

$$\begin{aligned}
 A_{pi} &= B A_{pi} = B_i A_{pi} \\
 &= \begin{pmatrix} x_i^{-1} & 0 \\ 0 & x_i \end{pmatrix} \begin{pmatrix} \alpha_i & 0 \\ 0 & \beta_i \end{pmatrix} \sigma_{pi} \\
 &= \begin{pmatrix} 1 & 0 \\ 0 & \alpha_i \beta_i \end{pmatrix} \sigma_{pi} \\
 &= (1) \times (\alpha_i \beta_i) \sigma_{pi}
 \end{aligned}$$

Globalmente: $A = \sigma_K \times IJ$

$$\begin{aligned}
 I \times J &\cong \sigma_K \times IJ \text{ como } \sigma_K \text{-módulos} \\
 I \times I^{-1} &\cong \sigma_K \times \sigma_K = \sigma_K^2 \text{ como } \sigma_K \text{-módulos.}
 \end{aligned}$$

En particular:

$$B^{-1} B_i \sim I$$

$$\begin{aligned}
 (*) \quad \text{Basta verf. si} \quad A_{pi} &= (B^{-1} B_i) A_{pi} \\
 &\Rightarrow B_i^{-1} B \in SL_2(\sigma_{pi}).
 \end{aligned}$$

$$\begin{aligned}
 \text{Si } (B_i^{-1} B) \sim I \Rightarrow B_i^{-1} B \in SL_2(\sigma_{pi}) \Rightarrow B_i^{-1} B \in SL_2(\sigma_{pi}).
 \end{aligned}$$

$$\begin{aligned}
 B_i^{-1} B &= \begin{pmatrix} x_i^{-1} & 0 \\ 0 & x_i \end{pmatrix} \begin{pmatrix} \alpha_i & 0 \\ 0 & \beta_i \end{pmatrix} \\
 &= \begin{pmatrix} x_i^{-1} \alpha_i & 0 \\ 0 & x_i \beta_i \end{pmatrix} = \begin{pmatrix} \alpha_i' & 0 \\ 0 & \beta_i' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I
 \end{aligned}$$

$$\begin{aligned}
 B_i^{-1} B &= \begin{pmatrix} x_i^{-1} & 0 \\ 0 & x_i \end{pmatrix} \begin{pmatrix} \alpha_i & 0 \\ 0 & \beta_i \end{pmatrix} \\
 &= \begin{pmatrix} x_i^{-1} \alpha_i & 0 \\ 0 & x_i \beta_i \end{pmatrix} = \begin{pmatrix} \alpha_i' & 0 \\ 0 & \beta_i' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I
 \end{aligned}$$

$$\begin{aligned}
 B_i^{-1} B &= \begin{pmatrix} x_i^{-1} & 0 \\ 0 & x_i \end{pmatrix} \begin{pmatrix} \alpha_i & 0 \\ 0 & \beta_i \end{pmatrix} \\
 &= \begin{pmatrix} x_i^{-1} \alpha_i & 0 \\ 0 & x_i \beta_i \end{pmatrix} = \begin{pmatrix} \alpha_i' & 0 \\ 0 & \beta_i' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I
 \end{aligned}$$

$$\begin{aligned}
 B_i^{-1} B &= \begin{pmatrix} x_i^{-1} & 0 \\ 0 & x_i \end{pmatrix} \begin{pmatrix} \alpha_i & 0 \\ 0 & \beta_i \end{pmatrix} \\
 &= \begin{pmatrix} x_i^{-1} \alpha_i & 0 \\ 0 & x_i \beta_i \end{pmatrix} = \begin{pmatrix} \alpha_i' & 0 \\ 0 & \beta_i' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I
 \end{aligned}$$

Funciones Aritméticas

$f: \mathbb{N} \rightarrow \mathbb{C}$ función.

para cada función de este tipo def. su serie de Dirichlet

$$\varphi(f, z) = \sum_{n=1}^{\infty} \frac{f(n)}{n^z}.$$

Ejemplo: Si $f_0(n) = 1 \forall n \in \mathbb{N}$

$$\varphi(f_0, z) = \sum_{n=1}^{\infty} \frac{f_0(n)}{n^z} = \sum_{n=1}^{\infty} \frac{1}{n^z} = \zeta(z) \quad (\text{zeta de Riemann})$$

formalmente: $\varphi(f, z) \varphi(g, z) = \left(\sum_{n=1}^{\infty} \frac{f(n)}{n^z} \right) \left(\sum_{m=1}^{\infty} \frac{g(m)}{m^z} \right)$

$$= \sum_{k=1}^{\infty} \frac{h(k)}{k^z}, \quad (k = nm)$$

donde $h(k) = \sum_{\substack{(n,m) \\ nm=k}} f(n)g(m) = \sum_{n|k} f(n)g\left(\frac{k}{n}\right)$, se dice que $h = f * g$ convolución de Dirichlet

obs: $1 = \varphi(I, z) = \sum_{n=1}^{\infty} \frac{I(n)}{n^z} \quad I(n) = \begin{cases} 1, & n=1 \\ 0, & \text{sino.} \end{cases}$

es el neutro de la convolución

obs: Si $f(1) \neq 0$ y definimos ρ p. $\rho(1) = f(1)^{-1}$

$$\rho(n) = -f(1)^{-1} \sum_{\substack{d|n \\ d \neq 1}} f(d) f\left(\frac{n}{d}\right)$$

entonces: $f * \rho = I$

$$f * \rho(1) = f(1)\rho(1) = 1$$

$$f * \rho(n) = \sum_{\substack{d|n \\ d \neq 1}} f\left(\frac{n}{d}\right) f(d) = \rho(n) f(1) + \sum_{\substack{d|n \\ d \neq 1}} f\left(\frac{n}{d}\right) \rho(d) = 0.$$

y $f * (p_1 + p_2) = f * p_1 + f * p_2$, $f * (p_1 * p_2) = (f * p_1) * p_2$.
(Anillo de func. aritméticas)

Ejemplo: Función ϕ de Euler
 $\phi(n) = |\{x/n \in \mathbb{Z}^* | \text{ s.t. } \text{mcm de los elementos de orden en } C_n\}|$

obs: m/n $\in C_n$ tiene una única copia de C_m
 y es $\langle a^{n/m} \rangle$ si $C_n = \langle a \rangle$.
 Cualesquier m de elementos de orden imparte C_m

Luego $n = |C_n| = \sum_{m|n} \# \{ \text{elementos de orden } m \text{ en } C_n \}$
 $\phi(n) = \sum_{m|n} \# \{ \text{elementos de orden } m \text{ en } C_m \}$
 $= \sum_{m|n} \phi(m)$.

entonces: $id = \phi * f_0$.

Def: μ de Möbius, $\mu(1) = 1$
 $\mu(n) = 0$ si n no es libre de cuadrados.

Si $n = p_1 \dots p_r$ distintos. $\mu(n) = (-1)^r$.

obs: $f_0 * \mu = I$
 $f_0 * \mu(1) = 1$

Basta ver que: $f_0 * \mu(n) = 0 \quad (n \geq 1)$

$n = p_1^{x_1} \dots p_r^{x_r}, x_i \geq 1$
 $f_0 * \mu(n) = \sum_{d|n} \mu(d) = f_0 * \mu(n_1), \quad n_1 = p_1 \dots p_r$

Sea $X_r = \{1, \dots, r\}$, $d|n_1 \Leftrightarrow d = \prod_{i \in \tau} p_i$, $\tau \subseteq X_r$
 $f_0 * \mu(n_1) = \sum_{\tau \subseteq X_r} \mu_r(\prod_{i \in \tau} p_i) = \sum_{\tau \subseteq X_r} (-1)^{|\tau|}$
 $= \sum_{r \in \tau} (-1)^{|\tau|} + \sum_{r \notin \tau} (-1)^{|\tau|} = (*)$

$$\{\tau \subseteq X_r \mid r \in \tau\} = \{S \subseteq X_r \mid S \subseteq X_{r-1}\}$$

$$\{\tau \subseteq X_r \mid r \notin \tau\} = \{S \subseteq X_r \mid S \subseteq X_{r-1}\}$$

Luego: $(*) = \sum_{r \in \tau} (-1)^{|\tau|+1} + \sum_{r \notin \tau} (-1)^{|\tau|} = 0$.

$$\mu * f_0 = I$$

$$\phi * f_0$$

$$\phi = id * \mu, \quad \text{por lo tanto} \quad \phi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$$

Ejemplo: $n = p^r f^s$ (p, f primos)
 $\{1, p, p^2, pf\}$ todos los otros div. por al menos dos

entonces: $\phi(n) = \mu(1)n + \mu(p)\frac{n}{p} + \mu(f)\frac{n}{f} + \mu(pf)\frac{n}{pf}$
 $= p^{r-1}f^s - p^{r-2}f^s - p^{r-1}f^{s-1} + p^{r-2}f^{s-1}$
 $= p^{r-2}f^{s-1}(p-1)(f-1).$

Fórmula de inversión de Möbius:

$$\text{Si } F(n) = \sum_{d|n} f(d) \text{ entonces } f(n) = \sum_{d|n} F(d) \mu\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right).$$

Dato: Conviene en el caso de polinomios ciclotómicos.

Ejemplo: $\Phi_n(x)$ es un n -ésimo polinomio ciclotómico,

$$\Phi_n(x) = \prod_{\substack{d=1 \\ (x,d)=1}}^{n-1} \left(1 - e^{\frac{2\pi i d}{n}}\right).$$

$$\prod_{d=0}^{n-1} \left(1 - e^{\frac{2\pi i d}{n}}\right) = x^n - 1$$

$$\prod_{d|n} \Phi_d(x) = x^n - 1.$$

Corolario: $\phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(d)}$.

Ejemplo: $\Phi_6(x) = \frac{(x-1)(x^2-1)}{(x^2-1)(x^3-1)} = \frac{(x^2-1)}{(x+1)(x^2-1)} = \frac{x^2+1}{(x+1)} = x^2 - x + 1.$

Def: Una función aritmética se dice totalmente multiplicativa si

$$f(nm) = f(n)f(m) \quad \forall n, m \in \mathbb{N}$$

f se dice multiplicativa si

$$f(nm) = f(n)f(m) \quad \forall n, m \in \mathbb{N} : (n|m) = 1.$$

Si $(n, m) = 1 \quad \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/nm\mathbb{Z} \Rightarrow \phi(nm) = \phi(n)\phi(m)$

Si f es una función aritmética, su p -série de Bell es

$$B(f, z) = \sum_{t=0}^{\infty} f(p^t) z^t.$$

Aff: Si f es multiplicativa, ssi:

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

Demo:

$$\prod_{p \text{ primo}} \left(f(1) + f(p) \frac{1}{p^z} + f(p^2) \frac{1}{p^{2z}} + \dots \right) = \prod_{p \text{ primo}} f(p^z).$$

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

$$B_p(f * g, x) = \sum_{t=0}^{\infty} f(p^t) g(p^t) x^t$$

$$= \sum_{t=0}^{\infty} \left(\sum_{d | p^t} f(d) g\left(\frac{p^t}{d}\right) \right) x^t$$

$$= \sum_{t=0}^{\infty} \left(\sum_{s=0}^t f(p^s) g(p^{t-s}) \right) x^t$$

$$= B_p(f, x) B_p(g, x).$$

$$\Psi(f * g, z) = \Psi(f, z) \Psi(g, z) \text{ por def.}$$

$$\Psi(f, z) = \prod_p B_p(f, \frac{1}{p^z})$$

$$\Psi(g, z) = \prod_p B_p(g, \frac{1}{p^z})$$

$$\underline{\Psi(f * g, z)} = \prod_p B_p(f * g, \frac{1}{p^z})$$

Conclusion: Ψ convolución de func. multp. es multiplicativa.

$$f^{-1} * f = I \quad \Psi(f^{-1}, z) = f(f, z)$$

en todos:

$$\underline{\Psi(f, z)} = \prod_p B_p(f, \frac{1}{p^z})$$

$$\prod_p B_p(f, \frac{1}{p^z}) = \Psi(f, z) = \left(\prod_p B_p(f, \frac{1}{p^z}) \right)^{-1}$$

Conclusion: $\{$ multiplication \Rightarrow $\{^{-1}$ multiplication.

Ej: $f_0 \circ f_1 \rightarrow f_1 \circ f_0$ mult.

$f_0 =$ void mult.

$$\text{Ej: } d(n) = \#\{\text{divisors of } n\} = \sum_{d|n} 1$$

$d = f_0 * f_0$ mult.

$$\sigma(n) = \sum_{d|n} d = \text{id} * f_0 \text{ mult.}$$

$$\text{Si: } n = p_1^{x_1} \dots p_r^{x_r}, \quad d(n) = \prod_{i=1}^r d(p_i^{x_i})$$

$$d(p_i^{x_i}) = p_i^{x_i} - p_i^{x_i-1} = p_i^{x_i-1}(p_i - 1).$$

$$(p_i - 1)(p_i^{x_i-1} - 1) = p_i^{x_i-1} + p_i^{x_i-2} + \dots + p_i + 1$$

$$\text{Luego: } \phi(n) = \prod_{i=1}^r p_i^{x_i-1} (p_i - 1) = \prod_{i=1}^r p_i^{x_i-1} \left(1 - \frac{1}{p_i}\right) = n \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right)$$

Ejemplo: Calcular la suma de los divisores de 10.000.

$$10.000 = 10^4 = 2^4 \cdot 5^4$$

$$\sigma(10.000) = \sigma(2^4) \sigma(5^4) = \frac{2^5 - 1}{2 - 1} \cdot \frac{5^5 - 1}{5 - 1}$$

$$\sigma(p^n) = 1 + p + \dots + p^n = \frac{p^{n+1} - 1}{p - 1} = 31 \cdot \frac{(5^4 - 1)}{4} = 24.211.$$

Conviene es multiplicativa: $\delta(10.000) = \delta(2^4) \delta(5^4) = 5 \cdot 5 = 25$.

$$\zeta(z) = \prod_p B_p(f_0, \frac{1}{p^z}) = \prod_p \sum_{t=0}^{\infty} x^t, \quad B_p(f_0, \frac{1}{p^z}) = \frac{1}{1 - \frac{1}{p^z}}$$

$$\text{Luego: } \zeta(z) = \prod_p \frac{1}{1 - \frac{1}{p^z}}.$$

$$\text{Pero: } \zeta(z) = \Psi(f_0, z) = \Psi(\mu_1 z), \quad \text{pues } \Psi(\mu_1 z) = \zeta(z) = \prod_p B_p(\mu_1, \frac{1}{p^z})$$

$$B_p(\mu_1, z) = 1 - z$$

$$\text{Así: } \zeta(z) = \prod_p \left(1 - \frac{1}{p^z}\right).$$

Distribución de primos

$$\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z} \quad \begin{array}{l} \text{converge si } \operatorname{Re}(z) > 1 \\ \text{divergente si } z = 1. \end{array}$$

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

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

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

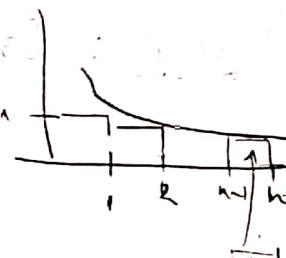
$$\log \prod_{p \text{ primo}} \left(1 - \frac{1}{p^z}\right)^{-1} = \frac{1}{p^z} + \frac{1}{2p^{2z}} + \frac{1}{3p^{3z}} + \dots$$

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

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

Sabemos que:

$$\sum_{n \geq 2} \frac{1}{n^t} \leq \int_2^{\infty} \frac{1}{x^t} dx = \left[\frac{x^{-t+1}}{-t+1} \right]_2^{\infty} = \frac{1}{t-1} = \text{fijo.}$$



Luego para $z \leq 1$ es $\zeta(z) = \sum_{p \text{ primo}} \frac{1}{p^z}$

$$\sum_{p \text{ primo}} \left(\sum_{j=2}^{\infty} \frac{1}{j p^{jz}} \right) \leq \sum_{j=2}^{\infty} \frac{1}{j} \sum_{p \text{ primo}} \frac{1}{p^j} = \frac{1}{2} + \dots + \frac{1}{9} = 1.7 \dots$$

$$\frac{1}{2-1} = \left(\frac{1}{2} + 1 \right) \leq \sum_{j=2}^{\infty} \frac{1}{j} \sum_{n \geq 2} \frac{1}{nj} \leq \sum_{j=2}^{\infty} \frac{1}{j(j-1)} = 1.$$

Luego para $\operatorname{Cond}(\overline{z})$, $\log \zeta(z)$ converge si

$$\sum_{p \text{ primo}} \frac{1}{p^z} \text{ converge.}$$

Parte 2: $\sum_{p \text{ primo}} \frac{1}{p}$ diverge, pues $\sum_{n=1}^{\infty} \frac{1}{n}$ diverge. ($\zeta(1)$ diverge)

- En particular:
- 1) Hay infinitos primos.
 - 2) Para cada $t < 1$ y $\varepsilon > 0$ existe n tal que

p_n es primo & satisface: $p_n < \varepsilon^{-t}$.

