INTRODUCCIÓN A LOS NÚMEROS P-ÁDICOS Y ANÁLISIS P-ÁDICO

Deyanira Maldonado Guerrero

Universidad Industrial de Santander
Facultad de Ciencias
Escuela de Matemáticas
Bucaramanga
2015

INTRODUCCIÓN A LOS NÚMEROS P-ÁDICOS Y ANÁLISIS P-ÁDICO

Autor

Deyanira Maldonado Guerrero

Trabajo de grado para optar el título de

Matemático

Director

MSc. Edilberto J. Reyes González

Universidad Industrial de Santander
Facultad de Ciencias
Escuela de Matemáticas
Bucaramanga
2015

Agradecimientos

⋆ Quiero agradecer a Dios por haberme acompañado y protegido a lo largo de este camino.

⋆ A todos los profesores que contribuyeron en mi formación profesional, en especial quiero agradecer a mi Director de tesis el Profesor Edilberto Reyes González por su apoyo, colaboración, sugerencias, valiosos consejos y por haber hecho parte de mi formación académica durante mi carrera.

⋆ A mi padre Orlando Maldonado porque su recuerdo me hace fuerte y será la guía en toda mi vida, y a mi madre Matilde Guerrero por sus dedicación, sacrificios y entrega.

⋆ Un agradecimiento sincero y especial a la persona que hizo posible que este sueño se hiciera realidad a Juan Carlos Obregón mi compañía y apoyo incondicional, gracias por haber compartido este sueño conmigo.

Índice

Resumen

TÍTULO:

INTRODUCCIÓN A LOS NÚMEROS P-ÁDICOS Y ANÁLISIS P-ÁDICO[1]

AUTORA: Deyanira Maldonado Guerrero[2]

PALABRAS CLAVE: Números p-ádicos, Análisis p-ádico.

Resumen

Como se conoce del análisis clásico es posible construir el cuerpo $\mathbb{R}$ que complete al cuerpo de los números racionales, usando sucesiones de Cauchy de números racionales, a partir del valor absoluto euclidiano. Sin embargo, la definición de una sucesión de Cauchy depende de la métrica elegida, entonces si se usa un concepto distinto de distancia en $\mathbb{Q}$, se obtendrá otro cuerpo distinto a $\mathbb{R}$, para esto se tomará una nueva noción de distancia llamada norma p-ádica para un primo p que permite construir el cuerpo de los números p-ádicos $\mathbb{Q}_p$ como la completación de $\mathbb{Q}$ con dicha norma.

El cuerpo de los números p-ádicos posee entonces la propiedad de completitud, y por tanto al igual que $\mathbb{R}$, contiene a $\mathbb{Q}$ como subconjunto denso y esto permite el desarrollo del Análisis p-ádico, similar al Análisis Real. Además el hecho de que esta nueva norma cumple una propiedad llamada no-arquimediana, introduce ciertas diferencias respecto al caso real. Quizás la más importante de tales diferencias es el hecho de que en un contexto no-arquimediano se tiene una nueva caracterización de las sucesiones de Cauchy y esto proporcionará diferencias en cuanto a convergencia respecto del caso real y además esta propiedad añade ciertas curiosidades topológicas al conjunto de los números p-ádicos.

[1] Tesis.

[2] Facultad de Ciencias, Escuela de Matemáticas.
Director: Edilberto Reyes G.

Abstract

TITLE:

INTRODUCTION TO P-ADIC NUMBERS AND ANALYSIS P-ADIC [3]

AUTHOR: Deyanira Maldonado Guerrero[4]

KEYWORDS: P-adic numbers, P-adic analysis

Abstract

As known from the classical analysis is possible to build the body $\mathbb{R}$ to complete the body of rational numbers using Cauchy sequences of rational numbers from Euclidean absolute value. However, the definition of a Cauchy sequence depends on the chosen metric, then if a different concept of distance used in $\mathbb{Q}$, another different body will be obtained to $\mathbb{R}$, for this new notion will be taken distance called p-adic norm for a prime p that allows to build the body of p-adic numbers $\mathbb{Q}_p$ as the completion of $\mathbb{Q}$ with this norm.

The body of p-adic then has the property of completeness, and therefore as well as $\mathbb{R}$ contains the set $\mathbb{Q}$ as dense subset and this allows the development of p-adic analysis, similar to Real Analysis. Besides the fact that this new norm meets a property called non-Archimedean, introduces some differences in the Real case. Perhaps the most important of these differences is that in a non-Archimedean context has a new characterization of the Cauchy sequences and this provides differences in terms of convergence with regard the real case, and also certain topological curiosities of the set p-adic numbers.

[3] Thesis.

[4] Faculty of Science, School of Mathematics.
Directed by: Edilberto Reyes G

Introducción

Fácilmente se puede verificar que $x \equiv 2\,(mod\,5)$ y $x \equiv 3\,(mod\,5)$ son las únicas soluciones de la congruencias $x^2 \equiv -1\,(mod\,5)$ o $x^2 + 1 \equiv 0\,(mod\,5)$, es decir que si se considera en particular $x \equiv 2\,(mod\,5)$ se tiene que todo entero de la forma $x_1 = 2+5t$ es solución de dicha congruencia. Eligiendo t tal que $x_1 = 2 + 5t$ también sea solución de $x^2 \equiv -1\,(mod\,5^2)$ se obtiene que $x_2 = 2+1.\,5$ satisface las congruencias $x^2 \equiv -1\,(mod\,5)$ y $x^2 \equiv -1\,(mod\,5^2)$. Por lo tanto $x_2 = 2 + 1(5) + t(5^2)$ con $t \in \mathbb{Z}$ es solución de $x^2 \equiv -1\,(mod\,5^2)$ y eligiendo apropiadamente t se obtiene $x_3 = 2 + 1(5) + 2(5^2)$ que satisface la congruencia $x^2 \equiv -1\,(mod\,5^3)$. Continuando de esta manera, se puede encontrar x tal que este sea solución de $x^2 \equiv -1\,(mod\,5^n)$ para todo $n \in \mathbb{N}$, que será de la forma

$$x = 2 + 1(5) + 2(5^2) + 1(5^3) + 3(5^4) + 4(5^5) + \ldots \;= \sum_{k=0}^{\infty} a_k 5^k$$

donde $0 \leq a_k < 5$. Tal expresión se llama desarrollo $5-$ *ádico* de la solución de la congruencia $x^2 \equiv -1\,(mod\,5^n)$ para n suficientemente grande. Se espera que entre más términos se hallen de esta serie se obtiene una mejor aproximación de la solución de $x^2 \equiv -1\,(mod\,5^n)$, por tal razón se puede definir una distancia apropiada para que la diferencia entre la solución y la aproximación sea suficientemente pequeña.

En este trabajo se enunciarán dos formas equivalentes de definir el conjunto de los números p-ádicos. La primera es mas intuitiva, ya que se basa en los desarrollos de un número entero en base p donde p es un número primo, mientras que la segunda permite manejar este conjunto de números con mayor simplicidad y más formalmente, esta definición se obtiene a partir de otra noción de distancia sobre $\mathbb{Q}$ diferente a la usual y de esta manera se construye el conjunto de los números p-ádicos como la completación de los racionales con dicha norma usando sucesiones de Cauchy. Este conjunto de números tienen aplicaciones en muchas áreas de las matemáticas e incluso de la física, y son una herramienta fundamental en la Teoría de Números actual, incluyendo, en la famosa prueba del Último Teorema de Fermat por Andrew Wiles.

1. Desarrollos p-ádicos

Se empezará esta sección con la introducción de números enteros p-ádicos de manera informal, haciendo referencia a la escritura de un número entero en una base dada p, para cualquier número primo p. Este enfoque permitirá demostrar que los números enteros p-ádicos forman un anillo con las operaciones definidas entre ellos, denotado por $\mathbb{Z}_p$. Luego se agregan los inversos de los elementos no nulos de este conjunto y esto permite la construcción del cuerpo $\mathbb{Q}_p$.

1.1. Expansión p-ádica

Habitualmente se tiene los noción de números racionales expresados en el sistema de numeración de base 10, es decir en cifras cuyos dígitos van del 0 al 9 donde se han establecido de manera adecuada determinadas operaciones entre ellos. El método para operar con los números racionales se basa en el hecho de que estos se expresan en forma decimal, así por ejemplo:

$1235 = 1.10^3 + 2.10^2 + 3.10 + 5.10^0$

Además de con 10 esto puede hacerse para cualquier p donde $p \in \mathbb{Z} - \{0\}$, en particular se tomará el caso en el que p es primo. La idea es expresar cualquier número racional q como un polinomio en p que quizás involucre potencias negativas cuyos coeficientes sean números naturales menores p, a este desarrollo se le denomina desarrollo p-ádico de q.

Un entero p-ádico es por definición una sucesión de enteros $(a_i)_{i\in\mathbb{N}}$ donde $0 \leq a_i < p$. Se escribe esto convencionalmente como

$$\ldots a_i \ldots a_3 a_2 a_1 a_0$$

(es decir, los a_i se escriben de izquierda a derecha). El desarrollo p-ádico de un número entero positivo, coincide exactamente con el desarrollo en base p.

Un número $p-\acute{a}dico\ n = \sum_{i=0}^{\infty} a_i\, p^i$ puede ser identificado como la sucesión $(a_i)_{i\geq 0}$ de sus coeficientes. Esto significa que la escritura de los números naturales son exactamente la misma que para los enteros p-ádicos solo que un número finito de cuyas cifras no es 0. Además se tiene en cuenta también que 0 es el entero p-ádico cuyas cifras son todas 0, y 1 es el entero p-ádico donde todos sus dígitos son 0 excepto la primera cifra de la derecha que es 1.

Para encontrar los desarrollos p-ádicos de un número entero positivo n se utiliza el algoritmo de la división de la siguiente manera: Primero se divide n por p. Luego, al cociente de dicha operación se divide de nuevo por p, y así sucesivamente hasta llegar a un cociente que sea menor que p. La sucesión escrita en orden inverso dada por los residuos de las respectivas divisiones son los coeficientes con las potencias de p y este es el desarrollo p-ádico de n.

Este desarrollo p-ádico es único, (esta demostración se puede encontrar en cualquier libro de teoría de número o en la referencia bibliográfica [4] pag 8).

Ejemplo 1. Usando el algoritmo de la división se escribirá el número entero 2351 en base 5

$$\begin{aligned} 2351 = 470.5 + 1 &= (94.5 + 0).5 + 1 \\ &= 94.5^2 + 0.5 + 1 \\ &= (18.5 + 4).5^2 + 0.5 + 1 \\ &= 18.5^3 + 4.5^2 + 0.5 + 1 \\ &= (3.5 + 3).5^3 + 4.5^2 + 0.5 + 1 \\ &= \ldots 0.5^5 + 3.5^4 + 3.5^3 + 4.5^2 + 0.5 + 1 \end{aligned}$$

luego $2351 = \ldots 0.5^5 + 3.5^4 + 3.5^3 + 4.5^2 + 0.5 + 1$ donde las coeficientes de las potencias de 5 cuyo exponente es mayor que cuatro tiene valor 0.

Esta expansión p-ádica es similar a la escritura decimal, entonces de manera análoga como se hace en el desarrollo decimal se pueden realizar operaciones entre los enteros usando el desarrollo p-ádico.

Observación 2. Sean $a = (a_s a_{s-1} \ldots a_1 a_0)$ y $b = (b_t b_{t-1} \ldots b_1 b_0)$ dos números enteros expresados en base p y supóngase $a \neq b$. Luego $a = a_s p^s + \ldots + a_1 p + a_0$ y $b = b_t p^t + \ldots + b_1 p + b_0$, por el orden de los naturales se tiene que $a < b$ esto es $a_s p^s + \ldots + a_1 p + a_0 < b_t p^t + \ldots + b_1 p + b_0$ si y solo si $s < t$ ó $s = t$ y $a_k < b_k$ donde $k = max\{1 \leq i \leq s = t \,/ a_i \neq b_i\}$ este k existe pues $a \neq b$, este orden es el orden lexicográfico. Esto permite comparar los coeficientes de dos o más desarrollos p-ádicos, para tener mayor claridad al operar entre ellos. Cabe decir en general este conjunto no es ordenado como se verá en la sección 3.1.

1.2. Operaciones con desarrollos p-ádicos.

La utilidad de la representación en serie se evidencia cuando se introducen las operaciones algebraicas entre ellas. Las operaciones suma, resta, multiplicación y división,

se realiza de manera similar al proceso hecho en el desarrollo decimal, se mostrará como hacer este proceso en otras bases.

Ejemplo 3. Calcular $(\ldots 251453)_7 + (\ldots 121132)_7$

Claramente este proceso es el mismo que se hace en base 10, ya que cada vez que se suma las cifras correspondientes y se supera el número dado como base se debe agregar 1 a la cifra siguiente, es decir, utilizando congruencias esto es sumar módulo la base dada " llevando unidades " así.

$$\begin{array}{cccccccc} & \ldots & {}^{+1}2 & 5 & 1 & {}^{+1}4 & 5 & 3 \\ + & \ldots & 1 & 2 & 1 & 1 & 3 & 2 \\ \hline & \ldots & 4 & 0 & 2 & 6 & 1 & 5 \end{array}$$

Esta adición es asociativa, conmutativa, y se verifica la existencia del neutro, el cero cuyo número como se dijo anteriormente tiene todos sus dígitos nulos. Como el conjunto de los números enteros no negativos no es un anillo, primero se describirá la operación de la resta utilizando el orden dado en la observación 2, de manera que pueda asegurarse que el resultado sea un número entero, así:

Ejemplo 4. Tomando $60 = (\ldots 002020)_3$ y $16 = (\ldots 00121)_3$ claramente $60 - 16 = 44$ y $44 = (\ldots 001122)_3$

Este proceso es el mismo que se usa para restar habitualmente en base 10, ya que se operan las cifras correspondientes y cada vez que se reste de una cifra menor una mayor, se debe " prestar " de la cifra a su izquierda p unidades según la base dada, en el ejemplo anterior sería 3 , y se debe restar 1 a la siguiente cifra, es decir, utilizando congruencias y sustrayendo unidades así:

$$\begin{array}{ccccccc} \ldots & 2 & 0 & {}^{-1}2 & {}^{+3}0 & & \\ - & \ldots & 1 & 2 & 1 & \to & \\ \hline & & & & 2 & & \end{array} \quad \begin{array}{ccccccc} \ldots & 2 & {}^{-1}0 & {}^{+3}1 & {}^{+3}0 & & \\ - & \ldots & 1 & 2 & 1 & \to & \\ \hline & & & 2 & 2 & & \end{array} \quad \begin{array}{ccccc} \ldots & 2^{-1} & {}^{-1}0^{+3} & {}^{+3}1 & {}^{+3}0 \\ - & \ldots & 1 & 2 & 1 \\ \hline \ldots & 1 & 1 & 2 & 2 \end{array}$$

Note que en la resta se pueden obtener números negativos, el desarrollo de estos números de mostrará mas adelante. De manera análoga como se hace en base 10 se define el producto usando los desarrollos como expresiones polinómicas y aplicando la ley distributiva como se verá en el siguiente ejemplo.

Ejemplo 5. Calcular $(\ldots 121)_3 \times (\ldots 2020)_3$ esto es

$$\begin{aligned}(\ldots 121)_3 \times (\ldots 2020)_3 &= (1.3^2 + 2.3 + 1) \times (2.3^3 + 0.3 + 2.3 + 0) \\ &= 2.3^5 + 4.3^4 + 2.3^3 + 2.3^3 + 4.3^2 + 2.3 \\ &= 2.3^5 + 4.3^4 + 4.3^3 + 4.3^2 + 2.3\end{aligned}$$

Y como se puede notar esto desarrollo no esta en base 3, por lo tanto se debe expresar este resultado en dicha base así:

$$\begin{aligned}2.3^5 + 4.3^4 + 4.3^3 + 4.3^2 + 2.3 &= 2.3^5 + (3+1).3^4 + (3+1).3^3 + (3+1).3^2 + 2.3 \\ &= 2.3^5 + 3^5 + 1.3^4 + 3^4 + 1.3^3 + 3^3 + 1.3^2 + 2.3 \\ &= 3.3^5 + 2.3^4 + 2.3^3 + 1.3^2 + 2.3 \\ &= 1.3^6 + 0.3^5 + 2.3^4 + 2.3^3 + 1.3^2 + 2.3\end{aligned}$$

De ahí que $(\ldots 121)_3 \times (2020)_3 = (\ldots 1022120)_3$ y es evidente que este producto es similar al usado habitualmente, salvo que luego de multiplicar las cifras se debe sumar usando congruencias módulo la base dada, así:

$$\begin{array}{cccccc} \ldots & 2 & 0 & 2 & 0 \\ \times & \ldots & 1 & 2 & 1 \\ \hline & 2 & 0 & 2 & 0 \\ & {}^{+1}0 & 1 & 0 & \end{array}$$

En esta caso $2 \times 2 = 4 = 3(1) + 1$ se coloca el residuo 1 como resultado y se adiciona el cociente al resultado siguiente de la multiplicación, siguiendo así hasta completar el producto con las otras cifras, luego se procede a sumar de este modo se tiene:

$$\begin{array}{cccccccc} & \ldots & 0 & 2 & 0 & 2 & 0 \\ \times & \ldots & 0 & 0 & 1 & 2 & 1 \\ \hline & & & 2 & 0 & 2 & 0 \\ + & 1 & {}^{+1}1 & 1 & 1 & 0 & \\ {}^{+1} & 2 & 0 & 2 & 0 & & \\ \hline \ldots 1 & 0 & 2 & 2 & 1 & 2 & 0 \end{array}$$

Esta operación satisface algunas propiedades inmediatas, como la distributiva y asociativa.

