BENEMÉRITA UNIVERSIDAD AUTÓNOMA DE PUEBLA

Facultad de Ciencias Físico Matemáticas

Postgrado en Ciencias Matemáticas

FUNCIONES ZETA LOCALES DE IGUSA VÍA LA FÓRMULA DE LA FASE ESTACIONARIA

TESIS

Que como parte de los requisitos para obtener el grado de

Maestro en Ciencias (Matemáticas)

Presenta:

Victor Antonio Aguilar Arteaga

Dirigido por:

Dr. Wilson Alvaro Zúñiga Galindo
Investigador Titular 3C
Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional

Dr. David Villa Hernández
Benemérita Universidad Autónoma de Puebla.

Puebla, Puebla. Julio de 2014.

Voy por el sueño de muchos...

AGRADECIMIENTOS

Quiero agradecer principalmente a mis padres Servando y Laura, por que sin su apoyo este trabajo no hubiera sido posible. Así como a mis hermanos Daniel y Lucero que también estuvieron conmigo en todo momento.

Agradezco:

Al Dr. Gilberto Reynoso Meza pues gracias a su ejemplo y consejos pude avanzar satisfactoriamente en mis estudios de maestría.

Al M.C. Roberto Torres Hernández pues me encamino en los estudios de postgrado y más que un profesor es un amigo.

Al Dr. Raúl Escobedo por su apoyo y amabilidad en mis días en Puebla.

Al Dr. Wilson A. Zuñiga Galindo por haberme aceptado como su estudiante, sugerir el tema de la presente tesis y darme confianza para trabajar con él.

Al Dr. David Villa Hernández por apoyarme durante todo el desarrollo de esta tesis, por sus enseñanzas, consejos y amistad.

Al Dr. Carlos Alberto López Andrade, Dr. Carlos Guillén Galvan, Dr. Iván Martínez Ruiz, Dr. Arnoldo Bezanilla López, Dr. Juan Alberto Escamilla Reyna y Dr. Edwin León Cardenal por sus valiosas observaciones que contribuyeron a mejorar este trabajo.

A todos mis amigos de la maestría que hicieron que estos años fueran bastante agradables. Con especial mención a: Vianney, Anabel, Neyfis, Aurelia, Giovanna, José Juan, Sergio, René, Ricardo y Eduardo.

A mis amigos de la UAQ: Iván, Jorge, Ely, Toñito, Esmeralda etc.; por su constante apoyo y amistad.

A mis amigos del CINVESTAV: Alexandra, Miriam y Anselmo; por su apoyo y ayuda en la realización de este trabajo.

Finalmente, agradezco al Consejo Nacional de Ciencia y Tecnología, CONACYT, por la beca con que me apoyaron durante mis estudios de Maestría.

INTRODUCCIÓN

El campo de los números $p-$ádicos, donde p es un número primo fijo, extiende la aritmética de los números racionales de una manera diferente a como lo hacen los números reales y los números complejos. Esta extensión se obtiene de una interpretación diferente del concepto de valor absoluto. De manera intuitiva, dos números enteros están $p-$ádicamente cerca si su diferencia es divisible por una potencia alta de p, cuánto más grande es la potencia más cerca están los números.
Kurt Hensel descubrió los números $p-$ádicos alrededor de finales del siglo diecinueve, estos números han aparecido en diferentes áreas de la matemática como son: teoría de números, geometría algebraica, topología algebraica, análisis, etc. Recientemente han surgido modelos nuevos de sistemas físicos usando números $p-$ádicos. Ver por ejemplo [5],[4],[22] y [23].
Las funciones zeta locales son funciones relativamente nuevas en matemáticas, en su estudio se mezclan ideas de varias teorías matemáticas, como son la geometría algebraica, la teoría de los números, la teoría de las singularidades y la lógica. Además, existe una gran cantidad de conjeturas que relacionan propiedades de las funciones zeta locales con conceptos y objetos de estas teorías.
Las funciones zeta locales se definen mediante integrales asociadas a polinomios con coeficientes en cuerpos locales no arquimedianos. Estos cuerpos son de dos tipos:

- cuerpos $p-$ádicos $K/\mathbb{Q}_p$, donde $\mathbb{Q}_p$ es el cuerpo de los números $p-$ádicos y K es una extensión finita $\mathbb{Q}_p$; y
- cuerpos $K/k((T))$, donde $k((T))$ es el cuerpo de las series meromorfas formales sobre un cuerpo finito k y K es una extensión finita de $k((T))$.

Estas funciones zeta fueron introducidas por André Weil en los años cincuenta, sus propiedades básicas fueron estudiadas sistemáticamente por Jun-Ichi Igusa en los años setenta. Desde entonces, especialmente durante los últimos 25 años se han obtenido resultados importantes.
Sobre el tema se puede consultar [15] y [13], que son los libros escritos por Igusa.
Sea $g(x) \in \mathbb{Q}_p[x_1, ..., x_n]$ un polinomio no constante, la potencia $p-$ádica compleja $|g|_K^s$ asociada a g (también llamada la función zeta local de Igusa de g) es la distribución

$$(|g|_K^s, \Phi) = \int_{\mathbb{Q}_p^n \setminus g^{-1}(0)} \Phi(x)|g(x)|_p^s |dx|, \ Re(s) > 0,$$

donde $|dx|$ denota una medida de Haar de $\mathbb{Q}_p^n$ normalizada por la condición $Vol(\mathbb{Z}_p^n) = 1$, y $\Phi : \mathbb{Q}_p \to \mathbb{C}$ es una función localmente constante y de soporte compacto.

El teorema básico, debido a Igusa, de la teoría de funciones zeta locales afirma la existencia de un conjunto finito de números racionales positivos $\{\frac{v_i}{N_i} : i \in T\}$ tal que

$$\Pi_{i\in T}(1 - p^{-N_{is-v_i}})\langle |g|_p^s, \Phi\rangle$$

es una función polinomial de p^{-s} para cualquier $\Phi \in S(\mathbb{Q}_p^n)$.
La conexión entre las funciones zeta locales y la teoría de los números es la siguiente. Supongamos que $g(x) \in \mathbb{Z}[x_1, ..., x_n]$ (o más generalmente en $\mathbb{Z}_p[x_1, ..., x_n]$), definimos

$$N_m = \#\{x \in (\mathbb{Z}_p/p\mathbb{Z}_p)^n : g(x) \equiv 0 \; mod \; p^m\}, \quad m \geq 1.$$

Un problema básico en teoría de los números es el estudio del comportamiento de los números N_m cuando m tiende a infinito. Para estudiar este problema se introduce la siguiente serie de Poincaré:

$$P(t, g) := P(t) = \sum_{m=0}^{\infty} N_m p^{-nm} t^m,$$

con $N_0 = 1$.
Una conjetura de Borevich-Shafarevich propuesta en los años sesenta afirma que $P(t)$ es una función racional de t. Definamos ahora

$$Z(s, g) = Z(s) = \int_{\mathbb{Q}_p^n \setminus g^{-1}(0)} \Phi(x)|g(x)|_p^s |dx|,$$

donde $Re(s) > 0$. Entonces, se puede probar que

$$P(t) = \frac{1 - tZ(s)}{1 - t}, \quad t = p^{-s}.$$

Por el resultado de Igusa antes mencionado $Z(s)$ es una función racional de p^{-s}, luego $P(t)$ es una función racional.

Vale la pena mencionar que la racionalidad de las funciones zeta locales de Igusa sobre campos de caracteristica positiva es un problema abierto.
Esta tesis está dedicada al estudio de los aspectos básicos de las funciones zeta locales de Igusa sobre $\mathbb{Q}_p$ vía la fórmula de la fase estacionaria introducida por Igusa en [14]. El punto central de la tesis es el estudio de las funciones zeta locales asociadas a polinomios semicuasihomogéneos, estos resultados fueron probados por Zuñiga-Galindo en [24].
La tesis está organizada de la siguiente forma. En el capítulo 1 se revisan los aspectos básicos del análisis $p-$ádico. Este capítulo está basado en las referencias [18],[16] y [23]. En el capítulo 2 se introducen las funciones zeta locales de Igusa y la fórmula de la fase estacionaria. Usando la fórmula de la fase estacionaria se calculan las funciones zeta locales asociadas a varios polinomios. Esta capítulo está basado en las referencias [27],[14],[15] y [1]. En el capítulo 3 se estudian las funciones zeta locales asociadas a

polinomios semicuasihomogéneos usando la fórmula de la fase estacionaria y algunas ideas sobre la $p-$desingularización de Nerón. Este capítulo está basado en la referencia [24].

ÍNDICE GENERAL

Dedicatoria I

Agradecimientos III

Introducción V

Índice general IX

1. Aspectos básicos del análisis p-ádico 1
1.1. Valores absolutos sobre campos 1
1.1.1. Definiciones básicas 1
1.1.2. Propiedades 5
1.1.3. Métrica inducida por un valor absoluto 8
1.2. Números p-ádicos 11
1.2.1. Valores Absolutos sobre $\mathbb{Q}$ 11
1.2.2. Completaciones 17
1.2.3. El campo $\mathbb{Q}_p$ 27
1.2.4. Lema de Hensel 38
1.2.5. Integración en $\mathbb{Q}_p$ 41
1.2.6. El caso n dimensional 47

2. Fórmula de la Fase Estacionaria 49
2.1. Funciones localmente constantes 49
2.2. Funciones zeta locales de Igusa 51
2.3. Fórmula de la fase estacionaria 57

3. Polinomios semicuasihomogéneos 73
3.1. Preliminares 73
3.2. Polinomios semicuasihomogéneos 76
3.3. Racionalidad de la función zeta local de Igusa asociada a un polinomio semicuasihomogéneo 81

4. Conclusiones 87

Bibliografía 89

I. ASPECTOS BÁSICOS DEL ANÁLISIS P-ÁDICO

En este capítulo se presentan los fundamentos del análisis p-ádico necesarios para el desarrollo de esta tesis.

I.1. Valores absolutos sobre campos

Aquí se presentan algunos hechos básicos de los valores absolutos sobre campos, para más detalles se puede consultar [16], [18].

I.1.1 Definiciones básicas

Definición 1.1 *Sea $\mathbb{k}$ un campo y $\mathbb{R}^+ = \{x \in \mathbb{R} : x \geq 0\}$ el conjunto de los números reales no negativos. Un **valor absoluto** sobre $\mathbb{k}$ es una función*

$$|\cdot| : \mathbb{k} \longrightarrow \mathbb{R}^+$$

que satisface las siguientes condiciones:

$i)$ $|x| = 0$ *si y sólo si* $x = 0$.

$ii)$ $|xy| = |x||y|$ *para todo* $x, y \in \mathbb{k}$.

$iii)$ $|x + y| \leq |x| + |y|$ *para todo* $x, y \in \mathbb{k}$.

Definición 1.2 *Un valor abosluto sobre un campo $\mathbb{k}$ es llamado **no arquimediano** si satisface además*

$$|x + y| \leq \text{máx}\ \{|x|, |y|\}$$

*para todo $x, y \in \mathbb{k}$. En otro caso se dice que el valor absoluto es **arquimediano**.*

Observación La condición $|x + y| \leq$ máx $\{|x|, |y|\}$ implica la condición $iii)$ de la definición de valor absoluto porque máx $\{|x|, |y|\} \leq |x| + |y|$.

Ejemplo 1.1 *Sea $\mathbb{k} = \mathbb{Q}$, se define un valor absoluto sobre $\mathbb{k}$ como:*

$$|x| = \begin{cases} x & \text{si } x \geq 0. \\ -x & \text{si } x < 0. \end{cases}$$

*Este valor absoluto se conoce como **valor absoluto usual**, en esta tesis se denotará por $|\cdot|_\infty$ y es arquimediano, pues si $x = y = 1$ se tiene*

$$|x + y| = 2 > \text{máx}\{|x|, |y|\} = 1.$$

Ejemplo 1.2 *Sea $\Bbbk$ un campo, se define un valor absoluto sobre $\Bbbk$ como:*

$$|x| = \begin{cases} 0 & \textit{si } x = 0. \\ 1 & \textit{si } x \neq 0. \end{cases}$$

*Este valor absoluto se conoce como **valor absoluto trivial**.*

Proposición 1.1 *Si $\Bbbk$ es un campo de orden finito entonces el único valor absoluto que se puede definir sobre $\Bbbk$ es el trivial.*

Demostración Sea $|\cdot| : \Bbbk \longrightarrow \mathbb{R}^+$ un valor absoluto sobre $\Bbbk$. Para 0 se tiene que $|0| = 0$ por la definición de valor absoluto.
Si $x \in \Bbbk$ es tal que $x \neq 0$ entonces $x^n = x$, donde $n \in \mathbb{N}$ es el orden de $\Bbbk$. Luego,

$$|x^n| = |x| \Longrightarrow |x|^n = |x| \Longrightarrow |x|^{n-1} = 1 \Longrightarrow |x| = 1.$$

Así, $|\cdot|$ es el valor absoluto trivial.

$\square$

Definición 1.3 *Sea $p \in \mathbb{Z}$ un número primo fijo. La **valuación** $p-$**ádica** sobre $\mathbb{Z}$ es la función*

$$v_p : \mathbb{Z} - \{0\} \longrightarrow \mathbb{R}$$

definida como sigue: Para cada entero $n \in \mathbb{Z}$,$n \neq 0$, sea $v_p(n)$ el único entero no negativo que satisface

$$n = p^{v_p(n)} n', \ \ \textit{donde} \ \ p \nmid n'.$$

El dominio de la función $v_p(n)$ se extiende al campo de los números racionales de la siguiente manera: si $x = \frac{a}{b} \in \mathbb{Q} - \{0\}$ entonces

$$v_p(x) = v_p(a) - v_p(b),$$

con la convención de que $v_p(0) = +\infty$.

Observación El teorema fundamental de la Aritmética garantiza la existencia y unicidad de la función $v_p(n), \forall n \in \mathbb{Z}$, en la definición anterior.

Observación La valuación $p-$ádica de cualquier $x \in \mathbb{Q} - \{0\}$ está determinada por la fórmula

$$x = p^{v_p(x)} \frac{a}{b} \ \text{ donde } \ a, b \in \mathbb{Z} \ y \ p \nmid ab.$$

Lema 1.1 *Si $m, n \in \mathbb{Z}$ entonces $v_p(mn) = v_p(m) + v_p(n)$.*

Demostración Sean $m, n \in \mathbb{Z}$, se tiene

$$n = p^{v_p(n)} n' \text{ donde } p \nmid n'.$$

y

$$m = p^{v_p(m)} m' \text{ donde } p \nmid m'.$$

Luego,

$$mn = p^{v_p(m)} m' p^{v_p(n)} n' \text{ donde } p \nmid m'n'.$$

Así,

$$mn = p^{v_p(m)+v_p(n)} m'n' \text{ donde } p \nmid m'n'.$$

Por tanto, $v_p(mn) = v_p(m) + v_p(n)$.

$\square$

Proposición 1.2 *La valuación $p-$ádica cumple las siguientes propiedades:*

1. *Para cualquier $x \in \mathbb{Q}$, el valor de $v_p(x)$ no depende de su representación como cociente de dos enteros.*
2. $v_p(xy) = v_p(x) + v_p(y)$, *para todo* $x, y \in \mathbb{Q}$.
3. $v_p(x+y) \geq$ *mín*$\{v_p(x), v_p(y)\}$, *para todo* $x, y \in \mathbb{Q}$.

Con la convención de que $x < +\infty$ para todo $x \in \mathbb{R}$ y $x + \infty = +\infty$.

Demostración

1. Sea $x \in \mathbb{Q}$ tal que $x = \frac{a}{b} = \frac{c}{d}$ con $a, b, c, d \in \mathbb{Z}$. Se tiene que

$$\begin{array}{rrcl} & ad & = & bc \\ \Longrightarrow & v_p(ad) & = & v_p(bc) \\ \Longrightarrow & v_p(a) + v_p(d) & = & v_p(b) + v_p(c) \\ \Longrightarrow & v_p(a) - v_p(b) & = & v_p(c) - v_p(d) \\ \Longrightarrow & v_p(\frac{a}{b}) & = & v_p\left(\frac{c}{d}\right). \end{array}$$

   Así, el valor de $v_p(x)$ no depende de su representación como cociente de dos enteros.

2. Para el caso en el que $x = 0$ o $y = 0$ la condición se cumple claramente. Sean $x, y \neq 0$ y además $x = \frac{a}{b}$ y $y = \frac{c}{d}$, se tiene

$$\begin{array}{rcl} v_p(x) + v_p(y) & = & v_p(a) - v_p(b) + v_p(c) - v_p(d) \\ & = & v_p(a) + v_p(c) - (v_p(b) + v_p(d)) \\ & = & v_p(ac) - v_p(bd) \\ & = & v_p\left(\dfrac{ac}{bd}\right) \\ & = & v_p(xy). \end{array}$$

3. Para el caso en el que $x = 0$ o $y = 0$, las condición se cumple claramente. Sean $x, y \neq 0$ y además $x = \frac{a}{b}$ y $y = \frac{c}{d}$, por la observación anterior

$$\begin{aligned} x + y &= p^{v_p(x)}\frac{a'}{b'} + p^{v_p(y)}\frac{c'}{d'} \\ &= p^t\left(p^{v_p(x)-t}\frac{a'}{b'} + p^{v_p(y)-t}\frac{c'}{d'}\right) \end{aligned}$$

donde $t =$mín $\{v_p(x), v_p(y)\}$. La última igualdad implica que

$$v_p(x + y) \geq \text{mín}\{v_p(x), v_p(y)\}.$$

□

Definición 1.4 *Para cualquier $x \in \mathbb{Q}$, se define el **valor absoluto p-ádico** de x como*

$$|x|_p = \begin{cases} p^{-v_p(x)} & \textit{si } x \neq 0, \\ 0 & \textit{si } x = 0. \end{cases}$$

Proposición 1.3 *La función $|\cdot|_p$ definida anteriormente es un valor absoluto no arquimediano sobre $\mathbb{Q}$.*

Demostración

1. Por definición $|x|_p = 0$ si y sólo si $x = 0$.

2. Sean $x, y \in \mathbb{Q}$, si alguno de ellos es cero entonces $|xy|_p = 0 = |x|_p|y|_p$.

   Para $x, y \neq 0$ se tiene

$$|xy|_p = p^{-v_p(xy)} = p^{-v_p(x)-v_p(y)} = p^{-v_p(x)}p^{-v_p(y)} = |x|_p|y|_p.$$

3. Sean $x, y \in \mathbb{Q}$, si alguno de ellos es cero entonces $|x + y|_p =$máx$\{|x|_p, |y|_p\}$.

   Para $x, y \neq 0$, sea $k :=$máx$\{-v_p(x), -v_p(y)\}$, luego $k = -$mín$\{v_p(x), v_p(y)\}$.

   Por la proposición anterior

$$\begin{aligned} & v_p(x + y) \geq -k \\ \Longrightarrow \quad & k \geq -v_p(x + y) \\ \Longrightarrow \quad & p^k \geq p^{-v_p(x+y)}. \end{aligned}$$

   Así, máx$\{|x|_p, |y|_p\} \geq |x + y|_p$.

□

I.1.2 Propiedades

Algunas propiedades de los valores absolutos se enuncian en la siguiente proposición.

Proposición 1.4 (Proposition 1.6, [16]) *Sea* $\mathbb{k}$ *un campo y* $|\cdot|$ *un valor absoluto sobre* $\mathbb{k}$*, para todo* $x, y \in \mathbb{k}$ *se cumple:*

1. $|1| = |-1| = 1$,
2. $|x| = |-x|$,
3. $||x| - |y||_{\mathbb{R}} \leq |x \pm y|$,
4. $|x - y| \leq |x| + |y|$,
5. $|\frac{x}{y}| = \frac{|x|}{|y|}$ *donde* $y \neq 0$.

$|\cdot|_{\mathbb{R}}$ *denota el valor absoluto usual definido en* $\mathbb{R}$.

Demostración 1.

$$|1| = |(1)(1)| = |1||1| \Longrightarrow |1| = 1.$$

Por otro lado,

$$1 = |1| = |(-1)(-1)| = |-1||-1| = |-1|^2 \Longrightarrow |-1| = 1.$$

2. $|-x| = |(-1)x| = |-1||x| = |x|$.
3. Se tiene

$$|y| = |y + (x - x)| = |(y + x) + (-x)| \leq |y + x| + |-x| = |y + x| + |x|$$

$$\Rightarrow -|y + x| \leq |x| - |y|. \quad (1)$$

Por otro lado,

$$|x| = |x + (y - y)| = |(x + y) + (-y)| \leq |x + y| + |-y| = |x + y| + |y|$$

$$\Rightarrow |x| - |y| \leq |x + y|. \quad (2)$$

De (1) y (2) se obtiene

$$-|y + x| \leq |x| - |y| \leq |x + y| \Longrightarrow ||x| - |y||_{\mathbb{R}} \leq ||x + y||_{\mathbb{R}} = |x + y|.$$

De la desigualdad anterior se sigue que

$$||x| - |-y||_{\mathbb{R}} \leq |x + (-y)| \Longrightarrow ||x| - |y||_{\mathbb{R}} \leq |x - y|.$$

4. $|x-y| \leq |x| + |-y| = |x| + |y|$.

5. $$|x| = \left|\frac{y}{y}(x)\right| = |y|\left|\frac{x}{y}\right| \Longrightarrow \frac{|x|}{|y|} = \left|\frac{x}{y}\right|.$$

$\square$

La siguiente es un caracterización de los campos no arquimedianos.

Teorema 1.1 *Sea $A \subset \mathbb{k}$ la imagen de $\mathbb{Z}$ bajo la función $f : \mathbb{Z} \to \mathbb{k}$ definida de la siguiente manera*

$$f(n) = \begin{cases} \underbrace{1+1+\cdots+1}_{n\ veces} & \textit{si } n > 0 \\ 0 & \textit{si } n = 0 \\ \underbrace{-(1+1+\cdots+1)}_{-n\ veces} & \textit{si } n < 0. \end{cases}$$

Un valor absoluto $|\cdot|$ sobre $\mathbb{k}$ es no arquimediano si y sólo si $|a| \leq 1$ para todo $a \in A$. En particular, un valor absoluto sobre $\mathbb{Q}$ es no arquimediano si y sólo si $|n| \leq 1$ para todo $n \in \mathbb{Z}$.

Demostración Sea $|\cdot|$ un valor absoluto no arquimediano sobre $\mathbb{k}$.

Se probará por inducción que $|f(n)| \leq 1$ para todo $n \in \mathbb{N}$.

Para $n = 1$ se tiene que $|f(1)| = |1| = 1$, así la proposición es válida para $n = 1$. Supóngase que la proposición es válida para n, es decir, si $|f(n)| \leq 1$, entonces para $n+1$ se tiene

$$|f(n+1)| = |\underbrace{1+1+\cdots+1}_{n}+1| \leq \text{máx}\{|f(n)|, 1\} = 1.$$

Así, $|f(n)| \leq 1$ para todo $n \in \mathbb{N}$.

Por la proposición 1.1.2, $|x| = |-x|$, si $n \in \mathbb{Z}$ y $n < 0$ entonces

$$|f(n)| = |-(\underbrace{1+1+\cdots+1}_{n})| = |\underbrace{1+1+\cdots+1}_{n}| \leq 1.$$

Para $n = 0$, se cumple que $|f(0)| = 0 \leq 1$. Por tanto, $|a| \leq 1$ para todo $a \in A$.

Inversamente, sea $|\cdot|$ un valor absoluto sobre $\mathbb{k}$, tal que $|a| \leq 1$ para todo $a \in A$.
Se probará que $|x+y| \leq \text{máx}\{|x|, |y|\}$ para todo $x, y \in \mathbb{k}$.
Si $y = 0$ entonces se cumple que $|x+y| \leq \text{máx}\{|x|, |y|\}$ para cualquier $x \in \mathbb{k}$.
Si $y \neq 0$ entonces se cumple la siguiente equivalencia

$$|x+y| \leq \text{máx}\{|x|, |y|\} \Longleftrightarrow \left|\frac{x}{y}+1\right| \leq \text{máx}\{\left|\frac{x}{y}\right|, 1\}.$$

Así, basta con probar que $|x+1| \leq \text{máx}\{|x|, 1\}$ para todo $x \in \mathbb{k}$.
Sea $x \in \mathbb{k}$, para m cualquier entero positivo se tiene

$$|x+1|^m = \left|\sum_{k=0}^{m} \binom{m}{k} x^k\right| \leq \sum_{k=0}^{m} \left|\binom{m}{k}\right| |x^k|.$$

Luego,

$$\binom{m}{k} \in A \Longrightarrow \left|\binom{m}{k}\right| \leq 1$$

$$\Longrightarrow |x+1|^m \leq \sum_{k=0}^{m} |x|^k$$

Si $|x| \geq 1$ entonces $|x|^k \leq |x|^m$ para todo $k = 0, 1, \cdots, m$ y si $|x| < 1$ entonces $|x|^k < 1$ para todo $k = 0, 1, \cdots, m$. Así,

$$\sum_{k=0}^{m} |x|^k \leq (m+1)\text{máx}\{1, |x|^m\}$$

$$\Longrightarrow |x+1| \leq \sqrt[m]{m+1}\,(\text{máx}\{1, |x|\})\,.$$

Lo anterior se hizo sin importar el número m, es decir, la última desigualdad es válida $\forall m \in \mathbb{N}$.
Haciendo $m \longrightarrow \infty$ y usando $\lim_{m\to\infty} \sqrt[m]{m+1} = 1$, se obtiene

$$|x+1| \leq \text{máx}\{|x|, 1\},$$

tal como se quería demostrar.

□

Ahora se puede justificar de alguna manera la diferencia entre un valor absoluto arquimediano y un valor absoluto no arquimediano.

Definición 1.5 *Un valor absoluto es* ***arquimediano*** *si tiene la siguiente propiedad:*

Dados $x, y \in \mathbb{k}$, $x \neq 0$, existe un entero positivo n tal que $|nx| > |y|$.

La propiedad anterior es conocida como la propiedad arquimediana. Esta propiedad se cumple para $\mathbb{Q}$ y $\mathbb{R}$ con el valor absoluto usual. Se puede ver que la propiedad arquimediana es equivalente a

$$sup\{|n| : n \in \mathbb{Z}\} = +\infty.$$

Es decir, hay enteros arbitrariamente “grandes ”. Con esta caracterización, se observa que un valor absoluto no arquimediano no tiene la propiedad arquimediana.

I.1.3 Métrica inducida por un valor absoluto

Definición 1.6 *Sea $\Bbbk$ un campo y $|\cdot|$ un valor absoluto sobre $\Bbbk$, se define la* ***distancia*** *$d(x,y)$ entre dos elementos $x, y \in \Bbbk$ como*

$$d(x,y) = |x-y|.$$

La función $d(x,y)$ es llamada la ***métrica inducida por el valor absoluto.***

El nombre de métrica está justificado por la siguiente proposición.

Proposición 1.5 *Sea $\Bbbk$ un campo y $|\cdot|$ un valor absoluto sobre $\Bbbk$, entonces la métrica inducida por el valor absoluto es efectivamente una métrica.*

Demostración Para cualquier valor absoluto sobre $\Bbbk$ se cumple:

1. $d : \Bbbk \longrightarrow \mathbb{R}^+$.

2. $$d(x,y) = |x-y| \geq 0 \quad \forall x, y \in \Bbbk.$$

   Además,
   $$d(x,y) = |x-y| = 0 \Leftrightarrow x-y = 0 \Leftrightarrow x = y.$$

3. $$d(x,y) = |x-y| = |-(y-x)| = |y-x| = d(y,x) \quad \forall x, y \in \Bbbk.$$

4. $$\begin{aligned} d(x,y) &= |x-y| \\ &= |x-y+(z-z)| \\ &= |(x-z)+(z-y)| \\ &\leq |x-z|+|z-y| \\ &= d(x,z)+d(z,y) \quad \forall x, y, z \in \Bbbk. \end{aligned}$$

De $1, 2, 3$ y 4 se concluye que la métrica inducida por el valor absoluto es una métrica.

□

Proposición 1.6 *La función valor absoluto, $|\cdot| : \Bbbk \to \mathbb{R}^+$, es continua.*

Demostración Sea $x \in \Bbbk$ y $\epsilon > 0$, si $|x-y| < \epsilon$ entonces

$$||x|-|y||_{\mathbb{R}} \leq |x-y| < \epsilon.$$

Así, $|\cdot|$ es continua en x.
Como $x \in \Bbbk$ se tomó de manera arbitraria se obtiene que $|\cdot|$ es continua.

□

La siguiente proposición da una primera consecuencia de dotar a un campo con una topología inducida por un valor absoluto.

Proposición 1.7 *Sea $\mathbb{k}$ un campo con un valor absoluto $|\cdot|$. Las operaciones de suma, producto y tomar inversos son funciones continuas.*

Demostración Se tiene,

1. Sean $x_0, y_0 \in \mathbb{k}$ fijos. Para cualquier $\epsilon > 0$, tomando $\delta = \frac{\epsilon}{2}$, se tiene que si

$$|x_0 - x| < \delta \quad y \quad |y_0 - y| < \delta$$

entonces

$$|(x_0 + y_0) - (x + y)| \leq |x_0 - x| + |y_0 - y| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon.$$

Así, la suma es una función continua.

2. Sean $x_0, y_0 \in \mathbb{k}$ fijos.
Para cualquier $\epsilon > 0$, tomando $\delta =$mín$\{\frac{\epsilon}{2(|x_0|+1)}, \frac{\epsilon}{2(|y_0|+1)}, 1\}$, se tiene que si

$$|x_0 - x| < \delta \quad y \quad |y_0 - y| < \delta$$

entonces

$$|y| = |y - y_0 + y_0| \leq |y - y_0| + |y_0| < 1 + |y_0|.$$

Así,

$$\begin{aligned}
|x_0y_0 - xy| &= |x_0y_0 - x_0y + x_0y - xy| \\
&\leq |x_0||y_0 - y| + |y||x_0 - x| \\
&< |x_0|\frac{\epsilon}{2(1 + |x_0|)} + (1 + |y_0|)\left(\frac{\epsilon}{2(|y_0| + 1)}\right) \\
&< \frac{\epsilon}{2} + \frac{\epsilon}{2} \\
&= \epsilon.
\end{aligned}$$

Por tanto, el producto es una función continua.

3. Sea $x_0 \in \mathbb{K}$ fijo. Para cualquier $\epsilon > 0$, tomando $\delta = \epsilon$ se obtiene

$$|x - x_0| < \delta \Longrightarrow |-x - (-x_0)| = |x_0 - x| < \delta = \epsilon.$$

Así, la operación de tomar inversos aditivos es continua.

4. Sea $x_0 \in \mathbb{k} \setminus \{0\}$ fijo. Para cualquier $\epsilon > 0$, tomando $\delta =$mín$\{\frac{|x_0|}{2}, \frac{\epsilon|x_0|^2}{2}\}$, se tiene que si

$$|x_0 - x| < \delta$$

entonces

$$\begin{array}{rrcccl} & ||x| - |x_0||_{\mathbb{R}} & \leq & |x - x_0| & < & \frac{|x_0|}{2} \\ \Longrightarrow & -\frac{|x_0|}{2} & < & |x| - |x_0| & < & \frac{|x_0|}{2} \\ \Longrightarrow & \frac{|x_0|}{2} & < & |x| & < & \frac{3|x_0|}{2} \\ \Longrightarrow & & & \frac{1}{|x|} & < & \frac{2}{|x_0|} \end{array}$$

Así,

$$\begin{aligned} \left|\frac{1}{x_0} - \frac{1}{x}\right| &= \frac{|x - x_0|}{|x||x_0|} \\ &< \left(\frac{2}{|x_0|}\right)\left(\frac{1}{|x_0|}\right)\left(\frac{\epsilon|x_0|^2}{2}\right) \\ &= \epsilon. \end{aligned}$$

Por tanto, la operación de tomar inversos multiplicativos es continua.

