mathbb{Z}^*$$

$$(8)(-8) = 64 \not\equiv 1 \pmod{6}$$

$$a_n \alpha^n + a_{n-1} \alpha^{n-1} + \dots + a_1 \alpha + a_0 = 0$$

$$a_n \alpha^n + \dots + a_0 + 1 = 1$$

$$a_0 = -\alpha (a_n \alpha^{n-1} + \dots + a_1)$$

I primo en $\mathbb{Z}[\alpha]$ $\Rightarrow \mathbb{Z}[\alpha]/I$ dominio.

I ideal, $I \neq (0)$

Supongamos que $I \neq \mathbb{Z}[\alpha]$

$\exists p \in \mathbb{Z}[\alpha] : p \notin I$

I no contiene unidades.

$$a_0 p = -\alpha p (a_n \alpha^{n-1} + \dots + a_1)$$

\uparrow

\dagger

$$I \not\subseteq \mathbb{Z} \quad \Rightarrow \quad \alpha \in \mathbb{Z} \quad \alpha \in I$$

I primo $\Rightarrow \exists a \in \mathbb{Z} : a \in I \quad (a \neq 0)$

$\exists p \notin I \quad \text{taq} \quad pa \in I$

$p \in \mathbb{Z}[\alpha] \quad p \notin I$

Pd. $\mathbb{Z}[\alpha]/I$ anillo

$(n) \neq (0)$

Sea $p \neq 0 \pmod{I} \Leftrightarrow p \notin I$

$qp = 1 \pmod{I} \Rightarrow qp - 1 \in I$

$$aq = (a_n \alpha^n + \dots + a_0 + 1)a \in I \quad | \quad \nexists q \in \mathbb{Z}[\alpha] : qp - 1 \notin I$$

$$aqp = (a_n \alpha^n p + \dots + a_0 p + p)a \quad | \quad m(qp - 1) \in I$$

$$mfp - m = m(qp - 1)$$

$$1 - 4\omega, \quad 2 - 5\omega \quad \text{in} \quad \mathbb{Z}[\omega]$$

$$\omega = \frac{-1 + \sqrt{-3}}{2}$$

$$\mathbb{N}(a+b\omega) = a^2 + ab +$$

$$2x^2 - 3y^2 = 5$$

$$(\sqrt{2}x + \sqrt{3}y)(\sqrt{2}x - \sqrt{3}y) = 1$$

$$x^2 + x - 3y^2 = 5$$

$$x^2 + (\quad) = 5$$

α en los algebraicos

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0 = 0 \quad a_i \in \mathbb{Z}$$

$$I \neq (0) \Rightarrow \exists p \in \mathbb{Z}[\alpha], \quad p \neq 0 \quad \text{taq} \quad p \in I$$

$$p(a_n\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0) = 0$$

$$a_n\alpha^n p + a_{n-1}\alpha^{n-1}p + \dots + a_1\alpha p + a_0 p = 0$$

$$\mathbb{Z}[\sqrt{2}] / (2, \sqrt{2}) \cong \mathbb{F}_2 \quad \left| \begin{array}{l} \alpha^2 - 2 = 0 \\ (\sqrt{2})^2 - 2 = 0 \end{array} \right.$$

$$\begin{aligned} a_0 &= -a_n\alpha^n + a_{n-1}\alpha^{n-1} - \dots - a_1\alpha + a_0 \\ &= \alpha(-a_n\alpha^{n-1} + a_{n-1}\alpha^{n-2} - \dots - a_1) \end{aligned}$$

$$\mathbb{Z}[\alpha] / I \text{ dominio}$$

$$I \subset J, \quad p \in J, \quad p \notin I$$

Clase de operaciones

21/05/14

$$\mathbb{Z}[\sqrt{D}]$$

$$x^2 = 4D$$

$$\mathbb{Z}[\sqrt{D}] = \mathbb{Z} \oplus \sqrt{D}\mathbb{Z}$$

$$(x'' - 6) + (x^4 + x^3 + x^2 + x + 1) = ?$$

$$\mathbb{Z}[x]$$

$$(x'' - 6, x^4 + \dots + x + 1)$$

$$\cong \frac{\mathbb{Z}[x]}{(x'' - 6)}$$

$$\cong \frac{\mathbb{Z}[x]}{(n'' - 6)}$$

$$\cong \frac{\mathbb{Z}[x]}{(n - 6)}$$

$$\zeta = e^{\frac{2\pi i}{5}}$$

$$\cong \frac{\mathbb{Z}[x]}{(x^4 + \dots + 1, x - 6)}$$

$$\cong \frac{\mathbb{Z}[x]}{(x^4 + 1, 0)}$$

$$\frac{\mathbb{Z}[i]}{(4i+2)}$$

$$\cong \frac{\mathbb{Z}}{n\mathbb{Z}}$$

?

$$1 \rightarrow 1$$

(Si fuese iso el $1 \rightarrow 1$)

$$\frac{\mathbb{Z}[i]}{(4i+2)} \cong$$

$$\frac{\mathbb{Z}[i]}{(20)}.$$

$$\cong \frac{\mathbb{Z}[i]}{(4i+2)(5i+2)}$$

$$\left| \frac{\mathbb{Z}[i]}{(20)} \right| = 400$$

$$N(4i+2) = 20$$

$$(4i+2)(-4i+2) = 20$$

$$\frac{\mathbb{Z}[i]}{(20)} \cong \frac{\mathbb{Z}}{(20)} \oplus i \frac{\mathbb{Z}}{(20)}$$

$$a+bi$$

$$4i+2 = 0$$

$$4i = -2$$

$$1 \cdot 10 \equiv 5 \cdot 2 \equiv 5 \cdot (-4i) \equiv -20i \equiv 0$$

PRO/ARTE

el 1 tiene orden 10 : los tienen orden 10

Class 24 exercises

21/03/14

$$\mathbb{Z}[\sqrt{D}] \quad x^2 = 4D$$

$$\mathbb{Z}[\sqrt{D}] = \mathbb{Z} \oplus \sqrt{D}\mathbb{Z}$$

$$(x^n - 6) + (x^4 + x^3 + x^2 + x + 1) = ?$$

$$\frac{\mathbb{Z}[x]}{(x^n - 6, x^4 + x^3 + x^2 + x + 1)} \cong \frac{\mathbb{Z}[z]}{(z^n - 6)} \cong \frac{\mathbb{Z}[v]}{(v - 6)}$$
$$v = e^{\frac{2\pi i}{n}}$$
$$\cong \frac{\mathbb{Z}[z]}{(z^4 + z^3 + z^2 + z + 1)} \cong \frac{\mathbb{Z}[v]}{(v^4 + v^3 + v^2 + v + 1)}$$

$$\frac{\mathbb{Z}[i]}{(4i+2)} \cong \frac{\mathbb{Z}}{n\mathbb{Z}} ?$$

$$1 \rightarrow \dots \rightarrow 1$$

(so first map will be $i \mapsto 1$)

$$\frac{\mathbb{Z}[i]}{(4i+2)} \cong \frac{\mathbb{Z}[i]/(20)}{(4i+2)/20}$$

$$\left| \frac{\mathbb{Z}[i]}{(20)} \right| = 400$$

$$N(4i+2) = 20$$

$$(4i+2)(-4i+2) = 20$$

$$\frac{\mathbb{Z}[i]}{(20)} \cong \frac{\mathbb{Z}}{(20)} \oplus i \frac{\mathbb{Z}}{(20)}$$

$$i+6i$$

$$4i+2 = 0$$

$$4i \equiv -2$$

$$1 \cdot 10 \equiv 5 \cdot 2 \equiv 5 \cdot (-4i) \equiv -20i \equiv 0$$

PROBLEME: $\begin{matrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{matrix}$ $\begin{matrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{matrix}$ $\begin{matrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{matrix}$

era más simple cocientar por (10)

$$\frac{\mathbb{Z}[i]}{(4i+2)} \cong \frac{\mathbb{Z}[i]}{(4i+2)(10)}$$

$$\left| \frac{\mathbb{Z}[i]}{(10)} \right| = 100$$

$$\frac{\mathbb{Z}[i]}{(10)} \cong \frac{\mathbb{Z}}{(10)} \oplus \frac{\mathbb{Z}}{(10)}$$

$$\langle \bar{1} \rangle \subseteq \frac{\mathbb{Z}[i]}{(4i+2)} \quad |\langle \bar{1} \rangle| = 10$$

$$(4i+2) = 2(2i+1)$$

$$N(2i+1) = 5$$

$$|\langle \bar{1} \rangle| = 10$$

$$|\langle \bar{2} \rangle| = 5$$

$$4i = -2$$

$$|\langle \bar{i} \rangle| = 20$$

$$\left| \frac{\mathbb{Z}[i]}{(4i+2)} \right| = 20$$

Luego no son isomórfas.

Otra forma:

$$\frac{\mathbb{Z}[i]}{(4i+2)} \cong \frac{\mathbb{Z}[i]}{(2(2i+1))} \cong \frac{\mathbb{Z}[i]}{2} \times \frac{\mathbb{Z}[i]}{(2i+1)}$$

$$\cong \frac{\mathbb{Z}/2\mathbb{Z}}{2} \times \frac{\mathbb{Z}/5\mathbb{Z}}{5} \quad \text{se ve mejor}$$

1 orden 2

1 orden 5

PROBLEMA

el cuadro viene ordenado así:

$$\frac{\mathbb{Z}/2\mathbb{Z}[t]}{(2, t^2+1)} \cong \frac{\mathbb{Z}[x]}{(2, x^2+1)} \cong \frac{\mathbb{F}_2[x]}{(x^2+1)} \cong \frac{\mathbb{F}_2[x]}{(x+1)^2}$$

$$\cong \frac{\mathbb{F}_2[t]}{(t^2)} \quad t = x+1.$$

$$\frac{\mathbb{Z}[i]}{(2+2i)} \cong \frac{\mathbb{Z}[c]}{((1+i)^3)}$$

$$\frac{\mathbb{Z}[c]}{(2+2i)} \cong \frac{\mathbb{Z}[x]}{(x^2+1, 2+2x)}$$

$$\frac{\mathbb{Z}[x]}{(2+2x)} \hookrightarrow \frac{\mathbb{Z}[x]}{(2)} \times \frac{\mathbb{Z}[x]}{(x+1)} \cong \mathbb{F}_2[x] \times \mathbb{Z}$$

$$\frac{\mathbb{Z}[x]}{(2, x+1)} \cong \frac{\mathbb{Z}[-1]}{(2)} \cong \mathbb{F}_2$$

$$(1+i)^2 = 2i$$

$$(1+i)^4 = -4$$

$$\mathbb{Z}[x]/J_a \subseteq \mathbb{Z}/J_a$$

$$J_a = \ker E_a$$

$$\frac{\mathbb{Z}[i]}{(1+i)^3} \cong \frac{\mathbb{Z}[i]/(4)}{(1+i)^3/(4)}$$

$$\left| \frac{\mathbb{Z}[i]}{(4)} \right| = 16$$

$$(1+i)^3 \not\equiv 0 \pmod{4}$$

$$2(1+i)^3 \equiv 0 \pmod{4}$$

PROBLEMA

$$\mathbb{Z}[i] = \mathbb{Z} \oplus i\mathbb{Z} = \mathbb{Z} \oplus (1+i)\mathbb{Z}$$

$$x+bi = (a-b) + b(1+i)$$

$$(1+i)^3 = \langle (1+i)^3, (1+i)^4 \rangle_{\mathbb{Z}}$$

$$(1+i)^5 = 2i(1+i)^3$$

$$i = -1 + (1+i)$$

$$(1+i)^5 = 2(-1 + (1+i))(1+i)^3 = -2(1+i)^3 + 2(1+i)^4$$

$$(1+i)^3 = 2i(1+i)$$

$$\cong 2(-1 + (1+i))(1+i)$$

$$= -2(1+i) + 2(1+i)^2$$

$$= -2(1+i) + 4i$$

$$= -2(1+i) + 4(-1 + (1+i))$$

$$= -4 + 2(1+i)$$

$$(1+i)^4 = -4$$

$$\mathbb{Z}[i] \cong \mathbb{Z}[i]$$

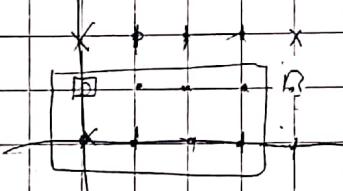
$$\frac{\mathbb{Z}[i]}{(1+i)^3} \cong \frac{\mathbb{Z}[i]}{\langle (1+i)^3, (1+i)^4 \rangle_{\mathbb{Z}}}$$

$$\begin{vmatrix} -4 & -4 \\ 2 & 0 \end{vmatrix}$$

= 8

$$\cong \frac{\mathbb{Z}^2}{\langle (-4, 2), (-4, 0) \rangle}$$

$$\cong \frac{\mathbb{Z}^2}{\langle (0, 2), (4, 0) \rangle}$$



$$\mathbb{Z}^2 / A\mathbb{Z}^2$$

$$\cong \frac{\mathbb{Z}}{i\mathbb{Z}}$$

$$A \text{ matrix } 2 \times 2$$

$$A = P D Q$$

$$A = \langle x, y \mid \begin{matrix} 3x + 2y = 0 \\ 5x + 8y = 0 \end{matrix} \rangle_{\mathbb{Z}}$$

$$D = \begin{pmatrix} d_1 & 0 \\ 0 & d_n \end{pmatrix}$$

$$\begin{vmatrix} 3 & 5 \\ 2 & 8 \end{vmatrix}$$

PROARTE

$$\text{Obs: } \left| \frac{\mathbb{Z}[i]}{(a+bi)} \right| = N(a+bi)$$

$$\left| \frac{\mathbb{Z}[i]}{(a+bi)} \right| = \left| \frac{\mathbb{Z}[i]}{(a-bi)} \right| \quad n = N(a+bi)$$

$$\left| \frac{\mathbb{Z}[i]}{(n)} \right| = n^2$$

$$\psi : \mathbb{Z}[i] \longrightarrow \frac{\mathbb{Z}[i]}{(n)}$$

$$\psi(c+di) = \overline{(c+di)(a+bi)}$$

$$\text{Im } \psi = \langle \overline{(a+bi)} \rangle = \frac{\langle a+bi \rangle}{\langle n \rangle}$$

$$\text{Ker } \psi = \{ c+di / n / (c+di)(a+bi) \} = \langle a-bi \rangle$$

$$A = \frac{\mathbb{Z}[i]}{(n)} \quad |A| = \left| \frac{A}{\text{Im } \psi} \right| \cdot |\text{Im } \psi|$$

$$= \left| \frac{\mathbb{Z}/(n)}{(a+bi)} \right| \cdot |\text{Im } \psi|$$

$$= \left| \frac{\mathbb{Z}}{(a+bi)} \right| \cdot |\text{Im } \psi|$$

$$\text{Im } \psi \cong \frac{\mathbb{Z}[i]}{\text{Ker } \psi}$$

$$|A| = \left| \frac{\mathbb{Z}}{(a+bi)} \right| \cdot \left| \frac{\mathbb{Z}[i]}{(a-bi)} \right|$$

$$n^2 = \left| \frac{\mathbb{Z}}{(a+bi)} \right|^2$$

$$\text{PROBLEME: } \left| \frac{\mathbb{Z}}{(a+bi)} \right| = n$$

(5)

G. 4b

$$\begin{array}{c} \xrightarrow{\quad \text{unitario} \quad} \\ x^2 - 2 \end{array}$$

$$\frac{\mathbb{Z}[x, x^{-1}]}{(x - 2x^{-1})} \cong \frac{\mathbb{Z}[x, x^{-1}]}{(x^2 - 2)} \cong \left(\frac{\mathbb{Z}[x]}{(x^2 - 2)} \right) [x^{-1}]$$

$$\cong \mathbb{Z}[\sqrt{2}] [\sqrt{2}^{-1}]$$

D.F.U

Loca. / reson.

