FUNCIÓN ZETA LOCAL DE IGUSA Y POLÍGONO DE NEWTON

JULIÁN ANDRÉS GARNICA CRUZ

UNIVERSIDAD INDUSTRIAL DE SANTANDER

FACULTAD DE CIENCIAS

ESCUELA DE MATEMÁTICAS

BUCARAMANGA

2021

FUNCIÓN ZETA LOCAL DE IGUSA Y POLÍGONO DE NEWTON

JULIÁN ANDRÉS GARNICA CRUZ

Trabajo de grado para optar al título de
matemático

Director
Adriana Alexandra Albarracín Mantilla
Profesora escuela de Matemáticas UIS

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE MATEMÁTICAS
BUCARAMANGA
2021

DEDICATORIA

Dedicado a mi familia y a las personas que me acompañaron durante este proceso.

AGRADECIMIENTOS

Agradezco a mi familia por todo el apoyo durante la carrera y a todas las personas que creyeron en mi durante este proceso.

Agradezco a la profesora Adriana por toda la ayuda y asesoría prestada durante este trabajo.

CONTENIDO

LISTA DE FIGURAS

pág.

RESUMEN

TÍTULO: FUNCIÓN ZETA LOCAL DE IGUSA Y POLÍGONO DE NEWTON [*]

AUTOR: JULIÁN ANDRÉS GARNICA CRUZ [**]

PALABRAS CLAVE: CUERPO NO ARQUIMEDIANO, FUNCIONES GENERADORAS, FUNCIÓN ZETA, RESOLUCIÓN DE SINGULARIDADES.

DESCRIPCIÓN:

Las funciones zeta locales son funciones generadoras, importantes en matemática por las relaciones que tienen con teoría de números, sistemas dinámicos, ecuaciones pseudo-diferenciales sobre cuerpos $p-$ádicos, geometría algebraica, big-data, criptografía sobre curvas elípticas, biología, genética y psicología entre otras. Estos objetos están fuertemente conectados con cuerdas y amplitudes de Feynman. En la década del 70, Igusa utiliza el destacado Teorema de resolución de singularidades de Hironaka para mostrar que, la función zeta local es una función racional, siempre y cuando el cuerpo no arquimediano tenga característica cero. En el caso no arquimediano, por ejemplo en el caso $p-$ádico, la función zeta local está relacionada con el número de congruencias polinomiales $\mod p^m$ y sumas exponenciales $\mod p^m$.

---

[*] Trabajo de grado

[**] Facultad de Ciencias. Escuela de Matemáticas. Director: Adriana Alexandra Albarracín Mantilla, Profesora escuela de Matemáticas UIS.

ABSTRACT

TITLE: LOCAL ZETA FUNCTION OF IGUSA AND NEWTON'S POLYGON. [*]

AUTHOR: JULIÁN ANDRÉS GARNICA CRUZ [**]

KEYWORDS: NON-ARCHIMEDEAN FIELDS, GENERATOR FUNCTIONS, ZETA FUNCTION, RESOLUTION OF SINGULARITIES.

DESCRIPTION:

The local zeta functions are generating functions, important in mathematics because of the relationships they have with number theory, dynamical systems, pseudo-differential equations on $p-$addic fields, algebraic geometry, big-data, cryptography on ellipticals, biology, genetics and psychology among others. These objects are strongly connected with strings and Feynman amplitudes. In the 1970s, Igusa used Hironaka's outstanding Singularity Resolution Theorem to show that the local zeta function is a rational function, as long as the fields does not have an Archimedean zero characteristic. In the non-Archimedean case, for example in the $p-$adic case, the local zeta function is related to the number of polynomial congruences $\mod p^m$ and exponential sums $\mod p^m$.

---

[*] Bachelor Thesis

[**] Facultad de Ciencias. Escuela de Matemáticas. Director: Adriana Alexandra Albarracín Mantilla, Profesora escuela de Matemáticas UIS.

INTRODUCCIÓN

Las funciones zeta locales fueron estudiadas inicialmente por Gelfand y Shilov en la década del 50, por su conexión con la existencia de soluciones fundamentales asociadas a operadores diferenciales con coeficientes constantes. Independientemente Atiyah y Berstein prueban que las funciones zeta locales admiten una continuación meromorfa a todo el plano complejo.

En la década del 70, Igusa utiliza el destacado Teorema de resolución de singularidades de Hironaka para mostrar que, la función zeta local es una función racional, siempre y cuando el cuerpo no arquimediano tenga característica cero. Más adelante en 1994, Igusa, descubre un método llamado $Fórmula\ de\ la\ Fase\ Estacionaria$ (FFE) [1], para integrales $p-$ádicas, que dicta que la forma de la función zeta está relacionada con los puntos singulares de la función asociada mód $p\mathbb{Z}$. Este es un procedimiento iterativo que permite, en muchos casos calcular las funciones zeta de una manera explícita. El caso de característica positiva, es aún un problema abierto.

Las funciones zeta locales son funciones generadoras, importantes en matemática por las relaciones que tienen con teoría de números, sistemas dinámicos, ecuaciones pseudo-diferenciales sobre cuerpos $p-$ádicos, geometría algebraica, big-data, criptografía sobre curvas elípticas, biología, genética y psicología entre otras. Estos objetos están fuertemente conectados con cuerdas y amplitudes de Feynman. En el caso no arquimediano, por ejemplo en el caso $p-$ádico, la función zeta local está relacionada con el número de congruencias polinomiales $\mod p^m$ y sumas expo-

---

[1] J. IGUSA. *A Stationary phase formula for p- adic integrals and its applicationes*. Algebraic Geometry e its Applications, Springer-Verlag, 1994, págs. 175-194.

nenciales $\mod p^m$.

Un considerable avance en el estudio de la función zeta local en característica arbitraria se obtiene de una larga lista de polinomios que satisfacen una $Condición\ de\ no\ degeneración$. La idea es asociar un poliedro de Newton a un polinomio f y definir una condición de no degeneración con respecto al poliedro para establecer una continuación meromorfa de la función zeta local.

Este trabajo es autocontenido de tipo monográfico, de forma tal que el lector encuentre lo relacionado con la función zeta local sobre el anillo de enteros $p-$ádicos $\mathbb{Z}_p$ del cuerpo $\mathbb{Q}_p$, [2,3] y su cálculo vía el poliedro de Newton, ilustrando con ejemplos los conceptos y resultados desarrollados.

El texto está organizado en 4 capítulos, de la siguiente manera, el capítulo 1, consta de la teoría básica y fundamental sobre el cuerpo de los números $p-$ádicos, esencial para la comprensión de los temas siguientes. En el capítulo 2, se define el Poliedro de Newton destacando los resultados importantes y relevantes para calcular funciones zeta locales de ciertos polinomios. En el capítulo 3, se desarrolla la teoría relacionada con las funciones zeta local y se describe un conjunto de candidatos a polos, de polinomios que satisfacen una condición de no degeneración en términos del poligono de Newton. Finalmente se implementa SAGE (sistema algebraico computacional) [4] como herramienta para comparar los resultados obtenidos en el

---

[2] A. ALBARRACÍN y LEON E. "Igusa's Local Zeta Functions and Exponential Sums for Arithmetically Non Degenerate Polynomials". En: *Journal de Théorie des Nombres de Bordeaux* (2018).

[3] W. ZÚÑIGA. "Local Zeta function and Newton Polyhedra". En: *Japón, Nagoya Mathematical Journal ISSN: 0027-7630 ed: Cambridge University Press* 172 (2001), págs. 31-58.

[4] J. VIU SOS. "Funciones zeta y poliedros de Newton: Aspectos teóricos y computacionales". Tra-

capítulo inmediatamente anterior.

Este trabajo es fundamental para la continuación de estudios de posgrado en el área de análisis $p-$ádico.

bajo Fin de Master, Director: Enrique Artal Bartolo. Universidad Zaragoza, 2012.

1. NÚMEROS P-ÁDICOS

1.1. NORMAS ARQUIMEDIANAS Y NO ARQUIMEDIANAS

Esta sección ilustrará los resultados que fundamentan la teoría de los números p-ádicos, [5, 4, 6].

Definición 1 *Sea X un conjunto no vacío. Una distancia o métrica sobre X es una función* $d : X \times X \to \mathbb{R}^+ \cup \{0\}$*, tal que para todo* $x, y, z \in X$ *se cumplen:*

- $d(x, y) = 0 \Leftrightarrow x = y$*,*
- $d(x, y) = d(y, x)$*,*
- $d(x, y) \leq d(x, z) + d(z, y)$ *(Desigualdad triangular).*

Un conjunto dotado de una métrica se denomina espacio métrico.
Una sucesión de puntos $\{x_n\}_{n\in\mathbb{N}}$, es llamada de **Cauchy** si

$$d(x_n, x_m) \to 0, \text{ con } m, n \to \infty.$$

Definición 2 *Sea X un espacio métrico con respecto a la metrica d. Se dice que X es completo si toda sucesión de Cauchy en X, converge a un valor de X.*

Definición 3 *Se dice que dos métricas* d_1, d_2*, sobre un conjunto X, son equivalentes si toda sucesión de Cauchy con respecto a la métrica* d_1 *es una sucesión de Cauchy con respecto a la métrica* d_2 *y viceversa.*

---

[5] V. VLADIMIROV, VOLOVICH I. y ZELENOV E. *p-adic Analysis and Mathematical Physics*. World Scientific Publishing Co., 1994.

[6] E. LEON y ZÚÑIGA W. “An Introduction to the Theory of Local Zeta Functions from Scratch”. En: *Revista Integración, temas de matemáticas. Escuela de Matemáticas, Universidad Industrial de Santander* ().

A continuación se definirá el valor absoluto sobre un cuerpo.

Definición 4 *Sea F un cuerpo. Un valor absoluto (Arquimediano) sobre F es una función de valores reales, $|\cdot| : F \to \mathbb{R}^+ \cup \{0\}$, que satisface para todo $x, y \in F$:*

i) $|x| = 0 \Leftrightarrow x = 0$,

ii) $|xy| = |x|\,|y|$,

iii) $|x + y| \leq |x| + |y|$ *(Desigualdad triangular).*

En el caso **no Arquimediano**:

Definición 5 *Un valor absoluto $|\cdot|$ es llamado no Arquimediano, si además satisface:*

$$|x + y| \leq \max\{|x|, |y|\}\ \forall x, y \in F \text{ (propiedad ultramétrica).}$$

Ejemplo 1 *El valor absoluto trivial es no Arquimediano*

$$|x|_{trivial} = \begin{cases} 1, \ si\ x \neq 0, \\ 0, \ si\ x = 0. \end{cases}$$

Definición 6 *Dados dos valores absolutos $|\cdot|_1$, $|\cdot|_2$ definidos sobre un cuerpo F, se dice que son equivalentes lo cual denotamos por $|\cdot|_1 \sim |\cdot|_2$, si inducen métricas equivalentes.*

Teorema 1 *Sean $|\cdot|_1, |\cdot|_2$ valores absolutos sobre F, si $|\cdot|_1 \sim |\cdot|_2$, se tiene:*

i) Si $|\cdot|_1$ es trivial, entonces $|\cdot|_2$ es trivial.

ii) $|x|_1 < 1$ *si y solo si* $|x|_2 < 1$*;* $|x|_1 > 1$ *si y solo si* $|x|_2 > 1$*;* $|x|_1 = 1$ *si y solo si* $|x|_2 = 1$.

$Demostración.$ $i)$ Suponga que $|\cdot|_1$ es trivial y $|\cdot|_2$ no es trivial, entonces existe $x \in F$, $x \neq 0$, tal que $|x|_2 \neq 1$, luego se tiene que $|x|_2 < 1$ ó $|x|_2 > 1$. Si $|x|_2 < 1$, se tiene que, $|x^n|_2 = |x|_2^n \to 0$, cuando $n \to \infty$, observe que la sucesión $\{x^n\}_{n\in\mathbb{N}}$ es de Cauchy con respecto a $|\cdot|_2$. Sea $\epsilon > 0$, como $|x|_2 < 1$, existe $n_0 \in \mathbb{N}$ tal que $|x|_2^{n_0} < \frac{\epsilon}{2}$. Sean $n_o \leq m < n$, se tiene:

$$|x^n - x^m|_2 \leq |x^n|_2 + |x^m|_2 < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon.$$

Por lo tanto $\{x^n\}_{n\in\mathbb{N}}$ es de Cauchy con respecto a $|\cdot|_2$. Ahora se mostrará que $\{x^n\}_{n\in\mathbb{N}}$ no es de Cauchy con respecto a $|\cdot|_1$. Puesto que $|x|_2 < 1$, $(x-1) \neq 0$ y como $|\cdot|_1$ es trivial, se tiene que, $|x-1|_1 = 1$;

$$\left|x^{n+1} - x^n\right|_1 = |x^n(x-1)|_1 = |x^n|_1 \, |x-1|_1 = 1.$$

Por lo tanto $\{x^n\}_{n\in\mathbb{N}}$ no es de Cauchy con respecto a $|\cdot|_1$, lo cual contradice que $|\cdot|_1 \sim |\cdot|_2$, por lo tanto $|\cdot|_2$ es trivial, (para el otro caso $|x|_2 > 1$, se toma x^{-1}).

$ii)$ Se sigue un argumento similar al item anterior. □

Teorema 2 *Dados dos valores absolutos* $|\cdot|_1$, $|\cdot|_2$ *definidos sobre un cuerpo* F, $|\cdot|_1 \sim |\cdot|_2$ *si y solo si existe* $c > 0$ *tal que:*

$$|x|_1 = |x|_2^c, \tag{1}$$

para todo $x \in F$.

$Demostración.$ Sea $|\cdot|_1 \sim |\cdot|_2$. Si $|\cdot|_1$ es trivial, por el Teorema 1, se tiene que $|\cdot|_2$ es trivial, y la igualdad (1) se tiene para cualquier $c > 0$.
Suponga que $|\cdot|_1$ no es trivial, entonces existe $a \in F$, $a \neq 0$, tal que $|a|_1 \neq 1$, y por lo

tanto se tiene que $|a|_1 < 1$ ó $|a|_1 > 1$, sin pérdida de la generalidad se puede suponer que $|a|_1 < 1$ ya que si $|a|_1 > 1$ entonces $|a^{-1}|_1 < 1$. Se define;

$$c = \frac{log\,|a|_2}{log\,|a|_1}.$$

Por el Teorema 1, $|a|_1 < 1$ implica que $|a|_2 < 1$, por lo tanto $c > 0$. Se mostrará que c satisface (1). Sea $x \in F$ tal que $|x|_1 < 1$ y se definen los siguientes conjuntos:

$$S_1 = \left\{ r = \frac{m}{n} : m, n \in \mathbb{N}, |x|_1^r < |a|_1 \right\},$$

$$S_2 = \left\{ r = \frac{m}{n} : m, n \in \mathbb{N}, |x|_2^r < |a|_2 \right\}.$$

Para todo $r \in S_1$ se cumple que,

$$|x|_1^m = (|x|_1^r)^n < |a|_1^n < 1,$$

es decir $\frac{|x^m|_1}{|a^n|_1} < 1$, por el Teorema 1, se tiene $\frac{|x^m|_2}{|a^n|_2} < 1$, así,

$$|x|_2^r = (|x|_2^m)^{\frac{1}{n}} < (|a|_2^n)^{\frac{1}{n}} = |a|_2\,,$$

lo cual implica $r \in S_2$, por lo tanto $S_1 \subset S_2$ y se concluye que $S_1 = S_2$. Con un razonamiento similar se obtiene $S_2 \subset S_1$. Dado que S_1 consta de todos los números racionales r tales que:

$$r > \frac{log\,|a|_1}{log\,|x|_1},$$

Analógamente S_2 consta de todos los números racionales r tales que:

$$r > \frac{log\,|a|_2}{log\,|x|_2}.$$

Dado que $S_1 = S_2$, se tiene que,

$$\frac{log\,|a|_1}{log\,|x|_1} = \frac{log\,|a|_2}{log\,|x|_2},$$

por lo tanto:

$$\frac{log\,|x|_2}{log\,|x|_1} = \frac{log\,|a|_2}{log\,|a|_1} = c,$$

lo cual implica que c no depende de x cuando $|x|_1 < 1$, de manera análoga se hace para el caso $|x|_1 > 1$ y $|x|_1 = 1$ usando el Teorema 1. El recíproco es inmediato haciendo uso del Teorema 1. □

Ahora se describirán todas las normas sobre $\mathbb{Q}$ equivalentes al valor abosoluto usual, $|\cdot|$.

Proposición 1 *La norma $|x|_1 = |x|^c$, $0 < c \in \mathbb{R}$, es una norma sobre $\mathbb{Q}$ si y solo si $c \leq 1$. En este caso es equivalente a $|x|$.*

$Demostración$. Supongamos primero que $c > 1$ y $|x|_1 = |x|^c$ es una norma sobre $\mathbb{Q}$, por otro lado se tiene:

$$|1+1|_1 = |1+1|^c = |2|^c > |1|^c + |1|^c = 2.$$

Lo cual contradice la propiedad $iii)$, de la definición 4. Por lo tanto $c \leq 1$.
Recíprocamente sean $x, y \in \mathbb{Q}$

i) $|x|_1 = 0 \Leftrightarrow |x|^c = 0 \Leftrightarrow x = 0$.

ii) $|xy|_1 = |xy|^c = |x|^c\,|y|^c = |x|_1\,|y|_1$.

iii) Sin pérdida de generalidad suponga que $|y| \leq |x|$, entonces;

$$|x+y|^c \leq (|x| + |y|)^c = |x|^c \left(1 + \frac{|y|}{|x|}\right)^c \leq |x|^c \left(1 + \frac{|y|}{|x|}\right).$$

Dado que $c \leq 1$ y $\left(1+\frac{|y|}{|x|}\right) \geq 1$, también se obtiene que $\left(1+\frac{|y|}{|x|}\right) \leq \left(1+\frac{|y|^c}{|x|^c}\right)$, puesto que $\frac{|y|}{|x|} \leq 1$. Por lo tanto;

$$|x+y|_1 = |x+y|^c \leq |x|^c \left(1+\frac{|y|^c}{|x|^c}\right) = |x|^c + |y|^c = |x|_1 + |y|_1 .$$

□

Teorema 3 *Las siguientes afirmaciones son equivalentes:*

i) $|\cdot|$ *es no-Arquimediana.*

ii) $|n| \leq 1$ *para todo* $n \in \mathbb{Z}$.

$Demostración.$ $i) \Rightarrow ii)$ Haciendo inducción sobre $|n|$ con $n \in \mathbb{N}$, se tiene que $|1| = 1 \leq 1$, suponga que $|n| \leq 1$, entonces:

$$|n+1| \leq \text{máx}\{|n|, |1|\} = 1.$$

Por lo tanto $|n| \leq 1$ para todo $n \in \mathbb{N}$. Dado que $|-n| = |n|$ y $|0| = 0$, se concluye que $|n| \leq 1$ para todo $n \in \mathbb{Z}$.

$ii) \Rightarrow i)$ Suponga que $|n| \leq 1$ para todo $n \in \mathbb{Z}$. Dado que los coeficientes binomiales $\binom{n}{k} \in \mathbb{Z}$, $k \leq n$, entonces $\left|\binom{n}{k}\right| \leq 1$. En consecuencia,

$$\begin{aligned} |x+y|^n = |(x+y)^n| = \left|\sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k\right| &\leq \sum_{k=0}^{n} \left|\binom{n}{k}\right| \left|x^{n-k}\right| \left|y^k\right|, \\ &\leq \sum_{k=0}^{n} |x|^{n-k} |y|^k \leq (n+1)[\text{máx}\{|x|, |y|\}]^n, \end{aligned}$$

Así para todo $n \in \mathbb{N}$ se tiene:

$$|x+y| \leq \sqrt[n]{n+1}\, \text{máx}\{|x|, |y|\},$$

si $n \to \infty$, se tiene:

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

por lo tanto $|\cdot|$ es no-Arquimediana. □

Del Teorema 3, se observa la diferencia entre una norma Arquimediana y una no-Arquimediana.

Definición 7 *Un valor absoluto (norma) es Arquimediano si, dados* $x, y \in F, x \neq 0$*, existe un entero positivo* n *tal que* $|nx| \geq |y|$*.*

Esta condición conocida como la propiedad Arquimediana, es equivalente a

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

y se cumple para $\mathbb{Q}$ y $\mathbb{R}$.

Las siguientes propiedades son consecuencia de que la norma sea no Arquimediana.

Proposición 2 *Sea F un cuerpo y sea* $|\cdot|$ *un valor absoluto no arquimediano sobre F. Si* $x, y \in F$ *y* $|x| \neq |y|$ *entonces*

$$|x+y| = \text{máx}\{|x|, |y|\}.$$

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

$$|x+y| \leq |x| = \text{máx}\{|x|, |y|\}. \tag{2}$$

Por otro lado,

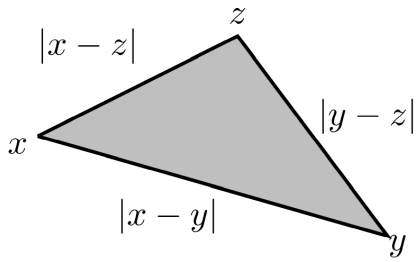
$$|x| = |(x+y) - y| \leq \text{máx}\{|x+y|, |y|\},$$

dado que $|x| > |y|$, entonces

$$\text{máx}\{|x+y|, |y|\} = |x+y| \Rightarrow |x| \leq |x+y|. \tag{3}$$

De (2) y (3) se obtiene $|x+y| = |x|$. □

Corolario 1 *En un cuerpo F con valor absoluto $|\cdot|$ no arquimediano todos los triángulos son isósceles.*



$Demostración.$ Sean $x, y, z \in F$ (vértices del triángulo). Las medidas de cada lado son:

$$|x-y|, |y-z|, |z-x| \text{ respectivamente},$$

dado que $(x-y)+(y-z) = x-z$.
Si $|x-y| = |y-z|$ el triángulo ya es isósceles.
Si $|x-y| \neq |y-z|$ entonces por la proposición anterior se obtiene

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

Así, todos los triángulos son isósceles. □

1.1.1. Construcción de la completación de un cuerpo normado En esta sección, a partir de un cuerpo normado arbitrario $(F, |\cdot|)$ (no necesariamente completo con la norma $|\cdot|$, se construirá otro cuerpo, $\hat{F}$, tal que $F \subset \hat{F}$, y con una norma, la inducida por $|\cdot|$ de F, tal que $\hat{F}$ sea un cuerpo normado completo.

Para el proceso de completación de F, las sucesiones de Cauchy tienen un papel importante.

Sea $\{F\}$ la colección de todas las sucesiones de Cauchy en $(F, |\cdot|)$, si $\{a_n\}, \{b_n\} \in \{F\}$ entonces se tiene que $\{a_n \pm b_n\}, \{a_n b_n\} \in \{F\}$, es decir, $\{F\}$ es cerrado para la adición y multiplicación usual de sucesiones. En consecuencia, $\{F\}$ constituye un anillo conmutativo. La identidad bajo la adición está dada por la siguiente sucesión

$$\hat{0} = \{0, 0, 0, \cdots\},$$

y la identidad bajo la multiplicación es la sucesión

$$\hat{1} = \{1, 1, 1. \cdots\}.$$

Es claro que $\{F\}$ no es un cuerpo, dado que tiene divisores de cero:

$$\{1, 0, 0, \cdots\}\{0, 1, 0, \cdots\} = \hat{0}.$$

Para todo $a \in F$, considere la sucesión constante $\hat{a} = \{a, a, a, \cdots\} \in \{F\}$, entonces el conjunto de todas estas sucesiones constantes es un subanillo de $\{F\}$, dado que la adición y multiplicación de sucesiones constantes es constante. Además, si $b \neq 0$, entonces la sucesión constante $\hat{b}^{-1} = \{b^{-1}, b^{-1}, b^{-1}, \cdots\}$, es la inversa de $\hat{b}$. Por lo tanto $\{F\}$ contiene un subanillo isomorfo a F.

Sea P el conjunto de todas las sucesiones nulas de $\{F\}$, es decir, la sucesión de

Cauchy $\{a_n\}$ de F tales que, $\lim_{n\to\infty} |a_n| = 0$. P es cerrado bajo la adición, es decir, si $\{a_n\}, \{b_n\} \in P$ entonces $\{a_n \pm b_n\} \in P$. Si $\{b_n\} \in \{F\}$, se cumple que $\{b_n\}$ es acotada, por ser de Cauchy, por lo tanto, si $\{a_n\} \in P$, se tiene que $\{a_n b_n\} \in P$. Por lo tanto P es un ideal de $\{F\}$, es decir, un subanillo de $\{F\}$, tal que para todo $p \in P$ y $a \in \{F\}$, se tiene que $ap \in P$.

