

UNIVERSIDAD DE EL SALVADOR
FACULTAD DE CIENCIAS NATURALES Y MATEMÁTICA
ESCUELA DE MATEMÁTICA



*Números p -ádicos y aplicaciones en
álgebra, geometría y teoría de números.*

Presentado por:
Ricardo José Córdova Soriano

Para optar al grado de
Licenciado en Matemática

Bajo la dirección de
M.Sc. Gabriel Alexander Chicas Reyes

Ciudad Universitaria, marzo de 2023

UNIVERSIDAD DE EL SALVADOR

M.Sc. Roger Armando Arias
Rector

Dr. Raúl Ernesto Azcúnaga López
Vicerrector Académico

Ing. Juan Rosa Quintanilla
Vicerrector Administrativo

M.Sc. Francisco Antonio Alarcón Sandoval
Secretario General

Lic. Rafael Humberto Peña Marín
Fiscal General

Lic. Luis Antonio Mejía Lipe
Defensor de los Derechos Universitarios

FACULTAD DE CIENCIAS NATURALES Y MATEMÁTICA

Lic. Mauricio Hernán Lovo Córdoba
Decano

M.Sc. Zoila Virginia Guerrero Mendoza
Vicedecana

Lic. Jaime Humberto Salinas Espinoza
Secretario de Facultad

ESCUELA DE MATEMÁTICA

Dr. Dimas Noé Tejada Tejada
Director

M.Sc. Carlos Ernesto Gámez Rodríguez
Secretario


TRIBUNAL CALIFICADOR



M.Sc. Gabriel Alexander Chicas Reyes
Asesor de Tesis



M.Sc. María Cecilia Martínez Reyes
Jurado



Dr. Aarón Ernesto Ramírez Flores
Jurado

Agradecimientos

A mi madre Rosa Lilian, por ser mi apoyo incondicional y sin medida para lograr mis objetivos y metas.

A Daniela Claros, por brindarme su amistad y apoyo incondicional

A mis amigos y compañeros durante toda la carrera, por la fraternidad formada y el amor por las matemáticas en común.

A mi asesor y amigo: M.Sc. Gabriel Alexander Chicas Reyes, por la dedicación, por ser mi mentor y modelo a seguir y por los conocimientos que me ha transmitido a lo largo de la realización de este trabajo de graduación.

A mi jurado: Dr. Aarón Ernesto Ramírez Flores y M.Sc. María Cecilia Reyes, por la revisión y aportación de ideas para la realización de un buen trabajo.

Índice general

Agradecimientos	I
Índice general	II
Referencias	III
Resumen	IV
Introducción	V
1. Motivación: Teorema de Monsky	1
2. Números p-ádicos	6
2.1. Valor absoluto en \mathbb{Q}_p	6
2.2. Topología en \mathbb{Q}_p	8
2.3. Teorema de Ostrowski	15
2.4. Completación de \mathbb{Q}_p ($\mathbb{Q}_p, \cdot _p$)	20
2.5. Explorando \mathbb{Q}_p	21
3. Elementos básicos del análisis p-ádico	29
3.1. Sucesiones y series	29
3.2. Función logaritmo y exponencial	35
3.3. Series binomiales	40
4. Teorema de Mahler	42
4.1. Expansiones de Mahler	42
4.2. Demostración del teorema de Mahler	49
5. Aplicaciones del teorema de Mahler	57
5.1. Motivación	57
5.2. Ejemplos	59

6. Conclusiones	62
7. Proyectos a futuro	64
Referencias	65

Resumen

Córdova Soriano, Ricardo José. 2023. *Números p -ádicos y aplicaciones en álgebra, geometría y teoría de números*. Trabajo de graduación de Licenciatura en matemática. San Salvador, Universidad de El Salvador.

Los números p -ádicos fueron motivados por Kurt Hensel principalmente en un intento de llevar las ideas y técnicas de los métodos de las series de potencias a la teoría de números. Ahora, su influencia se extiende mucho más allá del propósito inicial, ya que posee una estructura analítica y algebraica que le da a este sistema numérico una gran utilidad, la cual se trata de exponer a lo largo de este trabajo.

Por consiguiente, esta tesis exhibe: el teorema de Monsky como motivación, definiciones básicas y construcción de los números p -ádicos, algunos aspectos del análisis de sucesiones y series p -ádicas, el teorema de Mahler para funciones continuas, y por último, una aplicación del teorema de Mahler, para calcular funciones p -ádicas ergódicas a través de los coeficientes de su serie de Mahler.

Palabras clave: número p -ádico, teorema de Monsky, serie de Mahler, sistemas dinámicos, función ergódica, análisis p -ádico.

Introducción

Los números p -ádicos fueron descubiertos por el alemán Kurt Hensel a finales del s. XIX en relación a la resolución de congruencias en teoría de números. Actualmente son una herramienta indispensable en la teoría de números moderna; como una muestra de su importancia, podemos mencionar su uso en la demostración de Andrew Wiles del último teorema de Fermat.

Para despertar nuestra motivación por el estudio de los números p -ádicos y sus propiedades, en el capítulo I, denominado *Motivación: Teorema de Monsky*, que describiremos en los párrafos siguientes, observaremos cómo naturalmente surge la necesidad de utilizar la *valoración 2-ádica*, como una herramienta de argumentación para su demostración. A continuación, veamos una breve descripción de dicho teorema.

Teorema de Monsky

El teorema de Monsky (debido al matemático estadounidense Paul Monsky), vino motivado por una pregunta planteada y postulada por Fred Richman y John Thomas en *The American Mathematical Monthly*.

¿Se puede dividir un cuadrado S en un número impar de triángulos T_i que no se superponen, todos de la misma área?

Se demostró que la respuesta es no, siempre que $S = [0, 1] \times [0, 1]$ y que las coordenadas de los vértices de T_i sean números racionales con denominadores impares. Más aún, probaremos que nunca se puede separar un cuadrado de esta manera pasando por algunos resultados que nos darán el soporte para argumentarlo.

Luego de motivarnos a estudiar los números p -ádicos, el capítulo II y III, se desarrollan los fundamentos de los números p -ádicos y análisis p -ádico. Definiremos la valoración p -ádica y el valor absoluto p -ádico, que da lugar a un sistema

numérico con propiedades un tanto inusuales, por ejemplo, la **propiedad no arquimediana**. Estas propiedades son de suma utilidad para abordar problemas aritméticos. Más aún, es posible desarrollar teorías análogas a aquellas desarrolladas sobre los números reales. De particular interés para nosotros es el *análisis p -ádico*, que esencialmente ofrece una alternativa al cálculo y teoría de funciones de variable real. Un primer objetivo de este trabajo es dar una introducción a algunos aspectos básicos del análisis p -ádico y la teoría de funciones de variable p -ádica.

Por otra parte, los capítulos IV y V fueron motivados gracias a la participación del autor en el evento *CIMPA SCHOOL MEXICO "P-Adic Numbers, Ultrametric Analysis, and Applications"*, Guanajuato, May 2022. Entre los diversos temas de investigación abordados, el minicurso "The p-adic Ergodic Theory" [1] del profesor ruso Vladimir Anashin influyó decisivamente en el rumbo del presente trabajo. Tal y como se verá en dichos capítulos, Anashin propone diversos métodos originales para detectar y estudiar funciones ergódicas de variable p -ádica.

Una de las herramientas más importantes en este estudio (y en el análisis p -ádico en general) es el teorema de Mahler, que se aborda en detalle en el capítulo IV:

Teorema de expansión de Mahler:

Este teorema consiste en una expansión en serie para funciones continuas de \mathbb{Z}_p en \mathbb{Q}_p .

En el caso real \mathbb{R} , la densidad de los polinomios en $C([0, 1], \mathbb{R})$ se debe a Weierstrass (1885). La densidad de los polinomios en $C(\mathbb{Z}_p, \mathbb{Q}_p)$ fue probada por primera vez por Dieudonne (1944). Si bien no hay una buena descripción de todas las funciones en $C([0, 1], \mathbb{R})$ (no se pueden describir como series de potencias, ya que las series de potencias son infinitamente derivables y una función continua no necesita ser diferenciable ni una sola vez en todas partes), en 1958 Mahler dio una muy buena descripción de todas las funciones en $C(\mathbb{Z}_p, \mathbb{Q}_p)$ usando series infinitas de polinomios especiales. El resultado será estudiado en el *teorema de expansión de Mahler*.

Para finalizar este trabajo, en el capítulo V se hablará sobre el teorema ergódico de Anashin, que describe las condiciones necesarias y suficientes para asegurar la ergodicidad de las funciones continuas de variable p -ádica, mediante la inspección de sus coeficientes en la expansión de Mahler.

Objetivo general.

- Promover y profundizar el estudio de los números p -ádicos como una herramienta fundamental en la teoría de números.
- Desarrollar elementos básicos del análisis p -ádico.
- Mostrar ejemplos de aplicación de los números p -ádicos dentro de diversas ramas de las matemáticas.

Objetivos específicos.

- Dar un tratamiento detallado de la teoría de las expansiones de Mahler.
- Mostrar interacción entre el análisis p -ádicos y los sistemas dinámicos y funciones ergódicas.

Capítulo 1

Motivación: Teorema de Monsky

El problema del que se hablará en este capítulo fue planteado por Fred Richman en el American Mathematical Monthly en 1965 y fue probado por Paul Monsky en 1970. Dice de la siguiente manera:

Teorema 1.0.1. [6] *No es posible dividir un cuadrado en un número impar de triángulos de igual área.*

Antes de ir directamente a la prueba, es importante mencionar que este teorema motivará nuestro estudio de los números p -ádicos, ya que en su demostración podremos observar una aplicación directa de la valuación p -ádica y el valor absoluto p -ádico que esta define.

Definición 1.0.2. *Sea p un primo fijo. La valuación p -ádica sobre \mathbb{Z} es la función*

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

definida así: para cada entero $n \in \mathbb{Z}, n \neq 0$, sea $v_p(n)$ el único entero positivo que satisface

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

Invocando el Teorema fundamental de la aritmética, observamos que $v_p(n) = 0$, cuando n no posee a p en su factorización prima.

Podemos extender v_p al campo de los racionales como sigue: si $x = a/b \in \mathbb{Q}^\times$, entonces

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

Donde por convención se toma $v_p(0) = +\infty$. De aquí es fácil ver que la valuación p -ádica para cada $x \in \mathbb{Q}^\times$ viene dada por la fórmula

$$x = p^{v_p(x)} \cdot \frac{a'}{b'}, \quad p \nmid a'b'.$$

Definición 1.0.3. A través de la valuación p -ádica definida, se puede construir el valor absoluto p -ádico, que viene dado por:

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

Extendemos esta definición a todo \mathbb{Q} , definimos $|0|_p = 0$.

Para ver más detalles sobre estas definiciones, véase el Capítulo II.

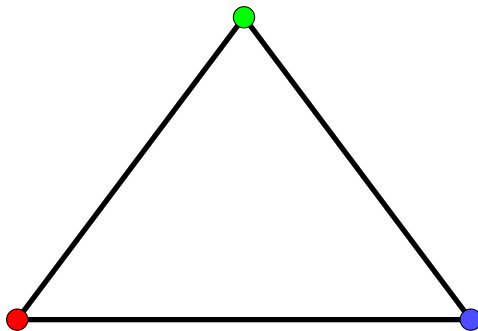
También utilizaremos un resultado de carácter combinatorio conocido como *Lema de Sperner*, el cual abordaremos luego de aclarar algunas notaciones.

- Sea P una región en el plano acotada por un polígono convexo P . Supongamos que P se divide en k triángulos T_i , con $i = 1, \dots, k$ disjuntos o no traslapados.
- Por vértice entenderemos que es un vértice de alguno de los k triángulo T_i .
- Por cara, entenderemos que es un lado de algún triángulo T_i o del polígono convexo P .
- Dos vértices son adyacentes si están sobre la misma cara y el segmento de línea que los une no contiene otro vértice.
- Un segmento básico será un segmento de línea que une dos vértices adyacentes.

Notemos que los límites o lados que crean a cada T_i es la unión de segmentos básicos no traslapados, de igual manera para la frontera de P .

Supongamos además que los vertices están divididos en tres conjuntos disjuntos llamados R , G y B (del inglés red-green-blue) que motivaremos posteriormente. Diremos que una cara o segmento básico es del tipo RB si tiene un vértice del tipo R y otro del tipo B .

Definición 1.0.4. Llamaremos *triángulo arcoiris* a un triángulo cuyos vértices son de colores distintos entre sí, es decir, uno R , uno G y uno B .



Lema 1.0.5 (Lema de Sperner en el plano). *Si dividimos un polígono convexo P en una cantidad finita de triángulos y el número de segmentos básicos RB en la frontera es impar, entonces el número de triángulos arcoiris es impar.*

Demostración. Llamemos Δ a cada triángulo formado en el polígono y sea n_Δ el número de aristas RB de Δ .

Sea S la suma de todos los n_Δ . Para comprender mejor lo que cuenta S , supongamos que tenemos dos triángulos internos Δ_1 y Δ_2 que compartan una arista RB , esta arista será contada dos veces en S , una vez por n_{Δ_1} y una vez por n_{Δ_2} . Pero si la arista RB es una cara o un segmento simple sobre la frontera de P , entonces será contada una sola vez. Luego:

$$S = \# \text{aristas } RB \text{ en frontera} + 2\# \text{aristas } RB \text{ internas.}$$

Por otro lado, vemos que de esta manera también estamos clasificando los tipos de triángulos formados en P , ya que S los cuenta así:

$$S = \#\Delta \text{ arcoiris} + 2\#\Delta(\text{RBB o RRB})$$

Por lo tanto como el $\#$ de aristas RB en P es impar, entonces el $\#$ de triángulos arcoiris es impar. ■

Como segundo paso para construir la prueba de nuestro teorema, probaremos que todo triángulo arcoiris tiene área con valor absoluto 2-ádico mayor a 1. Dividimos los puntos del plano en los tres grupos que mencionamos antes, asignando a cada grupo las siguientes restricciones:

$$(x, y) \in R \quad \text{si} \quad |x|_2 \geq |y|_2 \quad \text{y} \quad |x|_2 \geq 1$$

$$(x, y) \in G \quad \text{si} \quad |y|_2 > |x|_2 \quad \text{y} \quad |y|_2 \geq 1$$

$$(x, y) \in B \quad \text{si} \quad |x|_2 < 1 \quad \text{y} \quad |y|_2 < 1$$

Proposición 1.0.6. *Todo triángulo arcoiris con vértices $u \in R$, $v \in G$ y $w \in B$ con coordenadas racionales se puede trasladar a un triángulo arcoiris cuyo vértice en B es $(0,0)$, sustrayendo el vértice w .*

Demostración. Específicamente probaremos que $u - w \in R$, y $v - w \in G$.

Sean $u = (c, d) \in R$, $v = (e, f) \in G$ y $w = (a, b) \in B$. Es obvio que $w - w = (0,0) \in B$.

Sea $u - w = (c - a, d - b)$. Sabemos que $|c|_2 \geq 1$ y $|a|_2 < 1$, entonces $|c|_2 > |a|_2$. De esto tenemos que $|c - a|_2 = |c|_2 \geq 1$. Por otro lado

$$|c - a|_2 = |c|_2 \geq |d|_2 \geq |d - b|_2, \quad \text{cuando } |d|_2 \geq |b|_2$$

$$|c - a|_2 = |c|_2 \geq 1 > |b|_2 = |d - b|_2, \quad \text{cuando } |d|_2 < |b|_2$$

De aquí que $u - w \in R$.

Ahora bien, sea $v - w = (e - a, f - b)$. Sabemos que $|f|_2 \geq 1$ y $|b|_2 < 1$, de donde $|f|_2 > |b|_2$. De esto tenemos que $|f - b|_2 = |f|_2 \geq 1$. Por otro lado

$$|f - b|_2 = |f|_2 \geq |e|_2 \geq |e - a|_2, \quad \text{cuando } |e|_2 \geq |a|_2$$

$$|f - b|_2 = |f|_2 \geq 1 > |a|_2 = |e - a|_2, \quad \text{cuando } |e|_2 < |a|_2$$

Concluimos que $v - w \in G$. ■

Ya hemos probado que todo triángulo arcoiris se puede trasladar a otro con vértice en $(0,0)$. Por último, probaremos que este triángulo arcoiris Δ con vértice $(0,0) \in B$, $(c,d) \in R$ y $(e,f) \in G$ tiene área con valor absoluto 2-ádico mayor a 1.

Proposición 1.0.7. [6] *Todo triángulo arcoiris tiene área 2-ádica mayor a 1.*

Demostración. Recordemos que el área A_Δ de este triángulo viene dada de la siguiente manera.

$$A_\Delta = \frac{1}{2}(cf - ed).$$

Observamos que como $|c|_2 \geq |d|_2$ y $|f|_2 \geq |e|_2$, entonces $|cf|_2 \geq |ed|_2$. De aquí que

$$|A_\Delta|_2 = \left| \frac{1}{2} \right|_2 |cf - ed|_2 = \left| \frac{1}{2} \right|_2 |cf|_2 = \left| \frac{1}{2} \right|_2 |c|_2 |f|_2 > 1.$$

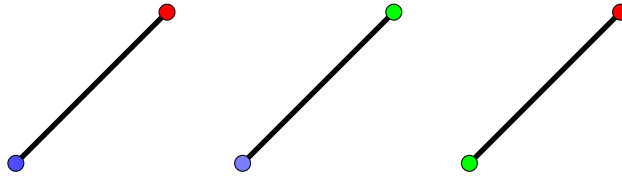
Con esto hemos demostrado que todo triángulo arcoiris posee área con valor absoluto 2-ádico mayor a 1. ■

Por último, probaremos el siguiente lema.

Lema 1.0.8. [6] *Una línea recta L no puede contener los tres tipos de puntos.*

Demostración. Supongamos que L contiene los tres tipos de puntos. Mediante una traslación de un punto del tipo B sobre L al origen, podemos asumir que $(0,0) \in L$; entonces esta línea recta es definida por una ecuación lineal de la forma $L : y = \alpha x$, con $\alpha \in \mathbb{R}$.

Sean $(c,d) \in R$ y $(e,f) \in G$ sobre L . Sabemos que $|c|_2 \geq |d|_2$ y $|f|_2 \geq |e|_2$, entonces $|cf|_2 > |ed|_2$. Pero esto es una contradicción, ya que ambos puntos cumplen con la ecuación de la recta y de esto tenemos que $cf = ed$.



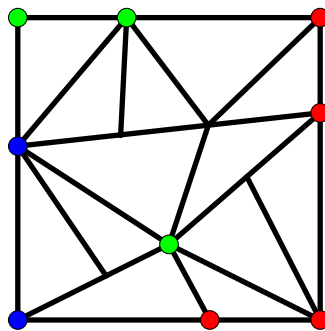
■

Ahora ya tenemos todos los ingredientes necesarios para justificar la demostración de nuestro teorema principal, a continuación.