(agregando + en el numerador de x^2 - 2 para que sea primo en el anillo)

* Encontrar primos de un anillo que son primos en otro.

 $\mathbb{Z}[\omega]$

$$\frac{\mathbb{Z}[\omega]}{(p)} \cong \frac{\mathbb{Z}[x]}{(p, x^2+x+1)} \cong \frac{\mathbb{F}_p[x]}{(x^2+x+1)}$$

alguno sea

 x^2+x+1

no tiene raíces

$$\frac{\mathbb{F}_2[x]}{(x^2+x+1)} \cong \mathbb{F}_1 \quad 2 \text{ es primo.}$$

$$x^2 + x + 1 = 0 \Rightarrow x = \frac{-1 \pm \sqrt{-3}}{2} \quad -3 \notin \mathbb{F}_2^2$$

$$\left(\frac{-3}{p}\right) = -1$$

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

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$$

PROARTE

$$p \equiv -1 \pmod{4}$$

$$\left(-\frac{3}{p} \right) = \left(-\frac{1}{p} \right) \left(\frac{3}{p} \right) = \left(\frac{p}{3} \right)$$

$$\left(\frac{p}{3} \right) = -1$$

$$p \equiv 2 \pmod{3}$$

③ 6. u. 5.

$$A = \frac{\mathbb{Z}[x, \frac{1}{x+1}]}{(x^2 + x + 1)} \cong \frac{\mathbb{Z}[x]}{(x^2 + x + 1)} \left[\frac{1}{x+1} \right] \cong \mathbb{Z}[\omega] \left[\frac{1}{\omega+1} \right]$$

$$\omega + 1 = -\bar{\omega} \in \mathbb{Z}[\omega]^* \quad \omega \bar{\omega} = 1$$

$$A \cong \mathbb{Z}[\omega].$$

④ 6. 5.

$$(x^2 + y^2) = z^2 \quad (x, y) = 1$$

$$(x+bi) \mid (x+iy), (x-iy)$$

$$(x+bi) \mid (x+iy) + (x-iy) = 2x$$

$$(x+bi) \mid (x+iy) - (x-iy) = 2iy$$

$$(x+bi) \mid 2$$

$$(x+bi) = 2$$

$$\frac{x+yi}{2} \in \mathbb{Z}[i]$$

$$\text{PROBARTIE } (x+bi) = 1, 1+i$$

Ejercicios algebraicos

$$3x^2 - 7y^2 = 20$$

$$9x^2 - 21y^2 = 60$$

$$N(3x - y\sqrt{21}) = 60$$

$$\mathbb{Z}[\sqrt{21}]$$

$$N(6 - \sqrt{21}) = 60 \quad (\text{comprobación})$$

$$(6 - \sqrt{21})(6 + \sqrt{21})$$

↓ norma 1

$$x^2 - 21 =$$

$$\text{soluciones de } x^2 - 2y^2 = 7 \quad (\text{enunciado})$$

$$\text{sol. } 3 \wedge 1$$

$$\mathbb{Z}[\sqrt{2}] \triangleleft \text{I.P.}$$

$$(3 - \sqrt{2})$$

$$x = 3$$

$$y = -1$$

$$(3 + \sqrt{2})$$

$$x = 3$$

$$y = 1$$

↓ D.F.U

$$\begin{pmatrix} \pm \\ \pm \end{pmatrix} = (3 - \sqrt{2})(3 + \sqrt{2}),$$

$$(3 - \sqrt{2})\eta$$

$$(3 + \sqrt{2})\eta^2$$

$$\eta = \pm \sqrt[3]{2}$$

$$\eta_0 = 1 + \sqrt{2}$$

unidad
y una
solución

+ los otros productos:

menos refiriéndose

cuando se multiplican

$$\text{de } x^2 + y^2 = 20?$$

$$x^2 + y^2 = 20$$

$$(x+iy)(x-iy) = 2^2 \cdot 5$$

PROARTÉ

$$= -(1+i)^4 (2+i) (2-i)$$

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

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

$$x^2 + y^2 = 65$$

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

$$(3+2i)(3-2i)$$

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

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

$$(2+i)(3+2i) = 4+7i \rightarrow \text{P } 4, \text{ I } 7$$

$$(2+i)(3-2i) = 8-i \rightarrow \text{P } 8, \text{ I } -1$$

Teoría de Números.

Prueba 2

Mayo 27, 2014

Resuelva cuatro de los siguientes cinco problemas:

1. Encontrar el máximo comun divisor de $1 - 4\omega$ y $2 - 5\omega$ en $\mathbb{Z}[\omega]$.

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

3. Sea α una raíz del polinomio $x^3 + x + 2$. Encuentre m tal que

$$\mathbb{Z}[\alpha]/(\alpha^2 + 5) \cong \mathbb{Z}/m\mathbb{Z}.$$

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

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

Bajo que condiciones se resuelve:

$$x^2 + ax + b \equiv 0 \pmod{p}, p \neq 2:$$

$$f'(x) = 2x + a$$

Si $f'(x) = 2x + a \equiv 0 \pmod{p}$, entonces: $x = 2^{-1} \cdot a \pmod{p}$.

Si $x = 2^{-1} \cdot a$: $(2^{-1}a)^2 + a(2^{-1}a) + b \equiv 0 \pmod{p}$

$$\frac{a^2}{4} + b \equiv 0 \pmod{p},$$

$$x^2 + ax + \frac{a^2}{4} \equiv 0 \pmod{p}$$

$$(x + \frac{a}{2})^2 \equiv 0 \pmod{p}.$$

Entonces:

Si $f(x)$ tiene soluciones módulo p , las soluciones de $f(x) \equiv 0 \pmod{p}$

pueden calcularse usando el Lema de Hensel.

O sea si: $p \nmid \Delta = a^2 - 4b$.

La ecuación: $x^2 + ax + b \equiv 0 \pmod{p}$ tiene soluciones si Δ es cuadrado módulo p .

¿Cuáles son los cuadrados módulo p ?

Si $p \neq 2$:

$$x^2 \equiv y^2 \pmod{p}$$

$$x^2 - y^2 \equiv 0 \pmod{p}$$

$$(x-y)(x+y) \equiv 0 \pmod{p}$$

Como $\mathbb{Z}/p\mathbb{Z}$ es cuerpo: $x-y \equiv 0 \pmod{p}$
 $x+y \equiv 0 \pmod{p}$

El nº de cuadrados perfectos en $\mathbb{Z}/p\mathbb{Z}$ es $\frac{p-1}{2} + 1 = \frac{p+1}{2}$.

$$\text{En } \mathbb{Z}/7\mathbb{Z} : \begin{array}{l} 1^2 = 1 \\ 2^2 = 4 \\ 3^2 = 9 \end{array} \Rightarrow \text{mádador} = \{ \bar{1}, \bar{4}, \bar{2} \}.$$

$$\text{Guz: } \begin{array}{l} 1: 1-5 \\ 2: 1-10 \\ 3: 1-9 \end{array} \}$$

Ej: $f(x) = x^3 - 8$: Det. las soluciones de $f(x) \equiv 0 \pmod{7^2}$.
 Claramente: $f(x) \equiv 0 \pmod{7}$ tiene $x \equiv 1 \pmod{7}$ y $x \equiv 2 \pmod{7}$ son soluciones.
 Además las sol. forman un grupo: $f(x) \equiv x^3 - 1 \pmod{7}$, $f'(x) = 3x^2$
 telesimórfico: $x \equiv 4 \pmod{7}$.

Paramos con: $x \equiv 1 \pmod{7}$, $x = 1+7t$.

$$f(x) \equiv 0 \pmod{7^2}$$

$$f(1+7t) \equiv 0 \pmod{7^2}$$

$$f(1) + 7t f'(1) \equiv 0 \pmod{7^2}$$

$$-7 + 7t \cdot 3 \equiv 0 \pmod{7^2}$$

$$-1 + 3t \equiv 0 \pmod{7}, 3t \equiv 1 \pmod{7}, t \equiv 5 \pmod{7}.$$

Luego: $x \equiv 36 \pmod{49}$.

Para: $x = 4 \pmod{7}$, $x = 4+7t$

$$f(x) \equiv 0 \pmod{7^2}$$

$$f(4+7t) \equiv 0 \pmod{7^2}$$

$$f(4) + 7t f'(4) \equiv 0 \pmod{7^2}$$

$$56 + 7t \cdot 3 \cdot 6 \equiv 0 \pmod{7^2}$$

$$8 + 3 \cdot 6t \equiv 0 \pmod{7}$$

$$1 + 3 \cdot 2t \equiv 0 \pmod{7}, t \equiv 1 \pmod{7}$$

Luego: $x \equiv 11 \pmod{49}$.

Un recuerdo: $|\mathbb{F}_p^*| = p-1$.

Así $\forall x \in \mathbb{F}_p^*$: $x^{p-1} - 1 = 0$

Si no es cíclico: $\mathbb{F}_p^* \cong A \times B$ con $(|A|, |B|) = 1$.

Pero cualquier grupo abeliano: $G \cong C_1 \times \dots \times C_d$, $d_1 | d_2 | \dots | d_r$

Otro camino: Prop: Si G es un grupo abeliano no cíclico,

existe $n \mid |G|$, $n < |G|$ tal que: $p^n = 1 \quad \forall p \in G$.

Dem: (Si \mathbb{F}_p^* no es cíclico, entonces $p(x) = x^n - 1 = 0 \quad \forall x \in \mathbb{F}_p^*$ con $n > p-1$
∴ $p(x)$ tiene más de n soluciones, pero todo elemento en \mathbb{F}_p^* es solución). \star)

Si: $|G| = p_1^{a_1} \cdots p_r^{a_r}$.

Para cada $|p| =$ menor r positivo: $p^r = 1$.

Entonces: $p^r = 1$ si $\text{ord}(p) \mid n$.

Tomamos $n = \text{lcm} \{ \text{ord}(p) \mid p \in G \}$.

Si: $\text{lcm} \{ \text{ord}(p) \mid p \in G \} = m \Rightarrow G$ es cíclico.

Para cada p_i , existe $p_i \in G$ tal que: $p_i^{a_i} \mid \text{ord}(p_i)$

Notación: Si p es primo: $N_p(n) =$ mayor potencia de p que divide a n .

$$\alpha = N_p(n) \Leftrightarrow p^\alpha \mid n, \quad p^{\alpha+1} \nmid n$$

obs: $N_p(\text{lcm}\{h_1, \dots, h_r\}) = \max \{ N_p(h_1), \dots, N_p(h_r) \}$

Dem: Si: $m = p_1^{a_1} \cdots p_r^{a_r}, \quad l = p_1^{b_1} \cdots p_r^{b_r}$

$$\text{lcm}(m, l) = p_1^{\max(a_1, b_1)} \cdots p_r^{\max(a_r, b_r)}$$

$$\Rightarrow N_p(\text{lcm}(m, l)) = \max \{ a_1, b_1 \} = \max \{ N_p(m), N_p(l) \}$$

$$N_p \{ \text{ord}(\rho) \mid \rho \in G \} = d_i$$

$$\text{máx} \{ N_p(\text{ord}\rho) \mid \rho \in G \} = d_i$$

$$N_p(\text{ord}\rho) = d_i$$

Se $\exists i$ tal que $|p| = p^i \cdot s_i$, $(s_i, p) = 1$.

$$\text{ord}(p, s_i) = p^i$$

$$\text{Sea } \rho = p_1^{r_1} \cdots p_r^{r_r}, \text{ así } |p| = p_1^{d_1} \cdots p_r^{d_r}$$

Luego $\langle \rho \rangle = G \Rightarrow G$ es cíclico.

$(\mathbb{Z}/(p))^*$ cíclico de orden p^t si p es primo.