Sino: $p_n \geq \varepsilon^{-t} \Rightarrow \sum_{n=1}^{\infty} \frac{1}{p_n} \leq \sum_{n=1}^{\infty} \frac{1}{\varepsilon^{-t}} = (\ast)$.
 diverge \downarrow conv

- Fijemos x y consideremos: $X = (\chi/\mu)_x^*$ \rightarrow \mathbb{C}^* homomorfismo.
 ↓ (Carácter)

$$\sum_{a \in (\mathbb{Z}/n\mathbb{Z})^*} X(a) = \begin{cases} \phi(n), & \text{si } x \equiv 1 \\ 0, & \text{si } x \neq 1 \end{cases} \quad \text{de propós.}$$

Si $x \neq 1 \Rightarrow b : X(b) \neq 1 \quad \sum_a X(a) = \sum_a X(ab) = \sum_a X(a)X(b)$

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

Se define: $L(x, z) = \sum_{(a, n)=1}^1 \frac{x(a)}{a^z}$. $\left| \begin{array}{l} x_0(\bar{a}) = 1, \text{ si } (n, a) = 1 \\ x_0(\bar{a}) = 0, \text{ si } (n, a) \neq 1 \end{array} \right.$

obs: Si $x \neq x_0$: $\sum_{a \leq N} X(a)$ no es acotada. más explícitamente:

$$\left| \sum_{a \leq N} X(a) \right| \leq \phi(n)$$

que es: $\sum_{a \leq N} X(a) \leq \phi(n)$ (fija en el círculo unitario de los elementos normales).

Si $z \in \mathbb{R}_{>1}$. Entonces: $\{X(\bar{a})\}_a$ es una parte acotada $\frac{1}{a^z}$ conv. a 0 uniformemente.

∴ $L(x, z)$ es uniformemente convergente (Criterion de Dirichlet)

$$L(x, z) = \sum_{(n, q)=1} \frac{x}{q^z}, \text{ donde } X(a) = \begin{cases} 1, & \text{si } (n, a) = 1 \\ 0, & \text{si } (n, a) \neq 1 \end{cases} \quad \text{multiplicativa.}$$

$$L(x_0, z) = \prod_{p \neq n} B_p(x_0, \frac{1}{p^z})$$

$$B_p(x_0, x) = \begin{cases} 1 + x + x^2 + \dots & \text{si } p+1 \mid x \\ 1 + \int_{\mathbb{F}_p} \chi_p(t) x^{p+1} dt & \text{si } p+1 \nmid x \end{cases}$$

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

Ejercicio: Si p_1, \dots, p_k son primos probar que:

$$T = \{n \mid q \neq n \quad \forall p \in p_1, \dots, p_k\} \text{ entero (z)} \quad \sum_{n \in T} \frac{1}{n} \text{ converge y es acotado}$$

$$\sum_{\substack{p \text{ primo} \\ p \neq n}} \frac{x(p)}{p^z} + p(z) = \log L(x_0, z)$$

$$\text{Si } z = 1 - \sum_{p \neq n} \frac{x_0(p)}{p^2} = \sum_{p \neq n} \frac{1}{p^2} \text{ diverge}$$

Lazosando del mismo modo para $1 \neq z$.

$$\text{y } \sum_{p \neq n} \frac{x(p)}{p^z} \text{ converge para } z \neq 1.$$

Yendo: $L(x_0, 1) \neq 0$.

Entonces $\sum_{p \neq n} \frac{x(p)}{p^1} = \log L(x_0, 1)$ converge en una vecindad de $z = 1$.

Por lo tanto: $\sum_{p \neq n} \frac{x(p)}{p^z}$ converge.

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

$(\bar{bc}) = \bar{1}$, en $(\mathbb{Z}/n\mathbb{Z})^*$.

Existe $x \in (\mathbb{Z}/n\mathbb{Z})^*$ tal que $\bar{c} = \bar{x} + b$.

Luego: $\bar{b} + \bar{x}$

$(\bar{b} + \bar{x})^*$ es propio abajo

Entonces $\bar{b} + \bar{x} \in (\mathbb{Z}/n\mathbb{Z})^*$

$$(\bar{b} + \bar{x})^* = \prod_{i=1}^r (d_i + 1)$$

$$\bar{b} \rightarrow (\bar{b}_1, \dots, \bar{b}_r) \text{ tal que } \bar{b}_i + \bar{x}$$

Entonces tomamos: $X: \prod_{i=1}^r (\mathbb{Z}/d_i\mathbb{Z}) \rightarrow \mathbb{C}^*$
 $(\bar{a}_1, \dots, \bar{a}_r) = e^{2\pi i \left(\frac{\bar{a}_1}{d_1} + \dots + \frac{\bar{a}_r}{d_r} \right)}$

para b: $e^{2\pi i \left(\frac{b}{d_j} \right)} \neq 1$.

$G = \{ X: (\mathbb{Z}/n\mathbb{Z})^* \rightarrow \mathbb{C}^* \text{ Carácter}\}$.

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

Dem: Si $\bar{b} \neq \bar{1} \Rightarrow \exists X_1: X_1(\bar{b}) \neq 1$.

Entonces: $\sum_{X \in G} X(\bar{b}) = \sum_{X \in G} (XX_1)(\bar{b}) = \sum_{X \in G} X(\bar{b}) \bar{X}_1(\bar{b})$

$$\therefore (1 - X_1(\bar{b})) \sum_{X \in G} X(\bar{b}) = 0 \quad \therefore \sum_{X \in G} X(\bar{b}) = 0.$$

Sea $\bar{b} \in (\mathbb{Z}/n\mathbb{Z})^*$ fijo. $\sum_{p \equiv b \pmod{n}} \frac{1}{p} = \sum_{p \neq n} \frac{1}{p} \left(\frac{1}{|G|} \sum_{X \in G} X(\bar{p}) \right)$

$$= \frac{1-1}{|G|} \sum_{X \in G} \sum_{p \in G} X(\bar{p}) \left(\sum_{p \neq n} \frac{X(\bar{p})}{p} \right).$$

Converge ssi $\sum_{p \neq n} \frac{1}{p}$ converge.

Luego no converge.

Teorema de Dirichlet sobre primos en progresión aritmética:

Si $b \in (\mathbb{Z}/n\mathbb{Z})^*$ (es decir $(b, n) = 1$)

entonces existen infinitos primos p tales que: $p \equiv b \pmod{n}$.

od: hay infinitos primos en $P = \{a + nb \mid a \in \mathbb{Z}\}$

Se puede demostrar que:

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

mais difícil:

$$\frac{\sum_{\substack{p \leq x \\ p \in h(\text{mod } n)}} 1}{\sum_{p \leq x} 1} \xrightarrow{x \rightarrow \infty} \frac{1}{\phi(n)}$$

Então $\pi(x) = \frac{1}{\phi(n)} \pi(h(\text{mod } n))$

$$\frac{\partial}{\partial x} \left(\frac{1}{\phi(n)} \pi(h(\text{mod } n)) \right) = \frac{1}{\phi(n)} \frac{\partial \pi(h(\text{mod } n))}{\partial x}$$

$$= \frac{1}{\phi(n)} \frac{\partial}{\partial x} \left(\frac{1}{\phi(n)} \sum_{p \leq x} 1 \right)$$

$$= \frac{1}{\phi(n)^2} \left(\frac{\partial}{\partial x} \sum_{p \leq x} 1 \right) + \frac{1}{\phi(n)} \frac{\partial}{\partial x} \left(\frac{1}{\phi(n)} \right)$$

$$= \frac{1}{\phi(n)^2} \left(\frac{d}{dx} \sum_{p \leq x} 1 \right) + \frac{1}{\phi(n)^2}$$

$$= \frac{1}{\phi(n)^2} \left(\frac{d}{dx} \sum_{p \leq x} 1 \right) + \frac{1}{\phi(n)^2}$$

$$= \frac{1}{\phi(n)^2} \left(\frac{d}{dx} \sum_{p \leq x} 1 \right) + \frac{1}{\phi(n)^2}$$

$$= \frac{1}{\phi(n)^2} \left(\frac{d}{dx} \sum_{p \leq x} 1 \right) + \frac{1}{\phi(n)^2}$$

$$= \frac{1}{\phi(n)^2} \left(\frac{d}{dx} \sum_{p \leq x} 1 \right) + \frac{1}{\phi(n)^2}$$

$$= \frac{1}{\phi(n)^2} \left(\frac{d}{dx} \sum_{p \leq x} 1 \right) + \frac{1}{\phi(n)^2}$$

$$= \frac{1}{\phi(n)^2} \left(\frac{d}{dx} \sum_{p \leq x} 1 \right) + \frac{1}{\phi(n)^2}$$

$$\text{Luego } u_p(k!) - k \leq \frac{k}{p-1} - k \xrightarrow[k \rightarrow \infty]{} 0$$

$$= k \left(\frac{2-p}{p-1} \right) \xrightarrow[k \rightarrow \infty]{} -\infty$$

Así $\sum_{k=0}^{\infty} p^k \binom{n_2}{k} = \sqrt{1+p} \in \mathbb{Q}_p$

Sí tomamos: $\sum_{k=0}^{\infty} 15^k \binom{n_2}{k} = \sqrt{1+15} \in \mathbb{Q}_3$
 $4 = \sqrt{1+15} \equiv 1 \pmod{3}$
 $-4 = \sqrt{1+15} \equiv 1 \pmod{3}$

$$(L = K(\sqrt{d}))$$

• L/K es ktz cuadrática $\Leftrightarrow K_P = L_{P_1} \times L_{P_2}$

equivalente: Hay 2 lugares sobre \mathbb{R}

equivalentemente: Hay 2 lugares sobre \mathbb{R} que tienen dos raíces en K_P .

Si P no se descomponer: entonces

equivalentemente: Hay un solo lugar sobre \mathbb{R} que tiene dos raíces en K_P .

Caso 1: Se descomponer: $|K^*| \subseteq \mathbb{R}$

$$f(L/\mathbb{R}) = [L : \mathbb{R}] = [K_P : \mathbb{R}]$$

$$e(L/\mathbb{R}) = [L : K_P]$$

$$\text{donde } K_P = \frac{m_K}{m_L}, \quad [L : K_P] = \frac{m_L}{m_K}$$

Siempre es cierto que $\frac{e(L/\mathbb{R})}{f(L/\mathbb{R})} = \frac{[L : K_P]}{[L : \mathbb{R}]} = \left[\frac{K_P}{\mathbb{R}} \right] = \left[\frac{K_P}{\mathbb{Q}} \right] = f(K/\mathbb{Q})$

• Para la extensión cuadrática: $[L/\mathbb{F}_p] = 2$

$$\begin{array}{ll} e=2 & e=1 \\ f=1 & f=2 \\ \text{ram.} & \text{no ram.} \end{array}$$

Así \mathbb{R} es no ramificada si existe $a \in \mathcal{O}_L$ tal que:

$i) \bar{a}, \bar{1}_K$ no tiene raíces en K

($\bar{a} \in \mathbb{L}$) Si solo hay la extensión es ramificada.

Ejemplo: $L = \mathbb{Q}(\sqrt{3})$.

$$\sigma_L = \mathbb{Z}[\sqrt{3}]$$

$$\begin{aligned} \text{Así: } f(x) &= x^2 - 3. \\ f'(x) &= 2x. \end{aligned}$$

observemos: $|f'(a)| \neq 1$ si $|a| \neq 1 \text{ o } |2| \neq 1$.

Si $a^2 \equiv 3(p)$ y $a \equiv 0 \pmod{p}$ sobre \mathbb{P} .

ssi $3 \equiv 0(\mathbb{R})$

$p=3 \Rightarrow \mathbb{P} = \mathbb{Z}/3\mathbb{Z}$ hay raíces en $\mathbb{W}_{\mathbb{P}}$ (\mathbb{P} es compuesto).

(Si: $x^2 - 3 \equiv 0 \pmod{p}$) \Leftrightarrow no hay raíces en $(\mathbb{W}_{\mathbb{P}})$

(Si: $p \neq 2, 3$ y $x^2 - 3 \not\equiv 0 \pmod{p} \Rightarrow$ toda solución $x \in \mathbb{F}_p$ genera una extensión

$x^2 - 3 \not\equiv 0 \pmod{p}$)

cuadrática.

luego \mathbb{P} es no ramificado (inerte).

Si: $p=2 \text{ o } 3$: $3 \in \mathbb{P}$ ramificado pues:

Supongamos $L_{\mathbb{P}} = \mathbb{Q}_3(\sqrt{3}) \Rightarrow |\sqrt{3}|_{\mathbb{P}} = 13|\mathbb{P}| = |\sqrt{3}|_3 = \frac{1}{3} \cdot 3$

$\therefore |\sqrt{3}|_{\mathbb{P}} = \frac{1}{\sqrt{3}} \notin 3\mathbb{Z}$. \therefore es ramificado.

$$\begin{aligned} 3 &= 1 \cdot 3 \\ p_{\mathbb{P}} &= (a)^2 \end{aligned}$$

Para $p=2$... Señor Notaremos
la ext. normativa de $\frac{12\sqrt{5}}{(x^2)}$

\therefore Es no ramificada.

(*) Por $a \in \mathbb{Z}_2^*$ es cuadrado ssi $a \equiv 1 \pmod{8}$

Si $d \equiv 1 \pmod{8} \Rightarrow 4|d$ decomposta.

Si $d \equiv 5 \pmod{8} \Rightarrow 4|d$ inerte.

Otro caso: Es ramificado.

(*) Por $a \in (\mathbb{Z}_{12}^*)^*$ es cuadrado

(caso $n=3$).

Si F es arquimediano: $d \equiv 1 \pmod{4}$
 $\zeta \in \mathbb{Q}(\alpha_F) = \mathbb{Q}(\zeta_3)$ $\alpha_F = \zeta + \zeta^2$
 $\alpha_F = \zeta + \zeta^2 \Rightarrow \alpha_F^2 = \zeta^2 + \zeta^4 \Rightarrow \alpha_F^2 = -1$

$L = \mathbb{Q}(\zeta_{12})$ $\zeta_{12} = e^{2\pi i/12} = e^{i\pi/6}$

$|\zeta_{12}|_p = 2^{-1/p}$ si generador

$\therefore \mathbb{F}_p \not\subseteq \mathbb{Q}(\zeta_{12})$ $\mathbb{F}_p = \mathbb{Q}(\zeta_{12})$ $\mathbb{F}_p = \mathbb{Q}(\zeta_{12})$

$$\sum_p f_p = 5$$

Caso $p \nmid 12$ dominio

\therefore Hay un solo lugar sobre \mathbb{R} y es ramificado.

Se da $\text{Si } p=5: \quad \textcircled{1} \quad \mathbb{R} = \mathbb{R} \times \mathbb{C} \times \mathbb{C}$ pues $\mathbb{M}(\zeta_{12}) \cong \mathbb{S}^1$

\therefore hay un lugar real y 2 complejos.

donde $K = \mathbb{Q}$

Si $p \neq 5$; $f(x) = x^5 - 2$, $\text{Si } a \in \mathbb{Z}_{12} \in \mathcal{O}_L$

Simplifica el criterio

$$f(a) = 0$$

$$f'(a) = 5a^4$$

Si $p \neq 5, 2$

L no ramificado en \mathbb{R} .

$$L(\mathbb{X})/\mathbb{Q}_p = L_{p_1} \times \dots \times L_{p_r} \text{ donde } L_{p_i}/\mathbb{Q}_p \text{ no ramificado.}$$

para cada t hay una única extensión no ramificada L/\mathbb{Q}_p con
 $L = \mathbb{Q}_p(t) \cong \mathbb{F}_{p^t}$.

Problema 7.4. Si α es un entero,

$$\alpha \in L_K \text{ si y sólo si } |\alpha|_K \leq 1 \text{ y } N_{L_K}(\alpha) \leq 1.$$

y α entero si $\alpha + 1$ entero.

$$|\alpha|_K \leq 1 \text{ si y sólo si } |N_{L_K}(\alpha + 1)| \leq 1.$$

Así se demuestra que: $p(\alpha) = |\alpha|_K$ es un n.v.a en L .

$$\text{Así si } p_0(\alpha) = |\alpha|_K$$

y p_0 son normas en $L \Rightarrow p \sim p_0$ como normas.

Así: las sucesiones suc. convergen en $p \wedge p_0$

Si $p_0 \neq p^r$, $\forall r$:

$$\text{Probar que: } \exists q \in K \text{ con: } \begin{cases} p_0(q) < 1 \\ p(q) > 1 \end{cases} \quad (*)$$

$\therefore q^n \text{ converge a } 0 \text{ en } p_0$

$q^n \text{ no converge a } 0 \text{ en } p$

$$\text{y s: } \alpha \in K: |\alpha|_K = |N_{L_K}(\alpha)|_K^s \\ = |\alpha|_{L_K}^s \Rightarrow s = \frac{1}{[L:K]}.$$

(*) Se $x \in K$, $p(x) = p_0(x)^r$ Como $p \neq p_0^r \Rightarrow \exists y \text{ con } p(y) > p_0(y)^r$ (SPG)

$$\text{entonces: } \frac{p(y)}{p_0(y)^r} > \frac{m}{n} > \frac{p(x)}{p_0(x)^r} = 1, \text{ o bien:}$$

$$\frac{\log p(y)}{\log p(x)} \geq \frac{m}{n} \geq \frac{\log(p_0(y))}{\log(p_0(x))}$$

$$\therefore n \log p(y) \geq m \log p(x)$$

$$\log(p(y)/p(x)^m) > 0$$

$$\therefore p(y^n/x^m) > 1$$

$$y \text{ protoavisino} = p_0(y^n/x^m) < 1$$

$$1 \geq f(x) \geq 1 - \epsilon$$

$$\therefore p_0(y^n/x^m) < 1 - \epsilon$$

notemos que $a \in r$ es el menor elemento, entonces $\frac{a-1}{m} < b$

Sólo falta ver que $a < \frac{a-1}{m}$. Si $a \geq \frac{a-1}{m}$

$$\text{entonces: } a < b - \frac{1}{m} < \frac{a-1}{m} - \frac{1}{m} = \frac{a-1}{m}.$$

Prop: $I_n = [x_n, b_n]$ tal que $I_{n+1} \subseteq I_n$

entonces: $\bigcap_{n \in \mathbb{N}} I_n \neq \emptyset$.