□

Proposición 1.8 *Sea* $\mathbb{k}$ *un campo y sea* $|\cdot|$ *un valor absoluto no arquimediano sobre* $\mathbb{k}$. *Si* $x, y \in \mathbb{k}$ *y* $|x| \neq |y|$ *entonces*

$$|x + y| = \textit{máx}\{|x|, |y|\}.$$

Demostración Sin pérdida de generalidad sea $|x| > |y|$. Se tiene que

$$|x + y| \leq |x| = \text{máx}\{|x|, |y|\}. \quad (*)$$

Por otro lado,

$$x = (x + y) - y \Longrightarrow |x| \leq \text{máx}\{|x + y|, |y|\},$$

como $|x| > |y|$

$$\Longrightarrow \text{máx}\{|x + y|, |y|\} = |x + y| \Longrightarrow |x| \leq |x + y|. \quad (**)$$

De $(*)$ y $(**)$ se obtiene $|x + y| = |x|$.

□

Corolario 1.1 *En un campo con un valor absoluto no arquimediano* $|\cdot|$, *todos los "triángulos"son isósceles.*

Demostración Sean x, y y z tres puntos del espacio (los vértices del triángulo). Las longitudes de los lados del triángulo son las tres distancias

$$d(x,y) = |x-y|, \quad d(y,z) = |y-z| \quad y \quad d(x,z) = |z-x|.$$

Como $(x-y)+(y-z) = x-z$.

Si $|x-y| = |y-z|$ el triángulo ya es isósceles.

Si $|x-y| \neq |y-z|$ entonces por la proposición anterior se obtiene

$$|x-z| = |(x-y)+(y-z)| = \text{máx}\{|x-y|, |y-z|\}.$$

Así, todos los triángulos son isósceles.

$\square$

I.2. Números p-ádicos

En esta sección, se aplica la teoría desarrollada anteriormente a la construcción de los números $p-$ádicos. Además, se introduce la integración en el campo de los números p-ádicos, usando la medida de Haar.

I.2.1 Valores Absolutos sobre $\mathbb{Q}$

El objetivo de esta sección es caracterizar los valores absolutos sobre $\mathbb{Q}$, de acuerdo a la topología que generan.

Definición 1.7 *Dos valores absolutos $|\cdot|_1$ y $|\cdot|_2$ sobre un campo $\mathbb{k}$ se dicen* ***equivalentes*** *si definen la misma topología sobre $\mathbb{k}$.*

Lema 1.2 *Sea $\mathbb{k}$ un campo y $|\cdot|$ un valor absoluto definido sobre él. Se tiene que*

$$\lim_{n\to\infty} x^n = 0 \Longleftrightarrow |x| < 1.$$

Demostración Supóngase que $\lim_{n\to\infty} x^n = 0$ entonces para $\epsilon = 1$ existe $N \in \mathbb{N}$ tal que

$$|x^n - 0| = |x^n| = |x|^n < 1$$

para $n \geq N$.
Luego, $|x|^N < 1$. Esto implica que $|x| < 1$.

Reciprocamente, si $x = 0$ no hay nada que probar. Para $x \neq 0$, sea $\epsilon > 0$.
Como $|x| < 1$ entonces $\frac{1}{|x|} > 1$.
Luego, existe $h \in \mathbb{R}$ con $h > 0$ tal que $\frac{1}{|x|} = 1 + h$.
Por la desigualdad de Bernoulli se tiene

$$\left(\frac{1}{|x|}\right)^k = (1+h)^k \geq 1 + kh \quad \forall k \in \mathbb{N}.$$

Por la propiedad Arquimediana existe $N \in \mathbb{N}$ tal que $Nh > \frac{1}{\epsilon} - 1$, es decir, $1 + Nh > \frac{1}{\epsilon}$.
Luego,

$$\frac{1}{|x|^N} > \frac{1}{\epsilon} \Longrightarrow \epsilon > |x|^N.$$

Así, para $n \geq N$ se tiene que $|x|^n < \epsilon$.
Por tanto, $\lim_{n\to\infty} x^n = 0$.

$\square$

Lema 1.3 *Sean $|\cdot|_1$ y $|\cdot|_2$ valores absolutos sobre un campo $\mathbb{k}$. Los siguientes enunciados son equivalentes:*

$i)$ *$|\cdot|_1$ y $|\cdot|_2$ son valores absolutos equivalentes;*

$ii)$ *Para cualquier $x \in \mathbb{k}$ se tiene que $|x|_1 < 1$ si y sólo si $|x|_2 < 1$;*

$iii)$ *Existe un número real positivo α tal que para cada $x \in \mathbb{k}$ se tiene*

$$|x|_1 = |x|_2^\alpha.$$

Demostración Para demostrar que $i)$ implica $ii)$, sea $x \in \mathbb{k}$ tal que $|x|_1 < 1$, por el lema anterior se tiene que $\lim_{n\to\infty} x^n = 0$ con $|\cdot|_1$.
Como los valores absolutos son equivalentes entonces todo abierto de $(\mathbb{k}, d_{|\cdot|_1})$ es un abierto en $(\mathbb{k}, d_{|\cdot|_2})$.
Así, $\lim_{n\to\infty} x^n = 0$ con $|\cdot|_2$ y por el lema anterior se obtiene $|x|_2 < 1$.
De manera análoga se prueba que si $|x|_2 < 1$ entonces $|x|_1 < 1$.

Para demostrar que $ii)$ implica $iii)$, se distinguen dos casos. Si $|\cdot|_1$ es el valor absoluto trivial para $x \neq 0, 1$ se tiene que si $|x|_1 = 1$ entonces $|x|_2 = 1$, pues de lo contrario se obtiene que $|x|_1 \neq 1$ siendo una contradicción a que $|\cdot|_1$ es el valor absoluto trivial.

Si $|\cdot|_1$ no es el valor absoluto trivial entonces existe $x_0 \neq 0, 1$ tal que $|x_0|_1 < 1$.
Luego, $|x_0|_2 < 1$. Sea

$$\alpha = log_{|x_0|_2}|x_0|_1.$$

Con esto $|x_0|_1 = |x_0|_2^\alpha$.
Se tiene que $\alpha > 0$ pues de lo contario se obtiene $|x_0|_1 \geq 1$, lo cual no es posible por que $|x_0|_1 < 1$.
Dado $x \in \mathbb{k}$, se tienen los siguientes casos:
Si $|x|_1 = 1$ entonces $|x|_2 = 1$ pues de lo contrario se obtiene que $|x|_1 \neq 1$ siendo una contradicción. Así, $|x|_1 = |x|_2^\alpha$.

Si $|x|_1 = |x_0|_1$ entonces $|x|_2 = |x_0|_2$, por que si $|x|_2 < |x_0|_2$ entonces $|\frac{x}{x_0}|_2 < 1$ esto implica que $|\frac{x}{x_0}|_1 < 1$ y así $|x|_1 < |x_0|_1$, que es una contradicción a la suposición inicial. Analógamente se obtiene una contradicción al suponer $|x|_2 > |x_0|_2$.
Así, $|x|_1 = |x_0|_1 = |x_0|_2^{\alpha} = |x|_2^{\alpha}$.
Si $|x|_1 \neq 1$ y $|x|_1 \neq |x_0|_1$ entonces sea

$$S = \left\{ r = \frac{m}{n} : m, n \in \mathbb{N} \ \ y \ \ |x|_1^{\frac{m}{n}} < |x_0|_1 \right\}.$$

Se tiene

$$\frac{m}{n} \in S \Longleftrightarrow |x|_1^{\frac{m}{n}} < |x_0|_1 \Longleftrightarrow |x|_1^m < |x_0|_1^n \Longleftrightarrow \left| \frac{x^m}{x_0^n} \right|_1 < 1 \Longleftrightarrow \left| \frac{x^m}{x_0^n} \right|_2 < 1$$

$$\Longleftrightarrow |x|_2^m < |x_0|_2^n \Longleftrightarrow |x|_2^{\frac{m}{n}} < |x_0|_2.$$

Así,

$$S = \left\{ r = \frac{m}{n} : m, n \in \mathbb{N} \ \ y \ \ |x|_2^{\frac{m}{n}} < |x_0|_2 \right\} = \left\{ r = \frac{m}{n} : m, n \in \mathbb{N} \ \ y \ \ |x|_1^{\frac{m}{n}} < |x_0|_1 \right\}.$$

Es decir,

$$S = \left\{ r = \frac{m}{n} : m, n \in \mathbb{N} \ \ y \ \ |x|_2 < |x_0|_2^{\frac{n}{m}} \right\} = \left\{ r = \frac{m}{n} : m, n \in \mathbb{N} \ \ y \ \ |x|_1 < |x_0|_1^{\frac{n}{m}} \right\}.$$

Sean

$$s = log_{|x_0|_1} |x|_1 \ \ y \ \ t = log_{|x_0|_2} |x|_2.$$

Se obtiene,

$$S = \left\{ r = \frac{m}{n} : m, n \in \mathbb{N} \ \ y \ \ s < \frac{1}{r} \right\} = \left\{ r = \frac{m}{n} : m, n \in \mathbb{N} \ \ y \ \ t < \frac{1}{r} \right\}.$$

Si $s \neq t$ se tiene que $s < t$ ó $t < s$.
Si $s < t$ entonces existe $p \in \mathbb{Q}$ tal que $s < p < t$, luego se tiene que $\frac{1}{p} \in S$ pues $s < \frac{1}{\frac{1}{p}} = p$. Por otro lado, $\frac{1}{p} \notin S$ pues $\frac{1}{\frac{1}{p}} = p < t$, luego $\frac{1}{p} \in S$ y $\frac{1}{p} \notin S$ con contradicción. Análogamente si $t < s$ se obtiene una contradicción, entonces $s = t$ y por lo tanto,

$$|x|_1 = |x_0|_1^s = (|x_0|_2^{\alpha})^s = (|x_0|^s)^{\alpha} = |x|_2^{\alpha}.$$

Para demostrar que $iii)$ implica $i)$, sea $B_{|\cdot|_1}(x, r)$ una bola abierta en $(\mathbb{k}, d_{|\cdot|_1})$.
Como para cualquier $z \in \mathbb{k}$ se tiene que

$$|z|_1 = |z|_2^{\alpha}$$

con α un número real positivo.
Luego,

$$y \in B_{|\cdot|_1}(x,r) \Longleftrightarrow |x-y|_1 < r \Longleftrightarrow |x-y|_2^{\alpha} < r \Longleftrightarrow |x-y| < \sqrt[\alpha]{r}$$

$$\Longleftrightarrow y \in B_{|\cdot|_2}(x, \sqrt[\alpha]{r}).$$

Así, toda bola abierta en $(\mathbb{k}, d_{|\cdot|_1})$ es una bola abierta en $(\mathbb{k}, d_{|\cdot|_2})$. Por tanto, $|\cdot|_1$ y $|\cdot|_2$ son equivalentes.

$\square$

Los siguientes corolarios se obtienen como consecuencia inmediata del teorema anterior.

Corolario 1.2 *En el campo de los números racionales, el valor absoluto usual no es equivalente a ningún valor absoluto $p-$ádico.*

Corolario 1.3 *En el campo de los números racionales, si p, q son primos distintos entonces $|\cdot|_p$ y $|\cdot|_q$ no son equivalentes.*

Lema 1.4 *Sea $|\cdot|$ un valor absoluto definido sobre $\mathbb{Q}$. Si se conoce $|n|$ para todo $n \in \mathbb{N}$ entonces se puede determinar $|x|$ para todo $x \in \mathbb{Q}$.*

Demostración Por definición se tiene $|0| = 0$. Para n entero negativo se tiene que $-n \in \mathbb{N}$, entonces $|n| = |-n|$. Para cualquier $n \in \mathbb{Z} - \{0\}$ se tiene que $|\frac{1}{n}| = \frac{1}{|n|}$. Así, si $\frac{a}{b} \in \mathbb{Q}$ se tiene $|\frac{a}{b}| = |a||\frac{1}{b}| = \frac{|a|}{|b|}$.

$\square$

Teorema 1.2 ***(Ostrowski)*** *Cada valor absoluto no trivial sobre $\mathbb{Q}$ es equivalente a uno de los valores absolutos $|\cdot|_p$, donde p es un número primo o $p = \infty$, recordando que $|\cdot|_\infty$ es el valor absoluto usual.*

Demostración Sea $|\cdot|$ un valor absoluto no trivial sobre $\mathbb{Q}$, se distinguen dos casos:

1. Si $|\cdot|$ es arquimediano, sea n_0 el menor entero positivo para el cual $n_0 > 1$, existe tal entero por que de lo contrario $|\cdot|$ sería no arquimediano. Sea $\alpha = log_{n_0}|n_0|$, entonces $|n_0| = n_0^{\alpha}$. Se probará que $|x| = |x|_\infty^{\alpha}$ para todo $x \in \mathbb{Q}$, por el lema anterior basta con checar esto para $n \in \mathbb{N}$. Sea $n \in \mathbb{N}$ escribiendo n en base n_0 se obtiene

   $$n = a_0 + a_1 n_0 + a_2 n_0^2 + \cdots + a_k n_0^k$$

   con $0 \leq a_i \leq n_0 - 1$ para $i = 1, \cdots, k$ y $a_k \neq 0$.

   Tomando valores absolutos se obtiene

$$\begin{aligned}
|n| &= |a_0 + a_1 n_0 + a_2 n_0^2 + \cdots + a_k n_0^k| \\
&\leq |a_0| + |a_1||n_0| + |a_2||n_0|^2 + \cdots + |a_k||n_0|^k \\
&= |a_0| + |a_1| n_0^\alpha + |a_2| n_0^{2\alpha} + \cdots + |a_k| n_0^{k\alpha},
\end{aligned}$$

como n_0 es el entero más pequeño cuyo valor absoluto es mayor que 1 se tiene que $|a_i| \leq 1$ para $i = 1, \cdots, k$. Luego,

$$\begin{aligned}
|n| &\leq 1 + n_0^\alpha + n_0^{2\alpha} + \cdots + n_0^{k\alpha} \\
&= n_0^{k\alpha}(1 + n_0^{-\alpha} + n_0^{-2\alpha} + \cdots + n_0^{-k\alpha}) \\
&\leq n_0^{k\alpha} \sum_{i=0}^{\infty} n_0^{-i\alpha} \\
&= n_0^{k\alpha} \left(\frac{n_0^\alpha}{n_0^\alpha - 1} \right).
\end{aligned}$$

Sea $C = \frac{n_0^\alpha}{n_0^\alpha - 1}$. Se tiene que $C > 0$. Entonces $|n| \leq C n_0^{k\alpha} \leq C n^\alpha$. Esta última desigualdad es válida para cada $n \in \mathbb{N}$, pues n se tomó de manera arbitraria.

Aplicando la desigualdad a un entero de la forma n^N se obtiene

$$|n^N| \leq C n^{N\alpha} \Longrightarrow |n| \leq \sqrt[N]{C} n^\alpha,$$

haciendo que $N \longrightarrow \infty$ se obtiene $|n| \leq n^\alpha$ pues $\lim_{N\to\infty} \sqrt[N]{C} = 1$. Esta desigualdad, es válida para cualquier número natural n por ser n arbitrario.

Por otro lado, como $n_0^{k+1} > n \geq n_0^k$ se tiene

$$\begin{aligned}
n_0^{(k+1)\alpha} &= |n_0^{k+1}| \\
&= |n + n_0^{k+1} - n| \\
&\leq |n| + |n_0^{k+1} - n|
\end{aligned}$$

$$\Longrightarrow n_0^{(k+1)\alpha} - |n_0^{k+1} - n| \leq |n|$$

$$\Longrightarrow n_0^{(k+1)\alpha} - (n_0^{k+1} - n)^\alpha \leq |n|.$$

Ahora como $n \geq n_0^k$ se obtiene

$$\begin{aligned} |n| &\geq n_0^{(k+1)\alpha} - (n_0^{k+1} - n_0^k)^\alpha \\ &= n_0^{(k+1)\alpha}\left(1 - \left(1 - \frac{1}{n_0}\right)^\alpha\right) \\ &= C' n_0^{(k+1)\alpha} \\ &> C' n^\alpha, \end{aligned}$$

donde $C' = 1 - (1 - \frac{1}{n_0})^\alpha > 0$ y no depende de n.

Aplicando la desigualdad a n^N se obtiene

$$|n^N| > C' n^{N\alpha} \Longrightarrow |n| > \sqrt[N]{C'} n^\alpha,$$

haciendo que $N \longrightarrow \infty$ se obtiene $|n| \geq n^\alpha$ pues $\lim_{N\to\infty} \sqrt[N]{C'} = 1$. Así, $|n| = n^\alpha$. Por tanto, $|n| = |n|_\infty^\alpha$ para todo $n \in \mathbb{N}$, tal como se quería probar.

2. Si $|\cdot|$ es no arquimediano se tiene que $|n| \leq 1$ para todo $n \in \mathbb{Z}$. Luego, por ser $|\cdot|$ distinto del trivial, al menos para un $m \in \mathbb{Z}$ se tiene que $|m| < 1$.

   Sea n_0 el menor número natural para el que $|n_0| < 1$, n_0 es primo, por que de lo contrario existen enteros a, b tales que $1 < a, b < n_0$ y $n_0 = ab$, por la elección de n_0 se tiene que $|a| = |b| = 1$ y así $|n_0| = 1$, contradiciendo el hecho de que $|n_0| < 1$.

   Sea entonces $n_0 = p$. Se probará que $|x| = |x|_p^\alpha$ para todo $x \in \mathbb{Q}$, por el lema anterior basta con checar esto para $n \in \mathbb{N}$.

   Sean $n \in \mathbb{N}$ y $\alpha = log_{\frac{1}{p}}|p|$. Si $p \nmid n$ entonces $n = pq + r$ donde $0 < r < p$, por la elección de p se tiene que $|r| = 1$.

   Además, $|pq| < 1$ pues $|p| < 1$ y $|q| \leq 1$. Esto implica que $|n| =$máx$\{|pq|, |r|\} = 1$, esto último es consecuencia de la proposición 1.8.

   Por otro lado, para n tal que $p|n$ se tiene que $n = p^v n'$ con $p \nmid n'$. Entonces

$$|n| = |p|^v |n'| = |p|^v = \left(\frac{1}{p}\right)^{v\alpha} = |n|_p^\alpha.$$

   Por tanto, $|\cdot|$ es quivalente a $|\cdot|_p$.

$\square$

Este teorema dice que si se quiere estudiar $\mathbb{Q}$ con algún valor absoluto no trivial, esencialmente sólo se tienen dos opciones: el valor absoluto trivial y algún valor absoluto p-ádico.

I.2.2 Completaciones

El objetivo de esta subsección es obtener el campo de los números $p-$ádicos, $\mathbb{Q}_p$, mediante un proceso de completación al campo de los números racionales $\mathbb{Q}$.

Definición 1.8 *Sea $\mathbb{k}$ un campo y sea $|\cdot|$ un valor absoluto sobre $\mathbb{k}$.*

1. *Una sucesión de elementos de $\mathbb{k}$, $\{x_n\}$, es llamada una **sucesión de Cauchy** si para cada $\epsilon > 0$ existe $M \in \mathbb{N}$ tal que $|x_n - x_m| < \epsilon$ siempre que $n, m \geq M$.*

2. *El campo $\mathbb{k}$ es llamado **completo con respecto a** $|\cdot|$ si cada sucesión de Cauchy de elementos de $\mathbb{k}$ tiene un límite en $\mathbb{k}$.*

Lema 1.5 *Una sucesión $\{x_n\}$ de números racionales es una sucesión de Cauchy con respecto a un valor absoluto no arquimediano $|\cdot|$ si y sólo si se tiene*

$$\lim_{n\to\infty} |x_{n+1} - x_n| = 0.$$

Demostración Sea $\epsilon > 0$, por ser $\{x_n\}$ sucesión de Cauchy existe $N \in \mathbb{N}$ tal que si $m, n \geq N$, entonces $|x_n - x_m| < \epsilon$. En particular, si $n \geq N$ entonces $|x_{n+1} - x_n| < \epsilon$. Así,

$$\lim_{n\to\infty} |x_{n+1} - x_n| = 0.$$

Reciprocamente, sea $\epsilon > 0$, como $\lim_{n\to\infty} |x_{n+1} - x_n| = 0$ existe $N \in \mathbb{N}$ tal que si $n \geq N$
entonces $|x_{n+1} - x_n| < \epsilon$.
Sean $n, m \geq N$, sin pérdida de generalidad se considera $m > n$, entonces $m = n + r$. Luego,

$$\begin{aligned} |x_m - x_n| &= |x_{n+r} - x_{n+r-1} + x_{n+r-1} - x_{n+r-2} + x_{n+r-2} - \cdots + x_{n+1} - x_n| \\ &\leq \text{máx}\{|x_{n+r} - x_{n+r-1}|, |x_{n+r-1} - x_{n+r-2}|, \cdots, |x_{n+1} - x_n|\} \\ &< \epsilon. \end{aligned}$$

Así, $\{x_n\}$ es una sucesión de Cauchy.

□

Teorema 1.3 *El campo $\mathbb{Q}$ de números racionales no es completo con respecto a cualquiera de los valores absolutos no triviales.*

Demostración Por el teorema de Ostrowski (teorema 1.2) es suficiente checar esto para los valores absolutos $|\cdot|_p$, donde p es un número primo ó $p = \infty$.
Es bien sabido que $\mathbb{Q}$ no es completo con $|\cdot|_\infty$, entonces solamente se analiza el caso cuando p es un número primo.

Sea $\mathbb{Q}$ con el valor absoluto $|\cdot|_p$, donde p es un número primo fijo. Considerese la sucesión

$$a_n = 1 + p + p^2 + p^3 + \cdots + p^n.$$

Se tiene que la sucesión (a_n) es de Cauchy, pues

$$\lim_{n\to\infty} |a_{n+1} - a_n|_p = \lim_{n\to\infty} |p^{n+1}|_p = \lim_{n\to\infty} p^{-n} = 0.$$

Además, a_n converge al número $1 + p + p^2 + p^3 + \cdots + p^n + \cdots$.
Si $1 + p + p^2 + p^3 + \cdots + p^n + \cdots$ es un número racional s, se tiene que

$$s = 1+p+p^2+p^3+\cdots+p^n+\cdots = 1+p(1+p+p^2+p^3+\cdots+p^n+\cdots) = 1+ps.$$

Es decir, s es igual a un número mayor que el, lo que es una contradicción. Así, $1+p+p^2+p^3+\cdots+p^n+\cdots$ no es un número racional.
Por tanto, $\mathbb{Q}$ con el valor absoluto $|\cdot|_p$ no es completo.

$\square$

Definición 1.9 *Sea $|\cdot| = |\cdot|_p$ un valor absoluto no arquimediano sobre $\mathbb{Q}$. Se denota por $\mathcal{C}$ o $\mathcal{C}_p(\mathbb{Q})$, el conjunto de todas las sucesiones de Cauchy de elementos de $\mathbb{Q}$ con respecto a $|\cdot|_p$, es decir,*

$$\mathcal{C} = \mathcal{C}_p(\mathbb{Q}) = \{(x_n) : (x_n) \text{ es una sucesión de Cauchy con respecto a } |\cdot|_p\}.$$

Proposición 1.9 *Definiendo*

$$\begin{aligned}
(x_n) + (y_n) &= (x_n + y_n), \\
(x_n) \cdot (y_n) &= (x_n y_n), \\
0 &= (0) \ \ y \\
1 &= (1).
\end{aligned}$$

Se tiene que $\mathcal{C}$ es una anillo conmutativo con unidad.

Demostración Para ver que la suma es cerrada en $\mathcal{C}$ sean $(x_n), (y_n) \in \mathcal{C}$ y $\epsilon > 0$, existen $N_1, N_2 \in \mathbb{N}$ tal que si $n, m \geq N_1$ entonces $|x_n - x_m| < \epsilon$ y si $m, n \geq N_2$ entonces $|y_n - y_m| < \epsilon$. Sea $N =$máx$\{N_1, N_2\}$. Si $n, m \geq N$ entonces

$$\begin{aligned}
|x_n + y_n - (x_m + y_m)| &= |(x_n - x_m) + (y_n - y_m)| \\
&\leq \text{máx}\{|x_n - x_m|, |y_n - y_m|\} \\
&= \epsilon.
\end{aligned}$$

Así, $(x_n + y_n) \in \mathcal{C}$.

Para probar que el producto es cerrado en $\mathcal{C}$ primero se verá que toda sucesión de Cauchy es acotada. Sea (x_n) una sucesión de Cauchy, para $\epsilon = 1$ existe $N \in \mathbb{N}$ tal que si $n, m \geq N$ entonces $|x_n - x_m| < 1$. En particular $|x_n - x_N| < 1$ si $n > N$, entonces

$$||x_n| - |x|_N|_{\mathbb{R}} \leq |x_n - x_N| < 1$$

Luego, $-1 < |x_n| - |x_N| < 1$ si $n > N$. Esto implica que $|x_n| < |x_N| + 1$ si $n > N$.
Sea $k =$máx$\{|x_1|, |x_2|, \cdots, |x_N|, |x_N| + 1\}$. Se tiene que $|x_n| \leq k$ para todo $n \in \mathbb{N}$. Así, la sucesión (x_n) está acotada. Se probará ahora que el producto es cerrado.
Sean $(x_n), (y_n) \in \mathcal{C}$ y $\epsilon > 0$, por lo anterior existen $k_1, k_2 \in \mathbb{R}$ mayores que cero, tal que $|x_n| < k_1$ y $|y_n| < k_2$ para todo $n \in \mathbb{N}$.
Sea $k =$máx$\{k_1, k_2\}$. Para $\frac{\epsilon}{k}$ existen $N_1, N_2 \in \mathbb{N}$ tal que si $n, m \geq N_1$ entonces $|x_n - x_m| < \frac{\epsilon}{k}$ y si $m, n \geq N_2$ entonces $|y_n - y_m| < \frac{\epsilon}{k}$. Sea $N =$máx$\{N_1, N_2\}$. Si $n, m \geq N$ entonces

$$\begin{aligned}
|x_n y_n - x_m y_m| &= |x_n y_n - x_m y_n + x_m y_n - x_m y_m| \\
&= |y_n(x_n - x_m) + x_m(y_n - y_m)| \\
&\leq \text{máx}\{|y_n||x_n - x_m|, |x_m||y_n - y_m|\} \\
&< \text{máx}\{k\frac{\epsilon}{k}, k\frac{\epsilon}{k}\} \\
&= \epsilon.
\end{aligned}$$

Así, $(x_n y_n) \in \mathcal{C}$.
Las propiedades de Anillo se heredan por ser $\mathbb{Q}$ un campo y de la definición de las operaciones, también comprobar que el elemento neutro es $0 = (0)$ y el elemento unidad es $1 = (1)$ se sigue de la definición de las operaciones.

□

Lema 1.6 *La función $f : \mathbb{Q} \longrightarrow \mathcal{C}$ definida por $f(x) = (x)$ es una inclusión de $\mathbb{Q}$ en $\mathcal{C}$.*

Demostración La función está bien definida y es inyectiva pues

$$x = y \Longleftrightarrow (x) = (y) \Longleftrightarrow f(x) = f(y).$$

Además es un morfismo de anillos, pues $f(x+y) = (x+y) = (x)+(y) = f(x)+f(y)$, $f(1) = (1)$ y $f(xy) = (xy) = (x) \cdot (y) = f(x) \cdot f(y)$.

□

Definición 1.10 *Se define $\mathcal{N} \subset \mathcal{C}$ como el conjunto*

$$\mathcal{N} = \{(x_n) : x_n \to 0\} = \{(x_n) : \lim_{n\to\infty} |x_n|_p = 0\}$$

es decir, el conjunto de sucesiones que convergen a cero con respecto al valor absoluto $|\cdot|_p$.

Proposición 1.10 *$\mathcal{N}$ es un ideal en $\mathcal{C}$.*

Demostración Se tiene,

1. $(0) \in \mathcal{N}$ pues $\lim_{n\to 0} |0|_p = 0$.

2. Si $(x_n), (y_n) \in \mathcal{N}$ para $\epsilon > 0$ existen N_1, N_2 tal que si $n \geq N_1$ y $m \geq N_2$ entonces
$$|x_n|_p < \epsilon \;\; y \;\; |x_m|_p < \epsilon.$$
Sea $N =$máx$\{N_1, N_2\}$. Para $n \geq N$ se tiene $|x_n + y_n|_p \leq$máx$\{|x_n|_p, |y_n|_p\} < \epsilon$
$$\Longrightarrow \lim_{n\to\infty} x_n + y_n = 0.$$
Así, $(x_n) + (y_n) \in \mathcal{N}$.

3. Sea $(y_n) \in \mathcal{C}$ y $(x_n) \in \mathcal{N}$, se tiene $(x_n)(y_n) = (x_n y_n)$, luego $|x_n y_n|_p = |x_n|_p |y_n|_p$, como $(y_n) \in \mathcal{C}$ entonces existe $k \in \mathbb{R}$ tal que $|y_n|_p \leq k$ para todo $n \in \mathbb{N}$.

   Luego,
$$\lim_{n\to\infty} |x_n|_p |y_n|_p \leq \lim_{n\to\infty} k|x_n|_p = 0 \Longrightarrow \lim_{n\to\infty} |x_n y_n|_p = 0.$$
Así, $(x_n)(y_n) \in \mathcal{N}$.

□

Lema 1.7 *Si (x_n) es una sucesión de Cauchy tal que $x_n \nrightarrow 0$ entonces existen $c > 0$ y $N \in \mathbb{N}$ tal que $|x_n|_p > c$, para $n \geq N$.*

Demostración Como $x_n \nrightarrow 0$ existe $\epsilon > 0$ tal que para todo $M \in \mathbb{N}$ se cumple $|x_k|_p > \epsilon$ para algún $k \geq M$.
Para este $\epsilon > 0$ existe $N' \in \mathbb{N}$ tal que si $m, n \geq N'$ entonces $|x_n - x_m|_p < \epsilon$. Sea $N \in \mathbb{N}$ tal que $|x_N|_p > \epsilon$ y $N \geq N'$. Para cualquier $n \geq N$ se tiene

$$\begin{aligned} & |x_n - x_N|_p < \epsilon \\ \Longrightarrow \;\; & ||x_n| - |x_N||_{\mathbb{R}} \leq |x_n - x_N|_p < \epsilon \\ \Longrightarrow \;\; & -\epsilon < |x_n|_p - |x_N|_p < \epsilon \\ \Longrightarrow \;\; & |x_N|_p - \epsilon < |x_n|_p. \end{aligned}$$

Poniendo $c = |x_N|_p - \epsilon$ se cumple que $|x_n|_p > c > 0$, para todo $n \geq N$.