Demostración. Sea el cuadrado $S = [0,1] \times [0,1]$, se divide en k triángulos Δ_i con área igual a $1/k$ cada uno. Observamos al conjunto que pertenece cada uno de sus vértices de S : $(0,0) \in B$, $(1,0) \in R$, $(1,1) \in R$ y $(0,1) \in G$. Vemos que solo hay un segmento simple del tipo RB que es el segmento que une los vértices $(0,0)$ y $(1,0)$, entonces por el lema de Sperner, tenemos que hay al menos un triángulo arcoiris, digamos Δ , y aplicando lo demostrado anteriormente, tenemos que:

$$|A_\Delta|_2 = |1/k|_2 > 1$$

Por lo tanto, k es par y con esto demostramos que el cuadrado solo puede ser dividido en un número par de triángulos de igual área. ■



Capítulo 2

Números p -ádicos

2.1. Valor absoluto en \mathbb{Q}_p

Para obtener los números p -ádicos, necesitamos iniciar con el campo de racionales \mathbb{Q} . Tratando de cimentar una teoría clara para el lector, primero recordaremos la definición de valor absoluto para un campo \mathbb{K} general.

Definición 2.1.1. [5] *Un valor absoluto en \mathbb{K} es una función $|\cdot| : \mathbb{K} \rightarrow \mathbb{R}_+$, que satisface las siguientes condiciones:*

- i). $|x| = 0$ si y sólo si $x = 0$;
- ii). $|xy| = |x||y|$, para todo $x, y \in \mathbb{K}$;
- iii). $|x + y| \leq |x| + |y|$, para todo $x, y \in \mathbb{K}$;

Diremos que un valor absoluto sobre \mathbb{K} es no arquimediano si satisface la condición adicional:

- iv). $|x + y| \leq \max\{|x|, |y|\}$, para todo $x, y \in \mathbb{K}$

de lo contrario, diremos que el valor absoluto es arquimediano.

Notamos que la condición no arquimediana [iv] implica a la desigualdad triangular [iii] ya que $\max\{|x|, |y|\}$ es menor o igual que $|x| + |y|$.

Tomando $\mathbb{K} = \mathbb{Q}$, y eligiendo un primo $p \in \mathbb{Z}$. Todo entero $n \in \mathbb{Z}$ se puede escribir como $n = p^{v_p(n)}n'$, con $p \nmid n'$, y esta representación es única. Dado que v está determinado por p y n , tiene sentido definir una función v_p como $v_p(n) = v$, de modo que $v_p(n)$ es sólo la multiplicidad de p como divisor de n . Formalmente:

Definición 2.1.2. [5] Para un primo fijo $p \in \mathbb{Z}$. La valuación p -ádica sobre \mathbb{Z} es la función

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

Definida así: para cada entero $n \in \mathbb{Z}$, $n \neq 0$, sea $v_p(n)$ el único entero positivo que satisface

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

Podemos extender v_p al campo de los racionales como sigue: si $x = a/b \in \mathbb{Q}^\times$, entonces

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

Donde por convención se toma $v_p(0) = +\infty$. De aquí es fácil ver que la valuación p -ádica para cada $x \in \mathbb{Q}^\times$ viene dada por la fórmula

$$x = p^{v_p(x)} \cdot \frac{a'}{b'}, \quad p \nmid a'b'.$$

Las propiedades básicas de la valuación p -ádica son las siguientes:

Lema 2.1.3. [5] para todo x e $y \in \mathbb{Q}$, tenemos

- I). $v_p(xy) = v_p(x) + v_p(y)$,
- II). $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$,

recordando que por convención se toma $v_p(0) = +\infty$.

Demostración.

- I). Sean $x = p^{v_p(x)}n$ y $y = p^{v_p(y)}n'$ donde por definición $p \nmid nn'$. Vemos que

$$xy = p^{v_p(x)}np^{v_p(y)}n' = p^{v_p(x)+v_p(y)}nn' \quad \text{donde } p \nmid nn'$$

De aquí que $v_p(xy) = v_p(x) + v_p(y)$.

- II). Supongamos que $v_p(x) < v_p(y)$, entonces

$$v_p(x + y) = v_p(x) \geq \min\{v_p(x), v_p(y)\}$$

Se logra la igualdad cuando alguno de los elementos es idénticamente 0. ■

Definición 2.1.4. [5] Para todo $x \in \mathbb{Q}$ no nulo, definimos el valor absoluto p -ádico de x como

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

Extendemos esta definición a todo \mathbb{Q} , definimos $|0|_p = 0$.

Proposición 2.1.5. [5] La función $|\cdot|_p$ es un valor absoluto no arquimediano.

Demostración.

- Por definición sabemos que $|x|_p = p^{-v_p(x)} > 0$.
- $|x|_p = p^{-v_p(x)} = \frac{1}{p^{v_p(x)}} = 0 \Leftrightarrow v_p(x) = \infty \Leftrightarrow x = 0$
- $|x| \cdot |y| = p^{-v_p(x)} p^{-v_p(y)} = p^{-(v_p(x)+v_p(y))} = |xy|_p$
- Sin pérdida de generalidad, supongamos que

$$\begin{aligned} |x|_p \geq |y|_p \\ p^{-v_p(x)} \geq p^{-v_p(y)} \Rightarrow v_p(y) \geq v_p(x) \Rightarrow \min\{v_p(x), v_p(y)\} = v_p(x) \end{aligned} \quad (2.1)$$

De esto y la definición de valuación, tenemos que

$$\begin{aligned} v_p(x+y) &\geq v_p(x) \\ -v_p(x+y) &\leq -v_p(x) \\ p^{-v_p(x+y)} &\leq p^{-v_p(x)} \\ |x+y|_p &\leq |x|_p = \max\{|x|_p, |y|_p\} \end{aligned}$$

■

Hemos comprobado que la función $|\cdot|_p$ es un valor absoluto, por lo tanto cumple con todas las propiedades clásicas de un valor absoluto y además es no aequimediano. Lo llamamos valor absoluto p -ádico.

2.2. Topología en Q_p

Ahora hablaremos un poco sobre la topología que envuelve al campo de los números p -ádicos. Para ello, definiremos la distancia entre dos números cualesquiera a través de la noción de “tamaño” que hemos adquirido al definir el valor absoluto p -ádico. Teniendo una métrica, podremos definir conjuntos abiertos y cerrados y con esto la topología p -ádica.

Definición 2.2.1. [5] Sea \mathbb{K} un campo y sea $|\cdot|$ un valor absoluto sobre \mathbb{K} . Definimos la función distancia entre dos elementos $x, y \in \mathbb{K}$ por

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

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

El hecho de que un valor absoluto no sea arquimediano también se puede expresar en términos de la métrica:

Lema 2.2.2. [5] Sea $|\cdot|$ un valor absoluto definido en un campo \mathbb{K} y definimos una métrica por $d(x, y) = |x - y|$. Entonces $|\cdot|$ es no arquimediano si y sólo si para todo $x, y, z \in \mathbb{K}$ tenemos

$$d(x, y) \leq \max\{d(x, z), d(z, y)\}.$$

Demostración. Sabemos que $|a + b| \leq \max\{|a|, |b|\}$, para todo $a, b \in \mathbb{K}$. Tomando $a = x - z, b = z - y$,

$$\begin{aligned} |x - z + z - y| &\leq \max\{|x - z|, |z - y|\} \\ |x - y| = d(x, y) &\leq \max\{d(x, z), d(z, y)\} \end{aligned}$$

recíprocamente, tomando $y = -y_1$ y $z = 0$ y utilizando la hipótesis, tenemos

$$\begin{aligned} |x - (-y_1)| &\leq \max\{|x - 0|, |0 - (-y_1)|\} \\ |x + y_1| &\leq \max\{|x|, |y_1|\} \end{aligned}$$

■

Esta desigualdad se conoce como “desigualdad ultramétrica” y una métrica para la cual siempre se cumple es llamada “ultramétrica”. Un espacio con ultramétrica es llamado un “espacio ultramétrico”.

Al ser $|\cdot|_p$ un valor absoluto no arquimediano, los siguientes resultados son válidos para el campo de los números p -ádicos \mathbb{Q}_p con respecto a dicho valor absoluto.

Proposición 2.2.3. [5] Sea \mathbb{K} un campo y sea $|\cdot|$ un valor absoluto no arquimediano sobre \mathbb{K} . Si $x, y \in \mathbb{K}$ y $|x| \neq |y|$, entonces

$$|x + y| = \max\{|x|, |y|\}.$$

Demostración. Sin pérdida de generalidad supongamos que $|x| > |y|$. Entonces, sabemos que

$$|x + y| \leq \max\{|x|, |y|\} = |x|$$

Por otro lado, observamos que $x = (x + y) - y$. Utilizando la equivalencia del lema anterior con $z=0$:

$$|x| = |(x + y) - y| = d(x + y, y) \leq \max\{d(x + y, 0), d(y, 0)\} = \max\{|x + y|, |y|\}.$$

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

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

De esto obtenemos la otra desigualdad $|x| \leq |x + y|$, y concluimos la igualdad $|x| = |x + y|$. ■

Corolario 2.2.4. [5] *En un espacio ultramétrico todos los triángulos son isósceles.*

Demostración. Sean x, y, z tres elementos de nuestro espacio ultramétrico (los vértices de un triángulo). Las longitudes de sus lados son $d(x, y) = |x - y|$, $d(y, z) = |y - z|$ y $d(x, z) = |x - z|$.

Sin pérdida de generalidad, supongamos que $|x - y| \neq |y - z|$ y $|x - y| > |y - z|$ (dos lados del triángulo son distintos). Entonces, invocando la proposición anterior, tenemos que $|x - z| = |(x - y) + (y - z)| = \text{máx}\{|x - y|, |y - z|\} = |x - y|$. ■

En los espacios métricos, más importantes que los triángulos son las “bolas” o “discos”. Estos también resultan ser bastante extraños en el caso de un ultramétrico.

Definición 2.2.5. [5] *Sea \mathbb{K} un campo con valor absoluto $|\cdot|$. Sea $a \in \mathbb{K}$ y $r \in \mathbb{R}_+$. La bola abierta de radio r y centro a es el conjunto*

$$B(a, r) = \{x \in \mathbb{K} : d(x, a) < r\} = \{x \in \mathbb{K} : |x - a| < r\}.$$

La bola cerrada de centro a y radio r es el conjunto

$$\bar{B}(a, r) = \{x \in \mathbb{K} : d(x, a) \leq r\} = \{x \in \mathbb{K} : |x - a| \leq r\}.$$

Estas definiciones son clásicas a la hora de hablar de un espacio métrico. Las bolas abiertas son prototipos de conjuntos abiertos y las bolas cerradas son prototipos de los conjuntos cerrados. Para tener claro de lo que se está hablando, recordamos las definiciones de conjuntos abiertos y cerrados.

Definición 2.2.6. [5] *Un conjunto U es abierto si todo elemento $x \in U$ es el centro de una bola abierta completamente contenida dentro de U .*

Definición 2.2.7. [5] *Un conjunto S es cerrado si su complemento es un conjunto abierto.*

Recordemos que para todo valor absoluto (arquimediano o no), las bolas abiertas son siempre conjuntos abiertos y las bolas cerradas son siempre conjuntos cerrados.

Para valores absolutos no arquimedianos, se tienen las siguientes propiedades:

Proposición 2.2.8. [5] Sea \mathbb{K} un campo con un valor absoluto no arquimediano.

- I). Si $b \in B(a, r)$, entonces $B(a, r) = B(b, r)$; en otras palabras todo punto contenido dentro de la bola abierta es también centro de dicha bola abierta.
- II). Si $b \in \bar{B}(a, r)$, entonces $\bar{B}(a, r) = \bar{B}(b, r)$; en otras palabras todo punto contenido dentro de la bola cerrada es también centro de dicha bola cerrada.
- III). El conjunto $B(a, r)$ es abierto y cerrado. $B(a, r)$ tiene frontera vacía.
- IV). Si $r \neq 0$, el conjunto $\bar{B}(a, r)$ es abierto y cerrado y tiene frontera vacía.
- V). Si $a, b \in \mathbb{K}$ y $r, s \in \mathbb{R}_+^\times$, tenemos que $B(a, r) \cap B(b, s) \neq \emptyset$ si y sólo si $B(a, r) \subset B(b, s)$ o $B(a, r) \supset B(b, s)$; en otras palabras, dos bolas abiertas cualesquiera son ambas disjuntas o está contenida una dentro de la otra.
- VI). Si $a, b \in \mathbb{K}$ y $r, s \in \mathbb{R}_+^\times$, tenemos que $\bar{B}(a, r) \cap \bar{B}(b, s) \neq \emptyset$ si y sólo si $\bar{B}(a, r) \subset \bar{B}(b, s)$ o $\bar{B}(a, r) \supset \bar{B}(b, s)$; en otras palabras, dos bolas cerradas cualesquiera son ambas disjuntas o está contenida una dentro de la otra.

Demostración.

- I). Por definición, $b \in B(a, r)$ si y sólo si $|b - a| < r$. Ahora, tomando un $x \in B(a, r)$, por la propiedad no arquimediana tenemos que

$$|x - b| \leq \max\{|x - a|, |b - a|\} < r,$$

entonces $x \in B(b, r)$, es decir, $B(a, r) \subset B(b, r)$.

Por otro lado, tomando un $x \in B(b, r)$, por la propiedad no arquimediana tenemos que

$$|x - a| \leq \max\{|x - b|, |b - a|\} < r,$$

entonces $x \in B(a, r)$, es decir, $B(b, r) \subset B(a, r)$. De aquí que $B(a, r) = B(b, r)$.

- II). Reemplazando $<$ por \leq en la proof de I).
- III). En (I) probamos que $\forall x \in B(a, r)$ tenemos que $B(x, r) = B(a, r)$ y en particular $B(x, r) \subset B(a, r)$. Por lo tanto $B(a, r)$ es abierta.

Por otro lado, para probar que $B(a, r)$ es cerrada, tomamos el complemento, digamos

$$C = \{x \in \mathbb{K} : d(x, a) \geq r\}$$

y probaremos que es abierto. Sea $y \in C$, entonces $|y - a| \geq r$. Hacemos una bola abierta $B(y, s)$ tal que $s < r$. Sea $z \in B(y, s)$, de aquí tenemos $|y - z| < s < r \leq |y - a|$, recordamos que todos los triángulos son isósceles, entonces

$$|z - a| = \max\{|y - z|, |y - a|\} = |y - a| \geq r$$

es decir que $z \in C$. Entonces $B(y, s) \subset C$ y por lo tanto C es un conjunto abierto y su complemento $B(a, r)$ es cerrado.

Por último, supongamos que $x \in B(a, r)$ es un punto límite y sea $B(x, s)$ con $s < r$. Por definición de punto límite, $B(x, s)$ contiene punto tanto de $B(a, r)$ como de su complemento C , pero eso significa que x también es un punto límite de C . Recordamos que ambos conjuntos $B(a, r)$ y C son cerrados, concluimos que cualquier punto límite debe pertenecer a $B(a, r) \cap C = \emptyset$.

- iv). Sea $b \in \bar{B}(a, r)$. Sea $B(b, r)$ y sea $y \in B(b, r)$, entonces por triángulos isósceles tenemos

$$d(y, a) = \max\{|y - b|, |b - a|\} \leq r$$

es decir que $y \in \bar{B}(a, r)$, entonces $B(b, r) \subseteq \bar{B}(a, r)$, por tanto $\bar{B}(a, r)$ es abierta.

Por otro lado, sea $C = \{x \in \mathbb{K} : d(x, a) > r\}$ el complemento de $\bar{B}(a, r)$. Sea $x \in C$, entonces $|x - a| > r$. Hacemos una bola abierta $B(x, s)$ con $s < r$. Sea $y \in B(x, s)$, de aquí tenemos que $|x - y| < s < r < |x - a|$. Por triángulos isósceles tenemos que

$$|y - a| = \max\{|x - y|, |x - a|\} = |x - a| > r.$$

Es decir que $y \in C$, entonces $B(x, s) \subset C$, por lo tanto C es abierto $\bar{B}(a, r)$ es cerrada.

- v). Sin pérdida de generalidad asumamos que $r \leq s$. Sabemos $B(a, r) \cap B(b, s) \neq \emptyset$. Sea $c \in B(a, r) \cup B(b, s)$, por I) sabemos que $B(a, r) = B(c, r)$ y $B(b, s) = B(c, s)$. Por tanto

$$B(a, r) = B(c, r) \subset B(c, s) = B(b, s).$$

Se logra la inclusión contraria si al principio asumimos que $s \leq r$.

Para el converso, si $B(a, r) \subset B(b, s)$ o $B(a, r) \supset B(b, s)$, es claro que $B(a, r) \cap B(b, s) \neq \emptyset$.

vi). Sin pérdida de generalidad asumamos que $r \leq s$. Sabemos $\bar{B}(a, r) \cap \bar{B}(b, s) \neq \emptyset$. Sea $c \in \bar{B}(a, r) \cup \bar{B}(b, s)$, por II) sabemos que $\bar{B}(a, r) = \bar{B}(c, r)$ y $\bar{B}(b, s) = \bar{B}(c, s)$. Por tanto

$$\bar{B}(a, r) = \bar{B}(c, r) \subset \bar{B}(c, s) = \bar{B}(b, s).$$

Se logra la inclusión contraria si al principio asumimos que $s \leq r$.

Para el converso, si $\bar{B}(a, r) \subset \bar{B}(b, s)$ o $\bar{B}(a, r) \supset \bar{B}(b, s)$, es claro que $\bar{B}(a, r) \cap \bar{B}(b, s) \neq \emptyset$.

■

La geometría de las bolas en un espacio ultramétrico parece muy extraña a primera vista; tener una buena sensación de ello puede ser el paso inicial más importante hacia la comprensión del valor absoluto p -ádico.

Los conjuntos que son abiertos y cerrados son bastante raros en el cálculo habitual, pero son muy comunes cuando se trata de valores absolutos no arquimedianos (como \mathbb{Q} dotado de $|\cdot|_p$). Así que les damos un nombre.

Definición 2.2.9. [5] Sea \mathbb{K} un campo con un valor absoluto $|\cdot|$ (o más generalmente, un espacio métrico). Decimos que un conjunto $S \subset \mathbb{K}$ es “clopen” si y sólo si es abierto y cerrado a la vez.

El hecho de que haya tantos conjuntos clopen alrededor hace que la topología de los campos con valoraciones no arquimedianas sea bastante extraña. Por ejemplo, un conjunto S se llama disconexo si se pueden encontrar dos conjuntos abiertos U_1 y U_2 tales que

- $S = (S \cap U_1) \cup (S \cap U_2)$,
- $(S \cap U_1) \cup (S \cap U_2) \neq \emptyset$,
- ni $S \cap U_1$ ni $S \cap U_2$ son vacíos.

La idea, es que tal S se compone de dos “piezas” (a saber, las intersecciones con cada uno de los conjuntos abiertos). Los conjuntos que no se pueden dividir de esta manera se denominan conexos.

Ahora, estudiamos algunos aspectos de las componentes conexas en el caso no arquimediano, para observar la diferencia extrema que hay con el caso arquimediano que utilizamos normalmente.

Proposición 2.2.10. *En un campo \mathbb{K} con un valor absoluto no arquimediano, la componente conexa de un punto $x \in \mathbb{K}$ es el conjunto $\{x\}$ que es unipuntual.*

Demostración. Supongamos $a, b \in C(x)$, donde $C(x)$ es la componente conexa de x . Sea $d(a, b) = r$ y sea $U_1 = B(a, r/2)$ y su complemento $U_2 = C_{C(x)}(U_1)$, recordamos que tanto U_1 como U_2 son abiertos.