Sea $U = \{ \overline{1+pr} \in \mathbb{Z}/p^t\mathbb{Z} \}$, claramente $|U| = p^{t-1}$ para $x^t = 0$.

$$y \quad U \subseteq (\mathbb{Z}/p^t\mathbb{Z})^*$$

$$\text{AF: } U \text{ es cíclico, si } p \neq 2$$

$$- (1+pr)^p = 1 + p^2r + \binom{p}{2} p^2r^2 + \sum_{i=3}^p (\rho) p^i r^i$$

$$- (1+pr)^p = 1 + p^2r + \binom{p}{2} p^2r^2 + \dots$$

$$- (1+pr)^p = 1 + p^2r + \binom{p}{2} p^2r^2 + \dots$$

$$\text{Como } p \neq 2: \quad p \mid \binom{p}{2}$$

$$(1+pr)^p = 1 + p^2r + p^3r^2, \text{ si } r=1;$$

$$N_p((1+p)^p - 1) = 2.$$

$$\text{Así: } (1+p)^{p^2} = (1+pr)^p = \frac{1 + p^3r + \binom{p}{2} p^3r^2 + \dots}{1 + p^3r^2 + \dots}$$

$$\text{Por inducción: } N_p((1+p)^{p^l} - 1) = l+1.$$

$$\text{Bajo las condiciones } (1+p)^{p^l} \equiv 1 \pmod{p^t} \Rightarrow p^t \mid (1+p)^{p^l} - 1, \text{ así:}$$

$$\text{Si } N_p((1+p)^{p^l} - 1) \geq t$$

$$l+1 \geq t$$

$$\therefore \text{ord}(1+p) = p^{t+1} \Rightarrow \langle 1+p \rangle = U.$$

Ejercicio: Si $n|m \Rightarrow N_p(n) \leq N_p(m)$, $\forall p$.

Luego \mathbb{Z}_{p^t} es cíclico de orden p^t .

$$x^{p-1} \equiv 1 \pmod{p}$$

Tiene solución x_0 con x_0 de orden $p-1$.

Sea $f(x) = x^{p-1} - 1$, $f'(x) = (p-1)x^{p-2}$, $f'(x_0) = -x_0^{p-2} \pmod{p} \neq 0 \pmod{p}$

Por el teorema de Hensel, existe x_1 con:

$$x_1^{p-1} \equiv 1 \pmod{p^t}$$

y $x_1 \equiv x_0 \pmod{p}$, $x_1^n \neq 1 \pmod{p^t}$, si $n < p-1$

Luego: $x_1^n \neq 1 \pmod{p^t}$, si $n < p-1$.

Así: $\text{ord}(x_1) = p-1$; en $(\mathbb{Z}/p^t\mathbb{Z})^*$

Luego: $\text{ord}(x_1(p+1)) = p^t(p-1) = |(\mathbb{Z}/p^t\mathbb{Z})^*|$

Así: $(\mathbb{Z}/p^t\mathbb{Z})^*$ es cíclico. ($\because p \neq 2$).

Ahora bien: Si $t+1 \mid p+2$:
 $|(\mathbb{Z}/p^t\mathbb{Z})^*| = p^t(p-1) \in \text{par}$

$$(\mathbb{Z}/p^t\mathbb{Z})^* \cong \langle u \rangle \cong C_{2e}$$

$$\bar{a} = \bar{u}^b \pmod{p^t}$$

Para resolver a :
 $x^2 \equiv a \pmod{p^t}$ tiene solución si $b \in \text{par}$.

Si $x = \bar{u}^c$, $\bar{x}^2 = \bar{u}^{2c} = \bar{u}^b$ (ssi. $b \equiv 2c \pmod{2e} \Leftrightarrow b \in \text{par}$)

Luego, la mitad de los elementos de $(\mathbb{Z}/p^t\mathbb{Z})^*$ son cuadrados.

$$(\mathbb{Z}/p^t\mathbb{Z})^* \cong \cup_{i \in \mathbb{Z}} \langle \bar{x}_i \rangle \cong C_{p^{t-1}} \times C_{p-1}$$

$$\bar{a} \mapsto (1+r^p, x_i)$$

$$a \equiv x_i^l (1+r^p) \pmod{p^t}$$

Si:

(Cuando a es cuadrado).

$$a \equiv f^2 (p^t), f \equiv x_i^m (1+r^p) (p^t)$$

Así:

$$x_i^{2m} \equiv x_i^l \text{ssi } l \text{ par}$$

$$(1+r^p)^2 \equiv 1+r^p \text{ tiene solucion.}$$

Ejercicio: En un grupo de orden impar, cada elemento es cuadrado.

Ejercicio: En un grupo de orden impar, cada elemento es cuadrado.

Así: a es cuadrado módulo p si es cuadrado módulo p^t

$$a \equiv x_i^l (1+r^p) \pmod{p^t}$$

Pues:

$$a \equiv x_i^l \pmod{p}$$

(por la inducción, basta estudiar $f(x) = x^2 - a$)

Def: Sea p un primo impar y $a \in \mathbb{Z}$, con $p \nmid a$, definimos:

$$\left(\frac{a}{p} \right) = \begin{cases} 1, & \text{si } a \text{ es cuadrado} \\ -1, & \text{si no.} \end{cases}$$

Prop: $\left(\frac{a}{p} \right) \equiv a^{\frac{p-1}{2}} \pmod{p}$

Sea $a \equiv u^b$, luego: $a^{\frac{p-1}{2}} \equiv u^b \left(\frac{p-1}{2} \right)$

Primera obs: $u^{\frac{p-1}{2}-2} \equiv u^{p-1} \equiv 1$, así: $u^{\frac{p-1}{2}} \in \{1, -1\}$

Luego: $a^{\frac{p-1}{2}} = 1$ ssi $p-1 = \text{ord}(u) \mid b \cdot \frac{p-1}{2}$

Luego, es bimultiplicativo: $2 \mid b$, luego a es cuadrado.

∴ $a^{\frac{p-1}{2}} = 1$ ssi $2 \mid b$ ssi a es cuadrado

$$\psi: (\mathbb{Z}/\mathbb{Z})^* \rightarrow \{1, -1\}$$

Corolario: La función $\bar{a} \mapsto \left(\frac{a}{p}\right)$ es un homomorfismo.

Multiplicativo.

Ej: q es cuadrado módulo n

$$q^{\frac{n-1}{2}} = q^5 \equiv (-2)^5 \equiv -2^5 \equiv -(-1) \equiv 1 \pmod{n}.$$

Otra forma: $\left(\frac{q}{n}\right) = \left(\frac{3}{11}\right)\left(\frac{3}{11}\right) = \left(\frac{3}{11}\right)^2 = 1$.

Si queremos calcular: $\left(\frac{31}{37}\right) = \left(\frac{-6}{37}\right) = \left(\frac{-1}{37}\right)\left(\frac{3}{37}\right)\left(\frac{3}{37}\right) \rightarrow$ simbolo de Jacoby

$$y = m(x - x_0) + y_0 \quad ; \quad m = -\frac{x_0 y_0}{a^2 - x_0^2}$$

$$\Rightarrow y = -\frac{x_0 y_0}{a^2 - x_0^2} (x - x_0) + y_0 = \frac{x_0 y_0}{a^2 - x_0^2} (x_0 - x) + y_0 \quad / a^2 - x_0^2$$

$$y(a^2 - x_0^2) = x_0 y_0 (x_0 - x) + y_0 (a^2 - x_0^2)$$

~~$$a^2 y - x_0^2 y = x_0^2 y_0 - x_0 y_0 x + a^2 y - x_0^2 y$$~~

$$\begin{aligned} & \because x_0 y_0 x - x_0^2 y = 0 \\ & x_0 y_0 x - \left(\frac{1}{b^2} (a^2 b^2 - a^2 y_0^2) \right) y = 0 \\ & x_0 y_0 x - \left(a^2 - \frac{a^2 y_0^2}{b^2} \right) y = 0 \\ & x_0 y_0 x - a^2 y + \frac{a^2}{b^2} y_0^2 y = 0 \end{aligned}$$

~~$$a^2 y - x_0^2 y = x_0^2 y_0 - x_0 y_0 x + a^2 y_0 - x_0^2 y_0$$~~

$$a^2 y - x_0^2 y = a^2 y_0 - x_0 y_0 x$$

$$(a^2 - x_0^2) y \neq x_0 y_0 x = a^2 y_0$$

$$\therefore b x_0 x + a^2 y y_0 = a^2 b^2$$

$$\begin{aligned} a^2 y - x_0^2 y &= -x_0 y_0 x + x_0^2 y_0 + a^2 y_0 - x_0^2 y_0 \\ &= -x_0 y_0 x + a^2 y_0 \end{aligned}$$

$$y(a^2 - x_0^2) = y_0(a^2 - x_0 x)$$

$$y a^2 \left(1 - \frac{x_0^2}{a^2}\right) = y_0(a^2 - x_0 x)$$

$$y a^2 \frac{x_0^2}{b^2} = y_0(a^2 - x_0 x) \Rightarrow y \frac{a^2}{b^2} y_0 = a^2 - x_0 x \quad / b^2$$

$$a^2 y y_0 = a^2 b^2 - b^2 x_0 x$$

- $I+J \subseteq C$ Son comaximales (si $I+J = C$)
Prop: Si I, J son comaximales entonces $IJ = I \cap J$ ($I \text{ y } J$ son primos entre sí)
- Dem: Claramente $I \supseteq IJ, IJ \supseteq I \cap J$, así $I \cap J \subseteq IJ$.
- Sea $a \in I \cap J$: $a = i+j$ con $i \in I, j \in J$.
Entonces: $a = i+j = a_i + a_j \in I + J$ (ya que $I + J$ es un ideal)
- Entonces: $I = a + I = a_i + I + a_j + J \subseteq I + J$ (ya que $I + J$ es un ideal)
- Entonces: $(n) + (m) = (1)$ ($n, m \in \mathbb{Z}$)
- Entonces: $\text{Si } n, m \in \mathbb{Z} \text{ son relativamente primos.}$
- Prop: (Teorema Chino de los Restos) Si $I, J \subseteq C$ son comaximales
- Entonces: $C/IJ \cong C/I \times C/J$
- o bien: $C/IJ \cong C/I \times C/J$ ($I \text{ y } J$ primos entre sí)
- Dem: Sea $\pi_1: C \rightarrow C/I, \pi_2: C \rightarrow C/J$ homomorfismos
Entonces: $\varphi = \pi_1 \times \pi_2: C \rightarrow C/I \times C/J$ ($C/I \times C/J$ es un anillo)
- Entonces: φ es un homomorfismo, $\ker \varphi = IJ$.
- Observación: $\ker \varphi = \{c \in C : c+I = I, c+J = J\} = \{c \in C : c \in I, c \in J\} = IJ$.
- Nota: Si $(b+I, a+J) \in C/I \times C/J$. Pd: existe $c \in C$:
 $c+I = b+I, c+J = a+J$.
Sabemos: $c = i+j \in I+J$
 $i \equiv b \pmod{I}, i \equiv 0 \pmod{J}$
 $j \equiv a \pmod{J}, j \equiv 0 \pmod{I}$

$$C \equiv b \pmod{I}$$

$$C \equiv a \pmod{J}$$

Sea $C = jb + ia$. Así:

$$C \equiv 1 \cdot b + 0 \cdot a \equiv b \pmod{I}$$

$$C \equiv 0 \cdot b + 1 \cdot a \equiv a \pmod{J}$$

$\therefore \Phi$ es epíjetiva.

Prop: Si I, J son comaximales el sistema:

$$\begin{cases} X \equiv b \pmod{I} \\ X \equiv a \pmod{J} \end{cases}$$

Siempre tiene solución única módulo $I \cap J = (m - d)$.

(es único módulo $I \cap J$)

Es única porque si x, y son soluciones de (*)

$$x \equiv d \pmod{I} \quad \text{y} \equiv d \pmod{J}$$

$$x \equiv d \pmod{J} \quad I \cap J = (m - d)$$

Asi:

$$x - d \in I, \quad x - d \in J \Rightarrow x - d \in I \cap J$$

$$x - d \equiv d \pmod{I \cap J}$$

Luego:

En un DIP: n, m primos relativos: $I = n\mathbb{Z} + m\mathbb{Z}$

y tener el sistema

$$\begin{cases} X \equiv b \pmod{n} \\ X \equiv a \pmod{m} \end{cases}$$

$$\Rightarrow X = a + b + mnk \pmod{mn}$$

$$I = n\mathbb{Z} + m\mathbb{Z} \subset (n\mathbb{Z} + m\mathbb{Z})^2$$

$\therefore C \in I$

$$I = n\mathbb{Z} + m\mathbb{Z} \subset (n\mathbb{Z} + m\mathbb{Z})^2$$

$$(I_{\text{base}})^2 \subset I \quad (I_{\text{base}}) \subset I$$

$$(I_{\text{base}})^2 \subset I \quad (I_{\text{base}}) \subset I$$

Un ejemplo: $\begin{cases} x \equiv 5 \pmod{k} \\ x \equiv 7 \pmod{19} \end{cases}$

Observación: $19 = 12 \cdot 1 + 7$

$$12 = 7 \cdot 1 + 5$$

$$5 = 2 \cdot 2 + 1$$

$$2 = 1 \cdot 2 + 0$$

$$\rightarrow (0) \rightarrow 5$$

$$\rightarrow (1, 0) \rightarrow 1$$

$$d = 7 \cdot 9 + 5$$

luego:

$$x = 2 \cdot 5 \cdot 19 + 8 \cdot 12 \equiv 2 \cdot 5 \cdot 7 + 8 \cdot 1 \pmod{12 \cdot 19}$$

$$\begin{aligned} x &\equiv -5 \cdot 5 \cdot 19 + 8 \cdot 7 \cdot 12 \pmod{12 \cdot 19} \\ &\equiv 19 - 12 \pmod{12 \cdot 19} \\ &\equiv -27 \pmod{12 \cdot 19} \end{aligned}$$