□

Proposición 1.11 *$\mathcal{N}$ es un ideal maximal en $\mathcal{C}$.*

Demostración Sea I un ideal de $\mathcal{C}$ tal que $\mathcal{N} \subset I$ y $\mathcal{N} \neq I$, se probará que $I = \mathcal{C}$. Como $I \neq \mathcal{N}$ existe $(x_n) \in I$ tal que $x_n \nrightarrow 0$, usando además que (x_n) es una sucesión de Cauchy, por el lema 1.7 existen $c > 0$ y $N \in \mathbb{N}$ tal que si $n \geq N$ entonces $|x_n|_p > c$. Se define (y_n) como

$$y_n = \begin{cases} 0, & \text{si } n < N, \\ \frac{1}{x_n}, & \text{si } n \geq N. \end{cases}$$

Se tiene

$$|y_{n+1} - y_n|_p = \left| \frac{1}{x_{n+1}} - \frac{1}{x_n} \right|_p = \frac{|x_n - x_{n+1}|_p}{|x_{n+1}|_p |x_n|_p} < \frac{|x_n - x_{n+1}|_p}{c^2} \ \ para \ \ n \geq N.$$

La sucesión (x_n) es de Cauchy y por la proposición 1.5 se tiene $\lim_{n\to\infty} |x_{n+1} - x_n|_p = 0$,

$$\Longrightarrow \lim_{n\to\infty} |y_{n+1} - y_n|_p \leq \lim_{n\to\infty} \frac{|x_n - x_{n+1}|_p}{c^2} = 0 \Longrightarrow \lim_{n\to\infty} |y_{n+1} - y_n|_p = 0.$$

Entonces por la proposición 1.5 se obtiene que (y_n) es sucesión de Cauchy.
Luego, $(x_n)(y_n) \in I$ por ser I un ideal de $\mathcal{C}$.
Por otro lado,

$$(x_n y_n) = \begin{cases} 0 & \text{si } n < N \\ 1 & \text{si } n \geq N \end{cases}$$

Entonces $1 - (x_n y_n) \in \mathcal{N}$, sea $(z_n) = 1 - (x_n y_n)$. Luego, $1 = (x_n y_n) + (z_n) \in I$ pues $(z_n), (x_n y_n) \in I$. Así, $I = \mathcal{C}$ y por tanto $\mathcal{N}$ es maximal en $\mathcal{C}$.

□

Definición 1.11 *Se define el* ***campo de los números*** $p-$***ádicos*** *como el campo*

$$\mathbb{Q}_p = \frac{\mathcal{C}}{\mathcal{N}}.$$

Observación La inclusión natural de los números racionales $\mathbb{Q}$ en $\mathbb{Q}_p$, $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$, es la función que a cada $x \in \mathbb{Q}$ le asigna la clase de equivalencia de la sucesión constante (x), esto porque dos sucesiones constantes nunca difieren por un elemento de $\mathcal{N}$.

Para extender el valor absoluto al campo $\mathbb{Q}_p$, se mostrará primero un hecho de las sucesiones de Cauchy.

Lema 1.8 *Sea $(x_n) \in \mathcal{C}$, $(x_n) \notin \mathcal{N}$. La sucesión de números reales es eventualmente estacionaria, es decir, existe un entero N tal que $|x_n|_p = |x_m|_p$ si $m, n \geq N$.*

Demostración Como (x_n) es una sucesión de Cauchy que no tiende a cero, por el lema 1.7 existen $c > 0$ y $N_1 \in \mathbb{N}$ tal que

$$n \geq N_1 \Longrightarrow |x_n|_p \geq c > 0.$$

Por otro lado, existe $N_2 \in \mathbb{N}$ tal que

$$n, m \geq N_2 \Longrightarrow |x_n - x_m|_p < c.$$

Sea $N =$máx$\{N_1, N_2\}$ si $n, m \geq N$ entonces

$$|x_n - x_m|_p < c \leq |x_n|_p \quad y \quad |x_n - x_m|_p < c \leq |x_m|_p.$$

Luego, si $n, m \geq N$ entonces $|x_n - x_m|_p <$máx$\{|x_n|_p, |x_m|_p\}$.
Como todos los triángulos son isósceles (corolario 1.1) se obtiene $|x_n|_p = |x_m|_p$ si $n, m \geq N$.

□

Definición 1.12 *Si $\lambda \in \mathbb{Q}_p$ y (x_n) es cualquier sucesión de Cauchy representante de λ, se define*

$$|\lambda|_p = \lim_{n\to\infty} |x_n|_p.$$

Observación Abusando de notación, se suele usar el mismo símbolo $(|\cdot|_p)$ para representar al valor absoluto $p-$ádico sobre $\mathbb{Q}$ y $\mathbb{Q}_p$, porque después solamente se trabajará con $\mathbb{Q}_p$.

Proposición 1.12 *El límite de la definición anterior está bien definido.*

Demostración Se tiene,

1. El límite existe pues por el lema anterior existe $N \in \mathbb{N}$ tal que $|x_n|_p = |x_m|_p$ si $m, n \geq N$. Así, $\lim_{n\to\infty} |x_n|_p = |x_N|_p$.

2. El límite no depende de la elección de la sucesión representante de λ, pues si (x_n) y (y_n) son representantes de λ entonces $(x_n) - (y_n) = (x_n - y_n) \in \mathcal{N}$.

   Sea $\epsilon > 0$, existe $N \in \mathbb{N}$ tal que si $n \geq N$ entonces $|x_n - y_n|_p < \epsilon$. De donde

$$||x_n|_p - |y_n|_p|_{\mathbb{R}} \leq |x_n - y_n|_p < \epsilon \Longrightarrow ||x_n|_p - |y_n|_p|_{\mathbb{R}} < \epsilon$$

$$\Longrightarrow \lim_{n\to\infty} |x_n|_p - |y_n|_p = 0 \Longrightarrow \lim_{n\to\infty} |x_n|_p = \lim_{n\to\infty} |y_n|_p.$$

□

Proposición 1.13 *La función $|\cdot|_p : \mathbb{Q}_p \longrightarrow \mathbb{R}^+$, definida anteriormente es un valor absoluto no arquimediano.*

Demostración Se tiene,

1. Si $|\lambda|_p = 0$ entonces $\lim_{n\to\infty} |x_n|_p = 0$ para toda sucesión representante de la clase λ. Entonces $(x_n) \in \mathcal{N}$, es decir, $\lambda = 0$.

   Por otro lado, si $\lambda = 0$ entonces para algún representante (x_n) de λ se tiene que $\lim_{n\to\infty} |x_n|_p = 0$, así $|\lambda|_p = 0$.

2. Se tiene,

$$\begin{aligned} |\lambda|_p|\beta|_p &= \lim_{n\to\infty} |x_n|_p \lim_{n\to\infty} |y_n|_p \\ &= \lim_{n\to\infty} |x_n|_p|y_n|_p \\ &= \lim_{n\to\infty} |x_n y_n|_p \\ &= |\lambda\beta|_p. \end{aligned}$$

3. Por el lema 1.8 existen naturales N_1, N_2 y N_3 tales que $|x_n|_p = |x_{N_1}|_p$ si $n \geq N_1$, $|y_n|_p = |y_{N_2}|_p$ si $n \geq N_2$ y $|x_n + y_n|_p = |x_{N_3} + y_{N_3}|_p$ si $n \geq N_3$.

   Sea $N =$máx$\{N_1, N_2, N_3\}$, entonces $|\lambda+\beta|_p = \lim_{n\to\infty} |x_n+y_n|_p = |x_N+y_N|_p$,

   $|\lambda|_p = \lim_{n\to\infty} |x_n|_p = |x_N|_p$ y $|\beta|_p = \lim_{n\to\infty} |y_n|_p = |y_N|_p$.

   Usando la desigualdad $|x_N + y_N|_p \leq$máx$\{|x_N|_p, |y_N|_p\}$ se obtiene

   $|\lambda + \beta|_p \leq$máx $\{|\lambda|_p, |\beta|_p\}$.

De $1, 2$ y 3 se concluye que $|\cdot|_p$ es un valor absoluto no arquimediano.

□

Observación De la definición se puede observar que la imagen de $\mathbb{Q}$ bajo $|\cdot|_p$ es igual a la imagen de $\mathbb{Q}_p$ bajo $|\cdot|_p$.
Además, si $x \in \mathbb{Q}$ y λ_x es su imagen bajo la inclusión, por la definición se obtiene que $|x|_p = |\lambda_x|_p$.

Proposición 1.14 *La imagen de $\mathbb{Q}$ bajo la inclusión $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ es un subconjunto denso en $\mathbb{Q}_p$.*

Demostración Sean $\epsilon > 0$ y $\lambda \in \mathbb{Q}_p$. Se construirá una sucesión constante que esta contenida en $B(\lambda, \epsilon)$.
Sea (x_n) una sucesión de Cauchy representante de λ y sea $\epsilon' > 0$ tal que $\epsilon' < \epsilon$.
Como (x_n) es de Cauchy existe $N \in \mathbb{N}$ tal que si $m, n \geq N$ entonces $|x_n - x_m| < \epsilon'$.
Sea $y = x_N$, se construye la sucesión constante (y).
Si $\beta \in \mathbb{Q}_p$ es representada por (y), se tiene que β es la imagen de $y \in \mathbb{Q}$ bajo la inclusión. Luego, $\lambda - \beta$ es representada por la sucesión $(x_n - y)$ y entonces

$$|(x_n - y)|_p = \lim_{n\to\infty} |x_n - y|_p.$$

Para $n \geq N$ se tiene $|x_n - y| = |x_n - x_N| < \epsilon'$.
Así,

$$\lim_{n\to\infty} |x_n - y|_p \leq \epsilon' < \epsilon.$$

Por tanto, $\beta \in B(\lambda, \epsilon)$.

$\square$

Proposición 1.15 *$\mathbb{Q}_p$ es completo con respecto a $|\cdot|_p$.*

Demostración Sea (λ_n) una sucesión de Cauchy de elementos de $\mathbb{Q}_p$.
Por la proposición anterior, para cada $i \in \mathbb{N}$ existe β_i que es clase de equivalencia de una sucesión constante de números racionales (y_i) y satisface

$$|\lambda_i - \beta_i|_p < \frac{1}{i}.$$

Sea $z_i = y_i$ para todo $i \in \mathbb{N}$.
Se tiene que (z_i) es una sucesión de números racionales, se probará que es sucesión de Cauchy.
Sea $\epsilon > 0$, existe $k \in \mathbb{N}$ tal que $\frac{1}{k} < \epsilon$, luego por ser (λ_n) sucesión de Cauchy existe $N \in \mathbb{N}$ tal que si $n, m \geq N$ entonces $|\lambda_n - \lambda_m|_p < \frac{1}{k}$.
Sea $N' =$máx$\{k, N\}$, usando que $\beta_n - \beta_m$ es la clase de equivalencia de la sucesión constante $(z_n - z_m) = (x_t)$, si $n, m \geq N'$ se obtiene

$$\begin{aligned}
|z_n - z_m|_p &= \lim_{t\to\infty} |x_t|_p \\
&= |\beta_n - \beta_m|_p \\
&= |\beta_n - \lambda_n + \lambda_n - \lambda_m + \lambda_m - \beta_m|_p \\
&\leq \text{máx}\{|\beta_n - \lambda_n|_p, |\lambda_n - \lambda_m|_p, |\lambda_m - \beta_m|_p\} \\
&< \text{máx}\left\{\frac{1}{n}, \frac{1}{k}, \frac{1}{m}\right\} \\
&= \frac{1}{k} \\
&< \epsilon.
\end{aligned}$$

Así, (z_n) es sucesión de Cauchy en $\mathbb{Q}$. Sea λ la clase de equivalencia de (z_n) en $\mathbb{Q}_p$, se probará que $\lim_{n\to\infty} \lambda_n = \lambda$.
Sea $\epsilon > 0$, existe $k \in \mathbb{N}$ tal que $\frac{1}{k} < \epsilon$. Como $(z_n) = (y_n)$ es sucesión de Cauchy en $\mathbb{Q}$, existe $N \in \mathbb{N}$ tal que si $m, n \geq N$ entonces $|y_m - y_n|_p < \frac{1}{k}$.
Sea $N' =$máx$\{k, N\}$, si $n \geq N'$ se tiene

$$|\lambda_n - \lambda|_p = |\lambda_n - \beta_n + \beta_n - \lambda|_p \leq \text{máx}\{|\lambda_n - \beta_n|_p, |\beta_n - \lambda|_p\}$$

como $n > k$ se cumple $|\lambda_n - \beta_n|_p < \frac{1}{n} < \frac{1}{k}$, además $|\beta_n - \lambda|_p = \lim_{m\to\infty} |z_n - z_m|_p \leq \frac{1}{k}$ pues si $m, n \geq N$ entonces $|y_m - y_n|_p < \frac{1}{k}$. Entonces,

$$|\lambda_n - \lambda|_p < \frac{1}{k} < \epsilon.$$

Así, $\lim_{n\to\infty} \lambda_n = \lambda$. Por tanto, $\mathbb{Q}_p$ es completo.

□

El siguiente teorema es muy importante, pues resume todo el trabajo relizado.

Teorema 1.4 *Para cada primo $p \in \mathbb{Z}$ existe un campo $\mathbb{Q}_p$ con un valor absoluto no arquimediano $|\cdot|_p$, tal que:*

1. *Existe una inclusión $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$, y el valor absoluto inducido por $|\cdot|_p$ sobre $\mathbb{Q}$ vía esta inclusión es un valor absoluto $p-$ádico.*

2. *La imagen de $\mathbb{Q}$ bajo esta inclusión es densa en $\mathbb{Q}_p$ (con respecto al valor absoluto $|\cdot|_p$); y*

3. *$\mathbb{Q}_p$ es completo con respecto al valor absoluto $|\cdot|_p$.*

El campo $\mathbb{Q}_p$ que satisface $1, 2$ y 3 es único salvo isomorfismos que preservan valores absolutos.

Demostración Los incisos $1, 2$ y 3 fueron probados en las proposiciones previas al teorema.
Resta ver la unicidad. Sea K un campo que satisface las condiciones $1, 2$ y 3 del teorema, entonces existe una inclusión h de $\mathbb{Q}$ en K tal que la imagen de $\mathbb{Q}$ es densa en K con respecto al valor absoluto $|\cdot|_p$.
Sea g la inclusión de $\mathbb{Q}$ en $\mathbb{Q}_p$, entonces se forma la función $f : \mathbb{Q}_p \to K$ de la siguiente manera: si $\lambda \in \mathbb{Q}_p$ entonces por la densidad de $g(\mathbb{Q})$ existe una sucesión (z_n) tal que $z_n \to \lambda$ y $z_n = g(z'_n)$ donde $z'_n \in \mathbb{Q}$ para todo $n \in \mathbb{N}$.
El valor absoluto se mantiene igual en $\mathbb{Q}$ y en $g(\mathbb{Q})$ entonces (z'_n) es sucesión de Cauchy en $\mathbb{Q}$ y luego $(h(z'_n))$ es sucesión de Cauchy en K, pues el valor absoluto se mantiene igual en K y en $h(K)$.
Como K es completo existe $k \in K$ tal que $k = \lim_{n\to\infty} h(z'_n)$. Se define $f(\lambda) = k$. Se tiene

1. Para ver f está bien definida y es inyectiva: sean $(z_n), (y_n) \subset g(\mathbb{Q})$ tal que $\lim_{n\to\infty} z_n = \lambda = \lim_{n\to\infty} y_n$. Entonces $z_n = g(z'_n)$ y $y_n = g(y'_n)$ con $z'_n, y'_n \in \mathbb{Q}$. Se tiene

$$\lim_{n\to\infty} z_n = \lambda = \lim_{n\to\infty} y_n \iff \lim_{n\to\infty} z_n - y_n = 0$$

$$\iff \lim_{n\to\infty} |g(z'_n) - g(y'_n)|_p = 0 \iff \lim_{n\to\infty} |g(z'_n) - g(y'_n)|_K = 0$$

$$\iff \lim_{n\to\infty} h(z'_n) - h(y'_n) = 0 \iff \lim_{n\to\infty} h(z'_n) = \lim_{n\to\infty} h(y'_n).$$

2. Para probar que f es sobreyectiva, sea $w \in K$, existe $(w_n) \subset h(\mathbb{Q})$ tal que $\lim_{n\to\infty} w_n = w$ y $w_n = h(w'_n)$ donde $w'_n \in \mathbb{Q}$ para todo $n \in \mathbb{N}$.

   Se tiene (w'_n) es sucesión de Cauchy en $\mathbb{Q}$ entonces $(g(w'_n))$ es sucesión de Cauchy en $\mathbb{Q}_p$. Sea $\lambda \in \mathbb{Q}_p$ tal que $\lim_{n\to\infty} g(w'_n) = \lambda$ entonces $f(\lambda) = w$.

3. Ahora se probará que f es morfismo. Por definición se tiene $f(1) = 1^*$ donde 1^* es la unidad en K.

   Luego, sean $x, y \in \mathbb{Q}_p$, existen $(g(x'_n)), g((y'_n))$ tal que

   $$\lim_{n\to\infty} g(x'_n) = x \quad \lim_{n\to\infty} g(y'_n) = y.$$

   Además,

   $$\lim_{n\to\infty} h(x'_n) = f(x) \quad \lim_{n\to\infty} h(y'_n) = f(y).$$

   Se tiene,

   $$f(x) + f(y) = \lim_{n\to\infty} h(x'_n) + \lim_{n\to\infty} h(y'_n) = \lim_{n\to\infty} h(x'_n) + h(y'_n).$$

   Por otro lado,

   $$\lim_{n\to\infty} g(x'_n) + g(y'_n) = x + y \Longrightarrow \lim_{n\to\infty} h(x'_n) + h(y'_n) = f(x) + f(y).$$

   Así, $f(x+y) = f(x) + f(y)$. Por tanto, f es morfismo.

   De manera análoga se obtiene $f(xy) = f(x)f(y)$.

De $1, 2$ y 3 se concluye que f es un isomorfismo. Para ver que f preserva valores absolutos sea $\lambda \in \mathbb{Q}_p$ entonces existe (z_n) tal que $z_n \to \lambda$ y $z_n = g(z'_n)$ donde $z'_n \in \mathbb{Q}$ para todo $n \in \mathbb{N}$. Se tiene

$$|\lambda|_p = \lim_{n\to\infty} |z_n|_p = \lim_{n\to\infty} |h(z'_n)|_K,$$

como $|\cdot|_K$ es continua (proposición 1.6) entonces $\lim_{n\to\infty} |h(z'_n)|_K = |f(\lambda)|_K$.
Así, $|\lambda|_p = |f(\lambda)|_K$.

$\square$

El teorema anterior permite fijar la atención solamente en los elementos de $\mathbb{Q}_p$ y considerar a $\mathbb{Q}$ como un subconjunto de $\mathbb{Q}_p$, exactamente igual a como se trabaja en $\mathbb{R}$.

I.2.3 El campo $\mathbb{Q}_p$

En la sección anterior se construyó para cada número primo p, el campo de los números $p-$ádicos $(\mathbb{Q}_p)$, a manera de resumen se presentan los siguientes hechos:

1. Hay un valor absoluto no arquimediano, $|\cdot|_p$, sobre $\mathbb{Q}_p$ y $\mathbb{Q}_p$ es completo respecto a este valor absoluto.

2. Existe una inclusión $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ cuya imagen es densa en $\mathbb{Q}_p$ y la restricción del valor absoluto $|\cdot|_p$ a la imagen de $\mathbb{Q}$ coincide con el valor absoluto $p-$ádico definido en $\mathbb{Q}$.

3. El conjunto de valores de $\mathbb{Q}$ y $\mathbb{Q}_p$ bajo $|\cdot|_p$ es el mismo, específicamente,

$$\begin{aligned}\{x \in \mathbb{R}^+ : x = |\lambda|_p, \lambda \in \mathbb{Q}\} &= \{x \in \mathbb{R}^+ : x = |\lambda|_p, \lambda \in \mathbb{Q}_p\} \\ &= \{p^n : n \in \mathbb{Z}\} \cup \{0\}.\end{aligned}$$

4. Como consecuencia del inciso anterior se tiene que para cada $x \in \mathbb{Q}_p$, $x \neq 0$, existe un entero $v_p(x)$ tal que $|x|_p = p^{-v_p(x)}$. En otras palabras, la valuación $p-$ádica se extiende a $\mathbb{Q}_p$.

En esta sección se presentan las propiedades de $\mathbb{Q}_p$ necesarias para el desarrollo de esta tesis.

Definición 1.13 *El **anillo de enteros** $p-$**ádicos** es el conjunto*

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}.$$

Observación Las unidades de $\mathbb{Z}_p$ son aquéllos elementos $x \in \mathbb{Z}_p$ tales que $|x|_p = 1$.

Proposición 1.16 *El anillo $\mathbb{Z}_p$ de enteros $p-$ádicos es un anillo local cuyo ideal maximal es el ideal principal $p\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq \frac{1}{p}\}$. Además, cada elemento del complemento $\mathbb{Z}_p - p\mathbb{Z}_p$ es invertible en $\mathbb{Z}_p$, siendo los únicos elementos invertibles en $\mathbb{Z}_p$.*

Demostración Se tiene,

1. Para probar que $\mathbb{Z}_p$ es subanillo de $\mathbb{Q}_p$, hay que observar lo siguiente:

   a) Sean $x, y \in \mathbb{Z}_p$ entonces $|x|_p \leq 1$ y $|y|_p \leq 1$.
   Luego, $|x-y|_p \leq$máx$\{|x|_p, |-y|_p\} =$máx$\{|x|_p, |y|_p\} \leq 1$. Así, $x-y \in \mathbb{Z}_p$.

   b) Sean $x, y \in \mathbb{Z}_p$ entonces $|xy|_p = |x|_p|y|_p \leq 1$. Así, $xy \in \mathbb{Z}_p$.

   c) $1 \in \mathbb{Z}_p$ pues $|1|_p = 1 \leq 1$.

   De $a), b)$ y $c)$ se obtiene que $\mathbb{Z}_p$ es subanillo de $\mathbb{Q}_p$.

2. Para probar que $p\mathbb{Z}_p$ es ideal de $\mathbb{Z}_p$, hay que observar lo siguiente:

   a) $0 \in p\mathbb{Z}_p$ pues $|0|_p = 0 \leq \frac{1}{p}$.

   b) Sean $x, y \in p\mathbb{Z}_p$ entonces $|x|_p \leq \frac{1}{p}$ y $|y|_p \leq \frac{1}{p}$.
   Se tiene que $|x - y|_p \leq$máx $\{|x|_p, |y|_p\} \leq \frac{1}{p}$.
   Por tanto, $(p\mathbb{Z}_p\ , +)$ es subrgrupo de $(\mathbb{Z}_p\ , +)$.

   c) Sean $r \in \mathbb{Z}_p$ y $x \in p\mathbb{Z}_p$. Se tiene

   $$|r|_p \leq 1 \Longrightarrow |rx|_p = |r|_p|x|_p \leq |x|_p \leq \frac{1}{p}.$$

   Así, $rx \in p\mathbb{Z}_p$.

   De $a)$, $b)$ y $c)$ se obtiene que $p\mathbb{Z}_p$ es un ideal de $\mathbb{Z}_p$.

3. Sea I ideal de $\mathbb{Z}_p$, se tiene que $I \subset \mathbb{Z}_p$.Si existe $z \in I$ tal que $z \notin p\mathbb{Z}_p$, entonces $|z|_p = 1$.

   Luego, la igualdad $|1|_p = |z|_p|z^{-1}|_p$ implica que $|z^{-1}|_p = 1$ por tenerse que $|z|_p = 1$. Entonces $z^{-1} \in \mathbb{Z}_p$ y por ser I ideal de $\mathbb{Z}_p$ se obtiene $1 = zz^{-1} \in I$.

   Para cualquier $x \in \mathbb{Z}_p$ se tiene que $1x \in I$, es decir, $x \in I$. Luego, $\mathbb{Z}_p \subset I$, es decir, $I = \mathbb{Z}_p$.

   Entonces cualquier ideal de $\mathbb{Z}_p$ distinto de $\mathbb{Z}_p$ consta de elementos que no son unidades de $\mathbb{Z}_p$, así esta contenido en $p\mathbb{Z}_p$.

   Por tanto, $p\mathbb{Z}_p$ es el único ideal maximal de $\mathbb{Z}_p$, es decir, $\mathbb{Z}_p$ es un anillo local.

4. Si $x \in \mathbb{Z}_p - p\mathbb{Z}_p$ entonces $|x|_p = 1$. Luego $x \neq 0$ y $x^{-1} \in \mathbb{Q}_p$. Se tiene $|x^{-1}|_p = \frac{1}{|x|_p} = 1$.

   Entonces $x^{-1} \in \mathbb{Z}_p - p\mathbb{Z}_p$. Así, cada elemento de $\mathbb{Z}_p - p\mathbb{Z}_p$ es invertible en $\mathbb{Z}_p$.

   Si $x \in p\mathbb{Z}_p$ fuera invertible se tendría que existe $y \in \mathbb{Z}_p$ tal que $xy = 1$, es decir, $|x|_p|y|_p = 1$, pero esta es una contradicción pues $|x|_p|y|_p \leq |x|_p \leq \frac{1}{p}$. Así, los únicos elementos invertibles de $\mathbb{Z}_p$ son los elementos de $\mathbb{Z}_p - p\mathbb{Z}_p$.

$\square$

La proposición anterior permite establecer la siguiente definición

Definición 1.14 *El grupo de unidades de $\mathbb{Z}_p$ es*

$$\mathbb{Z}_p^{\times} = \{x \in \mathbb{Z}_p : |x|_p = 1\}.$$

Definición 1.15 *Se define la* ***bola con centro en*** a ***y radio*** p^r *al conjunto*

$$B(a, p^r) = \{x \in \mathbb{Q}_p : |x - a|_p \leq p^r\}, \quad r \in \mathbb{Z}.$$

Observación Es irrelevante hacer distinción entre la bola abierta y la bola cerrada, pues

$$B(a,p^r) = \{x \in \mathbb{Q}_p : |x-a|_p < p^r\} = \{x \in \mathbb{Q}_p : |x-a|_p \leq p^{r-1}\} = \overline{B}(a,p^{r-1}).$$

Definición 1.16 *La **esfera con centro en** a **y radio** p^r es el conjunto*

$$S(a,p^r) = \{x \in \mathbb{Q}_p : |x-a|_p = p^r\}, \quad r \in \mathbb{Z}.$$

Proposición 1.17 *Se cumple lo siguiente:*

1. *$B(a,p^r)$ es un conjunto abierto y cerrado.*
2. *Si $b \in B(a,p^r)$ entonces $B(a,p^r) = B(b,p^r)$.*
3. *Si $a, b \in \mathbb{Q}_p$ entonces $B(a,p^r) \cap B(b,p^s) \neq \emptyset$ si y sólo si $B(a,p^r) \subset B(b,p^s)$ ó $B(b,p^s) \subset B(a,p^r)$.*

Demostración Se tiene,

1. El conjunto $B(a,p^r)$ es abierto por definición de abierto en un espacio métrico. Para probar que $B(a,p^r)$ es un conjunto cerrado, sea $c \notin B(a,p^r)$, entonces $|c-a|_p > p^r$. Sea $B(c,|c-a|_p - p^r)$, para cualquier $z \in B(c,|c-a|_p - p^r)$ se tiene
$$|a-z|_p \leq \text{máx}\{|a-c|_p, |z-c|_p\}.$$
Como todos los triángulos son isósceles, entonces
$$|a-z|_p = \text{máx}\{|a-c|_p, |z-c|_p\}.$$
Luego, $|a-z|_p = |a-c|_p > p^r$. Así, $B(c,|c-a|_p - p^r) \subset B(a,p^r)^c$.
Por tanto, $B(a,p^r)$ es un conjunto cerrado.

2. Sea $x \in B(a,p^r)$ entonces $|x-a| \leq p^r$.
$$\Longrightarrow |x-b|_p = |(x-a)+(a-b)|_p \leq \text{máx}\{|x-a|_p, |b-a|_p\} \leq p^r$$
$$\Longrightarrow x \in B(b,p^r) \Longrightarrow B(a,p^r) \subset B(b,p^r).$$
Análogamente se obtiene $B(b,p^r) \subset B(a,p^r)$.
Así, $B(a,p^r) = B(b,p^r)$.

3. Si $B(a,p^r) \cap B(b,p^s) \neq \emptyset$ entonces existe $c \in B(a,p^r) \cap B(b,p^s)$.

   Por 1, se tiene que $B(c,p^r) = B(a,p^r)$ y $B(c,p^s) = B(b,p^s)$.

   Sin pérdida de generalidad sea $p^r \leq p^s$

$$\Longrightarrow B(c,p^r) \subset B(c,p^s) \Longrightarrow B(a,p^r) \subset B(b,p^s).$$

   Así, $B(a,p^r) \subset B(b,p^s)$.

   Reciprocamente, las contenciones implican que la intersección es distinta del vacío.

$\square$

Proposición 1.18 *Sean $a \in \mathbb{Q}_p$ y $n \in \mathbb{Z}$, los conjuntos $a + p^n\mathbb{Z}_p$ son bolas en $\mathbb{Q}_p$, es decir, $a + p^n\mathbb{Z}_p = B(a,p^{-n})$.*

Demostración Se tiene $x \in a + p^n\mathbb{Z}_p \Longleftrightarrow x = a + p^n y$ con $y \in \mathbb{Z}_p \Longleftrightarrow x - a = p^n y \Longleftrightarrow |x-a|_p \leq p^{-n} \Longleftrightarrow x \in B(a,p^{-n})$.

$\square$

Proposición 1.19 *Sea $a \in \mathbb{Q}_p$ y $n \in \mathbb{Z}$, los conjuntos $a + p^n\mathbb{Z}_p^\times$ son esferas en $\mathbb{Q}_p$, es decir, $a + p^n\mathbb{Z}_p^\times = S(a,p^{-n})$.*

Demostración Se tiene $x \in a + p^n\mathbb{Z}_p^\times \Longleftrightarrow x = a + p^n y$ con $y \in \mathbb{Z}_p^\times \Longleftrightarrow x - a = p^n y \Longleftrightarrow |x-a|_p = p^{-n} \Longleftrightarrow x \in S(a,p^{-n})$.

$\square$

Proposición 1.20 *$\mathbb{Q}_p$ es un espacio de Hausdorff totalmente disconexo.*

Demostración Todo espacio métrico es de Hausdorff, así $\mathbb{Q}_p$ es un espacio de Hausdorff.
Sea $S \neq \emptyset$ un subconjunto de $\mathbb{Q}_p$. Si $x, y \in S$ con $x \neq y$, sea $p^r = |x-y|_p$, entonces $B(x, \frac{p^r}{2})$ es un conjunto abierto y cerrado que contiene a x y no contiene a y.
Luego, $\mathbb{Q}_p - B(x, \frac{p^r}{2})$ es un conjunto abierto que contiene a y y no contiene a x. Entonces, existen dos conjuntos abiertos $B(x, \frac{p^r}{2})$ y $\mathbb{Q}_p - B(x, \frac{p^r}{2})$ distintos del vacío y cuya intersección es vacía, además

$$S = \left(S \cap B\left(x, \frac{p^r}{2}\right)\right) \cup \left(S \cap \left(\mathbb{Q}_p - B\left(x, \frac{p^r}{2}\right)\right)\right).$$

Así, S es disconexo, Luego, ningún conjunto con dos o más puntos puede ser conexo, es decir, los únicos subconjuntos conexos son de la forma $\{x\}$.
Por tanto, $\mathbb{Q}_p$ es totalmente disconexo.