(ejercicio)

Prop: Toda sucesión monótona y acotada es convergente.

Sea $(x_n)_{n \in \mathbb{N}}$ creciente y acotada.

Vemos que $A = \{x_n\}_{n \in \mathbb{N}} \neq \emptyset$ y es acotado.

Por lo tanto existe $\text{Sup}(A)$.

pd: $\lim_{n \rightarrow \infty} x_n = \text{Sup}(A)$.

$$\forall \varepsilon > 0 \exists x \in A \text{ tal que } |\text{Sup}(A) - \varepsilon| \leq x_n \leq x_m$$

$$\therefore \forall \varepsilon > 0 \exists x \in A \text{ tal que: } \text{Sup}(A) - \varepsilon < x_n < \varepsilon$$

$$\therefore \forall \varepsilon > 0 \exists n \in \mathbb{N}: m > n \Rightarrow \text{Sup}(A) - x_m < \varepsilon$$

* Prop: Toda sucesión tiene una subsucesión monótona.

Prop: Bolzano-Weierstrass: toda suc. acotada tiene una subsucesión convergente.

Prop: Toda suc. de Cauchy es acotada.

Sea $(x_n)_{n \in \mathbb{N}}$ una sucesión de Cauchy.

$$\forall \varepsilon > 0 \exists n_0 \in \mathbb{N}: n, m > n_0 \Rightarrow |x_n - x_m| < \varepsilon$$

Sea $\varepsilon = \frac{1}{2} > 0$. $\exists n_0 \in \mathbb{N}$ tal que $n, m > n_0: |x_n - x_m| < \frac{1}{2}$

$$\therefore |x_n - x_{n_0}| \leq \frac{1}{2}$$

$$\therefore -\frac{1}{2} + x_{n_0} \leq x_n < \frac{1}{2} + x_{n_0}$$

\therefore la suc. es acotada.

Ayudantía Auditisis:

Aníomas de \mathbb{R} : Si $\phi \neq A \subseteq \mathbb{R}$ acotado superiormente, entonces

existe $\sup(A) = \alpha$ donde $\forall x \in A$:

$$x \leq \alpha \text{ y si } \forall x \in A \quad x \leq \beta \Rightarrow \alpha \leq \beta$$

1) Prop. Arquimediana: $\forall x > 0 \exists n \in \mathbb{N} \text{ tal que } n > x$

Supongamos falso: $\exists x > 0 \forall n \in \mathbb{N}: n \leq x$

$\therefore \{n \mid n \leq x\}$ esta acotado sup.

$\therefore \exists \sup(\mathbb{N}) \in \mathbb{R} \text{ tal que: } \text{Así: } \begin{cases} n \leq \sup(\mathbb{N}) \\ \sup(\mathbb{N}) \leq x \end{cases}$

(1+2)
Supr(N)

pd: $\sup(\mathbb{N}) + 1 \in \mathbb{N}$.

Por def de supremo: $\forall \varepsilon > 0: \exists n \in \mathbb{N}: \sup(\mathbb{N}) - \varepsilon \leq n$

Sea $\varepsilon = \frac{1}{2}$, teniendo $n \in \mathbb{N}: \sup(\mathbb{N}) - \frac{1}{2} \leq n$

Se tiene que: $n + 1 > \sup(\mathbb{N}) + \frac{1}{2} \geq \sup(\mathbb{N})$. \Rightarrow

2) $\forall x > 0 \exists n \in \mathbb{N} \text{ tal que: } 0 < \frac{1}{n} < x$.

Demonstración: Sea $x > 0 \Rightarrow \exists x > 0 \Rightarrow \exists n \in \mathbb{N}: n > \frac{1}{x}$

luego: $x > \frac{1}{n} > 0$.

Definición: $A \subseteq \mathbb{R}$ es denso en \mathbb{R} si: $\forall a < b$ se tiene que $(a, b) \cap A \neq \emptyset$.

Análogamente se define $\forall x \in \mathbb{R} \exists \{x_n\}_{n \in \mathbb{N}}$ sucesión en A tal que:

$\lim_{n \rightarrow \infty} x_n = x$.

Prop: \mathbb{Q} es denso en \mathbb{R} .

Dem: Sea $a < b$ por propiedad de arquimediana $\exists n \in \mathbb{N}$ tal que $\frac{1}{n} < b - a$. Sea $J = \{n \in \mathbb{Z} / n > mb\}$ cota inferior.

Sea $n_0 \in J$ menor elemento de J , entonces $n_0 \geq mb$, $b \leq \frac{n_0}{m}$

pd: $a < \frac{n_0 - 1}{m} < b \leq \frac{n_0}{m}$

$$\text{Luego } p^{p-1} - s_1 p^{p-2} + \dots + (p-1)! = (p-1)!$$

$$p^{p-1} - s_1 p^{p-2} + \dots - s_{p-2} p = 0$$

$$\text{reduciendo la ec. módulo } p^3: \quad s_{p-2} p \equiv 0 \pmod{p^3}$$

$$\text{Así: } p^3 \mid p s_{p-2} \Rightarrow p^2 \mid s_{p-2}, \text{ o sea: } s_{p-2} = \sum_{k=1}^p \frac{(p-1)!}{k} \equiv 0 \pmod{p^2}$$

Una aplicación del teo. Clínico de los Restos:

Sea f un polinomio con coef. ent. pol. m_1, \dots, m_r primos distintos

y $m = m_1 \cdots m_r$. Entonces \exists congruencia

$$f(x) \equiv 0 \pmod{m} \quad (1)$$

Tiene una sol. SSI. Otra ecuación:

$$f(x) \equiv 0 \pmod{m_i} \quad (2)$$

admita solución. Además:

$$\#\text{sol. (1)} = \prod \#\text{sol. (2)}.$$

Demarcación: Si $f(a) \equiv 0 \pmod{m} \Rightarrow f(a) \equiv 0 \pmod{m_i}$.

Si a_i es sol. de (2) entonces existe: {Princ. Clínico de los Restos} $a \equiv a_i \pmod{m_i}$

Luego: $f(a) \equiv f(a_i) \equiv 0 \pmod{m_i}$

Resumo que $(m_i, m_j) = 1$, si $i \neq j$ tenemos que: $m_i \mid f(a) \Rightarrow m \mid f(a) \Rightarrow f(a) \equiv 0 \pmod{m}$

Por lo tanto sol. de la ec. en $\mathbb{Z}/m\mathbb{Z}$ se tienen $v(m_1) \cdots v(m_r)$ soluciones ($i \neq j$).

Congruencias pol. relativistas a potencias de primos.

22236329

Teorema de Repetición: Dado un primo p , sea $f(x) = c_0 + \dots + c_n x^n$ \pmod{p} . Entonces la congruencia polinomial $f(x) \equiv 0 \pmod{p}$ tiene al menos n soluciones.

Demonstración: Por inducción. Si $n=1$ la congruencia lineal $(1x + c_0 \equiv 0 \pmod{p})$

tiene una solución pues $(c_1, p) = 1$.

Si el teo. es válido para $n-1$. Supongamos que (*) tiene $n+1$ (o más) soluciones congruentes módulo p , digámonos $\{x_0, \dots, x_n\}$.

Tendremos así que:

$$f(x) - f(x_0) = \sum_{r=1}^n (c_r(x^r - x_0^r)) = (x - x_0) p(x)$$

donde $d(p(x)) = n-1$. Entonces:

$$f(x_k) - f(x_0) = (x_k - x_0) p(x_k) \equiv 0 \pmod{p} \quad k \in \{1, \dots, n\}$$

pero que $x_k - x_0 \not\equiv 0 \pmod{p}$, $p(x) \equiv 0 \pmod{p}$ tiene más de $p-1$ soluciones. \Rightarrow

$\therefore f(x)$ tiene al menos n soluciones.

Por contrapositivo, si $f(x)$ tiene más de n soluciones $\Rightarrow (c_k \equiv 0 \pmod{p})$ todo $k \in \{1, \dots, n\}$

Teo: Para cada primo p todos los coef. de $f(x) = (x-1) \dots (x-p+1) - x^{p-1} + L$

Son divisibles por p .

Demonstración: observe que $\exists f(x) = p-1$, pero todo número $x_0 \in \{1, \dots, p-1\}$ tal que:

$$f(x_0) \equiv 0 - x_0^{p-1} + 1 \equiv 0 \pmod{p}$$

así $f(x)$ tiene $p-1$ soluciones \Rightarrow todos los coef. de $f(x)$ son divisibles por p .

Corolario: teorema de Wolstenholme: para todo primo $p \geq 5$ tenemos

$$\sum_{k=1}^{p-1} \frac{(p-1)!}{k} \equiv 0 \pmod{p^2}$$

Prueba: observe que la suma es el coef. de $-x$ en $f(x)$. Por lo tanto

$$\sum_{k=1}^{p-1} \frac{(p-1)!}{k} \equiv 0 \pmod{p}$$

pero $f(x) = (x-1) \dots (x-p+1) = x^{p-1} - S_1 x^{p-2} + \dots + (p-1)!$

por el teo. anterior cada $S_k \equiv 0 \pmod{p}$

observe además que $f(p) = (p-1) \dots (1) = (p-1)!$.

Ley de los inversos de los primos.

Supongamos que la sucesión converge, entonces: existe $k \in \mathbb{N}_0$:

$$\sum_{m=k+1}^{\infty} \frac{1}{p_m} < \frac{1}{2}$$

Esto significa: para $\varepsilon = \frac{1}{2}$, existe $N \in \mathbb{N}_0$ tal que:

$$\left| \sum_{m=1}^{\infty} \frac{1}{p_m} - \sum_{m=1}^N \frac{1}{p_m} \right| < \frac{1}{2},$$

$$\sum_{m=N+1}^{\infty} \frac{1}{p_m} < \frac{1}{2}.$$

Sea $U = p_1, \dots, p_k$ y considere $\{(1+hU)\}_{h \in \mathbb{N}_0} \subseteq \mathbb{N}_0$. observe que si

$p_i \mid 1+hU$, algún $p_i \in \{p_1, \dots, p_k\}$, $h \in \mathbb{N}_0$ entonces $p_i \mid h$ (\star)

Por consiguiente todos los factores primos de los números de la forma $1+hU$

se encuentran entre $p_{k+1}, \dots, p_n, \dots$. Así, para $t \geq 1$.

$$\sum_{n=1}^r \frac{1}{1+hU} \leq \sum_{t=1}^{\infty} \left(\sum_{m=k+1}^{\infty} \frac{1}{p_m} \right)^t. \quad (\star)$$

$$< \sum_{t=1}^{\infty} \left(\frac{1}{2} \right)^t$$

$$\sum_{n=1}^r \frac{1}{1+hU} \text{ converge } (\star).$$

Por lo tanto, por criterio de comparación:

Luego: $\sum_{m=1}^{\infty} \frac{1}{p_m}$ diverge.

$$(*) \quad \sum_{t=1}^{\infty} \left(\sum_{m=k+1}^{\infty} \frac{1}{p_m} \right)^t = \sum_{m=k+1}^{\infty} \frac{1}{p_m} + \left(\sum_{m=k+1}^{\infty} \frac{1}{p_m} \right)^2 + \dots + \left(\sum_{m=k+1}^{\infty} \frac{1}{p_m} \right)^t, \dots$$

$$\geq \sum_{m=k+1}^{\infty} \frac{1}{p_m} + \left(\frac{1}{p_m} \right)^2 + \dots + \left(\frac{1}{p_m} \right)^t, \dots$$

$$\geq \sum_{m=k+1}^{\infty} \frac{1}{p_m} + \left(\frac{1}{p_m} \right)^2 + \dots + \left(\frac{1}{p_m} \right)^s, \text{ donde } s = \text{máx exponentes de } m+k+1, m+k+2, \dots, m$$

$$\geq \sum_{m=k+1}^{\infty} \frac{1}{p_m} + \dots + \left(\frac{1}{p_m} \right)^s$$

$$\geq \sum_{n=1}^r \frac{1}{1+hU}.$$

Suma finita de los p_i que descomponen al número $1+hU$.

Problema 3: $\mathcal{L}(\sqrt{-1})$, $\mathcal{L}(w)$ son dominios do f.c. $\mathbb{C}[i]$
(de hecho euclidianos).

1) $\mathcal{L}(\sqrt{-1})$

- 1) Se $a+bi \in \mathcal{L}(i)$ y $c+di \in \mathcal{L}(i)$.

Si $x, y \in \mathcal{L}(i) \subseteq \mathcal{U}(i)$

entonces $x^{-1} \in \mathcal{U}(i)$

luego $x^{-1} = r+si$, $r, s \in \mathcal{U}(i)$

$$x^{-1} = (r+si)(\frac{c-di}{c^2+d^2}) = \frac{rc+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i$$

tenemos preferencias tales que: (enteros más cercanos).

$$|r-p| \leq \frac{1}{2}, |s-q| \leq \frac{1}{2}$$

Sea $\Theta = p+fi \in \mathcal{L}(i)$ y $M = \beta((r-p)+(s-f)i) \in \mathcal{U}(i)$, así:

$$\begin{aligned} 1) \quad \alpha &= (\alpha^{-1})p = (r+si)\beta = p((r-p)+(s-f)i) + \beta(p+fi) \\ &= \beta\Theta + M \end{aligned}$$

$$2) \quad M = \beta\Theta - \alpha \in \mathcal{L}(i)$$

$$3) \quad N(M) = N(p)N((r-p)+(s-f)i) = N(p)\left(\frac{1}{4}+\frac{1}{4}\right) = N\left(\frac{p}{2}\right) < N(p)$$

Si $M \neq 0$, si $M = 0$ se concluye.

$$2) \quad \mathcal{L}(w) = \mathcal{L}\left(\frac{1+\sqrt{-3}}{2}\right), \quad N(a+bw) = (a+b\left(\frac{1+\sqrt{-3}}{2}\right))(a+b\left(\frac{1-\sqrt{-3}}{2}\right)) = a^2 + ab + b^2$$

$$1) \quad \text{Si } \alpha, \beta \in \mathcal{L}(w) \quad \alpha^{-1} \in \mathcal{U}(w), \quad \alpha^{-1} = r+sw$$

Sean p, q enteros tales que $|r-p| \leq \frac{1}{2}, |s-q| \leq \frac{1}{2}$

Sea $\Theta = p+fi \in \mathcal{L}(w)$, $M = \beta((r-p)+(s-f)w) \in \mathcal{U}(w)$

$$1) \quad \beta\Theta + M = \beta((r-p)+(s-f)w) + \beta(p+fw) = \beta(r+sw) = \beta\alpha^{-1} = \alpha$$

$$2) \quad M = \alpha - \beta\Theta \in \mathcal{L}(w)$$

$$3) \quad N(M) = N(\beta)((r-p)^2 + (r-p)(s-f) + (s-f)^2) \leq N(\beta) \frac{3}{4} < N(\beta)$$

Si $M \neq 0$. Si $M = 0$ se concluye.

Definición 1: $D[x] = \{ f(x) \mid f(x) \in D[x] \}$.

x entero si

2) $D[x]$ es finitamente generado como D -módulo.

$$\text{Si } x \text{ es entero} \Rightarrow x^n + d_{n-1}x^{n-1} + \dots + d_0 = 0 \Rightarrow x^n = -d_{n-1}x^{n-1} - \dots - d_0.$$

$$\text{así: } x^{n+k} \in D \oplus Dx \oplus \dots \oplus Dx^{n-1}$$

$$\therefore D[x] = D \oplus Dx \oplus \dots \oplus Dx^{n-1}$$

\therefore es finita mente generado como D -módulo.

2) \exists si

3) \exists un D -módulo f generado con $\Pi \subseteq L$ y $\alpha \Pi \subseteq M$

Considera $D[x]$ un D -módulo fg y $D[x] \subseteq L$

$$\text{entonces: } \alpha D[x] = \{ \alpha f(x) \mid f(x) \in D[x] \} \subseteq D[x].$$

3) \Rightarrow x entero:

Supongamos $M = \langle m_1, \dots, m_r \rangle$ entero (\neq) como $\alpha \Pi \subseteq M$

$$\text{Supongamos } x m_i \in M \quad \text{y} \quad x m_i = \sum_{j=1}^r a_{ij} m_j, \quad \forall i \in \{1, \dots, r\}$$

$$\text{Luego: } \alpha x m_i = \sum_{j=1}^r a_{ij} \alpha m_j \quad \text{ss: } (\alpha I - A) \vec{m} = 0$$

$$\text{Si } \vec{m} = \begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix}, \quad \alpha I \vec{m} = A \vec{m} \quad \text{ss: } (\alpha I - A) \vec{m} = 0$$

$$\text{Luego: } \det(\alpha I - A) \vec{m} = 0, \quad \text{como } \vec{m} \neq \vec{0}$$

$$\text{entonces: } \det(\alpha I - A) = 0 = p(x) \quad (\text{polinomio con coefs en } D)$$

$\therefore x$ es entero.