Sea $\hat{F} = \{F\}/P$. Los elementos de $\hat{F}$ son clases de equivalencia de sucesiones de Cauchy en $(F, |\cdot|)$, dos sucesiones de Cauchy son equivalentes si su diferencia es una sucesión nula, es decir, su diferencia está en P. Sean dos elementos distintos $a, b \in F$, las respectivas sucesiones constantes $\hat{a}, \hat{b}$, se tiene que, $\lim_{n\to\infty} |a_n - b_n| = |a - b| > 0$, por lo tanto $\hat{a}$ y $\hat{b}$ están en clases diferentes de $\hat{F}$. Se denota $A = (\{a_n\})$ la clase de equivalencia de las sucesiones de Cauchy $\{a_n\}$, tal que $A \in \hat{F}$, y se identifica un elemento $a \in F$ como la clase $(\hat{a}) \in \hat{F}$, de esta manera se considera a F como un subconjunto de $\hat{F}$.

Teorema 4 *$\hat{F}$ es un cuerpo.*

$Demostración$. Se define en $\hat{F}$ la adición y multiplicación de la siguiente manera: sean $A, B \in \hat{F}$, si $\{a_n\} \in A$ y $\{b_n\} \in B$, entonces, $A + B := (\{a_n + b_n\})$ y $AB := (\{a_n b_n\})$. y dado que no dependen del representante de la clase, se obtiene que $\hat{F}$ es un anillo conmutativo con elementos identidad $(\hat{0})$ y $(\hat{1})$ para la adición y multiplicación respectivamente. $\hat{F}$ es un cuerpo, en efecto, si A es una clase de equivalencia en $\hat{F}$ diferente de la clase cero $(\hat{0}) = P$ y sea $\{a_n\} \in A$, entonces $\{a_n\}$ es una sucesión no nula, lo cual implica que existe $C > 0$ y un N natural tales que:

$$|a_n| > C, \forall n \geq N.$$

Considere la sucesión

$$a_n^* = \begin{cases} 0 \quad si, \quad n \leq N-1, \\ \\ \frac{1}{a_n} \quad si, \qquad N \leq n. \end{cases}$$

La sucesión $\{a_n^*\}$ es de Cauchy, dado que si $n, m \geq N$, se tiene:

$$0 \leq |a_m^* - a_n^*| = \left| \frac{1}{a_m} - \frac{1}{a_n} \right| = \frac{|a_m - a_n|}{|a_m|\,|a_n|} \leq c^{-2}\,|a_m - a_n|\,,$$

puesto que $\{a_n\}$ es de Cauchy, entonces $\{a_n^*\} \in \{F\}$. Sea $A^{-1} = (\{a_n^*\})$ y por lo anterior se tiene que $\{a_n\}\{a_n^*\} \in \{F\}$, tal que

$$\{a_n\}\{a_n^*\} = \{0, \cdots, 0, 1, 1, \cdots\},$$

donde los primeros $N-1$ términos son 0 y el resto tienen valor 1. Note que:

$$\{b_n\} = \{a_n\}\{a_n^*\} - \hat{1} = \{-1, \cdots, -1, 0, 0, \cdots\},$$

por lo tanto $\{b_n\} \in P$, lo cual implica que $\{a_n\}\{a_n^*\}$ y $\hat{1}$ son sucesiones de Cauchy equivalentes y en consecuencia $AA^{-1} = (\hat{1})$, lo que muestra que $\hat{F}$ es un cuerpo. □

Se extenderá la norma $|\cdot|$ de F al cuerpo $\hat{F}$:

Definición 8 *Sea A* $\in \hat{F}$*, se define,*

$$|A|_e = \lim_{n\to\infty} |a_n|\,,$$

donde $\{a_n\} \in A$.

Esta función está bien definida. Dado que $||a_m| - |a_n|| \leq |a_m - a_n|$ y $\{a_n\} \in \{F\}$, entonces la sucesión de números reales $\{|a_n|\}$ es de Cauchy, puesto que $\mathbb{R}$ es

completo, el $\lim_{n\to\infty}|a_n|$ existe. Ahora sea $\{b_n\}\in A$, entonces:

$$0\leq \lim_{n\to\infty}||a_n|-|b_n||\leq \lim_{n\to\infty}|a_n-b_n|=0;$$

Dado que $\{a_n\}$ y $\{b_n\}$ son sucesiones de Cauchy equivalentes. Por lo tanto, $\lim_{n\to\infty}|a_n|=\lim_{n\to\infty}|b_n|$, es decir, $|A|_e$ no depende del representante de la clase. Por otra parte, cada $a\in F$ está en $\hat{F}$ si se considera como la sucesión $\hat{a}=\{a,a,a,\cdots\}$, por lo tanto; $|(\hat{a})|_e=\lim_{n\to\infty}|a|=|a|$, en este caso se habla de extensión, pues la norma de la clase $\hat{a}$ coincide con la norma del elemento $a\in F$.

Proposición 3 $|\cdot|_e$ *es una norma sobre* $\hat{F}$*, además si la norma* $|\cdot|$ *sobre* F *es No-Arquimediana, su extensión también será No-Arquimediana.*

$Demostración$. Se mostrará que se cumplen las primeras tres popiedades de la definición 4.

$i)$ Si $A=(\hat{0})$, entonces $\{a_n\}\in A$, es una sucesión nula, lo que implica $|A|_e=0$. Si $A\neq(\hat{0})$ y $A=(\{a_n\})$, entonces existe $c>0$ y $N\in\mathbb{N}$, tal que para todo $n\geq N$, se tiene $|a_n|\geq c>0$. Por lo tanto $|A|_e>0$.

$ii)$ Sean $A=(\{a_n\})$ y $B=(\{b_n\})$, por propiedades de límites reales,

$$|AB|_e=\lim_{n\to\infty}|a_nb_n|=\lim_{n\to\infty}|a_n|\,|b_n|=\lim_{n\to\infty}|a_n|\lim_{n\to\infty}|b_n|=|A|_e\,|B|_e\,.$$

$iii)$ Sean $A=(\{a_n\})$ y $B=(\{b_n\})$, se tiene,

$$|A+B|_e=\lim_{n\to\infty}|a_n+b_n|\leq\lim_{n\to\infty}|a_n|+|b_n|=\lim_{n\to\infty}|a_n|+\lim_{n\to\infty}|b_n|=|A|_e+|B|_e\,.$$

Si $|\cdot|$ es No-Arquimediana sobre F y sean $A = (\{a_n\}), B = (\{b_n\}) \in \hat{F}$, entonces:

$$|A+B|_e = \lim_{n\to\infty} |a_n + b_n| \leq \lim_{n\to\infty} \text{máx}\{|a_n|, |b_n|\} = \text{máx}\{|A|_e, |B|_e\}.$$

□

Teorema 5 *El cuerpo $\hat{F}$ es completo con respecto a la norma $|\cdot|_e$, y F es un subconjunto denso en $\hat{F}$.*

$Demostración$. Inicialmente probamos la segunda parte. Sea $A = (\{a_m\}) \in \hat{F}$. Para cada n en los naturales se tiene $a_n \in F$ y sea la sucesión constante $(\hat{a_n})$. Entonces $\{a_m - a_n\}_{m=1}^{\infty}$ es la sucesión que representa la clase $A - (\hat{a_n})$, ya que $\{a_m\}$ es una sucesión de Cauchy, se tiene:

$$\lim_{n\to\infty} |A - (\hat{a_n})|_e = \lim_{n,m\to\infty} |a_m - a_n| = 0.$$

Esto muestra que F es denso en $\hat{F}$.
Ahora se mostrará que $\hat{F}$ es completo. Sea $\{A_n\} = \{A_1, A_2, \cdots\}$ una sucesión de Cauchy en $\hat{F}$. Por la densidad de F en $\hat{F}$, para cada A_n existe un $a_n \in F$ tal que:

$$|A_n - (\hat{a_n})|_e \leq \frac{1}{n}.$$

Por lo tanto $\{A - (\hat{a_n})\}$ es una sucesión de Cauchy nula. Así se tiene que:

$$\{(\hat{a_n})\} = \{A_n\} - \{A_n - (\hat{a_n})\}.$$

Es decir, $\{(\hat{a_n})\}$ es una sucesión de Cauchy en $\hat{F}$. Dado que todo elemento de $\{(\hat{a_n}\})$ está en F, la sucesión $\{a_n\}$ también es de Cauchy en F. Sea $A = (a_n)$, se tiene por otra parte que $\{A - (\hat{a_n})\}$ y $\{A_n - (\hat{a_n})\}$ son nulas en $\hat{F}$, por lo tanto:

$$\{A - A_n\} = \{A - (\hat{a_n})\} - \{A_n - (\hat{a_n})\},$$

es una sucesión nula en $\hat{F}$. Esto implica que:

$$\lim_{n\to\infty} |A - A_n|_e = 0,$$

es decir, $A = \lim_{n\to\infty} A_n$, por lo tanto $\hat{F}$ es completo. □

1.1.2. El cuerpo de los números p-ádicos $\mathbb{Q}_p$ El ejemplo básico de una norma sobre $\mathbb{Q}$, es el valor absoluto usual. Esta norma induce la métrica Arquimediana $d(x, y) = |x - y|$. ¿Será que existen otras normas sobre $\mathbb{Q}$?. La respuesta es sí.

Definición 9 *Sea $p \in \mathbb{Z}$ primo. Se define el orden p-ádico, $ord_p(x)$, de un $x \in \mathbb{Q}$ de la siguiente manera:*

i) Si $x \in \mathbb{Z}$ entonces $ord_p(x)$ es igual a la mayor potencia de p que divide a x.

ii) Si $x = \frac{a}{b}$, con $a, b \in \mathbb{Z}$ y $b \neq 0$, entonces $ord_p(x) = ord_p(a) - ord_p(b)$.

iii) $ord_p(0) = +\infty$.

El orden p-ádico también se denomina valuación p-ádica y se denota por $v_p(x)$.

Lema 1 *Para todo $x, y \in \mathbb{Q}$ se cumple:*

i) $ord_p(xy) = ord_p(x) + ord_p(y)$,

ii) $ord_p(x + y) \geq \min\{ord_p(x), ord_p(y)\}$.

Demostración. *i)* Sean $x, y \in \mathbb{Z}$ y $ord_p(x) = n, ord_p(y) = m$, es decir $x = x'p^n$, e $y = y'p^m$, para algunos $x', y' \in \mathbb{Z}$, donde $(x', p^n) = 1 = (y', p^m)$. Por lo tanto $xy = x'y'p^{n+m}$, con $(x'y', p^{n+m}) = 1$, se tiene que $ord_p(xy) = n+m = ord_p(x)+ord_p(y)$. Ahora sean $x, y \in \mathbb{Q}$, existen $a, b, c, d \in \mathbb{Z}$ con $b \neq 0 \neq d$, tal que $x = \frac{a}{b}$ y $y = \frac{c}{d}$, entonces

$$ord_p(xy) = ord_p\left(\frac{ac}{bd}\right) = ord_p(ac) - ord_p(bd) = ord_p(a) + ord_p(c) - (ord_p(b) + ord_p(d))$$
$$= (ord_p(a) - ord_p(b)) + (ord_p(c) - ord_p(d)) = ord_p(x) + ord_p(y),$$

$ii)$ Sean $x, y \in \mathbb{Q}$, existen $a, b, c, d \in \mathbb{Z}$ con $b, d \neq 0$, tal que $x = \frac{a}{b}$ y $y = \frac{c}{d}$, entonces $x + y = \frac{ad + bc}{bd}$, por lo tanto:

$$ord_p(x + y) = ord_p(ad + bc) - ord_p(bd),$$

sea $n = \min\{ord_p(ad), ord_p(bc)\}$, entonces p^n divide a ad y bc, por lo tanto divide a $ad + bc$, lo cual implica, $n \leq ord_p(ad + bc)$, entonces:

$$\begin{aligned} ord_p(x + y) &\geq \min\{ord_p(ad), ord_p(bc)\} - ord_p(bd) \\ &= \min\{ord_p(ad) - ord_p(bd), ord_p(bc) - ord_p(bd)\} \\ &= \min\{ord_p(a) - ord_p(b), ord_p(c) - ord_p(d)\} \\ &= \min\{ord_p(x), ord_p(y)\} \end{aligned}$$

□

El lema anterior garantiza que $ord_p(x)$ está bien definido, es decir, no depende de la representación de x. Sea $x = \frac{a}{b} \in \mathbb{Q}$, se tiene lo siguiente, $x = \frac{ac}{bc}$, por lo tanto:

$$ord_p(x) = ord_p(ac) - ord_p(bc) = ord_p(a) + ord_p(c) - ord_p(b) - ord_p(c) = ord_p(a) - ord_p(b).$$

Se define la función $|\cdot|_p : \mathbb{Q} \to \mathbb{R}^+$, de la siguiente manera:

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

Ejemplo 2 *Sea $p = 5$, se calculará $|5|_5, \left|\frac{25}{3}\right|_5, \left|-\frac{7}{125}\right|_5$,*

$$|5|_5 = 5^{-1}; \left|\frac{25}{3}\right|_5 = 5^{-2}; \left|-\frac{7}{125}\right|_5 = 5^3.$$

Note que $|\cdot|_p$, solo toma valores en el conjunto discreto $\{p^n, n \in \mathbb{Z}\} \cup \{0\}$. Si $a, b \in \mathbb{Z}$, entonces $a \equiv b \mod p^n$ sí y solo sí $|a - b|_p \leq p^{-n}$.

Proposición 4 *$|\cdot|_p$ es una norma No-Arquimediana sobre $\mathbb{Q}$.*

$Demostración$. Se mostrará que cumple los axiomas de la Definición 4 y la Definición 5. El axioma $i)$ es claro por la definición de $|x|_p$. Por otra parte se tiene:

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

Por lo tanto cumple el axioma (ii). El axioma (iii) y la Definición 5, es trivial si alguno de estos casos pasa, $x = 0$, $y = 0$ o $x + y = 0$. Sean x, y y $x + y$ distintos de cero, con $x, y \in \mathbb{Q}$, es decir existen $a, b, c, d \in \mathbb{Z}$ con $b \neq 0, d \neq 0$, tal que $x = \frac{a}{b}$ y $y = \frac{c}{d}$, entonces $x + y = \frac{ad + bc}{bd}$ y por el Lema 1, se tiene:

$$|x + y|_p = p^{-ord_p(x+y)} \leq \max\{p^{-ord_p(x)}, p^{-ord_p(y)}\} = \max\{|x|_p, |y|_p\} \leq |x|_p + |y|_p .$$

Por tanto $|\cdot|_p$ (también llamada **norma p-ádica**) es No-Arquimediana sobre $\mathbb{Q}$. □

Note que si en lugar de seleccionar un p primo, se escoge un número compuesto

$m > 1$, entonces el axioma (ii) de la Definición 4 no se cumple. Por ejemplo, sea $m = 9$, entonces: $9^{-1} = |9|_9 \neq |3|_9 |3|_9 = 1$.
Dado que $|p^n|_p = p^{-n}$, entonces $|p^n|_p \to 0$, cuando $n \to \infty$.
Si p, q son primos diferentes entonces las normas $|\cdot|_p$ y $|\cdot|_q$ no son equivalentes. En efecto, sea la sucesión $x_n = \left(\frac{p}{q}\right)^n$, $|x_n|_p \to 0$ y $|x_n|_q \to \infty$, cuando $n \to \infty$.

El siguiente teorema garantiza que no existen otras normas sobre $\mathbb{Q}$ excepto $|\cdot|_p$ y $|\cdot|_\infty$ (valor absoluto usual).

Teorema 6 (Ostrowski) *Todo valor absoluto $\|\cdot\|$ no trivial sobre $\mathbb{Q}$ es equivalente a $|\cdot|_p$ o al valor absoluto usual $|\cdot|_\infty$.*

$Demostración.$ Suponga que $\|\cdot\|$ es Arquimediana, es decir, existe $n \in \mathbb{N}$ tal que $\|n\| > 1$. Sea n_0 el más pequeño n, existe un número real $\alpha > 0$, tal que $\|n_0\| = n_0^\alpha$.
Todo número entero positivo n se puede escribir en base n_0 de la forma:

$$n = a_0 + a_1 n_0 + \cdots + a_s n_0^s,$$

donde $0 \leq a_i \leq n_0 - 1, i = 0, 1, \cdots, s, a_s \neq 0$, tal que

$$\|n\| \leq \|a_0\| + \|a_1 n_0\| + \cdots + \|a_s n_0^s\| = \|a_0\| + \|a_1\| n_0^\alpha + \cdots + \|a_s\| n_0^{s\alpha},$$

dado que $a_i \leq n_0 - 1 < n_0$ y n_0 es el más pequeño que cumple $\|n_0\| > 1$, entonces $\|a_i\| \leq 1$, así

$$\begin{aligned} \|n\| &\leq 1 + n_0^\alpha + \cdots + n_0^{s\alpha} = n_0^{s\alpha}(1 + n_0^{-\alpha} + \cdots + n_0^{-s\alpha}), \\ &\leq n_0^{s\alpha} \sum_{i=0}^{\infty} n_0^{-i\alpha} = n_0^{s\alpha} \frac{n_0^\alpha}{n_0^\alpha - 1}, \end{aligned}$$

puesto que $n \geq n_0^s$. Sea $C = \frac{n_0^\alpha}{n_0^\alpha - 1}$, una constante que no depende de n, entonces

$$\|n\| \leq C n_0^{s\alpha} \leq C n^\alpha.$$

Reemplazando n por un entero de la forma n^N se tiene

$$\left\|n^N\right\| \leq C n^{N\alpha} \Leftrightarrow \|n\| \leq n^\alpha \sqrt[N]{C},$$

cuando $N \to \infty$, se obtiene:

$$\|n\| \leq n^\alpha.$$

Ahora se mostrará la otra desigualdad. Puesto que $n = a_0 + a_1 n_0 + \cdots + a_s n_0^s$, $0 \leq a_i \leq n_0 - 1, i = 0, 1, \cdots, s, a_s \neq 0$, entonces $n_0^s \leq n < n_0^{s+1}$, esto se tiene dado que el valor más grande de a_i es $n_0 - 1$,

$$n \leq (n_0 - 1)(1 + n_0 + \cdots + n_0^s) = n_0^{s+1} - 1,$$

por lo tanto:

$$n_0^{(s+1)\alpha} = \left\|n_0^{s+1}\right\| = \left\|n + n_0^{s+1} - n\right\| \leq \|n\| + \left\|n^{s+1} - n\right\|,$$

por la desigualdad, $\|n\| \leq n^\alpha$, se obtiene, $\left\|n_0^{s+1} - n\right\| \leq (n_0^{s+1} - n)^\alpha$, lo cual implica:

$$\|n\| \geq n_0^{(s+1)\alpha} - (n_0^{s+1} - n)^\alpha = n_0^{(s+1)\alpha} \left(1 - \left(1 - \frac{1}{n_0}\right)^\alpha\right),$$

sea $C' = (1 - (1 - \frac{1}{n_0})^\alpha)$, una constante que no depende de n, entonces:

$$\|n\| \geq C' n_0^{(s+1)\alpha} \geq C' n^\alpha.$$

Reemplazando n por un entero de la forma n^N,

$$\left\|n^N\right\| \geq C' n^{N\alpha} \Leftrightarrow \|n\| \geq n^{\alpha} \sqrt[N]{C'},$$

cuando $N \to \infty$, se obtiene:

$$\|n\| \geq n^{\alpha}.$$

Por lo tanto $\|n\| = n^{\alpha}$ para todo $n \in \mathbb{N}$, teniendo en cuenta la propiedad $ii)$ de la norma, se tiene que $\|x\| = |x|_{\infty}^{\alpha}$, para todo $x \in \mathbb{Q}$.

Supóngase $\|\cdot\|$ No-Arquimediana, es decir $\|n\| \leq 1$ para todo $n \in \mathbb{N}$, dado que $\|\cdot\|$ es no trivial, existe $n_0 \in \mathbb{N}$ tal que $\|n_0\| < 1$. Sea n_0 el mínimo que cumple con esta propiedad, es claro que n_0 debe ser primo, de lo contrario, se tiene $n_0 = n_1 n_2$, con $n_1, n_2 < n_0$, entonces $\|n_1\| = \|n_2\| = 1$, lo cual implica $\|n_0\| = \|n_1\| \|n_2\| = 1$, lo cual es absurdo; Así, n_0 es un número primo y se denotará por p.
Ahora se mostrará que si $n \in \mathbb{Z}$ no es divisible por p, entonces $\|n\| = 1$. Por el algoritmo de la división existen $r, s \in \mathbb{Z}$, tal que, $n = rp + s$, con $0 < s < p$, por la minimalidad de p, se cumple $\|s\| = 1$, $\|r\| \leq 1$ y $\|p\| < 1$, entonces $\|rp\| < 1$, por lo tanto:

$$\|n - s\| = \|rp\| \leq \|s\| = 1,$$

por el Corolario 1, se tiene:

$$\|n\| = \|n - s + s\| = \max\{\|n - s\|, \|s\|\} = \|s\| = 1.$$

Finalmente, dado $n \in \mathbb{Z}$, n se puede escribir de la forma $n = p^a m$, donde p no divide a m, entonces:

$$\|n\| = \|p^a m\| = \|p^a\| \|m\| = \|p^a\| (1) = \|p\|^a.$$

Sea $\rho = \|p\| < 1$. Entonces $\rho = \left(\frac{1}{p}\right)^{\alpha}$, para algún $\alpha > 0$. Teniendo en cuenta la

propiedad $ii)$ de la norma, el resultado anterior se cumple para todo $x \neq 0 \in \mathbb{Q}$, por lo tanto $\|\cdot\|$ es equivalente a $|\cdot|_p$. □

La siguiente proposición establece una relación entre todas las normas no triviales sobre $\mathbb{Q}$.

Proposición 5 *Para todo $x \in \mathbb{Q}, x \neq 0$, se cumple:*

$$\prod_{2 \leq p \leq \infty} |x|_p = 1.$$

$Demostración$. Dado $x \in \mathbb{Q}, x \neq 0$, es posible escribir de manera única, $x = \epsilon p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, donde $|\epsilon| = 1$, los p_i son primos distintos, $\alpha_i \in \mathbb{Z}$, para $i = 1, \cdots, n$. Si q es primo y $q \notin \{p_1, \cdots, p_n\}$, se tiene:

$$|x|_{p_i} = p_i^{-\alpha_i};\ |x|_q = 1;\ |x|_\infty = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}. \tag{4}$$

De (4) se comprueba la proposición. □

Dado que $\mathbb{Q}$ no es completo con el valor absoluto usual y su completación es el cuerpo de los números reales $\mathbb{R}$. Considere $\{x_n\}, x_n = \sum_{i=0}^{n-1} p^i$ con $1 \leq n \in \mathbb{N}$, una sucesión en $\mathbb{Q}$ y $\epsilon > 0$, entonces existe $n_0 \in \mathbb{N}$ tal que $p^{-n_0} < \epsilon$. Sean $n > m \geq n_0$, tal que

$$|x^n - x^m|_p = \left|x^m + \cdots + x^{n-1}\right|_p = p^{-m} \leq p^{-n_0} < \epsilon,$$

es decir, $\{x_n\}$ es una sucesión de Cauchy con respecto a $|\cdot|_p$, que converge a $x = \sum_{i=0}^{\infty} p^i$, donde $x \notin \mathbb{Q}$, por lo tanto $\mathbb{Q}$ no es completo con resptecto a $|\cdot|_p$.

Sea p un número primo fijo, se define $\mathbb{Q}_p$ como la completación de $\mathbb{Q}$ con respecto a $|\cdot|_p$, donde $\mathbb{Q}_p$ es **el cuerpo de los números p-ádicos**. Los elementos de $\mathbb{Q}_p$

son clases de equivalencia de sucesiónes de Cauchy en $\mathbb{Q}$ con respecto a la norma p-ádica. Como se ha señalado anteriormente, $\mathbb{Q}$ puede identificarse como un subcuerpo de $\mathbb{Q}_p$ que consiste en las clases de equivalencia de sucesiones constantes. Sea $a = (\{a_n\}) \in \mathbb{Q}_p$, por la Definición 8,

$$|a|_p = \lim_{n\to\infty} |a_n|_p .$$

Así, por la Proposición 3, dado que $|\cdot|_p$ es No-Arquimediana sobre $\mathbb{Q}$, su extensión que se escribirá igual $|\cdot|_p$, es No-Arquimediana sobre $\mathbb{Q}_p$.

Corolario 2 *Si $|a|_p \neq 0$, entonces la sucesión de normas $\{|a_n|_p\}$ se estabiliza para un n suficientemente grande, es decir, $|a_m|_p = |a|_p$ para todo $m > n$.*

$Demostración$. En efecto, sea $0 < \epsilon < |a|_p$, existe $n_0 \in \mathbb{N}$, tal que si $n > n_0$, entonces:

$$|\hat{a_n} - a|_p < \epsilon < |a|_p ,$$

dado que $|\hat{a_n}|_p = |a_n|_p$, por lo tanto:

$$|\hat{a_n}|_p = |\hat{a_n} - a + a|_p = \max\{|\hat{a_n} - a|_p , |a|_p\} = |a|_p .$$

□

Por tanto, el conjunto de valores que $|\cdot|_p$ toma en $\mathbb{Q}_p$ es el mismo que toma en $\mathbb{Q}$, es decir, $\{p^n, n \in \mathbb{Z}\} \cup \{0\}$, un fenómeno bastante diferente de lo que ocurre con el valor absoluto euclidiano que, extendido de $\mathbb{Q}$ a $\mathbb{R}$, toma todos los valores reales no negativos.