Sean $A = C(x) \cap U_1$ y $B = C(x) \cap U_2$. Vemos que

- $C(x) = A \cup B$.
- $A \cap B = \emptyset$
- $A \neq \emptyset \neq B \quad (a \in A, b \in B)$

Hemos probado que la componente conexa de x es desconexa, lo cual es una contradicción. ■

Corolario 2.2.11. [5] *Si \mathbb{K} es un campo con un valor absoluto no arquimediano y \mathbb{R} con el valor absoluto usual entonces no existen funciones no constantes continuas de $\mathbb{R} \rightarrow \mathbb{K}$.*

Demostración. Recordamos que la imagen de un conjunto conexo bajo una función continua f es conexa, al ser \mathbb{R} un campo conexo cumple que su imagen es conexa. Aplicando la proposición anterior, vemos que al ser $f(\mathbb{R})$ conexa, entonces debe ser unipuntual. ■

Por otro lado, a continuación describiremos la relación entre los valores absolutos no arquimedianos y la estructura algebraica del campo subyacente. Estas conexiones resultan ser bastante fuertes. De hecho, apuntan a una estrecha relación entre las propiedades geométricas y algebraicas de tales campos. El mensaje principal es que la estrecha conexión entre el valor absoluto p -ádico y el número primo p es en realidad típica de los campos con valores no arquimedianos. Para empezar, cada valor absoluto no arquimediano se adjunta a un subanillo del campo \mathbb{K} , y este subanillo tiene algunas propiedades bastante agradables:

Proposición 2.2.12. [5] *Sea \mathbb{K} un campo, y sea $|\cdot|$ un valor absoluto no arquimediano sobre \mathbb{K} . El conjunto*

$$\mathcal{O} = \overline{B}(0, 1) = \{x \in \mathbb{K} : |x| \leq 1\}.$$

Es un subanillo de \mathbb{K} . Y el conjunto

$$\mathfrak{P} = B(0, 1) = \{x \in \mathbb{K} : |x| < 1\}$$

es un ideal de \mathcal{O} . Por tanto \mathfrak{P} es un ideal maximal en \mathcal{O} , y todo elemento del complemento $\mathcal{O} - \mathfrak{P}$ es invertible en \mathcal{O}

Se puede demostrar que \mathfrak{P} es el único ideal maximal en \mathcal{O} , lo que lo convierte en un anillo local.

Al anillo \mathcal{O} se le denomina **anillo de valuación** de $|\cdot|$. Al ideal \mathfrak{P} **ideal de valuación** de $|\cdot|$ y al cociente $k = \mathcal{O}/\mathfrak{P}$, es llamado **campo de residuos** de $|\cdot|$.

Proposición 2.2.13. Sea \mathbb{Q} con el valor absoluto p -ádico $|\cdot|_p$. Entonces:

- i). El anillo de valuación asociado es $\mathcal{O} = \mathbb{Z}_{(p)} = \{a/b \in \mathbb{Q} : p \nmid b\}$;
- ii). La valuación ideal es $\mathfrak{P} = p\mathbb{Z}_{(p)} = \{a/b \in \mathbb{Q} : p \nmid b \text{ y } p|a\}$;
- iii). el campo de residuos $k = \mathbb{F}_p$ (el campo con p elementos).

2.3. Teorema de Ostrowski

A partir de este punto, justificaremos algo sorprendente. Ya hemos encontrado algunos ejemplos de valores absolutos en el campo \mathbb{Q} de los números racionales. El siguiente paso será demostrar que estos son esencialmente todos los valores absolutos posibles; para eso necesitaremos introducir una noción refinada de lo que significa que dos valores absolutos sean "iguales". Hasta esa noción de equivalencia, podremos demostrar que los valores absolutos que tenemos son la lista completa de posibles valores absolutos en \mathbb{Q} .

Primero debemos hacer una buena definición de cuando dos valores absolutos son "iguales". La idea principal aquí es que usamos valores absolutos en un campo \mathbb{K} para introducir una topología (conjuntos abiertos y cerrados, conectividad, etc.) en \mathbb{K} . Por lo tanto, es razonable definir:

Definición 2.3.1. [5] Dos valores absolutos $|\cdot|_1$ y $|\cdot|_2$ sobre un campo \mathbb{K} son llamados equivalentes si ambos definen la misma topología sobre \mathbb{K} .

Lema 2.3.2. [5] Sea \mathbb{K} un campo con valor absoluto $|\cdot|$. Las siguientes condiciones son equivalentes

- i). $\lim_{n \rightarrow \infty} x_n = a$.

ii). Cualquier conjunto abierto que contenga a a también contiene todos, salvo muchos de los x_n .

Demostración. Sea $a \in U$, con U un conjunto abierto. Como U es abierto, existe r tal que $B(a, r) \subset U$. Por tanto existe N tal que $|x_n - a| < r$ para todo $n \geq N$. De aquí que a partir de algún n , todos los elementos $x_n \in B(a, r) \subset U$.

Para el recíproco, sea $B(a, \varepsilon)$ y sabemos que existe un N tal que todos salvo un número finito de elementos de $x_n \in B(a, \varepsilon)$. Por tanto, Para todo ε y N tal que para $n \geq N$ implica que $|x_n - a| < \varepsilon$, es decir $\lim_{n \rightarrow \infty} x_n = a$.

■

Proposición 2.3.3. [5] Sean valores absolutos $|\cdot|_1$ y $|\cdot|_2$ sobre un campo \mathbb{K} . Las siguientes condiciones son equivalentes

- i). $|\cdot|_1$ y $|\cdot|_2$ son equivalentes.
- ii). Para toda secuencia $(x_n) \subset \mathbb{K}$ tenemos $x_n \rightarrow a$ con respecto de $|\cdot|_1$ si y sólo si $x_n \rightarrow a$ con respecto de $|\cdot|_2$.
- iii). Para todo $x \in \mathbb{K}$ tenemos que $|x|_1 < 1$ si y sólo si $|x|_2 < 1$.
- iv). Existe un número real positivo α tal que para todo $x \in \mathbb{K}$, tenemos $|x|_1 = |x|_2^\alpha$

Con los resultados antes mencionados, ya tenemos los fundamentos necesarios para enunciar el siguiente teorema, el cual es muy importante en la teoría de los números p -ádicos.

Teorema 2.3.4. [5][Ostrowski.] Todo valor absoluto no trivial sobre \mathbb{Q} es equivalente a uno de los valores absolutos $|\cdot|_p$, donde cada p es un número primo o $p = \infty$.

Demostración.

- a. Supongamos que $|\cdot|$ es un valor absoluto arquimediano no trivial. Veremos que es equivalente al valor absoluto usual.

Sea n_0 el entero más pequeño que cumple $|n_0| > 1$. Podemos ver que

$$|n_0| = n_0^\alpha \iff \alpha = \frac{\log |n_0|}{\log n_0}$$

Probaremos que ese α nos permite ver que cualquier valor absoluto arquimediano es equivalente a $|\cdot|_\infty$, es decir, veremos que para $x \in \mathbb{Q}$, $|x| = |x|_\infty^\alpha$

Por propiedades de valor absoluto, sabemos que solo basta probar esto para los enteros positivos, es decir que $|n| = n^\alpha$, para todo entero positivo n .

Sabemos que funciona para $n = n_0$. Ahora, sea $n \in \mathbb{Z}$ arbitrario, y lo escribimos en base n_0 , es decir

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

con $0 \leq a_i \leq n_0 - 1$ y $a_k \neq 0$. Notamos que k está determinado por la desigualdad $n_0^k \leq n \leq n_0^{k+1}$, de donde vemos que

$$k = \left\lfloor \frac{\log n}{\log n_0} \right\rfloor.$$

Ahora, tomando valores absolutos, tenemos

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

Recordamos que tomamos a n_0 tal que sea el entero más pequeño que tiene valor absoluto mayor que 1, de aquí que $|a_i| \leq 1$, entonces tenemos que

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

Llamando $C = n_0^\alpha / (n_0^\alpha - 1) > 0$, podemos decir que

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

Esta fórmula aplica para todo n ; aplicándola a un entero de la fórmula n^N , para un N arbitrario, tenemos que

$$|n^N| \leq C n^{N\alpha}$$

Tomando raíz N – esima, tenemos

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

Como es para un N arbitrario, tomamos $N \rightarrow \infty$, donde $\sqrt[N]{C} \rightarrow 1$, y de aquí tenemos que $|n| \leq n^\alpha$. Ya tenemos una desigualdad.

Por otro lado, recordemos la expansión de n en base n_0

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

sabemos que $n_0^{k+1} > n > n_0^k$, tenemos

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

de aquí

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

Además, recordando que $n_0^{k+1} > n$, tenemos que

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

Hemos tomado $C' = 1 - (1 - 1/n_0)^\alpha > 0$ y no depende de n .

Nuevamente utilizando esta desigualdad para n^N , con N arbitrario, tenemos

$$|n^N| > C' n^{N\alpha}$$

Tomando raíz N – esima, tenemos

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

Como es para un N arbitrario, tomamos $N \rightarrow \infty$, donde $\sqrt[N]{C'} \rightarrow 1$, y de aquí tenemos que $|n| > n^\alpha$. De ambas desigualdades concluimos que $|n| = n^\alpha$. Esto prueba que el valor absoluto $|\cdot|$ es equivalente al valor absoluto usual $|\cdot|_\infty$.

- b. Ahora supongamos que $|\cdot|$ es no arquimediano. Por propiedades de valor absoluto no arquimediano sabemos que $|n| < 1$ para todo número entero n . Al ser $|\cdot|$ no trivial, podemos encontrar el menor entero n_0 tal que $|n_0| < 1$.

Supongamos que $n_0 = ab$, donde sabemos que a y b son menores que n_0 , entonces por la elección de n_0 , vemos que $|a| = |b| = 1$ y $|ab| = |n_0| < 1$, esto no puede ser. De aquí que n_0 debe ser un número primo, digamos $n_0 = p$. Probaremos que este valor absoluto debe ser equivalente al valor absoluto p -ádico, donde $p = n_0$.

A continuación verificaremos que si $n \in \mathbb{Z}$ no es divisible por p , entonces $|n| = 1$.

Si dividimos a n por p , tendremos un residuo, es decir

$$n = rp + s$$

con $0 < s < p$. Por la minimalidad de p , tenemos que $|s| = 1$. También tenemos que $|rp| < 1$, ya que $|r| \leq 1$. Ahora, por la propiedad de triángulos isósceles en espacios no arquimedianos, tenemos que $n = 1$.

Finalmente, sea $n \in \mathbb{Z}$, lo escribimos como $n = p^v n'$ con $p \nmid n'$. Entonces

$$|n| = |p|^v |n'| = |p|^v = c^{-v}$$

Donde $c = |p|^{-1} > 1$, entonces $|\cdot|$ es equivalente a el valor absoluto p -ádico. ■

Ejemplo 2.3.5. [5] Sea $|x| = c^{-v_p(x)}$ un valor absoluto no arquimediano, donde $c > 1$ es un número real. Vemos que este valor absoluto es equivalente al p -ádico que eligiendo α tal que $c^\alpha = p$, tenemos que

$$|x|_p = p^{-v(x)} = (c^{-v_p(x)})^\alpha = |x|^\alpha.$$

Como consecuencia de este teorema, enunciamos el siguiente resultado.

Proposición 2.3.6. [5][fórmula del producto.] Para todo $x \in \mathbb{Q}^\times$, tenemos

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

donde $p \leq \infty$ significa que tomamos el producto sobre todos los números primos de \mathbb{Q} , incluyendo el "primo en el infinito".

Demostración. Por propiedades del valor absoluto p -ádico, solo basta probar la fórmula para números enteros positivos, el caso general se sigue de él. Sea $x \in \mathbb{Z}$ positivo, entonces $x = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$. Entonces el resultado se sigue de:

$$\begin{cases} |x|_q = 1 & \text{si } q \neq p_i \\ |x|_{p_i} = p_i^{-a_i} & \text{para } i = 1, 2, \dots, k \\ |x|_\infty = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \end{cases}$$

■

2.4. Completación de \mathbb{Q}_p ($\mathbb{Q}_p, |\cdot|_p$)

La construcción del campo \mathbb{Q}_p como espacio métrico es un caso particular del procedimiento general de completación de un espacio métrico. Para detalles de la demostración, véase [5].

Definición 2.4.1. [5] Sea \mathbb{K} un campo con valor absoluto $|\cdot|$.

- I). Una sucesión $x_n \subset \mathbb{K}$ es una sucesión de Cauchy si para todo $\epsilon > 0$ se puede encontrar una cota M tal que tengamos $|x_n - x_m| < \epsilon$ siempre que $m, n \geq M$.
- II). El campo \mathbb{K} es llamado **completo** con respecto a $|\cdot|$ si toda sucesión de Cauchy en \mathbb{K} posee un límite en \mathbb{K} .
- III). Un subconjunto $S \subset \mathbb{K}$ es llamado denso en \mathbb{K} si toda bola abierta al rededor de cada elemento de \mathbb{K} contiene elementos de S .

Lema 2.4.2. [5] El campo \mathbb{Q} de los números racionales no es completo con respecto a ninguno de sus valores absolutos no triviales.

Definición 2.4.3. [5] Sea $|\cdot|_p$ el valor absoluto p -ádico no arquimediano en \mathbb{Q} . Denotamos por \mathcal{C} , o $\mathcal{C}_p(\mathbb{Q})$, si se quiere enfatizar a p y \mathbb{Q} , el conjunto de todas las sucesiones de Cauchy de elementos en \mathbb{Q} .

Definición 2.4.4. [5] Definimos $\mathcal{N} \subset \mathcal{C}$ como el ideal

$$\mathcal{N} = \{(x_n) : x_n \rightarrow 0\}.$$

Las sucesiones que tienden a cero con respecto de $|\cdot|_p$.

Definición 2.4.5. [5] Podemos definir el campo de los números p -ádicos como un cociente del anillo \mathcal{C} con el ideal (maximal) \mathcal{N} :

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

Proposición 2.4.6. [5] La imagen de \mathbb{Q} bajo la inclusión $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ es un conjunto denso de \mathbb{Q}_p .

Teorema 2.4.7. [5] \mathbb{Q}_p es completo con respecto de $|\cdot|_p$

Teorema 2.4.8. [5] Para cada primo $p \in \mathbb{Z}$, existe un campo \mathbb{Q}_p con un valor absoluto no arquimediano $|\cdot|_p$, tal que:

- I). Existe una inclusión $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$, y el valor absoluto inducido por $|\cdot|_p$ en \mathbb{Q} via inclusión es el valor absoluto p -ádico;
- II). La imagen de \mathbb{Q} bajo esta inclusión es densa en \mathbb{Q}_p ;
- III). \mathbb{Q}_p es completo con respecto de $|\cdot|_p$.

El campo \mathbb{Q}_p que satisface (I), (II) y (III) es único salvo isomorfismo único que preserva los valores absolutos.

2.5. Explorando \mathbb{Q}_p

A partir de este punto, exploraremos el campo completo \mathbb{Q}_p . Identificaremos \mathbb{Q} con su imagen bajo la inclusión en \mathbb{Q}_p , es decir, pensaremos en \mathbb{Q} como un subespacio de \mathbb{Q}_p . Para esto, reenunciamos un lema.

Lema 2.5.1. [5] Para cada $x \in \mathbb{Q}_p$, $x \neq 0$, existe un entero $n \in \mathbb{Z}$ tal que $|x|_p = p^{-n}$. Recíprocamente, para cada $n \in \mathbb{Z}$, podemos encontrar $x \in \mathbb{Q}_p$ tal que $|x|_p = p^n$

Otra forma de decir esto es en términos de la valoración p -ádica v_p . Recordemos que para $x \in \mathbb{Q}$, tenemos $|x|_p = p^{-v_p(x)}$.

Lema 2.5.2. [5] Para todo $x \in \mathbb{Q}_p$, $x \neq 0$, existe un entero $v_p(x)$ tal que $|x|_p = p^{-v_p(x)}$. En otras palabras, la valuación p -ádica extiende a \mathbb{Q}_p

Como antes, extendemos v_p a todo \mathbb{Q}_p , tomando $v_p(0) = +\infty$.

Ahora comenzamos a explorar la estructura de \mathbb{Q}_p . En particular, podemos considerar el anillo de valoración correspondiente, que tiene un nombre propio:

Definición 2.5.3. [5] El anillo de enteros p -ádicos es el anillo de valoración

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

Por supuesto, \mathbb{Z}_p también es la bola unitaria cerrada con centro 0, por lo que ya sabemos algunas cosas al respecto. Como \mathbb{Z}_p es un conjunto cerrado, toda sucesión convergente de elementos de \mathbb{Z}_p tiene un límite en \mathbb{Z}_p . Como \mathbb{Q}_p es completo, todas las sucesiones de Cauchy convergen. Entonces \mathbb{Z}_p es un espacio métrico completo. \mathbb{Z}_p también es un conjunto abierto, porque cada bola lo es. Aquí hay una descripción mucho más precisa:

Proposición 2.5.4. [5] El anillo \mathbb{Z}_p es un anillo local cuyo ideal maximal es el ideal principal $p\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p < 1\}$. Más aún

- I. $\mathbb{Q} \cap \mathbb{Z}_p = \mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} : p \nmid b \right\}$.
- II. La inclusión $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ tiene imagen densa. Específicamente, tomando $x \in \mathbb{Z}_p$ y $n \geq 1$, entonces existe un $\alpha \in \mathbb{Z}$, $0 \leq \alpha \leq p^n - 1$, tal que $|x - \alpha|_p \leq p^{-n}$. El entero α es único.
- III. Para todo $x \in \mathbb{Z}_p$, existe una sucesión de Cauchy (α_n) tal que $\alpha_n \rightarrow x$, del siguiente tipo:
 - $\alpha_n \in \mathbb{Z}$ satisface $0 \leq \alpha_n \leq p^n - 1$
 - Para todo $n \geq 2$, tenemos $\alpha_n \equiv \alpha_{n-1} \pmod{p^{n-1}}$.

La sucesión (α_n) con estas propiedades es única.

Esta proposición dice varias cosas importantes. Por ejemplo, muestra que cada elemento de \mathbb{Z}_p es el límite de una sucesión de números enteros, de modo que:

Corolario 2.5.5. [5] \mathbb{Z} es denso en \mathbb{Z}_p

Otra consecuencia es:

Corolario 2.5.6. [5] $\mathbb{Q}_p = \mathbb{Z}_p[1/p]$, esto es, para cada $x \in \mathbb{Q}_p$ existe $n \geq 0$ tal que $p^n x \in \mathbb{Z}_p$. El mapeo $\mathbb{Q}_p \rightarrow \mathbb{Q}_p$ dado por $x \mapsto px$ es un homeomorfismo. Los conjuntos $p^n \mathbb{Z}_p$, $n \in \mathbb{Z}$ forman un sistema fundamental de vecindades de $0 \in \mathbb{Q}_p$ que cubren todo \mathbb{Q}_p

Corolario 2.5.7. [5] Para todo $n \geq 1$, la sucesión

$$0 \rightarrow \mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p \rightarrow \mathbb{Z}/p^n\mathbb{Z} \rightarrow 0$$

Donde el mapeo $\mathbb{Z}_p \rightarrow \mathbb{Z}_p$ es dada por $x \mapsto p^n x$, es exacta, y los mapeos son continuos. En particular,

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

Recordemos que para una sucesión $A \xrightarrow{f} B \xrightarrow{g} C$ es exacta si $\text{Im}(f) = \text{ker}(g)$. Una sucesión de cinco términos como la anterior es exacta cuando lo es en cada etapa, de modo que las afirmaciones anteriores son:

- El mapeo $\mathbb{Z}_p \rightarrow \mathbb{Z}_p$ dado por la multiplicación por p^n es inyectiva.
- El mapeo $\mathbb{Z}_p \rightarrow \mathbb{Z}/p^n\mathbb{Z}$ es sobreyectivo.