1.3. Anillo de los números enteros p-ádicos

Hasta aquí se ha visto la forma de hallar la expansión p-ádica para un entero positivo, ahora se quiere hacer esto para números enteros negativos. Para ello se debe tener el desarrollo p-ádico de -1 y de ahí se pueden obtener los desarrollos de los demás números negativos esto es:

$$\begin{aligned} -1 = (p-1) - p &= (p-1) + [(p-1) - p] \,.\, p = (p-1) + (p-1) \,.\, p - p^2 \\ &= (p-1) + (p-1) \,.\, p + [(p-1) - p] \,.\, p \\ &= (p-1) + (p-1) \,.\, p + (p-1) \,.\, p^2 - p^3 \\ &= (p-1) + (p-1) \,.\, p + (p-1) \,.\, p^2 + [(p-1) - p] \,.\, p^3 \\ &= (p-1) + (p-1) \,.\, p + (p-1) \,.\, p^2 + (p-1) \,.\, p^3 - p^4 \ldots \end{aligned}$$

por lo tanto

$$-1 = (p-1) + (p-1) \,.\, p + (p-1) \,.\, p^2 + (p-1) \,.\, p^3 + (p-1) \,.\, p^4 + \ldots$$

de ahí que $-1 = (\ldots (p-1)\,(p-1)\,(p-1)\,(p-1))_p$ es la expansión p-ádica de -1 y análogamente se tiene que

$$-p = (\ldots (p-1)\,(p-1)\,(p-1)\,0)_p$$

Ejemplo 6. Escribir el desarrollo $7-$*ádico* de -12

Como $-12 \equiv 2\,(mod\,7)$ y además $-12 = -\,(1.\,7+5) = -7-5 = -7-7+2 = 2-7-7 = (2)_7 + (-7)_7 + (-7)_7 = (000002)_7 + (\ldots 66660)_7 + (\ldots 66660)_7 = (\ldots 666652)_7$

Como consecuencia de esto se tiene el siguiente lema.

Lema 7. *Si* $a = (a_t a_{t-1} \ldots a_1 a_0)_p$ *es la expansión en base* p *de un número entero positivo* a *entonces el desarrollo de* $-a$ *esta dado por*

$$(\ldots (p-1)\,(p-1)\,[(p-1) - a_t]\,[(p-1) - a_{t-1}] \ldots [(p-1) - a_1]\,(p - a_0))_p$$

Demostración. Basta ver que $a + (-a) = 0$ □

Como consecuencia de este *Lema* se tiene que los números enteros negativos están representados por sucesiones infinitas tales que solo un número finito de cifras es distinta de $p-1$ y estas aparecen al principio de la sucesión. Retomando el hecho de que un

número p-ádico n puede ser representado mediante la serie $n = \sum_{i=0}^{\infty} a_i\, p^i$ donde $0 \leq a_i < p$, y se puede identificar mediante la sucesión $(a_k)_{k\geq 0}$ de sus coeficientes. Si además n es un entero positivo entonces $n = a_{k-1} \ldots a_3 a_2 a_1 a_0$ se tiene que $a_i = 0$ si $i \geq k$.

Considerando ahora el conjunto de todas las sucesiones cuyos coeficientes cumplen que son enteros no negativos menores que p, entonces:

Definición 8. El conjunto

$$\mathbb{Z}_p = \{(\ldots a_3 a_2 a_1 a_0) \mid 0 \leq a_i < p\}$$

a este conjunto se le denomina *el anillo de los enteros $p-$ ádicos.*

El siguiente teorema es una propiedad algebraica de conjunto definido anteriormente.

Teorema 9. *El conjunto $\mathbb{Z}_p$ de los enteros p-ádicos es una anillo conmutativo con las operaciones definidas entre enteros p-ádicos*

Demostración. Esta demostración aunque básica es laboriosa, por lo tanto se omitirá la prueba, esta se puede encontrar en la referencia bibliográfica [1] pag. 37. □

Por construcción se observa que las expansiones en la base p de enteros producen enteros p-ádicos, y se obtiene así la contenencia del conjunto de los enteros $\mathbb{Z}$ en $\mathbb{Z}_p$.

$$\mathbb{Z} \hookrightarrow \mathbb{Z}_p$$

donde los números naturales están representados en $\mathbb{Z}_p$ como las sucesiones que tienen solo finitas cifras no nulas, mas aún la inclusión es propia, ya que una sucesión que no se estabiliza en $(p-1)$ o en 0, no representa un número entero. Dado que las unidades en un anillo son los elementos que tienen inverso multiplicativo, ¿Cuales son las unidades[5] en $\mathbb{Z}_p$? Sea $a = (\ldots a_2 a_1 a_0)_p$ para que a tenga inverso multiplicativo debe existir $b = (\ldots b_2 b_1 b_0)_p$ tal que $a \cdot b = b \cdot a = 1 = (\ldots 0001)$ entonces haciendo el producto $(\ldots a_2 a_1 a_0)_p \times (\ldots b_2 b_1 b_0)_p$ como se indicó anteriormente, donde además, como suele suceder, el resultado no esta escrito en base p pues primero se debe reducir la expresión; por lo tanto, para que se cumpla $a \cdot b = 1$ se debe tener $a_0 b_0 \equiv 1\,(mod\, p)$, de donde a_0 debe ser una unidad en $\mathbb{Z}_p$ y esto se tiene si y solo si a_0 es primo relativo

[5] Sea A un anillo con unidad. Se dice que un elemento $a \in A$ es una unidad si existe otro elemento $b \in A$ tal que $ab = ba = 1$. El conjunto de unidades de A se denota $\mathcal{U}(A)$.

con p, esto es $(a_0,\, p) = 1$. Si a_0 cumple esta condición, entonces b_0 queda completamente determinado por el inverso multiplicativo de a_0. Mas aún si $(a_0,\, p) = 1$ y como $a_0 b_0 \equiv 1\,(mod\, p\,)$, entonces existe existe $q_0 \in \mathbb{Z}$ tal que $b_0 a_0 = q_0 p + 1$, y según la definición dada anteriormente, para realizar la adición en la segunda cifra se debe sumar q_0 a $b_0 a_1 + b_1 a_0$ y luego reducir módulo p. Como se quiere tener que $a \cdot b = (\ldots 0001)$ entonces $b_0 a_1 + b_1 a_0 \equiv 0\,(mod\, p\,)$. De ahí que $b_1 a_0 \equiv -b_0 a_1 - q_0\,(mod\, p\,)$ y como a_0 es invertible en $\mathbb{Z}_p$ con inverso b_0, multiplicando a lo dos miembros por b_0 se tiene que

$$b_1 \equiv -b_0^2 a_1 - q_0 b_0\,(mod\, p\,)$$

ya que $0 \leq b_1 < p$ la ecuación anterior determina a b_1. Para hallar b_2 se procede de la misma forma. Si $b_1 a_0 + b_0 a_1 + q_0 \equiv 0\,(mod\, p\,)$ entonces por el algoritmo de la división existe $q_1 \in \mathbb{Z}$ tal que $b_1 a_0 + b_0 a_1 + q_0 = p.\, q_1$ y de nuevo sumando como el caso anterior q_1 al término siguiente se tiene que

$$b_0 a_2 + b_1 a_1 + b_2 a_0 + q_1 \equiv 0\,(mod\, p\,)$$

de donde $b_2 a_0 \equiv -b_1 a_1 - b_0 a_2 - q_1\,(mod\, p\,)$ y de forma similar al caso anterior se multiplica por b_0 y se tiene que

$$b_2 = -b_0 b_1 a_1 - b_0^2 a_2 - b_0 q_1\,(mod\, p\,)$$

Como $0 \leq b_2 < p$ esta ecuación determina a b_2. Siguiendo de esta forma recursiva se encuentra de manera única el número b que es el inverso multiplicativo de a si y solo si a_0 es primo relativo de p, por lo tanto, se ha demostrado la siguiente proposición.

Proposición 10. $\mathcal{U}\,(\mathbb{Z}_p) = \{(\ldots a_3 a_2 a_1 a_0) \in \mathbb{Z}_p \mid (a_0,\, p) = 1\}$

Este corolario muestra que como p es un número primo los únicos elementos que no son invertibles son aquellos que empiezan con cifra nula, a continuación se mostrará un ejemplo:

Ejemplo 11. Según el algoritmo mostrado anteriormente se puede hallar el inverso de $(\ldots 002)_3$ en $\mathbb{Z}_3$ que existe pues $(2, 3) = 1$, así que $2b_0 \equiv 1\,(mod\, 3)$ y como $2.\,2 = 4 \equiv 1\,(mod\, 3\,)$ se tiene que $b_0 = 2$ y además $4 \equiv 3.\,1 + 1$ lo que implica que $q_0 = 1$ luego

$b_1 \equiv -b_0^2 a_1 - q_0 b_0\,(mod\, 3\,)$

$b_1 = -2^2.\,0 - 2.\,1\,(mod\, 3\,)$

$b_1 = -2\,(mod\,3\,)$
$b_1 = 1\,(mod\,3\,)$ luego $b_1 = 1$.

Además $b_0a_1 + b_1a_0 + q_0 = 2.0 + 1.2 + 1 = 3 = 3.1$ por tanto $q_1 = 1$ así mismo
$b_2 = -b_0b_1a_1 - b_0^2a_2 - b_0q_1\,(mod\,3\,)$
$b_2 = -2^2.0 - 2.1.0 - 2.1\,(mod\,3)$
$b_2 = -2\,(mod\,3) \Rightarrow b_1 = 1\,(mod\,3\,)$ luego $b_2 = 1$
y $b_0a_2 + b_1a_1 + b_2a_0 + q_1 = 2.0 + 1.0 + 1.2 + 1 = 3 = 3.1$ de donde $q_2 = 1$.

Entonces $b_3 = -b_0^2a_3 - b_0b_1a_2 - b_0b_2a_1 - b_0q_2\,(mod\,3\,)$
$b_3 = -2^2.0 - 2.1.0 - 2.1.0 - 2.1\,(mod\,3\,)$
$b_3 = -2\,(mod\,3\,) \Rightarrow b_1 = 1\,(mod\,3\,)$ de ahí que $b_3 = 1$

Siguiendo de este modo se tiene que para $n \geq 2$, $b_n = 1$ y $q_n = 1$, ya que los términos de la expansión a partir del segundo se anulan. Y así se obtiene que
$(\ldots 0002)_3^{-1} = (\ldots 1112)_3$.

El siguiente resultado muestra otra propiedad que cumple $\mathbb{Z}_p$ como estructura algebraica.

Teorema 12. *El anillo $\mathbb{Z}_p$ de enteros p-ádicos es un dominio entero*[6]

Demostración. Se demostrará que $\mathbb{Z}_p$ carece de elementos no nulos que al multiplicarse den como resultado 0, es decir, no tiene divisores de 0. Por tanto, sea $a = \sum_{i=0}^{\infty} a_i\,p^i$ y $b = \sum_{i=0}^{\infty} b_i\,p^i$ con $a, b \neq 0$. Entonces sea a_k el primer coeficiente distinto de cero de a, como $0 < a_k < p$ y del mismo modo b_t es el primer coeficiente distinto de cero de b. En particular, p no divide a_k ni a b_t y en consecuencia no divide tampoco a su producto a_kb_t. Por definición de la multiplicación, el primer coeficiente distinto de 0 del producto ab es el coeficiente c_{k+t} de p^{k+t} donde $0 < c_{k+t} < p$ y este coeficiente se define por

$$c_{k+t} \equiv a_kb_t\,(mod\,p)$$

Luego

$$c_{k+t} \not\equiv 0\,(mod\,p)$$

Lo que se deseaba. □

[6]Un anillo conmutativo I que satisface para cualesquiera $a \in I$ y $b \in I$ no nulos entonces $a.b \neq 0$ es llamado un dominio entero.

1.4. Cuerpo de los números p-ádicos

Puesto que no todo elemento de $\mathbb{Z}_p$ tienen inverso, para construir un cuerpo que contenga a $\mathbb{Z}_p$ se debe adicionar los inversos de los elementos no nulos. La extensión de los números enteros a los números racionales en el desarrollo decimal se obtiene al hallar el inverso de todos los enteros no nulos.

$$\frac{1}{2} = 0,5 \qquad \frac{1}{9} = 0.\overline{1}$$

Así como el inverso de $p \in \mathbb{Q}$ es $\frac{1}{p} = p^{-1}$ entonces se deben introducir los inversos de las potencias de p, para ello se usará la misma notación dada en el desarrollo decimal; pero solo admitiendo finitas cifras después de la coma, así:

$(0,1)_p = 1.\, p^{-1}$

$(0,01)_p = 1.\, p^{-2}$

De la misma manera como se hace en el desarrollo decimal se puede expresar una expansión p-ádica, así por ejemplo, el número $(14,1256)_7$ se puede escribir como $(14,1253)_7 = 1.\, 7^1 + 4.\, 7^0 + 1.\, 7^{-1} + 2.\, 7^{-2} + 5.\, 7^{-3} + 3.\, 7^{-4}$.

En $\mathbb{Q}$, la escritura en base 10 admite infinitas cifras a la derecha, luego de la coma. Aquí se toma la convención opuesta, se admiten infinitas cifras a la izquierda y solo finitas a la derecha, después de la coma, esto se mostrará en el siguiente teorema.

Teorema 13. *Una expansión p-ádica representa un número racional si y solo si es finalmente periódica a la izquierda.*

Demostración. $\Leftarrow$ Multiplicando, si es necesario, el número p-ádico x por una potencia de p y restando un número racional, se puede considerar el caso en el que $x \in \mathbb{Z}_p$ tiene una expansión periódica de la forma

$$x = x_0 + x_1 p + x_2 p^2 + \ldots + x_{k-1} p^{k-1} + x_0 p^k + x_1 p^{k+1} \ldots$$

El número $a = x_0 + x_1 p + x_2 p^2 + \ldots + x_{k-1} p^{k-1}$ es un racional entero y x puede ser expresado como sigue

$$a\left(1 + p^k + p^{2k} + \ldots\right) = a.\, \frac{1}{1 - p^k}$$

Por lo tanto x es un número racional.

$\Rightarrow$Supóngase que

$$\frac{a}{b} = \sum_{i \geq 0} x_i p^i \in \mathbb{Z}_p$$

Se puede suponer que a y b son enteros que son primos relativos y b es primo relativo con p. La expansión p-ádica de $\frac{a}{b}$

$$\frac{a}{b} = x_0 + x_1 p + x_2 p^2 + \ldots \; x_{n-1} p^{n-1} + \ldots$$

y sea $A_n = x_0 + x_1 p + x_2 p^2 + \ldots + x_{n-1} p^{n-1}$ $0 \leq A_n \leq p^n - 1$. Ya que A_n es un número racional entero, se tiene

$$\frac{a}{b} = A_n + p^n \frac{r_n}{b}$$

donde r_n es un entero. De ahí que $r_n = \frac{(a - A_n b)}{p^n}$ y por lo tanto

$$\frac{a - (p^n - 1)\, b}{p^n} \leq r_n \leq \frac{a}{p^n}$$

para n suficientemente grande, de donde se tiene que $-b \leq r_n \leq 0$, lo que significa que r_n toma solo un número finito de valores. Ahora se puede escribir

$$x = A_n + p^n \frac{r_n}{b} = A_{n+1} + p^{n+1} \frac{r_{n+1}}{b} = A_n + x_n p^n + p^{n+1} \frac{r_{n+1}}{b}$$

y por lo tanto $r_n = x_n b + p r_{n+1}$ para todo n. Ya que r_n toma solo un número finito de valores, existe un índice m y un entero positivo P tal que $r_m = r_{m+P}$, por lo tanto

$$x_m b + p\, r_{m+1} = x_{m+P} b + p\, r_{m+P+1} \qquad (1)$$

de modo que

$$(x_m - x_{m+P})\, b = p\, (r_{m+P+1} - r_{m+1})$$

ya que $(b,\, p) = 1$, se sigue que p divide a $x_m - x_{m+P}$. Pero tanto x_m y x_{m+P} son dígitos entre $\{0,\, 1,\, 2,\, \ldots\, p-1\}$ por lo que $x_m = x_{m+P}$. Sustituyendo esto en (1) también se puede ver que $r_{m+1} = r_{m+P+1}$. Repitiendo este argumento se obtiene

$$r_n = r_{n+P} \quad \text{y} \quad x_n = x_{n+P} \;\; (n \geq m)$$

que demuestra que no solo la sucesión de dígitos x_n, sino también la sucesión de los numeradores r_n, tienen un periodo de longitud P para $n \geq m$ $\square$

Teniendo en cuenta que $\mathbb{Z}_p$ resulta ser un anillo (e incluso un dominio entero), se puede construir un cuerpo que lo contenga, así:

Definición 14. El conjunto

$$\mathbb{Q}_p = \{(\dots a_2 a_1 a_0 a_{-1} a_{-2} \dots a_{-t}) \mid 0 \leq a_i < p\,,\, a_{-t} \neq 0\}$$

se denomina el *anillo de los números $p-$adicos*.