Otra forma: $x \equiv 7 \pmod{5}, x = 7 + 5k$

$$7 + 5k \equiv 5 \pmod{12}$$

$$7 + 7k \equiv 5 \pmod{12}$$

$$0 \equiv 9 - 9 \pmod{12}$$

$$1 + k \equiv 5 \pmod{12}$$

$$k \equiv 34 \pmod{12}$$

$$k \equiv 10 \pmod{12}$$

$$12k \equiv 10 \pmod{12}$$

$$12k \equiv 10 \pmod{12}$$

$$12k \equiv 1 \pmod{12}$$

Sistemas

$$\begin{cases} x_1 \equiv 1 \pmod{12} \\ x_1 \equiv 0 \pmod{19} \end{cases}$$

$$12k \equiv 1 \pmod{12}$$

1. 1º) Solución:

$$x_1 = -12 \cdot 115 \pmod{12 \cdot 19}$$

Sea $A = A_1 \times A_2$

producto de anillos unitarios.

$$P = (10)$$

$$I - P = (0, 1) = P^c$$

$$P + P^c = I$$

$$P \cdot P^c = 0$$

$$\text{P es idempotente} \quad P^2 = P \quad (1-P)^2 = 1 - 2P + P^2 = 1 - P = P$$

Si P es un idempotente, $P \cdot P^c$ es idempotente

y $PA, P^c A$ son ideales: $(PA)^2 = PA \cdot PA = PA$

Entonces $P^c A = P + P^c$

y ¿Qué es $P \cap P^c A$?

$$S. c = P^c b = P^c b$$

$$P_c = P P^c b = P^c b = c \quad \text{y} \quad P^c b = 0 \quad \text{y} \quad P^c = P - P^2 = 0$$

$$P_c = P P^c b = 0 \quad \text{y} \quad P^c A = P^c A$$

$$\text{Así: } A \cong A/\langle s_0 \rangle \cong A/P \cap P^c A \cong A/PA \times A/P^c A$$

$$\text{Observemos: } P + P^c = I$$

$$P \equiv 0 \pmod{PA}$$

$$P \equiv 1 \pmod{P^c A}$$

Observemos si $i+j=1 \Rightarrow i, j$ son idempotentes complementearios en C/IJ .

$$\bar{i}^2 = \bar{i}^2 + \bar{i}\bar{j} = \bar{i}(\bar{i} + \bar{j}) = \bar{i}(1) = \bar{i}$$

$$j = \bar{i} - i$$

$\therefore \bar{i}, \bar{j}$ son idempotentes.

En el ejemplo anterior $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ es $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
 $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ es $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ si $I = J$

Ejercicio: Comprobar que: $(7 \cdot 18)^2 \equiv 7 \cdot 18 \pmod{12 \cdot 19}$.

Ejemplo: $\mathbb{Z}/_{12\mathbb{Z}} \cong \mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}/_{3\mathbb{Z}}$

$$P_1 = 4 \pmod{12}$$

$$D_1^c = -3 = 9 \pmod{12} \quad P_2 = 10$$

Respecto a todos los idempotentes formados $\mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}/_{3\mathbb{Z}}$ se tiene que $d = 18 \cdot 19$

$$\mathbb{Z}/_{30\mathbb{Z}} \cong \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{3\mathbb{Z}} \times \mathbb{Z}/_{5\mathbb{Z}}$$

$$6^2 \equiv 6 \pmod{30}$$

$$10^2 \equiv 10 \pmod{30}$$

$$(P+Q)^2 = P + 2PQ + Q = P + Q \text{ si } PQ = 0 \pmod{d} \quad d = x \circ b$$

$$\text{Ej: } 6, 10, 16, 25, 21, 15, 1, 0 \pmod{30} \quad d = x \circ b = 6$$

Correspondencias:

$$(100) \rightarrow 15 \quad (010) \rightarrow 10 \quad (001) \rightarrow 6$$

$$(110) \rightarrow 25 \quad (101) \rightarrow 21 \quad (011) \rightarrow 16$$

$$(111) \rightarrow 1$$

$$(100) \rightarrow 15 \quad (010) \rightarrow 10 \quad (001) \rightarrow 6$$

Así si tenemos que restar: $x \equiv a \pmod{30}$

$$(21) \pmod{30} \equiv (21) \pmod{5} \equiv 1$$

$$x \equiv c \pmod{5}$$

$$(15) \pmod{30} \equiv 15 \pmod{5} \equiv 0$$

$$(10) \pmod{30} \equiv 10 \pmod{5} \equiv 0$$

$$(6) \pmod{30} \equiv 6 \pmod{5} \equiv 1$$

Combinación de conjuntos:

$$A \subset X: \chi_A: X \rightarrow \mathbb{F}_2, \quad \underbrace{\chi_A^2}_{\text{idempotente.}} = \chi_A \wedge \chi_A = \chi_A$$

$$\chi_{A^c} = 1 - \chi_A$$

$$\chi_{A \cup B} = \chi_{(A^c \cap B^c)^c} = 1 - \chi_{A^c \cap B^c} = 1 - \chi_{A^c} \cdot \chi_{B^c} = 1 - (1 - \chi_A)(1 - \chi_B)$$

$$= \chi_A + \chi_B - \chi_A \chi_B$$

Si P_1, Q_1 son idempotentes: $P_1 Q_1 = P_1 Q_1$ son idempotentes.

Estabamos calculando: $12a \equiv x \pmod{12n}$

Sea: $a' = a + tn$ ($a' \equiv a \pmod{n}$) $a' = \{ \dots, -2, 0, 2, \dots \}$

$$12a' = 12a + 12tn \equiv 12a \pmod{12n} \quad \text{oríntate con el robot}$$

En general: $ax \equiv b \pmod{n}$ $\Rightarrow ax \equiv b \pmod{d}$

$$d = (a, n)$$

$$a = dc$$

$$n = dm$$

$$dcx \equiv b \pmod{dm}$$

$$dcx \equiv b \pmod{d} \quad (a \equiv 0 \pmod{d})$$

$$cx \equiv b \pmod{d}$$

$$b \equiv d \cdot e$$

$d \mid b$ & no hay soluc. si $d \nmid b$: $b \equiv d \cdot e$:

$$dex \equiv d \cdot e \pmod{dm}$$

$$(x \equiv e \pmod{m})$$

hay m soluciones distintas - módulo dm

Ejemplo: $12x \equiv 9 \pmod{15}$ $\Rightarrow d \mid c - b$

$$14x \equiv 3 \pmod{5}$$

$$x \equiv 2 \pmod{5}$$

Luego $x \equiv 2 \pmod{15}$, $x \equiv 2 + 5(15) \equiv 7(15)$.

$$(xy - 1)(x - 1)$$

$$= xy - x + y - 1$$

$$= xy - x - y + 1$$

?) (a) N° de extensiones del valor absoluto usual en $\mathbb{Q}(\sqrt[3]{2}) = L$

$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ extensión cúbica

$$m_{\sqrt[3]{2}}, \mathbb{Q}(x) = x^3 - 2$$

$$\begin{aligned} L \otimes_{\mathbb{Q}} \mathbb{Q}_\infty &= L \otimes_{\mathbb{Q}} \mathbb{R} \cong \frac{\mathbb{Q}[x]}{(x^3 - 2)} \otimes \mathbb{R} \cong \frac{\mathbb{R}[x]}{(x^3 - 2)} \\ &\cong \frac{\mathbb{R}[x]}{(x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + (\sqrt[3]{2})^2)} \end{aligned}$$

$$\Delta q(x) = (\sqrt[3]{2})^2 - 4(\sqrt[3]{2})^2 = \sqrt[3]{4} - 4\sqrt[3]{4} = -\sqrt[3]{4} < 0$$

$q(x)$ irreducible en \mathbb{R}

$$\therefore L \otimes_{\mathbb{Q}} \mathbb{R} \cong \frac{\mathbb{R}[x]}{(x - \sqrt[3]{2})} \times \frac{\mathbb{R}[x]}{(x^2 + \sqrt[3]{2}x + (\sqrt[3]{2})^2)} \cong \mathbb{R} \times \mathbb{C}$$

El valor absoluto usual se extiende de dos maneras en $\mathbb{Q}(\sqrt[3]{2})$, una real y una compleja.

(b) Probar con el valor absoluto 2-ádico:

$$L \otimes_{\mathbb{Q}} \mathbb{Q}_2 = \frac{\mathbb{Q}_2[x]}{(x^3 - 2)}$$

$$\text{si } \exists a \in \mathbb{Q}_2 : a^3 - 2 = 0 \Rightarrow |a^3 - 2|_2 = 0 \Rightarrow a^3 - 2 \equiv 0 \pmod{2^n}$$

$$\therefore a^3 - 2 \equiv 0 \pmod{2}$$

$$\therefore a \equiv 0 \pmod{2}.$$

$$\begin{aligned} f(x) &= x^3 - 2 \\ f'(x) &= 3x^2 \end{aligned} \quad \left\{ \rightarrow \text{parece que Hensel no sirve (?)} \right.$$

$$L_{\mathbb{Q}_2} \cong L_{P_1} \times \dots \times L_{P_r}, \quad P_i \text{ lugar sobre } 2$$

$$[L : K] = 3 = \sum_{i=1}^r \dim_{\mathbb{Q}_2} L_{P_i} = \sum_{i=1}^r e(L_{P_i}/\mathbb{Q}_2) f(L_{P_i}/\mathbb{Q}_2)$$

$$e(L_{P_i}/\mathbb{Q}_2) = e_i, \quad f(L_{P_i}/\mathbb{Q}_2) = f_i$$

$$\therefore 3 = \sum_{i=1}^r e_i f_i$$

$$3 = 1 + 1 + 1$$

$$= 1 + 2$$

$$= 3 + 0 \quad \checkmark \quad \text{Prueba}$$

$$\text{mod } 2: \quad f(x) = x^3 - 2 \equiv x^3, \quad f'(x) = 3x^2$$

f tiene raíces dobles.

Hecho

$$\frac{f}{1} \quad |^3 \sqrt{2}|_p^3 = |2|_p = |2|_2 = \frac{1}{2} \Rightarrow |^3 \sqrt{2}|_p = \frac{1}{3} \sqrt{2}$$

$\therefore \mathbb{Q}_2$ ramificado.

$\therefore | \cdot |_2$ se extiende sólo de una manera en $\mathbb{Q}(\sqrt[3]{2})$

Para $p=5$: Sea

$$\begin{array}{c} 8 \\ -1 \\ \hline 5 \end{array}$$

$$|\sqrt[3]{2}|_5 = |2|_5 = \frac{1}{5} \sqrt[5]{5^{(2)}} = \left(\frac{1}{5}\right)^0 = 1$$

$$\therefore |\sqrt[3]{2}|_5 = 1$$

(No hay información al respecto)

$$\begin{array}{l} f(x) = x^3 - 2 \equiv x^3 + 3 \quad ; \text{ mod } 5 . \\ f'(x) = 3x^2 \end{array} \quad \left| \begin{array}{l} 0^3 \equiv 0 \\ 1^3 \equiv 1 \\ 2^3 \equiv 3 \\ 3^3 \equiv 2 \end{array} \right. \quad 4^3 \equiv 4$$

f no tiene raíces dobles.

f tiene raíz en $\text{mod } 5$ $\xrightarrow{\text{Hensel}}$ f tiene raíz en \mathbb{Q}_5

$$\therefore L \otimes_{\mathbb{Q}} \mathbb{Q}_5 \cong \mathbb{Q}_5 \times L_5$$

A² Si f tiene raíces en $\mathbb{Q}_5 \iff f$ tiene raíces mod 5.

$$L \Rightarrow L \otimes_{\mathbb{Q}} \mathbb{Q}_5 \cong \mathbb{Q}_5 \times L_5$$

$\therefore 1 \cdot 1_5$ se extiende en dos raíces en $\mathbb{Q}(\sqrt[3]{2})$.

\downarrow \uparrow
solo auto?

$$PZ_1 \quad \Lambda = (1, 2, 3) \mathbb{Z} \oplus (1, 4, 5) \mathbb{Z} \oplus (1, 6, 8) \mathbb{Z}$$

Af. $\Lambda_0 = \mathbb{Z}^3 \Rightarrow \Lambda_p = \Lambda_{0p}$ para todo p .