Considere la serie:

$$\frac{d_{-m}}{p^m} + \frac{d_{-m-1}}{p^{m-1}} + \cdots + d_0 + d_1 p + d_2 p^2 + \cdots \tag{5}$$

donde $0 \leq d_i < p$, para todo $i \geq -m$ y $d_m \neq 0$.

Las sumas parciales $S_n = \sum_{i=-m}^{n} d_i p^i$, forman una sucesión de Cauchy con respecto a la norma $|\cdot|_p$, ya que para cada $\epsilon > 0$, existe $n_0 \in \mathbb{N}$ tal que $p^{-n_0} < \epsilon$ y para todo $k > n > n_0$ se tiene:

$$\left| \sum_{i=-m}^{k} d_i p^i - \sum_{i=-m}^{n} d_i p^i \right|_p = \left| \sum_{i=n+1}^{k} d_i p^i \right|_p \leq \max_{n<i\leq k} \{ \left| d_i p^i \right|_p \} = \max_{n<i\leq k} \{ \left| p^i \right|_p \} \leq p^{-n_0} < \epsilon.$$

Por lo tanto, cada serie de la forma (5) representa un elemento de $\mathbb{Q}_p$. Se demostrará que cada clase de equivalencia de una sucesión Cauchy en $\mathbb{Q}$, contiene una única sucesión representativa canónica de Cauchy (la sucesión de sumas parciales de una serie en la forma (5)).
Para describir su construcción, se necesita el siguiente lema.

Lema 2 *Sea $x \in \mathbb{Q}_p$ y $|x|_p \leq 1$, entonces para todo $i \in \mathbb{N}$, existe $\alpha \in \mathbb{Z}$ tal que $|\alpha - x|_p \leq p^{-i}$. El entero α se puede elegir en el conjunto $\{0, 1, 2, \ldots, p^i - 1\}$ y además es único.*

Demostración. Sea $x = \frac{a}{b}$, con $(a, b) = 1$. Dado $|x|_p \leq 1$, implica que p no divide a b, puesto que si p divide a b entonces $ord_p(b) \geq 1$ y $0 \leq ord_p(x) = ord_p(a) - ord_p(b)$, por lo tanto, $0 \geq -ord_p(x) = ord_p(b) - ord_p(a)$, lo cual implica, $ord_p(a) \geq ord_p(b) \geq 1$ y esto contradice que $(a, b) = 1$, de ello se deduce que b y p^i son primos relativos, entonces, se pueden encontrar enteros m y n tales que $mb + np^i = 1$. Sea $\alpha = am$, entonces

$$|\alpha - x|_p = \left|am - \frac{a}{b}\right|_p = \left|\frac{a}{b}\right|_p |mb-1|_p\,,$$
$$\leq |mb-1|_p = \left|np^i\right|_p = |n|_p \left|p^i\right|_p \leq p^{-i}.$$

Finalmente por el algoritmo de la división, existen únicos $q, r \in \mathbb{Z}, 0 \leq r < p^i$, tal que $am = qp^i + r$, sea $\alpha = r \in \{0, 1, \ldots, p^i - 1\}$ y usando la desigualdad triangular fuerte se tiene:

$$|\alpha - x|_p = \left|\left(am - \frac{a}{b}\right) - qp^i\right|_p \leq \text{máx}\left\{\left|am - \frac{a}{b}\right|_p, \left|qp^i\right|_p\right\} \leq p^{-i}.$$

□

Teorema 7 *Toda clase de equivalencia $a \in \mathbb{Q}_p$ con $|x|_p \leq 1$, tiene exactamente una sucesión de Cauchy $\{a_n\}$ que la representa, tal que:*

i) $a_i \in \mathbb{Z},\ 0 \leq a_i < p^i$ *para* $i = 1, 2, \ldots$

ii) $a_i \equiv a_{i+1} \mod p^i$ *para* $i = 1, 2, \ldots$

$Demostración$. Sea $\{b_i\}$ una sucesión de Cauchy representante de a. Se construirá una sucesión de Cauchy $\{a_i\}$ equivalente $\{b_i\}$ que satisfaga $i)$ y $ii)$. Dado

$$|b_i|_p \to |a|_p \leq 1, i \to \infty$$

se puede descartar varios términos iniciales, si es necesario, tal que $|b_i|_p \leq 1$ para todo i.

Para todo $j = 1, 2, \ldots$, sea $N(j)$ un entero positivo tal que

$$|b_i - b_k|_p \leq p^{-j}, \forall i, k \geq N(j).$$

Note que se puede escoger la sucesión $N(j)$ estrictamente creciente con respecto a j, es decir, $N(j) \geq j$. Por el Lema 2, existe $a_j \in \{0, 1, \ldots, p^j - 1\}$, tal que:

$$\left|a_j - b_{N(j)}\right|_p \leq p^{-j}.$$

Se demostrará ahora que $a_j \equiv a_{j+1} \mod p^j$ y $\{b_i\} \sim \{a_i\}$. La primera afirmación se tiene de:

$$\begin{aligned}
|a_{j+1} - a_j|_p &= \left|a_{j+1} - b_{N(j+1)} + b_{N(j+1)} - b_{N(j)} - (a_j - b_{N(j)})\right|_p \\
&\leq \text{máx}\{\left|a_{j+1} - b_{N(j+1)}\right|_p, \left|b_{N(j+1)} - b_{N(j)}\right|_p, \left|a_j - b_{N(j)}\right|_p\} \\
&\leq \text{máx}\{p^{-(j+1)}, p^{-j}, p^{-j}\} = p^{-j},
\end{aligned}$$

de modo que $a_j \equiv a_{j+1} \mod p^j$.

Para demostrar la segunda afirmación, sea j arbitrario; entonces para $i \geq N(j)$ se tiene:

$$\begin{aligned}
|a_i - b_i|_p &= \left|a_i - a_j + a_j - b_{N(j)} - (b_i - b_{N(j)})\right|_p, \\
&\leq \text{máx}\{|a_i - a_j|_p, \left|a_j - b_{N(j)}\right|_p, \left|b_i - b_{N(j)}\right|_p\}, \\
&\leq \text{máx}\{p^{-j}, p^{-j}, p^{-j}\} = p^{-j}.
\end{aligned}$$

Por lo tanto

$$|a_i - b_i|_p \to 0, i \to \infty \Leftrightarrow \{a_i\} \sim \{b_i\}.$$

Para la unicidad, suponga que existe una sucesión distinta $\{x_i\}$ que cumple con las condiciones $i)$ y $ii)$ del teorema con $a_{i_0} \neq x_{i_0}$ para algún i_0, entonces se tiene $a_{i_0} \not\equiv x_{i_0} \mod p^{i_0}$, ya que ambos a_{i_0} y x_{i_0} están entre 0 y $p^{i_0} - 1$. Por lo tanto, usando (ii), para $i > i_0$, se tiene:

$$a_i \equiv a_{i_0} \not\equiv x_i \equiv x_{i_0} \mod p^{i_0},$$

es decir, $a_i \not\equiv x_i \mod p^{i_0}$, por lo tanto,

$$|a_i - x_i|_p > p^{-i_0}, \forall i \geq i_0,$$

lo que implica que $\{a_i\} \not\sim \{x_i\}$, contradiciendo que son equivalentes, por lo tanto $\{a_i\}$ es la única que cumple las condiciones (i) y (ii) del teorema. □

Si $a \in \mathbb{Q}_p$ con $|a|_p \leq 1$, entonces se pueden escribir todos los términos a_i de la sucesión representativa dada por el teorema anterior de la siguiente manera:

$$a_i = d_0 + d_1 p + \cdots + d_{i-1} p^{i-1},$$

donde $d_j \in \{0, 1, \ldots . p-1\}, i = 0, 1, \ldots, p-1$. La condición (ii) implica precisamente que:

$$a_{i+1} = d_0 + d_1 p + \cdots + d_{i-1} p^{i-1} + d_i p^i,$$

donde los coeficientes d_0 a d_{i-1} son todos iguales a los de a_i, así, a está representado de manera única por la serie convergente (en la norma p-ádica),

$$a = \sum_{n=0}^{\infty} d_n p^n.$$

Si $a \in \mathbb{Q}_p$ y $|a|_p > 1$, entonces es posible multiplicar a por una potencia de p (es decir, por $p^m = |a|_p$) para obtener un número p-ádico $a' = ap^m$ que satisface $|a'|_p = 1$, y de acuerdo al razonamiento anterior se tiene que:

$$a' = \sum_{i=0}^{\infty} d_i p^i,$$

donde $d_n \in \{0, 1, \ldots . p-1\}$ para $n \geq 0$ y $d_0 \neq 0$. Dado que $a = p^{-m} a'$, entonces:

$$a = p^{-m} \sum_{i=0}^{\infty} d_i p^i = \sum_{n=-m}^{\infty} d_n p^n$$

donde $d_{-m} \neq 0$ y $d_n \in \{0, 1, \ldots . p-1\}$ para $n \geq -m$.

Por lo tanto, para todo $a \in \mathbb{Q}_p, a \neq 0$, tiene una única representación canónica de la forma:

$$a = \sum_{n=\gamma}^{\infty} d_n p^n = p^{\gamma} \sum_{k=0}^{\infty} x_k p^k,$$

donde $\gamma = -ord_p(x) \in \mathbb{Z}, x_k = d_{k+\gamma}, x_k \in \{0, 1, \ldots, p-1\}, x_0 \neq 0, k \geq 0$. Esta representación también se puede escribir como, $a = (\ldots d_2 d_1 d_0, d_{-1} d_{-2} \ldots d_{\gamma})_p$.

Ejemplo 3 *Calcular la representación canónica de* 23 *en* $\mathbb{Q}_3$.
Usando el algoritmo de la división se tiene:

$$\begin{aligned} 23 &= 7 \cdot 3 + 2 \\ &= (2 \cdot 3 + 1) \cdot 3 + 2 \\ &= 2 \cdot 3^2 + 1 \cdot 3 + 2. \end{aligned}$$

Así, $23 = 2 \cdot 3^0 + 1 \cdot 3^1 + 2 \cdot 3^2 = (\ldots 00212)_3$.

Ejemplo 4 *Demostrar que*

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

En efecto, sea

$$\begin{aligned} x_n :&= (p-1) + (p-1)p + \cdots + (p-1)p^n \\ &= (p-1)\frac{p^{n+1} - 1}{p-1} = p^{n+1} - 1 \end{aligned}$$

Entonces, $\lim_{n\to\infty} x_n = \lim_{n\to\infty} p^{n+1} - 1 = -1$*, puesto que,* $\lim_{n\to\infty} \left|p^{(n+1)}\right|_p = \lim_{n\to\infty} p^{-n-1} =$

0. *Análogamente se tiene*

$$-p = (p-1)p + (p-1)p^2 + (p-1)p^3 + \cdots$$

Ejemplo 5 *Calcular la representación canónica de* $\frac{23}{5}$ *en* $\mathbb{Q}_5$.

$$\begin{aligned}\frac{23}{5} &= \frac{4\cdot 5+3}{5} = 4 + 3\cdot 5^{-1} = (\ldots 0004, 0)_5 + 3(\ldots 0000, 1)_5,\\ &= (\ldots 0004, 0)_5 + (\ldots 0000, 3)_5 = (\ldots 0004, 3)_5.\end{aligned}$$

Definición 10 *Un número p-ádico* $a \in \mathbb{Q}_p$ *se dice que es un* **entero p-ádico** *si su representación canónica contiene solo potencias no negativas de* p. *El conjunto de los enteros p-ádicos se denota por* $\mathbb{Z}_p$ *y es equivalente a decir:*

$$\begin{aligned}\mathbb{Z}_p &= \left\{ x \in \mathbb{Q}_p : x = \sum_{i=i_0}^{\infty} x_i p^i, 0 \leq i_o \right\},\\ &= \{x \in \mathbb{Q}_p : |x|_p \leq 1\}.\end{aligned}$$

Proposición 6 $\mathbb{Z}_p$ *es un anillo local cuyo ideal maximal es el ideal* $p\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq \frac{1}{p}\}$. *Además, cada elemento del complemento* $\mathbb{Z}_p \setminus p\mathbb{Z}_p$ *es invertible en* $\mathbb{Z}_p$, *siendo los únicos elementos invertibles en* $\mathbb{Z}_p$.

$Demostración$.

1. Para ver que $\mathbb{Z}_p$ es un anillo, es equivalente mostrar que $\mathbb{Z}_p$ es un subanillo de $\mathbb{Q}_p$, entonces:

   $a)$ Sean $x, y \in \mathbb{Z}_p$ entonces $|x|_p \leq 1$ y $|y|_p \leq 1$.
   Luego, $|x-y|_p \leq \max\{|x|_p, |y|_p\} \leq 1$. Por lo tanto $(x-y) \in \mathbb{Z}_p$.

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

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

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

2. Para mostrar 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 $|y|_p \leq 1$. Se tiene que $|x-y|_p \leq \max\{|x|_p, |y|_p\} \leq \frac{1}{p}$. Por lo tanto, $(p\mathbb{Z}_p, +)$ es subgrupo de $(\mathbb{Z}_p, +)$.

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

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

   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 $\mathbb{Z}_p$. Si existe $w \in I$ tal que $w \notin p\mathbb{Z}_p$, entonces $|w|_p = 1$.
   Luego, la igualdad $|1|_p = |w|_p |w^{-1}|_p$ implica que $|w^{-1}|_p = 1$ dado que $|w|_p = 1$.
   Entonces $w^{-1} \in \mathbb{Z}_p$ y por ser I ideal de $\mathbb{Z}_p$ se obtiene $1 = ww^{-1} \in I$.
   Para cualquier $x \in \mathbb{Z}_p$ se tiene que $1x = x \in I$. Luego, $\mathbb{Z}_p \subseteq I$, es decir, $I = \mathbb{Z}_p$.
   Cualquier ideal propio de $\mathbb{Z}_p$ está contenido en $p\mathbb{Z}_p$, es decir $\mathbb{Z}_p$ es un dominio de ideales principales y además $p\mathbb{Z}_p$ es el único ideal maximal del anillo $\mathbb{Z}_p$, en consecuencia $\mathbb{Z}_p$ es un anillo local.

4. Si $x \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$ 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 $x^{-1} \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$. Así, cada elemento de $\mathbb{Z}_p \setminus p\mathbb{Z}_p$ 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 $\mathbb{Z}_p$ en $\mathbb{Z}_p$ son los elementos de $\mathbb{Z}_p \setminus p\mathbb{Z}_p$.

□

La proposicón anterior permite establecer la siguiente definición.

Definición 11 *El grupo de unidades de* $\mathbb{Z}_p$ *es:*

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

El **cuerpo residual** de $\mathbb{Q}_p$ es $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p = \{0, 1, \ldots, p-1\}$.

Corolario 3 *Sea* $n \in \mathbb{N}$ *se tiene*

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

$Demostración$. Usando el lema 2, para $x\mathbb{Z}_p$ existe un único $\alpha_x \in \mathbb{Z}$ que cumple $|x - \alpha_x|_p \leq p^{-n}$ y $0 \leq \alpha_x \leq p^n - 1$. Se define

$$\begin{aligned} f : \mathbb{Z}_p/p^n\mathbb{Z}_p &\longrightarrow \mathbb{Z}/p^n\mathbb{Z} \\ x + p^n\mathbb{Z}_p &\longmapsto \alpha_x + p^n\mathbb{Z}, \end{aligned}$$

- f está bien definida:
  Si $x + p^n\mathbb{Z}_p = y + p^n\mathbb{Z}_p$ entonces $(x - y) \in p^n\mathbb{Z}_p$, es decir, $|x - y|_p \leq p^{-n}$ esto implica que

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

  así $\alpha_x \equiv \alpha_y \mod p^n$ entonces $\alpha_x + p^n\mathbb{Z} = \alpha_y + p^n\mathbb{Z}$, así $f(x + p_p^{\mathbb{Z}}) = f(y + p^n\mathbb{Z})$.

- f es biyección:
  f es inyectiva puesto que

  $f(x + p^n\mathbb{Z}_p) = f(y + p^n\mathbb{Z}_p)$ entonces $\alpha_x + p^n\mathbb{Z} = \alpha_y + p^n\mathbb{Z}$, así $\alpha_x \equiv \alpha_y \mod p^n$.

Luego,

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

entonces $x-y \in p^n\mathbb{Z}_p$, así $x+p^n\mathbb{Z}_p = y+p^n\mathbb{Z}_p$. f es sobreyectiva dado que para cualquier $k+p^n\mathbb{Z}$ se tiene $f(k+p^n\mathbb{Z}_p) = k+p^n\mathbb{Z}$.

- f es homomorfismo:

  1. Sea $(1+p^n\mathbb{Z}_p) \in \mathbb{Z}_p/p^n\mathbb{Z}_p$, tal que $f(1+p^n\mathbb{Z}_p) = 1+p^n\mathbb{Z}$.
  2. Sean $x, y \in \mathbb{Z}_p$ tales que $x+p^n\mathbb{Z}_p, y+p^n\mathbb{Z}_p \in \mathbb{Z}/p^n\mathbb{Z}_p$, entonces $f(x+p^n\mathbb{Z}_p+y+p^n\mathbb{Z}_p) = f(x+y+p^n\mathbb{Z}_p) = \alpha_{x+y}+p^n\mathbb{Z} = \alpha_x+\alpha_y+p^n\mathbb{Z} = f(x+p^n\mathbb{Z}_p)+f(y+p^n\mathbb{Z}_p)$.
     En efecto,

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

     Esto implica $\alpha_x+\alpha_y \equiv \alpha_{x+y} \mod p^n$ entonces $\alpha_x+\alpha_y+p^n\mathbb{Z} = \alpha_{x+y}+p^n\mathbb{Z}$.
  3. Se tiene que

     $$\begin{aligned}f((x+p^n\mathbb{Z}_p)(y+p^n\mathbb{Z}_p)) &= f(xy+p^n\mathbb{Z}_p) = \alpha_{xy}+p^n\mathbb{Z} \\ &= \alpha_x\alpha_y+p^n\mathbb{Z} \\ &= f(x+p^n\mathbb{Z}_p)f(y+p^n\mathbb{Z}_p).\end{aligned}$$

La cadena de igualdades se justifica usando:

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

entonces $\alpha_x\alpha_y \equiv \alpha_{xy} \mod p^n \Rightarrow \alpha_x\alpha_y + p^n\mathbb{Z} = \alpha_{xy} + p^n\mathbb{Z}$.

□

1.1.3. Topología en $\mathbb{Q}_p$ En esta sección se introducen los conceptos de bolas y esferas en $\mathbb{Q}_p$.
$\mathbb{Q}_p$ es un espacio métrico con $d(x, y) = |x - y|_p$.

Definición 12 *Sea $r \in \mathbb{Z}$ y $a \in \mathbb{Q}_p$, denotaremos y definiremos*

- $B_r(a) = \{x \in \mathbb{Q}_p : |x - a|_p \leqslant p^r\}, r \in \mathbb{Z}$, *la bola con centro a y radio p^r.*
- $S_r(a) = \{x \in \mathbb{Q}_p : |x - a|_p = p^r\}, r \in \mathbb{Z}$, *la esfera con centro a y radio p^r.*

Proposición 7 *Sean $a \in \mathbb{Q}_p$ y $n \in \mathbb{Z}$, tales que los conjuntos $a + p^n\mathbb{Z}_p$ son bolas en $\mathbb{Q}_p$, más precisamente, $a + p^n\mathbb{Z}_p = B_{-n}(a)$.*

$Demostración$. Dado que $x \in a + p^n\mathbb{Z}_p$ se tiene que $x = a + p^n y$ con $y \in \mathbb{Z}_p$, por lo tanto

$$x - a = p^n y \text{ si y solo si } |x - a|_p \leq p^{-n} \text{ si y solo si } x \in B_{-n}(a)$$

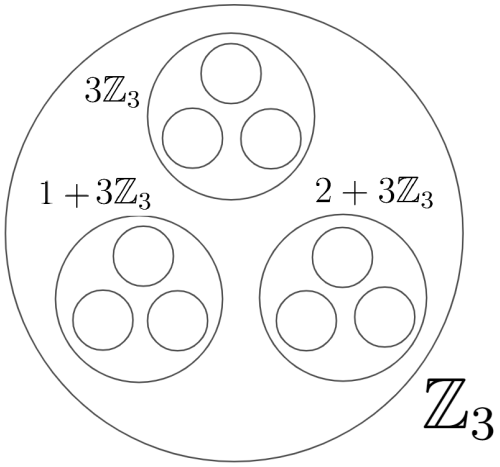
. □

Proposición 8 *Sean $a \in \mathbb{Q}_p$ y $n \in \mathbb{Z}$, los conjuntos $a + p^n\mathbb{Z}_p^\times$ son esferas en $\mathbb{Q}_p$, es decir, $a + p^n\mathbb{Z}_p^\times = S_{-n}(a)$.*

$Demostración$. Puesto que $x \in a + p^n\mathbb{Z}_p^\times$ se tiene que $x = a + p^n y$, con $y \in \mathbb{Z}_p^\times$ entonces $x - a = p^n y$ implica $|x - a|_p = p^{-n}$ por lo tanto $x \in S_{-n}(a)$. □

Ejemplo 6 *Las bolas unitarias se pueden asociar al conjunto de* **Cantor***, en el caso* $p = 3$

Figura 1. Bola unitaria en $\mathbb{Q}_3$



A continuación se presentan resultados sobre la topología de $\mathbb{Q}_p$, que provienen de la propiedad ultramétrica.

Lema 3 $S_r(a), B_r(a)$ *son conjuntos abiertos y cerrados en la topología de* $\mathbb{Q}_p$*.*

$Demostración$. Se mostrará que $S_r(a)$ es abierto. Puesto que $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus p\mathbb{Z}_p$, el Corolario 3, afirma que si $r \in \mathbb{N}$ entonces $\mathbb{Z}_p/p^r\mathbb{Z}_p \cong \mathbb{Z}/p^r\mathbb{Z}$. Esto implica que los números $0, 1, 2, \ldots, p^r - 1$ son representantes de las clases de $\mathbb{Z}_p/p^r\mathbb{Z}_p$, es decir,

$$\mathbb{Z}_p = \bigsqcup_{i=0}^{p^r-1} i + p^r\mathbb{Z}_p \text{ entonces } \mathbb{Z}_p^\times = \bigsqcup_{i=0}^{p-1} i + p\mathbb{Z}_p.$$

$$S_r(a) = a + p^{-r}\mathbb{Z}_p^\times = \bigsqcup_{i=1}^{p-1}(a + ip^{-r} + p^{-(r-1)}\mathbb{Z}_p) = \bigsqcup_{i=1}^{p-1} B_{r-1}(a + ip^{-r}),$$

$S_r(a)$ es unión de bolas abiertas de radio $r-1$, por lo tanto es un conjunto abierto. Observe que $S_r(a)$ es cerrado. Dado que $\overline{B_r(a)} = \left\{x \in \mathbb{Q}_p : |x-a|_p \leq r\right\}$ es cerrado

y $B_r(a)$ es abierto, entonces $(B_r(a))^c = \left\{x \in \mathbb{Q}_p : |x-a|_p \geq r\right\}$ es cerrado, por lo tanto, $S_r(a) = \overline{B_r(a)} \cap (B_r(a))^c$ es cerrado.
Para demostrar que $B_r(a)$ es cerrado, basta mirar que $(B_r(a))^c$ es abierto.
Note que $(B_r(a))^c = \left\{x \in \mathbb{Q}_p : |x-a|_p \geq r\right\} = S_r(a) \cup D; D = \left\{x \in \mathbb{Q}_p : |x-a|_p < r\right\}$, donde $S_r(a), D$ son abiertos, lo cual implica que $(B_r(a))^c$ es abierto, por lo tanto $B_r(a)$ es cerrado. □

Lema 4 *Si $b \in B_r(a)$ entonces $B_r(b) = B_r(a)$, es decir, todo punto de la bola $B_r(a)$ es su centro.*

$Demostración$. Sea $x \in B_r(a)$ lo cual implica $|b-x|_p < r$, por hipótesis se tiene que $|a-b|_p < r$ y usando la desigualdad triangular fuerte, se obtiene:
$|a-x|_p = |(a-b)+(b-x)|_p \leq máx\{|a-b|_p, |b-x|_p\} < r$, por lo tanto
$B_r(b) \subset B_r(a)$, análogamente, $B_r(a) \subset B_r(b)$, se concluye que, $B_r(b) = B_r(a)$. □

Proposición 9 *Las bolas en $\mathbb{Q}_p$ cumplen las siguientes condiciones:*

- *Si $B_r(a), B_s(b) \subset \mathbb{Q}_p$ entonces $B_r(a) \cap B_s(b) = \emptyset$ ó $B_r(a) \subset B_s(b)$ o $(B_r(b) \subset B_s(a))$.*
- *La frontera de toda bola es vacía.*

$Demostración$.