Definición 2: $\mathbb{Z}[\sqrt{-5}] = \bigcup_{\mathbb{Q}(\sqrt{-5})}$

$$\text{Como sabemos } \bigcup_{\mathbb{Q}(\sqrt{-5})} = \{ a + b\sqrt{-5} \mid a, b \text{ enteros satis } \mathbb{Z} \}$$

$$= \{ a + b\sqrt{-5} \mid a, b \in \mathbb{Z} \} = \mathbb{Z}[\sqrt{-5}]$$

Primeros $-5 \equiv -1 \equiv 3(4)$



$$A = \begin{pmatrix} \pi & 0 \\ 0 & \pi^{-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} \pi & \pi^{-1} \\ \pi^{-1} & 0 \end{pmatrix} \begin{pmatrix} 1 & \pi^{-2} \\ 0 & 1 \end{pmatrix}$$

Ajustables →

Para Ajustar A basta hacerlo con $\begin{pmatrix} \pi & \pi^{-1} \\ \pi & 0 \end{pmatrix}$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \pi & 0 \\ 0 & \pi^{-1} \end{pmatrix} = \begin{pmatrix} a\pi & b\pi^{-1} \\ c\pi & d\pi^{-1} \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & at+b \\ c & ct+d \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -b & a \\ -d & c \end{pmatrix}$$

$$\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ ct+d & c \end{pmatrix}$$

Problema 1 . en $\mathbb{Q}(\sqrt{21})$

Primos inertes:

$$\left(\frac{21}{p} \right) = \left(\frac{2}{p} \right) \left(\frac{3}{p} \right)$$

$$y \quad \left(\frac{2}{p} \right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{2} \right) = \begin{cases} 1 & p \equiv 1(28) \\ 1 & p \equiv 3(28) \\ -1 & p \equiv 5(28) \\ -1 & p \equiv 9(28) \\ 1 & p \equiv 11(28) \end{cases}$$

$$\therefore p \equiv 1(28) \quad \therefore p \equiv -3(28)$$

$$\therefore p \equiv -13(28) \quad \therefore p \equiv -11(28).$$

$$\therefore p \equiv -11(28)$$

$$\therefore p \equiv -9(28)$$

$$\therefore p \equiv -5(28)$$

$$\therefore \text{si } p \equiv 6(28)$$

$$\therefore \text{si } p \equiv 5(28)$$

$$\therefore \text{si } p \equiv 11(28)$$

$$\left(\frac{p}{2} \right) = \begin{cases} 1 & \text{si } p \equiv 1(12) \\ 1 & \text{si } p \equiv 2(12) \\ -1 & \text{si } p \equiv 3(12) \end{cases}$$

$$\therefore \text{si } p \equiv 6(12)$$

$$\therefore \text{si } p \equiv 5(12)$$

$$\therefore \text{si } p \equiv 11(12)$$

$$y \quad \left(\frac{3}{p} \right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{3} \right) = \begin{cases} 1 & \text{si } p \equiv 1(12) \\ -1 & \text{si } p \equiv 5(12) \\ -1 & \text{si } p \equiv 7(12) \\ 1 & \text{si } p \equiv 11(12) \end{cases}$$

Primeros 5 si: $p \equiv 5, 9, -13, -11, -3, -1(28)$ y $p \equiv 1, 7(12)$ o (por Heusell enc. sol en \mathbb{Q}^p)
 $p \equiv 1, 3, 11, 13, -5, -9(28)$ y $p \equiv 5, 11(12)$

P de) compuesto: $p \equiv 5, 9, -13, -11, -3, -1(28)$ y $p \equiv 5, 11(12)$ o
 $p \equiv 1, 3, 11, 13, -5, -9(28)$ y $p \equiv 1, 7(12)$.

Restan los casos $p = 7, 3$ y 2 .

si $p = 7$: $L_p = \mathbb{Q}_7(\sqrt{21}) \Rightarrow |\sqrt{21}|_p = \frac{1}{7^{1/2}} \notin 5^\infty \therefore$ estanificada.

(si fuese desc. (no ramificada) $\Rightarrow L_{p^2} = \mathbb{Q}_7^*$ \Rightarrow los v. abss son pot. de $5^\infty (\times)$)

si $p = 3$: $L_p = \mathbb{Q}_3(\sqrt{21}) \Rightarrow |\sqrt{21}|_p = \frac{1}{3^{1/2}} \notin 3^\infty \therefore$ estanificada.

si $p = 2$: $21 \equiv -3 \equiv 5(8) \therefore$ es inerte. f multiplicativa.

Problema: Si $f * f^* f = M$. Calcule $f(p^4)$, de sus pot. menores.

Solución: Trabajemos primero con $f * f = g$. multiplicativa.

$$-1 = M(p) = \sum_{d|p} f\left(\frac{p}{d}\right)g(d) = f(p)f(1) + g(p)f(1) = f(p) + 2f(p)$$

$$\Rightarrow f(1) = -\frac{1}{3}.$$

$$0 = M(p^2) = \sum_{d|p^2} f\left(\frac{p^2}{d}\right)g(d) = f(p^2)f(1) + f(p)f(p) + f(1)f(p^2) \\ = f(p^2) + 3f(p)^2 + 2f(p^2) \therefore f(p^2) = \frac{1}{3}.$$

$$0 = M(p^3) = f(p^3)f(1) + f(p^2)f(p) + f(p)f(p^2) + f(1)f(p^3).$$

$$\begin{aligned}
 \text{Luego: } 0 &= f(p^3) + \underline{f(p^2)} \underline{2f(p)} + \underline{f(p)} \underline{(2f(p^2) + f(p)^2)} + \underline{2f(p^3)} + \underline{2f(p^2)f(p)}. \\
 0 &= 3f(p^3) + 6f(p^2)f(p) + f(p)^3 \\
 0 &= 3f(p^3) - \frac{1}{27} + \frac{16}{3} - \frac{1}{3} \\
 3f(p^3) &= \frac{1+18}{27} \Rightarrow f(p^3) = \frac{19}{81}.
 \end{aligned}$$

Por lo tanto:

$$\begin{aligned}
 0 &= M(p^4) = f(p^4) + f(p^3)f(p) + f(p^2)f(p^2) + f(p)f(p^3) + f(p^4) \\
 &= \underline{f(p^4)} + 2f(p)\underline{f(p^3)} + \underline{(2f(p^2) + f(p)^2)}\underline{f(p^2)} + \underline{f(p)(2f(p^3) + 2f(p^2)f(p))} \\
 &\quad + (\underline{f(p^4)} + \underline{f(p^2)}\underline{f(p)} + \underline{f(p^2)^2}) \\
 0 &= 2f(p^4) + 6f(p^3)f(p) + 3f(p^2)^2 + 3f(p)^2f(p^2). \\
 0 &= 2f(p^4) + \frac{38}{27} - \frac{1}{3} + 3 \cdot \frac{1}{9} + \frac{1}{3} \cdot 3 + \frac{1}{9} \\
 0 &= 2f(p^4) + \frac{-38}{81} + \frac{1}{3} + 1 + \frac{1}{9} \\
 2f(p^4) &= \frac{38 - 27 - 81 - 9}{81} = -\frac{79}{81} \\
 f(p^4) &= \frac{-79}{162}.
 \end{aligned}$$

$T \in M_2(\mathbb{Z}_p)^*$ pues cada $|a_{ij}|_p \leq 1 \quad \forall p$.

Salvo si: $\det T = \det \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} = -1$

$\|\det T\|_p = p^0 = 1 \quad \therefore T \in M_2(\mathbb{Z}_p)^* \quad \forall p : \Lambda_p = \Lambda_0 p \quad \forall p$

En el caso de la toro: $\lambda = \mathbb{Z}(123) \oplus \mathbb{Z}(145) \oplus \mathbb{Z}(168)$

entonces $T = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 4 & 6 \\ 3 & 5 & 8 \end{pmatrix} \in M_3(\mathbb{Q})^*$

$$\Rightarrow \det T = \left| \begin{pmatrix} 1 & 1 & 1 \\ 2 & 4 & 6 \\ 3 & 5 & 8 \end{pmatrix} \right| = |146| - |24| + |24|$$

$T \in M_2(\mathbb{Z}_p)^*$ pues para cada $a_{ij} : |a_{ij}|_p \leq 1 \quad \forall p$.
 $\therefore \Lambda_p = \Lambda_0 p = \mathbb{Z}_p^3, \forall p$. (no divisible by p , fraccionarios).

problema: 1) como $L = \text{ker } (\sqrt{x})$ tiene por polo minimal $p = x^3 - 2$

\therefore tiene una raíz real y 2 complejas

$$\text{Liesgo} \quad L \circ R = R \circ I$$

$L(\mathbb{R})\mathbb{R} = \mathbb{R} \times \mathbb{C}$
 \therefore hay 2 v.n.p. extienden una recta y otra compleja, paralela.

2) Parallelogram law: $\|x+y\|^2 = \|x\|^2 + \|y\|^2$ \leftarrow proves multiplicativity.

$$\text{S: } \text{geometrie} \quad |2|_2 = |2|_{\mathbb{R}} = 2^{-1} \Rightarrow |\{f_2\}|_{\mathbb{R}} = 2$$

$$\text{d.h.: } e_p = e(L_p | \mathbb{K}_2) = 3. \text{ ja per: } \\ e(L_p | \mathbb{K}_2) = \left| \frac{L_p}{\mathbb{K}_2} \right| = 3 \text{ per s: } a+b\sqrt{2} + c\sqrt[3]{4} \in L_p^* \Rightarrow \\ \frac{L_p^*}{\mathbb{K}_2^*} = \{1, \sqrt{2}, \sqrt[3]{4}\}.$$

grupos multiplicativos.
 (cociente bien de factores $L_p^* \cong \mathbb{Z}_2^{k_1} \times L_p^* \cong \mathbb{Z}_2^{k_2}$ por ser abeliano con el producto)

i. la extensión es territorial

∴ la ejecución es la finalización
∴ hay un solo lugar sobre el que lo extiende. (4)

$$(*) \text{ aus: } f(L/K) = [L:K] = 1 \quad \therefore L = K \quad \therefore \frac{\sigma_L}{m_K} = \frac{\sigma_L}{m_L}$$

∴ tienen π_k, π_L par. unit $\Rightarrow \pi_k = u\pi_L^e$, cierto $e > 1$

$$\therefore z = u \pi_1 e$$

problem : $P = \mathcal{L}(1,1) \cap \mathcal{L}(2,1)$ ist nicht ausreichend um M^2

$$\text{Det loss: } \Pi_p \neq \mathbb{Z}^{p^2}$$

Dew:

$$\Pi_p = \mathbb{Z}((1))_{(p)} \oplus \mathbb{Z}(2)_{(p)}, \quad \text{basis set } \{1\},$$

$\|a, b\| = \max\{|a|_p, |b|_p\}$.

$$\text{Defn: } \gamma_{L(\{i\})}(q) = \underbrace{\text{cls}(\gamma_{L(\{i\})})}_{\{(q, q)\} \mid q \in L^P}$$

$$\therefore n_p = 1 \quad \left. \right\} \quad \Lambda_\infty = \mathbb{Z}^2$$

$$T_{e_1} = (11) \Rightarrow \underline{\Lambda} = T \underline{\Lambda}_0$$

$$T e_2 = (21) \quad , \quad T h_{op} =$$

$$T_{\mathcal{E}_2} = (21) \quad , \quad T_{\Lambda_0 p} = S_{\Lambda_0 p} \quad \text{such that } \in \Pi_2(\mathbb{Z}_p)^*$$

Exemplo: $T \in M_2(\mathbb{Q})^*$ \Rightarrow $T \in M_2(\mathbb{Z}_p)^*$ considerando p.

Se define

$$\Lambda p = \pi_{\mathcal{P}} v_1 \oplus \pi_{\mathcal{P}} v_2$$

autors: "S"

$$\Lambda p = T \Lambda \circ p.$$

Teoría de Números.

Prueba 3

$$\chi^2 - n = 0$$

Julio 15 de 2010

Resuelva cuatro de los siguientes cinco problemas:

11. Encuentre todos los enteros n tales que la ecuación $x^2 - n = 0$ tiene raíces en \mathbb{Q}_5 . Justifique.

2. Encuentre los primos ramificados, inertes, y descompuestos en la extensión $\mathbb{Q}(\sqrt{55})/\mathbb{Q}$.

- ~~3.~~ Sea ρ un valor absoluto en un cuerpo K que contiene a \mathbb{Q} . Suponga que $\rho(\mathbb{Z})$ es acotado. Probar que $\rho(\mathbb{Z})$ es constante.

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

para todo par de elementos a y b en K .

- E. Determine para que valores de $x \in \mathbb{Q}_3$ se cumple que

$\sum_{k=1}^{\infty} \frac{x^k}{(k!)^2}$ converge. Justifie.

converge. Justifie.

- ~~5.~~ Demuestre que la suma

$$\underline{(3)} \quad 1 \equiv -2 = (1+3)^{1/2} = \sum_{k=0}^{\infty} \binom{1/2}{k} 3^k \equiv$$

converge en \mathbb{Q}_3 a un elemento de \mathbb{Z} . Cuál?

converge en \mathbb{Q}_3 a un elemento de \mathbb{Z} . Cuál?

$$\boxed{P_5} \text{ observe que: } S_i = \sum_{k=0}^{60} \binom{11_k}{k} 3^k \rightarrow 2 \text{ Limite}$$

$$\Rightarrow \left\| \sum_{k=0}^{\infty} \binom{1/2}{k} 3^k - 2 \right\|_3 = 0,$$

Este es el da que

$$\left\| 1 + \binom{1}{1} 3 + \dots + \binom{1}{1} 3^k \dots \right\|_3 = 0$$

$$\text{zero } 31 \left(\frac{11_2}{K} \right) 3^k \text{ zero } 3+ -1 (\neq)$$

$$\sum_{k=1}^{\infty} \left(\frac{1}{2} \left| \frac{3}{5} \right|^k \right) \rightarrow -2.$$

$$\begin{aligned}
 & \text{S: } p\left(\frac{2}{b}\right) \leq 1 \\
 & \text{Pd: } p\left(\frac{2}{b} + 1\right) \leq 1 \\
 \underline{\text{Derm:}} \quad & p\left(\left(\frac{2}{b} + 1\right)^n\right) = p\left(\frac{2}{b} + 1\right)^n = p\left(\sum_{k=0}^n \binom{n}{k} \left(\frac{2}{b}\right)^k\right)^n \\
 & \leq \sum_{k=0}^n p\left(\binom{n}{k}\right) p\left(\left(\frac{2}{b}\right)^k\right)^n \\
 & \leq \sum_{k=0}^n 1 = n+1 \\
 \Rightarrow & p\left(\frac{2}{b} + 1\right) \leq \sqrt[n+1]{n+1} \xrightarrow[n \rightarrow \infty]{} 1 \quad //.
 \end{aligned}$$

zweiten $\rho \leq 5 \Rightarrow$ prim-freies. (primär der Eisenstein)

$$\text{für } p=2$$

$$\text{wodurch } \mathcal{O}_2^*/\mathcal{O}_2^{*2} \cong \mathbb{Z}_2^\times$$

$$a \equiv 1 \pmod{8} \Rightarrow \mathcal{O}_2^*/\mathcal{O}_2^{*2} \cong (\mathbb{Z}/(n))^\times \cong \mathbb{Z} \times \mathbb{Z}_2$$

$$\mathcal{O}_2^*/\mathcal{O}_2^{*2} \cong \mathbb{Z}/2\mathbb{Z}$$

$$\mathcal{O}_2 \xrightarrow{\quad} \mathcal{O}_2/\mathcal{O}_2^2 \cong \mathbb{Z}_2$$

} prim-freies.

problem 4e Converge en $\mathbb{R}[z]$: $\sum_{k=0}^{\infty} 2^k \binom{n_k}{k}$?

$$\text{Basta demostrar que } v_p(2^k \binom{n_k}{k}) = k - v_p\left(\frac{n_k}{k}\right) = k - \sum_{i=1}^k \frac{(-1)^{k+i} i \cdot 3 \cdots (2k-3)}{k! 2^k}.$$

$$\begin{aligned} &= k - v_p(1 \cdot 3 \cdots (2k-3)) + v_p(k!) + k \\ &= 2k - v_p((2k-3)!) + v_p(2^k (k-1)!) + v_p(k!) \\ &= 3k + v_p((k-1)!) + v_p(k!) - v_p((2k-3)!) \xrightarrow{k \rightarrow \infty} \infty \end{aligned}$$

pero: $v_p((k-1)!) = \sum_{i=1}^{\infty} \left[\frac{k-1}{2^i} \right] \geq \frac{k-1}{2}$.

$$v_p(k!) = \sum_{i=1}^{\infty} \left[\frac{k}{2^i} \right] \geq \frac{k}{2}.$$

$$v_p((2k-3)!) = \sum_{i=1}^{\infty} \left[\frac{2k-3}{2^i} \right] \leq \sum_{i=1}^{\infty} \left[\frac{2k-3}{2^i} \right] = \frac{2k-3}{2}.$$

$$\text{Luego: } v_p(2^k \binom{n_k}{k}) \geq 3k + \frac{k-1}{2} + \frac{k}{2} - \frac{2k-3}{2} = \frac{6k + k-1 + k - 4k + 6}{2} = \frac{4k+5}{2} \xrightarrow{k \rightarrow \infty} \infty.$$