Af. $\Lambda = T\Lambda_0$, $T(\hat{e}_1) = (1, 2, 3)$, $T(\hat{e}_2) = (1, 4, 5)$, $T(\hat{e}_3) = (1, 6, 8)$, $B = \{\hat{e}_1, \hat{e}_2, \hat{e}_3\}$

$$[T]_B = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 4 & 6 \\ 3 & 5 & 8 \end{pmatrix} = A$$

$$\det [T]_B = \begin{vmatrix} 4 & 6 \\ 5 & 8 \end{vmatrix} - \begin{vmatrix} 2 & 6 \\ 3 & 8 \end{vmatrix} + \begin{vmatrix} 2 & 4 \\ 3 & 5 \end{vmatrix} \\ = (32 - 30) - (16 - 18) + (10 - 12) = 2 - (-2) + 2 = 2$$

$$\left(\begin{array}{ccc|cc} 1 & 1 & 1 & 1 & 1 \\ 2 & 4 & 6 & & 1 \\ 3 & 5 & 8 & & 1 \end{array} \right) \xrightarrow{\quad} \left(\begin{array}{ccc|ccc} 1 & 1 & 1 & \frac{1}{2} & 0 & 0 \\ 0 & 2 & 4 & -2 & 1 & 0 \\ 0 & 2 & 5 & -1 & -1 & 1 \end{array} \right)$$

$$\xrightarrow{\quad} \left(\begin{array}{ccc|ccc} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 2 & 4 & -2 & 1 & 0 \\ 0 & 0 & 1 & -1 & -1 & 1 \end{array} \right)$$

$$\xrightarrow{\quad} \left(\begin{array}{ccc|ccc} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 2 & 0 & 2 & 5 & -4 \\ 0 & 0 & 1 & -1 & -1 & 1 \end{array} \right)$$

$$\xrightarrow{\quad} \left(\begin{array}{ccc|ccc} 1 & 1 & 0 & 2 & 1 & -1 \\ 0 & 2 & 0 & 2 & 5 & -4 \\ 0 & 0 & 1 & -1 & -1 & 1 \end{array} \right)$$

$$\xrightarrow{\quad} \left(\begin{array}{ccc|ccc} 1 & 1 & 0 & 2 & 1 & -1 \\ 0 & 1 & 0 & 1 & 5/2 & -2 \\ 0 & 0 & 1 & -1 & -1 & 1 \end{array} \right)$$

$$\xrightarrow{\quad} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & -3/2 & 1 \\ 0 & 1 & 0 & 1 & 5/2 & -2 \\ 0 & 0 & 1 & -1 & -1 & 1 \end{array} \right)$$

$$A^{-1} = \left(\begin{array}{ccc} 1 & -3/2 & 1 \\ 1 & 5/2 & -2 \\ -1 & -1 & 1 \end{array} \right) \\ = \frac{1}{2} \left(\begin{array}{ccc} 2 & -3 & 2 \\ 2 & 5 & -4 \\ -2 & -2 & 2 \end{array} \right)$$

$$A \in M_3(\mathbb{Q})^*$$

Hemos. $\frac{m}{n} \in \mathbb{Q}:$
 $\frac{m}{n} \in \mathbb{Z}_p \Leftrightarrow \left| \frac{m}{n} \right|_p \leq 1$
 $\Rightarrow p \nmid n$

Hemos. $T\Lambda_0 = \Lambda_0$
 $\Rightarrow T \in GL(\mathbb{Z})^*$

pero $T\Lambda_0 = \Lambda = (1, 2, 3) \mathbb{Z} \oplus (1, 4, 5) \mathbb{Z} \oplus (1, 6, 8) \mathbb{Z}$

$A \in \mathcal{M}_{3 \times 3}(\mathbb{Z}_p)^*$ \Leftrightarrow coef $\in \mathbb{Z}_p$

$A = \frac{1}{2} \begin{pmatrix} 2 & -3 & 2 \\ 2 & 5 & -4 \\ -2 & -2 & 2 \end{pmatrix}$ se cumple k_p nulo $p=2$ ($p \mid 2$).

P3 $W \subseteq V$ esp-vec. dimensión finita

$$\begin{array}{ccc} W & \subseteq & V \\ \cup & & \cup \\ M & \xrightarrow{\quad} & \Lambda \\ & & \searrow \\ & & \text{reticulados} \end{array}$$

Pd: $M_p \subseteq \Lambda_p$ para casi todo p .

$$V = K^n, W = K^m \quad (m \leq n)$$

$$W \hookrightarrow V \rightarrow W = K^m \times \{0\}^{n-m}$$

Λ \mathcal{O}_K -submódulo de K^n

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

M \mathcal{O}_K -submódulo de K^m

$$\tilde{\beta} \mathcal{O}_K^m \subseteq M \subseteq \tilde{\alpha} \mathcal{O}_K^m$$

K^m \mathcal{O}_K -submódulo de K^n : $K^m \cong K^m \times \{0\}^{n-m}$
(como \mathcal{O}_K -módulos)

$\therefore M$ es un \mathcal{O}_K -submódulo de K^n

$\therefore M, \Lambda$ \mathcal{O}_K -submódulos de $K^n \rightarrow M_p \subseteq \Lambda_p$ casi todo p .

Tenemos el anillo \mathbb{Q}_p (completado de \mathbb{Q} bajo $l \cdot l_p$), y

$$\mathbb{Z}_p = \text{cls}_{\mathbb{Q}_p}(\mathbb{Z})$$

Afirmación. $n_1, n_2 \in \mathbb{Z}$ satisfacen $|n_1 - n_2|_p < \varepsilon$

$\iff n_1 \equiv n_2 (p^r)$ para algún r que satisfaga $p^r < \varepsilon$.

Demotración.

$$(\Rightarrow) |n_1 - n_2|_p < \varepsilon \iff p^{-v_p(n_1 - n_2)} < \varepsilon$$

Tomamos $r = v_p(n_1 - n_2)$, $r \in \{0, 1, 2, \dots\}$

Cumple $p^{-r} < \varepsilon$ y $p^r \mid (n_1 - n_2)$

O de manera equivalente, $n_1 \equiv n_2 (p^r)$

(\Leftarrow) Supongamos que $n_1 \equiv n_2 (p^r)$ para algún r que cumple $p^{-r} < \varepsilon$

$$\Rightarrow \text{Si } n_1 \equiv n_2 (p^r) \iff v_p(n_1 - n_2) \geq r$$

$$\therefore |n_1 - n_2|_p = p^{-v_p(n_1 - n_2)} \leq p^{-r} < \varepsilon$$

$$\therefore |n_1 - n_2|_p < \varepsilon$$

Sea $\{a_n\}_{n \in \mathbb{N}}$ sucesión. $\{a_n\}_n$ es de Cauchy si:

$$\forall \epsilon > 0, \exists N \in \mathbb{N} : \forall i, j > N \Rightarrow |a_i - a_j|_p < \epsilon$$

Afirmación: La sucesión $\{a_n\}_{n \in \mathbb{N}}$ en \mathbb{Z}_p es de Cauchy si

$$\forall r \in \mathbb{N}, \exists N \in \mathbb{N} \text{ tal que } \forall i, j > N \Rightarrow a_i = a_j (p^r) \quad (*)$$

Demostración:

(\Rightarrow) Supongamos que $\{a_n\}_n$ es de Cauchy

$$\forall r \in \mathbb{N}, \exists N \in \mathbb{N} : \forall i, j > N \Rightarrow |a_i - a_j|_p < p^{-(r-1)}$$

pero $|a_i - a_j|_p < p^{-(r-1)}$ implica que $\nu_p(a_i - a_j) \geq r$,
ya que $|a_i - a_j|_p = p^{-\nu_p(a_i - a_j)} < p^{-(r-1)}$

$$\therefore p^r |(a_i - a_j)$$

$$\therefore a_i = a_j (p^r)$$

(\Leftarrow) Supongamos que $\{a_n\}_{n \in \mathbb{N}}$ cumple (*)

Sea $\epsilon > 0$, existe $r \in \mathbb{N}$ tal que $p^{-r} < \epsilon$

Para tal $r \in \mathbb{N}$, existe $N \in \mathbb{N}$ tal que

$$\forall i, j > N \Rightarrow a_i = a_j (p^r)$$

$$\text{pero } p^r |(a_i - a_j) \Rightarrow \nu_p(a_i - a_j) \geq r$$

$$\therefore |a_i - a_j|_p \leq p^{-r} < \epsilon$$

Propiedades básicas de los p-ádicos.

Hecho: Cada $m \in \mathbb{Z}_+^*$ puede escribirse de la forma

$$m = a_0 + a_1 p + a_2 p^2 + \dots + a_k p^k$$

donde $p \in \mathbb{Z}$ primo y $a_i \in \{0, \dots, p-1\} \quad \forall i=0, \dots, k$

Ejemplo. $\frac{25}{2} = 2^4 + 2^3 + 1$

Corolario. Sean $a = a_0 + a_1 p + \dots + a_n p^n$; $b = b_0 + b_1 p + \dots + b_m p^m$ $\in \mathbb{Z}_+^*$, entonces

$$a \equiv b \pmod{p^r} \Leftrightarrow a_i \equiv b_i \quad , \quad i \in \{0, \dots, p^{r-1}\}$$

(Coincidencia en la cifra r)

Para el caso de los negativos tenemos

$$-1 = \lim_{n \rightarrow \infty} p^n - 1 = (p-1) + (p-1)p + (p-1)p^2 + \dots$$

Conclusión: $a \in \mathbb{Z}_{(p)}$ puede pensarse como una expansión infinita en base p , es decir:

$$a = a_0 + a_1 p + a_2 p^2 + \dots + a_k p^k + \dots , \quad 0 \leq a_i \leq p-1$$

Proposición. Un entero $n \in \mathbb{Z}$ es una unidad en \mathbb{Z}_p si y sólo divide a n .

$$n \in \mathbb{Z} : n \in \mathbb{Z}_p^* \Leftrightarrow p \nmid n$$

$$\text{Primero: } n = a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots + a_k p^k$$

Segundo: $\mathbb{Z}/(p^r)$ sólo contiene unidades y nilpotentes

$$(\text{Si } p \nmid n \Rightarrow n = \alpha p \rightarrow n^r = \alpha^r p^r \rightarrow \bar{n}^r \equiv \bar{\alpha} \in \mathbb{Z}/(p^r))$$

(\Leftarrow) Si $p \nmid n$, entonces $n + p^r \mathbb{Z}$ es unidad en $\mathbb{Z}/(p^r) \quad \forall r \in \mathbb{Z}^+$.

Sea $m_r \in \mathbb{Z} : m_r n \equiv 1 \pmod{p^r}$ (el inverso de n mod p^r)

Ahora, si $s > r \Rightarrow m_s n \equiv 1 \pmod{p^s}$ y además

$$m_s n \equiv 1 \pmod{p^s} \Leftrightarrow p^s \mid m_s n - 1 \Rightarrow p^r \mid m_s n - 1$$

$$\therefore m_s n \equiv 1 \pmod{p^r}$$

$$\therefore m_r \equiv m_s \pmod{p^r} \quad s > r$$

En particular $m_i \equiv m_j \pmod{p^r}$ cuando $i, j > r$. Con ello obtenemos que $\{m_j\}_{j \in \mathbb{N}}$ es de Cauchy en \mathbb{Z} .

Pasando al límite, $\lim_{j \rightarrow \infty} m_j = m$, donde $mn = 1$

$$\therefore n \in \mathbb{Z}_p^*$$

(\Rightarrow) Si $p \mid n \Rightarrow |n|_p < 1$. Luego para cualquier $m \in \mathbb{Z}_p$ debe cumplirse que $|mn|_p = |m|_p |n|_p < |m|_p \leq 1$

$$\therefore |mn|_p < 1$$

Luego n no puede ser invertible. (En el caso de existir inversa $n' \in \mathbb{Z}_p$: $nn' = 1$ y $|nn'|_p = 1$).

Corolario. $\mathbb{Z}_p \cap \mathbb{D} = \left\{ \frac{n}{m} \mid m \notin p\mathbb{Z} \right\}$

Proposición. $\mathbb{Z}_p = \{ z \in \mathbb{Q}_p \mid |z|_p \leq 1 \}$

Si $n \in \mathbb{Z}$ $\Rightarrow |n|_p \leq 1$

$\Rightarrow z \in \mathbb{Z}_p \Rightarrow z = \lim_{j \rightarrow \infty} z_j$ donde $\{z_j\}$ sucesión en \mathbb{Z} .

$$|z|_p = \left| \lim_{j \rightarrow \infty} z_j \right| = \lim_{j \rightarrow \infty} |z_j| \leq 1 \therefore |z|_p \leq 1$$

Supongamos ahora que $z \in \mathbb{Q}_p \Rightarrow z = \lim_{j \rightarrow \infty} z_j$ $\{z_j\}$ sucesión en \mathbb{Q} (de Cauchy).

Si $|z| \leq 1 \Rightarrow |z_j| \leq 1$ para j suficientemente grande.

pero $|z_j| \leq 1 \Rightarrow z_j \in \mathbb{Z}_p \quad j \geq 1$

Como \mathbb{Z}_p es cerrado, $\lim_{j \rightarrow \infty} z_j = z \in \mathbb{Z}_p$.

Recordatorio. ¿ $z \in \mathbb{D} : |z|_p \leq 1 \Rightarrow z \in \mathbb{Z}_p$?

Importante saberlo.

$z = \frac{a}{b}$ donde $|z|_p = \left| \frac{a}{b} \right|_p \leq 1 \Rightarrow p \nmid b$, sea

$z = a \cdot \frac{1}{b}$, donde $a, \frac{1}{b} \in \mathbb{Z}_p$. Luego $z \in \mathbb{Z}_p$.

Lema. Para dos elementos en \mathbb{Q}_p , siempre se tiene que $|z_1 + z_2|_p \leq \max \{|z_1|_p, |z_2|_p\}$

Demonstración.

Para el caso en que $z_1, z_2 \in \mathbb{Z}_p$, se cumple automáticamente que

$$|z_1 + z_2|_p \leq \max \{|z_1|_p, |z_2|_p\}$$

por propiedad de la norma p -ádica.

Si $z_1, z_2 \in \mathbb{Q} \Rightarrow \exists N \in \mathbb{N}$ tal que $Nz_1, Nz_2 \in \mathbb{Z}_p$:
luego

$$|Nz_1 + Nz_2|_p \leq \max \{|Nz_1|_p, |Nz_2|_p\}$$

$$\Rightarrow |N|_p |z_1 + z_2|_p \leq |N|_p \max \{|z_1|_p, |z_2|_p\}$$

$$\therefore |z_1 + z_2|_p \leq \max \{|z_1|_p, |z_2|_p\}$$

Ahora si $z_1, z_2 \in \mathbb{Q}_p$, donde $z_1 = \lim_{j \rightarrow \infty} z_j^1$, $z_2 = \lim_{j \rightarrow \infty} z_j^2$
 $\{z_j^1\}, \{z_j^2\}$ sucesiones en \mathbb{Q} .

$$\forall j: |z_j^1 + z_j^2|_p \leq \max \{|z_j^1|_p, |z_j^2|_p\}$$

$$\lim_{j \rightarrow \infty} |z_j^1 + z_j^2|_p \leq \lim_{j \rightarrow \infty} \max \{|z_j^1|_p, |z_j^2|_p\}$$

$$\left| \lim_{j \rightarrow \infty} z_j^1 + \lim_{j \rightarrow \infty} z_j^2 \right|_p \leq \max \left\{ \left| \lim_{j \rightarrow \infty} z_j^1 \right|_p, \left| \lim_{j \rightarrow \infty} z_j^2 \right|_p \right\}$$

$$|z_1 + z_2|_p \leq \max \{|z_1|_p, |z_2|_p\}$$

Observación. $|\cdot|_p$, $\max \{\cdot, \cdot\}$ son funciones continuas.