- Si $B_r(a) \cap B_s(b) \neq \emptyset$, suponga que $r \leq s$ y sea $z \in B_r(a) \cap B_s(b)$, por el Lema 4, se tiene que $B_r(a) = B_r(z)$ y $B_s(b) = B_s(z)$, pero $B_r(z) \subset B_s(z)$ lo cual implica que $B_r(a) \subset B_s(b)$, (la otra contenencia se da cuando $s \leq r$).
- Se tiene $B_r(a) \nsubseteq B_s(b)$ y $B_s(b) \nsubseteq B_r(a)$. Note que $B_r(a) \cap B_s(b) = \emptyset$. Suponga que $B_r(a) \cap B_s(b) \neq \emptyset$, por lo anterior implica que $B_r(a) \subset B_s(b)$ o $B_r(b) \subset B_s(a)$, lo cual es absurdo, por lo tanto $B_r(a) \cap B_s(b) = \emptyset$.

- Sean $Fr(B_r(a))$, $int(B_r(a))$ la frontera y el interior de la bola $B_r(a)$ respectivamente. Note que $Fr(B_r(a)) = \overline{B_r(a)} \setminus int(B_r(a))$, pero $\overline{B_r(a)} = int(B_r(a)) = B_r(a)$ por lo tanto $Fr(B_r(a)) = \emptyset$.

□

1.1.4. Sucesiones y series p-ádicas

Teorema 8 *Una sucesión $\{a_n\}$ en $\mathbb{Q}_p$ es de Cauchy, y por lo tanto converge, si y solo si, satisface que:*

$$\lim_{n\to\infty} |a_{n+1} - a_n|_p = 0. \tag{6}$$

$Demostración$. Si $\{a_n\}$ es una sucesión de Cauchy, entonces:

$$\lim_{m,n\to\infty} |a_m - a_n|_p = 0,$$

en particular, si $m = n + 1$ se cumple (6). Recíprocamente, para todo $\epsilon > 0$, existe $N \in \mathbb{N}$, tal que si $n > N$ se cumple:

$$|a_{n+1} - a_n|_p < \epsilon,$$

sean $m > n > N$, por la norma p-ádica, se obtiene:

$$\begin{aligned} |a_m - a_n|_p &= |a_m - a_{m-1} + a_{m-1} - a_{m-2} + a_{m-2} - \cdots - a_{n+1} + a_{n+1} - a_n|_p \\ &\leq \text{máx}\{|a_m - a_{m-1}|_p, |a_{m-1} - a_{m-2}|_p, \ldots, |a_{n+1} - a_n|_p\} < \epsilon. \end{aligned}$$

Lo cual implica que $\{a_n\}$ es una sucesión de Cauchy. □

Ahora se considera la serie $\sum_{i=1}^{\infty} a_i$ en $\mathbb{Q}_p$. Se dirá que la serie converge si la sucesión de sumas parciales, $s_n = \sum_{i=1}^{n} a_i$, converge en $\mathbb{Q}_p$ y **converge absolutamente** si $\sum_{i=1}^{\infty} |a_i|_p$, converge en $\mathbb{R}$.

Proposición 10 *Si la serie* $\sum_{i=1}^{\infty} |a_i|_p$ *converge en* $\mathbb{R}$*, entonces la serie* $\sum_{i=1}^{\infty} a_i$ *converge en* $\mathbb{Q}_p$*.*

$Demostración$. Dado que la serie $\sum_{i=1}^{\infty} |a_i|_p$ converge, entonces su sucesión de sumas parciales también converge y es de Cauchy, es decir, para todo $\epsilon > 0$ existe $n \in \mathbb{N}$ tal que para todo $m > n > N$ se tiene:

$$\sum_{i=n+1}^{m} |a_i|_p < \epsilon,$$

entonces:

$$|s_m - s_n|_p = \left| \sum_{i=n+1}^{m} a_i \right|_p \leq \sum_{i=n+1}^{m} |a_i|_p < \epsilon,$$

en consecuencia $\{s_n\}$ es una sucesión de Cauchy y por tanto la serie $\sum_{i=1}^{\infty} a_i$ converge en $\mathbb{Q}_p$. □

Ahora se mostrará un resultado muy útil en $\mathbb{Q}_p$, consecuencia del Teorema 8.

Proposición 11 *Una serie* $\sum_{i=1}^{\infty} a_i$*, con* $a_i \in \mathbb{Q}_p$ *converge en* $\mathbb{Q}_p$ *si y solo si* $\lim_{n\to\infty} a_n = 0$*, en este caso:*

$$\left| \sum_{n=1}^{\infty} a_n \right|_p \leq \max_{n\in\mathbb{N}} \{|a_n|_p\}.$$

$Demostración$. La serie converge si y sólo si la sucesión de sumas parciales, $s_n = \sum_{i=1}^{n} a_i$ converge. Dado que $a_n = s_n - s_{n-1}$, por el Teorema 8, la serie converge si y solo si $\lim_{n\to\infty} a_n = 0$.
Suponiendo que $\sum_{n=1}^{\infty} a_n$ converge. Sea $S = |\sum_{n=1}^{\infty} a_n|_p$.
Si $S = 0$ el resultado es inmediato dado que $|a_n|_p \geq 0$. Si $S \neq 0$, por el Corolario 2, se tiene que $|S|_p = |s_N|_p$ para un N suficientemente grande. Por otra parte, dado

que a_n tiende a cero y por la desigualdad triangular fuerte:

$$|s_N|_p = \left|\sum_{n=1}^{N} a_n\right|_p \leq \max_{1\leq n\leq N}\{|a_n|_p\} = \max_{n\in\mathbb{N}}\{|a_n|_p\}.$$

□

Observación. El resultado anterior no se cumple en $(\mathbb{R}, |\cdot|)$, por ejemplo, la serie $\sum_{n=1}^{\infty} \frac{1}{n}$, diverge aunque $\frac{1}{n} \to 0$, cuando $n \to \infty$.

Ahora se darán dos definiciones importantes para el desarrollo de las secciones siguientes.

Definición 13 (Caracter aditivo) *Un caracter aditivo del campo $\mathbb{Q}_p$ está definido como una función continua $\chi : \mathbb{Q}_p \longrightarrow \mathbb{C}$, tal que $|\chi(x)| = 1$ y $\chi(x+y) = \chi(x)\chi(y), x, y \in \mathbb{Q}_p$.*

Propiedades:

1. Si $\chi(x)$ es un caracter aditivo arbitrario, se tiene $\chi(0) = 1$, dado que $\chi(x) = \chi(x+0) = \chi(x)\chi(0)$.
2. $\chi(-x) = \chi^{-1}(x) = \overline{\chi(x)}$, dado que $1 = \chi(0) = \chi(x-x) = \chi(x)\chi(-x)$ y por la unicidad del inverso, se tiene que $\chi(-x) = \chi^{-1}(x)$.
3. $\chi(nx) = (\chi(x))^n$, para todo $n \in \mathbb{Z}$. Es consecuencia de aplicar $|n| - 1$ veces la primera propiedad.

Si $x \in \mathbb{Q}_p$, el caracter aditivo $\chi(x) = 1$, se conoce como el caracter aditivo trivial.

Definición 14 *Sea $f(x) = \sum c_i x^i$ en $\mathbb{Q}_p[[x]]$ es una restricción especial de series de potencias (SRP), si $f(0) = 0$, es decir, $c_0 = 0$ y*

$$c_i \equiv 0 \mod p^{|i|-1},\ |i| = i_1 + \cdots + i_n,$$

para todo $i \neq 0$ en $\mathbb{N}^n$.

1.1.5. Integración en $\mathbb{Q}_p$ En $\mathbb{Q}_p$ existe una medida que es una generalización de la medida de Lebesgue en $\mathbb{R}^n$. En esta sección se presentan los resultados necesarios para el desarrollo de este trabajo, algunos sin demostración, para un estudio más profundo ver [7].

Teorema 9 *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 $U \neq \emptyset$.*
2. *$\int_{x*E} dx = \int_E dx$, para cada conjunto de Borel E.*

Una prueba de este teorema en [7], pág.254.

Definición 15 *La medida dx descrita en el teorema anterior es una* **Medida de Haar** *sobre G.*

Por lo visto en el capítulo anterior 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 $\mathbb{Q}_p$, es decir, $a + p^m\mathbb{Z}_p$, generan una $\sigma-$álgebra de Borel.

---

[7] P. HALMOS. *Measure Theory*. Van der Nostrand Reinhold Company, 1950, pág. 254.

La medida dx asigna a cada subconjunto abierto compacto U un número real no negativo $\int_U dx$, que además satisface

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

para todos los subconjuntos abiertos compactos U_n es $\mathbb{Q}_p$, que son disjuntos dos a dos, tal que $\bigcup_{n=1}^{\infty} U_n$ es compacto. También se cumple,

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

Definición 16 *Una función $\varphi : \mathbb{Q}_p \to \mathbb{C}$ es llamada localmente constante, si para todo $x \in \mathbb{Q}_p$ existe un compacto abierto $x \in U \subset \mathbb{Q}_p$, tal que $f(x) = f(u)$ para todo $u \in U$.*

Toda función localmente constante $\varphi : \mathbb{Q}_p \to \mathbb{C}$ puede expresarse como una combinación lineal de funciones características de la forma

$$\varphi(x) = \sum_{n=1}^{\infty} c_n 1_{U_n}(x),\ c_n \in \mathbb{C},$$

donde,

$$1_{U_n}(x) = \begin{cases} 0,\ si\ x\ \notin U_n \\ 1,\ si\ x \in U_n \end{cases}$$

y $U_n \subset \mathbb{Q}_p$ es un compacto abierto para cada n.

Definición 17 *Sea $\varphi : \mathbb{Q}_p \to \mathbb{C}$ una función localmente constante. Considere $A = \bigcup_{i=1}^{k} U_i,\ U_i \cap U_j = \emptyset, i \neq j$ con U_i compacto.*

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

Definición 18 *El soporte de una función compleja f definida en un espacio topológico X es la clausura del conjunto*

$$\{x \in X | f(x) \neq 0\}.$$

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

Definición 19 *Una función $\varphi : \mathbb{Q}_p \to \mathbb{C}$ es llamada* **localmente integrable***, $\varphi \in L^1_{loc}$, si*

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

existe para cada compacto K.

Proposición 12 *Sea $d(ax)$ definida por $d(ax)(U) = dx(aU)$, entonces $d(ax)$ es una medida de Haar y*

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

Es decir,

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

$Demostración$. Sea $T_a : \mathbb{Q}_p \longrightarrow \mathbb{Q}_p$, donde $T_a(x) = ax$. Note que T_a está bien definido y además es inyectivo pues $T_a(x) = T_a(y)$ si y solo si $ax = ay$ si y solo si$x = y$. Si $y \in \mathbb{Q}_p$ entonces $T_a\left(\frac{y}{a}\right) = y$, luego T_a es sobreyectiva.
Dado que 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:

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

Por lo tanto, $d(ax)$ es una medida de Haar sobre $\mathbb{Q}_p$, luego existe una constante positiva $C(a)$ tal que $\int_{aU} dx = C(a) \int_U dx$.

Para calcular $C(a)$ se puede escoger cualquier conjunto abierto compacto U, en este caso se tomará $U = \mathbb{Z}_p$. Suponga que $a \in \mathbb{Q}_p$, entonces $|a|_p = p^{-k}$ con $k \in \mathbb{N}$. Se tiene

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

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

implica que

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

Dado que $|a|_p = p^{-k}$ entonces $a = p^k u$ con $u \in \mathbb{Z}_p^\times$ y $\mathbb{Z}_p = u\mathbb{Z}_p$, por lo tanto:

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

Así,

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

De manera similar, para $a \notin \mathbb{Z}_p$, por tanto,

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

□

Como consecuencia inmediata de la proposición anterior se tiene:

Corolario 4 *Sea $\varphi : U \to \mathbb{C}$, donde U es un conjunto Borel, es decir, un abierto compacto, entonces*

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

donde $a \in \mathbb{Q}_p^\times, b \in \mathbb{Q}_p$.

$Demostración$. Haciendo el cambio de variable $x = ay + b$, se obtiene,

$$dx = d(ay+b) = d(ay) = |a|_p \, dy,$$

dado que es invariante bajo traslaciones, por otro lado se tiene; $y = a^{-1}x - a^{-1}b$,

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

□

Ejemplo 7 *Para todo $r \in \mathbb{Z}$,*

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

Ejemplo 8 *Para todo $r \in \mathbb{Z}$,*

$$\int_{S_r(0)} dx = \int_{B_r(0)} dx - \int_{B_{r-1}(0)} dx = p^r - p^{-r} = p^r(1-p^{-1}).$$

Ejemplo 9 *Sea $U = \mathbb{Z}_p \setminus \{0\}$, U no es compacto y, $\int_U dx = \int_{\mathbb{Z}_p} dx = 1$. En efecto,*

sea $\{p^n\}_{n\in\mathbb{N}}$*, una sucesión en* U *que converge a* 0*, tal que* U *no es compacto. Dado que,* $U = \mathbb{Z}_p \setminus \{0\} = \bigsqcup_{j=0}^{\infty} \left\{x \in \mathbb{Z}p : |x|_p = p^{-j}\right\}$*, se obtiene:*

$$\begin{aligned}\int_U dx &= \sum_{j=0}^{\infty} \int_{p^j\mathbb{Z}_p^\times} dx = \sum_{j=0}^{\infty} \left|p^j\right|_p \int_{\mathbb{Z}_p^\times} dy = \sum_{j=0}^{\infty} p^{-j} \int_{\mathbb{Z}_p^\times} dy; \quad (x = p^j y),\\ &= \left(\frac{1}{1-p^{-1}}\right) \int_{\mathbb{Z}_p^\times} dy = \left(\frac{1}{1-p^{-1}}\right) \left(\int_{\mathbb{Z}_p} dy - \int_{p\mathbb{Z}_p} dy\right),\\ &= \left(\frac{1}{1-p^{-1}}\right) \left(1-p^{-1}\right) = 1,\end{aligned}$$

Se observa que $\mathbb{Z}_p \setminus \{0\}$ *tiene medida Haar* 1 *y* $\{0\}$ *tiene medida Haar* 0*.*

Ejemplo 10 *Demostrar que*

$$\int_{\mathbb{Z}_p} \ln\left(|x|_p\right) dx = -\frac{\ln p}{p-1}.$$

Demostración.

$$\begin{aligned}\int_{\mathbb{Z}_p} \ln\left(|x|_p\right) dx &= \sum_{r=0}^{\infty} \int_{S_{-r}(0)} \ln\left(|x|_p\right) dx = (1-p^{-1}) \sum_{r=0}^{\infty} \ln(p^{-r}) p^{-r},\\ &= (1-p^{-1}) \sum_{r=0}^{\infty} -r\ln(p) p^{-r} = -(1-p^{-1})\ln(p) \sum_{r=0}^{\infty} r p^{-r},\\ &= -(1-p^{-1})\ln(p) \frac{p}{(p-1)^2},\end{aligned}$$

entonces

$$\int_{\mathbb{Z}_p} \ln|x|_p dx = -\frac{p-1}{p}\ln(p)\frac{p}{(p-1)^2} = -\frac{\ln p}{p-1}.$$

Recordando que $\sum_{r=0}^{\infty} r p^{-r} = \frac{p}{(p-1)^2}$*.*

Ahora, se define el espacio $\mathbb{Q}_p^n := \mathbb{Q}_p \times \mathbb{Q}_p \times \cdots \times \mathbb{Q}_p$, que consiste en los puntos

$x = (x_1, x_2, \ldots, x_n)$, con $x_i \in \mathbb{Q}_p$ para $j = 1, 2, \ldots, n$. La norma sobre $\mathbb{Q}_p^n$ es

$$\|x\|_p = \max_{1 \leq i \leq n} |x_i|_p; \ x \in \mathbb{Q}_p^n.$$

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

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

pero esta se cumple, puesto que

$$\begin{aligned} \|x + y\|_p &= \max_{1 \leq i \leq n} |x_i + y_i|_p \leq \max_{1 \leq i \leq n} \max\{|x_i|_p, |y_i|_p\}, \\ &= \max\{\max_{1 \leq i \leq n} |x_i|_p, \max_{1 \leq i \leq n} |y_i|_p\}, \\ &= \max\{\|x\|_p, \|y\|_p\}. \end{aligned}$$

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. Las bolas y esferas se definen de manera similar al caso unidimensional, como sigue:

Definición 20

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

es la bola con centro a *y radio* p^r*, y*

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

es la esfera con centro a *y radio* p^r*.*

Las bolas y esferas son conjuntos cerrados y abiertos en $\mathbb{Q}_p^n$, además si $a = (a_1, a_2, \ldots, a_n)$ entonces

$$B_r^n(a) = B_r(a_1) \times B_r(a_2) \times \cdots \times B_r(a_n). \tag{7}$$

Por otro lado, existe una medida de Haar $d^n x$ sobre $\mathbb{Q}_p^n$ y se puede normalizar por la condición

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

$d^n x$ es la **medida producto** de $dx_1, \ldots, dx_n$, donde dx_i es la medida de Haar sobre $(\mathbb{Q}_p, +)$ normalizada. En particular, si $A = A_1 \times \cdots \times A_n$, donde $A_i \subset \mathbb{Q}_p$ es compacto para $i = 1, \ldots, n$, se cumple

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

2. POLIEDRO DE NEWTON

En este capítulo se presentarán los conceptos y resultados importantes sobre el poliedro de Newton y se muestran ejemplos de polígonos de Newton, dado que se trabaja con polinomios en dos variables, tomando como referencia [8].

2.1. POLIEDRO DE NEWTON GLOBAL

Sean R un anillo conmutativo y $f(x) = f(x_1, \cdots, x_n) = \sum_{\omega \in \mathbb{N}^n} a_\omega x_1^{\omega_1} \cdots x_n^{\omega_n}$ polinomio definido sobre $R[x_1, \cdots, x_n]$ tal que $f(0) = 0$.
Se denota **soporte de f** al conjunto

$$supp(f) = \{\omega \in \mathbb{N}^n | a_\omega \neq 0\}$$

Definición 21 *El* **poliedro de Newton global de f**, $\Gamma_{gl}(f)$, *se define como la envolvente convexa de supp(f). Sea* $f \in R[x_1, \cdots, x_n]$ *y* $\mathbb{R}^+ = \{x \in \mathbb{R} | x \geq 0\}$. *El* **poliedro de Newton de f**, $\Gamma(f)$, *se define como la envolvente convexa en* $(\mathbb{R}^+)^n$ *del conjunto*

$$\bigcup_{\omega \in supp(f)} \omega + (\mathbb{R}^+)^n.$$

Note que $\Gamma(f) = \Gamma_{gl}(f) + (\mathbb{R}^+)^n$.

Definición 22 *La* **cara** *de* $\Gamma(f)$ *es todo subconjunto convexo* τ, *que se pueda obtener mediante la intersección de* $\Gamma(f)$ *y un hiperplano* H *de* $\mathbb{R}^n$ *tal que alguno de*

---

[8] J. DENEF y HOORNAERT K. "Newton polyhedra and Igusa's local zeta function". En: *J. Number Theory 89* (2001).

los semiespacios definidos por H contiene a $\Gamma(f)$. De forma análoga la definición de cara de $\Gamma_{gl}(f)$.

Nota. Se considera el poliedro $\Gamma(f)$ ó $(\Gamma_{gl}(f))$ como cara. Para toda cara distinta al vacío o al total, las cuales se llamarán $caras\ propias$.

Definición 23 *Sea C un conjunto convexo no vació en $\mathbb{R}^n$ y β un vector no nulo en $\mathbb{R}^n$. Se dice que C retrocede en la dirección de β sí, y sólo si $(x + \lambda\beta) \in C$ para todo $\lambda \geq 0$ y todo $x \in C$. En este caso se llama β una dirección de recesión de C. El vector β también se conoce como rayo.*

Definición 24 *Se define la dimensión de la cara τ como la dimensión del subespacio afin generado por τ. Los vértices serán caras de dimensión 0.*

Se puede dar una expresión de las caras del poliedro de Newton en forma de suma de Minkowski

$$\tau = \text{convex}\{v_1, \ldots, v_k\} + \sum_{i=1}^{l} \mathbb{R}^+ r_i,$$

donde,

- $\{v_1, \ldots, v_k\} \subset \text{supp}(f)$ son los vértices de la cara.
- $\{r_1, \ldots, r_l\} \subset \{e_1, \ldots, e_n\}$, donde $\{e_1, \ldots, e_n\}$ es la base canónica de $\mathbb{R}^n$ y éstos son los $rayos$ contenidos en la cara.

Se tiene que una cara en $\mathbb{R}^n$ es compacta si y sólo si ésta no contiene rayos.

2.2. COMPONENTES DEL POLIEDRO DE NEWTON

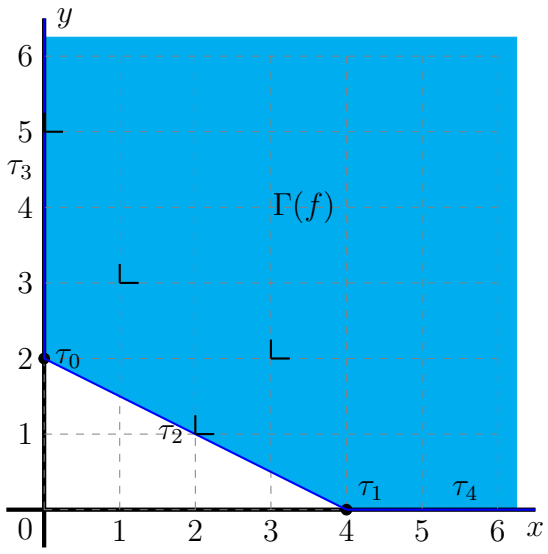
Definición 25 *Sea $f(x) = f(x_1, \cdots, x_n) = \sum_{\omega \in \mathbb{N}^n} a_\omega x_1^{\omega_1} \cdots x_n^{\omega_n}$ polinomio definido sobre un anillo R conmutativo tal que $f(0) = 0$. Para toda cara τ del poliedro de*

Newton $\Gamma(f)$, se define el polinomio asociado a τ como:

$$f_\tau(x) = \sum_{\omega \in \tau} a_\omega x^\omega.$$

Ejemplo 11 *Consideremos $f(x,y) = 2x^3y^2 + y^5 + x^4 - 2xy^3 - 2x^2y + y^2$, (ver [4])*

Figura 2. Polígono de Newton de $f(x,y)$.



Se tiene que:

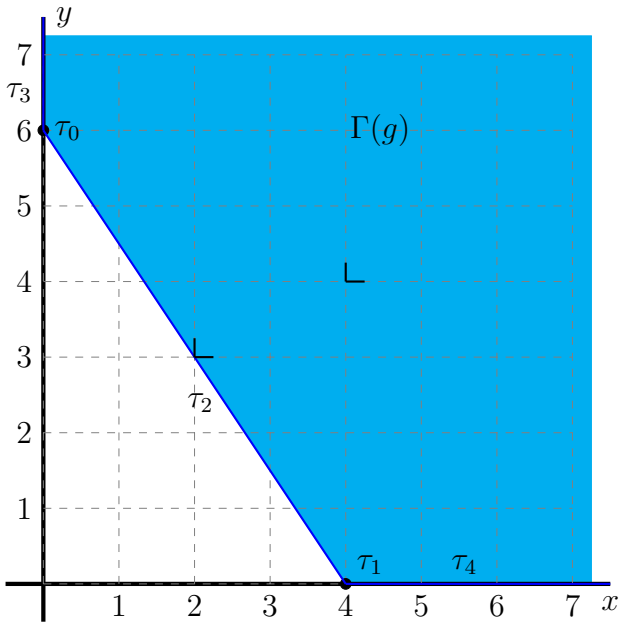
Cara propia τ	*Dimensión*
$\tau_0 = \{(0,2)\}$	0
$\tau_1 = \{(4,0)\}$	0
$\tau_2 = \{(1-\lambda)(0,2) + \lambda(4,0) \mid 0 < \lambda < 1\}$	1
$\tau_3 = \{(0,2) + \mathbb{R}^+(0,1)\}$	1
$\tau_4 = \{(4,0) + \mathbb{R}^+(1,0)\}$	1

y los polinomios asociados a cada cara son

$$
\begin{aligned}
f_{\tau_0} &= y^2, \\
f_{\tau_1} &= x^4, \\
f_{\tau_2} &= x^4 - 2x^2y + y^2, \\
f_{\tau_3} &= y^2 + y^5, \\
f_{\tau_4} &= x^4.
\end{aligned}
$$

Ejemplo 12 $g(x,y) = (y^3 - x^2)^2 + x^4y^4$

Figura 3. Polígono de Newton de $g(x, y)$.