Es claro que para obtener $\mathbb{Q}_p$ basta agregarle a $\mathbb{Z}_p$ sucesiones con finitos decimales.

$$\mathbb{Z} \subset \mathbb{Z}_p \subset \mathbb{Q}_p$$

Igual que en el caso anterior, este conjunto resulta ser un *anillo conmutativo* con las operaciones definidas anteriormente y además cumple otra propiedad que se muestra en el siguiente lema.

Lema 15. *$\mathbb{Q}_p$ es un cuerpo con las operaciones definidas anteriormente.*

Demostración. Se sabe que $\mathbb{Q}_p$ es un anillo conmutativo con identidad. Además como p es primo entonces todo número a_i tal que $0 < a_i < p$ es primo relativo con p. Luego si $a \in \mathbb{Q}_p$ no nulo tiene inverso multiplicativo, este hecho se dedujo anteriormente en la Proposición 10 . Por lo tanto $\mathbb{Q}_p$ es un cuerpo. □

Observación 16. $\mathbb{Q}_p$ se conoce como el *cuerpo de los números $p-$ ádicos*. Por construcción se tiene que $\mathbb{Z} \subset \mathbb{Q}_p$. Como $\mathbb{Q}_p$ es un cuerpo se sigue que $\mathbb{Q} \subseteq \mathbb{Q}_p$ para todo p. Ya que $\mathbb{Q}_p$ contiene a $\mathbb{Z}$ y por tanto contiene a $\mathbb{Q}$; puesto que todo cuerpo que contiene a $\mathbb{Z}$ contiene una copia de $\mathbb{Q}$ (Propiedades de cuerpos).

Como en los Ejemplos 3 , 4 y 5 se mostró como se suma, resta y multiplica con los números en base p. Ahora se presenta el caso de la división, este proceso es basado en el algoritmo de la división de polinomios, esto da lugar a la escritura de los números racionales en $\mathbb{Q}_p$.

Se puede notar que hay varios números que ya se pueden escribir en base p, usando el hecho que se muestra al iniciar Subsección 1.4 donde se definen los inverso de las potencias de p en $\mathbb{Q}_p$.

Ejemplo 17. Escribir el número $\frac{25}{49}$ en base 7 Se puede escribir

$$\frac{25}{49} = \frac{3.7+4}{7^2} = 3.7^{-1} + 4.7^{-2} = 3.(0,1)_7 + 4.(0,01)_7 = (0,3)_7 + (0,04)_7 = (0,34)_7$$

Pero hay otros números racionales en $\mathbb{Q}_p$ cuyo desarrollo no es tan evidente ese proceso se muestra a continuación:

Dado que se admite infinitas cifras a la izquierda, para realizar la división, se pondrá el divisor a la izquierda y al dividendo a la derecha, con el orden inverso. Así dados $a = (\ldots a_2a_1a_0)_p$ y $b = (\ldots b_2b_1b_0)$, se desea hacer el cociente $\frac{a}{b}$, se expresa:

$$\underline{\ldots a_2a_1a_0} \,\big|\, b_2b_1b_0 \ldots$$

Ahora bien, para escribir $\frac{a}{b}$ en base p, se procederá a dividir a por b de acuerdo al algoritmo que se mostrará en el siguiente ejemplo para una mayor simplicidad.

Ejemplo 18. Escribir $\frac{7}{11}$ en base 3

Como $7 = (\ldots 0021)_3$ y $11 = (\ldots 00102)_3$ y luego

$$\underline{\ldots 00102} \,\big|\, 1200 \ldots$$

Se debe hallar el número a tal que $2a \equiv 1\,(mod\,3)$ este número es $a = 2$, como $2\,(\ldots 00102)_3 = (\ldots 00211)_3$ y se realiza la resta $(\ldots 00102) - (\ldots 00211)_3$ como se mostró anteriormente en este caso se deben «prestar unidades» así:

$$\begin{array}{rccccccccccc}
\underline{\ldots 00102}\rfloor & \underbrace{1} & 2 & 0^{+3} & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\
110022 & 1 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 & 0 & \underbrace{1} & 1 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2
\end{array}$$

Repitiendo este proceso será ahora $2b \equiv 1\,(mod\,3)$ donde $b = 2$, se realiza la resta y siguiendo de esta manera se tiene:

$$\begin{array}{rccccccc}
\underline{\ldots 0000102}\rfloor & \underbrace{1} & 2 & 0^{+3} & 2 & 2 & 2 \\
1002110022 & -1 & 1 & 2 & 0 & 0 & 0 \\
 & 0 & \underbrace{1} & 1 & 2 & 2 & 2 \\
 & & 1 & 1 & 2 & 0 & 0 \\
 & & 0 & \underbrace{0} & \underbrace{0} & \underbrace{2} & 2 \\
 & & & & & 2 & 0
\end{array}$$

Por lo tanto $\frac{7}{11} = (\ldots 00211002110022)_3$, donde a partir de la cuarta cifra se repite el periodo 00211

Observación 19. Note que el algoritmo del Ejemplo 18 sirve para hallar los desarrollos de un número racional en cualquier base n sin importar si n es primo o no; siempre y cuando la cifra del denominador sea primo relativo con n.

2. Métricas sobre $\mathbb{Q}$

El objetivo de esta sección es comenzar a sentar una base sólida para la teoría que se ha descrito en la sección anterior. La idea principal será la de introducir una norma diferente en el campo de los números racionales. Esto dará una forma distinta de hallar distancias, y por lo tanto, un cálculo diferente. Una vez se tenga dicha distancia, se procederá a la construcción de los números p-ádicos.

2.1. Norma p-ádica

El sistema de números p-ádicos para cualquier número primo p extiende la aritmética ordinaria de los números racionales de una manera un tanto diferente a la extensión del sistema de los números racionales a los sistemas de números reales y complejos. Como ya se dijo al introducir esta sección, la extensión se logra mediante una interpretación alternativa del concepto de "proximidad". Para ello se empezará con la definición de valuación p-ádica.

Definición 20. Se define la *valuación $p-$ádica* de un número racional no nulo por:

1. $\nu_p(x) = max\{\, n \in \mathbb{Z} :\ p^n \mid x \,\}$,si $x \in \mathbb{Z}$- $\{0\}$
2. $\nu_p(q) = \nu_p(a) - \nu_p(b)$, si $q = \frac{a}{b} \in \mathbb{Q}$

Esta función $\nu_p : \mathbb{Q} \to \mathbb{Z}$ no es inyectiva. Además por convención se toma que $\nu_p(x) = \infty$ si y solo si $x = 0$

Proposición 21. *Sean $x, y \in \mathbb{Q} - \{0\}$ entonces se cumple que:*

1. $\nu_p(xy) = \nu_p(x) + \nu_p(y)$
2. $\nu_p(x+y) \geq min\ \{\nu_p(x), \nu_p(y)\}$ y si $\nu_p(x) \neq \nu_p(y)$ se obtiene la igualdad de esta expresión.

Demostración. 1. Si $x = p^n \frac{a}{b}$ y $y = p^m \frac{c}{d}$ con $n, m, a, b, c, d \in \mathbb{Z}$ y $b, d \neq 0$ donde a, b, c, d no son divisibles por p. Es claro que $\nu_p(x) = n$ y $\nu_p(y) = m$ y además como $xy = p^{m+n} \frac{ac}{bd}$ es evidente que $\nu_p(xy) = m + n$ de donde se tiene el resultado.

2. Supóngase que x, y son no nulos (si alguno de ellos lo fuera la proposición se cumple trivialmente). Entonces se puede escribir:

$x = p^r \frac{a}{b}$ y $y = p^s \frac{c}{d}$ con $r, s, a, b, c, d \in \mathbb{Z}$ y $b, d \neq 0$ donde a, b, c, d no son divisibles por p. Es claro que $\nu_p(x) = r$ y $\nu_p(y) = s$. Supóngase sin perdida de generalidad que $s \geq r$ y sea $t = s - r \geq 0$.

Por lo tanto

$$x + y = p^r \frac{a}{b} + p^s \frac{c}{d} = p^r \left(\frac{a}{b} + p^t \frac{c}{d} \right) = p^r \left(\frac{ad + p^t bc}{bd} \right)$$

por lo tanto $\nu_p(x+y) \geq r$ donde $r = min \{\nu_p(x) = r \, , \, \nu_p(y) = s\}$ de ahí que $\nu_p(x+y) \geq min \{\nu_p(x) = r \, , \, \nu_p(y) = s\}$. Supóngase que ahora $\nu_p(x) \neq \nu_p(y)$ en este caso se puede suponer $s > r$, esto es equivalente a tomar $t = s - r \geq 1$ ya que $s, r \in \mathbb{Z}$. Además p no divide ni al numerador ni al denominador de la fracción que acompaña a p^r pues por hipótesis p no divide a ninguno de los enteros a, b, c, d por lo tanto $\nu_p(x + y) = r$ donde $r = min \{\nu_p(x) = r \, : \, \nu_p(y) = s\}$ de ahí que $\nu_p(x+y) = min \{\nu_p(x) = r \, , \, \nu_p(y) = s\}$. $\square$

Como $v_p(xy) = v_p(x) + v_p(y)$ usando el Teorema Fundamental de la Aritmética, si se considera $n \in \mathbb{Z}$ y sea $n = p^\alpha p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \ldots p_{n-1}^{\alpha_{n-1}} p_n^{\alpha_n}$ la descomposición en factores primos de n , entonces $n = p^\alpha m$ donde $(p, m) = 1$ de donde p no divide a m y por lo tanto

$$v_p(n) = \alpha$$

donde α es la mayor potencia de p que aparece en la descomposición prima de n.

Esta valuación p-ádica permite definir la norma p-ádica de la siguiente manera:

Definición 22. Si p es un número primo fijo, se define en $\mathbb{Q}$ la norma $p - \acute{a}dica$ por:

$$\|x\|_p = p^{-v_p(x)} = \frac{1}{p^{v_p(x)}} \quad si \;\; x \neq 0$$

y si $x = 0$ se toma $\|0\|_p = 0$. La siguiente proposición muestra que en efecto $\| \; \|_p$ es una norma en $\mathbb{Q}$.

Proposición 23. $\|x\|_p = p^{-v_p(x)} = \frac{1}{p^{v_p(x)}}$ *define una norma en* $\mathbb{Q}$.

Demostración. 1. Sea $x \in \mathbb{Q}$ por definición se tiene que $\|x\|_p = 0$ si y solo si $x = 0$

2. Sean $x, y \in \mathbb{Q}$ y p un número primo fijo, además supóngase que $x = \frac{a}{b}$ e $y = \frac{c}{d}$ con $b, d \neq 0$ entonces $\|xy\|_p = \left\| \frac{a}{b} \frac{c}{d} \right\|_p = \left\| \frac{ac}{bd} \right\|_p$ por definición de norma p-ádica se tiene

que

$$\|xy\|_p = \frac{1}{p^{v_p(\frac{ac}{bd})}} = \frac{1}{p^{(v_p(ac)-v_p(bd))}} = \frac{p^{v_p(bd)}}{p^{v_p(ac)}} = \frac{p^{(v_p(b)+v_p(d))}}{p^{(v_p(a)+v_p(c))}} = \frac{p^{v_p(b)}p^{v_p(d)}}{p^{v_p(a)}p^{v_p(c)}}$$

$$= \frac{1}{p^{(v_p(a)-v_p(b))}}\frac{1}{p^{(v_p(c)-v_p(d))}} = \frac{1}{p^{(v_p(\frac{a}{b})}}\frac{1}{p^{(v_p(\frac{c}{d})}} = \left\|\frac{a}{b}\right\|_p \left\|\frac{c}{d}\right\|_p = \|x\|_p \|y\|_p$$

3. Se probará la desigualdad triangular. Si se tienen al menos uno de estos casos, $x = 0$, $y = 0$, $x + y = 0$ la desigualdad triangular se cumple trivialmente. Supóngase que $x \neq 0\,;\, y \neq 0\,;\, x + y \neq 0$. Entonces de lo enunciado en la *Proposición* 21 se tienen que $\nu_p(x + y) \geq min\ \{\nu_p(x), \nu_p(y)\}$ así $p^{\nu_p(x+y)} \geq p^{min\,\{\nu_p(x),\nu_p(y)\}}$ por lo tanto

$$\|x + y\|_p = \frac{1}{p^{(v_p(x+y))}} \leq \frac{1}{p^{min\,\{v_p(x);v_p(y)\}}} = max\left\{\frac{1}{p^{\nu_p(x)}}, \frac{1}{p^{\nu_p(y)}}\right\}$$

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

□

Realmente se ha probado una desigualdad más fuerte, que se enuncia en el ítem 3 de la *Proposición* 24. En particular se tiene que $\|\cdot\|_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ satisface las propiedades siguientes, análogas a la que se cumplen para la valuación p-ádica.

Proposición 24. *Si $x \in \mathbb{Q}$ entonces se verifican:*

1. $\|x\|_p = 0$ si y solo si $x = 0$
2. $\|xy\|_p = \|x\|_p \|y\|_p$
3. $\|x + y\|_p \leq máx\left\{\|x\|_p\ ,\ \|y\|_p\right\}$; y si $\|x\|_p \neq \|y\|_p$ se da la igualdad.

Una norma que satisface la propiedad 3 de esta proposición se llama $no-arquimediana$.

Observación 25. Note que $\|\ \|_p$ puede tomar solo un conjunto de valores, a saber, $\{p^n \mid n \in \mathbb{Z}\} \cup \{0\}$.

Dos números x e y están mas «cercanos» respecto a la norma p-ádica mientras mayor sea el valor de n tal que p^n divide a $(x - y)$. Esto es, un número es considerado

más pequeño cuanto mas divisible por p sea. Para $p = 5$ el resultado es que 135 esta mas cerca de 10 que de 35, así:

$\|135 - 10\|_5 = \|125\|_5 = \frac{1}{5^{\mathcal{V}_5(5^3)}} = \frac{1}{5^3} = \frac{1}{125}$
$\|135 - 35\|_5 = \|100\|_5 = \frac{1}{5^{\mathcal{V}_5(5^2.4)}} = \frac{1}{5^{2+0}} = \frac{1}{5^2} = \frac{1}{25}$

Como se mostró en la *Proposición* 24, la norma p-ádica, $\|x\|_p = p^{-v_p(x)} = \frac{1}{p^{v_p(x)}}$ es una norma $no - arquimediana$ o ultra-métrica y es esta propiedad la que conduce a la definición básica del análisis p-ádico.

Observación 26. La idea sobre distancia esta basada en la métrica inducida por el valor absoluto. Por tal motivo algunas propiedades de las normas no-arquimediana pueden parecer extrañas. Por ejemplo la propiedad que se conoce como desigualdad triangular, en el caso del cuerpo de los Números Complejos con la distancia usual dice que la suma entre los dos lados de un triángulo es mayor que el tercer lado esto es $d(x, y) = d(x, z) + d(z, y)$. (Propiedad es equivalente si se toma a $\mathbb{R}^2$ con la métrica usual).

Analizando ahora lo que sucede con una norma no-arquimediana sobre un cuerpo. Para simplificar, supóngase que $z = 0$, entonces la desigualdad triangular para una norma no-arquimediana se tiene así $\|x + y\| \leq máx\{\|x\|, \|y\|\}$. Supóngase primero que los dos lados x e y tienen distinta longitud , es decir, $\|x\| < \|y\|$ luego el tercer lado $x - y$ tiene longitud

$$\|x - y\| \leq \|y\| \qquad (1)$$

pero $\|y\| = \|x - (x - y)\| \leq máx\{\|x\|, \|x - y\|\}$ y como $\|x\| < \|y\|$ la única opción es que $\|y\| \leq \|x - y\|$ (2).

De (1) y (2) se tiene que $\|y\| = \|x - y\|$. En conclusión, si se tienen dos lados de un triángulo con diferente longitud; el lado de mayor longitud de estos debe tener la misma longitud del tercer lado. Por lo tanto se tiene la siguiente proposición.

Proposición 27. *Todo triángulo en un espacio métrico con una norma no-arquimediana es isósceles.*

El siguiente teorema es una condición necesaria y suficiente para que una norma sea no-arquimediana sobre un campo que contiene a $\mathbb{Z}$.

Teorema 28. *Las siguientes proposiciones son equivalentes*

1. $\|\cdot\|$ *es no-arquimediana*

2. $\|x\| \leq 1$ *para todo* $x \in \mathbb{Z}$

Demostración. (1) $\Rightarrow$ (2)

Se puede probar esta implicación por inducción.