Lema. Para $z_1, z_2 \in \mathbb{Q}_p$, con $|z_1|_p < |z_2|_p$ se tiene que $|z_1 + z_2|_p = |z_2|_p$

Demostación. Por la desigualdad triangular fuerte

$$|z_1 + z_2|_p \leq \max \{|z_1|_p, |z_2|_p\} = |z_2|_p$$

$$\text{Ahora, } |z_2|_p = |z_1 + (z_2 - z_1)|_p$$

$$\leq \max \{|z_1|_p, |z_2 - z_1|_p\}$$

$$= \max \{|z_1|_p, |z_2 + z_1|_p\}$$

$$\therefore |z_2|_p \leq |z_1 + z_2|_p.$$

$$\text{Conclusion, } |z_1 + z_2|_p = |z_2|_p.$$

Lema. El valor absoluto $|z|_p$ de cualquier elemento $z \in \mathbb{Q}_p$ es un elemento de $p^{\mathbb{Z}}$.

Demostación. Sea $z \in \mathbb{Q}_p$, entonces $z = \lim_{j \rightarrow \infty} r_j$

donde $r_j \in \mathbb{Q}$ $\forall j$. Luego para j suficientemente grande

$$|r_j - z|_p \leq |z|_p$$

Ahora por el principio de dominancia:

$$\forall j \gg 1 \quad |z|_p = |r_j - z + z|_p = |r_j|_p = p^{-v_p(r_j)}$$

(Este resultado es super importante)

Proposición: El conjunto $m_p = \{z \in \mathbb{Q}_p \mid |z|_p < 1\}$ es el único ideal maximal de \mathbb{Z}_p , y es un ideal generado por p .

Demonstración:

Pd: m_p es un ideal de \mathbb{Z}_p

Sean ~~$a_1, a_2 \in m_p$~~ $a_1, a_2 \in m_p$ y $b \in \mathbb{Z}_p$

$$|a_1 + a_2|_p \leq \max\{|a_1|_p, |a_2|_p\} < 1$$

$$|a_1 a_2|_p = |a_1|_p |a_2|_p < 1 \cdot 1 = 1$$

$$|ba_1|_p = |b|_p |a_1|_p \leq |a_1|_p < 1$$

$$\therefore m_p \trianglelefteq \mathbb{Z}_p$$

Pd: m_p es maximal

Si $\mu \in \mathbb{Z}_p \setminus m_p \Rightarrow |\mu|_p = 1 \Rightarrow \mu \in \mathbb{Z}_p^*$.

$$\therefore (\mu) = \mathbb{Z}_p$$

Pd: $m_p = (p) = p \mathbb{Z}_p$

Sea $z \in m_p \Rightarrow |z|_p$ es un elemento de $p \mathbb{Z}$

En particular, $|z|_p < \frac{1}{p}$

$$|\frac{z}{p}|_p = |z|_p |p|_p < 1 \cdot \frac{1}{p} < 1 \quad \therefore \frac{z}{p} \in \mathbb{Z}_p \Rightarrow z \in p \mathbb{Z}_p$$

$$\therefore m_p = p \mathbb{Z}_p$$

Proposición. El mero cociente $\mathbb{Z}/p\mathbb{Z}_p$ es isomorfo a $\mathbb{Z}/p\mathbb{Z}$

Demostración. Tenemos la aplicación $\psi: \mathbb{Z} \rightarrow \mathbb{Z}_p/p\mathbb{Z}_p$ dada por $\psi(a) = a + p\mathbb{Z}_p$ (homomorfismo de anillos).

Obviamente $\ker \psi = p\mathbb{Z}_p \cap \mathbb{Z} = p\mathbb{Z}$, induciendo así la inyectividad

$$\tilde{\psi}: \mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathbb{Z}_p/p\mathbb{Z}_p$$

Sea A el subanillo de $\mathbb{Z}_p/p\mathbb{Z}_p$ tal que $A \cong \mathbb{Z}/p\mathbb{Z}$

Pd : $A = \mathbb{Z}_p/p\mathbb{Z}_p$.

Sea $\bar{a} \in \mathbb{Z}_p/p\mathbb{Z}_p \Rightarrow a \in \mathbb{Z}_p$. Como $\text{cls}(\mathbb{Z}) = \mathbb{Z}_p$ (\mathbb{Z} es denso en \mathbb{Z}_p) tenemos que existe $a_n \in \mathbb{Z}$ tal que

$$|a_n - a|_p < \frac{1}{p} < 1$$

$$\therefore a_n - a \in m_p$$

Lo que es equivalente a que $a_n \equiv a \pmod{m_p}$

$$\therefore \bar{a}_n = \bar{a} \quad (\tilde{\psi} \text{ epiyectiva})$$

Conclusion: $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$. □

Notemos el diagrama:

$$\begin{array}{ccc}
 \mathbb{Z} & \xrightarrow{\psi} & \mathbb{Z}_p/p\mathbb{Z}_p \\
 p \downarrow & & \downarrow \psi \\
 \mathbb{Z}/p\mathbb{Z} & &
 \end{array}
 \quad \psi \circ p = \psi$$

Corolario. $\mathbb{Z}/p^r\mathbb{Z} \cong \mathbb{Z}_p/p^r\mathbb{Z}_p$

Dem. Repetimos el mismo argumento anterior, considerando el homomorfismo de anillos $\psi: \mathbb{Z}/p^r\mathbb{Z} \rightarrow \mathbb{Z}_p/p^r\mathbb{Z}_p$

Donde $\psi(a + (p^r)) = a + (p^r)$. ψ es inyectiva ya que si $a + (p^r) = 0 + (p^r) \Rightarrow a \in (p^r) \cap \mathbb{Z} = p\mathbb{Z}$
 $\therefore a \in p\mathbb{Z}$ (lo mismo que decir $\bar{a} = \bar{0}$).

Falta demostrar que ψ es sobre: Sea $\bar{a} \in \mathbb{Z}_p/p^r\mathbb{Z}_p$

$\Rightarrow a \in \mathbb{Z}_p$, como \mathbb{Z} es dominio en \mathbb{Z}_p , existe $a_n \in \mathbb{Z}$ tal que $|a_n - a|_p < \frac{1}{p^r}$

Considerando $b = \frac{a_n - a}{p^r}$, $|b|_p = \frac{|a_n - a|_p}{|p^r|_p} \leq \frac{\frac{1}{p^r}}{\frac{1}{p^r}} = 1$

$\therefore b \in \mathbb{Z}_p$

Aquí $a_n - a = bp^r \Rightarrow a_n - a \in (p^r) = p^r\mathbb{Z}_p$ ($\bar{a}_n = \bar{a}$)

Conclusion: $\mathbb{Z}/p^r\mathbb{Z} \cong \mathbb{Z}_p/p^r\mathbb{Z}_p$.

Proposición. Sea $r \in \mathbb{Q}$. Entonces $r \in \mathbb{Z}$ si $r \in \mathbb{Z}_p$ para cada primo p .

Demarcación. Si $r = \frac{a}{b}$, $\text{mcd}(a, b) = 1$, entonces $p \nmid b$ para ningún $p \in \mathbb{Z}$ primo $\Leftrightarrow b = \pm 1$. Lo que es equivalente a que

$$\frac{a}{b} \in \mathbb{Z}_p.$$

Corolario. Sea $r \in \mathbb{Q}$. Entonces $r \in \mathbb{Z}_p^*$ para cada primo p si $r = \pm 1$.

Demarcación. $r \in \mathbb{Z}_p^* \Leftrightarrow v_p(r) = 0 \Leftrightarrow p \nmid r$ para ningún p . $\therefore r = \pm 1$.

Valores absolutos no arquimedios

Definición. Sea K cuerpo, ρ valor absoluto en K .
 (K, ρ) es no arquimediano si $\forall a, b \in K$

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

Recordatorio. K tiene una copia isomorfa de \mathbb{Z} (\mathbb{Z}_K)

Lema. Si $\mathbb{Z}_K \subset K$ es acotado (por ρ), entonces $\mathbb{Z}_K \subseteq B[0_K, 1]$

Demarcación. Sea $n_K \in \mathbb{Z}_K$ ($n_K = \underbrace{1_K + \dots + 1_K}_{n-\text{veces}}$)

$$\rho(n_K) \leq R. \text{ Además } \forall t \in \mathbb{N}, \rho(n_K^t) \leq R$$

$$\rho(n_K^t) = \rho(n_K)^t \leq R \rightarrow \rho(n_K) \leq R \xrightarrow[t \rightarrow \infty]{} 1$$

$$\therefore \rho(n_K) \leq 1$$

$$\therefore \mathbb{Z}_K \subseteq B[0_K, 1]$$

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

Dem. (\Rightarrow) Supongamos que (K, ρ) es no arquimediano.

$$\rho(2_K) = \rho(1_K + 1_K) \leq \max\{\rho(1_K), \rho(1_K)\} = \rho(1_K)$$

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

Por inducción $\forall n \in \mathbb{N}$: $\rho(n_K) \leq \rho(1_K)$

Ahora como $\rho(-t_K) = \rho(t_K) \Rightarrow \rho(-n_K) = \rho(n_K)$

$$\therefore \rho(-n_K) \leq \rho(t_K)$$

Se concluye así que \mathbb{Z}_K es acotado.

(\Leftarrow) Supongamos que \mathbb{Z}_K es acotado. Por demostrar que (K, ρ) es no arquimediano.

Trivialmente se cumple si $a=0$, $b=0$.

Para $a, b \neq 0$, notar que si $\rho(a) \leq \rho(b)$

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

donde $\rho(\frac{a}{b}) \leq 1$.

Luego basta demostrar que $\rho(1_K + a) \leq 1$ cuando $\rho(a) \leq 1$ ($\rho(1_K) = 1$)

$$\begin{aligned} \text{Tenemos: } \rho(1+a)^n &= \rho((1+a)^n) \\ &= \rho\left(\sum_{j=0}^n \binom{n}{j} a^j\right) \\ &= \sum_{j=0}^n \rho\left(\binom{n}{j}\right) \rho(a)^j \end{aligned} \quad (n \in \mathbb{N})$$

Como $\binom{n}{j} \in \mathbb{Z}_K$, $\rho\left(\binom{n}{j}\right) \leq 1$

$$\therefore \rho(1+a)^n \leq \sum_{j=0}^n 1 \cdot \rho(a)^j \leq \sum_{j=0}^n 1 = n+1$$

$$\therefore \rho(1+a) \leq \sqrt[n]{n+1} \xrightarrow{n \rightarrow \infty} 1$$

Así $p(a+1) \leq 1$ cuando $p(a) \leq 1$. El resto sigue fácil.

Corolario. Si $\text{char } K > 0 \Rightarrow K$ es no arquimediano.

En efecto, ya que \mathbb{Z}_K tiene p elementos (p primo).

Generalización

Sea K no arquimediano, completo

$$\mathcal{O}_K = \{\alpha \in K \mid p(\alpha) \leq 1\}$$

$$m_K = \{\alpha \in K \mid p(\alpha) < 1\}$$

\mathcal{O}_K es un subanillo de K y m_K ideal maximal de \mathcal{O}_K
(análogo para \mathbb{Z}_p y $p\mathbb{Z}_p$).

Definición. \mathcal{O}_K/m_K se llama cuerpo residual de K

Observación. $p(K^*)$ es subgrupo de $R_{>0} \cong \mathbb{R}$ (logaritmo)

Definición. p se dice discreto si $p(K^*)$ discreto en $R_{>0}$.

(*) Hecho. $p(K^*) = c^{\mathbb{Z}}$, $c \in (0, 1)$

Cuando $p(K^*) = \{1\}$, p es el valor absoluto trivial, o sea

$$p(x) = \begin{cases} 0 & , x=0 \\ 1 & , x \neq 0 \end{cases}$$

Hecho. Cuando p es discreto y no trivial, existe $\pi \in K$ tal que $p(\pi) = c$ (π se llama parámetro uniformizante)

Hecho. Como $\rho(\pi) = c < 1 \Rightarrow \pi \in m_K$

Como $\rho(a) < 1$ cuando $a \in m_K$ y $\rho(a) = c^t$, entonces $t \in \mathbb{Z}_+$. En particular $\rho(a) \leq \rho(\pi)$

$$\rho(a) \leq \rho(\pi) \Rightarrow \rho\left(\frac{a}{\pi}\right) \leq 1$$

$$\therefore \frac{a}{\pi} \in \mathcal{O}_K$$

$$\therefore a \in \pi \mathcal{O}_K$$

Se concluye así que $m_K = (\pi)$.

Hecho. Sea $a \in K$, $\rho(a) = c^t$, donde $t \in \mathbb{Z}$.

Pero $\rho(\pi) = c$

$$\therefore \rho(a) = \rho(\pi^t)$$

$$\text{Así } \rho\left(\frac{a}{\pi^t}\right) = 1 \Rightarrow \frac{a}{\pi^t} \in \mathcal{O}_K^*$$

Por lo tanto,

$$\boxed{a \in K : a = \pi^t u, t \in \mathbb{Z}, u \in \mathcal{O}_K^*}$$

(Definición de división en K dividir entre π)

Lo anterior nos permite generalizar la expresión de los elementos de \mathcal{O}_K al igual como se hizo con \mathbb{Z}_p .

Sea K cuerpo completo con valor absoluto p .

$S \subset \mathcal{O}_K$ conjunto de representantes de \mathcal{O}_K/m_K , $o \in S$

$$\forall a \in \mathcal{O}_K : a = s_0 + s_1 \pi + s_2 \pi^2 + \dots + s_n \pi^n + s_{n+1} \pi^{n+1}$$

donde $s_i \in S$ y $s_{n+1} \pi^{n+1} \xrightarrow{} 0$.