Se tiene que:

Cara propia τ	*Dimensión*
$\tau_0 = \{(0, 6)\}$	0
$\tau_1 = \{(4, 0)\}$	0
$\tau_2 = \{(1-\lambda)(0, 6) + \lambda(4, 0) \mid 0 < \lambda < 1\}$	1
$\tau_3 = \{(0, 6) + \mathbb{R}^+(0, 1)\}$	1
$\tau_4 = \{(4, 0) + \mathbb{R}^+(1, 0)\}$	1

y los polinomios asociados a cada cara son

$$g_{\tau_0} = y^6,$$
$$g_{\tau_1} = x^4,$$
$$g_{\tau_2} = (y^3 - x^2)^2,$$
$$g_{\tau_3} = y^6,$$
$$g_{\tau_4} = x^4.$$

Definición 26 *Sean $f \in \mathbb{K}[x_1, \cdots, x_n]$ para $\mathbb{K}$ campo y S un subconjunto de caras de $\Gamma(f)$. Se dice que f es no degenerado sobre $\mathbb{K}$ con respecto a S, si para toda cara $\tau \in S$, el lugar de ceros de f_τ no tiene singularidades en $(\mathbb{K}^\times)^n$.*

La condición de no degeneración sobre $\mathbb{F}_p$ en una cara τ es equivalente a que el sistema de ecuaciones en congruencias:

$$\begin{cases} f_\tau \equiv 0 \ mód \ p \\ \\ \dfrac{\partial f_\tau}{\partial x_i} \equiv 0 \ mód \ p, \ i = 1, 2, \cdots, n \end{cases}$$

no tiene solución en $(\mathbb{Z}_p^\times)^n$.

Lema 5 *Sea $a \in (\mathbb{R}^+)^n$, se tiene que la función $\phi_a : \Gamma(f) \to \mathbb{R}$ con $\phi_a(x) = a \cdot x$ toma un mínimo sobre una cara de $\Gamma(f)$. En particular, éste se alcanza sobre el conjunto de vértices de $\Gamma(f)$.*

$Demostración.$ Si $a = 0$, es trivial. Suponga $a \neq 0$, es claro que ϕ_a es continua y alcanza un mínimo sobre $\Gamma_{gl}(f)$ por ser cerrado y acotado (compacto) en $\mathbb{R}^n$. Este mínimo también lo es sobre el poliedro de Newton $\Gamma(f) = \Gamma_{gl}(f) + (\mathbb{R}^+)^n$, dado que todo elemento se puede escribir de la forma $p + \lambda$ con $p \in \Gamma_{gl}(f)$ y $\lambda \in (\mathbb{R}^+)^n$, y puesto que $a \in (\mathbb{R}^+)^n$ se tiene:

$$a \cdot (p + \lambda) = a \cdot p + a \cdot \lambda \geq a \cdot p.$$

Sea $m(a)$ el valor mínimo de Γ_{gl}, tal que la ecuación $a \cdot x = m(a)$ no define un hiperplano de soluciones en $\mathbb{R}^n$, de tal forma que $\Gamma(f)$ está contenido en el semiespacio positivo $\{a \cdot x \geq m(a)\}$. Luego $\{a \cdot x = m(a)\} \cap \Gamma(f)$ es una cara del poliedro. De lo

anterior se tiene

$$m(a) = \min_{\omega \in supp(f)} \{a \cdot \omega\} = \min_{x \text{ vértice de } \Gamma(f)} \{a \cdot x\}.$$

□

2.3. PARTICIÓN CÓNICA DE $(\mathbb{R}^+)^n$

Definición 27 *Sea $f \in R[x_1, \cdots, x_n]$ tal que $f(0) = 0$ y $a \in (\mathbb{R}^+)^n$. Se define el* **primer lugar de encuentro de a** *como el conjunto*

$$F(a) := \{x \in \Gamma(f) | a \cdot x = m(a)\} \text{ y } m(a) := \inf_{y \in \Gamma(f)} \{a \cdot y\}.$$

Corolario 5 *Sea $a \in (\mathbb{R}^+)^n$ entonces $F(a)$ es es una cara de $\Gamma(f)$. En particular, $F(0) = \Gamma(f)$ y $F(a)$ es una cara propia de de $\Gamma(f)$, si $a \neq 0$.*

$Demostración.$ Válido a partir del Lema 5. □

Definición 28 *Un vector de $\mathbb{R}^n$ se dice primitivo si sus componentes son enteros primos relativos entre sí.*

Definición 29 *Se define el cono asociado a τ, para τ cara de $\Gamma(f)$, como:*

$$\Delta_\tau := \{a \in (\mathbb{R}^+)^n | F(a) = \tau\}.$$

Note que $\Delta_{\Gamma(f)} = \{0\}$.

Definición 30 *Dados los vectores $v_1, \ldots, v_p \in \mathbb{R}^n$ y los escalares $c_1, \ldots, c_p$, una combinación afín es una combinación lineal $c_1 v_1 + \cdots + c_p v_p$, tal que $c_1 + \cdots + c_p = 1$.*
El conjunto de todas las combinaciones afines de puntos de un conjunto S es ***la envolvente afín*** *de S y se denota como aff(S).*

Definición 31 *El **interior relativo** de un conjunto convexo C en $\mathbb{R}^n$, que se denota ri(C), es definido como el interior cuando C es considerado como un subconjunto de su aff(C).*

Teorema 10 *Sea $C = conv(S)$, donde S es un conjunto de puntos y direcciones, y sea C' una cara no vacía de C. Entonces $C' = conv(S')$, donde S' consiste de los puntos en S que perteneces a C' y las direcciones en S que son direcciones de recesión de C'.*

Lema 6 *Sea $f(x) = f(x_1, \ldots, x_n) = \sum_{\omega \in \mathbb{N}^n} a_\omega x^\omega$ un polinomio no nulo sobre $\mathbb{Z}_p$ con $f(0) = 0$ y τ una cara propia de $\Gamma(f)$, entonces:*

i) Δ_τ es un subconjunto relativamente abierto de $(\mathbb{R}^+)^n$;

ii) $\bar{\Delta}_\tau = \{a \in (\mathbb{R}^+)^n | \tau \subset F(a)\}$ y es un **cono poliédrico***;*

iii) La función m definida anteriormente es lineal sobre $\bar{\Delta}_\tau$.

$Demostración$. Suponga que $\Gamma(f)$ es la envolvente convexa de los puntos $P_1, \ldots, P_s$ y las direcciones de recesión $e_1, \ldots e_n$ donde $\{e_1, \ldots e_n\}$ es la base estándar de $\mathbb{R}^n$. Por el Teorema 10 se puede suponer que τ es la envolvente convexa de los puntos $\{P_1, \ldots, P_r\} = \tau \cap \{P_1, \ldots, P_r, P_{r+1}, \ldots, P_s\}$ y las direcciones de recesión $e_1, \ldots e_k$ con $r \leq s$ y $k \leq n$. Ahora se puede probar que

$$\begin{aligned}\Delta_\tau = \{a \in \mathbb{R}^n | & a \cdot P_1 = \cdots = a \cdot P_r,\ a \cdot P_1 < a \cdot P_{r+1}, \ldots, \\ & a \cdot P_1 < a \cdot P_s,\ a_i = 0 \text{ para } i = 1, \ldots, k, \\ & a_j > 0 \text{ para } j = k+1, \ldots, n\}.\end{aligned}$$

que es claramente un conjunto relativamente abierto. Se sigue que

$$\begin{aligned}\bar{\Delta}_\tau =& \{a \in \mathbb{R}^n | a \cdot P_1 = \cdots = a \cdot P_r,\ a \cdot P_1 \leq a \cdot P_{r+1}, \ldots, \\ & a \cdot P_1 \leq a \cdot P_s,\ a_i = 0 \text{ para } i = 1, \ldots, k, \\ & a_j > 0 \text{ para } j = k+1, \ldots, n\}, \\ =& \{a \in (\mathbb{R}^+)^n | \tau \subset F(a)\}.\end{aligned}$$

Finalmente, (ii) implica que $m(a) = a \cdot x_\tau$ para todo $a \in \bar{\Delta}_\tau$, donde x_τ es un elemento fijo de τ. Esto muestra que m es lineal sobre $\bar{\Delta}_\tau$. □

Definición 32 *Sea τ una cara de β, se dice que τ es una* **careta** *de β si* $\dim(\tau) = \dim(\beta) - 1$.

Cuando $\beta = \Gamma(f)$, solo se dirá que τ es una careta.

Lema 7 *Dado $\Gamma(f)$ se cumple*

i) Si H es un hiperplano soporte del Poliedro de Newton $\Gamma(f)$ y $a \in \mathbb{R}^n \setminus \{0\}$ es perpendicular a H, entonces a ó $-a \in (\mathbb{R}^+)^n$.

ii) Si τ es una careta, entonces existe $a \in \mathbb{N}^n \setminus \{0\}$ perpendicular a τ.

$Demostración.$

i) Sea $a \in \mathbb{R}^n \setminus \{0\}$, perpendicular a H, entonces existe $\beta \in \mathbb{R}$ tal que $H = \{x \in \mathbb{R}^n | a \cdot x = \beta\}$. Suponga que existen $i, j \in \{1, \cdots, n\}$ tal que $a_i < 0$ y $a_j > 0$. Sea $P \in H \cap \Gamma(f)$. Sean e_i, e_j (vectores canónicos de $\mathbb{R}^n$), las direcciones de recesión de $\Gamma(f)$, tales que los puntos $P + e_i$ y $P + e_j$ están en $\Gamma(f)$, pero $(P + e_i) \cdot a = \beta + a_i < \beta$ y $(P + e_j) \cdot a = \beta + a_j > \beta$, lo cual contradice el hecho de que H es un hiperplano soporte de $\Gamma(f)$.

ii) Se sabe que τ es la envolvente convexa del conjunto S, donde $S \subset supp(f)$ que están en τ y la dirección de recesión de τ en el conjunto $\{e_1, \cdots, e_n\}$. Dado que τ es una careta, se puede suponer que el hiperplano soporte H de $\Gamma(f)$, que satisface $\tau = H \cap \Gamma(f)$, es la envolvente afín de $\{t_1, \cdots, t_n\}$, donde $t_1, \cdots, t_n$, son vectores independientes afines en $\mathbb{N}^n \cap \tau$. Por lo tanto existe $a \in \mathbb{Z}^n \setminus \{0\}$ que es perpendicular a H. Por $i)$, se puede suponer que $a \in \mathbb{N}^n \setminus \{0\}$.

□

Lema 8 *Sea τ cara propia de $\Gamma(f)$ y $\gamma_1, \ldots, \gamma_e$ caras $(n-1)-$dimensionales de $\Gamma(f)$ que la contienen. Sean $a_1, \ldots, a_e$ los únicos vectores primitivos perpendiculares a $\gamma_1, \ldots, \gamma_e$ respectivamente.*
Se tiene que:

$$\Delta_\tau = \{\lambda_1 a_1 + \cdots + \lambda_e a_e | \lambda_i \in \mathbb{R}, \lambda_i > 0\},$$

con $\dim \Delta_\tau = n - \dim \tau$.

Definición 33 *Sea $a_1, \ldots, a_e \in \mathbb{R}^n \setminus \{0\}$, se define el conjunto*

$$\Delta = \left\{\lambda_1 a_1 + \cdots + \lambda_e a_e | \lambda_i \in \mathbb{R}^+ \setminus \{0\}, i = 1, 2, \ldots, e\right\},$$

como el cono **generado estrictamente positivo por los vectores** $a_1, \ldots, a_e$.
Si $a_1, \ldots, a_e$ son linealmente independientes sobre $\mathbb{R}$, se dirá que Δ es un **cono simplicial**. *Si además $a_1, \ldots, a_e \in \mathbb{Z}^n$, se dice que Δ es un* **cono simplicial racional**.
Si $\{a_1, \ldots, a_e\}$ es un subconjunto de una base de $\mathbb{Z}-$ módulo $\mathbb{Z}^n$, entonces Δ será un **cono simple**.

Lema 9 *Sea Δ un cono generado estrictamente positivo por los vectores $a_1, \ldots, a_e \in \mathbb{R}^n \setminus \{0\}$. Existe una partición finita de Δ en conos Δ_i tal que cada cono es generado estrictamente positivo por un subconjunto de vectores linealmente independientes*

de $\{a_1, \ldots, a_e\}$*. Además, si* Δ *es un cono simplicial racional, entonces existe una partición en conos simples.*

$Demostración$. Sea $\bar{\Delta}$ la clausura de Δ. Así $\bar{\Delta}$ es un cono poliédrico convexo cerrado. Si γ es un cono convexo cerrado, se denota el interior relativo de γ por, $ri\gamma$ (i.e. el interior en el espacio lineal generado por γ). La demostración es por inducción sobre $dim(\mathbb{R}a_1 + \cdots + \mathbb{R}a_r)$.
Se puede suponer que $\mathbb{R}^+a_1$ es una cara de $\bar{\Delta}$. Es posible ver que Δ es la unión disjunta de conos de la forma

$$W = \{\lambda_1 a_1 + b |\ \lambda_1 \in \mathbb{R}, \lambda_1 > 0,\ b \in ri(\gamma)\},$$

donde γ es una cara propia de $\bar{\Delta}$ tal que W no está contenido en una careta de $\bar{\Delta}$. Por inducción, se tiene que $ri(\gamma)$ es la unión disjunta de conos w_i con la propiedad requerida. Por lo tanto, W es la unión disjunta de conos

$$W_i = \{\lambda_1 a_1 + b | \lambda_1 \in \mathbb{R}, \lambda_1 > 0, b \in w_i\}.$$

□

Ejemplo 13

Como en el ejemplo 11, considere $f(x, y) = 2x^3y^2 + y^5 + x^4 - 2xy^3 - 2x^2y + y^2$ se calculará los vectores primitivos perpendiculares a cada cara:

$$\tau_2 = \{(1-\lambda)(0,2) + \lambda(1,0) |\ 0 < \lambda < 1\} \to a_2 = (1,2),$$

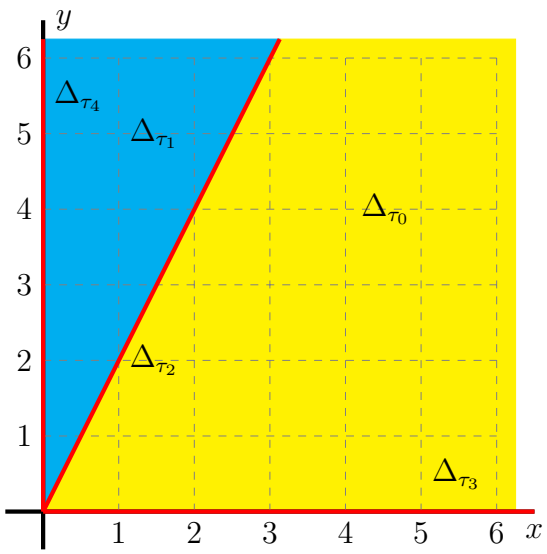
$$\tau_3 = \{(0,2) + \mathbb{R}^+(0,1)\} \to a_3 = (1,0),$$

$$\tau_4 = \{(4,0) + \mathbb{R}^+(1,0)\} \to a_3 = (0,1).$$

Luego, utilizando el Lema 8, se tiene:

$$\Delta_{\tau_0} = \mathbb{R}_{>0}(1,2) + \mathbb{R}_{>0}(1,0),$$
$$\Delta_{\tau_1} = \mathbb{R}_{>0}(1,2) + \mathbb{R}_{>0}(0,1),$$
$$\Delta_{\tau_2} = \mathbb{R}_{>0}(1,2),$$
$$\Delta_{\tau_3} = \mathbb{R}_{>0}(1,0),$$
$$\Delta_{\tau_4} = \mathbb{R}_{>0}(0,1).$$

Figura 4. Partición cónica $(\mathbb{R}^+)^2$.



Puesto que los vectores $\{(1,2),(1,0)\}$ no forman una base de $\mathbb{Z} - módulo\ Z^2$, dado que $(1,1) \notin gen\{(1,2),(1,0)\}$, por el Lema 9, se tiene:

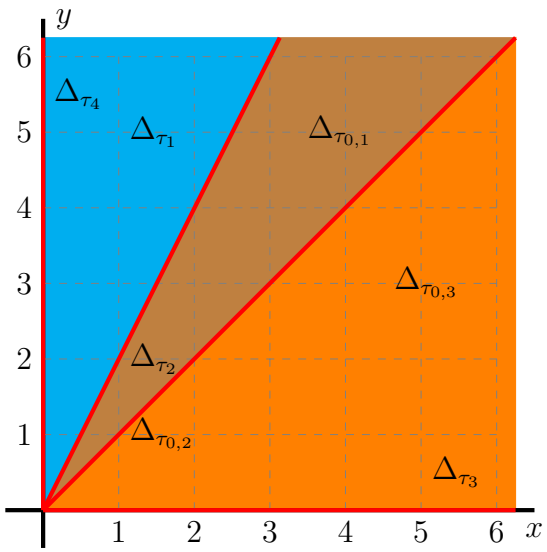
$$\Delta_{\tau_0} = \Delta_{\tau_{0,1}} \cup \Delta_{\tau_{0,2}} \cup \Delta_{\tau_{0,3}},$$

donde:

$$\Delta_{\tau_{0,1}} = \mathbb{R}_{>0}(1,2) + \mathbb{R}_{>0}(1,1),$$
$$\Delta_{\tau_{0,2}} = \mathbb{R}_{>0}(1,1),$$
$$\Delta_{\tau_{0,3}} = \mathbb{R}_{>0}(1,1) + \mathbb{R}_{>0}(1,0).$$

Así,

Figura 5. subdivisión cónica simple.



Ejemplo 14 *Partición cónica y subdivisión cónica del ejemplo 12*

Cono	*Generadores*
$\Delta_{\tau_{0,1}}$	$\mathbb{R}_{>0}(3,2)+\mathbb{R}_{>0}(2,1)$
$\Delta_{\tau_{0,2}}$	$\mathbb{R}_{>0}(2,1)$
$\Delta_{\tau_{0,3}}$	$\mathbb{R}_{>0}(2,1)+\mathbb{R}_{>0}(1,0)$
$\Delta_{\tau_{1,1}}$	$\mathbb{R}_{>0}(0,1)+\mathbb{R}_{>0}(1,1)$
$\Delta_{\tau_{1,2}}$	$\mathbb{R}_{>0}(1,1)$
$\Delta_{\tau_{1,3}}$	$\mathbb{R}_{>0}(1,1)+\mathbb{R}_{>0}(3,2)$
Δ_{τ_2}	$\mathbb{R}_{>0}(3,2)$
Δ_{τ_3}	$\mathbb{R}_{>0}(1,0)$
Δ_{τ_4}	$\mathbb{R}_{>0}(0,1)$

Figura 6. Partición cónica $(\mathbb{R}^+)^2$.

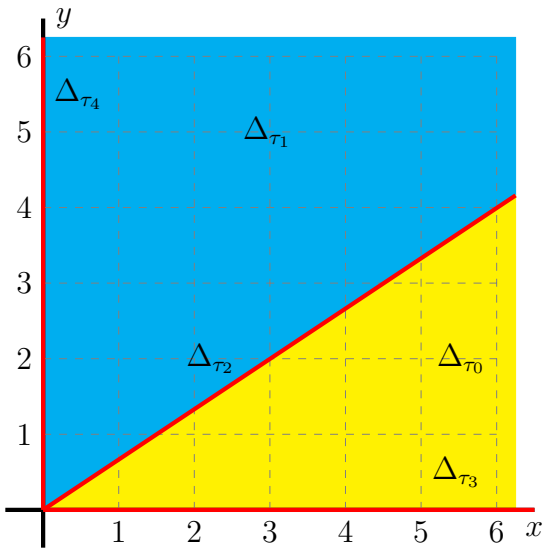
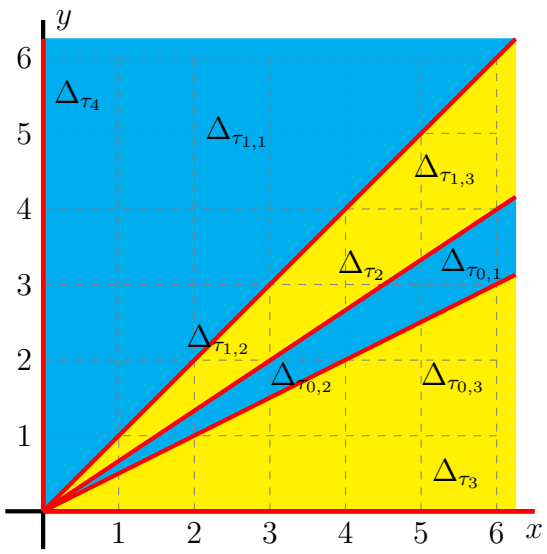


Figura 7. Subdivisión cónica simple.



Definición 34 *Sean $a_1, \ldots, a_r$ vectores en $\mathbb{Z}^n$ linealmente independientes sobre $\mathbb{Q}$. Se define la multiplicidad de $a_1, \ldots, a_r$ como el índice del retículo $\mathbb{Z}a_1 + \cdots + \mathbb{Z}a_r$ en el grupo de los puntos con coordenadas enteras del espacio vectorial generado por $a_1, \ldots, a_r$.*

Proposición 13 *Sean $a_1, \ldots, a_r \in \mathbb{Z}^n$ linealmente independientes sobre $\mathbb{R}$. se tiene:*

1. *La multiplicidad de $a_1, \ldots, a_r$ es igual al número de elementos del conjunto*

$$\left\{ \sum_{i=1}^{r} \lambda_i a_i | 0 \leq \lambda_i < 1 \right\} \cap \mathbb{Z}^n.$$

2. *La multiplicidad de $a_1, \ldots, a_r$ es igual al máximo común divisor de los determinantes de todas las matrices $r \times r$ obtenidas al omitir columnas de la matriz con filas $a_1, \ldots, a_r$.*

3. FUNCIÓN ZETA LOCAL DE IGUSA

3.1. LEMA DE HENSEL

Se construirá una sucesión $\{a_n\}$ de números $5-$ádica tal que:

$$\sqrt{6} = \sum_{i=0}^{\infty} a_i 5^i,$$

es decir $\sqrt{6} \in \mathbb{Q}_5$. Si esto se tiene, entonces

$$(a_0 + a_1 5 + a_2 5^2 + \cdots)^2 = 1 + (1)5. \tag{8}$$

De (8) se tiene $a_0^2 \equiv 1(\mod 5)$, eso implica que $a_0 = 1$ ó $a_0 = 4$.
Si $a_0 = 1$, entonces:

$$(2a_1)5 \equiv (1)5 \mod 5^2 \text{ entonces } 2a_1 \equiv 1 \mod 5, \text{ por lo tanto } a_1 = 3.$$

En el siguiente paso se tiene:

$$1 + (1)5 \equiv (1 + (3)5 + a_2 5^2)^2 \equiv 1 + (1)5 + (2a_2)5^2 \mod 5^3,$$

lo cual implica $2a_2 \equiv 0 \mod 5$, por lo tanto $a_2 = 0$. Entonces, se obtiene la siguiente serie:

$$\sqrt{6} = 1 + (3)5 + (0)5^2 + \cdots,$$

donde cada a_i con $i \geq 0$, se determina de forma única. Si $a_0 = 4$, se obtiene la solución:

$$-\sqrt{6} = 4 + (1)5 + (4)5^2 + (0)5^3 + \cdots.$$

El método anterior para resolver ecuaciones se puede generalizar usando el siguiente Lema.

Teorema 11 (Lema de Hensel) *Sea* $F(x) = c_0 + c_1 x + \cdots + c_n x^n$ *un polinomio cuyos coeficientes son enteros p-ádicos y*

$$F'(x) = c_1 + 2c_2 x + 3c_3 x^2 + \cdots + n c_n x^{n-1},$$

la derivada de $F(x)$*; suponga* $\bar{a}_0$ *un entero p-ádico que satisface* $F(\bar{a}_0) \equiv 0 \mod p$ *y* $F'(\bar{a}_0) \not\equiv 0 \mod p$*, entonces existe un único entero p-ádico* α *tal que* $F(\alpha) = 0$ *y* $\alpha \equiv \bar{a}_0 \mod p$.

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

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

con $b_i \in \{0, 1, \ldots, p-1\} \forall i$, tal que $F(a_k) \equiv 0 \mod p^{k+1}$ y $a_k \equiv \bar{a}_0 \mod p$.

1. Para $k = 0$ basta con tomar b_0 igual al primer dígito p-ádico de $\bar{a}_0$, luego se tiene $F(a_0) \equiv 0 \mod p$ y $a_0 \equiv \bar{a}_0 \mod p$.

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

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

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

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

para algún entero $\lambda_k \in \{0, 1, \ldots, p-1\}$.