Resposta: Sí.

problem 11 Encuentre todos los enteros naturales $x \geq n$ tales que $x^2 \equiv n^2 \pmod{5}$.

$$\sigma = \mathbb{Z}_5, m_L = 5 \in \mathbb{Z}_5^{\times}, \sigma / m \cong \frac{\mathbb{Z}_5}{5\mathbb{Z}_5} \text{ (como anillos)}$$

Se quiere que: $x^2 \equiv n^2 \pmod{5}$, pero: $\|n\|_5 \leq 1 \Rightarrow \|x\|_5 = \|x\|_5^2 \leq 1 \Rightarrow \|x\|_5 \leq 1$

$x \in \sigma = \mathbb{Z}_5$, entonces: si $\exists x \in \sigma : x^2 = n \Rightarrow x^2 \equiv h(m_L) \Rightarrow x^2 \equiv n(5)$

$$\text{si } n \in \{1, -1, 0\} : \begin{cases} 1^2 = 1 \\ 2^2 = 4 \\ 3^2 = 4 \\ 4^2 = 1 \\ 0^2 = 0 \end{cases} \quad n \in \{1, -1, 0\}.$$

Si $n \in \{1, -1, 0\}$, si: $n=0 : 0^2 = 0 \in \sigma$, pero si $n=-1 :$

$$2^2 = 4 = -1 \pmod{5} \quad (x^2 - n)^2 = 2x \neq 0 \pmod{5}$$

Luego por el teorema existen soluciones $\in \sigma$ para: $x^2 \equiv -1 \pmod{5}$

$$\Rightarrow \|x_{0(m)}^2 + 1\|_5 = \left(\frac{1}{m} \right) \xrightarrow{m \rightarrow \infty} 0 \quad \therefore \exists x_0 = \lim_{m \rightarrow \infty} x_{0(m)} : x_0^2 = -1 \in \sigma_L.$$

problema 2. Encuentra los primos inertes, ramificando y de scorr (pares)

$$\mathbb{Q}(\sqrt{55})/\mathbb{Q}$$

Demonstración: Si $p \nmid 55$

$\Rightarrow m(x) = x^2 - 55$ polinomio de Eisenstein

\Rightarrow El primo es ramificado.

los inertes: $\Leftrightarrow \left(\frac{p}{11} \right), \left(\frac{p}{5} \right) = -1$

$$\left(\frac{p}{11} \right) = \begin{cases} \left(\frac{1}{11} \right) = 1 & \left(\frac{5}{11} \right) = 1 & \left(\frac{9}{11} \right) = 1 \\ \left(\frac{2}{11} \right) = -1 & \left(\frac{6}{11} \right) = -1 & \left(\frac{10}{11} \right) = -1 \\ \left(\frac{3}{11} \right) = 1 & \left(\frac{7}{11} \right) = -1 & \\ \left(\frac{4}{11} \right) = 1 & \left(\frac{8}{11} \right) = -1 & \end{cases}$$

$$\left(\frac{p}{5} \right) = \begin{cases} \left(\frac{1}{5} \right) = 1 & \left(\frac{3}{5} \right) = -1 \\ \left(\frac{2}{5} \right) = -1 & \left(\frac{4}{5} \right) = 1 \end{cases}$$

$\therefore p \equiv 2, 3 \pmod{5} \text{ o } p \equiv 2, 6, 7, 8, 10 \pmod{11}$.

• El resto son descompuestos.

• Salvo si $p = 2$.

$$p \equiv 2, 6, 7, 8, 10 \pmod{11}$$

$$p \equiv 2, 3 \pmod{5}$$

$$\begin{array}{ll} x \equiv 0 \pmod{5} & 5k \equiv 1 \pmod{11} \\ x \equiv 1 \pmod{5} & k \equiv -2 \pmod{11} \end{array}$$

$$x \equiv -2 \pmod{55}$$

Luego $y^p = \alpha^p + \alpha^{-p}$, si $p \equiv \pm 1 \pmod{8}$.
 $= \alpha^{\pm 1} + \alpha^{\mp 1}$
 $= y \Rightarrow y \in \mathbb{F}_p$. (fijo por aut. de frobenius)

$$y^p = \alpha^p + \alpha^{-p}, \text{ si } p \equiv \pm 5 \pmod{8}$$
 $= \alpha^{\pm 5} + \alpha^{\mp 5}$
 $= -y \quad \therefore y \notin \mathbb{F}_p, \text{ pues si estuviera: } y^p = y.$

En el primer caso: $\left(\frac{2}{p}\right) = 1 = (-1)^{\frac{p^2-1}{8}}$

en el otro caso: $\left(\frac{2}{p}\right) = -1 = (-1)^{\frac{p^2-1}{8}}$

Ley de reciprocidad l.: l. p primos: $\left(\frac{l}{p}\right) = \left(\frac{p}{l}\right) (-1)^{\frac{p-1}{2} \cdot \frac{l-1}{2}}$.

Dem.: En $\overline{\mathbb{F}_p}$ tome w raiz l-ésima primitiva de la unidad.

$x \in \mathbb{F}_l$: w^x tiene toda su informacion.

Por suma de Gauss: $y = \sum_{u \in \mathbb{F}_l} \left(\frac{u}{l}\right) w^u \in \overline{\mathbb{F}_p}$.

Lema: $y^2 = (-1)^{\frac{l-1}{2}} l$.

Dem: $\left(\sum_{u \in \mathbb{F}_l} \left(\frac{u}{l}\right) w^u \right) \left(\sum_{s \in \mathbb{F}_l} \left(\frac{s}{l}\right) w^s \right) = \sum_{u \in \mathbb{F}_l} w^u \left(\sum_{t \in \mathbb{F}_l} \left(\frac{t(u-t)}{l}\right) \right)$

Pero: $\left(\frac{-1}{l}\right) \left(\frac{1-u t^{-1}}{l}\right) = (-1)^{\frac{l-1}{2}} \left(\frac{1-u t^{-1}}{l}\right)$

Asi: $y^2 = \sum_{u \in \mathbb{F}_l} w^u c_u, \quad c_u = (-1)^{\frac{l-1}{2}} \sum_{t \in \mathbb{F}_{l^2}} \left(\frac{1-u t^{-1}}{l}\right)$

Luego: $y^2 = (-1)^{\frac{l-1}{2}} \sum_{u \in \mathbb{F}_l} w^u c_u, \quad (u = \sum_{t \in \mathbb{F}_{l^2}} \left(\frac{1-u t^{-1}}{l}\right))$.

Pero: $c_0 = \sum_{t \in \mathbb{F}_{l^2}} \left(\frac{1}{l}\right) = l-1$ Junto al D como n. \square .

$n \neq 0$: $c_n = \sum_{t \in \mathbb{F}_{l^2} - \{1\}} \left(\frac{1-u t^{-1}}{l}\right) = \sum_{t \in \mathbb{F}_{l^2} - \{1\}} \left(\frac{t}{l}\right) = \sum_{t \in \mathbb{F}_{l^2} - \{1\}} \left(\frac{t}{l}\right) - 1 = -1$.

De esto: $y^2 = (-1)^{\frac{l-1}{2}} \left(l-1 - \sum_{u \in \mathbb{F}_l, u \neq 0} w^u c_u\right) = (-1)^{\frac{l-1}{2}} l$.

Pero $-1 - \sum_{u \in \mathbb{F}_l, u \neq 0} w^u c_u = \sum_{u \in \mathbb{F}_l, u \neq 0} w^u c_u$.

$$\underline{\text{Lema 2}} \quad . \quad y^{p-1} = \left(\frac{p}{\ell} \right)$$

$$\underline{\text{Demostación}} : \quad y^p = \sum_{n \in \mathbb{F}_\ell} \left(\frac{n}{\ell} \right)^p w^{np}$$

$$= \sum_{n \in \mathbb{F}_\ell} \left(\frac{n}{\ell} \right) w^{np} = \sum_{z \in \mathbb{F}_p} \left(\frac{p^{-1}z}{\ell} \right) w^z$$

$$= \left(\frac{p^{-1}}{\ell} \right) \sum_{z \in \mathbb{F}_p} \left(\frac{z}{\ell} \right) w^z = \left(\frac{p^{-1}}{\ell} \right) y$$

$$\therefore y^{p-1} = \left(\frac{p}{\ell} \right).$$

$$\text{Altavoz: } \left(\frac{(-1)^{\frac{p-1}{2}} \lambda}{p} \right) = \left(\frac{y^2}{p} \right) \quad [y^2 \in \mathbb{F}_p, y \text{ nos sabemos}]$$

$$= \left(y^2 \right)^{\frac{p-1}{2}} = y^{p-1} = \left(\frac{p}{\ell} \right)$$

$$\text{Por lo: } (-1)^{\frac{p-1}{2} \cdot \frac{p-1}{2}} = \left(\frac{(-1)^{\frac{p-1}{2}}}{p} \right) \left(\frac{\lambda}{p} \right) = \left(\frac{p}{\ell} \right).$$

$$\underline{\text{Volviendo}} \quad . \quad \text{Caro } K = p^f$$

$$S(x^u) = \sum_{x \in K} x^u \quad , \quad K \text{ cuerpo de carac. } p. \quad [p^f = 1]$$

Proposición :

$$S(x^u) = \begin{cases} -1 & , \text{ si } p^{f-1} \mid u \\ 0 & , \text{ si } p^{f-1} \nmid u \end{cases}$$

$$\underline{\text{Dem:}} \quad \text{Si } u = 0 : \quad S(x^0) = p^f = 0.$$

$$\text{Si } p^{f-1} \mid u \rightarrow u = r(p^{f-1}).$$

$$S(x^u) = \sum_{x \in K} x^{((p^{f-1})r)} = \sum_{x \in K} \underbrace{\left(x^{p^{f-1}} \right)^r}_{\text{Si } x \neq 0} = p^{f-1} = -1.$$

Si $p^{f-1} \nmid u$. (Ej.) $y \in K^*$: $y^{p-1} \neq 1$, ← y unperfección.

$$y^u \sum_{x \in K} x^u = \sum_{x \in K} (yx)^u = \sum_{x \in K} (x^u) \Rightarrow S(x^u) = 0.$$

$K(x_1, \dots, x_n) = \{ \text{polinomios en } n \text{ variables con coef. ent.}\}$

$$V(\{f_\alpha\}_\alpha) = \{v \in K^n \mid f_\alpha(v) = 0 \forall \alpha\}.$$

pol. $X_V = \prod_{\alpha} (1 - f_\alpha^{p^{t-1}}).$

$\forall v \in V \quad X_V(v) = \prod_{\alpha} (1 - f_\alpha^{p^{t-1}}) = 1.$

Sin d.v.: $\exists \alpha \text{ tal que } f_\alpha(v) \neq 0 \Rightarrow f_\alpha(v)^{p^{t-1}} = 1 \Rightarrow 1 - f_\alpha(v)^{p^{t-1}} = 0$
 $\therefore X_V(v) = 0.$

Asi. $S(\prod_{\alpha} (1 - f_\alpha^{p^{t-1}})) = \sum_{v \in V} X_V(v) = |V|.$

teorema: Si $\sum_i \deg f_i < n \Rightarrow |V| \leq O(p)$

Dem: Hay que demostrar que: $S(\prod_{\alpha} (1 - f_\alpha^{p^{t-1}})) \leq O(p).$

$$\deg \prod_{\alpha} (1 - f_\alpha^{p^{t-1}}) = \sum_{\alpha} \deg (1 - f_\alpha^{p^{t-1}}) = \sum_{\alpha} (p^t - 1) \deg f_\alpha < n(p^t - 1).$$

Pero $X_V = \sum_{v_1, \dots, v_n} \chi^{v_1} \cdots \chi^{v_n} \Rightarrow \sum_i v_i < n(p^t - 1).$

Asi. si $S(X_V) = \sum_{v_1, \dots, v_n} S(\underbrace{\chi^{v_1} \cdots \chi^{v_n}}_{\leq O(p)}) \leq O(p).$

En base p pura: $\exists r_i: v_i < p^t - 1. \quad \underline{\text{es q: }} \chi_i = \chi_1^r.$

$$\sum_{v \in V} \chi^{v_1} \cdots \chi^{v_n} = \left(\sum_{k \in K} \chi^k \right) \left(\sum_{v \in V} \chi^{v_2} \cdots \chi^{v_n} \right) = 0.$$

$$\therefore p \mid S(X_V) \Rightarrow |V| \leq O(p).$$

dej: $\sum_i \deg f_i < n.$ f no tiene término libre $\Rightarrow \{f_\alpha\}_{\alpha \in K^n}$ tienen ceros canón. (no trivial)

Por teo. previo: $|V| \leq O(p).$

$$\therefore V = \{0\} \Rightarrow (\text{pues } |V| \leq O(p)).$$

iii.- Observe que $A = \mathbb{Z}[i]$ es un dominio de integridad. Luego podemos ocupar el teorema chino de los restos sobre este anillo A .

En efecto, $(3i+1) = ((i+1)(i+2)) = (i+1)(i+2)$, donde $(i+2) - (i+1) = 1$. Por ello los ideales $(i+1)$ e $(i+2)$ son relativamente primos. Así:

$$\mathbb{Z}[i]/(3i+1) \cong \mathbb{Z}[i]/(i+1) \times \mathbb{Z}[i]/(i+2)$$

Sabemos que, por lo visto en [i] que:

$$\mathbb{Z}[i]/(i+2) \cong \mathbb{Z}/5\mathbb{Z},$$

De forma análoga se demuestra que [ejercicio]:

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

Finalmente:

$$\mathbb{Z}[i]/(3i+1) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/10\mathbb{Z}.$$

$$\begin{aligned} \underline{\mathbb{Z}[w]} &\cong \frac{\mathbb{Z}\left(\frac{1}{3}\right)}{(3w-1)} \\ &\cong \frac{\mathbb{Z}[x]}{(3x+1, x^2+1)} \cong \frac{\mathbb{Z}[-1]_3}{(10/9)} \cong \frac{\mathbb{Z}[-1]_3}{(10)} \cong \frac{\mathbb{Z}[x]}{(3x+1)} \cong \frac{\mathbb{F}_{10}[x]}{(3x+1)} \cong \frac{\mathbb{F}_{10}}{(x-3)}. \end{aligned}$$

$$1) \quad \frac{\mathbb{Z}[w]}{(3w-1)} \cong \frac{\mathbb{Z}[x]}{(3x+1, x^2+1)} \cong \frac{\mathbb{Z}[-1]_3}{(10/9)} \cong \frac{\mathbb{Z}[-1]_3}{(10)} \cong \frac{\mathbb{Z}[x]}{(3x+1)} \cong \frac{\mathbb{F}_{10}[x]}{(3x+1)} \cong \frac{\mathbb{F}_{10}}{(x-3)}.$$

$$2) \quad \frac{\mathbb{Z}[w]}{(3w-1)} \cong \frac{\mathbb{Z}[x]}{(3x+1, x^2+1)} \cong \frac{\mathbb{Z}[x]/(3x-1)}{(3x+1, x^2+1)/(3x-1)} \cong \frac{1}{9} + \frac{1}{3} + 1 = \frac{9+3+1}{9} = \frac{13}{9}.$$

$$\text{imp: } \frac{\mathbb{Z}[x]}{(ax-1)} \cong \mathbb{Z}\left(\frac{1}{a}\right) = S^{-1}\mathbb{Z}$$

$$\text{pd: } \underline{\mathbb{Z}\left(\frac{1}{3}\right)} \cong \frac{\mathbb{Z}[x]}{(3x-1)}$$

$$\text{Dem: } \text{Sea } \phi: \mathbb{Z}[x] \rightarrow \mathbb{Z}\left(\frac{1}{3}\right), \quad S = \{1, 3, 3^2, \dots\}$$

$$\phi(x) \mapsto \phi\left(\frac{1}{3}\right) = a_0 + a_1 \frac{1}{3} + \dots + a_n \frac{1}{3^n} = \frac{b}{3^n} \in S^{-1}\mathbb{Z}$$

$$\left(\frac{a}{b}\right)^n = \frac{a^n}{b^n}$$

$$\text{Claramente sobreyectiva } \frac{a}{3^n} = \phi(ax^n).$$

$$\text{observe que: } \phi\left(\frac{1}{3}\right) = 0. \quad 0 = 3^n a_0 + 3^{n-1} a_1 + \dots + a_n$$

$$\phi(x) = a_0 + a_1 x + \dots + a_{n-1} x^{n-1} - x^n (3^n a_0 + \dots + 3 a_{n-1})$$

=

$$(k - \frac{1}{3}) \mid \phi(x) \quad \text{ed:}$$

$\text{Si } \phi\left(\frac{1}{3}\right) = 0 \text{ entonces en } \mathbb{Z}[x]:$

$$\phi(x) = (k - \frac{1}{3})r(x), \quad r(x) \in \mathbb{Z}[x], \quad \text{por lema de Gauss}$$

$$r(x) = (3k-1) \bar{r}(x), \quad \bar{r}(x) \in \mathbb{Z}[x].$$

$$\text{Así } \text{Ker } (\phi) = (3x-1).$$

$$\begin{aligned} p &\mid x_1 - 2 \\ p^n &\mid \|x_1 - 2\| = \frac{1}{n} \end{aligned}$$

$$x_1 = \lim_{n \rightarrow \infty} x_n, \quad x_n \in \mathbb{Q}$$

$$p \nmid \|x_n - 2\|$$

$$p \nmid \|x_{t+1}\|$$

$$x_1^3 = 2 \text{ en } \mathbb{Q}$$

Teoría de Números.