Para $n = 1$, $\|1\| = 1 \leq 1$. Supóngase que $\| n-1 \| \leq 1$ para $n \in \mathbb{N}$, se probará que $\|n\| \leq 1$. Observese que $\| n \| = \|(n-1)+1\| \leq max\{\|n-1\|, 1\} = 1$ esto se tiene por hipótesis de inducción. Además como $\|-1\| = 1 \leq 1$ y como $\| n \| \leq 1$ para todo $n \in \mathbb{N}$.

Por lo tanto $\|-n\| = \|-1\| \| n \| = \|n\| \leq 1$. Luego se concluye que $\|n\| \leq 1$ para todo $n \in \mathbb{Z}$.

(2) $\Rightarrow$ (1)

$$\|x+y\|^n = \|(x+y)^n\| = \left\|\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}\right\|$$

$$\leq \sum_{k=0}^{n} \left\|\binom{n}{k}\right\| \|x\|^k \|y\|^{n-k}$$

como $\binom{n}{k}$ es un entero entonces por hipótesis de $\left\|\binom{n}{k}\right\| \leq 1$ y por lo tanto

$$\sum_{k=0}^{n} \left\|\binom{n}{k}\right\| \|x\|^k \|y\|^{n-k} \leq \sum_{k=0}^{n} \|x\|^k \|y\|^{n-k}$$

pero además $\|x\|^k \|y\|^{n-k} \leq max(\|x\|, \|y\|)^{k+n-k}$ como se tienen $n+1$ sumandos entonces

$$\sum_{k=0}^{n} \|x\|^k \|y\|^{n-k} \leq (n+1)(max(\|x\|, \|y\|))^n$$

Así que, para cada entero n se tiene

$$\|x+y\| \leq \sqrt[n]{n+1}\, max(\|x\|, \|y\|)$$

Haciendo $n \to \infty$, como $\lim_{n\to\infty} \sqrt[n]{n+1} = 1$ entonces se tiene que

$$\|x+y\| \leq max(\|x\|, \|y\|)$$

□

El siguiente teorema es muy importante e interesante por que dice que en esencia solo hay dos tipos de valores absolutos en los racionales, el usual y el p-ádico.

Teorema 29. *(**Teorema de Ostrowski**). Toda norma no trivial $|\ |$ sobre $\mathbb{Q}$ es equivalente a $\|\ \ \|_p$ para algún primo p o a la norma usual.*

Demostración. Sea $|\ |$ una norma sobre $\mathbb{Q}$ y $A = \{\, n \in \mathbb{N} / \,|\, n \,|\, > 1 \,\}$ se tienen dos posibilidades mutuamente excluyentes $A \neq \emptyset$ o $A = \emptyset$ CASO 1: Para $A \neq \emptyset$

Por el el principio del buen orden, existe $n_0 \in A$ tal que $n_0 \leq n$ para todo $n \in A$. Como $|\, n_0 \,| > 1$ existe un número real positivo α tal que $|\, n_0| = n_0^{\alpha}$. Dado $n \in \mathbb{N}$, su desarrollo en la base n_0 es de la forma

$$n = a_0 + a_1 n_0 + a_2 n_0^2 + \ldots + a_s n_0^s$$

donde $0 \leq a_i < n_0$ y $a_s \neq 0$. Entonce

$$|\, n \,| \leq |\, a_0| + |\, a_1 n_0| + \left|\, a_2 n_0^2 \right| + \ldots + |\, a_s n_0^s| = |\, a_0| + |\, a_1|\, n_0^{\alpha} + |\, a_2|\, n_0^{2\alpha} + \ldots + |\, a_s|\, n_0^{s\alpha}$$

Ya que todo $a_i < n_0$ para $0 \leq i \leq s$, por la elección de n_0 se tiene que $|\, a_i| \leq 1$ y como $n \geq n_0^s$ entonces

$$|\, n \,| \leq 1 + n_0^{\alpha} + n_0^{2\alpha} + \ldots + n_0^{s\alpha} = n_0^{s\alpha} \left(1 + n_0^{-1} + n_0^{-2\alpha} + \ldots + n_0^{-s\alpha}\right)$$

$$\leq n^{\alpha} \left(\sum_{i=0}^{\infty} \left(\frac{1}{n_0^{\alpha}} \right)^i \right)$$

Es claro que esta serie es una constante finita, nótese esta constante por C. Entonces $|\, n \,| \leq C n^{\alpha}$ para todo $n \in \mathbb{N}$. Tomando un n arbitrario y N suficientemente grande, reemplazando n por n^N en la desigualdad anterior y tomando raíz $N - \acute{e}sima$ resulta $|\, n \,| \leq \sqrt[N]{C\, n^{\alpha}}$ y como $lim_{N \to \infty} \sqrt[N]{C} = 1$ de ahí que $|\, n \,| \leq n^{\alpha}$ para todo $n \in \mathbb{N}$ (1). Por otro lado, tomando el desarrollo de $n \in \mathbb{N}$ en base n_0 se tiene que $n_0^{s+1} > n \geq n_0^s$ entonces

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

por lo tanto

$|\, n \,| \geq \left|\, n_0^{s+1} \right| - \left|\, n_0^{s+1} - n \right|$ pero como $|\, n \,| \leq n^{\alpha}$ entonces $|\, n \,| \geq n_0^{(s+1)\alpha} - \left(n_0^{s+1} - n\right)^{\alpha}$ ya que $\left|\, n_0^{s+1} \right| = |\, n_0|^{s+1}$, usando la desigualdad $|\, n \,| \leq n^{\alpha}$ y el hecho de que $n \geq n_0^s$ se

obtiene que

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

para alguna constante C' que depende de n_0 y de α pero no depende de n de manera análoga a lo hecho anteriormente tomando raíces $N - ésimas$ y haciendo $N \to \infty$ se obtiene $|\,n\,| \geq n^{\alpha}$ para todo $n \in \mathbb{N}$ (2).

Luego de (1) y (2) se tiene que $|\,n\,| = n^{\alpha}$ para todo $n \in \mathbb{N}$ y en consecuencia de la *Propiedad* 2 de normas se concluye que $|\,x\,| = \|\,x\|^{\alpha}$ para todo $x \in \mathbb{Q}$ donde $\|\ \|$ es la norma usual en $\mathbb{Q}$. CASO 2: Para $A = \emptyset$

Supongamos en efecto $|\,n\,| \leq 1$ para todo $n \in \mathbb{N}$ y sea n_0 el menor entero positivo tal que $n_0 < n$ y $|n_0| < 1$; n_0 existe porque se asumió que $|\ |$ es no trivial. Se debe tener que n_0 es primo, en caso contrario si $n_0 = n_1 n_2$ con $n_1, n_2 < n_0$ entonces $|\,n_1| = |\,n_2| = 1$ y $|\,n_0| = |\,n_1|\,|\,n_2| = 1$ lo que es contradictorio. Nótese ahora a p como el primo n_0 , sea q un primo distinto de p, y se probará que $|\,q| = 1$. Por contradicción supóngase que $|q| < 1$, y para algún N grande tal que $\left|q^N\right| = |q|^N < \frac{1}{2}$. También, para algún M grande de modo que $\left|p^M\right| < \frac{1}{2}$. Dado que p^M y q^N son primos relativos por el *Lema de Bezout* se puede encontrar enteros m y n tales que $mp^M + nq^N = 1$ entonces

$$1 = |1| = \left|mp^M + nq^N\right| \leq \left|mp^M\right| + \left|nq^N\right| = |\,m|\,\left|\,p^M\right| + |\,n|\,\left|\,q^N\right|$$

por la *Propiedad* 2 y 3 de la definición de norma. Pero $|\,m| \leq 1$ y $|\,n| \leq 1$ se obtiene

$$1 \leq \left|\,p^M\right| + \left|\,q^N\right| < \frac{1}{2} + \frac{1}{2} = 1$$

Lo que es contradictorio por lo tanto $|\,q| = 1$.

Sea ahora $a \in \mathbb{N}$, su descomposición es factores primos esta dada por $a = p_1^{b_1} p_2^{b_2} \ldots p_r^{b_r}$ entonces $|a| = |p_1|^{b_1}\,|p_2|^{b_2} \ldots |p_r|^{b_r}$ pero el único $|p_i|$ que no es igual a 1 podría ser $|p|$, si alguno de los p_i es p entonces su correspondiente b_i ser $\nu_p(a) = b_i$ y

$$|a| = |p_1|^{b_1}\,|p_2|^{b_2} \ldots |p|^{b_i} \ldots |p_r|^{b_r} = |p|^{b_i} = |p|^{\nu_p(a)}$$

Sea $r = |p| < 1$, luego $|a| = r^{\nu_p(a)}$ para todo $n \in \mathbb{N}$, por la *Propiedad Multiplicativa* de normas, la igualdad anterior se extiende a cualquier racional no nulo x de donde

$|x| = r^{\nu_p(x)} = \|x\|_p$ para todo $x \in \mathbb{Q} - \{0\}$. Se obtiene así que $|\ |$ es equivalente a $\|\ \|_p$ esto concluye la prueba. □

Observación 30. Como se conoce del análisis clásico, es posible construir un cuerpo $\mathbb{R}$, los números reales, que complete al cuerpo $\mathbb{Q}$ de los números racionales, esto es, que incluya también los números llamados "irracionales", con la distancia usual o norma euclidiana, usando sucesiones de Cauchy de números racionales. Sin embargo, la definición de una sucesión de Cauchy depende de la métrica elegida, y entonces, escogiendo una diferente, se podrá construir otros números distintos a los reales. Usando el mismo método se desea completar el cuerpo $\mathbb{Q}$ pero en este caso respecto a la norma definida anteriormente, esta completación dará como resultado en cuerpo $\mathbb{Q}_p$, el *cuerpo de los números* $p-$*ádicos*, esta construcción se mostrará en la Sección 2.2.

2.2. Completación de $\mathbb{Q}$

Como se dijo anteriormente es posible construir un cuerpo $\mathbb{R}$, los reales, que complete al cuerpo $\mathbb{Q}$ de los números racionales. Para ello se ha tenido que construir las sucesiones de Cauchy, usando el concepto de valor absoluto o de distancia euclidiana. El conjunto infinito de los números reales puede definirse como un cuerpo conmutativo, ordenado y completo. A continuación se mostrará brevemente el proceso para la construcción de $\mathbb{R}$ desde el cuerpo $\mathbb{Q}$ de los números racionales mediante sucesiones, así:

1. Definir el conjunto de las sucesiones de números racionales.
2. Considerar el conjunto de las sucesiones de números racionales con límite.
3. Definir el concepto de sucesión de Cauchy.[7] Note que el conjunto de las sucesiones de Cauchy está contenido en el conjunto de las sucesiones acotadas, y también, contiene al conjunto de las sucesiones con límite.
4. Determinar una relación de equivalencia. Esto posibilita la construcción de $\mathbb{R}$ «añadiendo» todos los elementos de una misma clase como un solo elemento que los representará y que define la noción de conjunto cociente.
5. Se define $\mathbb{R}$ como la completación de $\mathbb{Q}$, esto se da si toda sucesión de Cauchy tiene límite dentro del espacio $\mathbb{R}$.

[7] Una sucesión (a_n) es de Cauchy en conjunto con norma $|\ |$, si y solo si $\forall\, \epsilon > 0$, existe $n_0 \in \mathbb{N}$ tal que si $n, m \geq n_0$ entonces $|a_n - a_m| < \epsilon$

Una de las propiedades importantes sobre el campo $\mathbb{R}$ de los números reales es que es un campo completo, es decir, que toda sucesión de Cauchy converge. En términos intuitivos, $\mathbb{R}$ es el campo más pequeño que contiene a $\mathbb{Q}$ y que se completa con respecto a este valor absoluto. Se puede ver esto porque cualquier campo tendría que incluir el límite de cualquier sucesión de Cauchy de elementos de $\mathbb{Q}$, y puesto que $\mathbb{Q}$ es denso en $\mathbb{R}$, cualquier elemento de $\mathbb{R}$ es un límite de dicha sucesión. Se usará un proceso análogo para establecer otra completación de conjunto $\mathbb{Q}$ pero en este caso respecto a la norma p-ádica para ello se requiere dar una caracterización de las sucesiones de Cauchy respecto a una norma no-arquimediana.

Teorema 31. *Una sucesión (x_n) de números racionales es una sucesión de Cauchy con respecto a un norma no-arquimediana $\| \|_p$ si y solo si se cumple que*

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

Demostración. $\Rightarrow$Sea $m = n + r > n$ se obtiene

$$\|x_m - x_n\|_p = \|x_{n+r} - x_{n+r-1} + x_{n+r-1} - x_{n+r-2} + \ \ldots \ + x_{n+1} - x_n\|_p$$

como $\| \|_p$ es una norma no-arquimediana se tiene que

$$\|x_m - x_n\|_p \leq máx \left\{ \|x_{n+r} - x_{n+r-1}\|_p , \|x_{n+r-1} - x_{n+r-2}\|_p , \ \ldots \ \|x_{n+1} - x_n\|_p \right\}$$

pero como (x_n) es una sucesión de Cauchy con respecto a un norma no-arquimediana $\| \|_p$, entonces dado $\epsilon > 0$ se tiene que $\|x_m - x_n\|_p < \epsilon$, y por lo tanto

$$\leq máx \left\{ \|x_{n+r} - x_{n+r-1}\|_p , \|x_{n+r-1} - x_{n+r-2}\|_p , \ \ldots \ \|x_{n+1} - x_n\|_p \right\} < \epsilon$$

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

$\Leftarrow$ En particular tomando el caso $m = n + 1$ y como $\lim_{n\to\infty} \|x_{n+1} - x_n\|_p = 0$ por lo tanto $\|x_m - x_n\|_p < \epsilon$ para $\epsilon > 0$ luego la sucesión es de Cauchy. (Note que este caso no se cumple en $\mathbb{R}$, por ejemplo la sucesión $(-1)^n$ satisface esta condición pero no es de Cauchy). $\square$

Esta caracterización de sucesiones de Cauchy hace el análisis mucho más simple cuando el campo es no-arquimediano. A continuación se mostrará que el campo $\mathbb{Q}$ no es completo.

Lema 32. *El campo $\mathbb{Q}$ de números racionales no es completo con respecto a cualquiera de sus valores absolutos no triviales.*

Demostración. Según el Teorema 29 llamado Teorema de Ostrowski, solo se necesita comprobar que $\mathbb{Q}$ no es completo para $\| \|_p$ para $p \leq \infty$; como $\mathbb{Q}$ no es completo respecto al valor absoluto (por ejemplo construir una sucesión de racionales que converge a $\sqrt{2}$ que no es racional). Así que se verá ahora que $\mathbb{Q}$ no es completo para la norma p-ádica. Tomando la norma $\| \|_p$ donde p es un número primo; se quiere construir una sucesión de Cauchy en $\mathbb{Q}$ que no tenga limite en $\mathbb{Q}$. Para construir la sucesión de Cauchy, solo se tiene que encontrar una sucesión coherente de soluciones módulop^n de una ecuación que no tiene soluciones en $\mathbb{Q}$, se hará en el caso $p \neq 2$. Entonces, supóngase un primo $p \neq 2$. Se debe elegir un entero $a \in \mathbb{Z}$ tal que se cumplan la siguientes condiciones: a no es un cuadrado en $\mathbb{Q}$, p no divide a a y además a sea un residuo cuadrático módulo p, es decir, la congruencia $x^2 \equiv a \,(mod\, p)$ tiene solución. (el caso $p = 2$ se tiene de manera análoga eligiendo a tal que no es cubo en $\mathbb{Q}$).

Por ejemplo, podría tomarse cualquier cuadrado en $\mathbb{Z}$ y añadir un múltiplo de p para conseguir un a que sea adecuado. Ahora se pueden construir sucesiones de Cauchy respecto a la norma p-ádica de la siguiente manera: Elegir un x_0 que sea cualquier solución de $x_0^2 \equiv a \,(mod\, p)$. Tomar x_1 de modo que $x_1 \equiv x_0 \,(mod\, p)$ y $x_1^2 \equiv a \,(mod\, p^2)$; en general se tiene que $x_n \equiv x_{n-1} \,(mod\, p^n)$ y $x_n^2 \equiv a \,(mod\, p^{n+1})$. De hecho tales sucesiones existen cada vez que el elemento inicial x_0 existe (se garantiza la existencia de x_0, el resto sigue porque $p \neq 2$). Ahora se comprobará que realmente es una sucesión de Cauchy; esto es claro por la construcción.

$$\|x_{n+1} - x_n\|_p = \left\|\beta\, p^{n+1}\right\|_p \leq p^{-(n+1)} \longrightarrow 0$$

Por lo tanto por el Lema 31 la sucesión de los x_n es ciertamente una sucesión de Cauchy. Por otro lado

$$\left\|x_n^2 - a^2\right\|_p = \left\|\mu p^{n+1}\right\|_p \leq p^{-(n+1)} \longrightarrow 0$$

De modo que si el limite existiese en $\mathbb{Q}$, sería una raíz cuadrada de a. Como a no es cuadrado en $\mathbb{Q}$, no puede haber ningún limite, lo que muestra que $\mathbb{Q}$ no es completo respecto respecto a la norma p-ádica $\| \|_p$. □

Ya que $\mathbb{Q}$ no es completo, se necesita construir una completación. Hay varias formas de hacerlo; se va a seguir el camino mas intuitivo. Lo que se quiere hacer es «agregar a

$\mathbb{Q}$ los límites de todas las sucesiones de Cauchy», para ello se empieza con el conjunto de todos sucesiones de Cauchy como el objeto de base, a continuación, se utilizan las operaciones algebraicas en $\mathbb{Q}$ para manejar el objeto resultante. (La construcción utiliza algunas nociones de álgebra abstracta). Sea p un primo fijo, se construye la completación de $\mathbb{Q}$ con respecto a la norma p-ádica $\| \|_p$ dada en la definición 22. Se toman los siguientes conjuntos:

Definición 33. Sea $\mathcal{C}$ el conjunto de las sucesiones de Cauchy en $\mathbb{Q}$ con respecto a $\| \|_p$

$$\mathcal{C} = \mathcal{C}_p(\mathbb{Q}) = \left\{(x_n) : (x_n) \ \ es\, sucesion\, de\, Cauchy\, respecto\, a\ \| \|_p\right\}$$

Se puede verificar que $\mathcal{C}$ tiene estructura de anillo conmutativo, usando las definiciones para la suma y el producto de dos sucesiones. Así:

$$(x_n) + (y_n) = (x_n + y_n)$$

$$(x_n)(y_n) = (x_n . y_n)$$

se puede probar que $\mathcal{C}$ es un anillo conmutativo con unidad. Este anillo contiene el campo $\mathbb{Q}$, de hecho, cabe notar que si $x \in \mathbb{Q}$ es cualquier número de la sucesión x, x, x, ... es sin duda de Cauchy, que se llama sucesión *constante* asociada a x denotada por (x).