Luego, se busca que se cumpla $\lambda_k + b_k F'(a_{k-1}) \equiv 0 \mod p$, dado $a_{k-1} \equiv \bar{a}_0 \mod p$ entonces, $F'(a_{k-1}) \equiv F'(\bar{a}_0) \not\equiv 0 \mod p$, entonces $\lambda_k + b_k F'(a_{k-1}) \equiv 0 \mod p$ esto implica $b_k \equiv \dfrac{-\lambda_k}{F'(a_{k-1})} \mod p$. Así, $F(a_k) \equiv 0 \mod p^{k+1}$. Completando el proceso de inducción.

Ahora, sea

$$\alpha = b_0 + b_1 p + b_2 p^2 + \cdots,$$

se tiene que $F(\alpha) = 0$, dado que para todo k se cumple $F(\alpha) \equiv F(a_k) \equiv 0 \mod p^{k+1}$.

La unicidad de α se sigue de la unicidad de la sucesión $\{a_k\}$.

□

A continuación algunas consecuencias del Lema de Hensel.

Proposición 14 *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 $\{a_k\}$ donde

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

tal que

$$a \equiv a_k \mod p^k,$$

entonces $F(a_k) \equiv F(a) \mod p^k$ y $F(a) = 0$. Luego

$$F(a_k) \equiv 0 \mod p^k.$$

Recíprocamente, suponga que $F(x) \equiv 0 \mod p^k$ tiene una solución a_k para cualquier $k \geq 1$. Dado que $\mathbb{Z}_p$ es compacto entonces la sucesión $\{a_k\}$ contiene una subsucesion $\{a_{k_i}\}$ convergente. Si $a = \lim_{i \to \infty} a_{k_i}$.
$F(x)$ es continua por ser un polinomio, entonces

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

Por otro lado,

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

Así,

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

y por tanto, $F(a) = 0$. □

Proposición 15 *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 $x^2 \equiv a \mod p$ tiene solución, es decir, a es un residuo cuadrático módulo p.
Recíprocamente, si a es un residuo cuadrático módulo p, entonces $a \equiv a_0^2 \mod p$, para algún $a_0 \in \{1, 2, \ldots, p-1\}$ entonces $P(a) \equiv 0 \mod p$. Como $P'(a) = 2a \not\equiv 0 \mod p$, por el Lema de Hensel existe $a_0 \in \mathbb{Z}_p$ tal que $a_0^2 - a = 0$, es decir, $a_0^2 = a$. □

Proposición 16 *Considere $f(x) \in \mathbb{Z}_p[x], k \in \mathbb{N} \setminus \{0\}$. Sea $a \in \mathbb{Z}_p$ tal que $f(a) \equiv 0 \mod p$ y $f'(a) \not\equiv 0 \mod p$. Entonces existe $\xi \in \mathbb{Z}_p$ tal que*

$$\xi + p^k\mathbb{Z}_p = \{x \in a + p\mathbb{Z}_p : f(x) \equiv 0 \mod p^k\}.$$

Demostración. Por el Lema de Hensel, se tiene que existe un único $\xi \in \mathbb{Z}_p$ tal que $f(\xi) = 0$ y $\xi \equiv a \mod p$. Para la inclusión $\subset$, sea $x \in \xi + p^k\mathbb{Z}_p$, entonces $x \equiv \xi \mod p^k$, lo cual implica que $x \equiv \xi \equiv a \mod p$ y $f(x) \equiv f(\xi) \equiv 0 \mod p^k$. Para la segunda inclusión, sea $x \in a + p\mathbb{Z}_p$ y suponga $f(x) \equiv 0 \mod p^k$. Dado que $x \equiv a \mod p$, se tiene que $f'(x) \equiv f'(a) \not\equiv 0 \mod p$, se sigue del Lema de Hensel que existe un único $\eta \in \mathbb{Z}_p$ tal que $f(\eta) = 0$ y $\eta \equiv x \mod p^k$. Además, $\eta \equiv x \equiv a (\mod p)$ y por la unicidad de η se tiene que $\eta = \xi$, en consecuencia, $x \equiv \xi \mod p^k$. □

Lema 10 *Sea $f(x) = f(x_1, \cdots, x_n) \in \mathbb{Z}_p[x_1, \cdots, x_n]$ y $k \in \mathbb{N} \setminus \{0\}$. Suponga $a = (a_1, \ldots, a_n) \in \mathbb{Z}_p^n$, tal que $f(a) \equiv 0 \mod p$ y $\frac{\partial f}{\partial x_1}(a) \not\equiv 0 \mod p$. Sea $c_2, \ldots, c_n \in \mathbb{Z}_p$ con $c_i \equiv a_i \mod p$ para $i = 2, \ldots, n$, entonces existe $c_1 \in \mathbb{Z}_p$, tal que para todo $x_2, \ldots, x_n \in \mathbb{Z}_p$ satisface que $x_i \equiv c_i \mod p^k$, para $i = 2, \ldots, n$ y se tiene que*

$$c_1 + p^k\mathbb{Z}_p = \{x_1 \in a_1 + p\mathbb{Z}_p : f(x_1, \ldots, x_n) \equiv 0 \mod p^k\}.$$

Esto implica que el conjunto

$$\{(x_1, \ldots, x_n) \in a + (p\mathbb{Z}_p)^n : f(x_1, \ldots, x_n) \equiv 0 \mod p^k\}$$

$$= \bigcup (c_1, c_2, \ldots, c_n) + (p\mathbb{Z}_p)^n,$$

donde la unión es tomada sobre todas las $(n-1)$ *tuplas* $(c_2 + p^k\mathbb{Z}_p, \ldots, c_n + p^k\mathbb{Z}_p)$ *con* $c_i \equiv a_i \mod p$*, para cada* $i = 2, \ldots, n$*.*

$Demostración$. El resultado se sigue de la Proposición 16, dado que $f(x_1, x_2, \ldots, x_n) \equiv f(x_1, c_2, \ldots, c_n) \mod p^k$ para cada $x_2, \ldots, x_n \in \mathbb{Z}_p$ con $x_i \equiv c_i \mod p^k$, $f(a_1, c_2, \ldots, c_n) \equiv f(a_1, a_2, \ldots, a_n) \equiv 0 \mod p$ y $\frac{\partial f}{\partial x_1}(a_1, c_e, \ldots, c_n) \equiv \frac{\partial f}{\partial x_1}(a_1, a_2, \ldots, a_n) \not\equiv 0 \mod p$. $\square$

3.2. FUNCIÓN ZETA LOCAL

Sea K un cuerpo local no-Arquimediano de característica arbitraria con valuación v, donde $v(\mathfrak{p}) = 1$, fijando un parámetro uniformizador $\mathfrak{p}$ de O_K. Sea O_K su anillo de enteros y su grupo de unidades $O_K^\times$. Suponga que el cuerpo residual de O_k es $\mathbb{F}_q$, un cuerpo finito con q elementos. La norma para K está definida por $|z|_k = q^{-v(z)}, z \in K$, se define la componente angular de z por $ac(z) = z\mathfrak{p}^{-v(x)}$. Sea $f(x) = f(x_1, \cdots, x_n) \in O_K[x_1, \cdots, x_n]$, un polinomio no constante y χ un caracter de $O_K^\times$. Se define la función zeta local como

$$Z(s, f, \chi) := \int_{O_k^n} \chi(ac(f(x)))|f(x)|_k^s |dx|, \ s \in \mathbb{C},$$

donde $Re(s) > 0$, y $|dx|$ denota la medida de Haar de $(K^n, +)$ normalizada tal que O_k^n tiene medida 1.

En el caso, $K = \mathbb{Q}_p$ y χ es el caracter trivial, se tiene

$$Z(s, f, \chi) = Z(s, f) = \int_{\mathbb{Z}_p^n} |f(x)|_p^s |dx|. \tag{9}$$

Proposición 17 *La integral (9) converge para* $Re(s) > 0$.

$Demostración.$ Sea $s = \alpha + i\beta, \alpha, \beta \in \mathbb{R}$. Se tiene que

$$\begin{aligned}\int_{\mathbb{Z}_p^n} |f(x)|_p^{\alpha}\, |dx| &= \int\limits_{\bigcup_{m=0}^{\infty} f^{-1}(p^m\mathbb{Z}_p \setminus p^{m+1}\mathbb{Z}_p)} |f(x)|_p^{\alpha}\, |dx|, \\ &= \sum_{m=0}^{\infty} p^{-m\alpha} \cdot \text{ medida de } \{f^{-1}(p^m\mathbb{Z}_p \setminus p^{m+1}\mathbb{Z}_p)\},\end{aligned}$$

pero, la medida de $\{f^{-1}(p^m\mathbb{Z}_p)\} \leq p^{-m(n+1)} \leq 1$, luego

$$\sum_{m=0}^{\infty} p^{-m\alpha} \cdot \text{ medida de } \{f^{-1}(p^m\mathbb{Z}_p \setminus p^{m+1}\mathbb{Z}_p)\} \leq \sum_{m=0}^{\infty} (p^{-\alpha})^m,$$

suma que converge para $\alpha > 0$. □

Ahora se verán las propiedades analíticas de $Z(s, f)$. Para esto se usará un criterio que implica que una función definida por una integral en un grupo topológico localmente compacto es analítica.

Sea G un grupo topólogico localmente compacto con medida de Haar dx. Sea $D \subseteq \mathbb{C}$ una región y sea $h : G \times D \to \mathbb{C}$ una función continua tal que:

1) Para $x \in G$ fijo, $h(x, s)$ es una función analítica en D;

2) Para $s \in D$ fijo, $h(x, s)$ y $h_s(x, s)$ son integrables respecto a dx, donde $h_s(x, s)$ denota la derivada de $h(x, s)$ respecto a s.

Se define

$$g(s) := \int_G h(x,s)|dx|, \quad s \in D. \tag{10}$$

Definición 35 *Sean G, D y h como se definió anteriormente. Si $E \subseteq D$ entonces se dice que (10) converge uniformemente en E si, dado $\epsilon > 0$, existe un conjunto compacto $C = C(\epsilon, E)$, tal que*

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

para todo $s \in E$. (10) converge uniformemente en subconjuntos compactos de D si ésta converge uniformemente en todo subconjunto compacto de D.

Entonces se tiene el siguiente resultado:

Teorema 12 *Sean h, g, G y D como se definieron antes. Si*

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

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

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

Para $h(x,s) = Z(s,f)$, solo resta verificar la convergencia uniforme en subconjuntos compactos del semiplano $Re(s) > 0$. Así si $\delta > 0$, es suficiente ver que la integral

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

converge uniformemente para $Re(s) \geq \delta > 0$. Puesto que

$$\left| \int_{\mathbb{Z}_p^n} |f(x)|_p^s |dx| \right| \leq \frac{1}{1 - p^{-\alpha}};$$

Si $l > 0$ es un entero que satisface

$$\frac{1 - p^{l(n+\delta)}}{1 - p^{-\delta}} < \epsilon,$$

entonces

$$\left| \int_{\mathbb{Z}_p^n \setminus (p^l \mathbb{Z}_p)^n} |f(x)|_p^s |dx| \right| < \epsilon,$$

y claramente $(p^l \mathbb{Z}_p)^n$ es compacto, por lo tanto se tiene que

Teorema 13 *$Z(s, f)$ es una función analítica para $Re(s) > 0$.*

Existe una relación entre la serie de Poincaré de f y la función zeta local de Igusa asociada a f.

Definición 36 *Sea $f(x) = f(x_1, \ldots, x_n) \in \mathbb{Z}_p[x_1, \ldots, x_n]$ con p primo. Se define la serie de Poincaré de f como la serie de potencias*

$$P(t) := \sum_{e=0}^{\infty} N_e p^{-ne} t^e,$$

donde N_e es el número de elementos del conjunto

$$\{x + p^e \mathbb{Z}_p^n | x \in \mathbb{Z}_p^n \ y \ f(x) \equiv 0 \mod p^e\},$$

para $e \geq 1$ y $N_0 = 1$.

Lema 11 *Sea $f(x) = f(x_1, \ldots, x_n) \in \mathbb{Z}_p[x_1, \ldots, x_n]$, $p-$primo y $t = p^{-s}$ con $s \in \mathbb{C}, Re(s) > 0$. Entonces*

$$Z(s, f) = P(t) - \frac{P(t) - 1}{t}.$$

$Demostración$. Puesto que la función zeta local de Igusa asociada a f se puede

escribir

$$\begin{aligned} Z(s,f) &= \int_{\mathbb{Z}_p^n} |f(x)|_p^s \, |dx|, \\ &= \sum_{e=0}^{\infty} \int_{\{x \in \mathbb{Z}_p^n |\ \mathsf{ord}(f(x))=e\}} |f(x)|_p^s \, |dx|, \\ &= \sum_{e=0}^{\infty} p^{-es} \cdot \text{ medida de } \{x \in \mathbb{Z}_p^n |\ \mathsf{ord}(f(x)) = e\}. \end{aligned}$$

Por lo tanto

medida de $\{x \in \mathbb{Z}_p^n |\ \mathsf{ord}(f(x)) = e\}$

$=$ medida de $(\{x \in \mathbb{Z}_p^n |\ f(x) \equiv 0 \mod p^e\} \setminus \{x \in \mathbb{Z}_p^n |\ f(x) \equiv 0 \mod p^{e+1}\})$

$=$ medida de $\{x \in \mathbb{Z}_p^n |\ f(x) \equiv 0 \mod p^e\}$ $-$ medida de $\{x \in \mathbb{Z}_p^n |\ f(x) \equiv 0 \mod p^{e+1}\}$

$$= \text{medida de } \left\{ \bigcup_{\substack{a \in \{0,1,\ldots,p^e-1\}^n \\ f(a) \equiv 0 \mod p^e}} a + p^e \mathbb{Z}_p^n \right\}$$

$$- \text{ medida de } \left\{ \bigcup_{\substack{a \in \{0,1,\ldots,p^{e+1}-1\}^n \\ f(a) \equiv 0 \mod p^{e+1}}} a + p^{e+1} \mathbb{Z}_p^n \right\}$$

$= N_e p^{-en} - N_{e+1} p^{-(e+1)n}.$

Así,

$$\begin{aligned} Z(s,f) &= \sum_{e=0}^{\infty} p^{-es}\left(N_e p^{-en} - N_{e+1}p^{-(e+1)n}\right), \\ &= \sum_{e=0}^{\infty} N_e p^{-en}(p^{-s})^e - \sum_{e=0}^{\infty} N_{e+1}p^{-n(e+1)}(p^{-s})^e, \\ &= P(t) - \frac{P(t)-1}{t}. \end{aligned}$$

Lema 12 (Igusa) *Sea $f(x)$ un polinomio no constante en $\mathbb{Q}_p[x_1,\ldots,x_n]$, entonces existe un número finito de pares $(N_E, v_E) \in (\mathbb{N}\setminus\{0\})\times(\mathbb{N}\setminus\{0\}), E \in T$, tal que*

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

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

$Demostración$: La demostración requiere de algunos temas de geometría algebraica, que involucra el Teorema de resolución de singularidades de Hironaka que están fuera del alcance de este trabajo, ver [9] Teorema 8.2.1.

Corolario 6 *$P(t)$ es una función racional de t.*

La racionalidad de $P(t)$ fue conjeturada en los años sesenta por Borevich y Shafarevich. Igusa demostró este resultado a mediados de los setenta. La racionalidad de $Z(s,f)$ también permite encontrar el límite de N_e.

Ejemplo 15

$$Z(s) = \int_{\mathbb{Z}_p} |x|_p^s \, dx, s \in \mathbb{C},\ \textit{Re}(s) > -1.$$

---

9 J. IGUSA. *An introduction to the theory of local zeta functions*. Algebraic Geometry e its Applications,AMS/IP Studies in Advanced Mathe,atics, 2000.

$$
\begin{aligned}
Z(s) &= \int_{\mathbb{Z}_p\setminus\{0\}} |x|_p^s = \sum_{j=0}^{\infty} \int_{S_{-j}(0)} |x|_p^s \, dx = \sum_{j=0}^{\infty} p^{-js} \int_{S_{-j}(0)} dx, \\
&= \sum_{j=0}^{\infty} p^{-js} p^{-j}(1-p^{-1}) = (1-p^{-1}) \sum_{j=0}^{\infty} p^{-j(s+1)}, \\
&= \frac{1-p^{-1}}{1-p^{-1-s}}, \ \textit{Re}(s) > -1.
\end{aligned}
$$

Proposición 18 *Sea $f(x) = f(x_1, \cdots, x_n) \in \mathbb{Z}_p[x_1, \cdots, x_n]$ y $a \in \mathbb{Z}_p^n$. Suponga que el conjunto de congruencias*

$$
\begin{cases}
f(x) & \equiv 0 \ \textit{mód} \ p \\
\frac{\partial f}{\partial x_i}(x) & \equiv 0 \ \textit{mód} \ p, \ i = 1, 2, \cdots, n
\end{cases}
$$

no tiene solución en la clase $a + (p\mathbb{Z}_p)^n$, entonces para $s \in \mathbb{C}$ con $Re(s) > 0$ se tiene:

$$
\int_{a+(p\mathbb{Z}_p)^n} |f(x)|_p^s |dx| = \begin{cases}
p^{-n} & si \ f(a) \not\equiv 0 \mod p \\
p^{-n}(p-1)\frac{p^{-(s+1)}}{1-p^{-(s+1)}} & si \ f(a) \equiv 0 \mod p.
\end{cases}
$$

Demostración. **Caso 1.** $f(a) \not\equiv 0 \mod p$. Para cada $x \in a + (p\mathbb{Z}_p)^n$, se tiene que $f(x) \equiv f(a) \not\equiv 0 \mod p$. De ahí que $ord(f(x) = 0)$ y $|f(x)|^s = 1$ para cada $x \in a + (p\mathbb{Z}_p)^n$, por lo tanto,

$$
\int_{a+(p\mathbb{Z}_p)^n} |f(x)|_p^s |dx| = \int_{a+(p\mathbb{Z}_p)^n} 1 \, |dx| = p^{-n}.
$$

Caso 2. $f(a) \equiv 0 \mod p$, para cada $x \in a + (p\mathbb{Z}_p)^n$ se tiene que $f(x) \equiv f(a) \equiv 0 \mod p$, de donde se obtiene que $ord(f(x)) \geq 1$ para cada $x \in a + (p\mathbb{Z}_p)^n$. Por lo

anterior,

$$\int_{a+(p\mathbb{Z}_p)^n} |f(x)|_p^s|dx| = \sum_{k=1}^{\infty} \int_{x\in a+(p\mathbb{Z}_p)^n \ ord(f(x))=k} |f(x)|_p^s|dx|,$$

$$= \sum_{k=1}^{\infty} p^{-ks} \cdot \text{medida de } \{x \in a+(p\mathbb{Z}_p)^n \ : ord(f(x)) = k\}.$$

La medida de $\{x \in a+(p\mathbb{Z}_p)^n : ord(f(x)) = k\} = p^{-k-n+1} - p^{-k-n}$, en efecto, puesto que el conjunto de la igualdad de arriba es igual al complemento de $\{x \in a+(p\mathbb{Z}_p)^n : f(x) \equiv 0 \mod p^{k+1}\}$ en $\{x \in a+(p\mathbb{Z}_p)^n : f(x) \equiv 0 \mod p^k\}$, la aditividad de la medida implica que es suficiente probar que la medida de $\{x \in a+(p\mathbb{Z}_p)^n : f(x) \equiv 0 \mod p^k\}$ es igual a p^{-k-n+1} para $k \in \mathbb{N} \setminus \{0\}$. Por hipótesis y el hecho que $f(a) \equiv 0 \mod p$ se sigue que existe $i \in \{1, 2, \ldots, n\}$ tales que $\frac{\partial f}{\partial x_i}(a) \not\equiv 0 \mod p$. Sin pérdida de generalidad se puede suponer que $\frac{\partial f}{\partial x_1}(a) \not\equiv 0 \mod p$, entonces por el Lema 10, se tiene que el conjunto $\{x \in a+(p\mathbb{Z}_p)^n : f(x) \equiv 0 \mod p^k\}$ es igual a $\bigcup(c_1, c_2, \ldots, c_n)+(p\mathbb{Z}_p)^n$, donde c_1 es como en el Lema 10 y la unión es tomada sobre todas las $(n-1)$ tuplas $(c_2+p^k\mathbb{Z}_p, \ldots, c_n+p^k\mathbb{Z}_p)$ con $c_i \equiv a \mod p$, para $i = 2, 3, \ldots, n$, esta unión es disjunta y la medida de $c + (p^k\mathbb{Z}_p)^n$ es igual a p^{-kn}. Por lo tanto, la medida de $\{x \in a+(p\mathbb{Z}_p)^n : f(x) \equiv 0 \mod p^k\}$ es igual a $p^{(k-1)(n-1)}p^{-kn} = p^{-k-n+1}$. En consecuencia se obtiene que,

$$\int_{a+(p\mathbb{Z}_p)^n} |f(x)|_p^s|dx| = \sum_{k=1}^{\infty} p^{-ks}(p^{-k-n+1} - p^{-k-n}),$$

$$= p^{-n}(p-1)\sum_{k=1}^{\infty}(p^{-(s+1)})^k,$$

$$= p^{-n}(p-1)\frac{p^{-(s+1)}}{1-p^{-(s+1)}}.$$

Dado que $Re(s) > 0$, implica que el valor absoluto de $p^{-(s+1)} < 1$. □

Sea $\mathbb{F}_p = \{0, 1, \cdots, p-1\}$ el cuerpo finito con p elementos.
Se define la función " $-$ " como

$$- : \mathbb{Z}_p \to \mathbb{F}_p$$

$$x_0 + p(\cdots) \to x_0.$$

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

Corolario 7 *Sea p un número primo y sea $f(x) = f(x_1, \ldots, x_n) \in \mathbb{Z}_p[x_1, \ldots, x_n]$. Denote por $\bar{f}$ el polinomio sobre $\mathbb{F}_p$ obtenido al reducir cada coeficiente de f módulo $p\mathbb{Z}_p$. Sea N es número de elementos en el conjunto $\{a \in (\mathbb{F}_p^\times)^n : \bar{f}(a) = 0\}$. Suponga que el conjunto de congruencias*

$$\begin{cases} f(x) \equiv 0 \mod p, \\ \frac{\partial f}{\partial x_i}(x) \equiv 0 \mod p,\ i = 1, 2, \cdots, n, \end{cases}$$

no tiene solución en $(\mathbb{Z}_p^\times)^n$, entonces para $s \in \mathbb{C}$ con $Re(s) > 0$ se tiene

$$\int_{(\mathbb{Z}_p^\times)^n} |f(x)|_p^s |dx| = p^{-n} \left((p-1)^n - N \frac{1 - p^{-s}}{1 - p^{-(s+1)}} \right)$$

$Demostración$. Dado que $\bigcup_{a \in \{1, \ldots, p-1\}^n} a + (p\mathbb{Z}_p)^n$ es una partición de $(\mathbb{Z}_p^\times)^n$, se tiene que

$$\int_{(\mathbb{Z}_p^\times)^n} |f(x)|_p^s |dx| = \sum_{\substack{a \in \{1,\dots,p-1\}^n \\ f(a) \not\equiv 0 \mod p}} \int_{a+(p\mathbb{Z}_p)^n} |f(x)|_p^s |dx| + \sum_{\substack{a \in \{1,\dots,p-1\}^n \\ f(a) \equiv 0 \mod p}} \int_{a+(p\mathbb{Z}_p)^n} |f(x)|_p^s |dx|$$

De la condición establecida en la Proposición 18 y la hipótesis, se tiene que:

$$\begin{aligned}\int_{(\mathbb{Z}_p^\times)^n} |f(x)|_p^s |dx| &= ((p-1)^n - N)p^{-n} + Np^{-n}(p-1)\frac{p^{-(s+1)}}{1-p^{-(s+1)}} \\ &= p^{-n}\left((p-1)^n - N\frac{1-p^{-s}}{1-p^{-(s+1)}}\right).\end{aligned}$$

□

Se introduce la fórmula de la fase estacionaria que es un método elemental para calcular integrales $p-$ádicas del tipo $Z(s,f)$. Igusa conjeturó que este método podría conducir a una prueba nueva y elemental de la racionalidad de $Z(s,f)$, el cual es un problema abierto.

Proposición 19 (Fórmula de la fase estacionaria) *Sean $f(x) \in \mathbb{Z}_p[x_1, \cdots . x_n]$, $\bar{E} \subset \mathbb{F}_p^n$ y $\bar{S} = \{\bar{a} \in \bar{E} : \bar{f}(\bar{a}) = \frac{\partial \bar{f}}{\partial x_i}(\bar{a}) = 0, 1 \leq i \leq n\}$. Considere E y S las preimágenes de $\bar{E}$ y $\bar{S}$ bajo $- : \mathbb{Z}_p^n \to \mathbb{F}_p^n$ y sea N el número de ceros de $\bar{f}(x)$ en $\bar{E}$. Entonces*

$$Z(s,f) = \int_E |f(x)|_p^s \, |dx| = p^{-n}(\#\bar{E} - N) + \frac{p^{-n-s}(1-p^{-1})(N - \#\bar{S})}{1-p^{-1-s}} + \int_S |f(x)|_p^s \, |dx|$$

Demostración. Como $E = \bigsqcup_{\bar{a}\in\bar{E}} a + (p\mathbb{Z}_p)^n$, entonces

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

Sea $\bar{a} \in \bar{E} \setminus \bar{S}$ tal que $\bar{f}(\bar{a}) \neq 0$, es decir, $|f(a+px)|_p = 1$, en este caso

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

por como se definió N, se tiene como primer sumando, $p^{-n}(\#\bar{E} - N)$.