$$\lim_{n \rightarrow \infty} x_n^3 = 2 \text{ en } \mathbb{Q}$$

Tarea 4

$x_n \in \mathbb{Z}_p$ para todos.

$$\frac{x-2}{q}$$

Fecha de entrega: Julio 3 de 2014

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

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

Sobre \mathbb{Q} : Sean $W \subseteq V$ espacios vectoriales de dimensión finita. Sea Λ un reticulado en V , y sea M un reticulado en W . Probar que $M_p \subseteq \Lambda_p$ para todo p salvo un número finito.

problema 1) Si p es un λ en $\mathbb{Q}(\sqrt[3]{2})$ y $p \mid \lambda$ $\Rightarrow p \mid \lambda$

Si λ se extiende a otras extensiones:

$$a + b\sqrt[3]{2} + c\sqrt[3]{4} \rightarrow a + b\sqrt[3]{2} + c\sqrt[3]{4}$$

$$\begin{array}{l} \text{ssi:} \\ \begin{array}{c} a_n \rightarrow a \\ b_n \rightarrow b \\ c_n \rightarrow c \end{array} \end{array}$$

∴ Esas

2) el 5-ádico: observe que $3^3 = 27 = 2$ en \mathbb{F}_5 ∴ 2 cubo en \mathbb{F}_5

Hasta normal. ∴ 2 es un cubo en \mathbb{Q}_5 . (o sea existe $a \in \mathbb{Q}: a^3 = 2$ en \mathbb{Q}_5).

$$\text{Entonces } \mathbb{Q}(\sqrt[3]{2}) \hookrightarrow \mathbb{Q}_5, \quad \mathbb{Q}(\sqrt[3]{2}) \xrightarrow{\exists \sqrt[3]{2} \rightarrow a} \mathbb{Q}_5, \quad \mathbb{Q}(\sqrt[3]{2}) \xrightarrow{\sqrt[3]{2} \rightarrow a} \mathbb{Q}_5$$

Dan 3 ext. del v.a. a L. (isomorfias)¹

3) Del 2-ádico: $K = \mathbb{Q}_2$, $f(x) = x^3 - 2$, $f'(x) = 3x$

$$\mathbb{Q}(\sqrt[3]{2}) \rightarrow \mathbb{Q}_2$$

Def: Ein \mathbb{K} -Modul ist ein \mathbb{V} -Vektorraum mit \mathbb{K} -Skalarmultiplikation.

$$\beta \in \Lambda \subseteq \alpha \in \mathcal{N}^n.$$

Enton cos es un reticulado.

fd: $\lambda \# N$ es ein set. env. ols: $N + 1$ es ein λ -env.

Dem: Se beweisen für: $\begin{cases} \mathbb{Z}^n \subseteq A \subseteq d\mathbb{Z} \\ \mathbb{Z}^n \subseteq B \subseteq d'\mathbb{Z}^n \end{cases}$, $d, d' \in \mathbb{N} - \{0\}$.

Seja: $\beta\beta' \in \mathbb{W}^*$ existem $\lambda, \mu \in \mathbb{K}$ s.t. $\lambda\beta + \mu\beta' \in \mathbb{W}$.
 $\therefore \text{nm } \beta \subseteq \mathbb{W}^n \rightarrow \text{nm } \beta' \subseteq \text{nm } \beta^n \subseteq \beta^n \subseteq \mathbb{W}^n$
 $\therefore \text{nm } \beta' \subseteq \mathbb{W}^n \rightarrow \text{nm } \beta' \subseteq \beta^n \subseteq \mathbb{W}^n$
analogamente: $\exists \lambda', \mu' \in \mathbb{K}$: $\lambda' \beta + \mu' \beta' \in \mathbb{W}$, n.m.e. $\lambda' = \lambda - \lambda$, $\mu' = \mu - \mu$.
 $\therefore \text{nm } \beta \subseteq \mathbb{W}^n \subseteq \text{nm } \beta'$ s.i. $\beta \in \text{nm } \beta'$ $\rightarrow \text{nm } \beta \subseteq \text{nm } \beta'$.
 $\therefore \text{nm } \beta \subseteq \mathbb{W}^n$ reticulado.

Função para visitar as classes: $(n+A) p = np$

$$p_0: \quad (\Pi + \Lambda)_P = \Pi_P + \Lambda_P.$$

$$\text{Denn: } (\pi + \lambda) \rho = \text{cls}(\pi + \lambda) = \text{cls}(\pi) + \text{cls}(\lambda) = \text{He} + \lambda\rho$$

(einfach)

$$\therefore M_1 \cup A_p = A_p, V \text{ exists w.r.t } p.$$

$$\therefore \mathcal{N}_p \subseteq \mathcal{N}_e \quad , \text{V rästitulo } p.$$

obviously: ΛM is a \mathbb{Z} -module of finite type

$$\therefore (\Lambda \cap \Pi)_P = \text{cls}(\Pi \cap \Lambda) = \text{cls} \cap \text{cls} \Lambda = \underline{\Lambda_P \cap \Pi_P} = \Pi_P, \forall \text{ visitado } P$$

$\therefore \pi_p \subseteq \Lambda_p$, & casito do p.

Teoría de Números.
Prueba 2

Junio 12 de 2012

Escoja 4 de los cinco problemas siguientes:

✓ 1. Demuestre que $(x^n, x - 1) = \mathbb{Z}[x]$ para todo entero n .✓ 2. Encuentre un entero n tal que

$$\mathbb{Z}[\sqrt[3]{3}] / (\sqrt[3]{9} - 2) \cong \mathbb{Z}/n\mathbb{Z}$$

✓ 3. Encuentre todos los primos en \mathbb{Z} que son primos en el anillo $\mathbb{Z}[\omega]$ donde $\omega = e^{2\pi i/3}$.✓ 4. Probar que el ideal $(2, 2\sqrt{D})$ no es principal en $\mathbb{Z}[2\sqrt{D}]$ para ningún entero D .✓ 5. Encuentre todos los pares de enteros positivos (n, p) , con p primo, tal que

$$\mathbb{Z}[\sqrt[3]{p}] / (\sqrt[3]{p^2} + \sqrt[3]{p} + 1) \cong \mathbb{Z}/n\mathbb{Z}$$

 $\zeta_3 = 0, \zeta_3, \dots, \zeta_{3m-1}$

$$(\mathbb{Z}[\zeta_3][x]) \rightarrow \mathbb{F}_p[x]$$

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

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

$$\mathbb{Z}(\sqrt[3]{p}) / (\sqrt[3]{p^2} + \sqrt[3]{p} + 1) \cong \frac{\mathbb{Z}(x)}{(x^3 - p, x^2 + x + 1)} \cong \frac{\mathbb{Z}(\omega)}{(x^3 - p)} \quad (3) = \frac{1 + \sqrt{-3}}{2}$$

$$\begin{array}{l} x^3 - p : x^2 + x + 1 = x - 1 \\ -x^3 - x^2 - x \\ \hline -x^2 - x - x \\ +x^2 + x + 1 \\ \hline 1 - p \end{array}$$

$$\cong \frac{\mathbb{Z}(x)}{(x^2 + x + 1, p-1)} \cong \frac{\mathbb{F}_{p-1}(x)}{(x^2 + x + 1)}$$

Si $x^2 + x + 1$ tiene raíz en \mathbb{F}_{p-1} :Si $\text{p-1} \equiv 0 \pmod{3}$: $\mathbb{F}_{p-1} \cong \mathbb{F}_{p-1}$) $y^3 + y + 1$ tiene raíz si :

$$A = \frac{\mathcal{U}(\sqrt[p]{\rho})}{(\sqrt[p]{\rho}, \sqrt[p]{\rho+1})} \cong \frac{\mathcal{U}(w)}{(p-1)}$$

$$\therefore \left| \frac{\mathcal{U}(w)}{(p-1)} \right| = (p-1)^2$$

$$\text{S. } \frac{\mathcal{U}(w)}{(p-1)} \cong \mathcal{U}/h\mathcal{U} \Rightarrow \frac{\mathcal{U}(w)}{(p-1)} \cong \mathcal{U}/(p-1)^2\mathcal{U}$$

$$\therefore p-1 = 0 \text{ en } \frac{\mathcal{U}(w)}{(p-1)}$$

$$\therefore p-1 = 0 \text{ en } \frac{\mathcal{U}(w)}{(p-1)^2}$$

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

$$\text{N) Así: } A = \frac{\mathcal{U}(w)}{(1)} \cong \{0\} \cong \mathcal{U}/1\mathcal{U} \quad \therefore h=1.$$

Problema 1. Demuestra que $(x^n, x^{-1}) = \mathbb{Z}(x)$, $\forall n \in \mathbb{N}$.

Demostación: Esto sucede si $\frac{\mathbb{Z}(x)}{(x^n, x^{-1})} \cong (\circ)$

Demo: 1) como sabemos $\frac{\mathbb{Z}(x)}{(x^n, x^{-1})} \cong \frac{\mathbb{Z}(x)/(x^{-1})}{(x^n)} \cong \frac{\mathbb{Z}}{(1)} \cong (\circ)$

$$\therefore (x^n, x^{-1}) = \mathbb{Z}(x).$$

Problema 2. Encuentre la orden de x en $\mathbb{Z}/\mathbb{Z}(x)$

$$\mathbb{Z}(\sqrt[5]{3}) / (\sqrt[5]{3}-2) \cong \mathbb{Z}/h\mathbb{Z}$$

$$q - 32 = -23$$

Demostación: Sabemos que:

$$\frac{\mathbb{Z}(\sqrt[5]{3})}{(\sqrt[5]{3}-2)} \cong \frac{\mathbb{Z}(x)}{(x^5-3, x^2-2)} \cong \frac{\mathbb{Z}(x)}{(4x-3, x^2-2)} \cong \frac{\mathbb{Z}\left[\frac{3}{4}\right]}{\left(\left(\frac{3}{4}\right)^2-2\right)} \cong \frac{\mathbb{Z}\left[\frac{3}{4}\right]}{\left(-\frac{23}{4^2}\right)}$$

$$\cong \frac{\mathbb{Z}\left[\frac{3}{4}\right]}{(2^3)} \cong \frac{\mathbb{Z}(x)}{(4x-3, 2^3)} \cong \frac{\mathbb{Z}(x)}{(4x-3)} \cong \mathbb{F}_{23}(x)$$

$$x^5-3 : x^2-2 \equiv x^3+2x$$

$$\begin{array}{r} x^7+2x^5 \\ -2x^5-3 \\ \hline 4x-3 \end{array}$$

$$\text{existe } 4^{-1} \text{ en } \mathbb{F}_{23} \text{ otro } \left\{ \begin{array}{l} \cong \mathbb{F}_{23}\left[\frac{3}{4}\right] \cong \mathbb{F}_{23}[3] \cong \frac{\mathbb{Z}}{23\mathbb{Z}}, h=23 \\ \text{pues } (23, 4)=1. \quad \left(\begin{array}{l} \cong \frac{\mathbb{F}_{23}(x)}{(4(x+5))} \cong \frac{\mathbb{F}_{23}(x)}{(x+5)} \cong \mathbb{F}_{23}. \\ \text{formula: } \frac{\mathbb{F}_{23}(x)}{(4(x+5))} \cong \frac{\mathbb{F}_{23}(x)}{(4x+20)} \cong \frac{\mathbb{F}_{23}(x)}{(4x)} \cong \mathbb{F}_{23}. \end{array} \right) \end{array} \right.$$

$$x^2-2 : 4x-3$$

Problema 3. Encuentre todos los primos en \mathbb{Z} que son primos en el anillo $\mathbb{Z}(w)$ donde $w = e^{2\pi i/3}$.

Sabemos que $p \in \mathbb{Z}$ primo en $\mathbb{Z}(w)$ si

$$\frac{\mathbb{Z}(w)}{(p)} \in D.I$$

$$\text{y es así: } \frac{\mathbb{Z}(w)}{(p)} \cong \frac{\mathbb{Z}(x)}{(x^n, x^{-1})} \cong \frac{\mathbb{F}_p(x)}{(x^n + x^{-1})} \text{ es } D.I \text{ si:}$$

$x^2 + x + 1$ no tiene raíces en \mathbb{F}_p
 si y solo si $D = b^2 - 4ac = -3$ no es divisible en \mathbb{F}_p

$$\text{Pues } \left(\frac{-3}{p} \right) = \left(-1 \right)^{\frac{p-1}{2}} \cdot \left(\frac{3}{p} \right)$$

$$= (-1)^{\frac{p-1}{2}} (-1)^{\frac{p-1}{2}} \cdot \left(\frac{p}{3} \right) = \left(\frac{p}{3} \right)$$

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

Si $p \equiv 2 \pmod{3}$: teniendo $x=1$.

∴ Es $\frac{\mathcal{L}(w)}{(p)}$ DI si $p \equiv 2 \pmod{3}$.

Problema 4. Probar que el ideal $(2, 2\sqrt{D})$ no es principal en $\mathcal{L}(2\sqrt{D}) \subseteq \mathcal{L}(\sqrt{D})$ para ningún entero D.

Demostración: $\mathcal{L}(2\sqrt{D}) = \{a + 2b\sqrt{D} / a, b \in \mathcal{L}\}$.

Supongamos que

A sí:

$$(v) = (2, 2\sqrt{D})$$

$$2 = v(a + 2b\sqrt{D}) \Rightarrow 2 = \bar{v}(a - 2b\sqrt{D})$$

$$2\sqrt{D} = v(c + 2d\sqrt{D}) \Rightarrow -2\sqrt{D} = \bar{v}(c - 2d\sqrt{D})$$

Luego:

$$4 = (v\bar{v})(a^2 - 4b^2D) \quad \text{y } v\bar{v} \in \mathcal{L}$$

$$-4D = (v\bar{v})(c^2 - 4d^2D)$$

$$\therefore v\bar{v} \in \{1, 2, 4\}$$

Si: $\bar{v}v = 1 \Rightarrow v \text{ inverso} \Rightarrow (2, 2\sqrt{D}) = R (\times) \text{ pero } 1 \notin (2, 2\sqrt{D})$

Si: $\bar{v}v = -1 \Rightarrow (-\bar{v})(v) = 1 \Rightarrow v \text{ inv. } (\times)$

Si: $\bar{v}v = 4 \Rightarrow -D = (c^2 - 4d^2D)$

$$1 = a^2 - 4b^2D$$

Problema 4.

D: $D=0$ $\mathbb{Z}(2\sqrt{D}) \cong \mathbb{Z}$ $\Rightarrow (2, 2\sqrt{D})$ es principal.

S: D es dividido $\mathbb{Z}(2\sqrt{D}) \cong \mathbb{Z}$ $\Rightarrow (2, 2\sqrt{D})$ es principal.

Si D es libre de cuadrados: $S: \eta = (2, 2\sqrt{D})$

$$\eta\bar{\eta} \in \{1, -4\}.$$

$$\text{a) } \eta\bar{\eta} = 0(4) \Rightarrow \eta\bar{\eta}\bar{\eta} \equiv 0(2)$$

Si $D = -1$,

$$\text{a) } \eta\bar{\eta} = 4 \Rightarrow \eta = 2+2i.$$

$$\therefore 2^2 = 2^{(1+i)}(c+2id) \Rightarrow c+2d=1 \not\in \mathbb{Z}.$$

$$\therefore \frac{1}{2} = \frac{(1+i)(c+2id)}{(1+i)(c+2id)} \Rightarrow c+2d=0$$

$$\text{b) } D = -4 \quad \eta\bar{\eta} = x^2 - 4Dy^2 \equiv 0(2) \Rightarrow x \text{ par.}$$

$$\therefore 2\sqrt{D} = (x+2iy)(c+2\sqrt{D}d) \Rightarrow 0 = \left(\frac{x}{2}\right)c + Ddy.$$

$$\Rightarrow \begin{cases} 0 = y'c + 2Ddy \\ 0 = y'c + 2x'd \end{cases} \Rightarrow y' \text{ c impares} \Rightarrow y \text{ c impares} \Rightarrow x \text{ par.}$$

$$1 = (x+2iy)(c+2\sqrt{D}d)$$

$$1 = x'a + 2yb$$

$$\therefore \begin{cases} 0 = y'a + 2by \\ 0 = x'a + 2yb \end{cases} \Rightarrow y \text{ par, pero } a \text{ no es par} \Rightarrow \begin{cases} x \text{ par} \\ y \text{ par} \end{cases} \Rightarrow \text{imposible}$$

\therefore no es DFP.

$$\mathbb{Z} \frac{(2\sqrt{D})}{(2, 2\sqrt{D})}$$

$$\frac{\mathcal{U}(x)}{(2x+2)} \underset{\approx}{=} \frac{\mathcal{U}(x)}{\left((1+i)^3\right)} \underset{\approx}{=} \frac{\mathcal{U}(x)}{(x^3+2x^2)}$$

$$\frac{\mathcal{U}(x)}{(2x+2)} \hookrightarrow \frac{\mathcal{U}(x)}{(x)} \times \frac{\mathcal{U}(x)}{(x+1)}$$

to solve can approximate thus $\frac{\mathcal{U}(x)}{(x+1)} \underset{\approx}{=} \frac{\mathcal{U}(1)}{e^x}$

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

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

$$\therefore \frac{\mathcal{U}(i)}{(2x+2)} \underset{\approx}{=} \frac{\mathcal{U}(i)/(4)}{(2x+2)/(4)} \underset{\approx}{=} \frac{\mathcal{U}(i)/(4)}{(1+i)^3/(4)}$$

$$\therefore \left| \frac{\mathcal{U}(i)}{(4)} \right| = (6 + (1+i)^3 + o(u)) \cdot 2(1+i)^2 \underset{\approx}{=} o(4)$$

$$\mathcal{U}(i) \in \mathcal{U} \oplus (1+i) \mathcal{U}$$

$$(a+ib) \mapsto (a-b) + b(1+i)$$

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

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

$$\begin{aligned} (1+i)^3 &= (2i)(1+i) = 2(-1+(1+i))(1+i) = -2(1+i) + 2(1+i)^2 \\ &= -2(1+i) + 4i = -2(1+i) + (4(-1+i)) \\ &= -4 + 2(1+i). \end{aligned}$$

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

$$\frac{\mathcal{U}(i)}{(1+i)^3} \underset{\approx}{=} \frac{\mathcal{U}(i)}{\langle (1+i)^3, (1+i)^4 \rangle_{\mathcal{U}}} \underset{\approx}{=} \frac{\mathcal{U}}{\langle (-4i), (-4, 0) \rangle_{\mathcal{U}}} \underset{\approx}{=} \frac{\mathcal{U}}{\langle (0, 1), (1, 0) \rangle_{\mathcal{U}}}$$

obs: $\left| \frac{\mathcal{U}(i)}{(a+ib)} \right| = N(a+ib)$,

$$\left| \frac{\mathcal{U}(i)}{(2+ib)} \right| = \left| \frac{\mathcal{U}(-i)}{(a-i)} \right| = \left| \frac{\mathcal{U}(i)}{(a-i)} \right|, \quad \left| \frac{\mathcal{U}(i)}{(n)} \right| = h^2$$

$$\Psi: \mathcal{U}(i) \rightarrow \frac{\mathcal{U}(i)}{(n)}, \quad \text{Im } \Psi = \overline{\langle (2+ib) \rangle} = \frac{(2+ib)}{(n)}.$$

$$\text{Ker } \Psi = \{ c(1+i) / ((1+di)(2+bi)) \mid c, d \in \mathbb{Z}, \text{ and } (1+di)(2+bi) \text{ is divisible by } n \}$$

Claudio Abraham Bravo Castillo
Lic. Matemáticas.