$\square$

Proposición 1.21 *La inclusión $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ tiene una imagen densa. En particular, dado $x \in \mathbb{Z}_p$ y $n \geq 1$ existe $\alpha \in \mathbb{Z}$ con $0 \leq \alpha \leq p^n - 1$, tal que $|x - \alpha|_p \leq p^{-n}$. El entero α con estas propiedades es único.*
Para cualquier $x \in \mathbb{Z}_p$ existe una sucesión de Cauchy α_n que converge a x con las siguientes caracteristicas:

(i) *$\alpha_n \in \mathbb{Z}$ para todo n y $0 \leq \alpha_n \leq p^n - 1$.*

(ii) *Para cada n se tiene $\alpha_n \equiv \alpha_{n-1} \pmod{p^{n-1}}$.*

La sucesión (α_n) con estas propiedades es única.

Demostración Se tiene,

1) Por las propiedades de $|\cdot|_p$ basta verificar que cada bola centrada en un entero $p-$ádico y de radio p^{-n} con $n \in \mathbb{N}$ contiene un entero. Sea $x \in \mathbb{Z}_p$ y $n \in \mathbb{N}$.

   Como $\mathbb{Q}$ es denso en $\mathbb{Q}_p$, existe $\frac{a}{b} \in \mathbb{Q}$, con m.c.d$(a, b) = 1$, tal que $|x - \frac{a}{b}|_p \leq p^{-n} < 1$. Además,

$$\left|\frac{a}{b}\right|_p = \left|\frac{a}{b} - x + x\right|_p \leq \text{máx}\left\{|x|_p, \left|x - \frac{a}{b}\right|_p\right\} \leq 1,$$

   esto implica que $p \nmid b$.

   Como $p \nmid b$ entonces $p^n \nmid b$ y en consecuencia $(p^n, b) = 1$. Luego, existen $b', c \in \mathbb{Z}$ tal que $bb' + cp^n = 1$. Esto implica que $bb' \equiv 1 \pmod{p^n}$. Entonces

$$\left|\frac{a}{b} - ab'\right|_p = \left|\frac{a - abb'}{b}\right|_p = \left|\frac{a(1 - bb')}{b}\right|_p$$

   usando el hecho de que $p \nmid b$ y $p^n | 1 - bb'$ se obtiene

$$\frac{a(1 - bb')}{b} = p^t \frac{a'}{b} \quad t \geq n \Longrightarrow \left|\frac{a(1 - bb')}{b}\right|_p \leq \frac{1}{p^n}$$

$$\Longrightarrow |x - ab'|_p = \left|x - \frac{a}{b} + \frac{a}{b} - ab'\right|_p \leq \text{máx}\{\left|x - \frac{a}{b}\right|_p, \left|\frac{a}{b} - ab'\right|_p\} \leq p^{-n}.$$

   Así, ab' es un entero contenido en $B(x, p^{-n})$. Por tanto, la imagen de $\mathbb{Z}$ es densa en $\mathbb{Z}_p$.

   Para la segunda parte, sea α el único entero que satisface $0 \leq \alpha \leq p^n - 1$ y $\alpha \equiv ab' \pmod{p^n}$, se tiene

$$|x - \alpha|_p \leq |x - ab' + ab' - \alpha|_p \leq \text{máx}\{|x - ab'|_p, |ab' - \alpha|_p\} \leq p^{-n}.$$

   Así, α es el único entero que satisface $0 \leq \alpha \leq p^n - 1$ y $|x - \alpha|_p \leq p^{-n}$.

2) Sea $x \in \mathbb{Z}_p$, usando lo probado en $1)$, se tiene que para todo $n \in \mathbb{N}$ existe un único α_n que satisface

$$0 \leq \alpha_n \leq p^n - 1 \quad y \quad |x - \alpha_n|_p \leq p^{-n}.$$

Sea (α_n) la sucesión descrita. Se tiene

$$|\alpha_{n+1} - \alpha_n|_p = |\alpha_{n+1} - x + x - \alpha_n|_p \leq \text{máx}\{|\alpha_{n+1} - x|_p, |x - \alpha_n|_p\} = p^{-n}$$

$$\Longrightarrow \lim_{n\to\infty} |\alpha_{n+1} - \alpha_n|_p \leq \lim_{n\to\infty} p^{-n} = 0 \Longrightarrow \lim_{n\to\infty} |\alpha_{n+1} - \alpha_n|_p = 0.$$

Luego, por el lema 1.5 se tiene que (α_n) es de Cauchy. Por otro lado

$$|x - \alpha_n|_p \leq p^{-n} \quad \forall n \in \mathbb{N} \Longrightarrow \lim_{n\to\infty} |x - \alpha_n| = 0 \Longrightarrow \lim_{n\to\infty} \alpha_n = x.$$

La sucesión (α_n) satisface (i) por como fue escogida. Además, por como se escogio la sucesión se tiene que

$$|\alpha_n - \alpha_{n-1}|_p = |\alpha_n - x + x - \alpha_{n-1}|_p \leq \text{máx}\{|\alpha_n - x|_p, |x - \alpha_{n-1}|_p\} = p^{-(n-1)},$$

esto último implica $\alpha_n \equiv \alpha_{n-1} \pmod{p^{n-1}}$.Así, se satisface (ii).

Por último, la unicidad en $1)$ garantiza la unicidad de (α_n).

$\square$

Corolario 1.4 *Sea $n \in \mathbb{N}$ se tiene*

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

Demostración Para $x \in \mathbb{Z}_p$ sea $\alpha_x \in \mathbb{Z}$ el único entero que cumple $|x - \alpha_x|_p \leq p^{-n}$ y $0 \leq \alpha_x \leq p^n - 1$. Se define

$$f : \mathbb{Z}_p / p^n\mathbb{Z}_p \longrightarrow \mathbb{Z} / p^n\mathbb{Z}.$$

como

$$f(x + p^n\mathbb{Z}_p) = \alpha_x + p^n\mathbb{Z}.$$

<u>f esta bien definida:</u>
Si $x + p^n\mathbb{Z}_p = y + p^n\mathbb{Z}_p$ entonces $x - y \in p^n\mathbb{Z}_p$, es decir, $|x - y|_p \leq p^{-n}$

$$\Longrightarrow |\alpha_x - \alpha_y|_p = |\alpha_x - x + y - \alpha_y + x - y|_p \leq \text{máx}\{|\alpha_x - x|_p, |y - \alpha_y|_p, |x - y|_p\} = p^{-n}$$

$\Longrightarrow \alpha_x \equiv \alpha_y \pmod{p^n} \Longrightarrow \alpha_x + p^n\mathbb{Z} = \alpha_y + p^n\mathbb{Z} \Longrightarrow f(x+p^n\mathbb{Z}_p) = f(y+p^n\mathbb{Z})$.

<u>f es biyección:</u>

f es inyectiva pues

$$f(x+p^n\mathbb{Z}_p) = f(y+p^n\mathbb{Z}) \Longrightarrow \alpha_x + p^n\mathbb{Z} = \alpha_y + p^n\mathbb{Z} \Longrightarrow \alpha_x \equiv \alpha_y \pmod{p^n}.$$

Luego,

$$|x-y|_p = |x-\alpha_x+\alpha_x-\alpha_y+\alpha_y-y|_p \leq \text{máx}\{|x-\alpha_x|_p, |\alpha_x-\alpha_y|_p, |\alpha_y-y|_p\} \leq p^{-n}$$

$$\Longrightarrow x-y \in p^n\mathbb{Z}_p \Longrightarrow x+p^n\mathbb{Z}_p = y+p^n\mathbb{Z}_p.$$

f es sobreyectiva pues para cualquier $k+p^n\mathbb{Z}$ se tiene $f(k+p^n\mathbb{Z}_p) = k+p^n\mathbb{Z}$.

<u>f es homomorfismo:</u>

1. Se tiene que $f(1+p^n\mathbb{Z}_p) = 1+p^n\mathbb{Z}$.
2. Se tiene que $f(x+p^n\mathbb{Z}_p+y+p^n\mathbb{Z}_p) = f(x+y+p^n\mathbb{Z}_p) = \alpha_{x+y}+p^n\mathbb{Z} = \alpha_x+\alpha_y+p^n\mathbb{Z} = f(x+p^n\mathbb{Z}_p)+f(y+p^n\mathbb{Z}_p)$.

   La cadena de igualdades se justifica por lo siguiente

$$\begin{aligned} |\alpha_x+\alpha_y-\alpha_{x+y}|_p &= |\alpha_x-x+\alpha_y-y+x+y-\alpha_{x+y}|_p \\ &\leq \text{máx}\{|\alpha_x-x|_p, |\alpha_y-y|_p, |x+y-\alpha_{x+y}|_p\} \\ &\leq p^{-n} \end{aligned}$$

$$\Longrightarrow \alpha_x+\alpha_y \equiv \alpha_{x+y} \pmod{p^n} \Longrightarrow \alpha_{x+y}+p^n\mathbb{Z} = \alpha_x+\alpha_y+p^n\mathbb{Z}.$$

3. Se tiene $f((x+p^n\mathbb{Z}_p)(y+p^n\mathbb{Z}_p)) = f(xy+p^n\mathbb{Z}_p) = \alpha_{xy}+p^n\mathbb{Z} = \alpha_x\alpha_y+p^n\mathbb{Z} = f(x+p^n\mathbb{Z}_p)f(y+p^n\mathbb{Z}_p)$.

   La cadena de igualdades se justifica usando

$$\begin{aligned} |\alpha_{xy}-\alpha_x\alpha_y|_p &= |\alpha_{xy}-xy+xy-y\alpha_x+y\alpha_x-\alpha_x\alpha_y|_p \\ &\leq \text{máx}\{|\alpha_{xy}-xy|_p, |y|_p|x-\alpha_x|_p, |\alpha_x|_p|y-\alpha_y|_p\} \\ &\leq p^{-n} \end{aligned}$$

$$\Longrightarrow \alpha_x\alpha_y \equiv \alpha_{xy} \pmod{p^n} \Longrightarrow \alpha_{xy}+p^n\mathbb{Z} = \alpha_x\alpha_y+p^n\mathbb{Z}.$$

$\square$

Corolario 1.5 *Las esferas son conjuntos abiertos y cerrados.*

Demostración Por la proposición 1.16 se tiene que $\mathbb{Z}_p^\times = \mathbb{Z}_p - p\mathbb{Z}_p$, el corolario 1.4 afirma que si $n \in \mathbb{N}$ entonces $\mathbb{Z}_p / p^n\mathbb{Z}_p \cong \mathbb{Z} / p^n\mathbb{Z}$.
Esto implica que los números $0, 1, 2, \cdots, p^n - 1$ son representantes de las clases de $\mathbb{Z}_p / p^n\mathbb{Z}_p$, es decir,

$$\mathbb{Z}_p = \bigsqcup_{i=0}^{p^n-1} i + p^n\mathbb{Z}_p \Longrightarrow \mathbb{Z}_p^\times = \bigsqcup_{i=1}^{p-1} i + p\mathbb{Z}_p.$$

Usando la proposición 1.19 se obtiene

$$S(a, p^n) = a + p^{-n}\mathbb{Z}_p^\times = \bigsqcup_{i=1}^{p-1} a + ip^{-n} + p^{-(n-1)}\mathbb{Z}_p = \bigsqcup_{i=1}^{p-1} B(a + ip^{-n}, p^{-(n-1)}).$$

Así, $S(a, p^n)$ es un conjunto abierto y cerrado, para cada $a \in \mathbb{Q}_p$ y $n \in \mathbb{Z}$, pues las bolas son conjuntos abiertos y cerrados.

□

Los siguientes resultados serán de mucha utilidad cuando sea necesario introducir un proceso de integración en $\mathbb{Q}_p$.

Proposición 1.22 *$\mathbb{Z}_p$ es compacto.*

Demostración Como $\mathbb{Z}_p = B(0, 1)$ es un conjunto cerrado y además $\mathbb{Z}_p \subset \mathbb{Q}_p$ que es un conjunto completo entonces $\mathbb{Z}_p$ es completo.
Por otro lado, por el corolario 1.4 si $n \in \mathbb{N}$ entonces $\mathbb{Z}_p / p^n\mathbb{Z}_p \cong \mathbb{Z} / p^n\mathbb{Z}$.
Entonces, los números $0, 1, 2, \cdots, p^n - 1$ son representantes de las clases de $\mathbb{Z}_p / p^n\mathbb{Z}_p$, es decir,

$$\mathbb{Z}_p = \bigsqcup_{i=0}^{p^n-1} i + p^n\mathbb{Z}_p \Longrightarrow \mathbb{Z}_p = \bigsqcup_{i=0}^{p^n-1} B(i, p^n),$$

por la proposición 1.18. Luego, para cualquier $\epsilon > 0$ existe $n \in \mathbb{N}$ tal que $p^{-n} < \epsilon$ y se obtiene

$$\mathbb{Z}_p = \bigsqcup_{i=0}^{p^n-1} B(i, p^n) \subset \bigcup_{i=0}^{p^n-1} B(i, \epsilon).$$

Así, $\mathbb{Z}_p$ es totalmente acotado.
Como $\mathbb{Z}_p$ es completo y totalmente acotado, por el teorema de Heine Borel se concluye que $\mathbb{Z}_p$ es compacto.

□

Proposición 1.23 *Las esferas y las bolas son conjuntos compactos.*

Demostración Para cualquier $n \in \mathbb{Z}$ y $a \in \mathbb{Q}_p$ se tiene que $B(a, p^n) = a + p^{-n}\mathbb{Z}_p$.
Sea $h : \{p^{-n}\} \times \mathbb{Z}_p \longrightarrow \mathbb{Q}_p$ definida por $h((x, y)) = xy$.
Se tiene que h es la operación producto restringida al conjunto $\{p^{-n}\} \times \mathbb{Z}_p$ y como la operación producto es continua se obtiene que h es continua.
Luego, $B(0, p^n) = h(\{p^{-n}\} \times \mathbb{Z}_p)$, entonces $B(0, p^n)$ es un compacto pues es la imagen continua de un compacto.
Sea $g : \{a\} \times p^{-n}\mathbb{Z}_p \longrightarrow \mathbb{Q}_p$ definida por $h((x, y)) = x + y$.
Se tiene que g es la operación suma restringida al conjunto $\{a\} \times p^{-n}\mathbb{Z}_p$ y como la operación suma es continua se obtiene que g es continua.
Luego, $B(a, p^n) = g(\{a\} \times p^{-n}\mathbb{Z}_p)$, entonces $B(a, p^n)$ es un compacto pues es la imagen continua de un compacto.
Así, las bolas son conjuntos compactos.
De mamera análoga se prueba que las esferas son conjuntos compactos.

□

Corolario 1.6 *$\mathbb{Q}_p$ es localmente compacto.*

Demostración Para $a \in \mathbb{Q}_p$, basta con tomar $B(a, 1)$ que es un conjunto compacto por la proposición anterior.

□

De la misma manera a como se obtuvieron los resultados anteriores, se obtienen

Proposición 1.24 *$\mathbb{Z}_p^\times$ es compacto.*

Proposición 1.25 *$\mathbb{Q}_p^\times$ es localmente compacto.*

Para finalizar la subsección, se muestra la forma de representar un número $p-$ádico como una serie de potencias, es importante conocer esta forma pues permite operar con estos números.

Proposición 1.26 *Cada $x \in \mathbb{Z}_p$ puede escribirse en la forma*

$$x = b_0 + b_1 p + b_2 p^2 + \cdots + b_n p^n + \cdots$$

con $0 \leq b_i \leq p - 1$. Además, esta representación es única.

Demostración Sea $x \in \mathbb{Z}_p$, por la proposición 1.21, existe una sucesión de Cauchy (α_n) que converge a x, y satisface

1. $\alpha_n \in \mathbb{Z}$ y además $0 \leq \alpha_n \leq p^n - 1$.
2. $\alpha_n \equiv \alpha_{n-1} \pmod{p^{n-1}}$.

La sucesión con estas propiedades es única. Poniendo los α_n en base p se obtiene una serie de la siguiente manera

1. $\alpha_1 = b_0$ donde $0 \leq b_0 \leq p-1$.

2. $\alpha_2 = b_0' + b_1 p$ con $0 \leq b_0', b_1 \leq p-1$ y $0 \leq \alpha_2 \leq p^2 - 1$.

   Como $\alpha_2 \equiv \alpha_1 \pmod{p}$ entonces $b_1 p + b_0' \equiv b_0 \pmod{p}$, luego $b_0' \equiv b_0 \pmod{p}$.

   Esto implica que $b_0' = b_0$ y así $\alpha_2 = b_0 + b_1 p$.

3. En general se tiene que si

   $\alpha_{n+1} = b_0' + b_1' p + b_2' p^2 + \cdots + b_n' p^n$ con $0 \leq b_i' \leq p-1$ y $0 \leq \alpha_{n+1} \leq p^{n+1} - 1$

   $\alpha_{n+1} = b_0 + b_1 p + b_2 p^2 + \cdots + b_{n-1} p^{n-1}$ con $0 \leq b_i \leq p-1$ y $0 \leq \alpha_n \leq p^n - 1$

   Como $\alpha_{n+1} \equiv \alpha_n \pmod{p^n}$ entonces

$$b_0' + b_1' p + b_2' p^2 + \cdots + b_n' p^n \equiv b_0 + b_1 p + b_2 p^2 + \cdots + b_{n-1} p^{n-1} \pmod{p^n}$$

$$\begin{array}{rrcl} \Longrightarrow & b_0 + b_1 p + b_2 p^2 + \cdots + b_{n-1} p^{n-1} & = & b_0' + b_1' p + b_2' p^2 + \cdots + b_n' p^n \\ \Longrightarrow & b_i & = & b_i' \quad \forall i : 1, ..., n-1. \end{array}$$

Asi, se obtiene

$$\begin{array}{cc} \alpha_1 = b_0 & 0 \leq b_0 \leq p-1 \\ \alpha_2 = b_0 + b_1 p & 0 \leq b_1 \leq p-1 \\ \alpha_3 = b_0 + b_1 p + b_2 p^2 & 0 \leq b_2 \leq p-1 \\ \vdots & \vdots \\ \alpha_n = b_0 + b_1 p + b_2 p^2 + \cdots + b_{n-1} p^{n-1} & 0 \leq b_{n-1} \leq p-1 \\ \alpha_{n-1} = b_0 + b_1 p + b_2 p^2 + \cdots + b_{n-1} p^{n-1} + b_n p^n & 0 \leq b_n \leq p-1 \\ \vdots & \vdots \end{array}$$

Como las sumas parciales de la serie recién construida son los α_n que convergen a x se cumple que la serie construida converge a x. Así, x puede escribirse en la forma

$$x = b_0 + b_1 p + b_2 p^2 + \cdots + b_n p^n + \cdots$$

con $0 \leq b_i \leq p-1$. La unicidad se obtiene de la unicidad de la sucesión (α_n).

$\square$

Corolario 1.7 *Cada $x \in \mathbb{Q}_p$ puede ser escrito en la forma*

$$x = b_{-n_0} p^{-n_0} + b_{-n_0+1} p^{-n_0+1} + \cdots + b_0 + b_1 p + \cdots + b_n p^n + \cdots = \sum_{n \geq -n_0} b_n p^n$$

con $0 \leq b_n \leq p-1$ y $b_{-n_0} \neq 0$. Esta representación es única y además $v_p(x) = -n_0$.

Demostración Sea $x \in \mathbb{Q}_p$.
Si $x \in \mathbb{Z}_p$ entonces por la proposición anterior

$$x = b_0 + b_1 p + b_2 p^2 + \cdots + b_n p^n + \cdots$$

con $0 \leq b_i \leq p-1$ y esta representación es única.
Por otro lado, sea n_k el menor entero positivo tal que $b_{n_k} \neq 0$ se tiene

$$x = \sum_{n \geq n_k} b_n p^n = b_{n_k} p^{n_k} + \sum_{n \geq n_k + 1} b_n p^n$$

$$\begin{array}{rrcl}
\Longrightarrow & |x|_p & = & \left|\sum_{n \geq n_k} b_n p^n\right|_p \\
 & & \leq & \text{máx}\left\{|b_{n_k} p^{n_k}|_p, \left|\sum_{n \geq n_k+1} b_n p^n\right|_p\right\} \\
\Longrightarrow & |x|_p & = & \text{máx}\left\{p^{-n_k}, \left|\sum_{n \geq n_k} b_n p^n\right|_p\right\} \\
\Longrightarrow & |x|_p & = & p^{-n_k} \\
\Longrightarrow & v_p(x) & = & n_k.
\end{array}$$

Si $x \notin \mathbb{Z}_p$, sea $n_0 = -v_p(x)$ se tiene que $n_0 \in \mathbb{Z}$, $n_0 \geq 0$ y además $xp^{n_0} \in \mathbb{Z}_p$. Luego,

$$xp^{n_0} = \sum_{n \geq 0} b_n p^n$$

con $b_0 \neq 0$. Entonces

$$x = p^{-n_0} \sum_{n \geq 0} b_n p^n = \sum_{n \geq -n_0} b_n p^n.$$

La unicidad de la representación se deduce de la unicidad de xp^{n_0} y además se tiene $v_p(x) = -n_0$.

□

Ejemplo 1.3 *Se tiene que*

$$-1 = (p-1) + (p-1)p + (p-1)p^2 + \cdots$$

Esto por que tomando sumas parciales se obtiene

$$s_n = (p-1) + (p-1)p + (p-1)p^2 + \cdots + (p-1)p^n = (p-1)\frac{p^{n+1}-1}{p-1} = p^{n+1} - 1.$$

Luego,

$$\lim_{n \to \infty} s_n = \lim_{n \to \infty} p^{n+1} + \lim_{n \to \infty} -1 = -1$$

pues

$$\lim_{n \to \infty} |p^{n+1}|_p = \lim_{n \to \infty} p^{-n-1} = 0 \Longrightarrow \lim_{n \to \infty} p^{n+1} = 0.$$

Ejemplo 1.4 *En el ejemplo anterior se obtuvo*

$$-1 = (p-1)\sum_{i=1}^{\infty} p^i.$$

Esto implica que

$$\frac{1}{1-p} = \sum_{i=1}^{\infty} p^i.$$

I.2.4 Lema de Hensel

Para decidir si un número como $\sqrt{6}$ pertenece a $\mathbb{Q}_5$, la manera que se tiene hasta el momento es buscar "a mano"una representación en series de potencias del $\sqrt{6}$, es decir, es necesario encontrar una sucesión de dígitos $5-$ádicos: $a_0, a_1, a_2, \cdots$ con $0 \leq a_i \leq 4$, tal que

$$(a_0 + a_1 5 + a_2 5^2 + \cdots)^2 = 1 + 1 \cdot 5.$$

Ecuaciones de este tipo, $(x^2 - 6 = 0)$, pueden resolverse utilizando un resultado conocido como "lema de Hensel".

Definición 1.17 *Sean $a, b \in \mathbb{Q}_p$, decimos que a, b son **congruentes módulo** p^n y se escribe $a \equiv b \pmod{p^n}$ si y sólo si $|a-b|_p \leq \frac{1}{p^n}$.*

Teorema 1.5 (Lema de Hensel) *Sea $F(x) = c_0 + c_1 x + \cdots + c_n x^n$ un polinomio cuyos coeficientes son enteros $p-$ádicos. Sea $F'(x) = c_1 + 2c_2 x + 3c_3 x^2 + \cdots + c_n x^{n-1}$ la derivada formal de $F(x)$. Si $\overline{a_0}$ es un entero $p-$ádico que satisface $F(\overline{a_0}) \equiv 0 \pmod{p}$ y $F'(\overline{a_0}) \not\equiv 0 \pmod{p}$ entonces existe un entero $p-$ádico a tal que $F(a) = 0$ y $a \equiv \overline{a_0} \pmod{p}$.*

Demostración Se prueba por inducción el siguiente enunciado:
$s(k)$: Existe un entero $p-$ádico de la forma

$$a_k = b_0 + b_1 p + \cdots + b_k p^k$$

con $b_i \in \{0, 1, \cdots, p-1\}$ $\forall i$, tal que $F(a_k) \equiv 0 \pmod{p^{k+1}}$ y $a_k \equiv \overline{a_0} \pmod{p}$.

1. Para $k = 0$ basta con tomar b_0 igual al primer dígito $p-$ádico de $\overline{a_0}$, luego se tiene $F(a_0) \equiv 0 \pmod{p}$ y $a_0 \equiv \overline{a_0} \pmod{p}$.

2. Asumiendo que se cumple $s(k-1)$.

   Sea $a_k = a_{k-1} + b_k p^k$ para algún dígito b_k, por determinar. Se tiene

$$\begin{aligned} F(a_k) &= F(a_{k-1} + b_k p^k) \\ &= \sum_{i=0}^{n} c_i (a_{k-1} + b_k p^k)^i \\ &= c_0 + \sum_{i=1}^{n} c_i (a_{k-1}^i + i a_{k-1}^{i-1} b_k p^k + p^{k+1} t) \\ &\equiv F(a_{k-1}) + b_k p^k F'(a_{k-1}) \pmod{p^{k+1}}. \end{aligned}$$

Por hipótesis de inducción $F(a_{k-1}) \equiv 0 \pmod{p^k}$, entonces

$$F(a_k) \equiv \alpha_k p^k + b_k p^k F'(a_{k-1}) \pmod{p^{k+1}}$$

para algún entero $\alpha_k \in \{0, 1, \cdots, p-1\}$.

Luego, se busca que se cumpla $\alpha_k + b_k F'(a_{k-1}) \equiv 0 \pmod{p}$, como $a_{k-1} \equiv \overline{a_0} \pmod{p}$ entonces $F'(a_{k-1}) \equiv F'(\overline{a_0}) \not\equiv 0 \pmod{p}$.

Entonces $\alpha_k + b_k F'(a_{k-1}) \equiv 0 \pmod{p}$ esto implica $b_k \equiv \frac{-\alpha_k}{F'(a_{k-1})} \pmod{p}$. Así, $F(a_k) \equiv 0 \pmod{p^{k+1}}$. Completando el proceso de inducción.

Ahora sea $a = b_0 + b_1 p + b_2 p^2 + \cdots$, se tiene que $F(a) = 0$ pues para todo k se obtiene $F(a) \equiv F(a_k) \equiv 0 \pmod{p^{k+1}}$.

La unicidad de a se sigue de la unicidad de la sucesión (a_k).

□

Ejemplo 1.5 *Para decidir si $x^2 - 6 = 0$ tiene solución en $\mathbb{Q}_5$ se define $F(x) = -6 + x^2$, entonces $F'(x) = 2x$. Tomando $\overline{a_0} = 1$ se obtiene*

$$F(1) = 1 - 6 = 5 \equiv 0 \pmod{5} \quad y \quad F'(1) = 2 \not\equiv 0 \pmod{5}.$$

Entonces existe un entero $5-$ádico a tal que $F(a) = a^2 - 6 = 0$, es decir, $a^2 = 6$. Así, $\sqrt{6}$ pertenece a $\mathbb{Q}_5$.

Algunas consecuencias del lema de Hensel, son las siguientes

Proposición 1.27 *Un polinomio con coeficientes enteros tiene una raíz en $\mathbb{Z}_p$ si y sólo si tiene una raíz módulo p^k para cualquier $k \geq 1$.*

Demostración Sea $F(x)$ un polinomio con coeficientes en $\mathbb{Z}$.
Supóngase que $a \in \mathbb{Z}_p$ es raíz, es decir, $F(a) = 0$.
Luego, existe una sucesión $\{a_1, a_2, \cdots, a_k, \cdots\}$ donde

$$a_k = b_0 + b_1 p + b_2 p^2 + \cdots + b_{k-1} p^{k-1}$$

tal que

$$a \equiv a_k \pmod{p^k}.$$

Entonces $F(a_k) \equiv F(a) \pmod{p^k}$ y $F(a) = 0$.

$$\Longrightarrow F(a_k) \equiv 0 \pmod{p^k}.$$

Reciprocamente, supóngase que $F(x) \equiv 0 \pmod{p^k}$ tiene una solución a_k para cualquier $k \geq 1$.
Como $\mathbb{Z}_p$ es compacto entonces es secuencialmente compacto, luego la sucesión $\{a_k\}$ contiene una subsucesión $\{a_{k_i}\}$ convergente. Sea

$$a = \lim_{i \to \infty} a_{k_i}.$$

$F(x)$ es una función continua pues es un polinomio, entonces

$$F(a) = \lim_{i \to \infty} F(a_{k_i}).$$

Por otro lado,

$$F(a_{k_i}) \equiv 0 \pmod{p^{k_i}}.$$

Así,

$$\lim_{i \to \infty} F(a_{k_i}) = 0$$

y por tanto, $F(a) = 0$.

□

Proposición 1.28 *Un entero racional a no divisible por p tiene una raíz cuadrada en $\mathbb{Z}_p$ $(p \neq 2)$ si y sólo si a es un residuo cuadrático módulo p.*

Demostración Sea $P(x) = x^2 - a$, entonces $P'(x) = 2x$.
Por el teorema anterior, si $P(x)$ tiene una raíz en $\mathbb{Z}_p$ entonces $x^2 \equiv a \pmod{p}$ tiene solución, es decir, a es un residuo cuadrático módulo p.

Reciprocamente, si a es un residuo cuadrático módulo p, entonces

$$a \equiv a_0^2 \pmod{p}$$

para algún $a_0 \in \{1, 2, \cdots, p-1\}$.

$$\Longrightarrow P(a) \equiv 0 \pmod{p}.$$

Como $P'(a) = 2a \not\equiv 0 \pmod{p}$ por el Lema de Hensel existe $a_0 \in \mathbb{Z}_p$ tal que $a_0^2 - a = 0$, es decir, $a_0^2 = a$.

□

Ejemplo 1.6 *El número* $\sqrt{-1}$ *pertenece a* $\mathbb{Z}_5$ *por que* $-1 = 4 - 5 \equiv 2^2 \pmod 5$*, es decir,* -1 *es un residuo cuadrático* $\pmod 5$.
Sin embargo, $\sqrt{-1}$ *no pertenece a* $\mathbb{Z}_3$ *por que* $-1 \equiv 2 \pmod 3$ *que no es un residuo cuadrático* $\pmod 3$.

I.2.5 Integración en $\mathbb{Q}_p$

En $\mathbb{Q}_p$ existe una medida que es una generalización de la medida de Lebesgue en $\mathbb{R}^n$, aqui se presentan los resultados necesarios para el desarrollo de este trabajo, algunos sin demostración, un estudio más profundo de este tema se puede consultar en [10].

Teorema 1.6 *Sea* $(G, *)$ *un grupo topológico localmente compacto. Existe una medida regular de Borel, única salvo multiplicación por constantes positivas, tal que*

1. $\int_U dx > 0$ *para cada conjunto abierto de Borel* U *distinto del vacío, y*
2. $\int_{x*E} dx = \int_E dx$ *para cada conjunto de Borel.*

Una prueba de este teorema puede consultarse en [10].

Definición 1.18 *La medida* dx *descrita en el teorema anterior es una* ***Medida de Haar*** *sobre* G.

Por lo visto en las secciones anteriores se tiene que $(\mathbb{Q}_p, +)$ es un grupo topológico abeliano localmente compacto, así que existe una medida de Haar dx sobre $(\mathbb{Q}_p, +)$. Por otro lado, $\mathbb{Z}_p$ es compacto y por ser dx una medida regular se obtiene

$$\int_{\mathbb{Z}_p} dx < \infty.$$

Así, se puede normalizar esta medida por la condición

$$\int_{\mathbb{Z}_p} dx = 1$$

y entonces dx es única.
Los abiertos compactos de $\mathbb{Q}_p$, e.g. $a + p^m\mathbb{Z}_p$, generan la $\sigma-$álgebra de Borel.
La medida dx asigna a cada subconjunto abierto compacto U un número real no negativo $\int_U dx$, que además satisface

$$\int_{\cup_{n=1}^{\infty} U_n} dx = \sum_{n=1}^{\infty} \int_{U_n} dx,$$

para todos los subconjuntos abiertos compactos U_n en $\mathbb{Q}_p$, que son disjuntos por parejas, tales que $\cup_{n=1}^{\infty} U_n$ es igualmente compacto. También cumple,

$$\int_{x_0+U} dx = \int_U dx.$$

La siguiente fórmula es de gran utilidad en el proceso de integración pues permite hacer cambio de variables.