Sea $\bar{a} \in \bar{E} \setminus \bar{S}$ tal que $\bar{f}(\bar{a}) = 0$ y $\frac{\partial \bar{f}}{\partial x_i}(\bar{a}) \neq 0$ para algún $i \in \{1,\dots,n\}$, sin pérdida de generalidad, suponga $i = 1$. Se define

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

Entonces los $g_i(x)$ son SRP y $\det\left[\frac{\partial g_i}{\partial x_j}(0)\right] = \frac{\partial f}{\partial x_1}(0) \not\equiv 0 \mod p$, sea $y_i = g_i(x)$ para $i = 1,\dots,n$, una función de $\mathbb{Z}_p^n$ en sí mismo que preserva la medida. Para más detalles consultar [[9], pág. 110, 168.]

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

Por lo tanto:

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

□

En los siguientes ejemplos, dx y $dxdy$ representan las medidas de Haar $|dx|$ y $|dxdy|$ respectivamente.

Ejemplo 16 *Sea* $f(x) = x^2 - 1$, *con* $p \neq 2$, *entonces*

$$Z(s,f) = \int_{\mathbb{Z}_p} |x^2-1|_p^s dx,$$

$Re(s) > -1$.
$\bar{E} = \mathbb{F}_p = \{0, 1, \ldots, p-1\}$ *entonces* $E = \mathbb{Z}_p$, *por otra parte* $f'(x) = 2x$ *implica que* $x = 0$ *es la única solución de* $f'(x) = 0$, *pero* $f(0) = -1$ *por lo tanto* $\bar{S} = \emptyset = S$.

$$\text{Sea } N = \#\{x \in \mathbb{F}_p : x^2 - 1 \equiv 0 \mod p\} = \#\{1, p-1\} = 2,$$

aplicando la Fórmula de la fase estacionaria se cumple

$$Z(s,f) = \int_{\mathbb{Z}_p} |x^2-1|_p^s \, dx = p^{-1}(p-2) + \frac{2p^{-1-s}(1-p^{-1})}{1-p^{-1-s}}.$$

Ejemplo 17 *Sea* $f(x,y) = x^2 + xy + y^2, p \neq 2, 3$,

$$Z(s,f) = \int_{\mathbb{Z}_p^2} |x^2 + xy + y^2|_p^s \, dxdy,$$

$E = \mathbb{Z}_p^2, \bar{E} = \mathbb{F}_p^2, \frac{\partial f}{\partial x} = 2x + y, \frac{\partial f}{\partial y} = x + 2y$, igualando ambas derivadas parciales a 0 se tiene, $0 = 2x + y = x + 2y$ implica $y = -2x, x = -2y$, luego $y = -2(-2y) = 4y$, en consecuencia $y = 0 = x$, y $f(0,0) = 0$ entonces $\bar{S} = \{(0,0)\}, S = p\mathbb{Z}_p \times p\mathbb{Z}_p$, y $N = \#\{(x,y) \in \mathbb{F}_p^2 : x^2 + xy + y^2 \equiv 0 \mod p\}$.

$$Z(s,f) = p^{-2}(p^2 - N) + \frac{p^{-2-s}(1-p^{-1})(N-1)}{1-p^{-1-s}} + \int_{p\mathbb{Z}_p \times p\mathbb{Z}_p} |x^2 + xy + y^2|_p^s \, dxdy.$$

Haciendo un cambio de variables $x = pu, y = pv$, con $u, v \in \mathbb{Z}_p$ se tiene que $dxdy = p^{-2}dudv$, por lo tanto

$$\begin{aligned}
\int_{p\mathbb{Z}_p \times p\mathbb{Z}_p} |x^2 + xy + y^2|_p^s \, dxdy &= p^{-2} \int_{\mathbb{Z}_p^2} |p^2u^2 + p^2uv + p^2v^2|_p^s \, dudx, \\
&= p^{-2} \int_{\mathbb{Z}_p^2} |p^2|_p^s |u^2 + uv + v^2|_p^s \, dudv, \\
&= p^{-2-2s} \int_{\mathbb{Z}_p^2} |u^2 + uv + v^2|_p^s \, dudv, \\
&= p^{-2-2s} Z(s,f),
\end{aligned}$$

así,

$$Z(s,f) = p^{-2}(p^2 - N) + \frac{p^{-2-s}(1-p^{-1})(N-1)}{1-p^{-1-s}} + p^{-2-2s}Z(s,f),$$

por lo anterior,

$$Z(s,f) = \frac{1}{1-p^{-2-s}} \left(p^{-2}(p^2 - N) + \frac{p^{-2-s}(1-p^{-1})(N-1)}{1-p^{-1-s}} \right),$$

con $Re(s) > -2$.

Ejemplo 18 *Sea* $f(x,y) = x^2 + y^3$*, entonces*

$$Z(s,f) = \int_{\mathbb{Z}_p^2} |x^2 + y^3|_p^s \, dxdy$$

Aplicando FFE, $E = \mathbb{Z}_p^2, \bar{E} = \mathbb{F}_p^2, \frac{\partial f}{\partial x} = 2x, \frac{\partial f}{\partial y} = 3y^2$*, se tiene que* $\bar{S} = \{(0,0)\}, S = p\mathbb{Z}_p \times p\mathbb{Z}_p$ *y* $N = \#\{(x,y) \in \mathbb{F}_p^2 : x^2 + y^3\} = p$*, dado que* $x = \alpha^3, y = \alpha^2, \alpha \in \mathbb{F}_p$*.*

$$\begin{aligned} Z(s,f) &= p^{-2}(p^2 - p) + \frac{p^{-2-s}(1-p^{-1})(p-1)}{1-p^{-1-s}} + \int_{(p\mathbb{Z}_p)^2} |x^2 + y^3|_p^s \, dxdy, \\ &= (1-p^{-1})\frac{1-p^{-2-s}}{1-p^{-1-s}} + \int_{(p\mathbb{Z}_p)^2} |x^2 + y^3|_p^s \, dxdy. \end{aligned}$$

Haciendo un cambio de variables $x = pu, y = pv, u, v \in \mathbb{Z}_p, dxdy = p^{-2}dudv$*, se tiene*

$$\begin{aligned} Z(s,f) &= p^{-2}(p^2 - p) + \frac{p^{-2-s}(1-p^{-1})(p-1)}{1-p^{-1-s}} + \int_{\mathbb{Z}_p^2} |p^2u^2 + p^3v^3|_p^s \, dudv, \\ &= (1-p^{-1})\frac{1-p^{-2-s}}{1-p^{-1-s}} + \int_{\mathbb{Z}_p^2} |p^2|_p^s |u^2 + pv^3|_p^s \, dudv, \\ &= (1-p^{-1})\frac{1-p^{-2-s}}{1-p^{-1-s}} + p^{-2-s}\int_{\mathbb{Z}_p^2} |u^2 + pv^3|_p^s \, dudv, \\ &= (1-p^{-1})\frac{1-p^{-2-s}}{1-p^{-1-s}} + p^{-2-s}Z_1(s,g), \end{aligned}$$

donde $g(u,v) = u^2 + pv^3$*. Aplicando de nuevo FFE sobre* $Z_1(s,g)$*,* $E = \mathbb{Z}_p^2, \bar{E} = \mathbb{F}_p^2$*, dado que* $\bar{g}(u,v) = u^2$*, entonces la solución de* $\bar{g}(u,v) = 0$ *está dada por,*

$$\bar{g}(u,v) = \frac{\partial \bar{g}}{\partial u}(u,v) = \frac{\partial \bar{g}}{\partial v}(u,v) = 0 \text{ implica } u^2 = 2u = 0, \text{ es decir}$$

$\bar{S} = \{0\} \times \mathbb{F}_p$, *entonces* $S = p\mathbb{Z}_p \times \mathbb{Z}_p$ *y* $N = \#\{(u,v) \in \mathbb{F}_p^2 : u^2 = 0\} = p$, *así*

$$\begin{aligned} Z_1(s,g) &= p^2(p^2-p) + \frac{p^{-2-s}(1-p^{-1})(p-p)}{1-p^{-1-s}} + \int_{p\mathbb{Z}_p \times \mathbb{Z}_p} |u^2 + pv^3|_p^s \, dudv \\ &= p^2(p^2-p) + \int_{p\mathbb{Z}_p \times \mathbb{Z}_p} |u^2 + pv^3|_p^s \, dudv \end{aligned}$$

haciendo $u = ps$, *con* $s \in \mathbb{Z}_p,\ du = p^{-1}du$, *se tiene,*

$$\begin{aligned} Z_1(s,g) &= p^2(p^2-p) + p^{-1-s} \int_{\mathbb{Z}_p^2} |ps^2 + v^3|_p^s \, dsdv \\ &= p^2(p^2-p) + p^{-1-s} Z_2(s,h), \end{aligned}$$

donde $h(s,v) = ps^2 + v^3$. *Nuevamente por FFE sobre* $Z_2(s,h)$, $E = \mathbb{Z}_p^2, \bar{E} = \mathbb{F}_p^2$, *puesto que* $\bar{h}(s,v) = v^3$, *la solución del sistema* $\bar{H}(s,v) = 0$ *está dado por*

$\bar{h}(s,v) = \dfrac{\partial \bar{h}}{\partial s}(s,v) = \dfrac{\partial \bar{h}}{\partial v}(s,v) = 0$ *lo cual implica que,* $v^3 = 0 = 3v^2$ *y por lo tanto*

$\bar{S} = \mathbb{F}_p \times \{0\},\ S = \mathbb{Z}_p \times p\mathbb{Z}_p$ *y* $N = \#\{(s,v) \in \mathbb{F}_p^2 : v^3 = 0\} = p$, *entonces*

$$Z_2(s,h) = p^{-2}(p^2-p) + \int_{\mathbb{Z}_p \times p\mathbb{Z}_p} |ps^2 + v^3|_p^s \, dsdv,$$

haciendo $v = pt$, *con* $t \in \mathbb{Z}_p, dx = p^{-1}dt$,

$$\begin{aligned} Z_2(s,h) &= p^{-2}(p^2-p) + p^{-1-s} \int_{\mathbb{Z}_p^2} |s^2 + p^2t^3|_p^s \, dsdt, \\ &= p^{-2}(p^2-p) + p^{-1-s} Z_3(s,j), \end{aligned}$$

donde $j(s,t) = s^2 + p^2t^3$. *Repitiendo el proceso de FFE sobre* $Z_3(s,j)$, $E = \mathbb{Z}_p^2, \bar{E} = \mathbb{F}_p^2$, *dado que* $\bar{j(s,t)} = s^2$, *el sistema*

$\bar{j}(s,t) = \dfrac{\partial \bar{j}}{\partial s}(s,t) = \dfrac{\partial \bar{j}}{\partial t}(s,t) = 0$ *implica* $s^2 = 2s = 0,$ *así se tiene*

$\bar{S} = \{0\} \times \mathbb{F}_p, S = p\mathbb{Z}_p \times \mathbb{Z}_p$ *y* $N = \#\{(s,t) \in \mathbb{F}_p^2 : s^2 = 0\} = p$*, entonces*

$$Z_3(s,j) = p^{-2}(p^2 - p) + \int_{p\mathbb{Z}_p \times \mathbb{Z}_p} |s^2 + p^2 t^3|_p^s \, dsdt,$$

haciendo $s = pr$*, con* $r \in \mathbb{Z}_p, ds = p^{-1}dr$*, entonces*

$$\begin{aligned} Z_3(s,j) &= p^{-2}(p^2 - p) + p^{-1-2s} \int_{\mathbb{Z}_p^2} |r^2 + t^3|_p^s \, drdt, \\ &= p^{-2}(p^2 - p) + p^{-1-2s} Z(s,f), \end{aligned}$$

por lo tanto,

$$\begin{aligned} Z(s,f) = (1 - p^{-1})\frac{1 - p^{-2-s}}{1 - p^{-1-s}} + p^{-2-2s}(1 - p^{-1}) + p^{-3-3s}(1 - p^{-1}) \\ + p^{-4-4s}(1 - p^{-1}) + p^{-5-6s} Z(s,f), \end{aligned}$$

es decir,

$$\begin{aligned} Z(s,f) &= \frac{1 - p^{-1}}{1 - p^{-5-6s}} \left(\frac{1 - p^{-2-s}}{1 - p^{-1-s}} + p^{-2-2s} + p^{-3-3s} + p^{-4-4s} \right) \\ &= \frac{1 - p^{-1}}{(1 - p^{-1-s})(1 - p^{-5-6s})}(1 - p^{-2-s} + p^{-2-2s} - p^{-5-6s}). \end{aligned}$$

3.3. FÓRMULA EXPLÍCITA PARA LA FUNCIÓN ZETA DE IGUSA

En esta sección se dará una fórmula para la función zeta de Igusa para polinomios que sean no degenerados sobre $\mathbb{F}_p$ con respecto a todas las caras de su poliedro de Newton (caso global) o con respecto a sus caras compactas (caso local en el origen).

Se introducirán las funciones con las que se expresará la fórmula para la función zeta de Igusa, en relación con las caras del poliedro de Newton, los conos duales asociados como partición de $(\mathbb{R}^+)^n$ y los puntos enteros contenidos en éstos.

Definición 37 *Para $k = (k_1, \ldots, k_n) \in \mathbb{R}^n$, se considera la suma de componentes:*

$$\sigma(k) = \sum_{i=1}^{n} k_i.$$

Definición 38 *Sea τ cara de $\Gamma(f)$, $p-$primo y $s \in \mathbb{C}$ tal que $Re(s) > 0$. Se definen las siguientes expresiones:*

$$\begin{aligned} N_\tau &:= \#\{a \in (\mathbb{F}_p^\times)^n | \bar{f}_\tau(a) = 0\}, \\ L_\tau(s) &:= p^{-n}\left((p-1)^n - pN_\tau \frac{p^s - 1}{p^{s+1} - 1}\right), \\ S_{\Delta_\tau}(s) &:= \sum_{k \in \mathbb{N}^n \cap \Delta_\tau} p^{-\sigma(k) - m(k)s}, \end{aligned}$$

note que también se considera $\tau = \Gamma(f)$.

Para calcular $S_{\Delta_\tau}(s)$, se toma una partición de Δ_τ en conos simpliciales racionales Δ_{τ_i} (también están incluidos los subconos simpliciales maximales que aparecen como intersección de los conos de mayor dimensión, cubriendo de esta manera todo

el interior de Δ_τ), sobre cada cono de la partición,

$$\begin{aligned} S_{\Delta_\tau}(s) &= \sum S_{\Delta_{\tau_i}}(s) \text{ con } S_{\Delta_{\tau_i}}(s) \\ &= \sum_{k \in \mathbb{N}^n \cap \Delta_{\tau_i}} p^{-\sigma(k)-m(k)s}. \end{aligned}$$

Proposición 20 *En las condiciones anteriores, sea Δ_i un cono simplicial estrictamente generado por $a_1, \ldots, a_e \in \mathbb{N}^n$ linealmente independientes. Entonces:*

$$S_{\Delta_i} = \frac{\sum_h p^{\sigma(h)+m(h)s}}{(p^{\sigma(a_1)+m(a_1)s}-1)\cdots(p^{\sigma(a_e)+m(a_e)s}-1)},$$

donde h recorre los puntos enteros de $\{\sum_{i=1}^e \lambda_i a_i | 0 \leq \lambda_i < 1\}$.

$Demostración.$ Sea $x_\tau \in \tau$ fijo, se tiene que $m(k) = k \cdot x_\tau$ para todo $k \in \Delta_\tau$, luego:

$$S_{\Delta_i} = \sum_{k \in \mathbb{N}^n \cap \Delta_i} p^{-\sigma(k)-(k\cdot x_\tau)s}$$

Se consideran los siguientes dos casos:

- Δ_i **cono simple:** Es equivalente a

$$\mathbb{N}^n \cap \Delta_i = \mathbb{N}^+ a_1 + \cdots + \mathbb{N}^+ a_e, \text{ donde } \mathbb{N}^+ = \mathbb{N} \setminus \{0\}.$$

  Dado que $a_1, \ldots, a_e$ son linealmente independientes:

$$\begin{aligned} S_{\Delta_i} &= \sum_{\lambda_1,\ldots,\lambda_e \in \mathbb{N}^+} p^{-\sigma(\lambda_1 a_1+\cdots+\lambda_e a_e)-((\lambda_1 a_1+\cdots+\lambda_e a_e)\cdot x_\tau)s}, \\ &= \sum_{\lambda_1=1}^{\infty} (p^{-\sigma(a_1)-(a_1\cdot x_\tau)s})^{\lambda_1} \cdots \sum_{\lambda_e=1}^{\infty} (p^{-\sigma(a_e)-(a_e\cdot x_\tau)s})^{\lambda_e}, \end{aligned}$$

  puesto que $Re(s) > 0$ y $p > 1$, se tiene $|p^{-\sigma(a_j)-(a_j\cdot x_\tau)s}| < 1$ para $j = 1, \ldots, e$,

por lo tanto las series geométricas convergen y:

$$S_{\Delta_i} = \frac{p^{-\sigma(a_1)-(a_1\cdot x_\tau)s}}{1-p^{-\sigma(a_1)-(a_1\cdot x_\tau)s}} \cdots \frac{p^{-\sigma(a_e)-(a_e\cdot x_\tau)s}}{1-p^{-\sigma(a_e)-(a_e\cdot x_\tau)s}},$$
$$= \frac{1}{(p^{\sigma(a_1)+(a_1\cdot x_\tau)s}-1)\cdots(p^{\sigma(a_e)+(a_e\cdot x_\tau)s}-1)},$$

con $a_j \cdot x_\tau = m(a_j)$ dado que $a_i \in \{a \in (\mathbb{R}^+)^n | \tau \subset F(a)\} = \bar{\Delta}_\tau$, para todo $j = 1, \ldots, e$.

- **Caso general:** Se considera el conjunto,

$$\mathbb{Z}^n \cap \left\{ \sum_{j=1}^{e} \mu_j a_j | 0 < \mu_j \leq 1 \right\}, \tag{11}$$

se obtiene que

$$\mathbb{N}^n \Delta_i = \bigsqcup (g + \mathbb{N}a_1 + \cdots + \mathbb{N}a_e),$$

con g recorriendo el conjunto (11), luego,

$$S_{\Delta_i} = \left(\sum_g p^{-\sigma(g)-(g\cdot x_\tau)s} \right) \sum_{\lambda_1,\ldots,\lambda_e \in \mathbb{N}^+} p^{-\sigma(\lambda_1 a_1+\cdots+\lambda_e a_e)-((\lambda_1 a_1+\cdots+\lambda_e a_e)\cdot x_\tau)s},$$

dado que $Re(s) > 0$, se cumple:

$$S_{\Delta_i} = \left(\sum_g p^{-\sigma(g)-(g\cdot x_\tau)s} \right) \frac{p^{-\sigma(a_1+\cdots+a_e)+((a_1+\cdots+a_e)\cdot x_\tau)s}}{(p^{\sigma(a_1)+(a_1\cdot x_\tau)s}-1)\cdots(p^{\sigma(a_e)+(a_e\cdot x_\tau)s}-1)},$$
$$= \frac{\sum_g p^{-\sigma(a_1+\cdots+a_e-g)+((a_1+\cdots+a_e-g)\cdot x_\tau)s}}{(p^{\sigma(a_1)+(a_1\cdot x_\tau)s}-1)\cdots(p^{\sigma(a_e)+(a_e\cdot x_\tau)s}-1)},$$

con g recorriendo el conjunto (11). Los elementos a_j y $(a_1 + \cdots + a_e - g)$ pertenecen a $\bar{\Delta}_\tau$, luego $a_j \cdot x_\tau = m(a_j)$ y $(a_1 + \cdots + a_e - g) \cdot x_\tau = m(a_1 + \cdots + a_e - g)$.

De esta forma, haciendo $h = a_1 + \cdots + a_e - g$ se tiene:

$$S_{\Delta_i} = \frac{\sum_h p^{\sigma(h)+m(h)s}}{(p^{\sigma(a_1)+m(a_1)s} - 1) \cdots (p^{\sigma(a_e)+m(a_e)s} - 1)},$$

donde h recorre $\mathbb{Z}^n \cap \{\sum_{i=1}^{e} \lambda_i a_i |\ 0 \leq \lambda_i < 1\}$.

□

Teorema 14 *Sea $p-$primo y $f \in \mathbb{Z}_p[x_1, \ldots, x_n]$ polinomio no degenerado sobre $\mathbb{F}_p$ con respecto a todas las caras de su poliedro de Newton $\Gamma(f)$.*
Se tiene:

$$Z(s, f) = L_{\Gamma(f)}(s) + \sum_{\substack{\tau \ cara \ propia \\ de \ \Gamma(f)}} L_\tau(s) S_{\Delta_\tau}(s).$$

para $s \in \mathbb{C}$ con $Re(s) > 0$.

$Demostración$. Puesto que los conos asociados a las caras de $\Gamma(f)$ forman una partición de $(\mathbb{R}^+)^n$, es decir:

$$(\mathbb{R}^+)^n = \{0\} \cup \bigcup_{\substack{\tau \ cara \ propia \\ de \ \Gamma(f)}} \Delta_\tau.$$

De esta forma, se tiene:

$$Z(s,f) = \int_{\mathbb{Z}_p^n} |f(x)|_p^s \, |dx| = \sum_{k \in \mathbb{N}^n} \int_{\substack{x \in \mathbb{Z}_p^n \\ \text{ord}_p(x) = k}} |f(x)|_p^s |dx|$$

$$= \int_{(\mathbb{Z}_p^\times)^n} |f(x)|_p^s |dx| + \sum_{\substack{\tau \; cara \; propia \\ de \; \Gamma(f)}} \sum_{k \in \mathbb{N}^n \cap \Delta_\tau} \int_{\substack{x \in \mathbb{Z}_p^n \\ \text{ord}_p(x) = k}} |f(x)|_p^s |dx|,$$

donde ord_p se toma componente a componente. Suponga que τ es cara propia de $\Gamma(f), k \in \mathbb{N}^n \cap \Delta_\tau$ y $x = (x_1, \ldots, x_n) \in \mathbb{Z}_p^n$ tal que $\text{ord}_p(x) = k$. Sea $x_j = p^{k_j} u_j$ con $u_i \in \mathbb{Z}_p^\times, j = 1, \ldots, n$, entonces,

$$|dx| = p^{\sigma(k)} |du| \text{ y } x^\omega = (x_1^{\omega_1}, \ldots, x_n^{\omega_n}) = p^{k \cdot \omega} u^\omega,$$

dado que $m(a) = \min_{\omega \in \text{supp}(f)} \{k \cdot \omega\}$ y $F(k) = \tau$, luego $k \cdot \omega = m(k)$ para todo $\omega \in \text{supp}(f) \cap \tau$ y $k \cdot \omega > m(k)$ para todo $\omega \in \text{supp}(f) \setminus \tau$. De esta forma, se puede expresar el polinomio f de la siguiente manera con el respectivo cambio de variable:

$$f(x) = p^{m(k)} (f_\tau(u) + p \tilde{f}_{\tau,k}(u)),$$

donde $\tilde{f}_{\tau,k} \in \mathbb{Z}_p[u_1, \ldots, u_n]$ depende de f, τ y k. Luego,

$$Z(s,f) = \int_{(\mathbb{Z}_p^\times)^n} |f(x)|_p^s \, |dx| + \sum_{\substack{\tau \; cara \; propia \\ de \; \Gamma(f)}} \sum_{k \in \mathbb{N}^n \cap \Delta_\tau} p^{-\sigma(k) - m(k)s} \int_{(\mathbb{Z}_p^\times)^n} |f_\tau(u) + p \tilde{f}_{\tau,k}(u)|_p^s \, |du|,$$

haciendo,

$$L_{\Gamma(f)}(s) = \int\limits_{(\mathbb{Z}_p^\times)^n} |f(x)|_p^s \, |dx|,$$
$$L_\tau(s) = \int\limits_{(\mathbb{Z}_p^\times)^n} |f_\tau(u) + p\tilde{f}_{\tau,k}(u)|_p^s \, |du|.$$

Por hipótesis, f es no degenerado sobre $\mathbb{F}_p$ con respecto a todas las caras del poliedro de Newton, por lo tanto los sistemas de congruencias

$$\begin{cases} f(x) \equiv 0 & \text{mód } p \\ \frac{\partial f}{\partial x_i}(x) \equiv 0 & \text{mód } p, i = 1, \ldots, n \end{cases} \text{ y } \begin{cases} f_\tau(u) + p\tilde{f}_{\tau,k}(u) \equiv 0 & \text{mód } p \\ \frac{\partial (f_\tau + p\tilde{f}_{\tau,k})}{\partial u_i}(u) \equiv 0 & \text{mód } p, i = 1, \ldots, n \end{cases}$$

no tienen soluciones en $(\mathbb{Z}_p^\times)^n$. Luego, por el Corolario 7 se tiene:

$$L_{\Gamma(f)}(s) = p^{-n}\left((p-1)^n - pN_{\Gamma(f)}\frac{p^s-1}{p^{s+1}-1}\right),$$
$$L_\tau(s) = p^{-n}\left((p-1)^n - pN_\tau\frac{p^s-1}{p^{s+1}-1}\right),$$

para toda τ cara propia de $\Gamma(f)$. Note que L_τ no depende de k, solamente de la cara τ, por lo tanto,

$$Z(s,f) = L_{\Gamma(f)}(s) + \sum_{\substack{\tau \; cara \; propia \\ de \; \Gamma(f)}} L_\tau(s) S_{\Delta_\tau}(s), \text{ con } S_{\Delta_\tau} = \sum_{k \in \mathbb{N}^n \cap \Delta_\tau} p^{-\sigma(k) - m(k)s}.$$

□

Ejemplo 19 *Sea* $f(x,y) = x^2 + xy + y^2$*,* $supp(f) = \{(2,0),(1,1),(0,2)\}$*, entonces*

$\Gamma(f)$ *es igual a la envolvente convexa del siguiente conjunto*

$$\bigcup_{\omega \in \mathit{supp}(f)} \omega + (\mathbb{R}^+)^2.$$

Cara propia τ	*Dimensión*
$\tau_0 = \{(0,2)\}$	0
$\tau_2 = \{(2,0)\}$	0
$\tau_1 = \{(0,2) + \mathbb{R}^+(0,1)\}$	1
$\tau_3 = \{(1-\lambda)(0,2) + \lambda(2,0) \mid 0 < \lambda < 1\}$	1
$\tau_4 = \{(2,0) + \mathbb{R}^+(1,0)\}$	1

Polinomios asociados a cada cara:

$$f_{\tau_0} = f_{\tau_1} = y^2;$$
$$f_{\tau_2} = f_{\tau_4} = x^2;$$
$$f_{\tau_3} = x^2 + xy + y^2.$$

Conos asociados a cada cara:

$$\Delta_{\tau_0} = \{(x,y) \in \mathbb{R}^2 | (x,y) = \alpha(1,1) + \beta(1,0); \alpha, \beta \in \mathbb{R}^+\}$$
$$\Delta_{\tau_1} = \{(x,y) \in \mathbb{R}^2 | (x,y) = \alpha(1,0); \alpha \in \mathbb{R}^+\}$$
$$\Delta_{\tau_2} = \{(x,y) \in \mathbb{R}^2 | (x,y) = \alpha(1,1) + \beta(0,1); \alpha, \beta \in \mathbb{R}^+\}$$
$$\Delta_{\tau_3} = \{(x,y) \in \mathbb{R}^2 | (x,y) = \alpha(1,1); \alpha \in \mathbb{R}^+\}$$
$$\Delta_{\tau_4} = \{(x,y) \in \mathbb{R}^2 | (x,y) = \alpha(0,1); \alpha \in \mathbb{R}^+\}$$

por lo tanto todos los conos son simples.