- el núcleo de este mapa es precisamente la imagen de \mathbb{Z}_p bajo el primer mapeo, que por supuesto es $p^n\mathbb{Z}_p$.

Recordemos que dados dos puntos, siempre podemos encontrar bolas a su alrededor que no se cruzan (lo cual es útil saber sobre una topología: los puntos se pueden separar). En grandes palabras:

Corolario 2.5.8. [5] \mathbb{Q}_p es un espacio topológico Hausdorff totalmente desconexo.

Una propiedad topológica más interesante es la compacidad, que juega un papel importante en el análisis clásico. Un subconjunto X de un espacio topológico se llama compacto si tiene la siguiente propiedad:

- cualquier colección de conjuntos abiertos que cubre X tiene una subcolección finita que también cubre X .

Esta es una definición bastante poco intuitiva, pero resulta ser bastante importante. Por ejemplo, los conjuntos compactos en \mathbb{R} son precisamente los conjuntos cerrados y acotados, que juegan un papel importante en el análisis real.

Corolario 2.5.9. [5] \mathbb{Z}_p es compacto, y \mathbb{Q}_p es localmente compacto

Demostración. Como \mathbb{Z}_p es una vecindad de cero, probar que es compacto es suficiente para probar que \mathbb{Q}_p es localmente compacto, por lo que el segundo enunciado se sigue del primero.

Para probar el primer enunciado, sabemos que \mathbb{Z}_p es completo (porque es un conjunto cerrado en un campo completo), por lo que lo que necesitamos probar es que es totalmente acotado, es decir, que para cualquier $\varepsilon > 0$ se puede cubrir \mathbb{Z}_p con un número finito de bolas de radio ε . Basta comprobar esto para todo $\varepsilon = p^{-n}$, $n \geq 0$. Pero recordamos que

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

y que las clases laterales de $p^n\mathbb{Z}_p$ in \mathbb{Z}_p también son bolas en la topología p -ádica. y que las clases laterales de $p^n\mathbb{Z}_p$ en \mathbb{Z}_p también son bolas en la topología p -ádica. Esto significa que a medida que a oscila entre $0, 1, \dots, p^n - 1$ (o cualquier otro conjunto de representantes), las p^n bolas

$$a + p^n\mathbb{Z}_p = \{a + p^n x : x \in \mathbb{Z}_p\} = \{y \in \mathbb{Z}_p : |y - a| \leq p^{-n}\} = \bar{B}(a, p^{-n})$$

Cubren a \mathbb{Z}_p , Por lo tanto, \mathbb{Z}_p es compacto y se sigue que \mathbb{Q}_p es localmente compacto. ■

Las unidades p -ádicas son los elementos invertibles de \mathbb{Z}_p . Denotaremos el conjunto de todos estos elementos por \mathbb{Z}_p^\times . Dado $x \in \mathbb{Z}_p$, entonces $|x|_p \leq 1$ y $x^{-1} \in \mathbb{Z}_p$ donde $|x^{-1}|_p = |x|_p^{-1} \leq 1$, vemos que

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

De aquí notamos que

$$\mathbb{Z}_p^\times \cap \mathbb{Q} = \left\{ \frac{a}{b} \in \mathbb{Q} : p \nmid ab \right\}$$

Como los elementos invertibles de todo anillo, las unidades p -ádicas forman un grupo. En nuestro caso, este grupo contiene bastantes elementos. Observemos que es un subconjunto cerrado de \mathbb{Z}_p y, por lo tanto, es compacto.

Los elementos de \mathbb{Q}_p son, en este punto, difíciles de comprender, porque solo conocemos \mathbb{Q}_p a través de sus propiedades básicas. Para contrarrestar esto, daremos ahora dos descripciones diferentes de los elementos de \mathbb{Q}_p : como “sucesiones coherentes” y como “expansiones p -ádicas”. La descripción en términos de sucesiones coherentes, que daremos primero, es interesante por razones teóricas, mientras que la descripción en términos de expansiones nos dará la versión más “concreta” de \mathbb{Q}_p . Para la primera descripción, partimos del literal II) de la proposición 10: dado $x \in \mathbb{Z}_p$, podemos encontrar un tipo bastante especial de sucesión de Cauchy que converge a x . Esta sucesión tiene la propiedad de ser “coherente”, es decir

- $\alpha_n \in \mathbb{Z}, \quad 0 \leq \alpha_n \leq p^n - 1$
- $\alpha_{n+1} \equiv \alpha_n \pmod{p^n}$

Adicionalmente, por la relación entre las congruencias y el valor absoluto p -ádico, tenemos que la sucesión converge a x porque $|x - \alpha_n|_p \leq p^{-n}$. Recordamos que es única.

Por otro lado, supongamos que tenemos tal sucesión (α_n) . La propiedad de coherencia claramente la convierte en una sucesión de Cauchy, porque $|\alpha_{n+1} - \alpha_n|_p \leq p^{-n}$. Por lo tanto, debe converger a algún elemento, que estará en \mathbb{Z}_p porque los α_n están en \mathbb{Z} .

Proposición 2.5.10. [5] *El límite de una sucesión de Cauchy de números enteros es un elemento de \mathbb{Z}_p*

Demostración. Recordemos que $|x|_p \leq 1$, para $x \in \mathbb{Z}_p$.

Supongamos que para una sucesión (x_n) de números enteros, $x_n \rightarrow x$, donde x es p -ádico, entonces, para $n \geq N$,

$$|x|_p = |x_n + (x - x_n)|_p \leq \max\{|x_n|_p, |x - x_n|_p\} \leq 1$$

de aquí que $|x|_p \leq 1$. Por lo tanto $x \in \mathbb{Z}_p$. ■

Esto significa que podemos identificar los elementos de \mathbb{Z}_p con tales sucesiones. Resumiremos esto en la siguiente proposición, pero en un lenguaje bastante sofisticado. Para configurarlo, escribamos φ_n para la proyección sobre el cociente

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

Para un elemento de $\mathbb{Z}/p^n\mathbb{Z}$, tenemos entonces que $\varphi_n(x) \equiv \alpha_n \pmod{p^n}$ (solo porque el conjunto de enteros entre 0 y $p^n - 1$ da representantes para las clases laterales, y los α_n se eligen como los representantes correspondientes a x). también establecemos el conjunto

$$A_n = \mathbb{Z}/p^n\mathbb{Z}_p$$

y pensar en ello como un anillo topológico con una topología discreta. Tenemos un mapa obvio $\psi_n : A_n \longrightarrow A_{n-1}$, que manda $(a \pmod{p^n})$ a $(a \pmod{p^{n-1}})$. Queremos considerar el producto de todos estos anillos, es decir, el anillo de sucesiones (α_n) tales que $\alpha_n \in A_n$. (Las operaciones se definen de manera obvia, término por término). Para este producto utilizamos la topología del producto. Esta topología es bastante complicada de describir, y realmente no necesitamos saber mucho al respecto. Solo señalamos que el anillo del producto será compacto con esta topología. Con todo esto configurado, podemos afirmar:

Proposición 2.5.11. [5] *Los mapeos de proyección φ_n juntos dan la inclusión*

$$\varphi : \mathbb{Z}_p \hookrightarrow \prod_{n \geq 1} A_n$$

que identifica a \mathbb{Z}_p , como un anillo topológico, con el subanillo cerrado de $\prod A_n$ formado por las sucesiones coherentes, es decir, aquellas sucesiones (α_n) para las que tenemos $\psi_n(\alpha_n) = \alpha_{n-1}$ para todo $n > 1$.

A continuación vamos a obtener una forma canónica de representar los elementos de \mathbb{Q}_p como "serie de potencias en p ". Comenzamos con un entero p -ádico $x \in \mathbb{Z}_p$. Como acabamos de mostrar, existe una sucesión coherente de enteros α_n que convergen en x tal que:

- $\alpha_n \equiv x \pmod{p^n}$
- $\alpha_{n+1} \equiv \alpha_n \pmod{p^n}$
- $0 \leq \alpha_n \leq p^n - 1$

Para entender un poco mejor las α_n , las escribimos en base p . Para los enteros escritos en base p , el proceso de reducción del módulo p^n es muy simple: simplemente elimine todos menos los últimos n dígitos. Esto significa que la condición de coherencia

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

simplemente dice que los últimos n dígitos de ambos números son iguales. Pero estos son solo una secuencia de sumas parciales de una serie.

$$\begin{aligned} \alpha_1 &= b_0 & 0 \leq b_0 \leq p-1 \\ \alpha_2 &= b_0 + b_1p & 0 \leq b_1 \leq p-1 \\ \alpha_3 &= b_0 + b_1p + b_2p^2 & 0 \leq b_2 \leq p-1 \end{aligned}$$

Entonces obtenemos una expansión en serie

$$x = b_0 + b_1p + b_2p^2 + \dots + b_np^n + \dots$$

Por supuesto, para poder escribir realmente ese signo igual con la conciencia tranquila, debemos comprobar que la serie de la derecha sí converge a x . Pero eso es fácil:

Lema 2.5.12. [5] *Dado cada $x \in \mathbb{Z}_p$, la serie*

$$b_0 + b_1p + b_2p^2 + \dots + b_np^n + \dots$$

como se obtuvieron anteriormente, converge a x .

Demostración. Recordemos que una serie converge a x si y sólo si la sucesión de sus sumas parciales converge a x . Pero las sumas parciales de nuestra serie son exactamente las α_n , que ya sabemos que convergen en x (las elegimos así). ■

En resumen, esto nos da

Corolario 2.5.13. [5] *Todo $x \in \mathbb{Z}_p$ puede escribirse de la forma*

$$x = b_0 + b_1p + b_2p^2 + \dots + b_np^n + \dots$$

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

Demostración. Hemos comprobado todo menos la unicidad. Para ver eso, observemos que ya sabemos que los α_n son únicos, y esto implica que los b_n también lo son (porque son solo los dígitos en base p).

■

Ahora, necesitamos obtener todo \mathbb{Q}_p . Pero recuerda que cualquier elemento de \mathbb{Q}_p se puede escribir en la forma $p^m y$ con $y \in \mathbb{Z}_p$ y $m \in \mathbb{Z}$ (el caso interesante para nosotros es cuando m es negativa, por supuesto). Si expresamos y como una serie de potencias en p , luego multiplicamos por p^m , solo obtenemos una serie de potencias en p donde algunas de las potencias pueden ser negativas. Así que:

Corolario 2.5.14. [5] *Todo $x \in \mathbb{Q}_p$ puede escribirse de la forma*

$$\begin{aligned} x &= b_{-m}p^{-m} + \dots + b_{-1}p^{-1} + b_1p^1 + b_0 + b_1p + b_2p^2 + \dots + b_np^n + \dots \\ &= \sum_{n \geq -m} b_np^n \end{aligned}$$

con $0 \leq b_n \leq p - 1$ y $-m = v_p(x)$. La representación es única.

Proposición 2.5.15. [5] *Sea $x \in \mathbb{Z}_p$. En la expansión p -ádica, que condición nos garantiza que x es una unidad p -ádica*

Demostración. Recordamos que $x = b_0 + b_1p + b_2p^2 + \dots + b_np^n + \dots$, con $0 \leq b_i \leq p - 1$. Vemos que si pedimos que $b_0 \neq 0$, entonces $v_p(x) = 0$ y por tanto $|x|_p = p^0 = 1$.

■

Corolario 2.5.16. [5] *Sea $A \subset \mathbb{Z}_p$ un conjunto de representantes de clase de \mathbb{Z}/\mathbb{Z}_p . Todo $x \in \mathbb{Q}_p$ puede escribirse de la forma*

$$\begin{aligned} x &= b_{-m}p^{-m} + \dots + b_{-1}p^{-1} + b_1p^1 + b_0 + b_1p + b_2p^2 + \dots + b_np^n + \dots \\ &= \sum_{n \geq -m} b_np^n \end{aligned}$$

con $0 \leq b_n \leq p - 1$ y $-m = v_p(x)$. La representación es única

Demostración. Supongamos primero que $x \in \mathbb{Z}_p$ y miramos su imagen en $\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$. Por nuestra elección de A existe un único elemento $b_0 \in A$ tal que $x - b_0 \in p\mathbb{Z}_p$. Entonces $x - b_0 = px_1$ para algún $x_1 \in \mathbb{Z}_p$. Como antes, existe un único $b_1 \in A$ tal que $x_1 - b_1 \in p\mathbb{Z}_p$, de modo que $x = b_0 + b_1p + p^2x_2$ para algún $x_2 \in \mathbb{Z}_p$. Continuando así, obtenemos para cada n :

$$x = b_0 + b_1p + b_2p^2 + \dots + b_np^n + p^{n+1}x_{n+1}$$

Con $x \in \mathbb{Z}_p$, así que

$$|x - (b_0 + b_1p + b_2p^2 + \dots + b_np^n)| \leq p^{-(n+1)}$$

Con esto, mostramos que la serie $b_0 + b_1p + b_2p^2 + \dots + b_np^n + \dots$ converge a x .
Si $x \notin \mathbb{Z}_p$, escribimos $x = p^{-m}x_0$ con $x_0 \in \mathbb{Z}_p$, expandimos x_0 como sabemos hacerlo y luego multiplicamos por p^{-m} para obtener dicha serie.

■

Capítulo 3

Elementos básicos del análisis p -ádico

3.1. Sucesiones y series

Comenzamos estudiando las propiedades básicas de convergencia de sucesiones y series. Ya se ha señalado el hecho más importante: \mathbb{Q}_p es un campo completo, por lo que toda sucesión de Cauchy converge. Además, observamos que todos los axiomas que se cumplen para el valor absoluto en \mathbb{R} todavía se cumplen en \mathbb{Q}_p (ser no arquimediano es una propiedad extra). Por lo tanto, la mayoría de los teos básicos todavía se cumplen en el contexto p -ádico, con las mismas demostraciones.

Quizás la diferencia más importante es el hecho, también señalado anteriormente, de que en un contexto no arquimediano es más fácil probar la propiedad de Cauchy.

Lema 3.1.1. *Una sucesión $(x_n) \in \mathbb{Q}_p$ es una sucesión de Cauchy, por tanto convergente, si y sólo satisface*

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

Demostración. Solo nos basta analizar que si $m = n + r > n$, tenemos

$$|x_m - x_n| = |x_{n+r} - x_{n+r-1} + x_{n+r-1} - x_{n+r-2} + \dots + x_{n+1} - x_n| \\ \max\{|x_{n+r} - x_{n+r-1}|, |x_{n+r-1} - x_{n+r-2}|, \dots, |x_{n+1} - x_n|\}$$

esto viene de la propiedad ultramétrica. El resultado se sigue de esta desigualdad y las hipótesis. ■

Excepto por esta importante diferencia, la teoría de las sucesiones y sus propiedades de convergencia es prácticamente idéntica a la teoría sobre \mathbb{R} . La definición básica de convergencia es la misma. Por supuesto, algunas sucesiones convergerán en \mathbb{Q}_p que no convergen en \mathbb{R} , y viceversa.

Ejemplo 3.1.2. [5] Sea $a_1 = 1 + p$ y definimos una sucesión recursiva por $a_n = (a_{n-1})^p$. Notamos que

$$(1 + p)^p = 1 + p^2 + \binom{p}{2} p^2 + \binom{p}{3} p^3 + \dots + p^p$$

Dado que $\binom{p}{k}$ es divisible por p para $0 < k < p$, entonces vemos que $(1 + p)^p - 1$ es divisible por p^2 , es decir que $a_2 \equiv 1 \pmod{p^2}$. Repitiendo este argumento, podemos concluir que para cada n tenemos que $a_n \equiv 1 \pmod{p^n}$, es decir,

$$|a_n - 1| \leq p^{-n}$$

De aquí vemos que a_n converge a 1 cuando $n \rightarrow \infty$.

Ejemplo 3.1.3. [5] Sea $a_n = n!$.

Recordamos que $a_n \rightarrow 0 \iff v_p(a_n) \rightarrow \infty$.

Observamos que

$$v_p(n) = v_p\left(\frac{a_n}{a_{n-1}}\right) = v_p(n!) - v_p((n-1)!)$$

Es decir $v_p(n) = v_p(n!) - v_p((n-1)!)$ y sabemos que cuando $n \rightarrow \infty$ entonces $v_p(n) \rightarrow \infty$, con esto tenemos que

$$\lim_{n \rightarrow \infty} |v_p(n!) - v_p((n-1)!)| = \infty$$

Recordamos que una sucesión es convergente si y sólo si $\lim_{n \rightarrow \infty} |a_n - a_{n-1}| = 0$. Por tanto $v_p(a_n) \rightarrow \infty$, y con esto concluimos que $a_n \rightarrow 0$.

Ejemplo 3.1.4. [5] Sea $a_n = (1 + px)^{p^n}$. Notamos que

$$(1 + p)^{p^n} = 1 + p^{n+1}x + \binom{p^n}{2} p^2 x^2 + \dots + p^{p^n} x^{p^n}$$

Dado que $\binom{p^n}{k}$ es divisible por p^n para $0 < k < p^n$, entonces vemos que $(1+p)^p - 1$ es divisible por p^{n+1} , es decir que $a_n \equiv 1 \pmod{p^{n+1}}$. Es decir,

$$|a_n - 1| \leq p^{-(n+1)}$$

De aquí vemos que a_n converge a 1 cuando $n \rightarrow \infty$.

Lo mismo ocurre con las series: la teoría clásica sigue siendo válida. Por ejemplo, lo siguiente sigue siendo cierto:

Proposición 3.1.5. [5] Sea $a_n \in \mathbb{Q}_p$, convergencia absoluta implica convergencia, es decir, que si la serie de valores absolutos $\sum |a_n|$ converge en \mathbb{R} , entonces la serie $\sum a_n$ converge en \mathbb{Q}_p

Este es un resultado importante y útil en el análisis real. Sin embargo, en el contexto p -ádico, tenemos algo mucho mejor:

Corolario 3.1.6. [5] Una serie infinita $\sum_{n=0}^{\infty} a_n$ con $a_n \in \mathbb{Q}_p$ es convergente si y sólo si

$$\lim_{n \rightarrow \infty} a_n = 0$$

en dicho caso, también tenemos que

$$\left| \sum_{n=0}^{\infty} a_n \right| \leq \max_n |a_n|.$$

Demostración. Una serie converge cuando la sucesión de sus sumas parciales converge. Observamos que el término a_n se puede escribir como

$$a_n = \sum_{k=0}^n a_k - \sum_{k=0}^{n-1} a_k$$

si $|a_n|_p \rightarrow 0$, por el lema 3.1.1 concluimos que la sucesión de sumas parciales es de Cauchy y por lo tanto la serie converge.