Luego $a \in \mathcal{O}_K$ puede verse de la forma :

$$a = s_0 + s_1 \pi + s_2 \pi^2 + s_3 \pi^3 + \dots$$

Más generalmente : Sea $a \in K$

$$a = \pi^t u ; t \in \mathbb{Z}, u \in \mathcal{O}_K$$

$$a = \pi^t (s_0 + s_1 \pi + s_2 \pi^2 + \dots)$$

$$a = s_0 \pi^t + s_1 \pi^{t+1} + s_2 \pi^{t+2} + \dots \quad (s_0 \neq 0)$$

Ejemplo. $\mathbb{Z}_p = \{a_0 + a_1 p + a_2 p^2 + \dots / a_i \in \{0, \dots, p-1\}\}$

$\mathcal{O}_p = \{a_n p^n + a_{n+1} p^{n+1} + \dots / a_i \in \{0, 1, \dots, p-1\} \cup \{0\}\}$
 $t \in \mathbb{Z}$

Valores absolutos en \mathbb{Q}

Definición. Sean p, p' valores absolutos. p, p' se dicen equivalentes si $\exists \lambda > 0$ tal que

$$p'(a) = p(a)^\lambda \quad \forall a \in K.$$

Observación. Dos valores absolutos equivalentes p, p' definen las mismas sucesiones de Cauchy

* Proposición. Si p, p' son valores absolutos no equivalentes en K , entonces

$$\Delta_K = \{ (a, a) / a \in K \}$$

es densa en $K_p \times K_{p'}$.

La proposición anterior tiene la siguiente consecuencia:

Teorema (aproximación débil).

Si p_1, \dots, p_n valores absolutos en K no equivalentes entre sí, entonces para cada $a_1, \dots, a_n \in K$ existe una sucesión $(b_k)_{k \in \mathbb{N}}$ tal que $b_k \xrightarrow[p_i]{} a_i$.

Teoría de Números

Desarrollo Guía 6

Problema 1. Probar que si una función $\rho: K \rightarrow [0, \infty)$ definida en un cuerpo K , satisface las condiciones siguientes

$$(a) \rho(x) = 0 \Leftrightarrow x = 0$$

$$(b) \rho(ab) = \rho(a)\rho(b)$$

$$(c) \rho(u) \leq 1 \Rightarrow \rho(1+u) \leq 1$$

entonces ρ es un valor absoluto y satisface la desigualdad triangular fuerte

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

Demonstración

Debemos demostrar que $\forall a, b \in K : \rho(a+b) \leq \rho(a) + \rho(b)$, & de manera equivalente,

$$\begin{aligned} \rho(a+b) \leq \rho(a) + \rho(b) &\Leftrightarrow \rho(a)\rho\left(1 + \frac{b}{a}\right) \leq \rho(a)\left(1 + \frac{\rho(b)}{\rho(a)}\right) \\ &\Leftrightarrow \rho\left(1 + \frac{b}{a}\right) \leq 1 + \frac{\rho(b)}{\rho(a)} \end{aligned}$$

Pd: $\forall u \in K : \rho(1+u) \leq 1 + \rho(u)$

(Sólo estudian casos en que $u \neq 0$, cuando $a, b, u = 0$ es trivial)

$$\rho(u) \leq 1 : \rho(u) \leq 1 \Rightarrow \rho(1+u) \leq 1 \leq 1 + \rho(u)$$

$$\rho(u) \geq 1 : \rho(1) \leq 1 \leq \rho(u) \Rightarrow \rho\left(\frac{1}{u}\right) \leq 1$$

$$\begin{aligned} \rho(u+1) &= \rho(u)\rho\left(1 + \frac{1}{u}\right) \leq \rho(u)(\rho(1) + \rho\left(\frac{1}{u}\right)) = \rho(u) + \rho(u)\rho\left(\frac{1}{u}\right) \\ &= \rho(u) + \rho(1) \leq \rho(u) + 1 \end{aligned}$$

∴ Se cumple la desigualdad triangular

Por demostrar: $p(a+b) \leq \max\{p(a), p(b)\} \quad \forall a, b$

Supongamos que $p(a) \leq p(b)$

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

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

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

Análogamente, si $p(b) \leq p(a) \Rightarrow p(a+b) \leq p(a)$

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

Anexo. Estudiar $p(\mathbb{Z})$ ($\mathbb{Z} \hookrightarrow K$)

Tenemos que $p(0) = 0$, $\Rightarrow p(1) \leq 1$.

Pero $p(1) = p(1)^2 \geq 0 \Rightarrow p(1) = 1 \quad \forall p \text{ valor absoluto en } K$

cuando $a \in \mathbb{N}$:

$p(1) \leq 1 \Rightarrow p(n) \leq 1 \quad (\text{inductivamente})$

$$\therefore p(\mathbb{N}) \subseteq B[0, 1]$$

$-a \in \mathbb{N}^-$: $p(-a) = p(-1) p(a) \leq p(-1)$

pero $p(-1) = p(1) p(-1) \quad \because p(-1) = 1$

$$p(\mathbb{Z}) \subseteq B[0, 1]$$

Problema 2. Probar que si ρ es un valor absoluto en K , entonces para todo $x \in K$ se tiene $\rho(-x) = \rho(x)$.

Demotstración. Se ve que $\rho(x)^2 = \rho(x^2) = \rho(-x)^2$
 $\therefore \rho(x)^2 - \rho(-x)^2 = 0$

$$\rho(x)^2 - \rho(-x)^2 = (\rho(x) - \rho(-x))(\underbrace{\rho(x) + \rho(-x)}_{\geq 0})$$

cuando $x \neq 0$ (caso $x=0$ es fácil):

$$\rho(x)^2 - \rho(-x)^2 = 0 \iff \rho(x) = \rho(-x).$$

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

$$(a). a_n = 2^n, p = 2$$

$$|a_n|_2 = |2^n|_2 = |2|_2^n, \text{ pero } |2|_2 = 2^{-v_2(2)} = 2^{-1} = \frac{1}{2}.$$

$$\text{Así que } |a_n|_2 = \frac{1}{2^n} \xrightarrow{n \rightarrow \infty} 0$$

$$\text{Obvio que } a_n \xrightarrow{| \cdot |_2} 0$$

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

Como $|2^n|_2 = \frac{1}{2^n}$, entonces $|2^{-n}| = 2^n$. Luego la sucesión $a_n = 2^{-n}$ no está acotada en $| \cdot |_2$. Luego no puede converger.

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

$$\text{Por álgebra, } 1 + 2 + 2^2 + \dots + 2^n = \frac{2^{n+1} - 1}{2 - 1} = 2^{n+1} - 1$$

$$\text{Nuestro candidato a límite es } a = \frac{1}{1-2} = -1$$

$$a_n - a = \frac{2^{n+1}}{2-1} = 2^{n+1}; \quad |a_n - a|_2 = |2^{n+1}|_2 \xrightarrow{n \rightarrow \infty} 0$$

$$\therefore (a_n) \text{ es convergente y } a_n \xrightarrow{| \cdot |_2} -1.$$

$$(d) a_n = 1 + 4^n$$

Primero veamos que (b_n) , $b_n = 4^n = 2^{2n}$ es una subsecuencia de $c_n = 2^n$, y por lo que vimos $c_n \xrightarrow{1+1_2} 0$.
Además $1 \xrightarrow{1+1_2} 1$, entonces (a_n) es convergente y

$$a_n \xrightarrow{1+1_2} 1$$

En efecto,

$$\|a_n - 1\|_2 = \|4^n\|_2 = \|2\|_2^{2n} = \left(2^{-\psi_2(2)}\right)^{2n} = \left(\frac{1}{2}\right)^{2n} \xrightarrow{n \rightarrow \infty} 0.$$

$$(e) a_n = 4^n, p = 3.$$

Problema 5. Probar que si K es un cuerpo con valor absoluto ρ que satisface la desigualdad triangular fuerte y si definimos

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

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

Demonstración

Sea $b \in B(a, r) : \rho(b-a) < r$

Pd : $B(b, r) = B(a, r)$

Sea $x \in B(b, r)$,

$$\begin{aligned} \rho(x-a) &= \rho((x-b)+(b-a)) \\ &\leq \max \{ \rho(x-b), \rho(b-a) \} \end{aligned}$$

Como $\rho(x-b) < r$, $\rho(b-a) < r$, se tiene $\rho(x-a) < r$

Ahora sea $x \in B(a, r)$

$$\begin{aligned} \rho(b-x) &= \rho((b-a)+(a-x)) \\ &\leq \max \{ \rho(b-a), \rho(a-x) \} \end{aligned}$$

Como $\rho(b-a), \rho(a-x) < r$ se tiene $\rho(b-x) < r$

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

↓ Ver si f tiene raíces

$$f(x) = 0 \quad (p)$$

ver raíces $\Leftrightarrow f(x), f'(x)$ rel. primos

raíces distintas \Rightarrow no ramificado \rightarrow grado local \rightarrow
 { g. l=1 \rightarrow descompuesto \rightarrow 2 raíces
 g. l=2 \rightarrow inerte

Cuando hay raíces dobles \rightarrow ramificado

Cuando $f'(x)$ — pol. de Eisenstein \rightarrow lugar ramificado.

$$\mathbb{Q}(\sqrt{3})/\mathbb{Q}, \quad f(x) = x^2 - 3, \quad f'(x) = 2x$$

$p \in \mathbb{Z}$ no se descompone $\Leftrightarrow f(x) = 0$ no tiene raíces en \mathbb{Q}_p

$$\text{Sup } \exists x_0 \in \mathbb{Q}_p : f(x_0) = 0 \Rightarrow x_0^2 - 3 = 0$$

$$\therefore |x_0 - 3|_p = 0 \Rightarrow x_0 \equiv 3 \pmod{p^t} \quad \forall t \in \mathbb{N}.$$

$$\therefore x_0^2 \equiv 3 \pmod{p}$$

$$\left(\frac{3}{p}\right) \equiv 1 \Leftrightarrow \left(\frac{3}{p}\right) = 3^{\frac{p-1}{2}} \equiv 1 \pmod{p} \quad (p \neq 3)$$

(Caso 3 es trivial?)

$$\left(\frac{3}{p}\right) = (-1)^{\frac{3-1}{2} \cdot \frac{p-1}{2}} \left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right)$$

$$\left(\frac{0}{3}\right) = 1, \quad \left(\frac{1}{3}\right) = 1, \quad \left(\frac{2}{3}\right) = -1$$

$$\left(\frac{3}{p}\right) \equiv 1 \pmod{p} \Leftrightarrow (-1)^{\frac{p-1}{2}} \equiv 1, \quad \left(\frac{p}{3}\right) \equiv 1$$

$$\Leftrightarrow p \equiv 0, 1 \pmod{3}, \quad \frac{p-1}{2} = 2t, \quad t \in \mathbb{Z}.$$

| 1º Caso!

(1)

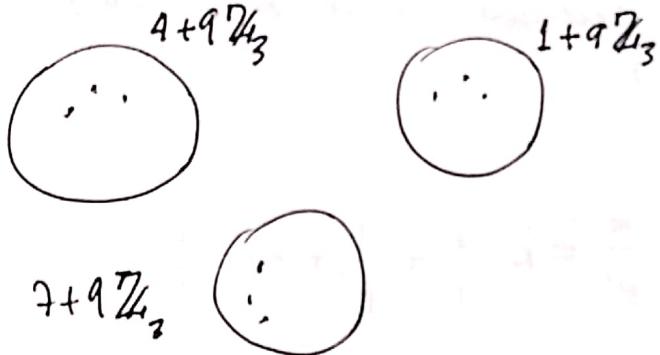
Teoría de Números

Clase de ejercicios

P1) $a_n = 4^n$, $p=3$

módulo 9

$$a_0 \equiv 1, a_1 \equiv 4, a_2 \equiv 7, a_3 \equiv 1, a_4 \equiv 4, \dots$$



Si $b_n = 4^{\frac{n}{3}} = (1+3)^{\frac{n}{3}} = \exp_p(\log_p(1+3)^{\frac{n}{3}})$
 $= \exp_p\left(\underbrace{3^{\frac{n}{3}} \log_p(1+3)}_0\right)$

$$\Rightarrow \exp_p(0) = 1$$

$$\exp_p(\log_p(1+x)) = 1+x \text{ si } |x|_p < p^{-\frac{1}{p-1}}$$

$$|\log_p(1+x)|_p = |x|_p$$

Bueno 6.4.c

$$\sum_{k=0}^{\infty} p^k \left(\frac{1}{2}\right)_k \text{ con } p \neq 2 \text{ converge?}$$

Horario de Consulta
 Vi 2.30 - 4.00
 Lu. 11.00 - 12.30

$$\left(\frac{y_2}{k}\right) = \frac{\frac{1}{2} \cdot \left(1 - \frac{1}{2}\right) \cdot \left(2 - \frac{1}{2}\right) \cdots \left(k-1 - \frac{1}{2}\right)}{k!}, \quad |z|_p = 1$$

$$\text{Tenemos } \left| \left(\frac{y_2}{k}\right) \right|_p \leq \left| \frac{1}{k!} \right|_p = v_p^{v_p(k!)}.$$

$$\left| p^k \left(\frac{y_2}{k}\right) \right|_p = p^{v_p(k!) - k} \quad \text{queremos saber si } \longrightarrow 0 \\ \Leftrightarrow v_p(k!) - k \longrightarrow \infty ?$$

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

$$v_p(k!) - k \leq \frac{k}{p-1} - k = k \left(\frac{1-(p-1)}{p-1} \right) = k \left(\frac{2-p}{p-1} \right) \longrightarrow \infty$$

$$\sum_{k=0}^{\infty} p^k \left(\frac{y_2}{k}\right) = \sqrt{1+p} \in \mathbb{Q}_p.$$

Ejemplo. $\sum_{k=0}^{\infty} 15^k \left(\frac{y_2}{k}\right) = \sqrt{1+15} \in \mathbb{Q}_3 \quad \in \mathbb{Q}_5 \quad \begin{cases} 15 \text{ es uniformizante} \\ \text{en } \mathbb{Q}_3 \text{ y } \mathbb{Q}_5 \\ \text{simultáneamente} \end{cases}$

$$4 = \sqrt{1+15} \equiv 1 \pmod{3} \\ -4 = \sqrt{1+15} \equiv 1 \pmod{5}.$$

$$f(t) = t^2 - (1+x) \in \underbrace{\mathbb{Z}_2\left[\frac{1}{2}\right][[x]][t]}_A$$

$$f(1) = x \\ f'(1) = 2, \quad 2 \in A^*$$

Podemos aplicar Hensel, ...