El principal problema con $\mathcal{C}$ es que aún no se capta la idea de "agregar los límites de toda sucesión de Cauchy " porque diferentes sucesiones de Cauchy cuyos términos se acercan entre sí deberían tener el mismo límite, pero son diferentes en $\mathcal{C}$. Este tipo de situación requiere de la identificación de dos sucesiones que deben tener el mismo límite, lo que significa que se debe pasar al cociente de $\mathcal{C}$, esto es, se tiene que introducir una relación de equivalencia de algún tipo, y así identificar elementos equivalentes. En este caso, se busca aprovechar el álgebra abstracta, ya que $\mathcal{C}$ es un anillo conmutativo, y así es más fácil para describir cuando dos sucesiones tienen el mismo límite: esto sucede cuando sus términos se acercan el uno al otro, es decir, cuando la diferencia de las sucesiones tiende a cero. Así se definirá el conjunto de sucesiones que tiende a cero.

Definición 34. Sea $\mathcal{N} \subset \mathcal{C}$ donde

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

sucesiones que tienden a cero respecto a la norma $p-ádica$ $\| \|_p$. Usando esta definición

se puede verificar que $\mathcal{N}$ es un ideal de $\mathcal{C}$ usando el producto entre sucesiones.

Como $\mathcal{N} \subset \mathcal{C}$ es un ideal, y $\mathcal{C}$ es un anillo; se mostrará la relación existente entre ellos como estructuras algebraicas.

Lema 35. *$\mathcal{N}$ es un ideal maximal de $\mathcal{C}$*[8]

Demostración. Sea $(x_n) \in \mathcal{C}$ una sucesión de Cauchy que no tiende a cero, esto es, no pertenece a $\mathcal{N}$ y sea I el ideal generado por (x_n) y $\mathcal{N}$. Lo que se quiere mostrar es que I debe ser todo $\mathcal{C}$, para esto se mostrará que el elemento unidad (1), es decir, la sucesión correspondiente a 1, esta en I. Esto basta, ya que cualquier ideal que contiene el elemento unidad debe ser todo el anillo. Ahora ya que (x_n) no tiende a cero y es una sucesión de Cauchy que debe a partir de cierto momento alejarse de cero, es decir, debe existir un $c > 0$ y un entero N tal que $\|x_n\| \geq c > 0$ cuando $n \geq N$. Ahora en particular esto significa que $x_n \neq 0$ para $n \geq N$. Por lo que se puede definir una nueva sucesión (y_n) fijando

$$y_n = 0 \text{ si } n < N \text{ y } y_n = \frac{1}{x_n} \text{ si } n \geq N.$$

Lo primero es probar que (y_n) es un sucesión de Cauchy, que es claro porque si $n \geq N$ se tiene.

$$\|y_{n+1} - y_n\|_p = \left\| \frac{1}{x_{n+1}} - \frac{1}{x_n} \right\|_p = \frac{\|x_{n+1} - x_n\|_p}{\|x_{n+1} x_n\|_p} \leq \frac{\|x_{n+1} - x_n\|_p}{c^2} \to 0$$

que muestra que $(y_n) \in \mathcal{C}$ porque $\| \ \|_p$ es no-arquimediana. Además,

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

Esto significa que la sucesión $(x_n)\,(y_n)$=$(x_n y_n)$ consiste en un número finito de ceros seguido por una cadena infinita de unos. En particular, si se resta de la sucesión constante (1), se obtiene una sucesión que tiende a cero. Es decir:

$$(1) - (x_n)\,(y_n) = (1,\, 1,\, \ldots 0,\, 0, 0 \ldots) \in \mathcal{N}$$

[8]Un ideal $I \subset A$ es un ideal maximal de A si $I \neq A$ y si $K \subseteq A$ es ideal tal $I \subseteq K$ entonces $J = A$

Pero esto es que la sucesión (1) se puede escribir como un múltiplo de (x_n) más un elemento de $\mathcal{N}$, y por lo tanto pertenece a I, como se quería. □

Se quiere identificar sucesiones que difieren por elementos de $\mathcal{N}$, con el argumento de que deberían tener el mismo límite. Esto se realiza en la forma habitual, tomando el cociente del anillo $\mathcal{C}$ por el ideal $\mathcal{N}$. Además, lo que hace esto aún más interesante es el hecho de que teniendo un cociente de un anillo por el ideal maximal se obtiene un campo.

Definición 36. Se define el campo de los números p-ádicos como el cociente del anillo $\mathcal{C}$ por el ideal maximal $\mathcal{N}$, así

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

Los elementos de $\mathbb{Q}_p$ son clases de equivalencia de sucesiones de Cauchy en $\mathbb{Q}$ con respecto a la extensión de la norma p-ádica $\| \|_p$. Note que dos sucesiones constantes distintas nunca se diferencian por un elemento de $\mathcal{N}$, su diferencia es simplemente otra sucesión constante. Por lo tanto, se tiene la inclusión

$$\mathbb{Q} \hookrightarrow \mathbb{Q}_p$$

mediante el envío de $x \in \mathbb{Q}$ a las clases de equivalencia de la sucesión constante (x). Luego se ha encontrado un campo, y una inclusión de $\mathbb{Q}$ en el campo. Queda por comprobar que cumple las propiedades de la completación. La primera es que la norma p-ádica $\| \|_p$ se extiende a $\mathbb{Q}_p$ esto se obtiene fácilmente del siguiente lema.

Lema 37. *Sea $(x_n) \in \mathcal{C}$, $(x_n) \notin \mathcal{N}$. La sucesión de números reales $\| x_n\|_p$ es finalmente estable, es decir, existe un entero N tal que $\| x_n\|_p = \| x_m\|_p$ siempre que $m, n \geq N$*

Demostración. Ya que (x_n) es una sucesión de Cauchy que no tiende a cero. Dado $\varepsilon > 0$, existe $N_1 \in \mathbb{N}$ tal que si

$$n \geq N_1 \implies \| x_n\|_p \geq \varepsilon > 0$$

Por otra parte, también existe un entero N_2 para el que

$$n, m \geq N_2 \implies \| x_n - x_m\|_p < \varepsilon$$

como se quiere que ambas sean verdaderas a la vez; sea $N = max\{N_1, N_2\}$ entonces se tiene

$$n, m \geq N \implies \varepsilon \leq \| x_n - x_m + x_m \|_p \leq max \left\{ \| x_n - x_m \|_p , \| x_m \|_p \right\}$$

de ahí que $\| x_n \|_p \leq \| x_m \|_p$ por la propiedad no-arquimediana. Análogamente se puede ver que $\| x_n \|_p \geq \| x_m \|_p$ y por lo tanto $\| x_n \|_p = \| x_m \|_p$. □

Esto significa que la definición que se dará a continuación tiene sentido.

Definición 38. Si $\lambda \in \mathbb{Q}_p$ y (x_n) es cualquier sucesión de Cauchy que representa a λ, se define

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

Observación 39. Cabe recordar que $\mathbb{Q}_p$ se definió como un cociente, por lo que los elementos de $\mathbb{Q}_p$ son clases de equivalencia de sucesiones de Cauchy. Se puede mostrar que el limite que se definió anteriormente existe y no depende de la elección de la sucesión de Cauchy (a_n) en $\mathbb{Q}_p$, es decir, si $(a_n) \sim (\overline{a}_n)$ entonces $\lim_{n \to \infty} \| a_n \|_p = \lim_{n \to \infty} \| \bar{a}_n \|_p$. Como se tiene que

$$\left| \| a_n \|_p - \| \overline{a}_n \|_p \right|_p \leq \| a_n - \overline{a}_n \|_p$$

usando la desigualdad triangular y por la desigualdad anterior

$$0 \leq \lim_{n \to \infty} \left| \| a_n \|_p - \| \bar{a}_n \|_p \right|_p \leq \lim_{n \to \infty} \| a_n - \bar{a}_n \|_p$$

y como $(a_n) = (\overline{a}_n) + \mathcal{N}$ entonces $(a_n) - (\overline{a}_n) \to 0$, ya que son sucesiones de Cauchy y por tanto $\lim_{n \to \infty} \| a_n \|_p = \lim_{n \to \infty} \| \bar{a}_n \|_p$

Para comprobar que efectivamente se ha obtenido la completación se debe ahora comprobar dos propiedades mas: $\mathbb{Q}$ es denso en $\mathbb{Q}_p$ y que $\mathbb{Q}_p$ es completo.

Proposición 40. *$\mathbb{Q}$ es un subconjunto denso de $\mathbb{Q}_p$*

Demostración. Se tiene que probar que cualquier bola abierta alrededor de un elemento $\varphi \in \mathbb{Q}_p$ contiene un elemento de $\mathbb{Q}$ es decir una sucesión constante. Sea ε un radio fijo. Se mostrará que hay una sucesión constante que pertenece a la bola abierta $B(\varphi, \varepsilon)$.

Tomando (x_n) una sucesión de Cauchy que representa a φ y sea ε' tal que $\varepsilon' < \varepsilon$. Por ser sucesión de Cauchy, existe un número N tal que $\| x_n - x_m \|_p < \varepsilon'$ siempre que

$n, m \geq N$. Sea $y = x_N$ y considerando la sucesión constante (y). Se afirma que

$$(y) \in B(\varphi, \varepsilon)$$

es decir, $\|\varphi - (y)\| < \varepsilon$ y además,

$$\varphi - (y) = (\ldots (x_n) - (x_N)) = (\ldots (x_{N+1} - x_N)(0)(x_{N-1}) \ldots (x_2)(x_1))$$

es representada por la sucesión $(x_n - y)$ y usando la Definición 38

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

Pero para cualquier $n \geq N$ se tiene

$$\|x_n - y\|_p = \|x_n - x_N\|_p < \varepsilon'$$

de modo que, en el limite, se obtiene

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

por lo tanto (y) en efecto pertenece a $B(\varphi, \varepsilon)$. □

Para probar que $\mathbb{Q}_p$ es completo se debe mostrar que cada sucesión de Cauchy en $\mathbb{Q}_p$ converge en $\mathbb{Q}_p$

Proposición 41. *$\mathbb{Q}_p$ es completo con respecto a la norma $\| \ \|_p$.*

Demostración. Sea $(\varphi_n) = \{\varphi_1, \varphi_2, \varphi_3 \ldots \varphi_k \ldots\}$ es una sucesión de Cauchy en $\mathbb{Q}_p$ como $\mathbb{Q}$ es denso en $\mathbb{Q}_p$ para algún φ_n existe un elemento $a_n \in \mathbb{Q}$ tal que $\|\varphi_n - a_n\|_p < \frac{1}{n}$ usando la demostración anterior, por lo tanto:

$$\lim_{n\to\infty} \|\varphi_n - a_n\|_p = 0$$

Esto implica que $(\varphi_n - a_n)$ es una sucesión nula, y por lo tanto una sucesión de Cauchy en $\mathbb{Q}_p$. Se tiene

$$(a_n) = (\varphi_n) - (\varphi_n - (a_n))$$

y de ahí que (a_n) es una sucesión de Cauchy en $\mathbb{Q}_p$, pero ya que todos sus elementos pertenecen a $\mathbb{Q}$, (a_n) es una sucesión de Cauchy en $\mathbb{Q}$. Denotando las clases de equi-

valencia de (a_n) por φ , luego $\{\varphi - (a_n)\}$ y $\{\varphi_n - (a_n)\}$ son sucesiones nulas en $\mathbb{Q}_p$ y además su diferencia.

$$\{\varphi - \varphi_n\} = \{\varphi - (a_n)\} - \{\varphi_n - (a_n)\}$$

es una sucesión nula en $\mathbb{Q}_p$ esto implica que

$$\lim_{n\to\infty} \|\varphi - \varphi_n\|_p = 0$$

pero esto es precisamente $\varphi = \lim_{n\to\infty} \varphi_n$ □

A continuación se enuncia otra forma de identificar los elementos de $\mathbb{Z}_p$ que son llamados *enteros* $p-$*ádicos*

Definición 42. El conjunto de los *enteros* $p-$*ádicos* esta dado por:

$$\mathbb{Z}_p = \left\{\alpha \in \mathbb{Q}_p \mid \|\alpha\|_p \leq 1\right\}$$

Como ya se hizo el proceso de completación de $\mathbb{Q}$, se puede ahora mostrar de manera mas general como se puede hallar la expansión p-ádica de cualquier número para ello se requiere de antemano enunciar algunos resultados.

Teorema 43. *Si* $\| \ \|$ *es una norma no-arquimediana en un campo* K *entonces se cumple que* $\|K\| = \left\|\tilde{K}\right\|$ *donde* $\tilde{K}$ *es la completación de* K*.*

Demostración. Sea $\alpha \in \tilde{K}$. Si $\alpha = 0$, $\|\alpha\| = 0$. Suponga que $\alpha \neq 0$ ya que K es denso en $\tilde{K}$, existe una sucesión de Cauchy (a_n) de elementos de K tal que $\lim_{n\to\infty} a_n = \alpha$. Sin embargo como $\| \ \|$ es una norma no-arquimediana en K entonces

$$\| a_n\| = \|\alpha + (a_n - \alpha)\| \leq max\left\{\|\alpha\|, \| a_n - \alpha\|\right\}$$

Como $\|\alpha\| \neq 0$ y $\| a_n - \alpha\|$ se puede hacer arbitrariamente pequeño tomando n suficientemente grande se tiene que

$$\lim_{n\to\infty} \|a_n\| = \lim_{n\to\infty} \|\alpha\|$$

lo que concluye la prueba. □

Lema 44. *Si* $x \in \mathbb{Q}$ *y* $\|x\|_p \leq 1$ *entonces para cualquier* i *existe un número entero* $\alpha \in \mathbb{Z}$ *tal que*

$$\|\alpha - x\|_p \leq \frac{1}{p^i}$$

donde el entero α *puede ser elegido del conjunto* $\{0, 1, 2, \ldots, p^i - 1\}$

Demostración. Sea $x = \frac{a}{b}$ donde a y b son primos relativos, esto es, $(a, b) = 1$. Ya que $\|x\|_p \leq 1$, se sigue que p no divide a b y por lo tanto b y p^i son primos relativos. Así que se pueden encontrar enteros m y n tales que $mb + np^i = 1$. Sea $\alpha = am$. Entonces

$$\|\alpha - x\|_p = \left\|am - \frac{a}{b}\right\|_p = \left\|\frac{amb - a}{b}\right\|_p = \left\|\frac{a}{b}(mb - 1)\right\|_p = \left\|\frac{a}{b}\right\|_p \|mb - 1\|_p$$

como $\left\|\frac{a}{b}\right\|_p \leq 1$ entonces

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

ya que $n \in \mathbb{Z}$ se tiene que $\|n\|_p \leq 1$. Por último usando la desigualdad triangular, se puede añadir un múltiplo de p^i al entero α para obtener un entero entre 0 y p^i para el que $\|\alpha - x\|_p \leq p^{-i}$. □

Teorema 45. *Toda clase de equivalencia* a *en* $\mathbb{Q}_p$ *que satisface* $\|a\|_p \leq 1$ *tiene exactamente una representación* (a_i) *de la sucesión de Cauchy tal que:*

1. $a_i \in \mathbb{Z},\ 0 \leq a_i < p^i$ para $i = 1, 2 \ldots$
2. $a_i \equiv a_{i+1} \pmod{p^i}$ para $i = 1, 2 \ldots$

Demostración. Sea (b_i) una sucesión de de Cauchy. Se quiere encontrar una sucesión equivalente (a_i) que satisfaga (1) y (2). Para cada $j = 1, 2, \ldots$ sea $N(j)$ un entero positivo tal que

$$\|b_i - b_{i'}\|_p \leq \frac{1}{p^j} \ \forall\, i, i' \geq N(j)$$

Tomando la sucesión de $N(j)$ que sea creciente con j así $N(j) \geq j$. Además, como $\|b_i\|_p \leq 1$ si $i \geq N(1)$ por lo tanto para todo $i' \geq N(1)$ se tiene que

$$\|b_i\|_p = \|b_i + b_{i'} - b_{i'}\| \leq max\left\{\|b_{i'}\|_p, \|b_i - b_{i'}\|_p\right\} \leq max\left\{\|b_{i'}\|_p, \frac{1}{p}\right\}$$

y

$$\|b_{i'}\|_p \to \|a\|_p \leq 1 \text{ cuando } i' \to \infty$$

por el Lema 44 se puede hallar una sucesión de enteros a_j donde $0 \leq a_j < p^j$ tal que

$$\left\| a_j - b_{N(j)} \right\|_p \leq \frac{1}{p^j}$$

Supóngase que (a_j) es la sucesión requerida, se mostrará que $a_j \equiv a_{j+1} \,(mod\, p^j)$ y $(b_i) \sim (a_j)$. La primera afirmación se sigue del hecho de que

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

$$\leq max \left\{ \frac{1}{p^{j+1}}, \frac{1}{p^j}, \frac{1}{p^j} \right\} = \frac{1}{p^j}$$

por lo tanto $a_j \equiv a_{j+1} \,(mod\, p^j)$ y para probar que $(b_i) \sim (a_j)$. Tomar cualquier j, entonces para $i \geq N(j)$se tiene

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

$$\leq max \left\{ \frac{1}{p^j}, \frac{1}{p^j}, \frac{1}{p^j} \right\} = \frac{1}{p^j}$$

de ahí que $\|a_i - b_i\|_p \to 0$ cuando $i \to \infty$.