Por último, extendiendo la propiedad no arquimediana a una cantidad arbitraria de elementos, y recordando que $|a_n|_p \rightarrow 0$, entonces el máximo se alcanza. ■

Luego de ver algunas propiedades análogas del caso real al caso p -ádico para las sucesiones y series, hablaremos sobre las series de potencias, otro objeto clásico

y de importancia en el análisis. Recordamos que la forma de una serie de potencias es

$$\sum_{n=0}^{\infty} a_n (X - \alpha)^n$$

como dijimos, este objeto ofrece una forma conveniente para la representación de funciones, y en particular es utilizado para para definir funciones de suma importancia, como son las funciones exponenciales y trigonométricas. Como era de esperar, la teoría p -ádica resulta ser bastante similar a la versión clásica, excepto que algunos de los puntos difíciles se vuelven mucho más fáciles de manejar. Por otro lado, la propiedad no arquimediana introduce algunas sorpresas. La mayor de estas sorpresas es el hecho de que la relación entre la composición formal de las series de potencias y la composición de las funciones que definen se vuelve más complicada en el contexto p -ádico que en la situación clásica.

Al inicio de esta sección, establecimos algunos de nuestros resultados para series de potencias en X , pero por supuesto siguen siendo válidos para series de potencias en $(X - \alpha)$ si reemplazamos todas las condiciones $|x| < k$ por $|x - \alpha| < k$.

Consideremos la serie de potencias

$$f(X) = \sum_{n=0}^{\infty} a_n X^n.$$

Dado $x \in \mathbb{Q}_p$, queremos considerar $f(x) = \sum a_n x^n$, por el corolario 3.1.6 sabemos que esta serie converge si y sólo si $|a_n x^n| \rightarrow 0$. Como en el caso clásico, el conjunto de las x (que llamaremos **región de convergencia**) es un disco cuyo radio se puede calcular directamente.

Proposición 3.1.7. [5] Sea $f(X) = \sum_{n=0}^{\infty} a_n X^n$, definimos

$$\rho = \frac{1}{\limsup_{n \rightarrow \infty} \sqrt[n]{|a_n|}},$$

usando la convención usual cuando el límite tiende a 0 o ∞ , entonces $0 \leq \rho \leq \infty$.

1. Si $\rho = 0$, entonces $f(x)$ converge solamente cuando $x = 0$.
2. Si $\rho = \infty$, entonces $f(x)$ converge $\forall x \in \mathbb{Q}_p$.
3. Si $0 < \rho < \infty$ y $\lim_{n \rightarrow \infty} |a_n| \rho = 0$, entonces $f(x)$ converge a si y sólo si $|x| \leq \rho$

-
4. Si $0 < \rho < \infty$ y $|a_n|\rho$ no tiende a 0 cuando $n \rightarrow \infty$, entonces $f(x)$ converge si y sólo si $|x| < \rho$.

Demostración. Primero, recordemos que la interpretación del \limsup de una manera rápida. Si $\limsup b_n = B$ entonces para todo $\varepsilon > 0$, sucedes dos cosas: primero, $b_n < B + \varepsilon$ para una cantidad finita de n ; segundo, $b_n > B - \varepsilon$ para una cantidad infinita de n . Sabemos que la región de convergencia es

$$\{x \in \mathbb{Q}_p : \lim_{n \rightarrow \infty} |a_n x^n| = 0\}$$

El objetivo del teorema es dar información más precisa sobre esta región. Primero, observamos que $f(0)$ claramente converge. Ahora, si $|x| > \rho$ es claro que $|a_n||x|^n$ no tiende a 0 cuando $n \rightarrow \infty$: la definición de ρ implica que para infinitos valores de n , $|a_n|$ tiende a $\frac{1}{\rho^n}$, y como $|x| > \rho$, $\left(\frac{|x|}{\rho}\right)^n$ crece cada vez más (p -ádicamente) cuando $n \rightarrow \infty$.

Similarmente, si $|x| < \rho$, tomamos $|x| < \rho_1 < \rho$. Entonces $|x|/\rho_1 < 1$ y para todos salvo una cantidad finita de n tenemos que $|a_n| < 1/\rho_1^n$, entonces $|a_n x^n| \leq |x^n|/\rho_1^n$ y entonces $|a_n x^n| \rightarrow 0$. Finalmente para $|x| = \rho$, obtenemos el resultado debido a que $|a_n \rho^n| \rightarrow 0$, por el corolario 3.1.6

■

El resultado de este teorema refleja una diferencia con respecto a su análogo sobre \mathbb{R} o \mathbb{C} . En nuestro caso p -ádico sucede algo más amigable con los puntos de convergencia de la serie sobre la frontera de la región de convergencia ($|x| = \rho$), y es simple: Nuestra serie converge para todos o para ninguno de los puntos de la frontera.

Ahora que ya hemos definido un criterio de convergencia para series de potencias formales, podemos pensar en definir operaciones en este sentido formal. Viendo estas operaciones formales, nos podemos preguntar: ¿Cómo se traducen las propiedades formales en propiedades de las funciones definidas por la serie de potencias?. Comencemos por las operaciones fáciles de definir. Consideremos las series de potencias $f(X)$ y $g(X)$, y definamos la suma y producto. Si

$$f(X) = \sum_{n=0}^{\infty} a_n X^n \quad y \quad g(X) = \sum_{n=0}^{\infty} b_n X^n$$

Definimos

$$(f + g)(X) = \sum_{n=0}^{\infty} (a_n + b_n) X^n$$

y

$$(fg)(X) = \sum_{n=0}^{\infty} \left(\sum_{k=0}^n a_k b_{n-k} X^n \right)$$

Tal como lo hemos definido, esta es solo una operación formal. Por supuesto, nos gustaría saber que realmente funciona cuando ingresamos números para X . No es demasiado difícil ver que todo funciona como se esperaba:

Proposición 3.1.8. [5] *Sea $f(X)$ y $g(X)$ dos series de potencias formales, y supongamos $x \in \mathbb{Q}_p$. Si ambas $f(x)$ y $g(x)$ convergen, entonces:*

1. $(f + g)(x)$ converge y es igual a $f(x) + g(x)$ y;
2. $(fg)(x)$ converge y es igual a $f(x)g(x)$.

De ello se deduce que los radios de convergencia de $f + g$ y de fg son cada uno mayor o igual que el menor de los radios de convergencia de f y g .

Ahora que hemos definido algunas operaciones de importancia sobre las series de potencias formales y observamos cómo se comportan las propiedades, hablaremos sobre algunas propiedades que adquieren las funciones que se pueden definir a través de las series de potencias. En específico, cuando se define f sobre la región de convergencia de la serie de potencias, la función adquiere continuidad.

Lema 3.1.9. [5] *Sea $f(X) = \sum a_n X^n$ una serie de potencias con coeficientes en \mathbb{Q}_p . Si $f(x)$ converge para $|x| < r$, entonces la función $f : \bar{B}(0, r) \rightarrow \mathbb{Q}_p$ definida como $x \rightarrow f(x)$ es acotada y uniformemente continua.*

Para los detalles de la demostración ver [5].

Al pensar en este lema, se debe tener en cuenta que mientras trabajamos sobre \mathbb{Q}_p estamos tratando de dar argumentos que se apliquen de la manera más general posible. Las bolas cerradas en \mathbb{Q}_p son compactas y recordemos que las funciones continuas en un conjunto compacto siempre son acotadas y uniformemente continuas. Entonces, mientras permanezcamos en \mathbb{Q}_p , el lema realmente no nos dice más que la función es continua. La esencia de la prueba no es más que el uso de la propiedad no arquimediana, por lo que el resultado será verdadero en un campo no arquimediano completo incluso si estamos en un contexto donde las bolas cerradas no son compactas.

Corolario 3.1.10. [5] *Sea $f(X) = \sum a_n X^n$ una serie de potencias con coeficientes en \mathbb{Q}_p y sea $\mathcal{D} \subset \mathbb{Q}_p$ su región de convergencia, es decir, el conjunto $x \in \mathbb{Q}_p$, tal que $f(x)$ converge. Entonces, la función*

$$f : \mathcal{D} \rightarrow \mathbb{Q}_p$$

Definida como $x \rightarrow f(x)$ es continua para todo $x \in \mathcal{D}$.

Como en el caso clásico, podemos cambiar el centro de la expansión de la serie, es decir, reescribir nuestra función como una serie de potencias en $(X - \alpha)$ para cualquier α en la región de convergencia. En el caso clásico, la serie resultante puede tener (y suele tener) una región de convergencia diferente a la de la serie original, y este hecho es una de las formas de obtener “continuaciones analíticas”. Sorprendentemente, en el caso p -ádico, cambiar el centro nunca ayuda a la continuación analítica.

Proposición 3.1.11. [5] Sea $f(X) = \sum a_n X^n$ una serie de potencias con coeficientes en \mathbb{Q}_p , y sea $\alpha \in \mathbb{Q}_p$, $\alpha \neq 0$, un punto tal que $f(\alpha)$ converge. Para todo $m \geq 0$ definimos

$$b_m = \sum_{n \geq m} \binom{n}{m} a_n \alpha^{n-m},$$

y consideramos la serie de potencias

$$g(X) = \sum_{m=0}^{\infty} b_m (X - \alpha)^m.$$

1. La serie definida por los b_m converge para todo m , es decir que b_m está bien definido.
2. Las series de potencias $f(X)$ y $g(X)$ tienen la misma región de convergencia, es decir, $f(\lambda)$ converge si y sólo si $g(\lambda)$ converge.
3. Para cada λ en la región de convergencia, $f(\lambda) = g(\lambda)$.

Para los detalles de la demostración ver [5].

3.2. Función logaritmo y exponencial

Nuestro objetivo es usar series de potencias para definir funciones p -ádicas que son análogas a las funciones exponenciales y logarítmicas clásicas. A diferencia del caso arquimediano, es el logaritmo el que tiene mejores propiedades de convergencia. Comenzamos con la serie de potencias habitual para el logaritmo:

$$f(X) = \log(1 + X) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{X^n}{n} = X - \frac{X^2}{2} + \frac{X^3}{3} + \dots$$

Dado que los coeficientes de esta serie de potencias son números racionales, tiene sentido pensar en la serie como una serie de potencias en \mathbb{Q}_p (para cualquier primo p). El primer paso para comprenderlo es, por supuesto, calcular su radio de convergencia. Sin embargo, antes de saltar al cálculo del límite, debemos notar otro contraste clásico versus p -ádico. En el caso clásico, todos los números enteros

en los denominadores ayudan a la convergencia, porque tienden a hacer más pequeños los términos de la serie. En el caso p -ádico, esto es exactamente al revés: los números enteros en el denominador no cambian el valor absoluto (cuando no son divisibles por p) o lo hacen más grande (cuando lo son). Lo que salva la convergencia en el caso de esta serie es que "en general" n no es demasiado divisible por p .

Para calcular el radio de convergencia ρ , sea $f(x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n}$, de aquí $a_n = \frac{(-1)^n}{n}$, entonces

$$|a_n| = \left| \frac{1}{n} \right| = p^{v_p(n)}.$$

De esto, tenemos que

$$\sqrt[n]{|a_n|} = p^{v_p(n)/n} \rightarrow 1$$

cuando $n \rightarrow \infty$. De aquí que $\rho = 1$.

Esto no decide por nosotros si la convergencia ocurre en la bola abierta o cerrada de radio 1. Para decidir, debemos ver qué sucede cuando $|x| = 1$. Pero está claro que en ese caso el valor absoluto $|a_n x^n| = |a_n| = |1/n|$ no tiende a cero (es igual a 1 siempre que p no divide a n). Entonces obtenemos

Lema 3.2.1. [5] *La serie*

$$f(X) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{X^n}{n}$$

Converge para $|x| < 1$ y diverge en otro caso.

La conclusión es que $f(X)$ define una función sobre la bola abierta $B(0, 1)$ de radio 1 y centro 0. Esto sugiere que deberíamos definir el logaritmo de la manera obvia, de modo que $f(x) = \log(1 + x)$.

Definición 3.2.2. [5] *Sea $U_1 = B(1, 1) = \{x \in \mathbb{Z}_p : |x - 1| < 1\} = 1 + p\mathbb{Z}_p$. Definimos el logaritmo p -ádico para $x \in U_1$ como*

$$\log_p(x) = \log(1 + (x - 1)) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{(x - 1)^n}{n}.$$

Por supuesto, esta función merezca ser llamada logaritmo satisface la ecuación funcional que caracteriza a los logaritmos.

Para los detalles, ver [5].

Proposición 3.2.3. [5] Supongamos que $a, b \in 1 + p\mathbb{Z}_p$. Entonces

$$\log_p(ab) = \log_p(a) + \log_p(b).$$

Habiendo obtenido un logaritmo, las exponenciales no se pueden quedar atrás. En el caso clásico, la serie

$$\exp(X) = \sum_{n=0}^{\infty} \frac{X^n}{n!} = 1 + X + \frac{X^2}{2} + \frac{X^3}{6} + \dots$$

converge para todo $x \in \mathbb{R}$, porque los coeficientes $1/n!$ tienden muy rápidamente a cero con respecto al valor absoluto real. En el contexto p -ádico, por supuesto, esto cambia drásticamente, porque $n!$ tiende a cero, por lo que $1/n!$ se vuelve arbitrariamente grande a medida que n crece. Esto significa que no podemos esperar tener un gran radio de convergencia. Para determinar cuál será ese radio, tenemos que calcular exactamente qué tan rápido son los coeficientes $1/n!$ crecer, es decir, tenemos que averiguar cuán divisible es $n!$ es por p .

Lema 3.2.4 (Fórmula de Legendre). [5] Sea p un primo. Entonces

$$v_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor < \frac{n}{p-1}.$$

donde $\lfloor x \rfloor$ es la función piso. En particular

$$|n!|_p > p^{-n/(p-1)}.$$

En un capítulo posterior, nosotros utilizaremos una forma alternativa de esta fórmula en términos de la expansión p -ádica de n . Denotemos $s_p(n)$ como la suma de los dígitos de la expansión p -ádica de n , entonces

$$v_p(n!) = \frac{n - s_p(n)}{p-1}.$$

Ahora usaremos la siguiente aproximación para calcular el radio de convergencia de la exponencial.

Lema 3.2.5. [5] Sea

$$g(X) = \sum_{n=0}^{\infty} \frac{X^n}{n!} = 1 + X + \frac{X^2}{2!} + \frac{X^3}{3!} + \dots$$

Entonces $g(x)$ converge si y solo si $|x| < p^{-1/(p-1)}$.

Demostración. Dado que

$$|a_n| = \frac{1}{n!} = p^{v_p(n!)} < p^{n/(p-1)}$$

De esta primera estimación, obtenemos

$$\rho \geq p^{-1/(p-1)}.$$

De aquí que esta serie converge para $|x| < p^{-1/(p-1)}$.

Por otro lado, sea $|x| = p^{-1/(p-1)}$ y sea $n = p^m$ una potencia de p , en ese caso, tenemos

$$v_p(n!) = v_p(p^m)! = 1 + p + \dots + p^{m-1} = \frac{p^m - 1}{p - 1}.$$

Entonces, dado que $v_p(x) = 1/(p - 1)$,

$$v_p\left(\frac{x^n}{n!}\right) = \left(\frac{x^{p^m}}{p^{m!}}\right) = \frac{p^m}{p-1} - \frac{p^m - 1}{p-1} = \frac{1}{p-1}$$

¡Esto no depende de m , por lo tanto $x^n/n!$ no puede tender a cero y la serie no converge. Como sabemos que la región de convergencia es un disco, esto prueba el lema. ■

Hay algo un poco extraño acerca de la desigualdad en el lema. Si $p \neq 2$ y $x \in \mathbb{Z}_p$, entonces el valor absoluto de x puede ser igual a $1 > p^{-1/(p-1)}$ o menor o igual a $1/p = p^{-1}$ (que es más pequeño): no hay valores en el medio. Así, si $p \neq 2$,

$$|x| < p^{-1/(p-1)} \iff |x| \leq p^{-1} \iff x \in p\mathbb{Z}_p \iff |x| < 1.$$

así que el disco en el lema es solo el disco abierto de radio uno.

Mientras permanezcamos en \mathbb{Q}_p , las cosas son bastante simples. Si $p = 2$, $g(x) = \exp(x)$ converge para $x \in p\mathbb{Z}_p$. Si $p = 2$, $-1/(2-1) = -1$, entonces el lema nos dice que $g(x) = \exp(x)$ converge cuando $|x| < 1/2$, lo que sucede cuando $x \in 4\mathbb{Z}_2$.

Ahora definiremos la función exponencial p -ádica usando la serie formal $\exp(X)$.

Definición 3.2.6. [5] Sea $D = B(0, p^{-1/(p-1)}) = \{x \in \mathbb{Z}_p : |x| < p^{-1/(p-1)}\}$. El exponencial p -ádico es la función $\exp_p : D \rightarrow \mathbb{Q}_p$ definida por:

$$\exp_p(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

Nótese que $\exp_p(1)$ no está definida, por lo que, no es una analogía natural p -ádica de e en \mathbb{Q}_p . Dentro de su dominio, sin embargo, la exponencial p -ádica satisface la mayoría de las propiedades formales de la exponencial clásica. Continuaremos con la más famosa:

Proposición 3.2.7. [5] Si $x, y \in D$ tenemos que $x + y \in D$ y $\exp_p(x + y) = \exp_p(x) \exp_p(y)$

Demostración. Se demuestra haciendo manipulación de las series formales:

$$\begin{aligned} \exp(x + y) &= \sum_{n=0}^{\infty} \frac{(x + y)^n}{n!} = \sum_{n=0}^{\infty} \frac{1}{n!} \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k \\ &= \sum_{n=0}^{\infty} \sum_{k=0}^n \frac{1}{n!} \frac{n!}{(n-k)!k!} x^{n-k} y^k \\ &= \sum_{n=0}^{\infty} \sum_{k=0}^n \frac{x^{n-k}}{(n-k)!} \frac{y^k}{k!} \\ &= \left(\sum_{m=0}^{\infty} \frac{x^m}{m!} \right) \left(\sum_{k=0}^{\infty} \frac{y^k}{k!} \right) \\ &= \exp_p(x) \exp_p(y). \end{aligned}$$

■

Esto muestra que, aparte del pequeño radio de convergencia, hemos obtenido algo que se parece mucho a la exponencial clásica. Por supuesto, hay una propiedad formal más que nos gustaría que fuera cierta también en el contexto p -ádico: el hecho de que el logaritmo y la exponencial son inversas, es decir, la relación

$$\exp(\log(1 + X)) = 1 + X$$

y su inversa.

Proposición 3.2.8. [5] Sea $x \in \mathbb{Z}_p$, $|x| < p^{-1/(p-1)}$. Entonces tenemos

$$|\exp_p(x) - 1| < 1$$

Esto quiere decir que $\exp_p(x)$ está en el dominio de $\log_p(x)$, y

$$\log_p(\exp_p(x)) = x.$$

Recíprocamente, si $|x| < p^{-1/(p-1)}$ tenemos

$$|\log_p(1 + x)| < p^{-1/(p-1)}$$

entonces el $\log_p(1 + x)$ está dentro del dominio de \exp_p , y

$$\exp_p(\log_p(1 + x)) = 1 + x.$$

Para los detalles de la demostración ver [5].