Proposición 1.29 *Sea $d(xa)$ definida por $d(ax)(U) = dx(aU)$, entonces $d(ax)$ es una medida de Haar y*

$$d(ax) = |a|_p dx \qquad a \in \mathbb{Q}_p^{\times}.$$

Es decir,

$$\int_{aU} dx = |a|_p \int_U dx$$

para cada conjunto de Borel U.

Demostración Sea $T_a : \mathbb{Q}_p \to \mathbb{Q}_p$, donde $T_a(x) = ax$.
T_a está bien definido y es inyectivo pues $T_a(x) = T_a(y) \Leftrightarrow ax = ay \Leftrightarrow \ x = y$.
Si $y \in \mathbb{Q}_p$ entonces $T_a(\frac{y}{a}) = y$, luego T_a es sobreyectiva.
T_a es la restricción de la operación producto al conjunto $\{a\} \times \mathbb{Q}_p$, esto implica que T_a es continua.
Por la continuidad de la operación de tomar inversos multiplicativos se obtiene que T_a^{-1} es continua.
Luego, T_a es un homeomorfismo de $\mathbb{Q}_p$ en $\mathbb{Q}_p$; entonces $d(ax)$ es una medida de Borel regular sobre $\mathbb{Q}_p$.
La invarianza de traslación de dx implica la invarianza de traslación de $d(ax)$, esto es, para cualquier $y \in \mathbb{Q}_p$ se tiene

$$d(ax)(y + U) = dx(a(y + U)) = dx(ay + aU) = dx(aU) = d(ax)(U).$$

Por tanto, $d(ax)$ es una medida de Haar sobre $\mathbb{Q}_p$.
Por el teorema 1.6 existe una constante positiva $C(a)$ tal que $\int_{aU} dx = C(a) \int_U dx$.
Para calcular $C(a)$ se puede esocoger cualquier conjunto abierto compacto U, en este caso se toma $U = \mathbb{Z}_p$.
Supóngase que $a \in \mathbb{Z}_p$, entonces $|a|_p = p^{-k}$ con $k \in \mathbb{N}$. Se tiene

$$\mathbb{Z}_p = \bigsqcup_{i=0}^{p^k-1} i + p^k\mathbb{Z}_p$$

$$\Longrightarrow 1 = \int_{\mathbb{Z}_p} dx = \sum_{i=0}^{p^k-1} \int_{i+p^k\mathbb{Z}_p} dx = \sum_{i=0}^{p^k-1} \int_{p^k\mathbb{Z}_p} dx = p^k \int_{p^k\mathbb{Z}_p} dx$$

$$\Longrightarrow \int_{p^k\mathbb{Z}_p} dx = p^{-k} = |a|_p.$$

Como $|a|_p = p^{-k}$ entonces $a = p^k u$ con $u \in \mathbb{Z}_p^{\times}$, usando que $\mathbb{Z}_p = u\mathbb{Z}_p$ se obtiene

$$\int_{a\mathbb{Z}_p} dx = \int_{p^k u\mathbb{Z}_p} dx = \int_{p^k\mathbb{Z}_p} dx = |a|_p.$$

Así,

$$\int_{a\mathbb{Z}_p} dx = C(a) \int_{\mathbb{Z}_p} dx \Longrightarrow C(a) = |a|_p.$$

El caso $a \notin \mathbb{Z}_p$ se trata de manera similar. Por tanto,

$$d(ax) = |a|_p dx \qquad a \in \mathbb{Q}_p^\times.$$

$\square$

Una consecuencia de la proposición anterior es

Corolario 1.8 *Sea $f : U \to \mathbb{C}$, donde U es un conjunto de Borel, esto porque los conjuntos borelianos son abiertos y compactos. Entonces*

$$\int_U f(x)dx = |a|_p \int_{a^{-1}U + a^{-1}b} f(ay+b)dy$$

para cualesquiera $a \in \mathbb{Q}_p^\times$ y $b \in \mathbb{Q}_p$.

Demostración Poniendo $x = ay+b$ y usando la invarianza bajo traslaciones se obtiene $dx = d(ay+b) = d(ay) = |a|_p dy$

$$\int_U f(x)dx = |a|_p \int_{a^{-1}U - a^{-1}b} f(ay+b)dy.$$

$\square$

A continuación se presentan algunos ejemplos de cálculo de integrales que serán de utilidad en este trabajo.

Ejemplo 1.7 *Para calcular*

$$\int_{B(0,p^r)} dx, \quad r \in \mathbb{Z},$$

Poniendo $x = p^{-r}y$ con $y \in \mathbb{Z}_p$ se obtiene $dx = d(p^{-r}y) = p^r y$, luego

$$\int_{B(0,p^r)} dx = \int_{p^{-r}\mathbb{Z}_p} dx = p^r \int_{\mathbb{Z}_p} dx = p^r.$$

Ejemplo 1.8 *Para cualquier $r \in \mathbb{Z}$ se tiene*

$$\int_{S(0,p^r)} dx = \int_{B(0,p^r)} dx - \int_{B(0,p^{r-1})} dx = p^r - p^{r-1} = p^r(1-p^{-1}).$$

Ejemplo 1.9 *Sea*

$$Z(f,s)=\int_{\mathbb{Z}_p}|x|_p^s dx$$

donde $s\in\mathbb{C}$ *y satisface* $Re(s)>-1$. *Tomando* $\{0,1,2,\cdots,p-1\}\subset\mathbb{Z}\subset\mathbb{Z}_p$ *como un sistema de representantes de* $\mathbb{F}_p\simeq\mathbb{Z}_p/p\mathbb{Z}_p$, *entonces*

$$\mathbb{Z}_p=\bigsqcup_{k=0}^{p-1}k+p\mathbb{Z}_p.$$

Luego,

$$\begin{aligned}Z(f,s) &= \int_{\mathbb{Z}_p}|x|_p^s dx\\ &= \sum_{k=1}^{p-1}\int_{k+p\mathbb{Z}_p}|x|_p^s dx+\int_{p\mathbb{Z}_p}|x|_p^s dx.\end{aligned}$$

Si $x\in k+\mathbb{Z}_p$ *con* $k=1,2,\cdots,p-1$, *se cumple que* $x=k+pw$ *donde* $w\in\mathbb{Z}_p$. *De esta manera se tiene que* $|x|_p=|k+pw|\leq$ *máx*$\{|k|_p,|pw|_p\}=$ *máx*$\{1,p^{-1}|w|_p\}$, *usando la proposición 1.8. Esto implica que* $|x|_p=1$, *entonces*

$$\begin{aligned}Z(f,s) &= \sum_{k=1}^{p-1}\int_{k+p\mathbb{Z}_p}|x|_p^s dx+\int_{p\mathbb{Z}_p}|x|_p^s dx\\ &= \sum_{k=1}^{p-1}\int_{k+p\mathbb{Z}_p}dx+\int_{p\mathbb{Z}_p}|x|_p^s dx\\ &= \frac{p-1}{p}+\int_{p\mathbb{Z}_p}|x|_p^s dx.\end{aligned}$$

Con un razonamiento similar se tiene

$$\begin{aligned}Z(f,s) &= \frac{p-1}{p}+\int_{p\mathbb{Z}_p}|x|_p^s dx\\ &= \frac{p-1}{p}+\sum_{k=1}^{p-1}\int_{pk+p^2\mathbb{Z}_p}|x|_p^s dx+\int_{p^2\mathbb{Z}_p}|x|_p^s dx\\ &= \frac{p-1}{p}+\sum_{k=1}^{p-1}\int_{pk+p^2\mathbb{Z}_p}(p^{-1})^s dx+\int_{p^2\mathbb{Z}_p}|x|_p^s dx\\ &= \frac{p-1}{p}+\sum_{k=1}^{p-1}p^{-s}\int_{pk+p^2\mathbb{Z}_p}dx+\int_{p^2\mathbb{Z}_p}|x|_p^s dx\\ &= \frac{p-1}{p}+\frac{p-1}{p^2}p^{-s}+\int_{p^2\mathbb{Z}_p}|x|_p^s dx.\end{aligned}$$

Continuando con este proceso se obtiene

$$\begin{aligned} Z(f,s) &= \int_{\mathbb{Z}_p} |x|_p^s dx \\ &= \frac{p-1}{p} + \frac{p-1}{p^2}p^{-s} + \frac{p-1}{p^3}p^{-2s} + \cdots \\ &= \frac{p-1}{p}(1 + p^{-s-1} + p^{2(-s-1)} + p^{3(-s-1)} + \cdots) \\ &= \frac{p-1}{p}\frac{1}{1-p^{-s-1}} \quad si \quad Re(s) > -1. \end{aligned}$$

Ejemplo 1.10 *Sea* $U = \mathbb{Z}_p - \{0\}$.
Considerando la sucesión $(p^{-n})_{n=1}^{\infty}$ *se tiene que* $\lim_{n\to\infty} p^{-n} = 0$ *y además cualquier subsucesión* (p^{n_k}) *converge a* $0 \notin U$. *Así,* U *no es secuencialmente compacto y por tanto no es compacto.*
Por otro lado,

$$\{0\} = \bigcap_{n=1}^{\infty} p^n \mathbb{Z}_p.$$

Como cada $p^n\mathbb{Z}_p$ *es un conjunto de Borel,* $p\mathbb{Z}_p \supset p^2\mathbb{Z}_p \supset p^3\mathbb{Z}_p \supset \cdots$ *y* $\int_{p\mathbb{Z}_p} = p^{-1}$, *entonces*

$$\lim_{n\to\infty} \int_{p^n\mathbb{Z}_p} dx = \lim_{n\to\infty} p^{-n} = 0 = \int_{\{0\}} dx.$$

Así,

$$\int_{\mathbb{Z}_p - \{0\}} dx = \int_{\mathbb{Z}_p} dx - \int_{\{0\}} dx = 1.$$

Además,

$$\begin{aligned} U &= \mathbb{Z}_p - \{0\} \\ &= \bigsqcup_{i=1}^{p-1} (i + p\mathbb{Z}_p) \bigsqcup (p\mathbb{Z}_p - \{0\}) \\ &= \bigsqcup_{i=1}^{p-1} (i + p\mathbb{Z}_p) \bigsqcup \left(\bigsqcup_{i=1}^{p-1} \left(ip + p^2\mathbb{Z}_p\right) \right) \bigsqcup \left(p^2\mathbb{Z}_p - \{0\}\right) \\ &\vdots \end{aligned}$$

Continuando con este proceso, se observa que U *es la unión contable de subconjuntos abiertos, compactos y disjuntos. Es decir,* U *es un conjunto de Borel.*

Como $(\mathbb{Q}_p^\times, \cdot)$ es también un grupo topológico localmente compacto existe una medida de Haar $d\mu^\times$ que se puede normalizar por la condición

$$\int_{\mathbb{Z}_p^\times} d\mu^\times = 1.$$

Proposición 1.30 *Se tiene la siguiente relación entre medidas*

$$d\mu^\times(x) = \frac{1}{1-p^{-1}} \frac{dx}{|x|_p}.$$

Demostración Sea la medida definida en $\mathbb{Q}_p^\times$ como

$$A \to \int_A \frac{1}{1-p^{-1}} \frac{dx}{|x|_p}.$$

Para $b \in \mathbb{Q}_p^\times$, haciendo el cambio de variables $x = bz$, se tiene

$$\int_{bA} \frac{1}{1-p^{-1}} \frac{dx}{|x|_p} = \int_A \frac{1}{1-p^{-1}} \frac{|b|_p dz}{|b|_p |z|_p} = \int_A \frac{1}{1-p^{-1}} \frac{dx}{|x|_p}.$$

Así, esta medida es invariante bajo la multiplicación.
Como la medida de Haar está únivocamente determinada salvo por múltiplos positivos, se tiene que la medida antes definida es un múltiplo de la medida $d\mu^\times$. Por otro lado,

$$\int_{\mathbb{Z}_p^\times} \frac{1}{1-p^{-1}} \frac{dx}{|x|_p} = \frac{1}{1-p^{-1}} \int_{\mathbb{Z}_p^\times} = \frac{1}{1-p^{-1}}(1-p^{-1}) = 1.$$

Entonces, $d\mu^\times$ es igual a la medida antes definida. Por tanto,

$$d\mu^\times(x) = \frac{1}{1-p^{-1}} \frac{dx}{|x|_p}.$$

□

Definición 1.19 *Una función $h : U \to \mathbb{Q}_p$ donde U es un subconjunto abierto, se dice que h es **analítica sobre** U, si para $x \in V \subset U$, con V abierto, existe una serie de potencias convergente $\sum_i a_i x^i$ tal que $h(x) = \sum_i a_i x^i$.*

En este caso, $h'(x) = \sum_i i a_i x^{i-1}$ es una serie de potencias convergente.

Definición 1.20 *Una función f es **bianalítica** si f y f^{-1} son analíticas.*

Teorema 1.7 (Cambio de variables (caso general), [23], pág. 41) *Sean $K, K_1 \subset \mathbb{Q}_p$ subconjuntos abiertos y compactos. Sea $\sigma : K_1 \to K$ una función bianalítica tal que $\sigma'(y) \neq 0$ para cada $y \in K_1$. Si f es una función continua sobre K entonces*

$$\int_K f(x)dx = \int_{K_1} f(\sigma(y))|\sigma'(y)|_p dy, \quad x = \sigma(y).$$

I.2.6 El caso n dimensional

El espacio $\mathbb{Q}_p^n = \mathbb{Q}_p \times \mathbb{Q}_p \times \cdots \times \mathbb{Q}_p$ consiste de los puntos $x = (x_1, x_2, \cdots x_n)$, con $x_j \in \mathbb{Q}_p$ para $j = 1, 2, 3, \cdots n$. La norma sobre $\mathbb{Q}_p^n$ es

$$\|x\|_p = \text{máx}_{1 \leq j \leq n} |x_j|_p, \quad x \in \mathbb{Q}_p^n.$$

La norma recién definida es no arquimediana, la única propiedad que no es evidente es la desigualdad

$$\|x + y\|_p \leq \text{máx}\{\|x\|_p, \|y\|_p\}, \quad x, y \in \mathbb{Q}_p^n$$

pero esta se cumple, pues

$$\begin{aligned} \|x + y\|_p &= \text{máx}_{1 \leq j \leq n} |x_j + y_j|_p \leq \text{máx}_{1 \leq j \leq n} \text{máx}\{|x_j|_p, |y_j|_p\} \\ &= \text{máx}\{\text{máx}_{1 \leq j \leq n} |x_j|_p, \text{máx}_{1 \leq j \leq n} |y_j|_p\} \\ &= \text{máx}\{\|x\|_p, \|y\|_p\}. \end{aligned}$$

Como las propiedades de ser completo, totalmente disconexo y localmente compacto se conservan en la topología producto se obtiene que $\mathbb{Q}_p^n$ es un espacio métrico completo, totalmente disconexo y localmente compacto. La bola y la esfera se definen de manera similar al caso unidimensional, es decir,

Definición 1.21 *Se define la* ***bola con centro en*** a ***y radio*** p^r *al conjunto*

$$B^n(a, p^r) = \{x \in \mathbb{Q}_p^n : \|x - a\|_p \leq p^r\}, \ \ r \in \mathbb{Z}.$$

Definición 1.22 *La* ***esfera con centro en*** a ***y radio*** p^r *es el conjunto*

$$S^n(a, p^r) = \{x \in \mathbb{Q}_p^n : \|x - a\|_p = p^r\}, \ \ r \in \mathbb{Z}.$$

La bola y la esfera son conjuntos cerrados y abiertos en $\mathbb{Q}_p^n$, además si $a = (a_1, a_2, \cdots, a_n)$ entonces $B^n(a, p^r) = B(a_1, p^r) \times B(a_2, p^r) \times \cdots \times B(a_n, p^r)$.

Por otro lado, existe una medida de Haar $d^n x$ sobre Q_p^n y se puede normalizar por la condición

$$\int_{\mathbb{Z}_p^n} d^n x = 1.$$

Para más detalles se puede consultar [22].

II. FÓRMULA DE LA FASE ESTACIONARIA

Se introducen las funciones zeta locales de Igusa y la fórmula de la fase estacionaria que es una técnica que permite calcular dichas funciones en muchos casos. Este capítulo esta basado en [27] y [15].

II.1. Funciones localmente constantes

Definición 2.1 *Una función $\varphi : \mathbb{Q}_p \to \mathbb{C}$ se dice que es* ***localmente constante*** *si para cada $x \in \mathbb{Q}_p$ existe un subconjunto abierto y compacto U tal que $x \in U$ y $\varphi(u) = \varphi(x)$ para todo $u \in U$.*

Lema 2.1 *Sean φ una función localmente constante y A un conjunto abierto y compacto entonces*

$$\varphi(x) = \sum_{j=1}^{t} \varphi(x_j) 1_{B(x_j, p^{m_j})}(x) \quad x \in A,$$

donde $x_i \in A$ para $i = 1, 2, \cdots, t$, $m_i \in \mathbb{Z}$ para cada $i = 1, 2, \cdots, n$ y

$$1_{B(x_j, p^{m_j})}(x) = \begin{cases} 0 & \text{si } x \notin B(x_j, p^{m_j}) \\ 1 & \text{si } x \in B(x_j, p^{m_j}). \end{cases}$$

Demostración Para cada $x \in A$ existe $m_x \in \mathbb{Z}$ tal que si $y \in B(x, p^{m_x})$ entonces $\varphi(x) = \varphi(y)$. Sea $C = \{B(x, p^{m_x}) : x \in A\}$, entonces C es una cubierta abierta de A, por ser compacto existen $x_1, x_2, \cdots, x_t \in A$ tales que

$$A = \bigcup_{i=1}^{t} B(x_i, p^{m_i}).$$

Ahora, como dos bolas son ajenas o una contiene a la otra, sin pérdida de generalidad se puede suponer

$$A = \bigsqcup_{i=1}^{t} B(x_i, p^{m_i}).$$

Así,

$$\varphi|_A(x) = \sum_{j=1}^{t} \varphi(x_j) 1_{B(x_j, p^{m_j})}(x) \quad x \in A.$$

$\square$

Definición 2.2 *El **soporte** de una función compleja f definida en un espacio topológico X es la cerradura de el conjunto*

$$\{x : f(x) \neq 0\}.$$

Observación En esta tesis el soporte de una función f se denotará por $supp\ f$.

Corolario 2.1 *Cualquier función localmente constante $\varphi : \mathbb{Q}_p \to \mathbb{C}$ con soporte compacto puede ser expresada como una combinación lineal de funciones caracteristicas de bolas de la forma*

$$\varphi(x) = \sum_{n=1}^{N} c_n 1_{B(x_n, p^M)}(x)$$

donde $c_n \in \mathbb{C}$, $M \in \mathbb{Z}$ y $\{B(x_n, p^M)\}_{1 \leq n \leq N}$ cubren el soporte de φ.

Definición 2.3 *Sea $\varphi : \mathbb{Q}_p \to \mathbb{C}$ una función localmente constante y A un subconjunto abierto y compacto de $\mathbb{Q}_p$. Por el lema anterior $\varphi|_A(x) = \sum_{i=1}^{k} c_i 1_{U_i}(x)$, con U_i abierto y compacto. Se define*

$$\int_A \varphi(x)dx = c_1 \int_{U_1} dx + c_2 \int_{U_2} dx + \cdots + c_k \int_{U_k} dx.$$

Proposición 2.1 *Si $\varphi : \mathbb{Q}_p \to \mathbb{C}$ es una función localmente constante entonces es continua.*

Demostración Sea $U \subset \mathbb{C}$ abierto. Para cada $s \in U$ existe un abierto $U_s \subseteq \mathbb{Q}_p$ tal que $\varphi|_{U_s} = s$, por que φ es localmente constante, entonces

$$\varphi^{-1}(U) = \bigcup_{s \in U} U_s.$$

□

Definición 2.4 *Una función localmente constante con soporte compacto se llama **función de Schwartz-Bruhat**.*

Las funciones de Schwartz-Bruhat forman un $\mathbb{C}-$espacio vectorial denotado por S. Además, se tiene

Proposición 2.2 *S es un subespacio denso de C_0, el espacio de funciones continuas con soporte compacto.*

Una prueba de este resultado se puede consultar en [21].

Definición 2.5 *Una función $\varphi : \mathbb{Q}_p \to \mathbb{C}$ se dice que es **localmente integrable**, $\varphi \in L^1_{loc}$, si*

$$\int_K \varphi(x)dx$$

existe para cada compacto K.

Definición 2.6 (Integral impropia) *Una función $\varphi \in L^1_{loc}$ se dice que es **integrable en** $\mathbb{Q}_p$ si*

$$\lim_{N\to+\infty} \int_{B(0,p^N)} \varphi(x)dx = \lim_{N\to+\infty} \sum_{j=-\infty}^{N} \int_{S(0,p^j)} \varphi(x)dx$$

*existe. Si el límite existe, se denota por $\int_{\mathbb{Q}_p} \varphi(x)dx$ y se dice que la **integral impropia** existe.*

Observación Se tiene que

$$\int_{\mathbb{Q}_p} \varphi(x)dx = \sum_{j=-\infty}^{+\infty} \int_{S(0,p^j)} \varphi(x)dx.$$

II.2. Funciones zeta locales de Igusa

Definición 2.7 *Sea p un número primo fijo, se define*

$$A_m := \mathbb{Z}/p^m\mathbb{Z} \quad m \in \mathbb{N} \setminus \{0\}$$

*como el **anillo de enteros modulo** p^m.*

Recordando que todo entero se puede escribir en forma única como

$$a_0 + a_1 p + \cdots + a_{m-1}p^{m-1} \quad a_i \in \{0, 1, 2, \cdots, p-1\}$$

entonces se puede identificar A_m (como conjuntos), con el conjunto

$$\{a_0 + a_1 p + \cdots + a_{m-1}p^{m-1} : a_i \in \{0, 1, 2, \cdots, p-1\}\}.$$

Sea $f(x) \in \mathbb{Z}[x_1, \cdots, x_n] \setminus \mathbb{Z}$ se define

$$N_m = \begin{cases} \#(\{x \in (\mathbb{Z}/p^m\mathbb{Z})^n : f(x) \equiv 0 \pmod{p^m}\}) & \text{si } m \geq 1 \\ 1 & \text{si } m = 0. \end{cases}$$

Un problema básico es estudiar el comportamiento de N_m cuando $m \to \infty$.
De manera más general, tomando $f(x) \in \mathbb{Z}_p[x_1, \cdots, x_n] \setminus \mathbb{Z}_p$ (recordando que $\mathbb{Z} \subset \mathbb{Z}_p$ y $\mathbb{Z}/p^m\mathbb{Z} \simeq \mathbb{Z}_p/p^m\mathbb{Z}_p$) se define

$$N_m = \begin{cases} \#(\{x \in (\mathbb{Z}_p/p^m\mathbb{Z}_p)^n : f(x) \equiv 0 \pmod{p^m}\}) & \text{si } m \geq 1 \quad [*] \\ 1 & \text{si } m = 0. \end{cases}$$

donde $x \equiv y \pmod{p^m}$ significa que $x - y \in p^m\mathbb{Z}_p$.
Para estudiar la sucesión $\{N_m\}_{m\in\mathbb{N}}$ se introduce la siguiente serie de Poincaré.

Definición 2.8 *Se define la* ***serie de Poincaré*** *asociada a [*] como la serie*

$$P(t) := \sum_{m=0}^{+\infty} N_m(p^{-n}t)^m,$$

donde $t \in \mathbb{C}$ *con* $|t| < 1$.

Observación Para cada $m \in \mathbb{N}$ se tiene $N_m \leq p^{nm}$, luego

$$\sum_{m=0}^{k} |N_m(p^{-n}t)^m| \leq \sum_{m=0}^{k} p^{mn}p^{-nm}|t|^m = \sum_{m=0}^{k} |t|^m, \quad \text{donde } |t| < 1.$$

Como $|t| < 1$ entonces $\sum_{m=0}^{\infty} |t|^m$ converge. Así, $P(t)$ es absolutamente convergente por el criterio de comparación.
Por tanto, la serie de Poincaré converge.

Se espera que las propiedades analíticas de $P(t)$ proporcionen información acerca del comportamiento asintótico de la sucesión $\{N_m\}_{m=1}^{\infty}$. Una pregunta fundamental es

¿$P(t)$ es una función racional?.

Observación Dado $a > 0$ y $s \in \mathbb{C}$ se define $a^s = e^{s\ ln\ a}$.

Definición 2.9 *Sean* $f(x) \in \mathbb{Q}_p[x_1, \cdots, x_n] \setminus \mathbb{Q}_p$ *y* φ *una función localmente constante con soporte compacto, es decir, un elemento de* $S(Q_p^n)$. *La* ***función zeta local*** *(también llamada* ***función zeta local de Igusa****) asociada a* (f, φ) *es*

$$Z_\varphi(s, f) := \int_{\mathbb{Q}_p^n \setminus f^{-1}(0)} \varphi(x)|f(x)|_p^s d^n x, \quad s \in \mathbb{C}, Re(s) > 0,$$

donde $d^n x$ *es la medida de Haar de* $(\mathbb{Q}_p^n, +)$ *normalizada de tal manera que* $\int_{\mathbb{Z}_p^n} d^n x = 1$.

Observación $d^n x$ es la medida producto de las medidas $dx_1, dx_2, \cdots, dx_n$, donde dx_i es la medida de Haar normalizada de $(\mathbb{Q}_p, +)$. En particular, si $A = A_1 \times \cdots \times A_n$, donde cada A_i es medible con respecto a dx_i,

$$\int_A d^n x = \prod_{i=1}^{n} \int_{A_i} dx_i.$$

Para más detalles se puede consultar [10].

Proposición 2.3 *La integral*

$$Z_\varphi(s,f) = \int_{\mathbb{Q}_p^n \setminus f^{-1}(0)} \varphi(x)|f(x)|_p^s d^n x$$

converge para $Re(s) > 0$.

Demostración Se tiene

$$\left| \int_{\mathbb{Q}_p^n \setminus f^{-1}(0)} \varphi(x)|f(x)|_p^s d^n x \right| \leq \int_{supp\ \varphi} |\varphi(x)||f(x)|_p^{Re(s)} d^n x,$$

como $supp\ \varphi$ es compacto y las funciones $|\varphi|$ y $|f(x)|_p^{Re(s)}$ son continuas, entonces existe $C(s)$ tal que $|\varphi(x)||f(x)|_p^{Re(s)} \leq C(s)$ para todo $x \in supp\ \varphi$. Así,

$$\begin{aligned} \left| \int_{\mathbb{Q}_p^n \setminus f^{-1}(0)} \varphi(x)|f(x)|_p^s d^n x \right| &\leq \int_{supp\ \varphi} |\varphi(x)||f(x)|_p^{Re(s)} d^n x \\ &\leq C(s) \int_{supp\ \varphi} d^n x \\ &< +\infty. \end{aligned}$$

□

Para estudiar si $Z_\varphi(s,f)$ es analítica se introduce un resultado sobre grupos topológicos localmente compactos, para más detalles se puede consultar [9].

Sean G un grupo topológico localmente compacto con medida de Haar dx, $D \subset \mathbb{C}$ una región y $h : G \times D \to \mathbb{C}$ una función continua tal que:

1. Para $x \in G$ fijo, $h(x,s)$ es una función analítica de $s \in D$.
2. Para $s \in D$ fijo, $h(x,s)$ y $h_s(x,s)$ son integrables con respecto a dx, donde $h_s(x,s)$ indica la derivada de $h(x,s)$ con respecto a s.

Se puede entonces definir la función

$$g(s) = \int_G h(x,s)dx \quad \text{para } s \in D.$$

Definición 2.10 *Sean G, D y h como antes. Si $E \subseteq D$ entonces se dice que*

$$\int_G h(x,s)dx \tag{2.1}$$

converge uniformemente en *E si, dado $\epsilon > 0$, existe un subconjunto compacto $K = K(\epsilon, E) \subset G$ tal que*

$$\left|\int_{G\setminus K} h(x,s)dx\right| < \epsilon$$

para todo $s \in E$.
Se dice que la integral (2.1) ***converge uniformemente en subconjuntos compactos de*** *D si esta converge uniformemente en todo subconjunto compacto de D.*

Proposición 2.4 (Theorem 8-1-5, [9]) *Sean h, g, G y D como antes. Si*

$$\int_G |h(x,s)|dx$$

converge uniformemente en subconjuntos compactos de D, entonces $g(s)$ es analítica en D y

$$g_s(s) = \int_G h_s(x,s)dx.$$

Corolario 2.2 *La función $Z_\varphi(s,f)$ es analítica para $Re(s) > 0$.*

Demostración Tomando $G = \mathbb{Q}_p^n$, $h(x,s) = \varphi(x)1_{\mathbb{Q}_p^n\setminus f^{-1}(0)}(x)|f(x)|_p^s$ y $D = \{s \in \mathbb{C} : Re(s) > 0\}$ se tiene

1. para $x \in G$ fijo, $h(x,s) = \varphi(x)1_{\mathbb{Q}_p^n\setminus f^{-1}(0)}(x)e^{s\ ln|f(x)|_p}$ es una función analítica de $s \in D$.

2. para $s \in D$ fijo, $h(x,s)$ y $h_s(x,s) = \varphi(x)1_{\mathbb{Q}_p^n\setminus f^{-1}(0)}(x)ln|f(x)|_p e^{s\ ln|f(x)|_p}$ son integrables con respecto a $d^n x$.

La afirmación 1 se sigue del hecho que la función e^z, $z \in \mathbb{C}$, es analítica. Para la afirmación 2 hay que observar que

$$|h_s(x,s)| \leq |\varphi(x)|1_{\mathbb{Q}_p^n\setminus f^{-1}(0)}(x)|f(x)|_p^{Re(s)+1}$$

y esta última función es integrable para $Re(s) > 0$.
Por otro lado, sea $B(x_0, p^m)$ tal que $|f(x)|_p = |f(x_0)|_p$ para cada $x \in B(x_0, p^m)$ y $\varphi|_{B(x_0,p^m)} = \varphi(x_0) \neq 0$, es decir, $B(x_0, p^m) \subset supp\ \varphi$.
Sea $\epsilon > 0$ dado, como $B(x_0, p^m)$ es compacto, para verificar las hipótesis del teorema anterior es suficiente probar que

$$I := \int_{B(x_0,p^m)} |\varphi(x)||f(x)|_p^{Re(s)} d^n x < \epsilon$$

para s perteneciendo a un subconjunto compacto de D. Entonces se debe cumplir que

$$I = |\varphi(x_0)||f(x_0)|_p^{Re(s)} p^{-m} < \epsilon.$$

Esto es posible, dado que s pertenece a un conjunto compacto, $|\varphi(x_0)| \neq 0$ y $|f(x_0)| \neq 0$.

Así, se tienen las hipótesis de la proposición anterior y por tanto $Z_\varphi(s,f)$ es analítica para $Re(s)>0$.

$\square$

Definición 2.11 *Dado $f(x)\in\mathbb{Z}_p[x_1,\cdots,x_n]\setminus\mathbb{Z}_p$ se define*

$$Z(s):=\int_{\mathbb{Z}_p^n\setminus f^{-1}(0)}|f(x)|_p^s d^n(x),\quad s\in\mathbb{C}, Re(s)>0.$$

Proposición 2.5 *Con la notación anterior*

$$P(t)=\frac{1-tZ(s)}{1-t},\ t=p^{-s},\ \textit{para}\ \ Re(s)>0,$$

donde $P(t)$ es la serie de Poincaré definida en (2.8).