Ahora se probará la unicidad. Si (a'_i) es una sucesión diferente que satisface (1) y (2) y supóngase que $a_{i_0} \neq a'_{i_0}$ para algún i_0, entonces $a_{i_0} \not\equiv a'_{i_0} \,(mod\, p^{i_0})$ ya que a_{i_0} y a'_{i_0} están entre 0 y p^{i_0} entonces se deduce a partir de (2) para $i > i_0$

$$a_i \equiv a_{i_0} \not\equiv a'_{i_0} \equiv a'_i \left(mod\, p^{i_0}\right)$$

es decir, $a_i \not\equiv a'_i \,(mod\, p^{i_0})$. Esto significa que

$$\|a_i - a'_i\| > \frac{1}{p^{i_0}} \quad \forall\, i \geq i_0$$

lo que implica que $(a_i) \not\sim (a'_i)$. $\square$

Si $a \in \mathbb{Q}_p$ con $\| a\|_p \leq 1$ es conveniente escribir todos los términos a_i de la sucesión representativa propuesta por el teorema anterior de la siguiente manera:

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

donde cada d_i es un entero en $\{0,\, 1,\, \ldots\, , p-1\}$. La condición (2) significa precisamente que

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

Así a esta representada por la serie convergente (en la norma p-ádica).

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

Donde los dígitos d_i , $0 \leq i \leq p-1$ son los mismos que a_n en base p. Luego a puede ser pensado como un número escrito en base p, que se extiende infinitamente a la izquierda, es decir, se agrega un nuevo dígito cada vez que se pasa de a_n a a_{n+1}.

Si $\| a\|_p > 1$ a saber $p^m = \|a\|_p$ con $m \geq 1$, con el fin de obtener un número p-ádico $a' = ap^m$ que satisface $\| a'\|_p \leq 1$. Luego se puede escribir

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

donde $d_{-m} \neq 0$ y $b_i \in \{0,\, 1,\, 2,\, \ldots,\, p-1\}$ y representar al número p-ádico a como una fracción en la base p con infinitos dígitos antes del punto y finitos dígitos después. A continuación se muestra como generar la expansión canónica de una manera mas general que la dada en la sección 1.1.

Sea $\alpha \in \mathbb{Q}_p$ y $\alpha \neq 0$ usando el teorema 43 se tiene que

$$\|\mathbb{Q}_p\|_p = \|\mathbb{Q}\|_p = \left\{ \| p \|_p^n \mid n = 0,\, \pm 1,\, \pm 2,\, \pm 3,\, \ldots \right\}$$

así

$$\|\alpha\|_p = \| p \|_p^n \qquad (1)$$

y por lo tanto $\frac{\alpha}{p^n} = \beta$ es una unidad es decir $\|\beta\|_p = 1$. Se designará por $\mathcal{V}$, el anillo de $\| \ \|_p$ en $\mathbb{Q}$, por $\mathcal{P}$ el único ideal maximal de $\mathcal{V}$, por $\tilde{\mathcal{V}}$ el anillo de $\| \ \|_p$ en $\mathbb{Q}_p$ y por $\tilde{\mathcal{P}}$ el

único ideal maximal de $\tilde{\mathcal{V}}$. Claramente $\frac{\alpha}{p^n} = \beta \in \tilde{\mathcal{V}}$. Pero $\beta = lim\, c_k$ donde $c_k \in \mathbb{Q}$. Así $\|\beta - c_k\|_p < 1$ para k suficientemente grande, supóngase, $k \geq N$. Por lo tanto

$$\|c_N\|_p = \|\beta + (c_N - \beta)\|_p = max\left(\|\beta\|_p\ ,\ \|c_N - \beta\|_p\right) = \|\beta\|_p$$

luego

$$\|c_N\|_p = \|\beta\|_p = 1$$

donde $c_N \in \mathbb{Q}$ y por tanto $c_N \in \mathcal{V}$. Como $\|c_N\|_p = 1$ y $\|\beta - c_N\|_p < 1$ de donde $\beta + \tilde{\mathcal{P}} = c_N + \tilde{\mathcal{P}}$ ya que $\tilde{\mathcal{P}}$ es ideal de $\tilde{\mathcal{V}}$ donde se inducen una partición de $\tilde{\mathcal{V}}$ en clases de equivalencia.

Sea $c_N = \frac{e_n}{d_n}$ donde $e_n\ ,\ d_n \in \mathbb{Z}$ y además e_n y d_n son primos relativos con p que es posible ya que $\|c_N\|_p = 1$. Así que existen enteros x e y tal que

$$xd_n + yp = 1 \quad \text{ó} \quad xd_n \equiv 1\,(mod\, p)$$

entonces

$$\frac{e_n}{d_n} - e_n x = \frac{e_n\,(1 - d_n x)}{d_n} \equiv 0\,(mod\, p)$$

es decir, $c_N - e_n x \in \mathcal{P}$ de ahí que $c_N - e_n x \in \tilde{\mathcal{P}}$. Sea $e_n x = a_n$ entonces $a_n \in \mathbb{Z}$ y $\beta + \tilde{\mathcal{P}} = c_N + \tilde{\mathcal{P}} = a_n + \tilde{\mathcal{P}}$.

Ahora, $\|a_n - \beta\|_p < 1$ y se tiene

$$\|\, a_n p^n - \beta p^n\|_p < \|\, p^n\|_p \qquad (2)$$

de ahí que $\alpha = \beta p^n = a_n p^n + (\beta - a_n)\, p^n = a_n p^n + \gamma_1$ donde $\gamma_1 = (\beta - a_n)\, p^n$ y $\|\gamma_1\|_p < \|p\|_p^n$ esto por (2). Así $\|\gamma_1\|_p = \|p\|_p^m$ donde $m > n$, que es la misma relación con la que se partió para α en (1). Por lo tanto, se trata γ_1 como se hizo con α y se continúa el proceso. Después de k pasos, se obtiene

$$\alpha = a_n p^n + a_{n+1} p^{n+1} + \ldots + a_{n+k-1} p^{n+k-1} + \gamma_k$$

donde los $a_i \in \mathbb{Z}$ y $\|\, a_i\|_p = 1$ ó $a_i = 0$ y además $\|\gamma_k\|_p \leq \|\, p\|_p^{n+k}$. Ya que $\|\, p\|_p^{n+k} \to 0$ cuando $k \to \infty$ se puede establecer de manera más general lo dicho en la Definición **??**.

Definición 46. Cualquier número p-ádico α puede ser escrito en la forma

$$\sum_n^{\infty} a_i p^i$$

donde $a_i \in \mathbb{Z}$ con $0 \leq a_i \leq p-1$, y además n es tal que $\|\alpha\|_p = \|p\|_p^n$. Que es la representación canónica o expansión de α.

Existe una diferencia sutíl con respecto a la expansión decimal de un número real y es la *unicidad* nótese el caso de que $1,00000 = 0,99999$. En el caso $p-$*ádico* no hay tales excepciones. Si dos expansiones p-ádicas convergen al mismo número, sus dígitos son los mismos. Para ver esto supóngase que $\alpha \neq 0$ con $\alpha = a_0 + a_1 p + a_2 p^2 + \ldots$ y

$$\alpha = a_0' + a_1' p + a_2' p^2 + \ldots$$

es segunda expansión con la propiedad de la primera y supóngase que no todos los dígitos p-ádicos son iguales. Sea d el primer entero para la cual $a_d \neq a_d'$. Entonces restando las dos representaciones se seguiría que

$$0 = (a_d - a_d')\, p^d + \text{términos de mayor potencia de } p$$

que es evidentemente imposible. Ya que $a_d \neq a_d'$ y por tanto $a_d - a_d' \neq 0$.

De la Definición 46 se deduce inmediatamente el siguiente teorema.

Teorema 47. *El conjunto de los enteros p-ádicos es no contable*

Demostración. En efecto, tomando cualquier sucesión de números p-ádicos enteros

$$a = \sum_{i=0}^{\infty} a_i\, p^i \;\; ; \;\; b = \sum_{i=0}^{\infty} b_i\, p^i \;\; ; \;\; c = \sum_{i=0}^{\infty} c_i\, p^i \quad \ldots$$

se puede definir un entero p-ádico

$$x = \sum_{i=0}^{\infty} x_i\, p^i$$

escogiendo $x_0 \neq a_0$, $x_1 \neq b_1$, $x_2 \neq c_2$ ... construyendo un entero p-ádico distinto de a, b, c, ... Esto muestra que la sucesión a, b, c, ... no agota el conjunto de números enteros p-ádicos. Por tanto una función del conjunto de números naturales $\mathbb{N}$ en el conjunto de números enteros p-ádicos nunca es sobreyectiva. □

Como se pudo notar en la Sección 1.1 al hallar esta expansión se vuelve algo tedioso de calcular. Los ejemplos que se presentan a continuación son otra manera de hallar esta expresión.

En la Sección 1.3 se mostró que $-1 = (p-1)\sum_{i=0}^{\infty} p^i$, se tiene entonces

$$\sum_{i=0}^{\infty} p^i = \frac{1}{1-p}$$

Ejemplo 48. Hallar el desarrollo $5-$*ádico* de $-\frac{1}{4}$

Como $-\frac{1}{4}$ se puede expresar de la siguiente manera

$$-\frac{1}{4} = \frac{1}{1-5} = 5^0 + 5^1 + 5^2 + 5^3 + \dots$$

lo cual muestra el desarrollo de una serie geométrica de la forma $\sum a\, r^{n-1} = \frac{a}{1-r}$ que es convergente si $|r| < 1$ y como $|5|_p = \frac{1}{5} < 1$ entonces es convergente y la expansión $5-$*ádica* de $\alpha = -\frac{1}{4} = 5^0 + 5^1 + 5^2 + 5^3 + \dots$

Para ilustrar una manera mas general se seguirán los pasos previos que dieron lugar a la Definición 46 así:

Ejemplo 49. Hallar la expansión de $\frac{3}{8}$ en $\mathbb{Q}_5$

Entonces $\left\|\frac{3}{8}\right\|_5 = \|5\|_5^0 = 1$ como $n = 0$. Tomando una solución de

$$8x \equiv 1 \ (mod\, 5)$$

es $x = 2$ y entonces $2 \cdot 3 \equiv 1 \ (mod\, 5)$ y se obtiene $a_0 = 1$.

Ahora $\gamma_1 = \left(\frac{3}{8} - 1\right) = -\frac{5}{8}$ y $\left\|-\frac{5}{8}\right\|_5 = \|5\|_5^1$ que indica que $a_1 \neq 0$ y $-\left(\frac{5}{8}\right)/5 = -\frac{1}{8}$. De nuevo una solución de

$$8x \equiv 1 \ (mod\, 5)$$

es $x = 2$ y $2\ (-1) \equiv 3 \ (mod\, 5)$ y se obtiene entonces que $a_1 = 3$. Luego $\gamma_2 = \left(-\frac{1}{8} - 3\right) \cdot 5 = \left(-\frac{25}{8}\right) \cdot 5$.

Ahora $\|\gamma_2\| = \|5\|_5^3$ que indica que $a_2 = 0$ pero $a_3 \neq 0$ y entonces $\frac{\gamma_2}{5^3} = -\frac{1}{8}$ se nota como el hecho anterior que $a_3 = 3$. Continuando así, se puede ver que

$$a_4 = a_6 = \dots = 0 \quad y \quad a_5 = a_7 = \dots = 3$$

por tanto la expansión p-ádica de $\frac{3}{8}$ en $\mathbb{Q}_5$ es forma corta sería $\frac{3}{8} = 1, \overline{30}$

$$\frac{3}{8} = (1, 303030\dots)_5$$

3. Algunas propiedades de $\mathbb{Q}_p$

Desde cierto punto de vista, los campos $\mathbb{R}$ y $\mathbb{Q}_p$; son similares ya que son la completación de $\mathbb{Q}$, pero con respecto a diferentes normas. Se puede probar que $\mathbb{Q}_p$ no es cerrado algebraicamente ya que $x^2 - p = 0$ no tiene solución en $\mathbb{Q}_p$.

Ya que en el caso de que exista $\sqrt{p}$ será de esta forma:

$$\sqrt{p} = a_0 + a_1 p + a_2 p^2 + \dots$$

y eso es entonces

$$\left(a_0 + a_1 p + a_2 p^2 + \dots\right)^2 = 0 + 1p$$

de donde $a_0^2 \equiv 0\,(mod\,p)$ y por tanto $a_0 = 0$ ahora como $2a_1 a_0 \equiv 1\,(mod\,p)$ que es contradictorio por lo que $\mathbb{Q}_p$ no es algebraicamente cerrado así como tampoco los es $\mathbb{R}$.

Pero cabe aclarar que $\mathbb{Q}_p$ no es comparable con $\mathbb{R}$. Ya que por ejemplo $\sqrt{7} \notin \mathbb{Q}_5$ mientras que $i = \sqrt{-1} \in \mathbb{Q}_5$. Como se mostrará a continuación:

En caso de que exista $\sqrt{7}$ sera de la forma

$$\sqrt{7} = a_0 + a_1 5 + a_2 5^2 + \dots$$

y se debe tener que

$$\left(a_0 + a_1 5 + a_2 5^2 + \dots\right)^2 = 7 = 2 + 1.\,5$$

donde $a_0^2 \equiv 2\,(mod\,5)$ como esta ecuación no tiene solución se puede afirmar que $\sqrt{7}$ no existe en $\mathbb{Q}_5$. Así mismo como $-1 = (5-1) + (5-1)\,.\,5 + (5-1)\,.\,5^2 + \dots$ de ahí que $a_0^2 \equiv 4\,(mod\,5)$ de donde $a_0 = 2\,,\,3$ por lo tanto $\sqrt{-1} \in \mathbb{Q}_5$.

El siguiente teorema tiene cierta similitud con el teorema de Bolzano-Weierstrass para sucesiones en $\mathbb{R}$.

Teorema 50. *Toda sucesión infinita de enteros p-ádicos tiene una subsucesión convergente.*

Demostración. Tomando el hecho de que una subsucesión (x_{n_k}) de una sucesión (x_k) esta dada por una sucesión de números enteros positivos (n_k) tal que $n_1 < n_2 < n_3 < \dots$

Sea (x_k) una sucesión en $\mathbb{Z}_p$. Escribiendo la expansión canónica de cada termino así:

$$x_k = \dots a_2^k a_1^k a_0^k$$

ya que solo hay un número finito de posibilidades para los dígitos a_0^k a saber 0, 1, ... $p-1$ se puede encontrar un elemento $b_0 \in \{0, 1, \ldots p-1\}$ y una subsucesión infinita de (x_k), sea (x_{0k}) dicha subsucesión de tal manera que el último dígito de x_{0k} es siempre b_0. Usando el mismo razonamiento para $b_1 \in \{0, 1, \ldots p-1\}$ y una subsucesión (x_{1k}) de (x_{0k}) para los cuales los dos últimos dígitos son $b_1 b_0$. Continuando de esta manera, se obtienen b_0, b_1, b_2, ... junto con una «sucesión de sucesiones»

$$\begin{array}{ccccc} x_{00}, & x_{01}, & x_{02} & \ldots & , x_{0s} \\ x_{10}, & x_{11}, & x_{12} & \ldots & , x_{1s} \\ x_{20}, & x_{21}, & x_{22} & \ldots & , x_{2s} \\ \vdots & \vdots & \vdots & \ldots & \vdots \end{array}$$

de tal manera que cada sucesión es una subsucesión de la anterior, y de modo que que cada elemento de la fila n termina con b_n, ... $b_1 b_0$, Para cada $j = 0, 1, \ldots$ se tiene

$$x_{jj} \in \{x_{j-1\,j}, x_{j-1\,j+1}, \ldots\}$$

Por lo tanto la sucesión diagonal x_{00}, x_{11}, ... sigue siendo una subsucesión de la sucesión original, y obviamente converge a ... $b_3 b_2 b_1 b_0$ □

No es difícil extender este resultado a sucesiones acotados, que es el caso que se cumple para $\mathbb{R}$ y constituye el principal teorema acerca de la convergencia de sucesiones de números reales.