3.3. Series binomiales.

Queremos concluir nuestra exploración de las funciones elementales p -ádicas considerando series binomiales y las funciones que definen. En \mathbb{R} , sabemos que la función $x \rightarrow (1+x)^\alpha$ se puede desarrollar como una serie de potencias que converge para $|x| < 1$:

$$(1+X)^\alpha = B(\alpha, X) = \sum_{n=0}^{\infty} \binom{\alpha}{n} X^n,$$

donde

$$\binom{\alpha}{n} = \frac{(\alpha-n+1)(\alpha-n+2) \cdots (\alpha-1)\alpha}{n!}$$

Queremos usar esta serie para definir la versión p -ádica de esta función. En el contexto p -ádico, las propiedades de convergencia de la serie dependerán de la elección del número p -ádico α . Solo consideramos el caso cuando $\alpha \in \mathbb{Z}_p$ es un entero p -ádico.

Entonces, tomamos $\alpha \in \mathbb{Z}_p$ y consideramos la serie binomial

$$B(\alpha, X) = (1+X)^\alpha = \sum_{n=0}^{\infty} \binom{\alpha}{n} X^n.$$

Lo primero que debemos comprobar es que los coeficientes son enteros p -ádicos.

Sabemos que los coeficientes binomiales evaluados sobre los números enteros son números enteros. De la misma manera, los coeficientes binomiales evaluados sobre los números enteros p -ádicos, también son enteros p -ádicos, y lo mencionamos formalmente en el siguiente resultado.

Lema 3.3.1. [5] Si $\alpha \in \mathbb{Z}_p$, y $n \geq 0$, entonces $\binom{\alpha}{n} \in \mathbb{Z}_p$

Demostración. Para cada n , consideramos el polinomio

$$P_n(X) = \frac{X(X-1) \cdots (X-n+1)}{n!} \in \mathbb{Q}[X].$$

Al igual que cualquier polinomio, $P_n(X)$ define una función continua de \mathbb{Q}_p a \mathbb{Q}_p . Ahora, sabemos que el coeficiente binomial $\binom{m}{n}$ de dos enteros positivos $m, n \in \mathbb{Z}_+$ está en \mathbb{Z} . Por lo tanto, para $\alpha \in \mathbb{Z}_+$, tenemos

$$P_n(\alpha) = \binom{\alpha}{n} \in \mathbb{Z}$$

En otras palabras, la función continua P_n mapea el conjunto \mathbb{Z}_+ de enteros positivos a \mathbb{Z} . Por continuidad, debe mapear la clausura de \mathbb{Z}_+ en \mathbb{Z}_p a la clausura

de \mathbb{Z} . Pero recordemos que cualquier elemento en \mathbb{Z}_p es el límite de una sucesión de enteros positivos (las sumas parciales de su expansión p -ádica). Por lo tanto, el cierre de \mathbb{Z}_+ es todo \mathbb{Z}_p , y concluimos que P_n mapea \mathbb{Z}_p a \mathbb{Z}_p , que es lo que queremos probar. ■

A partir de la observación anterior, definimos los binomiales p -ádicos.

Definición 3.3.2. Podemos pensar en el coeficiente binomial p -ádico evaluado en la variable $x \in \mathbb{Z}_p$, como un polinomio de variable entera p -ádica y coeficientes en los números p -ádicos, así

$$\binom{x}{n} = \frac{x(x-1) \cdot \dots \cdot (x-n+2)(x-n+1)}{n!}$$

A la vez, sigue cumpliendo las propiedades elementales de los coeficientes binomiales:

- Fórmula de Pascal

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}; \quad 1 \leq k \leq n.$$

- $\binom{n}{k} = \frac{n}{k} \binom{n-1}{k-1}$
- $\binom{n}{k} \binom{m}{n-k} = \binom{m}{k} \binom{m-k}{n-k}$

Corolario 3.3.3. [5] Si $\alpha \in \mathbb{Z}_p$ y $|x| < 1$, la serie

$$B(\alpha, x) = \sum_{n=0}^{\infty} \binom{\alpha}{n} x^n,$$

converge.

Capítulo 4

Teorema de Mahler

4.1. Expansiones de Mahler

La motivación de este capítulo es el estudio de las funciones continuas de \mathbb{Z}_p en \mathbb{Q}_p . Desde el punto de vista del análisis funcional, es natural considerar el espacio $\mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p)$ de todas las funciones continuas $\mathbb{Z}_p \rightarrow \mathbb{Q}_p$. La analogía con el espacio “arquimediano” $\mathcal{C}([0, 1], \mathbb{R})$ de funciones continuas $[0, 1] \rightarrow \mathbb{R}$.

Observemos que así como $\mathcal{C}([0, 1], \mathbb{R})$, donde $[0, 1]$ es compacto y \mathbb{R} es completo, de la misma manera sucede con $\mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p)$, pues hemos demostrado que \mathbb{Z}_p es compacto y \mathbb{Q}_p es completo.

Para hablar sobre funciones continuas, es necesario definir la métrica sobre la que se completa el espacio, es decir:

$$d(f, g) = \begin{cases} \max_{x \in [0, 1]} |f(x) - g(x)| & \text{si } f, g : [0, 1] \rightarrow \mathbb{R}, \\ \max_{x \in \mathbb{Z}_p} |f(x) - g(x)|_p & \text{si } f, g : \mathbb{Z}_p \rightarrow \mathbb{Q}_p. \end{cases} \quad (4.1)$$

Observamos que en ambas métricas se alcanza el máximo, esto debido a que $|f(x) - g(x)| : [0, 1] \rightarrow \mathbb{R}$ y $|f(x) - g(x)|_p : \mathbb{Z}_p \rightarrow \mathbb{Q}_p$, son funciones continuas y toda función real evaluada y continua en un espacio compacto alcanza el máximo.

Teorema 4.1.1. La función definida en [4.1](#) es una métrica sobre $\mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p)$ respecto a la cual este se vuelve un espacio métrico completo.

Para una demostración detallada, véase [\[4\]](#).

A partir de lo anterior, podemos afirmar que el espacio $\mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p)$ dotado de la norma del supremo $\|\cdot\|_\infty$ definida por $\|f\|_\infty = \sup_{x \in \mathbb{Z}_p} |f(x)|_p$ es un **espacio de Banach p -ádico**.

A continuación observamos otra propiedad común a ambos espacios: la **densidad de las funciones polinomiales**.

- si $f : [0, 1] \rightarrow \mathbb{R}$, es continua y $\varepsilon > 0$, existe un polinomio $p(x)$ con coeficientes en reales tal que $|f(x) - p(x)| < \varepsilon$ para todo $x \in [0, 1]$.
- si $f : \mathbb{Z}_p \rightarrow \mathbb{Q}_p$, es continua y $\varepsilon > 0$, existe un polinomio $p(x)$ con coeficientes en \mathbb{Q}_p tal que $|f(x) - p(x)|_p < \varepsilon$ para todo $x \in \mathbb{Z}_p$.

La densidad de los polinomios con coeficientes reales fue mostrada por Weierstrass (1885). La densidad de los polinomios en $\mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p)$ fue probada por Dieudonné (1944). Mientras que las funciones reales no tienen buena descripción como una serie de potencias, ya que se comportan mal respecto a la diferenciabilidad; en 1985 Mahler muestra que las funciones p -ádicas continuas tienen una buena descripción como series infinitas de una clase especial de polinomios.

Teorema 4.1.2 (Mahler). *Toda función continua $f : \mathbb{Z}_p \rightarrow \mathbb{Q}_p$ se puede escribir en de la forma*

$$f(x) = \sum_{n \geq 0} a_n \binom{x}{n} = a_0 + a_1 x + a_2 \binom{x}{2} + a_3 \binom{x}{3} + \dots \quad (4.2)$$

Para todo $x \in \mathbb{Z}_p$, donde $a_n \in \mathbb{Q}_p$ y $a_n \rightarrow 0$ cuando $n \rightarrow \infty$.

Observación 4.1.3. *Veremos que hay una fórmula para los coeficientes de esta representación en términos de f al igual que pasa en el caso real para la fórmula de Taylor, sin embargo debe distinguirse que la fórmula descrita en nuestro teorema es para una función continua arbitraria. Recordemos que El hecho que $\binom{x}{n}$, sea diferenciable no implica que toda la representación adopte esta propiedad.*

La expansión [4.2](#) es llamada expansión de Mahler de f y los números a_n son los coeficientes de Mahler de f . Si $f_N(x) = \sum_{n=0}^N a_n \binom{x}{n}$, entonces

$$|f(x) - f_N(x)|_p = \left| \sum_{n \geq N} a_n \binom{x}{n} \right|_p \leq \sup_{n \geq N+1} |a_n|_p.$$

Esto sucede porque los coeficientes binomiales son enteros p -ádicos. El máximo sucede cuando $N \rightarrow \infty$, ya que $a_n \rightarrow 0$. Entonces la expansión de Mahler es una muy útil aproximación de funciones continuas $\mathbb{Z}_p \rightarrow \mathbb{Q}_p$ por polinomios.

La teoría de los espacios p -ádicos de Banach está muy lejos de ser tan rica como su contraparte de arquimediana; es bastante cercano al de los espacios de Hilbert. En particular, la siguiente noción reemplaza la de una base de Hilbert en un espacio de Hilbert.

En el lenguaje del análisis funcional, puede comprobarse que la familia de funciones $\binom{x}{n}$, donde $x \in \mathbb{Z}_p$, conforman una base ortonormal para el espacio de Banach p -ádico $\mathbb{C}(\mathbb{Z}_p, \mathbb{Q}_p)$. Para más detalles, véase [3].

Antes de ir a la demostración del teorema, probaremos algunos resultados preliminares.

Veamos porqué la serie infinita $\sum_{n \geq 0} a_n \binom{x}{n}$ con $a_n \rightarrow 0$ en \mathbb{Q}_p es una función continua y convergente en \mathbb{Z}_p .

- Cuando $a_n \rightarrow 0$ en \mathbb{Q}_p , la serie $\sum_{n \geq 0} a_n \binom{x}{n}$ es convergente.

Primero observemos que $\binom{x}{n} \in \mathbb{Z}_p$. Recordemos que para todo entero p -ádico x podemos encontrar una sucesión de enteros que converge a él, digamos $\{x_i\}_n \geq 0$. Por la continuidad p -ádica de los polinomios y evaluar el coeficiente binomial en \mathbb{N} , entonces para cada $x \in \mathbb{Z}_p$, una sucesión $\binom{x_i}{n}$ de enteros converge a $\binom{x}{n}$, por tanto es un entero p -ádico, de aquí que $\left| \binom{x}{n} \right|_p \leq 1$, $x \in \mathbb{Z}_p$, entonces $\left| a_n \binom{x}{n} \right|_p \leq |a_n|_p$. Esto prueba que $\left| a_n \binom{x}{n} \right|_p \rightarrow 0$ cuando $|a_n|_p \rightarrow 0$. Por lo tanto la serie es convergente.

- Cuando $a_n \rightarrow \mathbb{Q}_p$, la función $f : \mathbb{Z}_p \rightarrow \mathbb{Q}_p$ definida por $f(x) = \sum_{n \geq 0} a_n \binom{x}{n}$ es continua.

Probaremos que f es continua punto a punto, digamos x_0 . Sea $\varepsilon > 0$, como $|a_n| \rightarrow 0$, existe un N tal que $|a_n|_p < \varepsilon$ para $n \geq N$. Recordamos que al ser polinomio, $\binom{x}{n}$ es continua para $0 \leq n \leq N - 1$ en x_0 , entonces tomando

el δ mínimo usado en cada definición $\varepsilon - \delta$ de continuidad en x_0 para el coeficiente binomial, tenemos un $\delta > 0$ tal que

$$|x - x_0|_p < \delta \rightarrow \left| \binom{x}{n} - \binom{x_0}{n} \right| < \varepsilon \quad (4.3)$$

Para $n \in \{1, \dots, N-1\}$. Luego, si $|x - x_0|_p < \delta$,

$$|f(x) - f(x_0)|_p = \left| \sum_{n \geq 0} a_n \left(\binom{x}{n} - \binom{x_0}{n} \right) \right|_p \leq \max_{n \geq 0} |a_n|_p \left| \binom{x}{n} - \binom{x_0}{n} \right|_p.$$

Ya que $\binom{x}{n} - \binom{x_0}{n} \in \mathbb{Z}_p$ tenemos $|a_n|_p \left| \binom{x}{n} - \binom{x_0}{n} \right|_p \leq |a_n|_p < \varepsilon$, para $n \geq N$. Por otro lado, para $n \in \{1, \dots, N-1\}$, decimos que

$$|a_n|_p \left| \binom{x}{n} - \binom{x_0}{n} \right|_p \leq |a_n|_p \varepsilon$$

, por lo visto en (4.3). Tomemos $A = \max_{n \geq 0} |a_n|_p$, entonces $|a_n|_p \leq A$ para todo n . Entonces

$$|x - x_0|_p < \delta \rightarrow |f(x) - f(x_0)|_p \leq \max \{ \varepsilon, A\varepsilon \} = \max \{ 1, A\varepsilon \},$$

f es continua para x_0 arbitrario, por tanto es continua en todo \mathbb{Z}_p

Observación 4.1.4. Hemos utilizado la propiedad no arquimediana para una cantidad infinita de elementos. Lo podemos hacer debido a que $a_n \rightarrow 0$, entonces su máximo se alcanza en un n_0 , y luego los demás valores se vuelven pequeños cuando n crece. [2]

A continuación estudiamos algunas propiedades de los coeficientes de la expansión de Mahler. Resulta que en analogía a la forma de los coeficientes de la expansión de Taylor de una función de variable real, los coeficientes de la expansión de Mahler se determinan iterando cierto operador de diferencias.

Teorema 4.1.5. [4] Si $a_n \rightarrow 0$ en \mathbb{Q}_p y $f(x) = \sum_{n \geq 0} a_n \binom{x}{n}$ para $x \in \mathbb{Z}_p$, entonces en términos de f tenemos $a_n = (\Delta^n f)(0)$.

Para ilustrar la forma de estos coeficientes, hagamos unos cálculos sencillos para los primeros: tomando $x = 0$,

$$f(0) = \sum_{n \geq 0} a_n \binom{x}{n} = a_0 \binom{0}{0}$$

Obtenemos $f(0) = a_0$, ya que sabemos que el coeficiente binomial se anula para $n > 0$, entonces del lado derecho se anulan todos los términos excepto el término $a_0 \binom{0}{0} = a_0$. Haciendo un procedimiento similar podemos determinar algunos coeficientes más, por ejemplo con $x = 1$:

$$\begin{aligned} f(1) &= \sum_{n \geq 0} a_n \binom{x}{n} = a_0 \binom{1}{0} + a_1 \binom{1}{1} \\ &= a_0 + a_1 \end{aligned}$$

Pero $f(0) = a_0$, entonces podemos ver que $a_1 = f(1) - f(0)$. Tomando $x = 2$, determinamos que $a_2 = f(2) - 2f(1) + f(0)$. A partir de estos cálculos para los primeros coeficientes, podemos hacernos la idea de que pueden expresarse en términos de $f(0), f(1), f(2), \dots, f(n)$. En general, para un n arbitrario, necesitamos introducir el operador de diferencias Δ que para cada función $f : \mathbb{Z}_p \rightarrow \mathbb{Q}_p$, se define como $\Delta f : \mathbb{Z}_p \rightarrow \mathbb{Q}_p$ como:

$$(\Delta f)(x) : f(x+1) - f(x)$$

Esta función se puede iterar para obtener las funciones $\Delta^n f$ para $n \geq 1$, así: $\Delta^2 f = \Delta(\Delta f)$, y más generalmente $\Delta^n f = \Delta(\Delta^{n-1} f)$. Tomando $\Delta^0 f = f$, esto es análogo a la derivada $f^{(0)}$ de la función f que es sí misma.

El operador de diferencias Δ , es discreto ya que se define para sucesiones, en analogía con la derivada para funciones continuas de variable real. Se comporta muy bien en los polinomios del coeficiente binomial porque los desplaza hacia el anterior: $\Delta \binom{x}{n} = \binom{x}{n-1}$ para $n \geq 1$, y $\Delta \binom{x}{n} = \Delta(1)$ es la función cero. Por la recursión del triángulo de Pascal para coeficientes binomiales, si $n \geq 1$ tenemos

$$\Delta \binom{x}{n} = \binom{x+1}{n} - \binom{x}{n} = \left(\binom{x}{n-1} + \binom{x}{n} \right) - \binom{x}{n} = \sum_{n \geq 1} a_n \binom{x}{n-1}.$$

Aplicando Δ a la función $f : \mathbb{Z}_p \rightarrow \mathbb{Q}_p$ con expansión de Mahler $\sum_{n \geq 0} a_n \binom{x}{n}$ donde $a_n \rightarrow 0$,

$$\begin{aligned} (\Delta f)(x) &= \sum_{n \geq 0} a_n \binom{x+1}{n} - \sum_{n \geq 0} a_n \binom{x}{n} \\ &= \sum_{n \geq 0} a_n \left(\binom{x+1}{n} - \binom{x}{n} \right) \\ &= \sum_{n \geq 1} a_n \binom{x}{n-1} \end{aligned}$$

Donde el coeficiente a_0 ha bajado una posición y no aparece en la última expresión. Cambiando el índice de la serie a partir de $n = 0$,

$$\Delta \sum_{n \geq 0} a_n \binom{x}{n} = \sum_{n \geq 0} a_{n+1} \binom{x}{n} = a_1 + a_2 x + a_3 \binom{x}{2} + a_4 \binom{x}{3} + \dots$$

El efecto de aplicar el operador Δ a la expansión de Mahler m veces se traduce en bajar m posiciones a cada coeficiente:

$$\Delta^m \sum_{n \geq 0} a_n \binom{x}{n} = \sum_{n \geq 0} a_{n+m} \binom{x}{n} = a_m + a_{m+1} x + a_{m+2} \binom{x}{2} + a_{m+3} \binom{x}{3} + \dots$$

Evaluando $x = 0$, observamos que solamente todos los términos se anulan, excepto la constante a_m y de esta manera se sigue la demostración del teorema anterior.

Ahora vamos a encontrar una fórmula para $(\Delta^n f)(0)$ o verificar la conjetura anterior de que a_n puede escribirse en términos de $f(0), f(1), \dots, f(n)$. En lugar de centrarse en la función $\Delta^n f$ solamente en $x = 0$, es más fácil ver lo que está pasando obteniendo una fórmula para $(\Delta^n f)(x)$ para x general.