Sea p *primo, con* $p > 3$ *(para garantizar la condición de no degeneración sobre* $\mathbb{F}_p$ *sobre todas las caras* τ *de* $\Gamma(f)$*) y* $s \in \mathbb{C}$ *con* $Re(s) > 0$*, se calculará* $Z(s, f)$ *usando*

el Teorema 14, se tiene,

$$L_{\Gamma(f)}(s) = p^{-2}\left((p-1)^2 - pN_{\Gamma(f)}\frac{p^s-1}{p^{s-1}-1}\right),$$

Cara propia τ	*Generadores de* Δ_τ	S_{Δ_τ}	N_τ	$L_\tau(s)$
τ_0	$(1,1),(1,0)$	$\frac{1}{(p-1)(p^{2+2s}-1)}$	*0*	$p^{-2}(p-1)^2$
τ_1	$(1,0)$	$\frac{1}{p-1}$	*0*	$p^{-2}(p-1)^2$
τ_2	$(1,1),(0,1)$	$\frac{1}{(p-1)(p^{2+2s}-1)}$	*0*	$p^{-2}(p-1)^2$
τ_3	$(1,1)$	$\frac{1}{p^{2+2s}-1}$	N_{τ_3}	$p^{-2}\left((p-1)^2 - pN_{\tau_3}\frac{p^s-1}{p^{s+1}-1}\right)$
τ_4	$(0,1)$	$\frac{1}{p-1}$	*0*	$p^{-2}(p-1)^2$

Por lo tanto:

$$\begin{aligned} Z(s,f) = {} & p^{-2}\left((p-1)^2 - pN_{\Gamma(f)}\frac{p^s-1}{p^{s-1}-1}\right) + 2p^{-2}(p-1)\left(\frac{1}{p^{2+2s}-1}+1\right) \\ & + \frac{p^{-2}}{p^{2+2s}-1}\left((p-1)^2 - pN_{\tau_3}\frac{p^s-1}{p^{s+1}-1}\right). \end{aligned}$$

Ejemplo 20 *Sea* $g(x,y) = x^2y^2 + x^5 + y^5$*, entonces*

Cara propia τ	*Dimensión*
$\tau_0 = \{(0,5)\}$	0
$\tau_1 = \{(2,2)\}$	0
$\tau_2 = \{(5,0)\}$	0
$\tau_3 = \{(1-\lambda)(0,5) + \lambda(2,2) \mid 0 < \lambda < 1\}$	1
$\tau_4 = \{(1-\lambda)(2,2) + \lambda(5,0) \mid 0 < \lambda < 1\}$	1
$\tau_5 = \{(0,5) + \mathbb{R}^+(0,1)\}$	1
$\tau_6 = \{(5,0) + \mathbb{R}^+(1,0)\}$	1

Polinomios asociados a cada cara:

$$
\begin{aligned}
g_{\tau_0} &= y^5, \\
g_{\tau_1} &= x^2y^2, \\
g_{\tau_2} &= x^5, \\
g_{\tau_3} &= x^2y^2 + y^5, \\
g_{\tau_4} &= x^5 + x^2y^2, \\
g_{\tau_5} &= y^5, \\
g_{\tau_6} &= x^5.
\end{aligned}
$$

Subdivisión cónica:

$$
\begin{aligned}
\Delta_{\tau_{0,1}} &= \mathbb{R}_{>0}(1,0) + \mathbb{R}_{>0}(2,1), \\
\Delta_{\tau_{0,2}} &= \mathbb{R}_{>0}(2,1), \\
\Delta_{\tau_{0,3}} &= \mathbb{R}_{>0}(2,3) + \mathbb{R}_{>0}(2,1), \\
\Delta_{\tau_{1,1}} &= \mathbb{R}_{>0}(2,1) + \mathbb{R}_{>0}(1,1), \\
\Delta_{\tau_{1,2}} &= \mathbb{R}_{>0}(1,1), \\
\Delta_{\tau_{1,3}} &= \mathbb{R}_{>0}(3,2) + \mathbb{R}_{>0}(1,1), \\
\Delta_{\tau_{2,1}} &= \mathbb{R}_{>0}(3,2) + \mathbb{R}_{>0}(1,2), \\
\Delta_{\tau_{2,2}} &= \mathbb{R}_{>0}(1,2), \\
\Delta_{\tau_{2,3}} &= \mathbb{R}_{>0}(3,2) + \mathbb{R}_{>0}(0,1), \\
\Delta_{\tau_3} &= \mathbb{R}_{>0}(2,3), \\
\Delta_{\tau_4} &= \mathbb{R}_{>0}(3,2), \\
\Delta_{\tau_5} &= \mathbb{R}_{>0}(1,0), \\
\Delta_{\tau_6} &= \mathbb{R}_{>0}(0,1).
\end{aligned}
$$

Cara propia τ	*Generadores de* Δ_τ	S_{Δ_τ}	N_τ	$L_\tau(s)$
$\tau_{0,1}$	$(1,0),(2,1)$	$\frac{1}{(p-1)(p^{3+5s}-1)}$	0	$p^{-2}(p-1)^2$
$\tau_{0,2}$	$(2,1)$	$\frac{1}{(p^{3+5s}-1)}$	0	$p^{-2}(p-1)^2$
$\tau_{0,3}$	$(2,3),(2,1)$	$\frac{1}{(p^{5+10s}-1)(p^{3+5s}-1)}$	0	$p^{-2}(p-1)^2$
$\tau_{1,1}$	$(2,1),(1,1)$	$\frac{1}{(p^{3+5s}-1)(p^{2+5s}-1)}$	0	$p^{-2}(p-1)^2$
$\tau_{1,2}$	$(1,1)$	$\frac{1}{(p^{2+5s}-1)}$	0	$p^{-2}(p-1)^2$
$\tau_{1,3}$	$(3,2),(1,1)$	$\frac{1}{(p^{5+10s}-1)(p^{2+5s}-1)}$	0	$p^{-2}(p-1)^2$
$\tau_{2,1}$	$(3,2),(1,2)$	$\frac{1}{(p^{5+10s}-1)(p^{3+5s}-1)}$	0	$p^{-2}(p-1)^2$
$\tau_{2,2}$	$(1,2)$	$\frac{1}{(p^{3+5s}-1)}$	0	$p^{-2}(p-1)^2$
$\tau_{2,3}$	$(3,2),(0,1)$	$\frac{1}{(p-1)(p^{5+10s}-1)}$	0	$p^{-2}(p-1)^2$
τ_3	$(2,3)$	$\frac{1}{(p^{5+10s}-1)}$	N_{τ_3}	$p^{-2}\left((p-1)^2-pN_{\tau_3}\frac{p^s-1}{p^{s+1}-1}\right)$
τ_4	$(3,2)$	$\frac{1}{(p^{5+10s}-1)}$	N_{τ_4}	$p^{-2}\left((p-1)^2-pN_{\tau_4}\frac{p^s-1}{p^{s+1}-1}\right)$
τ_5	$(1,0)$	$\frac{1}{(p-1)}$	0	$p^{-2}(p-1)^2$
τ_6	$(0,1)$	$\frac{1}{(p-1)}$	0	$p^{-2}(p-1)^2$

Por lo tanto:

$$\begin{aligned}Z(s,g) = {} & p^{-2}\left((p-1)^2 - pN_{\Gamma(g)}\frac{p^s-1}{p^{s-1}-1}\right) + \frac{p^{-2}(p-1)(2p-1)}{p^{3+5s}-1} \\ & + \frac{2p^{-2}(p-1)^2}{(p^{5+10s}-1)(p^{3+5s}-1)} + \frac{p^{-2}(p-1)^2}{(p^{2+5s}-1)(p^{3+5s}-1)} \\ & + \frac{p^{-2}(p-1)^2}{(p^{5+10s}-1)(p^{2+3s}-1)} + \frac{p^{-2}(p-1)^2}{p^{2+5s}-1} \\ & + \frac{p^{-2}}{p^{5+10s}-1}\left((p-1)(2p-1) - \frac{p(p^s-1)}{p^{s+1}-1}(N_{\tau_3}+N_{\tau_4})\right) + 2p^{-2}(p-1).\end{aligned}$$

En esta sección se calculará mediante SAGE algunos ejemplos del poligono de Newton haciendo uso del programa ”ZetaFuntions.sage”.

3.4. COMANDOS ASOCIADOS A $Z(s, f)$

- `newton_plot()`: grafica el poliedro de Newton asociado a una función.
- `give_info_newton(faces=true)`: muestra la información de cada cara son sus respectivos vértices y rayos.
- `cones_plot()`: hace la partición cónica en los espacios $\mathbb{R}^2$ y $\mathbb{R}^3$.
- `igusa_zeta()`: calcula la función zeta de Igusa para polinomios no degenerados sobre sus caras.

3.5. EJEMPLOS

Ejemplo 21 *Sea* $f(x, y) = x^2 + xy + y^2$,

Figura 8. Polígono de Newton de $f(x, y)$

```
load('ZetaFunctions610Final.sage')
```

```
R.<x,y> = QQ[]
z = ZetaFunctions(x^2 +x*y + y^2)
z.newton_plot()
```

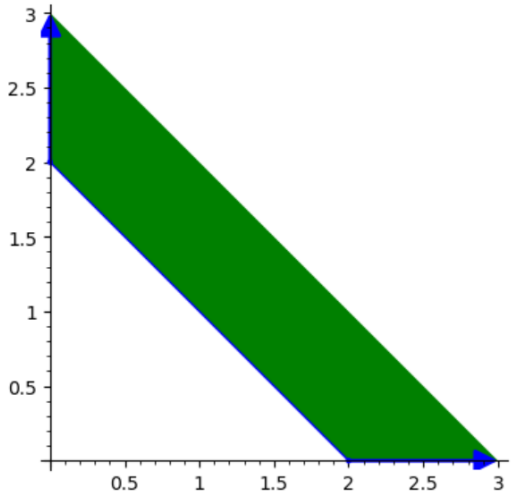


Figura 9. Caras de $\Gamma(f)$

```
z.give_info_newton(faces = True)
```

```
Newton's polyhedron of x^2 + x*y + y^2:
        support points = [(2, 0), (1, 1), (0, 2)]
        vertices = [(0, 2), (2, 0)]
        number of proper faces = 5
        Facet 1: x >= 0
        Facet 2: x + y - 2 >= 0
        Facet 3: y >= 0
Information about faces:
tau0: dim 0,  vertices = [(0, 2)],  rays = []

tau1: dim 1,  vertices = [(0, 2)],  rays = [(0, 1)]

tau2: dim 0,  vertices = [(2, 0)],  rays = []

tau3: dim 1,  vertices = [(0, 2), (2, 0)],  rays = []

tau4: dim 1,  vertices = [(2, 0)],  rays = [(1, 0)]
```

Figura 10. Partición cónica

```
z.cones_plot()
```

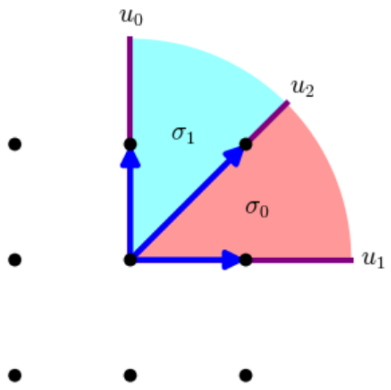


Figura 11. Conos de $\Gamma(f)$

```
z.give_info_newton(cones = True)
```

```
Newton's polyhedron of x^2 + x*y + y^2:
        support points = [(2, 0), (1, 1), (0, 2)]
        vertices = [(0, 2), (2, 0)]
        number of proper faces = 5
        Facet 1: x >= 0
        Facet 2: x + y - 2 >= 0
        Facet 3: y >= 0
Information about faces:
tau0: generators of cone = [(1, 1), (1, 0)], partition into simplicial cones = [[(1, 1), (1, 0)]]

tau1: generators of cone = [(1, 0)], partition into simplicial cones = [[(1, 0)]]

tau2: generators of cone = [(1, 1), (0, 1)], partition into simplicial cones = [[(1, 1), (0, 1)]]

tau3: generators of cone = [(1, 1)], partition into simplicial cones = [[(1, 1)]]

tau4: generators of cone = [(0, 1)], partition into simplicial cones = [[(0, 1)]]
```

Figura 12. $Z(s, f)$ para p primo.

```
z.igusa_zeta()
```

```
(p^6*p^(4*s) + N_Gamma*p^4*p^(2*s)*p^s - 2*p^5*p^(2*s)*p^s - N_Gamma*p^4*p^(4*
s) + N_Gamma*p^3*p^(2*s)*p^s - p^4*p^(4*s) - N_Gamma*p^3*p^(2*s) + p^4*p^(2*s)
+ 2*p^3*p^(2*s)*p^s + N_Gamma*p^2*p^(2*s) - N_tau3*p^2*p^(2*s) - N_Gamma*p^2*p^
s + N_tau3*p^2*p^s - p^2*p^(2*s) - N_Gamma*p*p^s + N_tau3*p*p^s + N_Gamma*p - N
_tau3*p)/((p^2*p^(2*s) - 1)*(p*p^s - 1)^2*p^2)
```

Figura 13. $Z(s, f)$ para $p = 5$.

```
z.igusa_zeta(5)
```

```
24/25*5^(2*s + 2)/(25*5^(2*s) - 1)
```

Ejemplo 22 *Sea* $g(x,y) = x^5 + x^2y^2 + y^5$*, entonces*

Figura 14. Polígono de Newton $g(x,y)$

```
load('ZetaFunctions610Final.sage')
```

```
R.<x,y> = QQ[]
z = ZetaFunctions(x^5 +x^(2)*y^(2) + y^5)
z.newton_plot()
```

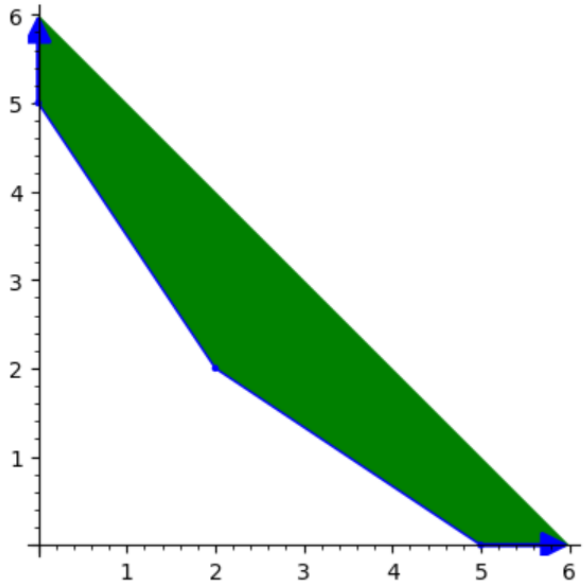


Figura 15. Caras de $\Gamma(g)$

```
z.give_info_newton(faces = True)
```

```
Newton's polyhedron of x^5 + y^5 + x^2*y^2:
        support points = [(5, 0), (0, 5), (2, 2)]
        vertices = [(0, 5), (2, 2), (5, 0)]
        number of proper faces = 7
        Facet 1: x >= 0
        Facet 2: 3*x + 2*y - 10 >= 0
        Facet 3: y >= 0
        Facet 4: 2*x + 3*y - 10 >= 0
Information about faces:
tau0: dim 0,  vertices = [(0, 5)],  rays = []

tau1: dim 1,  vertices = [(0, 5)],  rays = [(0, 1)]

tau2: dim 0,  vertices = [(2, 2)],  rays = []

tau3: dim 1,  vertices = [(0, 5), (2, 2)],  rays = []

tau4: dim 0,  vertices = [(5, 0)],  rays = []

tau5: dim 1,  vertices = [(5, 0)],  rays = [(1, 0)]

tau6: dim 1,  vertices = [(2, 2), (5, 0)],  rays = []
```

Figura 16. Partición cónica

```
z.cones_plot()
```

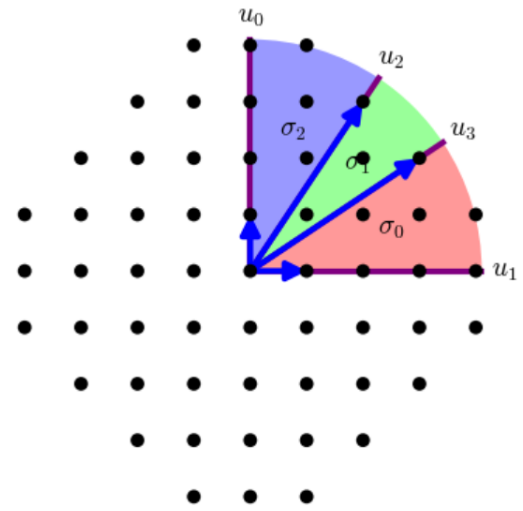


Figura 17. Conos de $\Gamma(g)$

```
z.give_info_newton(cones = True)
```

```
Newton's polyhedron of x^5 + y^5 + x^2*y^2:
        support points = [(5, 0), (0, 5), (2, 2)]
        vertices = [(0, 5), (2, 2), (5, 0)]
        number of proper faces = 7
        Facet 1: x >= 0
        Facet 2: 3*x + 2*y - 10 >= 0
        Facet 3: y >= 0
        Facet 4: 2*x + 3*y - 10 >= 0
Information about faces:
tau0: generators of cone = [(1, 0), (3, 2)], partition into simplicial cones = [[(1, 0), (3, 2)]]

tau1: generators of cone = [(1, 0)], partition into simplicial cones = [[(1, 0)]]

tau2: generators of cone = [(3, 2), (2, 3)], partition into simplicial cones = [[(3, 2), (2, 3)]]

tau3: generators of cone = [(3, 2)], partition into simplicial cones = [[(3, 2)]]

tau4: generators of cone = [(2, 3), (0, 1)], partition into simplicial cones = [[(2, 3), (0, 1)]]

tau5: generators of cone = [(0, 1)], partition into simplicial cones = [[(0, 1)]]

tau6: generators of cone = [(2, 3)], partition into simplicial cones = [[(2, 3)]]
```

Figura 18. $Z(s, g)$ para $p = 2$.

```
z.igusa_zeta(2)
```

```
(256*2^(10*s)*2^(5*s)*2^s - 128*2^(10*s)*2^(5*s) + 1536*2^(20*s)*2^s + 128*2^(1
6*s)*2^s + 32*2^(12*s)*2^s - 64*2^(10*s)*2^s + 8*2^(8*s)*2^s - 8*2^(5*s)*2^s +
2*2^(4*s)*2^s - 768*2^(20*s) - 64*2^(16*s) - 16*2^(12*s) + 48*2^(10*s) - 4*2^(8
*s) + 4*2^(5*s) - 2^(4*s) + 2^s - 1)/((32*2^(10*s) - 1)^2*(2*2^s - 1))
```

Figura 19. $Z(s, g)$ para $p = 7$.

```
z.igusa_zeta(7)
```

```
(69177612*7^(10*s)*7^(5*s)*7^(2*s) - 19765032*7^(10*s)*7^(5*s)*7^s + 1411788*7^
(10*s)*7^(5*s) + 12146435707*7^(20*s)*7^(2*s) + 207532836*7^(16*s)*7^(2*s) + 42
35364*7^(12*s)*7^(2*s) - 235298*7^(10*s)*7^(2*s) + 86436*7^(8*s)*7^(2*s) - 4116
*7^(5*s)*7^(2*s) + 1764*7^(4*s)*7^(2*s) - 2259801992*7^(20*s)*7^s - 59295096*7^
(16*s)*7^s - 1210104*7^(12*s)*7^s + 96040*7^(10*s)*7^s - 24696*7^(8*s)*7^s + 11
76*7^(5*s)*7^s - 504*7^(4*s)*7^s + 74942413*7^(20*s) + 4235364*7^(16*s) + 86436
*7^(12*s) - 8918*7^(10*s) + 1764*7^(8*s) - 84*7^(5*s) + 36*7^(4*s) + 7*7^(2*s)
- 8*7^s + 1)/((16807*7^(10*s) - 1)^2*(7*7^s - 1)^2)
```

BIBLIOGRAFÍA

ALBARRACÍN, A. y LEON E. “Igusa’s Local Zeta Functions and Exponential Sums for Arithmetically Non Degenerate Polynomials”. En: *Journal de Théorie des Nombres de Bordeaux* (2018) (vid. pág. 10).

DENEF, J. y HOORNAERT K. “Newton polyhedra and Igusa’s local zeta function”. En: *J. Number Theory 89* (2001) (vid. pág. 56).

HALMOS, P. *Measure Theory*. Van der Nostrand Reinhold Company, 1950, pág. 254 (vid. pág. 48).

IGUSA, J. *A Stationary phase formula for p- adic integrals and its applicationes*. Algebraic Geometry e its Applications, Springer-Verlag, 1994, págs. 175-194 (vid. pág. 9).

— *An introduction to the theory of local zeta functions*. Algebraic Geometry e its Applications,AMS/IP Studies in Advanced Mathe,atics, 2000 (vid. págs. 81, 86).

LEON, E. y ZÚÑIGA W. “An Introduction to the Theory of Local Zeta Functions from Scratch”. En: *Revista Integración, temas de matemáticas. Escuela de Matemáticas, Universidad Industrial de Santander* () (vid. pág. 12).

VIU SOS, J. “Funciones zeta y poliedros de Newton: Aspectos teóricos y computacionales”. Trabajo Fin de Master, Director: Enrique Artal Bartolo. Universidad Zaragoza, 2012 (vid. págs. 10, 12, 58).

VLADIMIROV, V., VOLOVICH I. y ZELENOV E. *p-adic Analysis and Mathematical Physics*. World Scientific Publishing Co., 1994 (vid. pág. 12).

ZÚÑIGA, W. “Local Zeta function and Newton Polyhedra”. En: *Japón, Nagoya Mathematical Journal ISSN: 0027-7630 ed: Cambridge University Press* 172 (2001), págs. 31-58 (vid. pág. 10).