3.1. Orden en $\mathbb{Q}_p$

El campo de los reales $\mathbb{R}$ con la norma usual $|\ |$, tiene la propiedad importante de ser ordenado. Un anillo K se dice ordenado si para sus elementos x la relación $>$ puede ser definida y cumple las siguientes propiedades.

1. Todo elemento x de K satisface una y solo una de las siguientes relaciones

$$x = 0 \quad \text{o} \quad x > 0 \quad \text{o} \quad -x > 0$$

2. Si x y y son dos elementos de K que satisfacen $x > 0$ y $y > 0$ entonces $x + y > 0$ y $xy > 0$

3. Si $x \in K$ $x \neq 0$ entonces $x^2 > 0$

Un anillo K no puede ser ordenado si contiene un número finito de elementos $x_1, x_2, \ldots, x_n$ distintos de 0 que satisfacen $x_1^2 + x_2^2 + \ldots + x_n^2 = 0$. Por ejemplo, en el campo de los números complejos que no es ordenado, pues $1^2 + i^2 = 0$.

En el caso de $\mathbb{Q}_p$, el anillo $\mathbb{Q}_p$ no es ordenado. Ya que si $p = 2$ entonces contiene un elemento $x \neq 0$ en particular tome x tal que $-7 = 1 - 8 = x^2$ y

$$A_1 = (00 \ldots 0\, x)\,, \;\; A_2 = A_3 = \ldots = A_8 = (00 \ldots 01)$$

y además

$$A_1^2 + A_2^2 + \ldots + A_8^2 = 0$$

Si $p \geq 3$ es primo y denotando por y el número p-ádico para el cual $1 - p = y^2$ y tome

$$A_1 = (00 \ldots 0\, y)\,, \;\; A_2 = A_3 = \ldots = A_p = (00 \ldots 01)$$

estos números p-ádico son todos distintos de 0, pero es evidente que

$$A_1^2 + A_2^2 + \ldots + A_p^2 = 0$$

lo que prueba la afirmación.

3.2. Lema de Hensel

El método usando para resolver ecuaciones en $\mathbb{Q}_p$ puede ser generalizado por un resultado importante llamado «Lema de Hensel», esta es probablemente la característica algebraica más importante de los números p-ádicos. Básicamente, se dice que en cualquier caso se puede decidir con bastante facilidad si un polinomio tiene raíces en $\mathbb{Z}_p$.

Teorema 51. ***(Lema de Hensel).*** *Sea* $F(x) = b_0 + b_1 x + b_2 x^2 + \ldots + b_n x^n$ *un polinomio cuyos coeficientes son enteros* $p-$*ádicos. Sea*

$$F'(x) = b_1 + 2b_2 x + 3b_3 x^2 + \ldots + n b_n x^{n-1}$$

la derivada de $F(x)$*. Supóngase que* $\widetilde{a}_0$ *es un entero p-ádico que satisface que*

$$F(\widetilde{a}_0) \equiv 0 \,(mod\, p) \;\; y \; F'(\widetilde{a}_0) \not\equiv 0 \,(mod\, p)$$

Entonces existe un único entero p-ádico a tal que $F(a) = 0$ *y* $a \equiv \widetilde{a}_0 \,(mod\, p)$

Demostración. Se probará la existencia de a construyendo su expansión p-ádica dada por $a = b_0 + b_1 p + b_2 p^2 + \ldots$ inductivamente. En el paso $k - ésimo$ de inducción, lo que se hará es encontrar $a_k = b_0 + b_1 p + \ldots b_k p^k$ la $k - ésima$ aproximación de a, mediante el uso de la versión p-ádica del método de Newton que se comenta al final de esta prueba. Cada a_k no será una verdadera raíz de $F(x)$ pero será solo una raíz módulo p^{k+1}, es decir, $F(a_k) \equiv 0 \left(mod\, p^{k+1}\right)$ para todo k. Cuando $k \to \infty$ se obtendrá a, la verdadera raíz para F.

Más concretamente, se probará la siguiente afirmación por inducción sobre k :

Para algún $n \geq 0$ existe un entero p-ádico de la forma $a_k = b_0 + b_1 p + \ldots + b_k p^k$ donde $b_i \in \{0,\, 1, \ldots\, p-1\}$ tal que

$$F(a_k) \equiv 0 \left(mod\, p^{k+1}\right) \quad \text{y} \quad a_k \equiv \widetilde{a}_0 \,(mod\, p)$$

Tomando b_0 igual al primer dígito p-ádico de $\widetilde{a}_0$, se tiene que $a_0 \equiv \widetilde{a}_0 \,(mod\, p)$ y además, $F(a_0) \equiv 0 \,(mod\, p)$.

Ahora sea $a_k = a_{k-1} + b_k p^k$ para algún dígito b_k (todavía desconocido) que satisface $0 \leq b_k < p$ y expande a $F(a_k)$, ignorando términos divisibles por p^{k+1}

$$F(a_k) = F\left(a_{k-1} + b_k p^k\right) = \sum_{i=0}^{n} c_i \left(a_{k-1} + b^k p^k\right)^i$$

$$= \sum_{i=0}^{n} c_i \left(a_{k-1}^i + i a_{k-1}^{i-1} b^k p^k + \text{términos divisibles por } \; p^{k+1}\right)$$

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

ya que $F(a_{k-1}) \equiv 0 \left(mod\, p^k\right)$ por la hipótesis de inducción se pude escribir

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

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

Así que la ecuación para el b_k desconocido es

$$\alpha_k + b_k F'(a_{k-1}) \,(mod\, p)$$

Que se resuelve siempre que $F'(a_{k-1}) \not\equiv 0 \,(mod\, p)$ pero este es de hecho el caso ya que

$a_{k-1} \equiv \widetilde{a}_0 \,(mod\, p)$, de modo que

$$F'(a_{k-1}) \equiv F'(\widetilde{a}_0) \not\equiv 0 \,(mod\, p)$$

Dividiendo por $F'(a_{k-1})$ se puede encontrar el dígito b_k requerido

$$b_k = \frac{-\alpha_k}{F'(a_{k-1})} \,(mod\, p)$$

y como $F(a_k) \equiv \alpha_k p^k + b_k p^k F'(a_{k-1}) \,(mod\, p)$. Por tanto $F(a_k) \equiv 0 \left(mod\, p^{k+1}\right)$ lo que completa la inducción.

Ahora sea $a = \widetilde{a}_0 + b_1 p + b_2 p^2 + \ldots$ se observa que $F(a) = 0$ ya que para todo k se tiene

$$F(a) \equiv F(a_k) \equiv 0 \,\left(mod\, p^{k+1}\right)$$

La unicidad de a se sigue de la unicidad de las sucesiones $\{a_k\}$. □

Observación 52. En el método de Newton en el caso real, si $f'(a_{n-1}) \neq 0$ se toma

$$a_n = a_{n-1} - \frac{f(a_{n-1})}{f'(a_{n-1})}$$

esta expresión es similar a la usada en la prueba del Lema de Hensel

$$b_n p^n \equiv \frac{-\alpha_n p^n}{F'(a_{n-1})} \equiv -\frac{F(a_{n-1})}{F'(a_{n-1})} \left(mod\, p^{n+1}\right)$$

Sin embargo el Lema de Hensel es mas eficiente que el método de Newton en el caso real ya que la convergencia de la raíz de un polinomio es garantizada en el caso p-ádico, mientras que el método de Newton no siempre converge.

A continuación se muestra un ejemplo usando el Lema de Hensel para el cálculo de raíces.

Ejemplo 53. En $\mathbb{Q}_3$ hallar lar raíces del polinomio $F(x) = x^2 + 2x$

Tomando $a_0 = 1$ ya que $F(a_0) = 1^2 + 2 \equiv 0 \,(mod\, 3)$ y como $F'(x) = 2x + 2$ entonces $F'(a_0) = 2 + 2 = 4 \not\equiv 0 \,(mod\, 3)$ entonces existe un entero p-ádico, sea $a = a_0 + a_1.3 + a_2.3^2 + \ldots \in \mathbb{Z}_3$ tal que

$$\left(a_0 + a_1.3 + a_2.3^2 + \ldots\right)^2 + 2\left(a_0 + a_1.3 + a_2.3^2 + \ldots\right) = 0$$

entonces

$$\left(a_0^2+2a_0\right)+\left(2a_0a_1+2a_1\right).3+\left(2a_0a_2+a_1^2+2a_2\right).3^2+\left(2a_0a_3+2a_1a_2+2a_3\right).3^3+\ldots=0$$

Comparando coeficientes se tiene $a_0^2+2a_0\equiv 4\,(mod\,3)$ implica que $a_0=1$, como $\left(a_0^2+2a_0\right)=1+2=3=1.3$ entonces para el siguiente término se tendrá $1.3+\left(2a_0a_1+2a_1\right).3\equiv 0\,(mod\,3^2)$ esto es $\left(1+2a_0a_1+2a_1\right)\equiv 0\,(mod\,3)$ y por tanto $4a_1+1\equiv 0\,(mod\,3)$ de donde $a_1=2$, y como $\left(1+2a_0a_1+2a_1\right).3=(4+4+1).3=(2+2.3+1).3=3^2+2.3^2=1.3^3$; para el próximo coeficiente $\left(2a_0a_2+a_1^2+2a_2\right).3^2\equiv 0\,(mod\,3^3)$ esto es $4a_2+4\equiv 0\,(mod\,3)$ de ahí que $a_2=2$. Como $\left(2a_0a_2+a_1^2+2a_2\right).3^2=(4+4+4).3^2=(1.3+1.3^2).3^2=1.3^3+1.3^4$ luego para el siguiente paso se tendrá en cuenta el factor 1.3^3 obtenido en los pasos anteriores, de donde el próximo coeficiente esta dado por $2.3^3+\left(2a_0a_3+2a_1a_2+2a_3\right).3^3\equiv 0\,(mod\,3^4)$ lo que implica que $4a_3+10\equiv 0\,(mod\,3)$ y por lo tanto $a_3=2$. Luego se sigue que $1.3^4+\left(2a_0a_4+2a_1a_3+a_2^2+2a_4\right).3^4\equiv 0\,(mod\,3^5)$ esto es $4a_4+13\equiv 0\,(mod\,3)$ de donde $a_4=2$ continuando de esta manera se obtiene la serie

$$a=1+2.3+2.3^2+2.3^3+2.3^4+\ldots$$

donde $F(a)=0$ así que a es una raíz de la ecuación en $\mathbb{Q}_3$.

Cabe recordar que en el Teorema 45 la expansión canónica de los números p-ádicos salió de una sucesión de congruencias, y el Lema de Hensel confirma esa conexión. El siguiente teorema hace esta relación mucho mas evidente.

Teorema 54. *Un polinomio con coeficientes enteros tiene una raíz en $\mathbb{Z}_p$ si y solo si tiene una raíz entera módulo p^k para algún $k\geq 1$.*

Demostración. $\Rightarrow$Sea $F(x)$ un polinomio con coeficientes en $\mathbb{Z}$. Supóngase que $a\in\mathbb{Z}_p$ es una raíz, esto es $F(a)=0$

Por el Teorema 45 existe una sucesión de número enteros $\{a_1,\,a_2,\,a_3,\ldots,a_k,\ldots\}$ tal que

$$a\equiv a_k\left(mod\,p^k\right)\qquad\left(a_k=b_0+b_1p+b_2p^2+\ldots+b_{k-1}p^{k-1}\right)$$

luego $F(a_k)\equiv F(a)\left(mod\,p^k\right)$ y como $F(a)=0$ implica que

$$F(a_k)\equiv 0\left(mod\,p^k\right)$$

$\Leftarrow$ Supóngase que la congruencia $F(a_k) \equiv 0 \left(mod\, p^k\right)$ tiene una solución a_k para algún $k \geq 1$. De acuerdo con el teorema 50 la sucesión (a_k) contiene una subsucesión convergente (a_{k_i}), con $\lim\limits_{i\to\infty} a_{k_i} = a$. Se quiere demostrar que a es una solución de $F(x)$. Dado que un polinomio es una función continua, se tiene que

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

(En esta caso se usarán las propiedades de suma y producto de limites.)

Por otra parte

$$F(a_{k_i}) \equiv 0 \left(mod\, p^{k_i}\right)$$

por lo tanto $\lim\limits_{i\to\infty} F(a_{k_i}) = 0$ y así $F(a) = 0$. □

Si un polinomio con coeficientes enteros no tiene raíces módulo p entonces no tiene raíces en $\mathbb{Z}_p$. Esta es una consecuencia del Teorema 54. Por lo general no es demasiado difícil encontrar sus raíces módulo p, si tiene alguna. Si una raíz módulo p no es una raíz de la derivada módulo p, entonces por el Lema de Hensel se puede encontrar una raíz en $\mathbb{Z}_p$.

Se dice que un número entero a que no es divisible por p, es llamado *residuo cuadrático módulo* p si la congruencia

$$x^2 \equiv a\,(mod\, p)$$

tiene una solución en $\{1, 2, \ldots, p-1\}$.

Proposición 55. *Un entero a no divisible por p tiene una raíz cuadrada en $\mathbb{Z}_p$ $(p \neq 2)$ si y solo si a es un residuo cuadrático módulo p.*

Demostración. $\Leftarrow$ Sea $P(x) = x^2 - a$ como $P'(x) = 2x$. Si a es un residuo cuadrático entonce

$$a \equiv a_0^2\,(mod\, p)$$

para algún $a_0 \in \{1, 2, \ldots, p-1\}$. Por lo tanto $P(a_0) \equiv 0\,(mod\, p)$, pero como $P'(a_0) = 2a_0 \not\equiv 0\,(mod\, p)$ automáticamente ya que $(a_0, p) = 1$, de modo que existe una solución en $\mathbb{Z}_p$ por el Lema de Hensel.

$\Rightarrow$ Si a no es un residuo cuadrático por el Teorema 54 no tiene raíz cuadrada en $\mathbb{Z}_p$. □

Por ejemplo $\sqrt{-1}$ en $\mathbb{Z}_5$ ya que $-1 = 4 - 5 \equiv 2^2 \,(mod\, 5)$ es un residuo cuadrático módulo 5. Mientras que $\sqrt{-1}$ en $\mathbb{Z}_3$, como $-1 = 2 - 3$ no es un residuo cuadrático módulo 3.

Se termina con un caso particular sobre la existencia de raíces de la unidad

Teorema 56. *El cuerpo $\mathbb{Q}_p$ contiene una raíz de la unidad de orden $p-1$*

Demostración. Considérese un entero c no divisible por p. La sucesión $\left\{c^{p^n}\right\}$ converge en $\mathbb{Z}_p$ pues

$$c^{p^{n+1}} - c^{p^n} = c^{p^n}\left(c^{(p-1)p^n} - 1\right) = c^{p^n}\left(c^{\phi\left(p^{n+1}\right)} - 1\right)$$

y $p^{n+1} \mid c^{\phi\left(p^{n+1}\right)} - 1$. Esto prueba que $c^{p^{n+1}} - c^{p^n}$ tiende a 0. Luego c^{p^n}es de Cauchy y por lo tanto convergente a un número $\zeta \in \mathbb{Z}_p$. Ahora bien, en realidad se ha probado que $c^{(p-1)p^n} - 1$ tiende a 0, y por otra parte esa sucesión converge a $\zeta^{p-1} - 1$, es decir, $\zeta^{p-1} = 1$.

Así mismo $c^{p^n} - c$ converge a $\zeta - c$ y $p \mid c^{p^n} - c$, o sea $v_p\left(c^{p^n} - c\right) \geq 1$. Por continuidad $v_p\left(\zeta - c\right) \geq 1$, o sea $\zeta \equiv c \,(mod\, p)$. Se ha probado que si $1 \leq c \leq p-1$ existe un $\zeta \in \mathbb{Z}_p$ tal que $\zeta^{p-1} = 1$ y $\zeta \equiv c \,(mod\, p)$. Por lo tanto hay al menos $p-1$ raíces $p-1$-ésimas de la unidad en $\mathbb{Z}_p$, luego tiene que haber raíces primitivas. □

3.3. Topología en $\mathbb{Q}_p$

El campo de los números p-ádicos es análogo en muchos aspectos al campo de los números reales: Se trata de un campo con una norma, que es completo respecto a la métrica dada como se mostró en la Proposición 41. Tanto $\mathbb{R}$ como $\mathbb{Q}_p$ son completaciones de $\mathbb{Q}$, donde los dos contienen a $\mathbb{Q}$ como subconjunto denso, y por lo tanto son separables.