Primero calculemos las fórmulas $(\Delta^2 f)(x)$ y $(\Delta^3 f)(x)$:

$$\begin{aligned} (\Delta^2 f)(x) &= (\Delta(\Delta f))(x) \\ &= (\Delta f)(x+1) - (\Delta f)(x) \\ &= (f((x+1)+1) - f(x+1)) - (f(x+1) - f(x)) \\ &= f(x+2) - 2f(x+1) + f(x) \end{aligned}$$

$$\begin{aligned} (\Delta^3 f)(x) &= (\Delta(\Delta^2 f))(x) \\ &= (\Delta^2 f)(x+1) - (\Delta^2 f)(x) \\ &= (f(x+3) - 2f(x+2) + f(x+1)) - (f(x+2) - 2f(x+1) + f(x)) \\ &= f(x+3) - 3f(x+2) + 3f(x+1) - f(x). \end{aligned}$$

Obtenemos este resultado para una función $f : \mathbb{Z}_p \rightarrow \mathbb{Q}_p$ en general. Notemos que el coeficiente binomial alterna los signos.

Teorema 4.1.6. [4] Sea $f : \mathbb{Z}_p \rightarrow \mathbb{Q}_p$ una función. Para $n \geq 0$ y $x \in \mathbb{Z}_p$,

$$(\Delta^n f)(x) = \sum_{k=0}^n (-1)^{n-k} \binom{n}{k} f(x+k).$$

Demostración.

Utilizando inducción sobre n , vemos que $\Delta^0 f(x) = f(x)$ cuando $n = 0$, y $\Delta^1 f(x) = f(x+1) - f(x)$. Suponiendo que la fórmula funciona hasta algún n y para todo $x \in \mathbb{Z}_p$, entonces

$$\begin{aligned} (\Delta^{n+1} f)(x) &= (\Delta(\Delta^n f))(x) \\ &= (\Delta^n f)(x+1) - (\Delta^n f)(x) \\ &= \sum_{k=0}^n (-1)^{n-k} \binom{n}{k} f((x+1)+k) - \sum_{k=0}^n (-1)^{n-k} \binom{n}{k} f(x+k) \\ &= \sum_{k=0}^n (-1)^{n-k} \binom{n}{k} f(x+(k+1)) + \sum_{k=0}^n (-1)^{n-k+1} \binom{n}{k} f(x+k) \\ &= \sum_{k=1}^{n+1} (-1)^{n-(k-1)} \binom{n}{k-1} f(x+k) + \sum_{k=0}^n (-1)^{n-(k-1)} \binom{n}{k} f(x+k) \end{aligned}$$

El término en la primera suma cuando $k = n+1$ es $f(x+n+1)$. El término en la segunda suma cuando $k = 0$ es $(-1)^{n+1} f(x)$. Los términos restantes en ambas sumas corren desde $k = 1$ hasta $k = n$, y ambas son iguales, entonces

$$\sum_{k=1}^n (-1)^{n-(k-1)} \left(\binom{n}{k-1} + \binom{n}{k} \right) f(x+k) = \sum_{k=1}^n (-1)^{n-(k-1)} \binom{n+1}{k} f(x+k).$$

Los términos $f(x+n+1)$ y $(-1)^{n+1} f(x)$ se pueden introducir a esta suma como $k = n+1$ y $k = 0$ entonces.

$$(\Delta^{n+1} f)(x) = \sum_{k=0}^{n+1} (-1)^{n-(k-1)} \binom{n+1}{k} f(x+k) = \sum_{k=0}^{n+1} (-1)^{n+1-k} \binom{n+1}{k} f(x+k).$$

■

Corolario 4.1.7. [4] Si $f(x) = \sum_{n \geq 0} a_n \binom{x}{n}$ para $x \in \mathbb{Z}_p$, donde $a_n \rightarrow 0$ en \mathbb{Q}_p , entonces

$$a_n = (\Delta^n f)(0) = \sum_{k=0}^n (-1)^{n-k} \binom{n}{k} f(k).$$

Demostración. Por el teorema 4.1.5 sabemos que $a_n = (\Delta^n f)(0)$. De aquí solo basta tomar $x = 0$ en el teorema 4.1.6 y obtenemos el resultado buscado.

■

Este corolario nos muestra que cada función continua $f : \mathbb{Z}_p \rightarrow \mathbb{Q}_p$ se puede escribir como una única expansión de Mahler ya que sus coeficientes se determinan evaluando la función f en los enteros no negativos. Que los coeficientes de la serie de Mahler estén determinados de esta manera no es una sorpresa, recordando que \mathbb{N} es un conjunto denso en \mathbb{Z}_p , pareciera que cada función continua f en \mathbb{Z}_p está determinada por los valores que toma en \mathbb{N} . A continuación pasamos a la demostración del teorema de Mahler, en el que observaremos qué tan importante es este factor.

4.2. Demostración del teorema de Mahler

Hasta este momento hemos probado que los desarrollos llamados series de Mahler con coeficientes $a_n \in \mathbb{Q}_p$ y $a_n \rightarrow 0$ son funciones continuas, y también que dichos coeficientes pueden escribirse en términos de la imagen de \mathbb{N} bajo f . Usaremos estos resultados a lo largo de la demostración del teorema.

Demostración.[Teorema de Mahler]

Para una función continua $f : \mathbb{Z}_p \rightarrow \mathbb{Q}_p$, con

$$a_n := (\Delta^n f)(0) = \sum_{k=0}^n (-1)^{n-k} \binom{n}{k} f(k),$$

probaremos dos cosas:

i). Probar que $a_n \rightarrow 0$ cuando $n \rightarrow \infty$, donde $a_n = (\Delta^n f)(0)$

ii). Probar que $f(x) = \sum_{n \geq 0} a_n \binom{x}{n}$, para todo $x \in \mathbb{Z}_p$

Comencemos la demostración observando que (ii) se sigue de (i), ya que tenemos que la serie $\sum_{n \geq 0} a_n \binom{x}{n}$ es continua en \mathbb{Z}_p , entonces, para demostrar que la serie es igual a f , basta con comprobar que estas dos funciones continuas son idénticamente iguales en el subconjunto denso de los enteros no negativos \mathbb{N} . Sea $m \in \mathbb{N}$,

$$\begin{aligned}
 \sum_{n \geq 0} a_n \binom{m}{n} &= \sum_{n \geq 0} \left(\sum_{k=0}^n (-1)^{n-k} \binom{n}{k} f(k) \right) \binom{m}{n} \\
 &= \left[\sum_{k=0}^0 (-1)^{0-k} \binom{0}{k} f(k) \right] \binom{m}{0} + \dots + \left[\sum_{k=0}^m (-1)^{m-k} \binom{m}{k} f(k) \right] \binom{m}{m} \\
 &= \sum_{k=0}^0 (-1)^{0-k} \binom{0}{k} \binom{m}{0} f(k) + \dots + \sum_{k=0}^m (-1)^{m-k} \binom{m}{k} \binom{m}{m} f(k) \\
 &= f(0) \left[(-1)^{0-0} \binom{0}{0} \binom{m}{0} + \dots + (-1)^{m-0} \binom{m}{0} \binom{m}{m} \right] \\
 &\quad + f(1) \left[(-1)^{1-1} \binom{1}{1} \binom{m}{1} + \dots + (-1)^{m-1} \binom{m}{2} \binom{m}{m} \right] \\
 &\quad + \dots + f(m) (-1)^{m-m} \binom{m}{m} \binom{m}{m} \\
 &= \sum_{k=0}^m \left(\sum_{n=k}^m (-1)^{n-k} \binom{n}{k} \binom{m}{n} \right) f(k)
 \end{aligned}$$

Luego, por propiedad del coeficiente binomial , vemos que

$$\begin{aligned}
 \sum_{k=0}^m \left(\sum_{n=k}^m (-1)^{n-k} \binom{n}{k} \binom{m}{n} \right) f(k) &= \sum_{k=0}^m \left(\sum_{n=k}^m (-1)^{n-k} \binom{m}{k} \binom{m-k}{n-k} \right) f(k) \\
 &= \sum_{k=0}^m \left(\sum_{n=k}^m (-1)^{n-k} \binom{m-k}{n-k} \right) \binom{m}{k} f(k) \\
 &= \sum_{k=0}^m \left(\sum_{n=0}^{m-k} (-1)^n \binom{m-k}{n} \right) \binom{m}{k} f(k)
 \end{aligned}$$

Observamos que el sumatorio más interno se comporta como el binomio de

Newton con $x = 1, y = -1$, hasta la potencia $n - k$, es decir, se anula así:

$$0 = (1 + (-1))^{m-k} = \sum_{n=0}^{m-k} (-1)^n \binom{m-k}{n} \quad \forall k < m.$$

Pero cuando $n = k$, tenemos $\sum_{n=0}^0 (-1)^n \binom{m-k}{n} = 1$. Este es el único valor no nulo del sumatorio interno, entonces:

$$\sum_{k=0}^m \left(\sum_{n=0}^{m-k} (-1)^n \binom{m-k}{n} \right) \binom{m}{k} f(k) = (1) \binom{m}{m} f(m) = f(m), \quad \forall m \in \mathbb{N}.$$

Por ser $\mathbb{N} \subset \mathbb{Z}_p$ un subconjunto denso, y como f y su respectiva expansión de Mahler son funciones continuas, por lo tanto estas coinciden en todo \mathbb{Z}_p , es decir

$$\sum_{n \geq 0} a_n \binom{m}{n} = f(x), \quad \forall x \in \mathbb{Z}_p.$$

Ahora, demostraremos [\(I\)](#), es decir que $a_n \rightarrow 0$, cuando $n \rightarrow \infty$, donde $a_n = (\Delta^n f)(0)$. Por [\[5\]](#), sabemos que la convergencia uniforme implica convergencia puntual para $a_n \in \mathbb{Q}_p$, es decir, veremos que $|(\Delta^n f(x))|_p \rightarrow 0$ uniformemente en x . Esto es $\|(\Delta^n f)\| \rightarrow 0$ cuando $n \rightarrow \infty$, donde $\|(\Delta^n f)\| := \max_{x \in \mathbb{Z}_p} |(\Delta^n f(x))|_p$. Observamos que para $n \in \mathbb{N}$

$$\begin{aligned} |(\Delta^{n+1} f)(x)|_p &= |(\Delta(\Delta^n f))(x)|_p \\ &= |(\Delta^n f)(x+1) - (\Delta^n f)(x)|_p \\ &\leq \max(|(\Delta^n f)(x+1)|_p, |(\Delta^n f)(x)|_p) \\ &\leq \|(\Delta^n f)\|, \end{aligned} \quad \forall x \in \mathbb{Z}_p$$

En particular, podemos decir que $\|(\Delta^{n+1} f)(x)\| \leq \|(\Delta^n f)(x)\|$. A partir de esta deducción, es fácil ver que $\|(\Delta^m f)(x)\| \leq \|(\Delta^n f)(x)\|$, para $m \geq n$, repitiendo este proceso las veces que deseamos. Hemos visto que la norma de Δ^n decrece cuando $n \rightarrow \infty$, entonces solo debemos probar que $\|(\Delta^{n_i} f)\| \rightarrow 0$ para una sucesión $n_1 < n_2 < \dots$ que tienda a ∞ conveniente. La sucesión adecuada para este proceso son las potencias p^r , es decir, $\|(\Delta^{p^r} f)\| \rightarrow 0$ con $r \rightarrow \infty$. Para $n \geq 1$ y $x \in \mathbb{Z}_p$,

$$\begin{aligned} (\Delta^n f)(x) &= \sum_{k=0}^n (-1)^{n-k} \binom{n}{k} f(x+k) - \sum_{k=0}^n (-1)^{n-k} \binom{n}{k} f(x) \\ &= \sum_{k=0}^n (-1)^{n-k} \binom{n}{k} (f(x+k) - f(x)), \end{aligned}$$

ya que $\sum_{k=0}^n (-1)^{n-k} \binom{n}{k} = (1-1)^n = 0$. El término para $k=0$ es $(-1)^n(f(x) - f(x)) = 0$, entonces el contador inicia desde $k=1$,

$$\sum_{k=1}^n (-1)^{n-k} \binom{n}{k} (f(x+k) - f(x)).$$

Tomando $n = p^r$ para $r \geq 0$, probaremos que en el sumatorio

$$(\Delta^{p^r} f)(x) = \sum_{k=1}^{p^r} (-1)^{p^r-k} \binom{p^r}{k} (f(x+k) - f(x)). \quad (4.4)$$

Cada término tiene un valor absoluto p -ádico pequeño cuando $r \rightarrow \infty$, independientemente del k y x . Para esto, la estrategia será probar que para $0 \leq k \leq p^r$, tenemos que $v_p \binom{p^r}{k} = r - v_p(k)$.

Por propiedad del coeficiente binomial, sabemos que $\binom{p^r}{k} = \frac{p^r}{k} \binom{p^r-1}{k-1}$. Además sabemos que $v_p \left(\frac{p^r}{k} \right) = p^r - v_p(k)$, entonces este cálculo se reduce a probar que

$$\begin{aligned} v_p \binom{p^r-1}{k-1} &= v_p \left(\frac{(p^r-1)!}{(k-1)!(p^r-k)!} \right) \\ &= v_p((p^r-1)!) - v_p((k-1)!(p^r-k)!) \\ &= v_p((p^r-1)!) - v_p((k-1)!) - v_p((p^r-k)!) = 0, \end{aligned}$$

es decir, que no es divisible entre p .

Por la fórmula de Polignac p -ádica, necesitamos contar la suma los dígitos p -ádicos de cada uno de estos factoriales:

$$\begin{aligned} p^r - 1 &= p^r + (p-1) + (p-1)p + \dots + (p-1)p^{r-1} + (p-1)p^r + \dots \\ &= (p-1) + (p-1)p + \dots + (p-1)p^{r-1} \end{aligned}$$

De aquí observamos que tiene un total de p^r -veces el dígito $p-1$, entonces $s_p((p^r-1)!) = (p-1)r$.

Supongamos que $k = c_i p^i + c_{i+1} p^{i+1} + \dots + c_{r-1} p^{r-1}$, con $c_i \neq 0$. De aquí que

$$\begin{aligned}
k-1 &= c_i p^i + c_{i+1} p^{i+1} + \dots + c_{r-1} p^{r-1} + (p-1) + (p-1)p + \dots + (p-1)p^r + \dots \\
&= (p-1) + (p-1)p + \dots + (p-1)p^i + c_i p^i + \dots + (p-1)p^{r-1} + \dots
\end{aligned}$$

Observamos que a partir de $(p-1)p^i$, el término p^{i+1} que sale de este, se anula con el de signo contrario del siguiente término y de igual manera con los términos que siguen a partir de este excepto el término $-p^i$. Entonces la expresión se reduce

$$k-1 = (p-1) + (p-1)p + \dots + (p-1)p^{i-1} + (c_i - 1)p^i + c_{i+1}p^{i+1} + \dots + c_{r-1}p^{r-1}$$

De aquí observamos que el dígito $p-1$ se repite i -veces, y los otros dígitos son $s_p(k) - 1$, entonces $s_p(k-1) = (p-1)i + s_p(k) - 1$.

Solo nos resta sumar los dígitos de $p^r - k = p^r - (c_i p^i + \dots + c_{r-1} p^{r-1})$. Los reordenamos convenientemente de la siguiente manera

$$\begin{aligned}
p^r - k &= p^r - (c_i p^i + \dots + c_{r-1} p^{r-1}) + p^{i+1} - p^{i+1} + \dots + p^{r-1} - p^{r-1} \\
&= (p - c_i) p^i + (p - 1 - c_{i+1}) p^{i+1} + \dots + (p - 1 - c_{r-1}) p^{r-1}.
\end{aligned}$$

De aquí que $s_p(p^r - k) = p + (p-1)(r-i-1) - s_p(k)$. Por lo tanto, aplicando la fórmula de Polignac, tenemos

$$\begin{aligned}
v_p \binom{p^r - 1}{k - 1} &= v_p((p^r - 1)!) - v_p((k - 1)!) - v_p((p^r - k)!) \\
&= \frac{p^r - 1 - s_p(p^r - 1)}{p - 1} - \frac{k - 1 - s_p(k - 1)}{p - 1} - \frac{p^r - k - s_p(p^r - k)}{p - 1} \\
&= \frac{s_p(k - 1) + s_p(p^r - k) - s_p(p^r - 1)}{p - 1} \\
&= \frac{(p - 1)i + s_p(k) - 1 + p + (p - 1)(r - i - 1) - s_p(k) - (p - 1)r}{p - 1} \\
&= 0,
\end{aligned}$$

lo que queríamos probar.

Queremos probar que para todo $\varepsilon > 0$, $|(\Delta^{p^r} f)(x)|_p < \varepsilon$ para $r \rightarrow \infty$ y todo $x \in \mathbb{Z}_p$. De (4.4),

$$|(\Delta^{p^r} f)(x)|_p \leq \max_{1 \leq k \leq p^r} \left| \binom{p^r}{k} \right|_p |f(x+k) - f(x)|_p.$$

Cada término en el máximo está acotado ya que $\left| \binom{p^r}{k} \right|_p \leq 1$ y $|f(x+k) - f(x)|_p \leq \|f\|$.

Para $1 \leq k \leq p^r$, probamos que $\left| \binom{p^r}{k} \right|_p = 1/p^{r-v_p(k)} = 1/(p^r |k|_p)$, entonces $\left| \binom{p^r}{k} \right|_p |k|_p = 1/p^r$. Por lo tanto $\left| \binom{p^r}{k} \right|_p \leq 1/\sqrt{p^r}$ o $|k|_p \leq 1/\sqrt{p^r}$. Tomando $\varepsilon > 0$, existe $\delta > 0$ tal que $|x-y|_p < \delta$ implica que $|f(x) - f(y)|_p < \varepsilon$. Ahora, tomemos R lo suficientemente grande tal que $1/\sqrt{p^R} < \min(\delta, \varepsilon)$. Entonces para $r \geq R$ y $1 \leq k \leq p^r$, tenemos dos opciones:

- Si $\left| \binom{p^r}{k} \right|_p \leq 1/p^r$, entonces

$$\left| \binom{p^r}{k} \right|_p |f(x+k) - f(x)|_p \leq (1/\sqrt{p^r}) \|f\|_p \leq \varepsilon \|f\|_p.$$

- Si $|k|_p \leq 1/\sqrt{p^r}$, tenemos $|k|_p \leq \delta$, entonces para $x \in \mathbb{Z}_p$ tenemos que $|x+k-x|_p \leq \delta$. De aquí que $|f(x+k) - f(x)|_p < \varepsilon$, entonces

$$\left| \binom{p^r}{k} \right|_p |f(x+k) - f(x)|_p \leq |f(x+k) - f(x)|_p < \varepsilon.$$

Por lo tanto, para todo $\varepsilon > 0$, existe $R > 0$, tal que $r \geq R \implies \|\Delta^{p^r} f\| \leq \varepsilon \max(\|f\|, 1)$. ■

A continuación desarrollaremos algunos ejemplos de funciones continuas en \mathbb{Z}_p a partir de una sucesión $a_n \rightarrow$ en \mathbb{Q}_p que sirven como el coeficiente de su expansión en serie de Mahler.