Demostración Se tiene que

$$Z(s)=\int_{\mathbb{Z}_p^n\setminus f^{-1}(0)}|f(x)|_p^s d^n(x)=\sum_{m=0}^{+\infty}p^{-ms}\int_{\{x\in\mathbb{Z}_p^n:|f(x)|_p=p^{-m}\}}d^nx.$$

La imagen de $|f|^s:\mathbb{Z}_p^n\to\mathbb{C}$ está contenida en $\{p^{-ms}:m\in\mathbb{Z},m\geq 0\}\cup\{0\}\subset\mathbb{C}$.
Para $m\in\mathbb{Z}$ con $m\geq 0$ la fibra para p^{-ms} está dada por

$$\begin{aligned}&(|f|_p^s)^{-1}(p^{-ms})\\&=\{x\in\mathbb{Z}_p^n:|f(x)|_p=p^{-m}\}\\&=\{x\in\mathbb{Z}_p^n:f(x)\equiv 0\quad(\text{mód } p^m)\}\setminus\{x\in\mathbb{Z}_p^n:f(x)\equiv 0\quad(\text{mód } p^{m+1})\}\\&=\textstyle\bigsqcup_{x\in A_m}x+p^m\mathbb{Z}_p^n\setminus\bigsqcup_{x\in A_{m+1}}x+p^{m+1}\mathbb{Z}_p^n\end{aligned}$$

donde $A_k=\{x\in(\mathbb{Z}_p/p^k\mathbb{Z}_p)^n:f(x)\equiv 0\ (\text{mód } p^k)\}$.
Luego,

$$\int_{\{x\in\mathbb{Z}_p^n:|f(x)|_p=p^{-m}\}}d^nx=N_mp^{-mn}-N_{m+1}p^{-(m+1)n}$$

para todo $m\in\mathbb{Z}$ con $m\geq 0$.
Para un número complejo s con $Re(s)>0$ se tiene

$$
\begin{aligned}
Z(s) &= \int_{\mathbb{Z}_p^n - f^{-1}(0)} |f(x)|_p^s d^n x \\
&= \sum_{m=0}^{+\infty} p^{-ms} \int_{\{x \in \mathbb{Z}_p^n : |f(x)|_p = p^{-m}\}} d^n x \\
&= \sum_{m=0}^{+\infty} p^{-ms} \left(N_m p^{-mn} - N_{m+1} p^{-(m+1)n} \right) \\
&= \sum_{m=0}^{+\infty} N_m p^{-mn-ms} - \sum_{m=0}^{+\infty} N_{m+1} p^{-ms-(m+1)n} \\
&= \sum_{m=0}^{+\infty} N_m (p^{-n} p^{-s})^m - p^s \sum_{m=0}^{+\infty} N_{m+1} p^{-(m+1)s-(m+1)n} \\
&= P(p^{-s}) - p^s \sum_{m'=1}^{+\infty} N_{m+1} p^{-(m')s-(m')n} \quad (m' = m+1) \\
&= P(p^{-s}) - p^s (P(p^{-s}) - 1).
\end{aligned}
$$

$$
\begin{aligned}
&\Longrightarrow \quad Z(s) - p^{-s} = P(p^{-s})(1 - p^s) \\
&\Longrightarrow \quad P(p^{-s}) = \frac{Z(s) - p^s}{1 - p^s} \\
&\Longrightarrow \quad P(p^{-s}) = \frac{1 - p^{-s} Z(s)}{1 - p^{-s}}.
\end{aligned}
$$

Por lo tanto,

$$
P(t) = \frac{1 - tZ(s)}{1 - t}, \ t = p^{-s}, \text{ para } \ Re(s) > 0.
$$

□

Teorema 2.1 (Igusa,[15]) *Sean $f(x)$ un polinomio no constante en $\mathbb{Q}_p[x_1, \cdots, x_n]$ y φ una función localmente constante con soporte compacto. Existe un número finito de parejas $(N_E, v_E) \in (\mathbb{N} \setminus \{0\}) \times (\mathbb{N} \setminus \{0\})$, $E \in T$, donde T es un subconjunto finito, tal que*

$$
\prod_{E \in T} (1 - p^{v_E - sN_E}) Z_\varphi(s, f)
$$

es un polinomio en p^{-s} con coeficientes racionales.

Del teorema 2.1 y la proposición 2.5 se obtiene

Corolario 2.3 *$P(t)$ es una función racional de t.*

La racionalidad de $P(t)$ fue conjeturada e los 60s por Borevich y Shafarevich. Igusa probó este resultado a mediados de los 70s. La racionalidad de $Z_\varphi(s,f)$ también permite encontrar cotas para los N_m's.
La prueba del teorema 2.1 dada por Igusa depende de un resultado profundo en geometría algebraica conocido como el teorema de resolución de singularidades de Hironaka. Una prueba de este teorema queda fuera de los intereses de esta tesis, pero se puede consultar en [15].

II.3. Fórmula de la fase estacionaria

Se introduce la fórmula de la fase estacionaria que es un método elemental para calcular integrales $p-$ádicas del tipo $Z_\varphi(s,f)$. Igusa conjeturó que este método podría conducir a una prueba nueva y elemental de la racionalidad de $Z_\varphi(s,f)$. La racionalidad de $Z_\varphi(s,f)$. en campos de característica arbitraria es un problema abierto, para más detalles se puede consultar [3].

Definición 2.12 *Se dice que $f(x) = \sum c_i x^i \in \mathbb{Q}_p[[x_1,\cdots,x_n]]$ es una **serie de potencias especial restringida**, abreviada SRP, si $f(0)=0$, es decir $c_0=0$, y $c_i \equiv 0 \pmod{p^{|i|-1}}$ para cualquier $i \in \mathbb{N}^n, i \neq 0$, donde $|i| = i_1+\cdots+i_n$.*

Lema 2.2 (Lemma 7.4.3,[15]) *Sea $f_i(x) \in \mathbb{Z}_p[[x_1,\cdots,x_n]]$, para $i=1,\cdots,n$, si cada*
$f_i(x)$ en $f(x)=(f_1(x),\cdots,f_n(x))$ es SRP en $x_1,\cdots,x_n$ y $det\left[\frac{\partial f_i}{x_j}\right] \not\equiv 0 \pmod p$, entonces la función bicontinua de $\mathbb{Z}_p^n$ en $\mathbb{Z}_p^n$ definida por $y=f(x)$ preserva la medida de Haar de $\mathbb{Q}_p^n$.

Se identifica al conjunto $\mathbb{F}_p$ con $\{0,1,\cdots,p-1\}$. Sea "$-$" la función reducción módulo p, es decir, la función

$$\begin{array}{rcl} \mathbb{Z}_p & \longrightarrow & \mathbb{F}_p \\ x_0+p(\cdots) & \longrightarrow & x_0. \end{array}$$

Esta función puede extenderse a $\mathbb{Z}_p^n \longrightarrow \mathbb{F}_p^n$. La reducción módulo p de un subconjunto $E \subset \mathbb{Z}_p^n$ será denotado por $\overline{E} \subset \mathbb{F}_p^n$. Si $f(x) \in \mathbb{Z}_p[x_1,\cdots,x_n] \setminus p\mathbb{Z}_p[x_1,\cdots,x_n]$ entonces $\overline{f}$ denota su reducción módulo p.
Si A es un conjunto finito $\#A$ denota su número de elementos.

Proposición 2.6 (Fórmula de la fase estacionaria) *Sea $\overline{E} \subset \mathbb{F}_p^n$ y se denota por $\overline{S}$ el subconjunto de $\overline{E}$ que consiste en todos los $\overline{a} \in \overline{E}$ tales que $\overline{f}(\overline{a}) = \frac{\partial \overline{f}}{\partial x_i}(\overline{a}) = 0$ para $1 \leq i \leq n$. Sean S y E las preimagenes de $\overline{S}$ y $\overline{E}$ bajo $\mathbb{Z}_p^n \longrightarrow \mathbb{F}_p^n$ y sea N el número de ceros de $\overline{f}(x)$ en $\overline{E}$. Entonces*

$$\int_E |f(x)|_p^s d^n x = p^{-n}(\#\overline{E}-N) + \frac{p^{-n-s}(1-p^{-1})(N-\#\overline{S})}{1-p^{-1-s}} + \int_S |f(x)|_p^s d^n x.$$

Demostración Por definición

$$E = \bigsqcup_{\overline{a}\in\overline{E}} a + (p\mathbb{Z}_p)^n.$$

Luego,

$$\begin{aligned}
\int_E |f(x)|_p^s d^n x &= \sum_{\overline{a}\in\overline{E}} \int_{a+(p\mathbb{Z}_p)^n} |f(x)|_p^s d^n x \\
&= \sum_{\overline{a}\in\overline{E}\setminus\overline{S}} \int_{a+(p\mathbb{Z}_p)^n} |f(x)|_p^s d^n x + \sum_{\overline{a}\in\overline{S}} \int_{a+(p\mathbb{Z}_p)^n} |f(x)|_p^s d^n x \\
&= \sum_{\overline{a}\in\overline{E}\setminus\overline{S}} \int_{a+(p\mathbb{Z}_p)^n} |f(x)|_p^s d^n x + \int_S |f(x)|_p^s d^n x \\
&= \sum_{\overline{a}\in\overline{E}\setminus\overline{S}} \int_{\mathbb{Z}_p^n} |f(a+px)|_p^s |p^n|_p d^n x + \int_S |f(x)|_p^s d^n x \\
&= p^{-n} \sum_{\overline{a}\in\overline{E}\setminus\overline{S}} \int_{\mathbb{Z}_p^n} |f(a+px)|_p^s d^n x + \int_S |f(x)|_p^s d^n x.
\end{aligned}$$

Tomando $\overline{a} \in \overline{E} - \overline{S}$ tal que $\overline{f}(\overline{a}) \neq 0$ se tiene $|f(a+px)|_p = 1$, en este caso

$$\int_{\mathbb{Z}_p^n} |f(a+px)|_p^s d^n x = \int_{\mathbb{Z}_p^n} d^n x = 1.$$

El número de estos $\overline{a}$ es $\#\overline{E} - N$. Así, la contribución de estos $\overline{a}$ es $p^{-n}(\#\overline{E} - N)$.

Sea ahora $\overline{a} \in \overline{E} - \overline{S}$ tal que $\overline{f}(\overline{a}) = 0$, $\frac{\partial \overline{f}}{\partial x_i}(\overline{a}) \neq 0$ para algún i, sin pérdida de generalidad se puede suponer que $i = 1$.
Se define

$$g_i(x) = \begin{cases} \frac{f(a+px)-f(a)}{p} & \text{si } i = 1 \\ x_i & \text{si } i > 1. \end{cases}$$

Se tiene que las funciones $g_1(x), \cdots, g_n(x)$ son SRP's en $x_1, \cdots, x_n$ y
$det[\frac{\partial g_i}{\partial x_j}(0)] = \frac{\partial f}{\partial x_1}(0) \not\equiv 0 \pmod{p}$.
Por el lema 2.2, $(y_1, \cdots, y_n) = (g_1(x), \cdots, g_n(x))$ es una función de $\mathbb{Z}_p^n$ en $\mathbb{Z}_p^n$ que preserva la medida de Haar. Así,

$$\begin{aligned}\int_{\mathbb{Z}_p^n} |f(a+px)|_p^s d^n x &= \int_{\mathbb{Z}_p} |py_1 + f(a)|_p^s dy_1 \\ &= p^{-s} \int_{\mathbb{Z}_p} \left| y_1 + \frac{f(a)}{p} \right|_p^s dy_1 \\ &= p^{-s} \int_{\mathbb{Z}_p} |y_1|_p^s dy_1 = p^{-s} \frac{1-p^{-1}}{1-p^{-1-s}}.\end{aligned}$$

Está última integral se calculó en el ejemplo 1.9, pág. 44, el número de estos $\overline{a}$ es $N - \#\overline{S}$. Así, la contribución de estos $\overline{a}$ es

$$\frac{p^{-n-s}(1-p^{-1})(N-\#\overline{S})}{1-p^{-1-s}}.$$

Por tanto,

$$\int_E |f(x)|_p^s d^n x = p^{-n}(\#\overline{E} - N) + \frac{p^{-n-s}(1-p^{-1})(N-\#\overline{S})}{1-p^{-1-s}} + \int_S |f(x)|_p^s d^n x.$$

□

Observación Tomando

$$f(a+px) := p^{e_a} \widetilde{f}(x) \quad con \quad \widetilde{f}(x) \in \mathbb{Z}_p[x_1, \cdots, x_n] \setminus p\mathbb{Z}_p[x_1, \cdots, x_n]$$

y

$$L(p^{-s}) = (1-p^{-1-s})(p^{-n}(\#\overline{E} - N)) + p^{-n-s}(1-p^{-1})(N - \#\overline{S}).$$

La fórmula de la fase estacionaria, abreviada FFE, puede ser reescrita como

$$\begin{aligned}\int_E |f(x)|_p^s d^n x &= \frac{L(p^{-s})}{1-p^{-1-s}} + \int_S |f(x)|_p^s d^n x \\ &= \frac{L(p^{-s})}{1-p^{-1-s}} + p^{-n} \sum_{\overline{a} \in \overline{S}} \int_{\mathbb{Z}_p^n} |f(a+px)|_p^s d^n x \\ &= \frac{L(p^{-s})}{1-p^{-1-s}} + p^{-n-e_a s} \sum_{\overline{a} \in \overline{S}} \int_{\mathbb{Z}_p^n} |\widetilde{f}(x)|_p^s d^n x,\end{aligned}$$

Se puede aplicar nuevamente FFE a cada una de las integrales $\int_{\mathbb{Z}_p^n} |\widetilde{f}(x)|_p^s d^n x$.

Igusa conjeturó que aplicando recursivamente FFE es posible establecer la racionalidad de integrales del tipo $\int_E |f(x)|_p^s d^n x$, en el caso en que el polinomio f tiene coeficientes en un campo completo no arquimediano de característica arbitraria.

Observación Sea $f(x) \in \mathbb{Z}_p[x_1, \cdots, x_n] \setminus p\mathbb{Z}_p[x_1, \cdots, x_n]$. Si el sistema de ecuaciones

$$\overline{f}(\overline{a}) = \frac{\partial \overline{f}}{\partial x_i}(\overline{a}) = 0, \;\; 1 \leq i \leq n,$$

no tiene soluciones en $\mathbb{F}_p^n$ entonces $S = \emptyset$ y por FFE,

$$Z(s, f) = p^{-n}(\#\overline{E} - N) + \frac{p^{-n-s}(1 - p^{-1})(N)}{1 - p^{-1-s}}.$$

Ejemplo 2.1 *Sea* $f(x, y) = x^4 + bx^2y^2 + y^4 \in \mathbb{Z}_p[x, y]$ *donde* $b^2 \not\equiv 4 \pmod{p}$ *y* $p \neq 2$. *Para calcular la función zeta asociada a este polinomio se procede a utilizar la FFE. Se tiene* $\overline{E} = \mathbb{F}_p^2$ *y* $E = \mathbb{Z}_p^2$. *Para calcular* S *se tiene que resolver el sistema*

$$\begin{aligned}
\overline{f}(x, y) &= x^4 + \overline{b}x^2y^2 + y^4 = 0 \\
\frac{\partial \overline{f}(x, y)}{\partial x} &= 4x^3 + 2\overline{b}y^2x = 0 \\
\frac{\partial \overline{f}(x, y)}{\partial y} &= 4y^3 + 2\overline{b}x^2y = 0
\end{aligned}$$

en $\mathbb{F}_p$. *Una solución es* $x = y = 0$ *y se cumple* $x = 0$ *si y sólo* $y = 0$. *Suponiendo que* $x, y \neq 0$ *entonces*

$$4x^3 + 2\overline{b}y^2x = 0 \Longrightarrow 2x(2x^2 + \overline{b}y^2) = 0 \Longrightarrow 2x^2 + \overline{b}y^2 = 0$$

$$4y^3 + 2\overline{b}x^2y = 0 \Longrightarrow 2y(2y^2 + \overline{b}x^2) = 0 \Longrightarrow 2y^2 + \overline{b}x^2 = 0$$

$$\begin{aligned}
&\Longrightarrow \;\; x^2 = -2^{-1}\overline{b}y^2 \quad\;\; y^2 = -2^{-1}\overline{b}x^2 \\
&\Longrightarrow \;\; x^2 = -2^{-1}\overline{b}(-2^{-1}\overline{b}x^2) = 4^{-1}\overline{b}^2x^2 \\
&\Longrightarrow \;\; 4 = \overline{b}^2 \quad \textit{con contradicción a la hipótesis.}
\end{aligned}$$

Así, $\overline{S} = \{(0, 0)\}$ *y* $S = p\mathbb{Z}_p \times p\mathbb{Z}_p$.
Aplicando FFE se obtiene

$$\begin{aligned}
Z(s, f) &= p^{-2}(p^2 - N) + \frac{p^{-2-s}(1 - p^{-1})(N - 1)}{1 - p^{-1-s}} \\
&+ \int_{p\mathbb{Z}_p \times p\mathbb{Z}_p} |x^4 + bx^2y^2 + y^4|_p^s dxdy.
\end{aligned}$$

Haciendo el cambio de variables $x = pu$, $y = pv$ *donde* $u, v \in \mathbb{Z}_p$ *se obtiene* $dxdy = p^{-2}dudv$ *y entonces*

$$
\begin{aligned}
Z(s,f) &= p^{-2}(p^2-N)+\frac{p^{-2-s}(1-p^{-1})(N-1)}{1-p^{-1-s}} \\
&\quad +\int_{\mathbb{Z}_p\times\mathbb{Z}_p}|p^4u^4+bp^4u^2v^2+p^4v^4|_p^s p^{-2}dudv \\
&= p^{-2}(p^2-N)+\frac{p^{-2-s}(1-p^{-1})(N-1)}{1-p^{-1-s}} \\
&\quad +p^{-4s-2}\int_{\mathbb{Z}_p\times\mathbb{Z}_p}|u^4+bu^2v^2+v^4|_p^s dudv \\
&= p^{-2}(p^2-N)+\frac{p^{-2-s}(1-p^{-1})(N-1)}{1-p^{-1-s}}+p^{-4s-2}Z(s,f).
\end{aligned}
$$

Por lo tanto,

$$
Z(s,f)=\frac{1}{1-p^{-4s-2}}\left\{p^{-2}(p^2-N)+\frac{p^{-2-s}(1-p^{-1})(N-1)}{1-p^{-1-s}}\right\}.
$$

Ejemplo 2.2 *Sea $f(x,y)=px+x^2-y^3\in\mathbb{Z}_p$ donde $p\neq 2,3$. Con la notación de la FFE se tiene $\overline{E}=\mathbb{F}_p^2$ y $E=\mathbb{Z}_p^2$.*
Para encontrar $\overline{S}$ se tiene que resolver el sistema de ecuaciones

$$
\begin{aligned}
\overline{f}(x,y) &= x^2-y^3=0 \\
\frac{\partial\overline{f}(x,y)}{\partial x} &= 2x=0 \\
\frac{\partial\overline{f}(x,y)}{\partial y} &= -3y^2=0,
\end{aligned}
$$

sobre $\mathbb{F}_p$. Se tiene

$$
\begin{aligned}
2x=0 &\Longrightarrow x=0 \\
-3y^2=0 &\Longrightarrow y=0.
\end{aligned}
$$

Así, $\overline{S}=\{(0,0)\}$ y entonces $S=p\mathbb{Z}_p\times p\mathbb{Z}_p$.

Para encontrar N, hay que resolver $x^2-y^3=0$ en $\mathbb{F}_p$. Una solución es $x=0$ y $y=0$, además se cumple que $x=0$ si y sólo si $y=0$. Por otro lado, sea g un generador de $(\mathbb{Z}/p\mathbb{Z})^\times$, escribiendo $x=g^t$ y $y=g^k$ donde t y k pertenecen al conjunto $\{1,2,\cdots,p-1\}$, la ecuación $x^2-y^3=0$ es equivalente a la ecuación $g^{3k}\equiv g^{2t}\pmod{p}$, que se convierte en la ecuación sobre los exponentes $3k\equiv 2t\pmod{p-1}$. Para la última ecuación se distinguen dos casos:

1. *Si $m.c.d(3,p-1)=1$ entonces $3k\equiv 2t\pmod{p-1}$ tiene solución única en la variable k para cada $t\in\{1,2,\cdots,p-1\}$. Así, hay $p-1$ soluciones.*

2. *Si* $m.c.d.(3, p-1) = 3$ *entonces la ecuación* $3k \equiv 2t \pmod{p}$ *tiene solución para* k *si y sólo si* $2t \equiv 0 \pmod{3}$*, hay exactamente* $\frac{p-1}{3}$ *valores de* t *que son múltiplos de* 3*. Luego, fijando* t *tal que* $2t \equiv 0 \pmod{3}$ *hay exactamente* $m.c.d.(3, 2t) = 3$ *soluciones de* $3k \equiv 2t \pmod{p} - 1$ *en la variable* k*. Así, hay* $3(\frac{p-1}{3}) = p - 1$ *soluciones.*

Por tanto, hay p *soluciones de* $x^2 - y^3 = 0$ *en* $\mathbb{F}_p$*, es decir,* $N = p$*.*

Aplicando la FFE se obtiene

$$\begin{aligned} Z(s,f) &= p^{-2}(p^{-2} - p) + \frac{p^{-2-s}(1-p^{-1})(p-1)}{1-p^{-1-s}} \\ &+ \int_{p\mathbb{Z}_p \times p\mathbb{Z}_p} |px + x^2 - y^3|_p^s dxdy. \end{aligned}$$

Haciendo el cambio de variables $x = pu$ *y* $y = pv$ *con* $u, v \in \mathbb{Z}_p$ *en la última integral, se obtiene*

$$\begin{aligned} Z(s,f) &= p^{-2}(p^{-2} - p) + \frac{p^{-2-s}(1-p^{-1})(p-1)}{1-p^{-1-s}} \\ &+ p^{-2} \int_{\mathbb{Z}_p^2} |p^2u + p^2u^2 - p^3v^3|_p^s dudv \\ &= p^{-2}(p^{-2} - p) + \frac{p^{-2-s}(1-p^{-1})(p-1)}{1-p^{-1-s}} \\ &+ p^{-2-2s} \int_{\mathbb{Z}_p^2} |u + u^2 - pv^3|_p^s dudv. \end{aligned}$$

Para aplicar la FFE al polinomio $g(u,v) = u + u^2 - pv^3$ *se tiene* $\overline{E} = \mathbb{F}_p^2$ *y* $E = \mathbb{Z}_p^2$*. Ahora, el sistema de ecuaciones*

$$\begin{aligned} \overline{g}(u,v) &= u + u^2 = 0 \\ \frac{\partial \overline{g}(u,v)}{\partial u} &= 1 + 2u = 0 \\ \frac{\partial \overline{g}(u,v)}{\partial v} &= 0 = 0 \end{aligned}$$

no tiene soluciones, entonces $\overline{S} = \emptyset$*.*
Además, $\{(m,n) \in \mathbb{F}_p^2 : u + u^2 = 0\} = \{(0,n) : n \in \mathbb{F}_p\} \cup \{(-1,m) : m \in \mathbb{F}_p\}$*, luego el número de ceros de* $u + u^2 = 0$ *en* $\mathbb{F}_p$ *es* $2p$*.*
Aplicando la FFE al polinomio g *se obtiene*

$$Z(s,g)=\int_{\mathbb{Z}_p^2}|u+u^2-pv^3|_p^s dudv=p^{-2}(p^2-2p)+\frac{p^{-2-s}(1-p^{-1})2p}{1-p^{-1-s}}.$$

Por tanto,

$$\begin{aligned}Z(s,f) &= p^{-2}(p^{-2}-p)+\frac{p^{-2-s}(1-p^{-1})(p-1)}{1-p^{-1-s}}\\ &\quad +p^{-2-2s}\left\{p^{-2}(p^2-2p)+\frac{2p^{-1-s}(1-p^{-1})}{1-p^{-1-s}}\right\}.\end{aligned}$$

Ejemplo 2.3 *Una* ***forma fuertemente no degenerada*** *es un polinomio $f(x_1,\cdots,x_k)$ homogéneo tal que $\overline{f}(\overline{a})=\frac{\partial\overline{f}(\overline{a})}{\partial x_i}(\overline{a})=0$, $1\leq i\leq n$, implica que $\overline{a}=0$.*
En [7], Jay R. Goldman probó que si $f(x)\in\mathbb{Z}_p[x_1,\cdots,x_n]$ es una forma fuertemente no degenerada de grado d, la serie de Poincaré está dada por

$$P(t)=\frac{R(t)}{(1-p^{n-1}t)(1-p^{n(d-1)}t^d)},\quad t=p^{-s},$$

donde $R(t)$ es un polinomio de grado d que se calcula de manera fácil y eficaz.

A continuación se calcula la función zeta local de Igusa asociada a este tipo de polinomos.

Sea $f(x)\in\mathbb{Z}_p[x_1,\cdots,x_n]\setminus p\mathbb{Z}_p[x_1,\cdots,x_n]$ una forma fuertemente no degenerada de grado d, la función $Z(s,f)$ se puede calcular usando la FFE de la siguiente manera. Se tiene
$E=\mathbb{Z}_p^n$, $\overline{E}=\mathbb{F}_p^n$, $S=(p\mathbb{Z}_p)^n$ y $\overline{S}=\{0\}$, luego

$$\begin{aligned}Z(s,f) &= p^{-n}(p^n-N)+\frac{p^{-n-s}(1-p^{-1})(N-1)}{1-p^{-1-s}}+\int_{(p\mathbb{Z}_p)^n}|f(x)|_p^s d^nx\\ &= p^{-n}(p^n-N)+\frac{p^{-n-s}(1-p^{-1})(N-1)}{1-p^{-1-s}}+p^{-n-ds}\int_{\mathbb{Z}_p^n}|f(y)|_p^s d^ny\\ &= p^{-n}(p^n-N)+\frac{p^{-n-s}(1-p^{-1})(N-1)}{1-p^{-1-s}}+p^{-n-ds}Z(s,f).\end{aligned}$$

Por lo tanto,

$$Z(s,f)=\frac{1}{1-p^{-n-ds}}\left\{p^{-n}(p^n-N)+\frac{p^{-n-s}(1-p^{-1})(N-1)}{1-p^{-1-s}}\right\}.$$

Ejemplo 2.4 *Sea $f(x,y) = x^2 - y^3$, donde $p \neq 2, 3$.*
Para usar la fórmula de la fase estacionaria hay que observar que $E = \mathbb{Z}_p^2$, $\overline{E} = \mathbb{F}_p^2$, $\overline{S} = \{(0,0)\}$, $S = p\mathbb{Z} \times p\mathbb{Z}_p$ y al igual que en el ejemplo 2.2 se tiene que $N = p$.
Aplicando la fórmula de la fase estacionaria se obtiene

$$\begin{aligned} Z(s) &= p^{-2}(p^2 - p) + \frac{p^{-2-s}(1-p^{-1})(p-1)}{1-p^{-1-s}} + \int_{(p\mathbb{Z}_p)^2} |x^2 - y^3|_p^s dxdy \\ &= (1-p^{-1})\frac{1-p^{-2-s}}{1-p^{-1-s}} + \int_{(p\mathbb{Z}_p)^2} |x^2 - y^3|_p^s dxdy. \end{aligned}$$

Haciendo el cambio de variables $x = pu$, $y = pv$, $u, v \in \mathbb{Z}_p$, se tiene $dxdy = p^{-2}dudv$ y así

$$\begin{aligned} Z(s) &= (1-p^{-1})\frac{1-p^{-2-s}}{1-p^{-1-s}} + p^{-2-2s}\int_{\mathbb{Z}_p^2} |u^2 - pv^3|_p^s dudv \\ &= (1-p^{-1})\frac{1-p^{-2-s}}{1-p^{-1-s}} + p^{-2-2s}Z_1(s). \end{aligned}$$

Para aplicar la fórmula de la fase estacionaria a $Z_1(s)$ hay que observar que $E = \mathbb{Z}_p^2$, $\overline{E} = \mathbb{F}_p^2$.
Sea $g(u,v) = u^2 - pv^3$. El conjunto solución de el sistema de ecuaciones

$$\begin{aligned} \overline{g}(u,v) &= u^2 = 0 \\ \frac{\partial \overline{g}(u,v)}{\partial u} &= 2u = 0 \\ \frac{\partial \overline{g}(u,v)}{\partial v} &= 0 = 0 \end{aligned}$$

es $\overline{S} = \{0\} \times \mathbb{F}_p$, entonces $S = p\mathbb{Z}_p \times \mathbb{Z}_p$. Además, el número de ceros de u^2 en $\mathbb{F}_p$ es igual al número $\#\{(u,v) \in \mathbb{F}_p^2 : u^2 = 0\} = p$.
Así,

$$\begin{aligned} Z_1(s) &= p^{-2}(p^2 - p) + \int_{p\mathbb{Z}_p \times \mathbb{Z}_p} |u^2 - pv^3|_p^s dudv \\ &= (1-p^{-1}) + p^{-1-s}\int_{\mathbb{Z}_p^2} |pu_1^2 - v^3|_p^s du_1 dv \qquad (u = pu_1, \;\; u_1 \in \mathbb{Z}_p) \\ &= (1-p^{-1}) + p^{-1-s}Z_2(s). \end{aligned}$$

Por tanto,

$$Z(s) = (1-p^{-1})\frac{1-p^{-2-s}}{1-p^{-1-s}} + p^{-2-2s}(1-p^{-1}) + p^{-3-3s}Z_2(s).$$

Para aplicar FFE a $Z_2(s)$ hay que observar que $E = \mathbb{Z}_p^2$, $\overline{E} = \mathbb{F}_p^2$.
Sea $g_1(u_1, v) = pu_1^2 - v^3$. El conjunto solución de el sistema de ecuaciones

$$\begin{aligned}
\overline{g_1}(u_1, v) &= -v^3 = 0 \\
\frac{\partial \overline{g_1}(u_1, v)}{\partial u_1} &= 0 = 0 \\
\frac{\partial \overline{g_1}(u_1, v)}{\partial v} &= -2v = 0
\end{aligned}$$

es $\overline{S} = \mathbb{F}_p \times \{0\}$, entonces $S = \mathbb{Z}_p \times p\mathbb{Z}_p$. Además, el número de ceros de $-v^3$ en $\mathbb{F}_p$ es igual al número $\#\{(u, v) \in \mathbb{F}_p^2 : -v^3 = 0\} = p$.
Así,

$$\begin{aligned}
Z_2(s) &= p^{-2}(p^2 - p) + \int_{\mathbb{Z}_p \times p\mathbb{Z}_p} |pu_1^2 - v^3|_p^s du_1 dv \\
&= (1 - p^{-1}) + p^{-1-s} \int_{\mathbb{Z}_p^2} |u_1^2 - p^2 v_1^3|_p^s du_1 dv_1 \qquad (v = pv_1, \;\; v_1 \in \mathbb{Z}_p) \\
&= (1 - p^{-1}) + p^{-1-s} Z_3(s).
\end{aligned}$$

Por tanto,

$$Z(s) = (1 - p^{-1}) \frac{1 - p^{-2-s}}{1 - p^{-1-s}} + p^{-2-2s}(1 - p^{-1}) + p^{-3-3s}(1 - p^{-1}) + p^{-4-4s} Z_3(s).$$