Teoría de Números.
Guía 4b. Localizaciones.

Mayo 15 de 2014

- A. Calcule la estructura de los siguientes anillos:

- (a) $\mathbb{Z}[\omega]/(3\omega - 1)$.
- (b) $\mathbb{Z}[i]/(5i + 2)$.
- (c) $\mathbb{Z}[\sqrt{2}]/(4\sqrt{2} + 1)$.
- (d) $\mathbb{Z}[\sqrt[3]{2}]/(7\sqrt[3]{2} + 1)$.
- (e) $\mathbb{Z}[\sqrt[3]{2}]/(\sqrt[3]{4} + 1)$.
- (f) $\mathbb{Z}[\sqrt[3]{2}]/(3\sqrt[3]{4} + 1)$.
- (g) $\mathbb{Z}[\eta]/(\eta^2 - 2)$, donde $\eta = e^{2\pi i/5}$.

$\textcircled{1}$ Probar que $\mathbb{Z}[i]/(4i + 2)$ no es isomorfo a ningún anillo de la forma $\mathbb{Z}/n\mathbb{Z}$.

$\textcircled{2}$ Encuentre todos los primos de \mathbb{Z} que son primos del anillo $\mathbb{Z}[\frac{1}{3i}]$.

$\textcircled{3}$ Sea $A = \mathbb{Z}[x, x^{-1}]$ el anillo de polinomios de Laurent, y sea $B = A/(x + 1 + x^{-1})$. Probar que B es un DFU.

$\textcircled{4}$ Sea $A = \mathbb{Z}[x, x^{-1}]$ como en el ejercicio anterior, y sea $B = A/(x - 2x^{-1})$. Probar que B es un DFU.

$\textcircled{5}$ Sea p un primo impar. Probar que si $\frac{a}{b} = 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{p-1}$, entonces p divide a a .

$\textcircled{6}$ Sea $f(x) = a_n x^n + \dots + a_1 x + a_0$ un polinomio con coeficientes enteros que tiene una raíz racional. Probar que su reducción módulo p tiene una raíz en $\mathbb{Z}/p\mathbb{Z}$ para todo primo p que no divide a a_n .

$$\begin{aligned} \mathbb{Z}[\sqrt[3]{2}] &\cong \frac{\mathbb{Z}(x)}{(3\sqrt[3]{4}+1)} \\ &\cong \frac{\mathbb{Z}(i)}{(3x^4+1)} \\ &\cong \frac{\mathbb{Z}(\sqrt{-3})}{(x^3-2, 3x^4+1)} \\ &\cong \frac{\mathbb{Z}(\sqrt{-3})}{((\sqrt{-3})^3)} \\ &\cong \frac{\mathbb{Z}(i/\sqrt{-3})}{(-i+2\sqrt{-3})} \end{aligned}$$

↓
teo. Clase de los restos

$$\frac{\mathbb{Z}(x)}{(x^3+1)} = \left(\frac{\mathbb{Z}}{3}\right)^3$$

$$\begin{aligned} \mathbb{Z}[\sqrt[3]{2}] &\cong \frac{\mathbb{Z}(x)}{(x^3-2)} \\ &\cong \frac{\mathbb{Z}(\sqrt{-3})}{(x^3-18)} \end{aligned}$$

↓
1. teo ordenado
y el anillo tiene
2º elemento

$$\frac{\mathbb{Z}(\sqrt[3]{2})}{(3\sqrt[3]{4}+1)} \cong \frac{\mathbb{Z}(\sqrt{-3}/3)}{(-\sqrt{-3}-18)}$$

$$\cong \frac{\mathbb{Z}(\sqrt{-3}/3)}{(-\sqrt{-3}-18)}$$

$$\cong \frac{\mathbb{Z}(x)}{(3x^3+1, -3x-18)}$$

Problema 4a.

$$s \in R^* \Rightarrow T^*R \cong (ST)^{-1}R$$

Sea $\Psi: (ST)^{-1}R \longrightarrow T^*R$.

$$\frac{a}{st} \mapsto \frac{as^{-1}}{t}$$

$$\Psi\left(\frac{a}{st}, \frac{a'}{s't'}\right) = \Psi\left(\frac{aa'}{sst'+tt'}\right) = \frac{aa(ss')^{-1}}{t+t'} = \Psi\left(\frac{a}{st}\right)\Psi\left(\frac{a'}{s't'}\right)$$

$$\Psi\left(\frac{a}{st}, \frac{a'}{s't'}\right) = \Psi\left(\frac{as't'+a'st}{sst'+tt'}\right) = \frac{(as't'+a'st)(ss')^{-1}}{(t+t')}$$

$$\Psi \text{ es biuniforme si: } \frac{a}{st} + \frac{a'}{s't'} = \Psi\left(\frac{a}{st}\right) + \Psi\left(\frac{a'}{s't'}\right)$$

$$\frac{a}{st} = \frac{a'}{s't'} \Rightarrow \exists s'' \in ST: (as't' - a'st) = 0 \quad / (ss')'$$

$$\text{Supo: } s''(as^{-1}t' - a'st^{-1}) = 0$$

$$\therefore \Psi\left(\frac{a}{st}\right) = \Psi\left(\frac{a'}{s't'}\right)$$

y es sobre pures para $\frac{a}{st} \in T^*R$ existe $s'' \in ST$ tal que $\Psi\left(\frac{as^{-1}}{t}\right) = \frac{s^{-1}s'a}{st} = \frac{a}{st}$.
 $\therefore T^*R \cong (ST)^{-1}R$.

Problema 4b. Demostre que $(ST)^{-1}R \cong (T/I)^{-1}(S^{-1}R)$

Sea: $\Psi: (ST)^{-1}R \longrightarrow (T/I)^{-1}(S^{-1}R)$

$$\frac{a}{st} \mapsto \frac{a/s}{t/I}$$

$$\Psi\left(\frac{a}{st}, \frac{a'}{s't'}\right) = \Psi\left(\frac{aa'}{sst'+tt'}\right) = \frac{aa'/ss'}{t/I \cdot t/I} = \frac{\frac{a}{s} \cdot \frac{a'}{s'}}{t/I \cdot t/I} = \frac{a/s \cdot a'/s'}{t/I} = \Psi\left(\frac{a}{st}\right)\Psi\left(\frac{a'}{s't'}\right)$$

$$\Psi\left(\frac{a}{st}, \frac{a'}{s't'}\right) = \Psi\left(\frac{as't'+a'st}{sst'+tt'}\right) = \frac{as't'+a'st/ss'}{t/I \cdot t/I} = \frac{\frac{a}{s} \cdot \frac{a'}{s'} + \frac{a}{s} \cdot \frac{a'}{s'}}{t/I \cdot t/I} = \Psi\left(\frac{a}{st}\right), \Psi\left(\frac{a'}{s't'}\right)$$

Claramente sobrejetiva, Ψ establece pures:

$$\frac{a}{st} = \frac{a'}{s't'} \text{ssi: } \exists s'' \in ST: s''(as't' - a'st) = 0 \text{ en } (I, T^*(S^{-1}R))$$

$$\frac{a/s}{t/I} = \frac{a'/s'}{t/I} \text{ssi: } \exists s'' \in ST: s''\left(\frac{a/t'}{s'} - \frac{a/t}{s}\right) = 0$$

$$\therefore \Psi\left(\frac{a}{st}\right) = \Psi\left(\frac{a'}{s't'}\right)$$

$\therefore \Psi$ biuniforme e inyectiva.

Álgebra I para el postgrado

Interrogación N° 2 Jueves 8 de Mayo, 2014

Se espera que explique su respuesta: motive su respuesta, mencione el teorema, proposición, lema, etc. que usted utiliza.

1. Sea X un conjunto no vacío y sea R el anillo de todas las funciones $f : X \rightarrow \mathbb{Z}$ bajo las operaciones $(f + g)(x) = f(x) + g(x)$ y $(fg)(x) = f(x)g(x)$. Para cada $a \in X$ define

$$M_a := \{f \in R \mid f(a) = 0\}$$

a) Demuestre: M_a es un ideal primo de R , pero M_a no es maximal

b) Encuentre todos las unidades y los divisores de cero en R

2. Sea D un dominio integral. Demuestre:

a) D es finito $\Rightarrow D$ es un cuerpo.

b) $D[x]$ es un dominio integral de ideales principales $\Rightarrow D$ es un cuerpo.

3. Sea $R = \mathbb{Z}[\sqrt{-13}] = \{a + b\sqrt{-13} \mid a, b \in \mathbb{Z}\}$, un subanillo de \mathbb{C} . Define

$$N(a + b\sqrt{-13}) := |a + b\sqrt{-13}|^2 = a^2 + 13b^2.$$

(Se puede asumir que $N : R \rightarrow \mathbb{N}$ es multiplicativo).

a) Demuestre: 2 es irreducible en R

b) Verifique si R es un dominio de factorización único DFU. Justifique bien su respuesta. (Indicación: considere $(1 + \sqrt{-13})^2$).

$$2(\sqrt{-13} + 6) = 2\sqrt{-13} + 12 = 1 + 2\sqrt{-13} - 13$$

4. Sean S y T subconjuntos multiplicativos de un anillo R comutativo. Considere los siguientes conjuntos multiplicativos:

$$ST := \{st \mid s \in S, t \in T\} \subset R,$$

$$R \longrightarrow S^{-1}R$$

$$T/1 := \{t/1 \mid t \in T\} \subset S^{-1}R$$

$$T/S := \{t/s \mid t \in T, s \in S\} \subset S^{-1}R$$

Demuestre:

$$S \subset R^\times \Rightarrow T^{-1}R \simeq (ST)^{-1}R$$

$$(ST)^{-1}R \simeq (T/1)^{-1}(S^{-1}R) \simeq (T/S)^{-1}(S^{-1}R)$$

$$\Psi: (S^{-1}R) \xrightarrow{\frac{a}{s}} (T/S)^{-1}(S^{-1}R)$$

$$\frac{a}{s} \mapsto \frac{a/s}{t/s}$$

$$\Psi: (S^{-1}R) \longrightarrow (T/S)^{-1}(S^{-1}R)$$

$$\frac{a}{s} \mapsto \frac{a/s}{t/s}$$

$\mathbb{P} \models f : Y \rightarrow \mathbb{Z}$ (f finito)

Problema: i) Mostrar que f es constante.

$$P/\mathbb{N}_0 \cong \mathbb{Z}$$

Prop: $\mathbb{P}, R \mapsto \mathbb{Z}$ es función de cuadros pues $\Psi(f(p)) = (p^2) = (\text{cuadrado})$
 $\Psi(f(q)) = ((q^2)) = (\text{cuadrado})$

Por tanto para $\forall n \in \mathbb{Z}$ existe f_0 tal que $(n^2) = f_0$ para $\mathbb{P} \models f_0 : \{x^2 = n^2\} = \mathbb{N}_0$

$\therefore \mathbb{P}/\mathbb{N}_0 \cong \mathbb{Z}$ DE \mathbb{P} es ideal primo pues $f = \{x^2 = n^2\} \in \mathbb{N}_0, n \in \mathbb{Z}$

(*) si no es maximal pues $\mathbb{N}_0 \subseteq \{f \mid f(a) = 0\} \cap \{f \mid f(b) = 0\} \neq \emptyset$ ($a^2 - b^2 = (a+b)(a-b) \in \mathbb{N}_0$)

b) Si f es un ideal de \mathbb{P} , $\mathbb{P}/f \cong \mathbb{Z}$.

$\therefore f = 1 \Rightarrow f(\mathbb{P}) = \mathbb{P} \times \mathbb{X}$ es f. es su complemento

$\therefore D^k = \{f \mid f = 1\}$ $\therefore f_p = \emptyset \Rightarrow (\text{es primo})$

\Rightarrow $\text{fondo de } f^{(k)} = \{f\}$ \Rightarrow $f^{(k)}$ es primo \Rightarrow $f = 1$

c) $\text{fondo de } f = \{f^{(k)} \mid k \in \mathbb{N}\} \cup \{f = 0\}$

Problema: a) Resolución $\mathbb{Z}[\sqrt{-13}] = \mathbb{Q}$

$\therefore \mathbb{Q} = \mathbb{Z}[\sqrt{-13}]$ (finito)

\therefore $\mathbb{Z}[\sqrt{-13}]$ es campo \Rightarrow $\mathbb{Z}[\sqrt{-13}] = \mathbb{Q}$ (por el teorema de la multiplicación)

Por tanto $\mathbb{Z}[\sqrt{-13}] = \mathbb{Q} = \mathbb{Z}[\sqrt{-13}] \cup \{0\} = \mathbb{Z}[\sqrt{-13}] \cup \{\mathbb{Q}\}$

\therefore $\mathbb{Z}[\sqrt{-13}]$ no es campo \Rightarrow $\mathbb{Z}[\sqrt{-13}] \neq \mathbb{Q}$

b) $R = \mathbb{C}[U]$ es campo \Rightarrow $\mathbb{C}[U] = \mathbb{C} \cup \{0\} = \mathbb{C}$

prop: $(1 + \sqrt{-13})^2 = 1 + 2\sqrt{-13} + (-13) = 2(-5 + 6) = 2$

$\therefore \mathbb{Z}[\sqrt{-13}]$ es simple $\therefore \mathbb{Z}[\sqrt{-13}] = \mathbb{Q} = \mathbb{Z}[\sqrt{-13}] \cup \{\mathbb{Q}\} = \mathbb{Z}[\sqrt{-13}] \cup \{0\}$

$\therefore \mathbb{Z}[\sqrt{-13}] \neq \mathbb{Q}$

$\therefore \mathbb{Z}[\sqrt{-13}] \neq \mathbb{C}$

$\therefore \mathbb{Z}[\sqrt{-13}] \neq \mathbb{R}$

g) $2\sqrt{-13} \in \mathbb{Z}[\sqrt{-13}]$ pues $\mathbb{P} = \mathbb{Z}[\sqrt{-13}]$ y $\mathbb{P} \models N(x) = Q^2 + 13B^2 = 1 + 2$

$\therefore 2 = \pm(1 + \sqrt{-13}) \in \mathbb{Z}[\sqrt{-13}] \Rightarrow \sqrt{-13} = \pm 1 + \sqrt{-13}$ \therefore $\sqrt{-13} \in \mathbb{Z}[\sqrt{-13}]$

$\therefore \mathbb{Z}[\sqrt{-13}] \neq \mathbb{R}$

h) Si $|A| = 1, \mathbb{N}_0 \subseteq \{f \in \mathbb{Z}[\sqrt{-13}] \mid f \neq 0\} \Rightarrow \{f \in \mathbb{Z}[\sqrt{-13}] \mid f \neq 0\} \subseteq \mathbb{Z}[\sqrt{-13}]$

Ejercicios Localización

Problema 1 Calcule la estructura de los siguientes cuotios.