Ejemplo 4.2.1. [4] Para $a \in 1 + p\mathbb{Z}_p$, tenemos que $|a-1|_p \leq 1/p$ en \mathbb{Q}_p entonces la serie

$$f(x) = \sum_{n \geq 0} (a-1)^n \binom{x}{n}$$

es continua en \mathbb{Z}_p ya que $|(a-1)^n|_p \rightarrow 0$. Para un entero positivo m tenemos que $\binom{m}{n} = 0$ para $n > m$, entonces

$$f(m) = \sum_{n=0}^m (a-1)^n \binom{m}{n} = (1 + (a-1))^m = a^m.$$

Entonces tenemos una interpolación p -ádica de la sucesión $\{a^m\}$ para $m \in \mathbb{N}$ a una función continua en todo \mathbb{Z}_p debido a la densidad de \mathbb{N} , la denotamos por a^x :

$$a^x = \sum_{n \geq 0} (a-1)^n \binom{x}{n}, \quad \text{para } x \in \mathbb{Z}_p.$$

Por ejemplo, en \mathbb{Q}_2 con $a = -1$ tenemos

$$\sum_{n \geq 0} (-2)^n \binom{x}{n} = (-1)^x \begin{cases} 1, & \text{si } x \in 2\mathbb{Z}_2, \\ -1 & \text{si } x \in 1 + 2\mathbb{Z}_2. \end{cases}$$

Es interesante lo “no trivial” que parece la expansión de Mahler de esta función localmente constante en \mathbb{Z}_2 .

Ejemplo 4.2.2. [4] Sea $\{p^n\}_{n \geq 0}$, es claro que $|p^n| \rightarrow 0$ en \mathbb{Q}_p cuando $n \rightarrow \infty$, entonces la serie

$$f(x) = \sum_{n \geq 0} p^n \binom{x}{n}$$

es continua en \mathbb{Z}_p . En particular, para $m \in \mathbb{N}$, tenemos

$$f(m) = \sum_{n=0}^m p^n \binom{m}{n} = (1+p)^m.$$

Por lo tanto, concluimos que esta es la representación en serie de Mahler para la función

$$(1+p)^x = \sum_{n \geq 0} p^n \binom{x}{n}.$$

Pregunta extra: ¿relación con la exponencial p -ádica?

Ejemplo 4.2.3. [4] Sea $z = a_{-1}p^{-1} + a_0 + a_1p + a_2p^2 + \dots$, con $a_{-1} \neq 0$ y $0 \leq a_i \leq p-1$, para $i > -1$. Tomemos en cuenta la sucesión $\{(p^2z)^n\}_{n \geq 0}$. Observamos que $|(p^2z)^n| \rightarrow 0$ en \mathbb{Q}_p cuando $n \rightarrow \infty$. Entonces la serie

$$f(x) = \sum_{n \geq 0} (p^2z)^n \binom{x}{n}$$

4.2. DEMOSTRACIÓN DEL TEOREMA DE MAHLER

es continua en \mathbb{Z}_p . En particular para $m \in \mathbb{N}$, tenemos

$$f(m) = \sum_{n=0}^m (p^2z)^n \binom{n}{m} = (1 + p^2z)^m.$$

Por lo tanto, concluimos que esta es la representación en serie de Mahler para la función

$$(1 + p^2z)^x = \sum_{n \geq 0} (p^2z)^n \binom{x}{n}.$$

En general, podemos escribir una función de este tipo tomando

$$z = a_{-i}p^{-i} + a_{-i+1}p^{-i+1} + \dots,$$

con $a_{-i} \neq 0$ y tomando la sucesión $\{(p^{i+1}z)^n\}_n \geq 0$, ya que esta sucesión converge a 0 en \mathbb{Q}_p .

Capítulo 5

Aplicaciones del teorema de Mahler

5.1. Motivación

En la teoría general de sistemas dinámicos, nos interesa estudiar funciones definidas sobre un espacio de medida X con características especiales respecto a la medida, como son las funciones que preservan medidas y las funciones ergódicas. En nuestro caso, nos interesa específicamente estudiar funciones ergódicas definidas sobre \mathbb{Z}_p^n .

Para estudiar una aplicación de las funciones expresadas en su representación de expansión de Mahler, primero escribiremos algunas definiciones y propiedades de nuestro interés.

Teorema 5.1.1. [1] Sea $f(x) = \sum_{n=0}^{\infty} a_i \binom{x}{n}$ la expansión de Mahler para una función $f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$; entonces f es 1-Lipschitz si y sólo si $a_i \equiv 0 \pmod{p^{-\lfloor \log_p i \rfloor}}$, para $i = 1, 2, \dots$

Notamos que $\lfloor \log_p m \rfloor = (\# \text{Dígitos base-} p \text{ de } m) - 1$; de aquí también asumimos que $\lfloor \log_p 0 \rfloor = 0$.

Básicamente la teoría de los sistemas dinámicos estudian transformaciones de espacios de medidas, entonces necesitamos definir una medida en el espacio métrico \mathbb{Z}_p^n (en realidad, esta medida será una medida de Haar).

Definición 5.1.2. [1] Definimos la medida de probabilidad $\mu = \mu_n$ en

$$\mathbb{Z}_p^n = \underbrace{\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_n$$

Los conjuntos medibles elementales son bolas $B_{p^{-r}}(a)$, $a \in \mathbb{Z}_p^n$ y $\mu(B_{p^{-r}}(a)) = p^{-r}$.

La medida μ es una medida de Borel: es decir, todo subconjunto abierto es μ -medible (por lo tanto, todo subconjunto cerrado también es μ -medible). La medida μ es regular: Es decir, para cualquier subconjunto A medible en μ

$$\begin{aligned}\mu(A) &= \sup\{\mu_p(S) : S \subset A, S \text{ es cerrado en } \mathbb{Z}_p^n\} \\ &= \inf\{\mu_p(S) : S \supset A, S \text{ es abierto en } \mathbb{Z}_p^n\}\end{aligned}$$

Un sistema dinámico en un espacio de fase (o espacio de configuración) S es una tripleta $(S; \mu; f)$, donde S es un espacio de medida dotado de una medida μ y $f : S \rightarrow S$ es una transformación medible; es decir, una f -preimagen $f^{-1}(S)$ de todo subconjunto $S \subset S$ medible en μ es un subconjunto medible en μ de S . Una trayectoria (u órbita) del sistema dinámico es una sucesión

$$x_0, x_1 = f(x_0), \dots, x_i = f(x_{i-1}) = f^i(x_0), \dots$$

de puntos del espacio S , x_0 es llamado el punto inicial de la trayectoria.

Definición 5.1.3 (Preservación de medida y ergodicidad.). *Un mapeo $F : S \rightarrow \mathbb{Y}$ de un espacio de medida S a un espacio de medida \mathbb{Y} dotados de medidas de probabilidad μ y ν , respectivamente, se dice que preserva medidas si y sólo si $\mu(F^{-1}(S)) = \nu(S)$ para cada subconjunto medible $S \subset \mathbb{Y}$.*

En el caso que $S = \mathbb{Y}$ y $\mu = \nu$ un mapeo que preserva medidas F es llamado ergodico si y sólo si dado un subconjunto medible S tal que $F^{-1}(S) = S$, entonces $\mu(S) = 1$ o $\mu(S) = 0$.

Ejemplo 5.1.4. *Sea S un conjunto finito, $\#S = N$, dotado de una medida de probabilidad uniforme μ : Dado $A \subset S$, $\#A = M$, decimos que $\mu(A) = \frac{M}{N}$. Una transformación f en S preserva medidas si y sólo si f es biyectiva, es decir, si f es una permutación de S .*

El mapeo f es ergodico si y sólo si consiste en un ciclo único, es decir, es transitivo.

Sea $(a_n)_{n=0}^{\infty}$ una sucesión de elementos de un espacio compacto S dotado de una medida de Borel μ , normalizada positiva, sea $N \in \mathbb{N}_0$, y sea $U \subset S$. Sea $\nu_N(U) = \sum_{n=0}^{N-1} \chi_U(a_n)$, donde χ_U es la función característica del subconjunto U ; es decir, $\chi_U(a) = 1$ si y sólo si $a \in U$, y $\chi_U(a) = 0$ en caso contrario. En otras palabras, $\nu_N(U)$ es el número de términos (de los primeros N términos de la sucesión (a_n)) que se encuentran en U .

Definición 5.1.5. *Una sucesión $(a_n)_{n=0}^{\infty}$ está uniformemente distribuida (con respecto a la medida μ) si y sólo si $\lim_{N \rightarrow \infty} \frac{\nu_N(U)}{N} = \mu(U)$ para todos los subconjuntos de Borel $U \subset S$ cuya frontera tiene medida 0.*

Teorema 5.1.6. Si $f : \mathbb{S} \rightarrow \mathbb{S}$ es ergódica, entonces μ -casi toda órbita

$$x_0, x_1 = f(x_0), \dots, x_i = f(x_{i-1}) = f^i(x_0), \dots$$

es uniformemente distribuida con respecto a μ .

Luego de enunciar las definiciones y propiedades anteriores, llegamos a la aplicación de la expansión de Mahler, que son resultados del profesor e investigador ruso Vladimir Anashin y compañía.

Para los siguientes dos teoremas, tengamos en cuenta $f(x) = \sum a_i \binom{x}{i}$, es decir, la representación en expansión de Mahler de una función f .

Teorema 5.1.7 (Condiciones suficientes para preservar medida, [1]). Una función f define una transformación 1-Lipschitz que preserva medidas sobre \mathbb{Z}_p si las siguientes condiciones se cumplen simultáneamente:

- a). $a_1 \not\equiv 0 \pmod{p}$
- b). $a_i \equiv 0 \pmod{p^{\lfloor \log_p i \rfloor + 1}}, i = 2, 3, \dots$

En el caso de $p = 2$ las condiciones suficientes también se vuelven necesarias; para el resto de primos $p > 2$ no lo son.

Teorema 5.1.8 (Condiciones suficientes para ergodicidad, [1]). La función f define una transformación 1-Lipschitz ergódica sobre \mathbb{Z}_p , con p impar, si las siguientes condiciones se cumplen simultáneamente:

- 1. $a_0 \not\equiv 0 \pmod{p}$;
- 2. $a_1 \equiv 1 \pmod{p}$, para p impar,
- 3. $a_1 \equiv 1 \pmod{4}$, para $p = 2$;
- 4. $a_i \equiv 0 \pmod{p^{\lfloor \log_p(i+1) \rfloor + 1}}, i = 2, 3, \dots$

5.2. Ejemplos

Observación 5.2.1. El siguiente es un ejemplo de una función continua y ergódica, propuesto en [1], y cuya demostración detallada paso a paso ha sido desarrollada por mí, Ricardo Córdova, como resultado de este proyecto de tesis.

Ejemplo 5.2.2. Mediante el teorema anterior [5.1.8], podemos comprobar que la función p -ádica de \mathbb{Z}_p en \mathbb{Z}_p y continua

$$f(x) = (1+p)x + (1+p)^x$$

5.2. EJEMPLOS

es ergódica.

Demostración.

Primero, expresaremos dicha función f en su representación por serie de Mahler. Para esto, invocamos el ejemplo 4.2.2.

$$f(x) = (1+p)x + (1+p)^x = \sum_{n=1}^1 p^n \binom{x}{n} + \sum_{n \geq 0} p^n \binom{x}{n}$$

de donde

$$f(x) = \sum_{n \geq 0} a_n \binom{x}{n}, \quad a_n = \begin{cases} 1, & n = 0 \\ 1 + 2p, & n = 1 \\ p^n, & n \geq 2 \end{cases}$$

De esta manera, podemos ver fácilmente que se cumplen los primeros dos requisitos del teorema:

- a) $a_0 = 1 \not\equiv 0 \pmod{p}$
- b) $a_1 = 1 + 2p \equiv 1 \pmod{p}$

Nos resta comprobar que

- c) $a_i = p^i \equiv 0 \pmod{p^{\lfloor \log_p(i+1) \rfloor + 1}}, i = 2, 3, \dots$

Esto se reduce a comprobar que $\lfloor \log_p(i+1) \rfloor + 1 \leq i$. Para esto, nos ayudaremos del siguiente lema.

Lema 5.2.3. Para $i = 2, 3, \dots$, y $p \geq 3$ se cumple la desigualdad

$$i + 1 \leq p^{i-1}.$$

Demostración.

Para $i = 2$ y $p = 3$, tenemos $3 \leq 3$. Supongamos que para $i = k$ se cumple $k + 1 \leq p^{k-1}$.

Como $p \geq 3$, observamos que

$$k + 2 \leq p(k + 1) \leq p^k.$$

De donde obtenemos el resultado. ■

Utilizando el resultado del lema anterior, y tomando en cuenta que la función real \log_p es creciente, tenemos que

$$\log_p(i + 1) \leq i - 1.$$

Ahora, ya que $\lfloor x \rfloor \leq x, \forall x \in \mathbb{R}^+$, tenemos

$$\lfloor \log_p(i+1) \rfloor \leq \log_p(i+1) \leq i-1.$$

Con lo que queda probada la desigualdad que necesitamos. Por lo tanto, la función $f(x) = (1+p)x + (1+p)^x$, es ergódica. ■

Observación 5.2.4. La función de este ejemplo, sigue siendo ergódica para $p = 2$.

- Observamos que se cumple el requisito para $p = 2$ del teorema:

$$a_1 = 1 + 2(2) \equiv 1 \pmod{4}.$$

- La desigualdad

$$\lfloor \log_p(i+1) \rfloor + 1 \leq i.$$

también cumple para $p = 2$.

Capítulo 6

Conclusiones

Conclusiones

El Teorema de Mahler es una herramienta poderosa en el análisis p -ádico, que permite aproximar cualquier función continua en un conjunto compacto de los números p -ádicos por una serie de funciones polinómicas. En particular, los resultados de Anashin han demostrado que el Teorema de Mahler es útil en la teoría ergódica para diagnosticar funciones ergódicas.

Este enfoque permite el estudio de ciertos sistemas dinámicos en los números p -ádicos, analizando las propiedades estadísticas de estos sistemas y detectando patrones y comportamientos recurrentes. La aplicación del Teorema de Mahler para diagnosticar funciones ergódicas tiene importantes implicaciones en áreas como la criptografía y la teoría de la información, donde se utilizan sistemas dinámicos en los números p -ádicos para proteger la información y garantizar la seguridad en la transmisión de datos.

En conclusión, el Teorema de Mahler y los resultados de Anashin tienen importantes aplicaciones en la teoría ergódica y en otras áreas de las matemáticas y la informática. Su estudio y aplicación pueden conducir a nuevos avances en el campo del análisis p -ádico y en la teoría de la información.

A continuación se mencionan los resultados centrales de este proyecto de tesis y las respectivas secciones donde se encuentran detallados.

Teorema 6.0.1 (Mahler). *Toda función continua $f : \mathbb{Z}_p \rightarrow \mathbb{Q}_p$ se puede escribir en de la forma*

$$f(x) = \sum_{n \geq 0} a_n \binom{x}{n} = a_0 + a_1 x + a_2 \binom{x}{2} + a_3 \binom{x}{3} + \dots \quad (6.1)$$

Para todo $x \in \mathbb{Z}_p$, donde $a_n \in \mathbb{Q}_p$ y $a_n \rightarrow 0$ cuando $n \rightarrow \infty$.

Para ver los detalles de la demostración y ejemplos, ver el capítulo 4.

Teorema 6.0.2 (Condiciones suficientes para ergodicidad, [1]). *La función f define una transformación 1-Lipschitz ergódica sobre \mathbb{Z}_p , con p impar, si las siguientes condiciones se cumplen simultáneamente:*

1. $a_0 \not\equiv 0 \pmod{p}$;
2. $a_1 \equiv 1 \pmod{p}$, para p impar,
3. $a_1 \equiv 1 \pmod{4}$, para $p = 2$;
4. $a_i \equiv 0 \pmod{p^{[\log_p(i+1)]+1}}$, $i = 2, 3, \dots$

Para ver los detalles de la demostración y ejemplos, ver el capítulo 5.

Ejemplo 6.0.3. [1] *Podemos comprobar que la función p -ádica de \mathbb{Z}_p en \mathbb{Z}_p y continua,*

$$f(x) = (1+p)x + (1+p)^x$$

es ergódica.

■

Para detalles, ver capítulo 5.

Capítulo 7

Proyectos a futuro

Proyectos a futuro

- En esta tesis se estudió una versión univariada del teorema de Mahler para funciones continuas de \mathbb{Z}_p en \mathbb{Q}_p , que nos permite representar dichas funciones de la siguiente manera:

$$f(x) = \sum_{n \geq 0} a_n \binom{x}{n} = a_0 + a_1 x + a_2 \binom{x}{2} + a_3 \binom{x}{3} + \dots$$

Se propone estudiar una versión multivariable del teorema de Mahler, con el objetivo de encontrar nuevas herramientas polinomiales para funciones multivariables continuas. Para más información, se propone confrontar [7].

- Calcular otras funciones de variable p -ádica, continuas y ergódicas a través del criterio coeficientes de Mahler.

Vale la pena mencionar que Anashin propone algunas funciones que cumplen estas condiciones en su artículo [1].

- Estudiar sucesiones p -ádicas equidistribuidas desde el punto de vista de los sistemas dinámicos p -ádicos, ya que existe una relación directa entre las órbitas que describen las funciones dentro de un sistema dinámico p -ádico y dichas sucesiones en el sentido que se mencionó en el capítulo 5.
- Estudiar espacios de Banach p -ádicos, para tener una mejor perspectiva del espacio de funciones sobre el que he trabajado en mi tesis. Para más información se propone confrontar [3].

Referencias

- [1] V. Anashin. *The p -adic Ergodic Theory and Applications*, volume 22 of *Progress in Mathematics*. Birkhäuser, 1989.
- [2] Y. Bilu. *P -adic Numbers and Diophantine Equations*, volume 153 of *Cambridge Tracts in Mathematics*. Cambridge University Press, 2000.
- [3] P. Colmez. *Éléments d'analyse et d'algèbre*, volume 28 of *Cours Spécialisés*. SMF, 2018.
- [4] K. Conrad. Mahler expansions. *The American Mathematical Monthly*, 112(7):612–629, 2005.
- [5] F. Q. Gouvêa. *p -adic Numbers: An Introduction*. Universitext. Springer, 1997.
- [6] P. Monsky. On dividing a square into triangles. *American Mathematical Monthly*, 77(2):161–164, 1970.
- [7] R. Rumely. A mahler measure for multivariable polynomials. *Journal of Number Theory*, 22(1):151–159, 1986.

Bibliografía

- Apostol, T. M. (1974). *Mathematical Analysis*. Addison-Wesley, Reading, MA, 2nd edition.
- Axler, S. (2017). *Linear Algebra Done Right*. Springer, New York, 3rd edition.
- Beshenov, A. (2018). *Álgebra abstracta: teoría de anillos y cuerpos*. Independently published.
- Hirsch, M. W., Smale, S., and Devaney, R. L. (1974). *Differential Equations, Dynamical Systems, and Linear Algebra*. Academic Press, New York, 1st edition.
- Lang, S. (1993). *Elliptic Functions*. Springer, New York, 2nd edition.
- Munkres, J. R. (2000). *Topology*. Prentice Hall.
- Niven, I., Zuckerman, H. S., and Montgomery, H. L. (1991). *An Introduction to the Theory of Numbers*. John Wiley Sons.
- Rudin, W. (1976). *Principles of Mathematical Analysis*. McGraw-Hill, New York, 3rd edition.
- Samuel, P. (2003). *Algebraic Theory of Numbers*. Dover Publications.