Otro ejercicio.

(3)

L/K extensión cuadrática. ($L = K(\sqrt{d})$)

$f \in \mathbb{P}(K)$ descompuesto si $L \otimes K_f = L_{f_1} \times L_{f_2}$

equivalentemente : - Hay 2 lugares sobre f

- d tiene raíces cuadradas en K_f .

Si f no se descompone, $L \otimes K_f = L_{\tilde{f}} \leftarrow$ un solo.

- hay un solo lugar sobre f

- d no tiene raíces en K_f

$$|K_f^*| \subseteq \mathbb{R}^+$$

$$|\mathcal{O}_f^*| = p^\mathbb{Z}, \quad |\mathcal{O}_{\tilde{f}}(\sqrt{p})^*| = p^{\frac{1}{2}\mathbb{Z}}$$

$$e(L_{\tilde{f}}/K_f) = [|\mathcal{O}_{\tilde{f}}^*| : |K_f^*|] = |\mathcal{O}_{\tilde{f}}^*| / |K_f^*|$$

↑ índice de ramificación

$$\text{grado residual } f(L_{\tilde{f}}/K_f) = [L : K]$$

$$K \cong \mathcal{O}_K/m_K, \quad L = \mathcal{O}_L/m_L$$

$$[L_{\tilde{f}} : K_f] = ef$$

$$[L_{\tilde{f}} : K_f] = 2$$

$$e=2$$

$f=1$
ramificada

$$e=1$$

$f=2$
no ramificada

(4)

f es no ramificada si existe $\alpha \in \mathcal{O}_L$ tal que

$\text{irr}_{\bar{\alpha}, K}(x)$ no tiene raíces en K .

Si no lo hay, la extensión es ramificada.

Ejemplo. $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ extensión cuadrática; $L = \mathbb{Q}(\sqrt{3}), K = \mathbb{Q}$

$$\mathcal{O}_L = \mathbb{Z}[\sqrt{3}], f(x) = x^2 - 3 = \text{irr}_{\sqrt{3}, K}(x)$$

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

$$|f'(a)| \neq 1 \text{ si } |a| \neq 1 \text{ ó } |2| \neq 1$$

$$a^2 \equiv 3 \pmod{p}$$

$$a \equiv 0 \pmod{p} \quad (\text{go sobre } p)$$

$$\text{ssi } 3 \equiv 0 \pmod{p}$$

$p = 3$ ó $p = 2$ únicas que pueden ser ramificadas.

Si $p \neq 2, 3$

$$x^2 - 3 \equiv 0 \pmod{p} \text{ tiene raíces}$$

Hensel \Rightarrow hay raíces en \mathbb{F}_p

$\Rightarrow p$ descompuesto.

Si $x^2 - 3 \equiv 0 \pmod{p}$ no tiene solución

\Rightarrow No hay soluciones en \mathbb{F}_p .

$0 = x^2 - 3$ no tiene soluciones en $\overline{\mathbb{F}_p} \Rightarrow$ toda solución $\alpha \in \overline{\mathbb{F}_p}$ genera una extensión cuadrática.

Luego p es no ramificada (inerte)

(5)

3 es ramificado pues $L_3 = \mathbb{Q}_3(\sqrt{3})$

$$\cancel{\text{---}} \quad |\sqrt{3}|_8^2 = |3|_8 = |3|_3 = \frac{1}{3}$$

$$\therefore |\sqrt{3}|_8 = \frac{1}{\sqrt{3}} \neq 3^{\frac{1}{2}}$$

No ramificado si $e=1$

$p=2$ La extensión no ramificada en $\mathbb{Q}(\sqrt{5})/\mathbb{Q}_2$

$a \in \mathbb{Z}_2^*$ es cuadrado si $a \equiv 1 \pmod{8}$

Si $d \equiv 1 \pmod{8} \rightarrow L/\mathbb{Q}$ descompuesta

Si $d \equiv 5 \pmod{8} \Rightarrow L/\mathbb{Q}$ inerte

Cualquier otro caso es ramificado.

$$a \in (\mathbb{Z}/2^n\mathbb{Z})^*, \quad a = 1 \Leftrightarrow a \equiv 1 \pmod{8} \quad |(f'(a_0)| > |f(a_0)|$$

Otro ejercicio:

$$\sum_{n=1}^{\infty} n! \quad \text{converge?}$$

Basta ver que $|n!|_p \rightarrow 0 \Leftrightarrow v_p(n!) \rightarrow \infty$

$$\sum_{k=1}^{\infty} \left[\frac{n}{p^k} \right] > \left[\frac{n}{p} \right] > \frac{n}{p} - 1$$

$$v_p(n!)$$

$$\mathbb{Q}_3(\sqrt{3}) / \mathbb{Q}_3(\sqrt{6}) / \mathbb{Q}_3(\sqrt{2})$$

$$|\alpha|_p = p^{-v_p(\alpha)}$$

En general, para F completo no arquimediano

$$|\alpha|_F = c^{v_F(\alpha)}, \quad c \in (0, 1)$$

$$\alpha = u \pi^{v_F(\alpha)}$$

$$L = \mathbb{Q}(\sqrt[5]{2}) \quad f(x) = x^5 - 2 \quad \leftarrow \text{irreducible en } \mathbb{Q}$$

$$|\sqrt[5]{2}|_8 = 2^{-\frac{1}{5}}$$

$$|2|_2 = |2|_8 = 2^{-1}$$

$$e_8 = e(L_p/\mathbb{Q}_2), \quad e_8 = 5$$

$$\sum_{g|2} e_g f_g = 5$$

Hay un solo lugar sobre 2 que es totalmente ramificado

Ahora $p = \infty$ (arquimediano)

$$L \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R} \times \mathbb{C} \times \mathbb{C}$$

$$p \neq 5, f(x) = x^5 - z$$

$$\alpha = \sqrt[5]{z} \in \mathbb{Q}_L, f(\alpha) = 0, f'(\alpha) = 5\alpha^4.$$

$$p \neq 5, 2.$$

L/\mathbb{Q} no ramificada en p .

$$L \otimes_{\mathbb{Q}} \mathbb{Q}_p = L_{p_1} \times \dots \times L_{g_r}$$

L_{g_1}/L no ramificada.

f tiene raíces distintas en $\overline{\mathbb{F}_p}$

$$\frac{\mathbb{F}_p[x]}{(f)} \cong \mathbb{F}_{p^{t_1}} \times \dots \times \mathbb{F}_{p^{t_r}}$$

Para cada t hay una única extensión no ramificada L/\mathbb{Q}_p

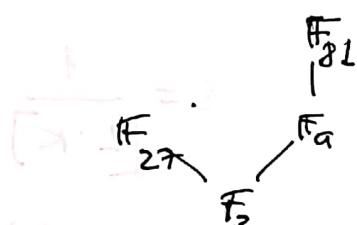
$$\text{con } L = \mathbb{Q}_p/m_L \cong \mathbb{F}_{p^t}$$

$$\alpha^5 \equiv z \pmod{3}$$

$$\Rightarrow \alpha \equiv z \pmod{3}$$

$$\mathbb{Q}_3 \otimes_{\mathbb{Q}} L \cong \mathbb{Q}_3 \times L_{g_r}$$

$$g_r = 4$$



Otro problema.

$$\alpha \in L/K, \alpha \text{ entero sobre } Cl_K \iff |N_{L/K}(\alpha)| \leq 1$$

α entero $\iff 1+\alpha$ entero

$$|N_{L/K}(\alpha)| \leq 1 \iff |N_{L/K}(1+\alpha)| \leq 1$$

(8)

$\alpha \mapsto |N_{L/K}(\alpha)|$ es un valor absoluto en L

$\rho : L^* \rightarrow \mathbb{R}^+$ valor absoluto que extiende $|\cdot|_K$

$$\rho_0(\alpha) = |N_{L/K}(\alpha)|_K$$

ρ, ρ_0 son valores absolutos en L .
en particular son normas en L

Dos normas en L son equivalentes

ρ, ρ_0 son equivalentes

Las mismas sucesiones convergen en ρ y ρ_0 .

Si $\rho_0 \neq \rho^r$ tr

probaremos que existe $a \in K$ con $\rho_0(a) < 1, \rho(a) > 1$

$$a^n \xrightarrow{\rho_0} 0, a^n \xrightarrow{\rho} 0$$

$$\text{Si } \alpha \in K, |\alpha|_K = |N_{L/K}(\alpha)|_K^s = |\alpha^{[L:K]}|_K^s$$

$$s = \frac{1}{[L:K]}$$

Tomemos $x \in K$, $\rho(x) = \rho_0(x)^r, \rho_0(x) \neq 1$
(fijo)

Como $\rho \neq \rho_0^r$, existe y con $\rho(y) \neq \rho_0(y)^r$

Supongamos que $\rho(y) > \rho_0(y)^r$ ($\log(\rho(y)) > \log(\rho_0(y)^r)$)

$$\frac{\log \rho(y)}{\log \rho_0(y)^r} \Rightarrow \frac{\log \rho(y)}{r \log \rho_0(y)} \Rightarrow \frac{\log \rho(y)}{\log \rho_0(y)} > r$$

a Q.E.D.

$$\frac{\log p(y)}{\log p(x)} > \frac{m}{n} > \frac{\log p_0(y)}{\log p_0(x)}$$

$$n \log p(y) > m \log p(x)$$

$$\log \left(\frac{(y)^n}{\log p(x)^m} \right) > 0$$

$$\therefore p\left(\frac{y^n}{x^m}\right) > 1$$

$$p_0\left(\frac{y^n}{x^m}\right) < 1$$

Teoría de Números

Clase ??, Ejercicios

$$K = \mathbb{F}_2(x), \quad p(x) = x^2 + x + 1$$

$$\mathcal{O}_K = \frac{\mathbb{F}_2[\lambda]}{(x^2 + x + 1)\mathbb{F}_2[x]}, \quad \lambda \in K_p : \lambda = \sum_{i=-n}^{\infty} (x^2 + x + 1)q_i, \quad q_i \in \{0, 1, x, x+1\}$$

$$F \in K[T] : \quad F(T) = T^2 + T + 1 \\ f(x) = x^2 + x + 1 = p(x) \\ F(x) \equiv 0 \pmod{p} \\ F'(x) \equiv 1$$

Hensel $\Rightarrow \exists \alpha \in \mathcal{O}_{K_p}$ tal que

- 1) $\alpha \equiv x \pmod{p}$
- 2) $\alpha^2 + \alpha + 1 \equiv 0$

$$\mathbb{F}_2(\alpha) \cong \mathbb{F}_4$$

$$\mathbb{F}_2(\alpha) \subseteq K_p$$

$$\lambda \in K_p \Rightarrow \lambda = \sum_{i=-n}^{\infty} b_i p^i, \quad b_i \in \{0, 1, \alpha, \alpha+1\}$$

$$K_p \cong \mathbb{F}_4((p))$$

$L_K ; \alpha \in K$, π parámetro uniformizante de K

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

1) π uniformizante en L ; $\pi \mathcal{O}_L = m_L$

$$\mathcal{O}_K/\pi \mathcal{O}_K \cong \mathcal{O}_L/\pi \mathcal{O}_L$$

$$\frac{\mathbb{F}_K}{\pi \mathbb{F}_K} \subseteq \frac{\mathbb{F}_L}{\pi \mathbb{F}_L}$$

$$\mathbb{F}_K = \{ \bar{a}_0, \bar{a}_1, \dots, \bar{a}_r \} \quad a_0 = 0$$

$$\mathbb{F}_L = \{ \bar{b}_0, \dots, \bar{b}_t \} \quad b_0 = 0$$

$$\alpha \in K \quad \beta \in L$$

$$\alpha = \sum_{i=-n}^{\infty} a_i \pi^i \quad \beta = \sum_{i=-n}^{\infty} b_i \pi^i$$

$$\mathbb{F}_L = \mathbb{F}_K[C] \quad , \quad \bar{p}(x) = m_C(x) \in \mathbb{F}_K[x]$$

$$c = \bar{b}_j \quad \bar{p}(b_j) = 0 \quad \text{en } \mathbb{F}_L$$

$$\bar{p}'(b_j) \neq 0 \quad \text{en } \mathbb{F}_L$$

$$p(b_j) = 0 \quad \text{en } \mathcal{O}_L$$

$$p'(b_j) \neq 0 \quad \text{en } \mathcal{O}_L$$

$p(x)$ irreducible $\Rightarrow p(x)$ irreducible

$$E = K[\gamma] \quad , \quad [E : K] = \deg p$$

$$= \deg \bar{p} = [\mathbb{F}_L : \mathbb{F}_K]$$

podemos suponer que

$$\{ \bar{b}_0, \dots, \bar{b}_t \} \quad b_i = h_i(\gamma) \quad \deg h_i < \deg p$$

h_i coeficiente en $\{a_0, \dots, a_r\}$

Supongamos que $\mathbb{F}_L = \mathbb{F}_K$.

π_L parámetro uniformizante de L , π_K parámetro uniformizante de K .

$$\pi_K \in L$$

$$e > 1 \quad \pi_K = u \pi_L^e$$

$e=1 \Rightarrow L=K$

indice de ramificación