$$(a) \frac{\mathcal{L}(w)}{(3w-1)} \cong \frac{\mathcal{L}(x)}{(x+1, 3x+1)} \cong \frac{\mathcal{L}\left[\frac{1}{3}\right]}{\left(\frac{1}{3} + 1, 3\left(\frac{1}{3}\right) + 1\right)} \cong \frac{\mathcal{L}\left[\frac{1}{3}\right]}{\left(\frac{4}{3}, 4\right)} \cong \frac{\mathcal{L}\left[\frac{1}{3}\right]}{(4)} \cong \frac{\mathcal{L}(x)}{(3x-1, 13)}$$

$$(b) e^{2w+3} \cong \frac{F_{13}(x)}{(3x-1)} \cong F_{13}\left[\frac{1}{3}\right] = F_{13}.$$

invertible

$$(c) \frac{\mathcal{L}(i)}{(5i+2)} \cong \frac{\mathcal{L}(x)}{(x+1, 5x+2)} \cong \frac{\mathcal{L}\left[\frac{2}{5}\right]}{\left(\frac{2}{5} + 1\right)} \cong \frac{\mathcal{L}\left[\frac{1}{5}\right]}{\left(2^9\right)} \cong \frac{\mathcal{L}(x)}{\left(2^9, 5x+2\right)} \cong \frac{F_{29}}{\left(5x+2\right)} \cong F_{29}\left[\frac{1}{5}\right]$$

inv.

$$(d) \frac{\mathcal{L}(\sqrt[3]{2})}{(2\sqrt[3]{2}+1)} \cong \frac{\mathcal{L}(x)}{(x^3-2, 7x+1)} \cong \frac{\mathcal{L}\left[\frac{-1}{7}\right]}{\left(\frac{1}{7} - 2\right)} \cong \frac{\mathcal{L}\left[-\frac{1}{7}\right]}{\left(-9^+\right)} \cong \frac{\mathcal{L}(x)}{\left(-9^+, 7x+1\right)} \cong \frac{F_{31}(x)}{972} \cong F_{31}\left[\frac{1}{7}\right]$$

inv.

$$(e) \frac{\mathcal{L}(\sqrt[3]{52})}{(\sqrt[3]{4^2}+1)} \cong \frac{\mathcal{L}(x)}{(x^2-1, x+1)} \cong \frac{\mathcal{L}(x)}{(x+2, x+1)} \cong \frac{\mathcal{L}(-2)}{(x^2+1)} \cong \mathcal{L}(ii).$$

$$(f) \frac{\mathcal{L}(\sqrt[3]{2})}{(3\sqrt[3]{4}+1)} \cong \frac{\mathcal{L}(x)}{(x^3-2, 3x^2+1)} \cong \frac{\mathcal{L}\left[\frac{\sqrt{-3}}{3}\right]}{\left(\frac{\sqrt{-3}}{3} - 2\right)} \cong \frac{\mathcal{L}\left(\frac{\sqrt{-3}}{3}\right)}{\left(\sqrt{-3} - 18\right)} \cong \frac{\mathcal{L}(x)}{\left(3x^2+1, 3x-18\right)}$$

$$\cong \frac{\mathcal{L}\left(\frac{1+i\sqrt{3}}{3}\right)}{\left(\frac{1+i\sqrt{3}}{3} + 1\right)} \cong \frac{\mathcal{L}\left(\frac{10}{3}\right)}{19+3} \cong \frac{\mathcal{L}}{973}\left[\frac{18}{3}\right] \cong \mathbb{Z}_{17, 3}\mathcal{L}$$

$$(g) \frac{\mathcal{L}(h)}{(h^2-2)} \cong \frac{\mathcal{L}(x)}{(x^4+x^3+x^2+1, x^2-1)} \cong \frac{\mathcal{L}(x)}{(x+1, x^2-1)} \cong \frac{\mathcal{L}(-1)}{(x^2-1)} \cong \frac{\mathcal{L}\left(-\frac{1}{2}\right)}{\left(\frac{1}{4}-2\right)} \cong \frac{\mathcal{L}\left(-\frac{1}{2}\right)}{\left(3\right)} \cong \frac{\mathcal{L}}{312}\left[-\frac{1}{2}\right]$$

inv.

$$h = e^{2w+3}$$

Problema 2. Probar que $\mathcal{L}(i)/(\mathcal{L}(i+2))$ no es isomorfo a ningun cuotio debiendo de la forma $\mathcal{L}/n\mathcal{L}$.

$$\frac{\mathcal{L}(i)}{(\mathcal{L}(i+2))} \cong \frac{\mathcal{L}(x)}{(x^2+4x+2)} \cong \frac{\mathcal{L}\left[-\frac{1}{2}\right]}{\left(\frac{1}{4}+1\right)} \cong \frac{\mathcal{L}\left(-\frac{1}{2}\right)}{\left(5\right)} \cong \frac{\mathcal{L}}{5}\left[-\frac{1}{2}\right] \cong \frac{\mathcal{L}}{5}\mathcal{L}(?)$$

inv.

$$\frac{\mathcal{L}(i)}{(\mathcal{L}(i+2))} \cong \frac{\mathcal{L}(x)}{(x^2+4x+2)} \cong \frac{\mathcal{L}(x)}{(x^2+4x+2)}$$

no es irreducible.

$$\frac{\mathcal{L}(x)}{(3, x-6)} \cong F_3.$$

Problema 3. Encuentre todos los primos de \mathbb{Z} primo pares $\mathcal{U}\left(\frac{1}{3}\right) = \mathcal{U}\left(\frac{1}{3}\right) = \mathcal{U}\left(\frac{1}{3}\right)$

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

$$\frac{\mathcal{U}\left(\frac{1}{3}\right)}{(p)} \cong \frac{\mathcal{U}\left(\frac{1}{3}\right)}{p\mathcal{U}} \cong \frac{\mathcal{U}(p\mathcal{U})}{(q^k+1)} \quad \text{Dado que } q^k+1 \text{ es primo} \\ \text{y } q=3 \Rightarrow q^k+1 \text{ es primo}$$

$$\begin{array}{l} \frac{1}{3} = x \\ 1 = qx \\ 1 - qx \end{array} \quad \text{por lo tanto} \quad \mathcal{U}\left(\frac{1}{3}\right) \cong \frac{\mathcal{U}\left(\frac{1}{3}\right)}{(p)} \quad \text{Si } p+3 \Rightarrow 3 \text{ invertible en } \mathbb{F}_p$$

$$q^k+1 \in \mathcal{O}(p) \quad \cong \frac{\mathcal{U}}{p\mathcal{U}}(1) \text{ ya que } D(p) = 3(4)$$

$$x^2 \in -q^{-1}(p) \quad \text{Si } p=3 \quad \mathcal{U}\left(\frac{-1}{3}\right) \text{ se reduce a } A = \left\{1, \frac{1}{2}\right\} \quad \frac{1}{2} = \frac{3}{1} \text{ en } \mathbb{Z}_2$$

$$\mathcal{U}\left(\frac{-1}{3}\right) \cong A^{-1}\left(\frac{1}{3}\right) \cong \left\{0\right\} \text{ de}$$

\therefore Primos $p \neq 3 \in D(p) = \{p+3\}$

o si $p = 3(4)$

Problema 4. $A = \mathcal{U}(x, x^{-1})$ (Anillo de polinomios de Laurent), $B = A/(x+x^{-1})$ $\text{pd: } B \in \text{DFU}$

$$\underline{\text{Dem:}} \quad B = \frac{\mathcal{U}(x, x^{-1})}{(x+x^{-1})} \cong \frac{\mathcal{U}(x, x^{-1})}{(x^2+1)} \cong \frac{\mathcal{U}(x(x^{-1}))}{(x^2+1)} \cong \frac{\mathcal{U}(w, w^{-1})}{(w^2+1)} = \mathcal{U}(w, w^{-1}) \cong \mathcal{U}(w) \in \text{DFU}$$

$$\text{y } x \in \text{DFU}, \quad A = \{x\} \quad \cong \bar{A} = \frac{\mathcal{U}(w)}{(w^2+1)} = \bar{A}^{-1}\mathcal{U}(w) \cong \mathcal{U}(w).$$

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

Problema 5. $A = \mathcal{U}(x, x^{-1})$ y sea $B = A/(x-2x^{-1})$ - Demuestre que $B \in \text{DFU}$

$$\underline{\text{Dem:}} \quad B \cong \frac{\mathcal{U}(x, x^{-1})}{(x^2-2)} \cong \frac{\mathcal{U}(x, x^{-1})}{(x^2-2)} \cong \frac{\mathcal{U}(\sqrt{2}, (\sqrt{2})^{-1})}{(x^2-2)} = \bar{A}^{-1}\mathcal{U}(\sqrt{2}) \cong \mathcal{U}(\sqrt{2}) \in \text{DFU}$$

$$\text{y } x \in \text{DFU}, \quad \frac{1}{\sqrt{2}} = \frac{\sqrt{2}}{2} \quad A = \{1, \sqrt{2}, \dots\} \quad \bar{A} = \{1, \sqrt{2}, \dots\}$$

Problema 6. Sea p un primo impar. Probar que $\frac{2}{p} = 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{p-1}$ enteros planos

$$\underline{\text{Dem:}} \quad \frac{2}{p} = \frac{(p-1)! + (p-1)!}{(p-1)!} = \frac{(p-1)! + (p-1)!}{(p-1)!}$$

$$\alpha(p-1) = b \left(\sum_{i=1}^{p-1} \frac{(p-1)!}{i} \right)$$

$$\text{Pero: } f(x) = (x-1) \dots (x-p+1) \in \mathbb{F}_p[x] \quad \therefore x^{p-1} - S_1 x^{p-2} + S_{p-1} x^{p-3} = 0 \quad \text{es decir } x^{p-1} - S_1 x^{p-2} + S_{p-1} x^{p-3} = 0 \quad \text{en } \mathbb{F}_p[x]$$

$$\text{módulo } p^2: \quad S_{p-1} = O(p^2) \quad S_{p-1} = O(p^2) \quad \sum_{i=1}^{p-1} \frac{(p-1)!}{i} \equiv p^2 \mid \alpha(p-1) \Rightarrow p^2 \mid \alpha \Rightarrow p \mid \alpha$$

Localización

Problema 1

$$\text{S}^{-1}A \text{ es un anillo con } \frac{a}{s}, \frac{a'}{s'} = \frac{aa'}{ss'}, \quad \frac{a}{s}, \frac{a'}{s'} = \frac{as' + a's}{ss'}$$

pd: $S^{-1}A \leq \text{Ufot}(A)$.

Dem: Primero lo haremos depende del representante, luego por la multiplicación:

$$\text{Si } \frac{a}{s} = \frac{b}{t} \Rightarrow \exists a'' \in S : a''(ta - sb) = 0 \quad (bsa - asb) = 0.$$

$$\text{observe que: } 1_{S^{-1}A} = \frac{s}{s} \text{ pues } \frac{s}{s} \cdot \frac{s}{s} = \frac{s}{s} \text{ y para: } (bsa - asb) = 0.$$

$$\text{Así: } \frac{a}{s} \cdot \frac{a'}{s'} = \frac{b}{t} \cdot \frac{a'}{s'} \text{ pues: } a''(aa'(s' - ba's)) = a''(ta - sb)a's' = 0.$$

$$i) \quad \frac{a}{s} + \frac{a'}{s'} = \frac{as' + sa'}{ss'} = \frac{b}{t} + \frac{a'}{s'} = \frac{bs' + ta'}{ts'} \text{ pues:}$$

$$a''(ts'(as' + sa') - ss'(bs' + ta')) = a''(ta(s')^2 + ts'sa' - sb(s')^2 - ts'a's) \\ = a''(ta - sb)(s')^2 = 0.$$

$$ii) \text{ Claramente: } \frac{a}{s} \cdot \frac{a'}{s'} = \frac{aa'}{ss'} \in A \in S^{-1}A.$$

$$\frac{a}{s} + \frac{a'}{s'} = \frac{as' + a's}{ss'} \in A \in S^{-1}A.$$

solución 2: $\Psi: A \rightarrow S^{-1}A$ es biomo. natural.

$$a \mapsto \frac{sa}{s} = a.$$

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

$$\Psi(ab) = \frac{sa'b}{s} = \frac{s^2ab}{s^2} = \frac{sa}{s} \cdot \frac{sb}{s} = \Psi(a) \cdot \Psi(b).$$

$$\text{Ker } \Psi = \left\{ a \mid \frac{sa}{s} = 0 \right\} = \left\{ a \in A \mid s''a = 0 \right\}. \quad (\text{S no contiene divisor})$$

Cero $\Rightarrow \Psi$ inyectiva.

$$s''(sa - 0) = 0 \rightarrow s''s^2a = 0$$

$$pd: S^{-1}A \cong \mathbb{U} \times \mathbb{U}$$

$$A = \mathbb{Z} \times \mathbb{Z} \quad S = \{ (c, d) \mid c, d \neq 0 \} \quad (\text{Vale para Adm. Int. } S = A - \{(0, 0)\})$$

$$\text{Dem: Sea: } \Psi: S^{-1}A \rightarrow \mathbb{U} \times \mathbb{U} \quad \begin{cases} \frac{(a, b)}{(c, d)} \mapsto \left(\frac{a}{c}, \frac{b}{d} \right) \end{cases}$$

$$S^{-1}A \cong \text{Ufot}(A) \times \text{Ufot}(A)$$

$$\text{Demi: Si } \frac{(a, b)}{(c, d)} = \frac{(a', b')}{(c', d')}$$

$$\text{entonces: } (x/y) \left[(a, b) \cdot (c', d') - (a', b') \cdot (c, d) \right] = (0, 0)$$

$$\text{haciendo } (x(a' - a'c), y(bd' - b'd)) = (0, 0)$$

$$\text{es decir } \begin{cases} a'c' - a'c = 0 \\ bd' - b'd = 0 \end{cases} \Rightarrow \begin{cases} \frac{a'}{c'} = \frac{a}{c} \\ \frac{b'}{d'} = \frac{b}{d} \end{cases}$$

\therefore Φ es biyectiva.

$$\text{Por tanto } (\frac{a}{b}, \frac{c}{d}) \in \mathbb{Q} \times \mathbb{Q} \Rightarrow (a, b), (c, d) \in \mathcal{V} \left(\frac{(a, b)}{(c, d)} \right) = \mathcal{V} \left(\frac{(a', b')}{(c', d')} \right).$$

$\Rightarrow \Phi$ es homomorfismo:

$$\Phi \left(\frac{(a, b)}{(c, d)} \cdot \frac{(a', b')}{(c', d')} \right) = \Phi \left(\frac{(a, b)(a', b')}{(c, d)(c', d')} \right) = \left(\frac{aa'}{cc'}, \frac{bb'}{dd'} \right) = \Phi \left(\frac{(a, b)}{(c, d)} \right) \cdot \Phi \left(\frac{(a', b')}{(c', d')} \right)$$

$$\Phi \left(\frac{(a, b)}{(c, d)} + \frac{(a', b')}{(c', d')} \right) = \Phi \left(\frac{(ac' + a'c, bd' + b'd)}{(cc', dd')} \right) = \left(\frac{ac' + a'c}{cc'}, \frac{bd' + b'd}{dd'} \right) = \Phi \left(\frac{(a, b)}{(c, d)} \right) + \Phi \left(\frac{(a', b')}{(c', d')} \right)$$

$\therefore S^{-1}\Lambda \cong \mathbb{Q} \times \mathbb{Q}$.

$$\text{Profil: } \overline{S}^{-1}(\Lambda|_T) \cong S^{-1}\Lambda / S^1\mathbb{L}.$$

$$\text{Ejemplo: } \Lambda = \mathbb{Z}[\frac{1}{i}], S = \{1, i, -1, -i\}, \Lambda = S^{-1}\mathbb{Z}, \overline{S} = \overline{\{1, i, -1, -i\}} = \overline{\{1, \sqrt{-3}, -1, -\sqrt{-3}\}} = \mathbb{Z}/3\mathbb{Z}.$$

$$\Lambda/\mathbb{Z} \cong \frac{S^{-1}\mathbb{Z}}{S^{-1}\mathbb{Z}} \cong \overline{S}^{-1}(\mathbb{Z}/\mathbb{Z}) \cong \{ \frac{0}{1}, \frac{1}{1}, \frac{2}{1} \} \cong \mathbb{Z}/3\mathbb{Z}.$$

$$\overline{S}^{-1}(\mathbb{Z}/\mathbb{Z}) = \overline{S}^{-1}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}) \cong \underbrace{\overline{S}^{-1}(\mathbb{Z}/2\mathbb{Z})}_{\text{separados}}, \underbrace{\overline{S}^{-1}(\mathbb{Z}/3\mathbb{Z})}_{\text{invertibles}} \cong \mathbb{Z}/3\mathbb{Z}$$

$$\text{Problema: } f(x) = a_n x^n + \dots + a_0, \text{ con } a_n \neq 0, \text{ tal que}$$

$$\text{Sea } p \text{ primo, } p \nmid a_n, \text{ en } \mathbb{Z}/p\mathbb{Z}: \Rightarrow p \nmid S \Rightarrow \exists S^{-1} \text{ en } \mathbb{Z}/p\mathbb{Z} \subset S^{-1}\Lambda \subset \mathbb{Z}/p\mathbb{Z}$$

$$f(x) = \bar{a}_n x^n + \dots + \bar{a}_0$$

$$\text{y } f(S^{-1}) = \bar{a}_n (S^{-1})^n + \dots + \bar{a}_0 = \bar{0}. \quad (\text{localizando})$$