Para aplicar FFE a $Z_3(s)$ hay que observar que $E = \mathbb{Z}_p^2$, $\overline{E} = \mathbb{F}_p^2$.
Sea $g_2(u_1, v_1) = u_1^2 - p^2 v_1^3$. El conjunto solución de el sistema de ecuaciones

$$\begin{aligned}
\overline{g_2}(u_1, v_1) &= u_1^2 \\
\frac{\partial \overline{g_2}(u_1, v_1)}{\partial u_1} &= 2u_1 = 0 \\
\frac{\partial \overline{g_1}(u_1, v_1)}{\partial v_1} &= 0 = 0
\end{aligned}$$

es $\overline{S} = \{0\} \times \mathbb{F}_p$, entonces $S = p\mathbb{Z}_p \times \mathbb{Z}_p$. Además, el número de ceros de u_1^2 en $\mathbb{F}_p$ es igual al número $\#\{(u, v) \in \mathbb{F}_p^2 : u^2 = 0\} = p$.
Así,

$$\begin{aligned}
Z_3(s) &= p^{-2}(p^2 - p) + \int_{p\mathbb{Z}_p \times \mathbb{Z}_p} |u_1^2 - p^2 v_1^3|_p^s du_1 dv_1 \\
&= (1 - p^{-1}) + p^{-1-2s} \int_{\mathbb{Z}_p^2} |u_2^2 - v_1^3|_p^s du_2 dv_1 \qquad (u_1 = pu_2, \;\; u_2 \in \mathbb{Z}_p) \\
&= (1 - p^{-1}) + p^{-1-2s} Z(s).
\end{aligned}$$

Luego,

$$\begin{aligned} Z(s) &= (1-p^{-1})\frac{1-p^{-2-s}}{1-p^{-1-s}} + p^{-2-2s}(1-p^{-1}) + p^{-3-3s}(1-p^{-1}) \\ &\quad + p^{-4-4s}(1-p^{-1}) + p^{-5-6s}Z(s). \end{aligned}$$

Por lo tanto,

$$\begin{aligned} Z(s) &= \frac{(1-p^{-1})}{1-p^{-5-6s}}\left(\frac{1-p^{-2-s}}{1-p^{-1-s}} + p^{-2-2s} + p^{-3-3s} + p^{-4-4s}\right) \\ &= \frac{1-p^{-1}}{(1-p^{-1-s})(1-p^{-5-6s})}\left(1-p^{-2-s}+p^{-2-2s}-p^{-5-5s}\right). \end{aligned}$$

Ejemplo 2.5 *Se calcula la función zeta local para un polinomio del tipo $f(x,y) = \alpha x^n + \beta y^m$, $\alpha, \beta \in \mathbb{Z}_p$, donde $m, n > 1$ son primos relativos y p no divide simultáneamente a n y m. La serie de Poncaré asociada a este tipo de polinomios fue calculada en el teorema 1 de [8]. También se caulcula en [1] y [24] usando la fórmula de la fase estacionaria.*
Sin pérdida sustancial de generalidad se puede suponer $\alpha \in \mathbb{Z}_p^\times$.
Sea

$$A = \{(x,y) \in \mathbb{Z}_p^2 : v_p(x) \geq m, v_p(y) \geq n\}.$$

Entonces $Z(f,s)$ se puede expresar como

$$Z(f,s) = \int_A |\alpha x^n + \beta y^m|_p^s dxdy + \int_{A^c} |\alpha x^n + \beta y^m|_p^s dxdy,$$

haciendo el cambio de variable $x = p^m u$, $y = p^n v$ con $u, v \in \mathbb{Z}_p$ se tiene $dx = p^{-m}du$, $dy = p^{-n}dv$ y $f(p^m u, p^n v) = p^{mn} f(u,v)$.
La primera integral queda

$$\begin{aligned} \int_A |\alpha x^n + \beta y^m|_p^s dxdy &= \int_{\mathbb{Z}_p^2} |p^{mn}(\alpha u^n + \beta v^m)|_p^s p^{-n-m} dudv \\ &= p^{-mns-n-m}\int_{\mathbb{Z}_p^2} |\alpha u^n + \beta v^m|_p^s dudv \\ &= p^{-mns-m-n} Z(f,s). \end{aligned}$$

$$\Longrightarrow Z(f,s) = p^{-mns-m-n} Z(f,s) + \int_{A^c} |\alpha x^n + \beta y^m|_p^s dxdy.$$

Así,

$$Z(f,s) = \frac{1}{1-p^{-mns-m-n}} \int_{A^c} |\alpha x^n + \beta y^m|_p^s dxdy. \tag{2.2}$$

Para calcular la integral restante hay que observar que el complemento de A con respecto a $\mathbb{Z}_p^2$, A^c, es la unión disjunta de los tres conjuntos:

$$\begin{aligned} A_1 &= \{(x,y) \in \mathbb{Z}_p^2 : v_p(x) < m, v_p(y) \geq n\}, \\ A_2 &= \{(x,y) \in \mathbb{Z}_p^2 : v_p(x) < m, v_p(y) < n\}, \\ A_3 &= \{(x,y) \in \mathbb{Z}_p^2 : v_p(x) \geq m, v_p(y) < n\}, \end{aligned}$$

de la ecuación (2.2) se obtiene

$$Z(f,s) = \frac{1}{1-p^{-mns-m-n}} \left\{ Z(f,A_1,s) + Z(f,A_2,s) + Z(f,A_3,s) \right\}.$$

<u>Cálculo de $Z(f,A_1,s)$:</u>

Si $(x,y) \in A_1$ se tiene

$$\begin{aligned} &|\beta y^m|_p = p^{-mv_p(y)-v_p(\beta)} \leq p^{-nm} < |\alpha x^n|_p = |x^n|_p \\ &\Longrightarrow |\alpha x^n + \beta y^m|_p = \text{máx}\{|\beta y^m|_p, |\alpha x^n|_p\} = |x^n|_p. \end{aligned}$$

Así,

$$\begin{aligned} Z(f,A_1,s) &= \int_{A_1} |\alpha x^n + \beta y^m|_p^s dxdy \\ &= \sum_{k=0}^{m-1} \int_{\{(x,y)\in A_1 : v_p(x)=k, v_p(y)\geq n\}} |x^n|_p^s dxdy \\ &= \sum_{k=0}^{m-1} p^{-kns} \int_{\{(x,y)\in A_1 : v_p(x)=k, v_p(y)\geq n\}} dxdy \\ &= \sum_{k=0}^{m-1} p^{-kns}(p^{-n}(p^{-k}(1-p^{-1}))) \\ &= p^{-n}(1-p^{-1}) \sum_{k=0}^{m-1} p^{-kns-k}. \end{aligned}$$

<u>Cálculo de $Z(f,A_2,s)$:</u>

Sea $L(i,j) := jm - in + v_p(\beta)$. El conjunto A_2 puede describirse como la unión disjunta de los tres subconjuntos

$$\begin{aligned} A_{2,1} &= \{(x,y) \in A_2 : L(v_p(x), v_p(y)) > 0\}, \\ A_{2,2} &= \{(x,y) \in A_2 : L(v_p(x), v_p(y)) < 0\}, \\ A_{2,3} &= \{(x,y) \in A_2 : L(v_p(x), v_p(y)) = 0\}. \end{aligned}$$

Luego,

$$Z(f, A_2, s) = Z(f, A_{2,1}, s) + Z(f, A_{2,2}, s) + Z(f, A_{2,3}, s).$$

1. *Para calcular* $Z(f, A_{2,1}, s)$ *hay que observar que*

$$L(v_p(x), v_p(y)) > 0 \Longrightarrow -nv_p(x) > -mv_p(y) - v_p(\beta) \Longrightarrow |\alpha x^n|_p > |\beta y^n|_p$$

$$\Longrightarrow |\alpha x^n + \beta y^m|_p = |\alpha x^n|_p.$$

Si i, j *satisfacen* $L(i,j) > 0$, $0 \leq i < m$, $0 \leq j < n$, *poniendo*

$$I = \int_{\{(x,y) \in A_{2,1} : v_p(x) = i, v_p(y) = j\}} |f(x,y)|_p^s dxdy$$

entonces

$$\begin{aligned} I &= \int_{\{(x,y) \in A_{2,1} : v_p(x) = i, v_p(y) = j\}} |x^n|_p^s dxdy \\ &= p^{-ins} p^{-i}(1 - p^{-1}) p^{-j}(1 - p^{-1}) \\ &= (1 - p^{-1})^2 p^{-i-j-ins}. \end{aligned}$$

Así,

$$Z(f, A_{2,1}, s) = (1 - p^{-1})^2 \sum_{i,j} p^{-i-j-ins}$$

donde i, j *satisfacen* $L(i,j) > 0$, $0 \leq i < m$, $0 \leq j < n$.

2. *Análogamente al caso anterior se obtiene*

$$Z(f, A_{2,2}, s) = (1 - p^{-1})^2 \sum_{i,j} p^{-i-j-(v_p(\beta)+mj)s}$$

donde i, j *satisfacen* $L(i,j) < 0$, $0 \leq i < m$, $0 \leq j < n$.

3. *Por último se tiene*

$$L(v_p(x), v_p(y)) = 0 \Longrightarrow v_p(x) = v_p(y) + v_p(\beta).$$

Si i, j *satisfacen* $L(i,j) = 0$, $0 \leq i < m$, $0 \leq j < n$, *entonces haciendo los siguientes cambios de variable*

$$\begin{aligned} \beta &= tp^{v_p(\beta)} \quad t \in \mathbb{Z}_p^\times, \\ x &= up^i \quad u \in \mathbb{Z}_p^\times, \\ y &= vp^j \quad v \in \mathbb{Z}_p^\times. \end{aligned}$$

y tomando

$$I = \int_{\{(x,y)\in A_{2,3}: v_p(x)=i, v_p(y)=j\}} |f(x,y)|_p^s dxdy$$

se obtiene

$$\begin{aligned} I &= \int_{\mathbb{Z}_p^\times \times \mathbb{Z}_p^\times} |p^{in}(\alpha u^n + tv^m)|_p^s p^{-i-j} dudv \\ &= p^{-i-j-ins} \int_{\mathbb{Z}_p^\times \times \mathbb{Z}_p^\times} |\alpha u^n + tv^m|_p^s dudv. \end{aligned}$$

Usando la fórmula de la fase estacionaria la integral anterior queda

$$\int_{\mathbb{Z}_p^\times \times \mathbb{Z}_p^\times} |\alpha u^n + tv^m|_p^s dudv = p^2((p-1)^2 - N) + \frac{p^{-2-s}(1-p^{-1})N}{1-p^{-1-s}}$$

pues $\overline{S} = \emptyset$.

Luego,

$$\begin{aligned} &\int_{\{(x,y)\in A_{2,3}: v_p(x)=i, v_p(y)=j\}} |f(x,y)|_p^s dxdy \\ &= p^{-i-j-ins}\left(p^2((p-1)^2 - N) + \frac{p^{-2-s}(1-p^{-1})N}{1-p^{-1-s}}\right) \end{aligned}$$

Así,

$$Z(f, A_{2,3}, s) = \left(p^2((p-1)^2 - N) + \frac{p^{-2-s}(1-p^{-1})N}{1-p^{-1-s}}\right) \sum_{i,j} p^{-i-j-ins}$$

donde i, j *satisfacen* $L(i,j) = 0$, $0 \leq i < m$, $0 \leq j < n$.

Cálculo de $Z(f, A_3, s)$:

Por el algoritmo de la división existen $t, r \in \mathbb{Z}$ tales que

$$v_p(\beta) = tn + r \quad 0 \leq r < n.$$

Sean

$$\begin{aligned} A_{3,1} &:= \{(x,y) \in A_3 : v_p(x) \geq m+t+r, v_p(y) < n\}, \\ A_{3,2} &:= \{(x,y) \in A_3 : v_p(x) \leq m+t+r-1, v_p(y) < n\}. \end{aligned}$$

Entonces $A_3 = A_{3,1} \bigsqcup A_{3,2}$ y $Z(f, A_3, s) = Z(f, A_{3,1}, s) + Z(f, A_{3,2}, s)$.

1. *Si $x, y \in A_{3,1}$ entonces*

$$-v_p(x) \leq -m-t-r \quad y \quad -n < -v_p(y)$$

$$\begin{aligned} \Longrightarrow \qquad |\alpha x^n|_p &\leq p^{-mn-tn-nr} \\ &\leq p^{-mn-v_p(\beta)} \\ &< |\beta y^m|_p. \end{aligned}$$

$$\Longrightarrow \quad |\alpha x^n + \beta y^m|_p = \textit{máx}\{|\alpha x^n|_p, |\beta y^m|_p\} = |\beta y^m|_p.$$

Así,

$$\begin{aligned} Z(f, A_{3,1}, s) &= \int_{A_{3,1}} |\beta y^m|_p^s dxdy \\ &= \sum_{k=0}^{n-1} \int_{\{(x,y)\in A_{3,1} : v_p(x)=m+t+r, v_p(y)=k\}} |\beta y^m|_p^s dxdy \\ &= \sum_{k=0}^{n-1} p^{-kms-v_p(\beta)s} \int_{\{(x,y)\in A_{3,1} : v_p(x)=m+t+r, v_p(y)=k\}} dxdy \\ &= \sum_{k=0}^{n-1} p^{-kms-v_p(\beta)s} \left(p^{-m-t-r} p^{-k}(1-p^{-1})\right) \\ &= (1-p^{-1}) p^{-m-t-r} \sum_{k=0}^{n-1} p^{-kms-v_p(\beta)s-k}. \end{aligned}$$

2. *El cálculo de $Z(f, A_{3,2}, s)$ es similar al de $Z(f, A_2, s)$. El conjunto $A_{3,2}$ puede descomponerse en la unión disjunta de los subconjuntos*

$$\begin{aligned} A_{3,2,1} &= \{(x,y) \in A_{3,2} : L(v_p(x), v_p(y)) > 0\}, \\ A_{3,2,2} &= \{(x,y) \in A_{3,2} : L(v_p(x), v_p(y)) < 0\}, \\ A_{3,2,3} &= \{(x,y) \in A_{3,2} : L(v_p(x), v_p(y)) = 0\}. \end{aligned}$$

Luego, $Z(f, A_{3,2}, s) = Z(f, A_{3,2,1}, s) + Z(f, A_{3,2,2}, s) + Z(f, A_{3,2,3}, s)$*.*
Así,

$$Z(f, A_{3,2,1}, s) = (1 - p^{-1})^2 \sum_{i,j} p^{-i-j-ins}$$

donde i, j *satisfacen* $L(i,j) > 0$*,* $m \leq i < m + t + r$*,* $0 \leq j < n$*;*

$$Z(f, A_{3,2,2}, s) = (1 - p^{-1})^2 \sum_{i,j} p^{-i-j-(v_p(\beta)+mj)s}$$

donde i, j *satisfacen* $L(i,j) < 0$*,* $m \leq i < m + t + r$*,* $0 \leq j < n$*, y*

$$Z(f, A_{3,2,3}, s) = \left(p^2((p-1)^2 - N) + \frac{p^{-2-s}(1 - p^{-1})N}{1 - p^{-1-s}} \right) \sum_{i,j} p^{-i-j-ins}$$

donde i, j *satisfacen* $L(i,j) = 0$*,* $m \leq i < m + t + r$*,* $0 \leq j < n$*.*

III. POLINOMIOS SEMICUASIHOMOGÉNEOS

En este capítulo se prueba que la función zeta local de Igusa asociada a un polinomio semicuasihomogéneo es racional. La exposición se basa en las referencias [24] y [1].

III.1. Preliminares

Para un anillo conmutativo A y $f(x) \in A[x]$, $x = (x_1, \cdots, x_n)$, se denota por $V_f(A)$ a la correspondiente hipersuperficie, es decir

$$V_f(A) = \{x \in A^n : f(x) = 0\}$$

y por $Sing_f(A)$ al conjunto de puntos singulares de $V_f(A)$, es decir

$$Sing_f(A) = \{x \in A^n : f(x) = \frac{\partial f}{\partial x_1}(x) = \cdots = \frac{\partial f}{\partial x_n}(x) = 0\}.$$

Ejemplo 3.1 *Tomando $f(x,y) = x^2 - y^3 \in \mathbb{Z}_p[x,y]$ con $p \neq 2,3$, se tiene que $(t^3)^2 - (t^2)^3 = 0$ para cualquier $t \in \mathbb{Z}_p$, luego $\{(t^3, t^2) : t \in \mathbb{Z}_p\} \subset Sing_f(\mathbb{Z}_p)$. Por otro lado, $(0,0)$ es la única solución del sistema*

$$\begin{aligned} f(x,y) = x^2 - y^3 &= 0 \\ \frac{\partial}{\partial x} f(x,y) = 2x &= 0 \\ \frac{\partial}{\partial y} f(x,y) = -3y &= 0. \end{aligned}$$

Así, $Sing_f(\mathbb{Z}_p) = \{(0,0)\}$.

Se usará $R = \{0, 1, \cdots, p-1\} \subset \mathbb{Z}_p$ como un conjunto de representantes del campo de residuos $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{1}, \cdots, \overline{p-1}\}$.

Definición 3.1 *Sean $f(x)$ un polinomio en n variables, $P_1 = (y_1, \cdots, y_n) \in \mathbb{Z}_p^n$ y $m_{P_1} = (m_1, \cdots, m_n) \in \mathbb{N}^n$. Un isomorfismo $\psi_{m_{P_1}} : \mathbb{Q}_p^n \to \mathbb{Q}_p^n$ es una **dilatación**, si satisface $\psi_{m_{P_1}}(x) = (z_1, \cdots, z_n)$, $z_i = y_i + p^{m_i} x_i$, para cada $i = 1, 2, \cdots, n$.*
*La **dilatación de** $f(x)$ **en** P_1 **inducida por** $\psi_{m_{P_1}}$ es el polinomio*

$$f_{P_1}(x) := p^{-e_{P_1}} f(\psi_{m_{P_1}}(x)), \tag{3.1}$$

donde e_{P_1} es el orden mínimo de p en los coeficientes de $f(\psi_{m_{P_1}}(x))$.

La $\mathbb{Q}_p-$hipersuperficie $V_{f_{P_1}}(\mathbb{Q}_p)$ es llamada la ***dilatación de*** V_f ***en*** P_1 ***inducida por*** $\psi_{m_{P_1}}(x)$.
El número e_{P_1} es llamado ***la multiplicidad aritmética de*** $f(x)$ ***en*** P_1 ***por*** $\psi_{m_{P_1}}(x)$.
El conjunto $S(f_{P_1}, E)$ es el subconjunto de $R^n \subset \mathbb{Z}_p^n$ que es enviado biyectivamente por el homomorfismo canónico al conjunto $Sing_{\overline{f}}(\mathbb{F}_p)$.

Ejemplo 3.2 *Sea $f(x,y) = x^2 - y^3 \in \mathbb{Z}_p[x,y]$ con $p \neq 2,3$, tomando $P = (p^2, p)$ y $m_P = (3,2)$, se tiene que $\psi_{m_P}(x,y) = (p^2 + p^3x, p + p^2y)$. Luego,*

$$f(p^2 + p^3x, p + p^2y) = p^4 + 2p^5x + p^6x^2 - p^3 - 3p^4y - 3p^5y^2 - p^6y^3.$$

Entonces, la dilatación de $f(x,y)$ en P inducida por ψ_{m_P} es el polinomio

$$\begin{aligned} f_P(x,y) &= p^{-3}(p^4 + 2p^5x + p^6x^2 - p^3 - 3p^4y - 3p^5y^2 - p^6y^3) \\ &= p + 2p^2x + p^3x^2 - 1 - 3py - 3p^2y^2 - p^3y^3 \\ &= p^3x^2 - p^3y^3 + 2p^2x - 3p^2y^2 - 3py + p - 1. \end{aligned}$$

Dada una sucesión de dilataciones $(\psi_{m_{P_k}}(x))_k$, se definen inductivamente $e_{P_1,\cdots,P_k}$, $f_{P_1,\cdots,P_k}(x)$ y $S(f_{P_1,\cdots,P_k})$ como sigue

$$f_{P_1,\cdots,P_k}(x) = \begin{cases} f(x) & \text{si } k = 0, \\ p^{-e_{P_1,\cdots,P_k}} f_{P_1,\cdots,P_k}(\psi_{m_{P_k}}(x)) & \text{si } k \geq 1, \end{cases} \tag{3.2}$$

donde $P_k \in S(f_{P_1,\cdots,P_{k-1}})$ y $e_{P_1,\cdots,P_k}$ es el mínimo orden de p en los coeficientes de $f_{P_1,\cdots,P_{k-1}}(\psi_{m_{P_k}})(x)$, y donde, para $k \geq 1$,

$$S_k(P_1) = \bigcup_{P_k \in S_{k-1}(P_1)} S(f_{P_1,\cdots,P_k})$$

se llama la $k-$**ésima generación de descendientes de** P_1, donde $S(f_{P_1,\cdots,P_k})$ es el subconjunto de $R^n \subset \mathbb{Z}_p^n$ que es enviado biyectivamente por el homomorfismo canónico al conjunto $Sing_{\overline{f}_{P_1,\cdots,P_k}}(\mathbb{F}_p)$. Por la $0-$ésima generación de descendientes de P_1 se entiende a $\{P_1\}$.

La fórmula de la fase estacionaria de Igusa, se puede reescribir desde el punto de vista de las dilataciones. Para esto, se fijan los m_{P_k}'s igual a $(1, \cdots, 1) \in \mathbb{N}^n$ en la ecuación 3.1, siguiendo la notación del Capítulo 2 se tiene:
La reducción módulo p de un subconjunto $E \subset \mathbb{Z}_p^n$ será denotado por $\overline{E} \subset \mathbb{F}_p^n$. Si $f(x) \in \mathbb{Z}_p[x_1, \cdots, x_n] \setminus p\mathbb{Z}_p[x_1, \cdots, x_n]$ entonces $\overline{f}$ denota su reducción módulo p.
Si A es un conjunto finito $\#A$ denota su número de elementos.

Proposición 3.1 (Fórmula de la fase estacionaria) *Sea $\overline{E} \subset \mathbb{F}_p^n$ y $S(f,E)$ el subconjunto de $R^n \subset \mathbb{Z}_p^n$ que es enviado biyectivamente por el homomorfismo canónico al conjunto $Sing_{\overline{f}}(\mathbb{F}_p) \cap \overline{E}$, cuando $\overline{E} = \mathbb{F}_p^n$ se escribe solamente $S(f)$. Sean S y E las preimagenes de $S(f,E)$ y $\overline{E}$ bajo $\mathbb{Z}_p^n \longrightarrow \mathbb{F}_p^n$ y sea $N_{(\overline{f},\overline{E})}$ el número de ceros de $\overline{f}(x)$ en $\overline{E}$, cuando $\overline{E} = \mathbb{F}_p^n$ se escribe solamente $N_{\overline{f}}$. Entonces*

$$\begin{aligned}\int_E |f(x)|_p^s d^n x &= p^{-n}(\#\overline{E} - N) + \frac{p^{-n-s}(1-p^{-1})(N - \#\overline{S})}{1-p^{-1-s}} \\ &\quad + \sum_{P\in S(f,E)} p^{-n-e_P s} \int_{\mathbb{Z}_p^n} |f_P(x)|_p^s d^n x,\end{aligned}$$

Demostración En la página 57 se probó la igualdad

$$\int_E |f(x)|_p^s d^n x = p^{-n}(\#\overline{E} - N_{(\overline{f},\overline{E})}) + \frac{p^{-n-s}(1-p^{-1})(N_{(\overline{f},\overline{E})} - \#\overline{S})}{1-p^{-1-s}} + \int_S |f(x)|_p^s d^n x.$$

Se tiene

$$\begin{aligned}\int_S |f(x)|_p^s d^n x &= \sum_{P\in S(f,E)} \int_{P+(p\mathbb{Z}_p)^n} |f(x)|_p^s d^n x \\ &= \sum_{P\in S(f,E)} \int_{\mathbb{Z}_p^n} |f(P+px)|_p^s |p|_p^n d^n x \\ &= \sum_{P\in S(f,E)} p^{-n} \int_{\mathbb{Z}_p^n} |f(P+px)|_p^s d^n x \\ &= \sum_{P\in S(f,E)} p^{-n} \int_{\mathbb{Z}_p^n} |p^{e_P} f_P(x)|_p^s d^n x \\ &= \sum_{P\in S(f,E)} p^{-n-e_P s} \int_{\mathbb{Z}_p^n} |f_P(x)|_p^s d^n x.\end{aligned}$$

□

Definición 3.2 *Se define I_k inductivamente como sigue:*

$$I_1 := \{P_1 : P_1 \in S(f,E)\}$$

y

$$I_k := \{(P_1, \cdots, P_k) : (P_1, \cdots, P_{k-1}) \in I_{k-1} \ \ y \ \ P_k \in S(f_{P_1,\cdots,P_{k-1}})\}, \quad k \geq 2.$$

Con la notación anterior e iterando la fórmula de la fase estacionaria se obtiene la siguiente expansión para $Z(f,s)$:

$$\begin{aligned}Z(f,s) &= p^{-n}(\#\overline{E} - N_{(\overline{f},\overline{E})}) + \frac{(1-p^{-1})p^{-n-s}(N_{(\overline{f},\overline{E})} - \#S(f,E))}{1-p^{-1}p^{-s}} \\ &\quad + \sum_{k\geq 1} p^{-kn} \left(\sum_{(P_1,\cdots,P_k)\in I_k} p^{-n}(p^n - N_{\overline{f}_{P_1,\cdots,P_k}}) p^{-E(P_1,\cdots,P_k)s} \right) \qquad (3.3)\end{aligned}$$

$$+L(p^{-s})\sum_{k\geq 1}p^{-kn}\left(\sum_{(P_1,\cdots,P_k)\in I_k}p^{-n}(N_{\overline{f}_{P_1\cdots,P_k}}-\#S(f_{P_1,\cdots,P_k}))p^{-E(P_1,\cdots,P_k)s}\right)$$

donde $L(p^{-s})=\frac{(1-p^{-1})p^{-s}}{1-p^{-1}p^{-s}}$ y $E(P_1,\cdots,P_k):=e_{P_1}+\cdots+e_{P_1,\cdots,P_k}$. La expansión (3.3) converge absolutamente sobre el semiplano $Re(s)>0$.

III.2. Polinomios semicuasihomogéneos

Definición 3.3 *Sea $f(x)$ un polinomio con coeficientes en $\mathbb{Q}_p$ y V_f la correspondiente $\mathbb{Q}_p-$hipersuperficie. Se dice que un punto $P\in\mathbb{Q}_p^n$ es una* ***singularidad aislada de*** *$V_f(\mathbb{Q}_p)$, si la única solución del sistema de ecuaciones*

$$f(x)=\frac{\partial f}{\partial x_1}(x)=\cdots=\frac{\partial f}{\partial x_n}(x)=0,$$

sobre una clausura algebraica fija de $\mathbb{Q}_p$ es el punto P.

Definición 3.4 *Sean $\alpha_1,\cdots,\alpha_n$, n enteros positivos y primos relativos. Un polinomio $f(x)\in\mathbb{Q}_p[x]$ se llama* ***polinomio cuasihomogéneo*** *de peso d y exponentes $\alpha_1,\cdots,\alpha_n$, si satisface*

$$f(t^{\alpha_1}x_1,\cdots,t^{\alpha_n}x_n)=t^d f(x),\quad \textit{para cada } t\in\mathbb{Q}_p$$

y el origen de $\mathbb{Q}_p^n$ es una singularidad aislada de la $\mathbb{Q}_p-$hipersuperficie V_f.

Ejemplo 3.3 *El polinomio $f(x,y)=x^2-y^3$ es un polinomio cuasihomogéneo de peso 6 y exponentes 3 y 2, pues*

$$f(t^3x,t^2y)=t^6x^2-t^6y^3=t^6(x^2-y^3)=t^6f(x,y).$$

Además, el origen de $\mathbb{Q}_p^n$ es una singularidad aislada de la $\mathbb{Q}_p-$hipersuperficie V_f.

Definición 3.5 *Un polinomio $F(x)$ se llama* ***polinomio semicuasihomogéneo*** *si tiene la forma $f(x)+\sum b_ie_i(x)\in\mathbb{Q}_p[x]$, donde $f(x)$ es un polinomio cuasihomogéneo, cada monomio $e_i(x)=x_1^{m_1}\cdots x_n^{m_n}$ satisface $\sum_{j=1}^n\alpha_jm_j>d$ y el origen de $\mathbb{Q}_p^n$ es una singularidad aislada de la $\mathbb{Q}_p-$hipersuperficie V_f. El polinomio $f(x)$ se llama la parte cuasihomogénea de $F(x)$.*

Ejemplo 3.4 *Cualquier polinomio cuasihomogéneo es un polinomio semicuasihomogéneo.*

Definición 3.6 *Sea un polinomio $f(x)\in\mathbb{Z}_p[x]$ y un punto $P\in\mathbb{Z}_p^n$ tal que $P\notin Sing_f(\mathbb{Z}_p)$. Se define*

$$L(f,P):=Inf\left(v_p(f(P)),v_p\left(\frac{\partial f}{\partial x_1}(P)\right),\cdots,v_p\left(\frac{\partial f}{\partial x_n}(P)\right)\right).$$

Ejemplo 3.5 *Sea $f(x,y) = x^2 - y^3 \in \mathbb{Z}_p[x,y]$, con $p \neq 2,3$. Tomando $P = (p^2, p)$, se tiene*

$$\begin{aligned} f(p^2,p) &= p^4 - p^3 \\ \frac{\partial f}{\partial x}(p^2,p) &= 2p^2 \\ \frac{\partial f}{\partial y}(p^2,p) &= -3p^2. \end{aligned}$$

Entonces

$$L(f,P) = Inf\left(v_p(p^4-p^3), v_p(2p^2), v_p(-3p^2)\right) = Inf(3,2,2) = 2.$$

Observación $L(f,P) = 0$ si y sólo si

$$\overline{f(x)} = \alpha_0 + \sum_{j=1}^{n} \alpha_j (x_j - \overline{a_j}) + (\text{términos de grado } \geq 2),$$

donde $P = (a_1, \cdots, a_n), \alpha_j \in \mathbb{F}_p^{\times}$ para algún $j = 0, 1, \cdots, n$.

Se denota por A_r, $r = (r_1 \cdots, r_n) \in (\mathbb{N} \setminus \{0\})^n$, el conjunto

$$A_r := \{x \in \mathbb{Z}_p^n : v(x_i) \geq r_i, \quad i = 1, \cdots, n\}.$$

Desde un punto de vista geométrico, A_r es un polidisco en $\mathbb{Z}_p^n$ centrado en el origen. El complemento de A_r en $\mathbb{Z}_p^n$ se denota por A_r^c.

Proposición 3.2 (Proposition 2.2,[24]) *Sean un polinomio $f(x) \in \mathbb{Z}_p[x]$, $P \in \mathbb{Z}_p^n$ una singularidad aislada de la hipersuperficie V_f y un subconjunto $D \subset \mathbb{Z}_p^n$ tal que $D \cap (P + A_r) = \emptyset$ para algún $r \in (\mathbb{N} \setminus \{0\})^n$. Entonces*

$$L(f,Q) \leq C(f,D), \quad \textit{para cada } Q \in D,$$

donde la constante $C(f,D)$ depende solamente de f y D.

Demostración Sin pérdida de generalidad se puede suponer que el punto P es el origen de $\mathbb{Q}_p^n$. La hipótesis de que el origen de $\mathbb{Q}_p^n$ es una singularidad aislada y teorema de los ceros (Nullstellensatz) de Hilbert, ver por ejemplo [6], implican que

$$p^{m_i} x_i^{t_i} = A_{i,0} f(x) + \sum_{j=1}^{n} A_{i,j}(x) \frac{\partial f}{\partial x_j}(x), \tag{3.4}$$

para algunos $m_i, t_i \in \mathbb{N}$, con $t_i \neq 0$, y algunos polinomios $A_{i,j}(x) \in \mathbb{Z}_p[x]$, para cada $i = 1, \cdots, n$. Ahora, sea $Q = (q_1, \cdots, q_n)$ un punto en D. Como $D \cap A_r = \emptyset$, existe una coordenada j_0 tal que $v_p(q_{j_0}) < r_{j_0}$. De 3.4, con $i = j_0$ y $x = Q$, se obtiene

$$m_{j_0} + t_{j_0} r_{j_0} \geq m_{j_0} + t_{j_0} v(q_{j_0}) \geq L(f,Q).$$

Así, es suficiente con tomar $C(f,D) \geq$máx$_i\{m_i + t_i r_i\}$.

□

Ejemplo 3.6 *Sea* $f(x,y) = x^2 - y^3 \in \mathbb{Z}_p[x,y]$ *con* $p \neq 2,3$, $P = (0,0)$, $D = p\mathbb{Z}_p^\times \times \mathbb{Z}_p^\times$ *y* $A_{(2,3)} = \{(x,y) \in \mathbb{Z}_p^2 : v_p(x) \geq 2 \text{ y } v_p(y) \geq 3\} = p^2\mathbb{Z}_p \times p^3\mathbb{Z}_p$. *Se tiene que* $D \cap A_{(2,3)} = \emptyset$.
Cualquier $Q \in D$ *es de la forma* $Q = (pu_1, u_2)$ *donde* $u_1, u_2 \in \mathbb{Z}_p^\times$. *Se tiene*

$$\begin{aligned} f(pu_1,u_2) &= p^2u_1^2 - u_2^3 \\ \frac{\partial f}{\partial x}(pu_1,u_2) &= 2pu_1 \\ \frac{\partial f}{\partial y}(pu_1,u_2) &= -3u_2^2. \end{aligned}$$

Entonces

$$\begin{aligned} L(f,Q) &= Inf\left(v_p(p^2u_1^2 - u_2^3), v_p(2pu_1), v_p(-3u_2^2)\right) \\ &= Inf(0,1,0) \\ &= 0 \leq 1 \quad \forall Q \in D. \end{aligned}$$

Observación La proposición anterior se puede hacer más general, de la siguiente manera, ver
proposición 2.2, en [25]. Sea $D \subset \mathbb{Z}_p^n$ un subconjunto abierto y compacto, y un polinomio $f(x) \in \mathbb{Z}_p[x]$ tal que $Sing_f(\mathbb{Q}_p) \cap D = \emptyset$. Entonces existe una constante $C(f,D) \in \mathbb{N}$, que depende solamente de f y D, tal que

$$L(f,P) \leq C(f,D), \quad \text{para cada } P \in D.$$

Proposición 3.3 (Proposition 2.3,[24]) *Sean un polinomio* $f(x) \in \mathbb{Z}_p[x]$ *y un punto* $P = (b_1, \cdots, b_n) \in \mathbb{Z}_p^n$ *tal que* $P \notin Sing_f(\mathbb{Z}_p)$. *Entonces existe un entero no negativo y mínimo* $\mu(f,P)$ *tal que el polinomio*

$$f_P(x) = p^{-e_{\mu,P}} f(P + p^\mu x),$$

donde $e_{\mu,P}$ *es el menor orden de* p *en los coeficientes de* $f(P + p^\mu x)$, *satisface*

$$\overline{f_P(x)} = \alpha_0 + \sum_{i=1}^{n} \alpha_i x_i, \quad \alpha_i \in \mathbb{F}_p^\times \quad \textit{para algún } i = 0, 1, \cdots, n.$$

Además, $\mu(f,P) \leq L(f,P) + 1$.

Demostración Se probará por inducción sobre $L(f,P)$.

<u>Caso $L(f,P) = 0$:</u>

En este caso, tomando $\mu(f,P) = 1$ se tiene

$$\begin{aligned} f_P(x) &= p^{-e_P} f(P+px) \\ &= p^{-e_P}\left(f(P) + \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(P) p x_i + \ p^2(\text{términos de grado } \geq 2)\right), \end{aligned}$$

donde e_P es el menor orden de π en los coeficientes de $f(P+px)$, como $L(f,P)=0$ entonces $e_P = 0$ ó $e_P = 1$. Así,

$$\overline{f_P(x)} = \alpha_0 + \sum_{i=1}^{n} \alpha_i x_i,$$

donde $\alpha_j \in \mathbb{F}_p^\times$ para algún $j = 0, 1, \cdots, n$.
Por otro lado, también se cumple $\mu(f,P) \leq L(f,P)+1$.

<u>Caso $L(f,P) > 0$:</u>

En este caso, se tiene

$$f(x) = \alpha_0 + \sum_{i=1}^{n} \alpha_i (x_i - b_i) + \ (\text{términos de grado } \geq 2),$$

donde $\alpha_i \equiv 0 \pmod{p}$, para $i = 0, 1, \cdots, n$. Luego,

$$f(P+px) = p\left(\alpha_0' + \sum_{i=1}^{n} \alpha_i x_i + \ p(\text{términos de grado } \geq 2)\right).$$

Se consideran dos casos dependiendo de si $\alpha_0' \not\equiv 0 \pmod{p}$ o no.

<u>$\alpha_0' \not\equiv 0 \pmod{p}$:</u>

En este caso, se tiene

$$f(P+px) = p f_p(x),$$

donde

$$f_P(x) = \alpha_0' + \sum_{i=1}^{n} \alpha_i x_i + \ p(\text{términos de grado } \geq 2).$$

Por tanto, $\overline{f_P(x)} = \overline{\alpha_0'} \in \mathbb{F}_p^\times$ y $\mu(f,P) = 1 \leq L(f,P)$.

<u>$\alpha_0' \equiv 0 \pmod{p}$:</u>

En este caso, se tiene

$$f(P+px) = p^2\left(\alpha_0'' + \sum_{i=1}^{n}\alpha_i' x_i + \quad \text{(términos de grado } \geq 2)\right) = p^{e_{\mu,P}} f_P(x),$$

donde $e_{\mu,P} \geq 2$. Entonces

$$f(P) = p^{e_{\mu,P}} f_P(0)$$

y

$$\frac{\partial f}{\partial x_i}(P) = p^{e_{\mu,P}-1}\frac{\partial f_P}{\partial x_i}(0), \quad i = 1, \cdots, n.$$

Así, $L(f_P, 0) \leq L(f, P) - 1$. Aplicando la hipótesis de inducción a f_P se tiene que existe un entero no negativo y mínimo $\mu(f_P, 0) := \mu'$ tal que el polinomio

$$f_{P,0}(x) = p^{-e_{\mu',0}} f_P(p^{\mu'} x),$$

donde $e_{\mu',0}$ es el menor orden de p en los coeficientes de $f_P(p^{\mu'} x)$, satisface

$$\overline{f_{P,0}(x)} = \alpha_0 + \sum_{i=1}^{n}\alpha_i x_i, \quad \alpha_i \in \mathbb{F}_p^{\times} \quad \text{para algún } i = 0, 1, \cdots, n.$$

Además, $\mu(f_P, 0) \leq L(f_P, 0) + 1$.
Por otro lado, se tiene

$$\begin{aligned} f_{P,0}(x) &= p^{-e_{\mu',0}} f_P(p^{\mu'} x) \\ &= p^{-e_{\mu',0}}(p^{-e_P} f(P + p^{\mu'+1} x)) \\ &= p^{-e_{\mu',0}-e_P} f(P + p^{\mu'+1} x). \end{aligned}$$

Por tanto, $\mu(f, P) = \mu(f_P, 0) + 1$.
Además $\mu(f, P) = \mu(f_P, 0) + 1 \leq L(f_P, 0) + 1 + 1 \leq L(f, P) + 1$.

□

Ejemplo 3.7 *Sea $f(x, y) = x^2 - y^3 \in \mathbb{Z}_p[x, y]$ con $p \neq 2, 3$, y $P = (p^2, p)$. Se tiene que $L(f, P) = 2$, por otro lado*

$$f(p^2 + p^{\mu}x, p + p^{\mu}y) = p^4 + 2p^{2+\mu}x + p^{2\mu}x^2 - p^3 - 3p^{2+\mu}y - 3p^{2\mu+1}y^2 - p^{3\mu}y^3.$$

El valor de μ buscado es $\mu = 2$. Se tiene,

$$f(p^2 + p^2 x, p + p^2 y) = p^4 + 2p^4 x + p^4 x^2 - p^3 - 3p^4 y - 3p^5 y^2 - p^6 y^3.$$

Luego,

$$\begin{aligned} f_P(x, y) &= p^{-3}(p^4 + 2p^4 x + p^4 x^2 - p^3 - 3p^4 y - 3p^5 y^2 - p^6 y^3) \\ &= p + 2px + px^2 - 1 - 3py - 3p^2 y^2 - p^3 y^3. \end{aligned}$$

Así,

$$\overline{f_P(x, y)} = -1.$$

Como una consecuencia de las dos proposiciones anteriores se obtiene el siguiente lema.

Lema 3.1 (Lemma 2.4,[24]) *Sea un polinomio $f(x) \in \mathbb{Z}_p[x]$ tal que el origen de $\mathbb{Q}_p^n$ es una singularidad aislada algebraicamente absoluta. Sea A_r un polidisco con $r \in (\mathbb{N} \setminus \{0\})^n$. Entonces existe $\gamma = \gamma(f, r) \in \mathbb{N} \setminus \{0\}$, tal que el polinomio*

$$f_Q(x) = p^{-e_{Q,\gamma}} f(Q + p^\gamma x),$$

satisface la condición de que $\overline{f_Q(x)}$ es una constante no cero o un polinomio lineal con o sin término constante, para todo $Q \in A_r^c$.

III.3. Racionalidad de la función zeta local de Igusa asociada a un polinomio semicuasihomogéneo

Lema 3.2 (Lemma 3.1,[24]) *Sea $D \subset \mathbb{Z}_p^n$ la preimagen bajo el homomorfismo canónico $\mathbb{Z}_p \to \mathbb{Z}_p/p\mathbb{Z}_p$ de un subconjunto $\overline{D} \subset \mathbb{F}_p^n$. Sea un polinomio $f(x) \in \mathbb{Z}_p[x]$ tal que el origen es una singularidad aislada de $V_f(\mathbb{Q}_p)$, si $D \cap A_r = \emptyset$, para algún $r \in (\mathbb{N} \setminus \{0\})^n$, entonces la integral $Z(f, D, s) = \int_D |f(x)|_p^s |dx|$ es una función racional de p^{-s}. Más precisamente,*

$$Z(f, D, s) = \frac{L(p^{-s}, D)}{1 - p^{-1}p^{-s}}. \tag{3.5}$$

Además, el polinomio $L(p^{-s}, D)$ se puede calcular efectivamente.

Demostración Aplicando la fórmula de la fase estacionaria $m + 1 = \gamma(f, r)$ veces, se obtiene

$$\begin{aligned} Z(f, s) = p^{-n}(\#\overline{E} - N_{(\overline{f},\overline{E})}) + \frac{(1 - p^{-1})p^{-n-s}(N_{(\overline{f},\overline{E})} - \#S(f, E))}{1 - p^{-1}p^{-s}} \\ + \sum_{k=1}^{m} p^{-kn} \left(\sum_{(P_1,\cdots,P_k)\in I_k} p^{-n}(p^n - N_{\overline{f}_{P_1,\cdots,P_k}}) p^{-E(P_1,\cdots,P_k)s} \right) \end{aligned} \tag{3.6}$$

$$+L(p^{-s}) \sum_{k=1}^{m} p^{-kn} \left(\sum_{(P_1,\cdots,P_k)\in I_k} p^{-n}(N_{\overline{f}_{P_1\cdots,P_k}} - \#S(f_{P_1,\cdots,P_k})) p^{-E(P_1,\cdots,P_k)s} \right)$$

$$+ \sum_{(P_1,\cdots,P_{m+1})\in I_{m+1}} p^{-(m+1)n-E(P_1,\cdots,P_{m+1})s} \int_{\mathbb{Z}_p^n} |f_{P_1,\cdots,P_{m+1}}(x)|_p^s d^n x.$$

Donde $L(p^{-s}) = \frac{(1-p^{-1})p^{-s}}{1-p^{-1}p^{-s}}$. Por otro lado, se tiene

$$f(P_1 + P_2 p + \cdots + P_m p^{m+1} + p^{m+2} x) = p^{E(P_1,\cdots,P_m)} f_{P_1,\cdots,P_m}(x), \tag{3.7}$$

y $P_1 + P_2 p + \cdots + P_m p^{m+1} \in A_r^c$. Como $m + 2 > \gamma(f, r)$ se sigue del lema 3.1 y (3.7) que la $\mathbb{F}_p-$hipersuperficie definida por $\overline{f_{P_1,\cdots,P_m}(x)}$ es suave o vacía. Entonces $I_{m+1} = \emptyset$, y la integral $Z(f, D, s)$ es una función racional de la forma (3.5).

□

Lema 3.3 (Lemma 3.2,[24]) *Sea $f(x) \in \mathbb{Z}_p[x]$ un polinomio tal que el origen es una singularidad aislada algebraicamente absoluta de $V_f(\mathbb{Q}_p)$. Entonces la integral $Z(f, A_r^c, s) = \int_{A_r^c} |f|_p^s d^n x$ es una función racional de p^{-s}. Más precisamente,*

$$Z(f, A_r^c, s) \quad = \quad \frac{L(p^{-s})}{1 - p^{-1} p^{-s}}. \tag{3.8}$$

Además, el polinomio $L(p^{-s})$ puede ser calculado de manera efectiva.

Demostración Se introduce una familia $\mathcal{L}$ de conjuntos definidos de la siguiente manera: para cada subconjunto B de $\{1, \cdots, n\}$ y cada $a = (a_1, \cdots, a_n) \in \mathbb{N}^n$ que satisface
$0 \leq a_i < r_i$ si $i \in B$, se define

$$D(B, a) := \begin{cases} \{x \in A_r^c : v_p(x_i) = a_i \ \text{ si } i \in B\}, & \text{si } B \neq \emptyset, \\ \emptyset, & \text{si } B = \emptyset. \end{cases} \tag{3.9}$$

La familia $\mathcal{L}$ es cerrada bajo intersecciones y su unión es A_r^c. Se denota por J el conjunto de índices $\{(B, a)\}$ y por $\mathcal{P}(J)_i$ la familia de subconjuntos de J con i elementos. Así,

$$Z(f, A_r^c, s) = \sum_{i=1}^{\#\{J\}} (-1)^{i-1} \sum_{T \in \mathcal{P}(J)_i} \int_{D(T)} |f|_p^s d^n x, \tag{3.10}$$

donde $D(T) := \cap_{(B,a) \in T} D(B, a)$. De (3.10) y el hecho de que la familia $\mathcal{L}$ es cerrada bajo intersecciones, se sigue que para probar el teorema es suficiente probar que cualquier integral del tipo

$$\int_{D(B,a)} |f|_p^s d^n x, \quad B \neq \emptyset, \tag{3.11}$$

es una función racional de la forma $L(p^{-s}, D(B, a))/(1 - p^{-1} p^{-s})$, donde el numerador del polinomio se puede calcular de manera efectiva. Haciendo el siguiente cambio de variables en (3.11):

$$x = \psi_{(B,a)}(y), \ \ donde \ \ x_i = \begin{cases} p^{a_i} y_i & \text{si } i \in B, \\ y_i & \text{si } i \notin B. \end{cases} \tag{3.12}$$

se obtiene

$$\int_{D(B,a)} |f|_p^s d^n x = p^{-e_{(B,a)}s - d_{(B,a)}} \int_{D'(B,a)} |f_B|_p^s d^n y,$$

donde $d_{(B,a)} = \sum_{i \in B} a_i$, $f_B(y)$ es la dilatación de f inducida por (3.12) y

$$D'(B,a) = \prod_{i=1}^{n} R_i,$$

donde $R_i = \mathbb{Z}_p$ si $i \notin B$ y $R_i = \mathbb{Z}_p^\times$ si $i \in B$.
Por otro lado, $\psi_{(B,a)}(y)$ define un $\mathbb{Q}_p-$isomorfismo de $\mathbb{Q}_p^n \to \mathbb{Q}_p^n$, así los puntos $\mathbb{Q}_p-$singulares de V_f son enviados de manera biyectiva a los puntos $\mathbb{Q}_p-$singulares de V_{f_B}. Por lo tanto, el polinomio f_B y el conjunto $D'(B,a)$, $B \neq \emptyset$, satisfacen las condiciones de el lema 3.2. Entonces la integral $\int_{D'(B,a)} |f_B|_p^s d^n x$ es una función racional de p^{-s} y su numerador puede ser calculado de manera efectiva.

□

Proposición 3.4 (Proposition 3.3,[24]) *Sea un polinomio $F(x) = f(x) + p^m g(x) \in \mathbb{Z}_p[x]$ tal que el origen de $\mathbb{Q}_p^n$ es una singularidad aislada de $V_F(\mathbb{Q}_p)$. Sea $D \subset \mathbb{Z}_p^n$ la preimagen bajo el homomorfismo canónico $\mathbb{Z}_p \to \mathbb{Z}_p/p\mathbb{Z}_p$ de un subconjunto $\overline{D} \subset \mathbb{F}_p^n$, y A_r un polidisco tal que $D \cap A_r = \emptyset$, $r \in (\mathbb{N} \setminus \{0\})^n$. Existe $\alpha(f,D)$, que se calcula de manera efectiva, tal que si $m \geq \alpha(f,D)$ entonces*

$$Z(F,D,s) = Z(f,D,s).$$

Demostración Por el 3.1 existe un $\gamma_0 = \gamma(F,r)$ tal que la reducción módulo p de el polinomio

$$F_{P_1,\cdots,P_n}(x) = p^{-E_F(P_1,\cdots,P_n)} F(P_1 + pP_2 + \cdots + p^n P_n + p^{n+1}x) \tag{3.13}$$

es una constante no cero o un polinomio lineal para cada $n \geq \gamma_0$ y cualquier $P_1 + pP_2 + \cdots + p^n P_n \in A_r^c$. Esto implica que $I_{\gamma+1} = \emptyset$. Entonces la integral admite una expansión finita de la forma (3.6). Se tiene

$$g_{P_1,\cdots,P_n} := p^{-E_g(P_1,\cdots,P_n)} g(P_1 + pP_2 + \cdots + p^n P_n + p^{n+1}x),$$

donde $E_g(P_1, \cdots, P_n)$ es el menor orden de p en los coeficientes de

$$g(P_1 + pP_2 + \cdots + p^n P_n + p^{n+1}x).$$

Con esta notación, se tiene que

$$\begin{aligned} F(P_1 + pP_2 + \cdots + p^n P_n + p^{n+1}x) &= p^{-E_f(P_1,\cdots,P_n)} f_{P_1,\cdots,P_n}(x) \\ &+ p^{-E_g(P_1,\cdots,P_n)+m} g_{P_1,\cdots,P_n}(x). \end{aligned} \quad (3.14)$$

Ahora, escogiendo

$$\alpha(f, D) := \text{máx}_{(P_1,\cdots,P_{\gamma_0})\in I_{\gamma_0}}\{1 + E_f(P_1, \cdots, P_{\gamma_0})\}. \quad (3.15)$$

Luego, si $m \geq \alpha(f, D)$, entonces

$$\overline{F_{P_1,\cdots,P_k}(x)} = \overline{f_{P_1,\cdots,P_k}(x)},$$

$$E_F(P_1, \cdots, P_k) = E_f(P_1, \cdots, P_k), \quad 1 \leq k \leq \gamma_0. \quad (3.16)$$

De 3.16 se sigue que

1. $p^{-n}(\#\overline{D} - N_{\overline{f}}) = p^{-n}(\#\overline{D} - N_{\overline{F}})$ e $I_1(f) = I_1(F)$ por que $\overline{f}(x) = \overline{F}(x)$.
2. Para cada $1 \leq k \leq \gamma_0$

   $$p^{-n}(\#\overline{D} - N_{\overline{f}_{P_1,\cdots P_k}}) = p^{-n}(\#\overline{D} - N_{\overline{F}_{P_1,\cdots,P_k}})$$

   para cada $(P_1, \cdots, P_k) \in I_k(f) = I_k(F)$.
3. Para cada $1 \leq k \leq \gamma_0$

   $$I_{k+1}(f) = I_{k+1}(F),$$

   por que $I_k(f) = I_k(F)$ y $\overline{f_{P_1,\cdots,P_k}(x)} = \overline{F_{P_1,\cdots,P_k}(x)}$ para cada $(P_1, \cdots, P_k) \in I_k(f) = I_k(F)$.

Por lo tanto, $I_{\gamma_0+1}(f) = I_{\gamma_0+1}(F) = \emptyset$ y $Z(f, s, D)$ admite una expansión finita de la forma 3.6.
De esto se sigue que $Z(F, D, s) = Z(f, D, s)$.

□

Lema 3.4 (Lemma 3.4, [24]) *Sea un polinomio $F(x) = f(x) + p^m g(x) \in \mathbb{Z}_p[x]$ tal que el origen de $\mathbb{Q}_p^n$ es una singularidad aislada de $V_F(\mathbb{Q}_p)$. Sea A_r un polidisco, con $r \in (\mathbb{N}\backslash\{0\})^n$. Existe $\alpha(f, r)$, que se calcula de manera efectiva, tal que si $m \geq \alpha(f, r)$ entonces*

$$Z(F, A_r^c, s) = Z(f, A_r^c, s).$$

Demostración Por (3.10) es suficiente probar el lema para integrales del tipo (3.11). Escogiendo $\alpha(f,r)$ tal que

$$\alpha(f,r) \geq \text{máx}_{(B,a)}\{e_{f,(B,a)}\}.$$

Con estas condiciones, es suficiente probar que

$$\int_{D'(B,a)} |F_B|_p^s d^n x = \int_{D'(B,a)} |f_B|_p^s d^n x, \tag{3.17}$$

con $D'(B,a)$ como en (3.13) y $F_B(x) = f_B(x) + p^{m-e_{f,(B,a)}} g(\psi_{(B,a)}(x))$.
El resultado se sigue de (3.17) y la proposición 3.4. Finalmente, hay que observar que $\alpha(f,r)$ esta dada por

$$\alpha(f,r) = \text{máx}_{(B,a)}\{e_{f,(B,a)} + \alpha(f_B, D'(B,a))\}.$$

□

Teorema 3.1 (Theorem 3.5, [24]) *Sea un polinomio semicuasihomogéneo $F(x) \in \mathbb{Q}_p[x]$ tal que la parte cuasihomogénea $f(x)$ tiene peso d y exponentes $\alpha_1, \cdots, \alpha_n$. Entonces la función zeta local de Igusa de $F(x)$ es una función racional de p^{-s}. Más precisamente,*

$$Z(F,s) = \frac{L(p^{-s})}{(1-p^{-1}p^{-s})(1-p^{-|\alpha|}p^{-ds})} \tag{3.18}$$

donde $\alpha = (\alpha_1, \cdots, \alpha_n)$ y $|\alpha| = \alpha_1 + \cdots + \alpha_n$. Además, el polinomio $L(p^{-s})$ se puede calcular de manera efectiva.

Demostración Se puede suponer sin pérdida de generalidad que $F(x) \in \mathbb{Z}_p[x]$. Descomponiendo $\mathbb{Z}_p^n$ como la unión disjunta de A_α y A_α^c, usando que $F(x)$ es un polinomio semicuasihomogéneo se obtiene

$$\begin{aligned} Z(F,s) &= \int_{A_\alpha} |F|_p^s d^n x + \int_{A_\alpha^c} |F|_p^s d^n x \\ &= p^{-|\alpha|-ds} \int_{\mathbb{Z}_p^n} |F_1|_p^s d^n x + \int_{A_\alpha^c} |F|_p^s d^n x, \end{aligned} \tag{3.19}$$

donde $F_1(x) = f(x) + p^{m_1} H_1(x)$, con $m_1 \geq 1$. Iterando la fórmula (3.19) $m+1$ veces se obtiene

$$Z(F,s) = Z(F, A_\alpha^c, s) + \sum_{k=1}^{m} p^{k(-|\alpha|-ds)} Z(F_k, A_\alpha^c, s) + p^{(m+1)(-|\alpha|-ds)} Z(F_{m+1}, s), \tag{3.20}$$

donde $F_k(x) = f(x) + p^{m_k} H_k(x)$ con $m_k \to \infty$. Por el lema 3.4, existe $\gamma_0 = \gamma_0(f,\alpha)$, que se puede calcular de manera efectiva, tal que

$$Z(F_k, A^c_\alpha, s) = Z(f, A^c_\alpha, s), \quad \text{para cada } m_k \geq \gamma_0.$$

Luego, de (3.20), se tiene

$$\begin{aligned} Z(F,s) &= Z(F, A^c_\alpha, s) + \sum_{k=1}^{\gamma_0 - 1} p^{k(-|\alpha|-ds)} Z(F_k, A^c_\alpha, s) \\ &+ Z(f, A^c_\alpha, s) p^{(\alpha_0+1)(-|\alpha|-ds)} \frac{1}{1 - p^{-|\alpha|-ds}}. \end{aligned} \tag{3.21}$$

Por el lema 3.3 las integrales $Z(f, A^c_r, s)$ y $Z(F_k, A^s_\alpha, s)$ son funciones racionales de la forma $\frac{L(p^{-s})}{1-p^{-1}p^{-s}}$, donde el polinomio del numerador puede calcularse de manera efectiva.

□

Ejemplo 3.8 *En el ejemplo 2.5 se calculó la función zeta local para un polinomio del tipo $f(x,y) = \alpha x^n + \beta y^n$, $\alpha, \beta \in \mathbb{Z}_p$, donde $m, n > 1$ son primos relativos y p no divide simultáneamente a n y m. En este ejemplo se evidencian los resultados de esta sección.*

Observación Este teorema también es válido si se considera la función zeta local de Igusa sobre cualquier campo local no arquimediano, como puede observarse en [24].

IV. CONCLUSIONES

En el estudio de las funciones zeta locales se mezclan de manera sorprendente ideas de varias teorías matemáticas, como son la geometría algebraica, la teoría de los números, la teoría de las singularidades y la lógica. Además, existe una gran cantidad de conjeturas que relacionan propiedades de las funciones zeta locales con conceptos y objetos de estas teorías.

La racionalidad de $Z(s, f)$ es un problema abierto en característica positiva. En un artículo reciente [14], Igusa ha sugerido que un estudio cuidadoso de su fórmula de la fase estacionaria puede conducir a una nueva demostración de la racionalidad de las funciones zeta locales en cualquier característica. Wilson A. Zuñiga Galindo ha empleado exitosamente esta sugerencia para comprobar la validez de la conjetura para amplias clases de polinomios, [24], [25], [26].

Los cálculos presentados en esta tesis son válidos en cualquier característica, lo cual hace pensar que la racionalidad de $Z(f, s)$ podrá probarse utilizando la fórmula de la fase estacionaria.

BIBLIOGRAFÍA

[1] V. S. Albis and W. A. Zuñiga, *Una introducción elemental a la teoría de las funciones zeta locales de Igusa*, Lecturas Matemáticas 20 (1999); 5-33.

[2] J. Denef, *The racionality of the Poincaré series associated to the p-adic points on a variety*, Invent. Math. 77 (1984), 1-23.

[3] J. Denef, *Report on Igusa's local zeta functions*, Seminaire Bourbaki 741 (1990-1991), Astérisque No. 201-302 (1991), 359-386.

[4] B. Dragovich, A. Yu. Khrennikov, S. V. Kozyrev and I. V. Volovich, *On p-adic Mathematical Physics*, P-Adic Numbers, Ultrametric Analysis, and Applications, 1:1,2009, 1-17.

[5] I. V. Volovich, *Number theory as the ultimate physical theory*, P-Adic Numbers, Ultrametric Analysis, and Applications, 1:2,2010, 77-87.

[6] William Fulton, *Curvas Algebraicas*, Editorial Reverté, España, 1971.

[7] J. R. Goldman, *Numbers of solutions of congruences: Poincare series for strongly nondegenerate forms* , Proc. Amer. Math. Soc. 87 No. 4 (1983), 586-590.

[8] J. R. Goldman, *Numbers of solutions of congruences: Poincaré series for algebraic curves*, Adv. in Math. 62 (1986), 68-83.

[9] L. J. Goldstein, *Analytic Number Theory*, Pretince Hall, Englewood Cliffs, 1971.

[10] P. Halmos, *Measure Theory*, Van der Nostrand Reinhold Company, New York, 1950.

[11] J.-I. Igusa, *Complex powers and asymptotic expansions I*, J. Reine Angew. Math. 268/269 (1974), 110-130.

[12] J.-I. Igusa, *Complex powers and asymptotic expansions II*, J. Reine Angew. Math. 278/279 (1975), 307-321.

[13] J.-I. Igusa, *Lectures on Forms of Higher Degree*, Tata Institute of fundamental Research, Bombay, 1978.

[14] J.-I. Igusa, *A stationary phase formula for p-adic integrals and its applications* (Conf. in honor of S. S. Abhyankar), Algebraic geometry and its applications, Springer-Verlag, 1994, pp. 175-194.

[15] J.-I. Igusa, *An Introduction to Theory of Local Zeta Functions*, Studies in Advanced Mathematics vol. 14, American Mathematical Society, Providence, RI, 2000.

[16] Svetlana Katok, *p-adic Analysis Compared with Real* , Student mathematical library vol.37, American Mathematical Society, Providence, RI, 2007.

[17] N. Koblitz, *p-adic Numbers, p-adic Analysis and Zeta-Functions*, Graduate texts in mathematics, 58, Springer-Verlag, New York, second edition, 1984.

[18] Fernando Quadros, *p-adic Numbers: An Introduction*, Universitext, Springer-Verlag, New York, second edition, 1997.

[19] Alain M. Robert, *A course in p-adic Analysis*, Graduate texts in mathematics, 198, Springer-Verlag, New York, 2000.

[20] J-P. Serre, *A course in arithmetic*, Graduate texts in mathematics, 7, Springer-Verlag, New York, 1973.

[21] Tableison M. H., *Fourier analysis on local fields*, Princeton University Press, 1975.

[22] Vladimirov V. S., *Generalized functions over the field of p-adic numbers* , Russian Math. Surveys 43:5, 1988, 19-64.

[23] Vladimirov V. S., Volovich I. V. and Zelenov E. I., *p-adic Analysis and Mathematical Physics*, World Scientific Publishing Co., Singapore, 1994.

[24] W. A. Zuñiga-Galindo, *Igusa's local zeta functions of semiquasihomogeneous polynomials*, Transactions of the American Mathematical society 353:8, 2001, 3193-3207.

[25] W. A. Zuñiga-Galindo, *Local zeta functions and Newton Polyhedra*, Nagoya Math. J., 172, 2003, 31-58.

[26] W. A. Zuñiga-Galindo, *Local zeta functions for nondegenerate homogeneous mappings*, Pacific Journal of Mathematics, 219:1, 2005.

[27] W. A. Zuñiga-Galindo, *An introduction to the theory of local zeta functions*, Notas escuela CIMPA, Colombia, 2012.