Se verán primero algunas nociones y teoremas básicos que se mantienen tanto para $\mathbb{R}$ como para $\mathbb{Q}_p$ ya que ambos son espacios métricos.

Una bola abierta en $\mathbb{R}$ es un intervalo abierto $B\left(a, r\right) = |x - a| < r$. Los intervalos abiertos forman una base de la Topología inducida en $\mathbb{R}$.

En $\mathbb{Q}_p$ las bolas abiertas son los conjuntos

$$B\left(a, r\right) = \left\{ x \in \mathbb{Q}_p \mid \left\| x - a \right\|_p < r \right\}$$

y puesto que la norma p-ádica tiene un conjunto discreto de valores, es decir, $\{0,\, p^n \mid n \in \mathbb{Z}\}$. Considerando las bolas de radio $r = p^n$ donde $n \in \mathbb{Z}$.

Sea la esfera en $\mathbb{Q}_p$

$$S(a,r) = \left\{ x \in \mathbb{Q}_p \mid \| x-a\|_p = r \right\}$$

Proposición 57. *La esfera $S(a,r)$ es un conjunto abierto en $\mathbb{Q}_p$*

Demostración. Sea $x \in S(a,r)$ con $\varepsilon < r$, se mostrará que $B(x,\varepsilon) \subset S(a,r)$. Sea $y \in B(x,\varepsilon)$ entonces por la propiedad no-arquimediana se tiene que

$$\|x-y\|_p \leq max \left\{ \|x-a\|_p, \|y-a\|_p \right\} < r$$

así que $y \in B(a,r)$ lo que se deseaba. □

Esto no sucede en $\mathbb{R}^n$ en particular en $\mathbb{R}$ ya que las esferas no son abiertas.

Proposición 58. *Las bolas en $\mathbb{Q}_p$ son abiertas y cerradas*

Demostración. La bola $B(a,r)$ es siempre un conjunto abierto en cualquier espacio métrico, ya que algún $x \in B(a,r)$ está en $B(a,r)$ que esta contenido en $B(a,r)$. Con el fin de probar que $B(a,r)$ es cerrada en $\mathbb{Q}_p$, vamos a demostrar que su complemento

$$C = \left\{ x \in \mathbb{Q}_p \mid \|x-a\|_p \geq r \right\}$$

es abierto. Pero $C = S(a,r) \cup D$ donde $D = \left\{ x \in \mathbb{Q}_p \mid \| x-a\|_p > r \right\}$.

Como $x \in S(a,r)$ es abierto, resta probar que el conjunto D es abierto (esto es cierto para todo espacio métrico). Para ver esto sea $y \in D$ entonces $\| y-a\|_p = r_1 > r$. Se afirma que la bola abierta $B(y,\, r_1 - r)$ esta contenida en D. De hecho, si no fuera así, entonces habría un $x \in B(y,\, r_1 - r)$ tal que $\| x-a\|_p \leq r$. Pero

$$r_1 = \| y-a\|_p = \| a-x+x-y\|_p \leq \| a-x\|_p + \| x-y\|_p < r + r_1 - r = r_1$$

que es una contradicción. Además como la unión de dos abiertos es abierto, se concluye la demostración. □

Ahora note que un punto $x \in M$ es un punto frontera de un conjunto $A \subset M$, si alguna bola abierta centrada en x contiene puntos de A y de su complemento, y un conjunto A es cerrado si y solo si contiene todos sus puntos frontera. Se deduce de

la definición que $S(a,r)$ no es frontera de la bola abierta $B(a,r)$. La Proposición 58 implica inmediatamente que $B(a,r)$ no tiene frontera. Y, por supuesto, la bola cerrada.

$$\overline{B(a\,,\,p^n)} = \{x \in \mathbb{Q}_p \mid \| x-a \| \leq p^n\}$$

$$= \left\{x \in \mathbb{Q}_p \mid \| x-a \| < p^{n+1}\right\} = B\left(a\,,\,p^{n+1}\right)$$

no es la clausura de la bola abierta $B(a\,,\,p^n)$. Se deduce entonces que todas las afirmaciones que se demostraron anteriormente para bolas abiertas se mantienen para las bolas cerradas en $\mathbb{Q}_p$.

A continuación se muestran las propiedades que se cumplen para las bolas en $\mathbb{Q}_p$, algunas pueden resultar un tanto extrañas como la siguiente proposición.

Proposición 59. *Si $b \in B(a,r)$, entonces $B(b,r) = B(a,r)$, en otras palabras, todo punto de la bola es un centro.*

Demostración. Sea $x \in B(b,r)$. A continuación, supóngase que

$$\| a-b \|_p < r, \quad \| b-x \|_p < r$$

y por la desigualdad del triangular

$$\| a-x \|_p = \| (a-b)+(b-x) \|_p \leq max\left(\|(a-b)\|_p, \|(b-x)\|_p\right) < r$$

por lo tanto $B(b,r) \subset B(a,r)$. Puesto que la condición $\| a-b \|_p < r$ para b que se encuentran en $B(a,r)$ es idéntica que para un a que esta en $B(b,r)$, entonces se tiene que $B(a,r) \subset B(b,r)$. Probando que las dos bolas coinciden. □

Se sigue con una propiedad adicional de bolas en $\mathbb{Q}_p$.

Proposición 60. *Cualesquiera dos bolas abiertas son disyuntas o están contenidas una en la otra, es decir,*

$$B(a,r) \cap B(b,s) \neq \emptyset \Longleftrightarrow B(a,r) \subset B(b,s) \;\; \acute{o}\; B(a,r) \supset B(b,s)$$

Demostración. Supóngase que $r \leq s$, y $y \in B(a,r) \cap B(b,s)$. Luego por la Proposición 59, se tiene que $B(a,r) = B(y,r)$ y $B(b,s) = B(y,s)$. Pero como $r \leq s$ entonces $B(y,r) \subset B(y,s)$, y se sigue la inclusión requerida $B(a,r) \subset B(b,s)$. Análogamente se prueba la otra contenencia. □

El conjunto de todas las bolas en $\mathbb{R}$ no es numerable ya que el conjunto de todos los números reales positivos no es contable (Teorema de Cantor), este resultado es completamente diferente para el conjunto de todas las bolas en $\mathbb{Q}_p$

Proposición 61. *El conjunto de todas las bolas en $\mathbb{Q}_p$ es contable.*

Demostración. Escribiendo el centro de la bola $B(a, p^{-s})$ en su forma canónica

$$a = \sum_{n=-m}^{\infty} a_n p^n$$

y sea

$$a_0 = \sum_{n=-m}^{s} a_n p^n$$

claramente, a_0 es un número racional, y $\| a - a_0 \|_p < p^{-s}$, es decir, $a_0 \in B(a, p^{-s})$. Entonces por la proposición 59

$$B\left(a_0, p^{-s}\right) = B\left(a, p^{-s}\right)$$

Aquí tanto los centros y las radios vienen de conjuntos numerables. Por consiguiente el conjunto de productos de todos los pares (a_0, s) es contable y también lo es el conjunto de todos bolas en $\mathbb{Q}_p$. □

Definición 62. Un conjunto K en un espacio métrico es llamado compacto por sucesiones o secuencialmente compacto si cada sucesión infinita de puntos en K contiene una subsucesión convergente a un punto en K.

Según Teorema de $Heine - Borel$, para espacios métricos esta propiedad es equivalente a la compacidad. (Cabe recordar que un conjunto K se llama compacto si todo recubrimiento abierto de K contiene un subrecubrimiento finito.). Ya se ha enunciado en el Teorema 50 que $\mathbb{Z}_p$ es secuencialmente compacto, por lo tanto $\mathbb{Z}_p$ es compacto, y también lo es cualquier bola en $\mathbb{Q}_p$.

El campo $\mathbb{R}$ es localmente compacto, es decir, cada punto esta contenido en un entorno compacto y también lo es $\mathbb{Q}_p$ como se vera a continuación.

Teorema 63. *El espacio $\mathbb{Q}_p$ es localmente compacto*

Demostración. Sean

$$\mathbb{Z}_p = \left\{ x \in \mathbb{Q}_p \mid \| x \|_p \leq 1 \right\} = \left\{ x \in \mathbb{Q}_p \mid \| x \|_p < p \right\}$$

es a la vez cerrado y abierto, $\mathbb{Z}_p$ es entorno compacto de 0. Dado que $\mathbb{Z}_p$ es una vecindad de cero, demostrando que es compacto es suficiente para probar que $\mathbb{Q}_p$ es localmente compacto. Las clases laterales en $\mathbb{Z}_p$ también son bolas en la topología p-ádica. Entonces

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

Se sigue fácilmente que para $a \in \mathbb{Q}_p$ la clase lateral $a + \mathbb{Z}_p$ es una vecindad compacta para a. □

La siguiente proposición puede parecer un tanto extraña, por que hasta ahora solo se ha hablado de la completitud de $\mathbb{Q}_p$. Otro conjunto que cumple esta importante propiedad es $\mathbb{Z}_p$ ya que hay sucesiones de Cauchy dentro de él que convergen en él.

Proposición 64. *El espacio $\mathbb{Z}_p$ es completo*

Demostración. Dado que cualquier sucesión de Cauchy en $\mathbb{Z}_p$ contiene una subsucesión convergente a un elemento en $\mathbb{Z}_p$, sea a, la sucesión en sí debe converger a a. Esto prueba la completitud de $\mathbb{Z}_p$ □

Como se mostró la contenencia $\mathbb{Z} \subset \mathbb{Z}_p$ en la Sección 1.3; a continuación una propiedad que hace esta relación mas fuerte.

Teorema 65. *El conjunto $\mathbb{Z}$ es denso en $\mathbb{Z}_p$*

Demostración. Sea $x = \ldots a_2 a_1 a_0 \in \mathbb{Z}_p$. Para cada $n \in \mathbb{N}$, tome

$$x_n = \ldots 00 a_n a_{n-1} \ldots a_0 = \sum_{i=0}^{n} a_i p^i$$

entonces $x_n \in \mathbb{Z}$ y $\| x - x_n \|_p < p^{-n}$, lo que se deseaba. □

Definición 66. Un espacio topológico X es llamado $cero - dimensional$ si para algún $a \in X$ y cualquier vecindad U de a (es decir, una bola centrada en a), hay un conjunto V, $a \in V \subset U$ que es a la vez abierto y cerrado.

La siguiente definición muestra otra diferencia entre $\mathbb{R}$ y $\mathbb{Q}_p$.

Definición 67. En espacio topológico X es llamado *disconexo* si se puede encontrar dos conjuntos abiertos no vacíos U y V de X tal que, $X = (X \cap U) \cup (X \cap V)$ donde

ni $X \cap U$ ni $X \cap V$ son vacíos. Un conjunto X que no puede ser descompuesto de esta manera se llama *conexo*. Un conjunto X se llama *totalmente disconexo* si los únicos subconjuntos conexos de X son el conjunto vacío y los puntos $\{a\}$, $a \in X$.

Cualquier intervalo en $\mathbb{R}$ es conexo, es decir, no se puede descomponer en una unión disjunta de dos conjuntos no vacíos los cuales son abiertos y cerrados. El siguiente teorema muestra lo que sucede en el caso p-ádico.

Teorema 68. *La topología en $\mathbb{Q}_p$ es cero-dimensional y $\mathbb{Q}_p$ es totalmente disconexo.*

Demostración. Para cada $a \in \mathbb{Q}_p$ y cada $n \in \mathbb{N}$ el conjunto

$$U_n(a) = \left\{ x \in \mathbb{Q}_p \mid \| x - a \|_p \leq p^{-n} \right\} = \left\{ x \in \mathbb{Q}_p \mid \| x - a \|_p < p^{-n+1} \right\}$$

es un entorno abierto y cerrado de a. De ahí que en su topología del espacio $a \in \mathbb{Q}_p$ es cero-dimensional.

Supóngase que $a \in A$ de modo que $A \neq \{a\}$. Entonces existe un $n \in \mathbb{N}$ tal que $U_n(a) \cap A \neq A$. Por consiguiente

$$A = (U_n(a) \cap A) \cup (\mathbb{Q}_p - U_n(a) \cap A)$$

donde ambos $U_n(a)$ y su complemento $\mathbb{Q}_p - U_n(a)$ son abiertos y no vacíos; esto implica que A es disconexo. Luego $\mathbb{Q}_p$ es totalmente disconexo. □

3.4. El conjunto de Cantor

Sea

$$\mathcal{C}_0 = [0,1], \ \mathcal{C}_1 = \left[0, \frac{1}{3}\right] \cup \left[\frac{2}{3}, 1\right], \ \mathcal{C}_2 = \left[0, \frac{1}{9}\right] \cup \left[\frac{2}{9}, \frac{1}{3}\right] \cup \left[\frac{2}{3}, \frac{7}{9}\right] \cup \left[\frac{8}{9}, 1\right] \ \ldots$$

En general, $\mathcal{C}_{k+1}$ se construye dividiendo en tres partes iguales a los intervalos que componen a $\mathcal{C}_k$ y borrando los intervalos abiertos intermedios. $\mathcal{C}_k$ es la unión de 2^k intervalos cerrados, cada uno de longitud 3^{-k} y $\mathcal{C}_0 \supset \mathcal{C}_1 \supset \mathcal{C}_2 \supset \ldots$ Cada $\mathcal{C}_k$ es cerrado, entonces

$$\mathcal{C} = \bigcap_{n=0}^{\infty} \mathcal{C}_n \neq \emptyset$$

es un subconjunto cerrado del intervalo $[0,1]$.

Representando los números reales en el intervalo $[0,1]$ como fracciones infinitas en base 3. Tomando el caso análogo a $\mathbb{R}$ en base 3 se tiene que $0.2222222 = 1$, y esto juega un papel esencial en la caracterización de uno de los fractales más conocidos: el conjunto de Cantor. El $n-ésimo$ dígito de la representación refleja la posición del punto en la $n-ésima$ etapa de la construcción. Por ejemplo, el punto $\frac{2}{3}$ se da con la representación usual de 0.2 o 0.20000, dado que está a la derecha de la primera etapa y a la izquierda de toda etapa de construcción posterior. El punto $\frac{1}{3}$ se representa no como 0.1 sino como $0.0222...$, pues está a la izquierda de la primera etapa y a la derecha de toda etapa de construcción posterior.

Todos los puntos de $[0,1]$ expresados por una expansión de la base 3 que contienen solo los dígitos 0 y 2 pertenece a la intersección de los conjuntos $\mathcal{C}_n$: si el primer dígito es 0, pertenece a $[0, 0.02222]$, si el primer dígito es 2, pertenece a $[0.2, 0.2222]$, el segundo dígito determina si pertenece a la izquierda (0) o derecha (2) del intervalo de $\mathcal{C}_2$, etc. Se puede resumir la discusión anterior de la siguiente manera.

Proposición 69. *El conjunto de cantor $\mathcal{C}$ consiste en todos los puntos de $[0,1]$ que pueden ser representados en base 3 por los dígitos 0 y 2*

El conjunto de Cantor presenta un modelo geométrico para los enteros p-ádico para cualquier primo p.

Teorema 70. *El conjunto de enteros diádicos $\mathbb{Z}_2$ es homeomorfo al conjunto de Cantor.*

Demostración. Sea $I = [0,1]$. Considere la siguiente función

$$\psi : \sum_{i=0}^{\infty} a_i 2^i \to \sum_{i=0}^{\infty} \frac{2a_i}{3^{i+1}}$$

Se va a demostrar que ψ es un homeomorfismo. En primer lugar, se observa que, por la unicidad de la representación tanto en $\mathbb{Z}_2$ y $\mathcal{C}$, ψ es una biyección.

Si $\|x_1 - x_2\| < \frac{1}{3^N}$, entonces x_1 y x_2 pertenecen al mismo intervalo o al adyacente en la partición de I en subintervalos de longitud $\frac{1}{3^N}$, pero como los intervalos cerrados que comprenden $\mathcal{C}_N$ no tienen puntos finales comunes, x_1 y x_2 pertenecen a la misma componente I_N de $\mathcal{C}_N$ y por lo tanto sus primeras cifras de N coinciden.

Recíprocamente, si los N primeros dígitos de $x_1, x_2 \in \mathcal{C}$ coinciden, pertenecen a la misma componente $I_N \subset \mathcal{C}_N$. Por otro lado, los N primeros dígitos de dos números $2-$ádicos y_1 y y_2 coinciden si y solo si $\|y_1 - y_2\|_2 < \frac{1}{2^N}$. Dado que tanto $\frac{1}{2^N}$ como $\frac{1}{3^N}$ tienden a 0 cuando $N \to \infty$, se concluye que ψ y ψ^{-1} son continuas. □

Corolario 71. *El conjunto de Cantor $\mathcal{C}$ es totalmente disconexo*

Demostración. Se sigue del Teorema 68 que $\mathbb{Z}_2$ es totalmente disconexo. Por tanto lo es también $\mathcal{C}$ ya que son homeomorfos □

Como consecuencia de este corolario se puede notar que el conjunto de Cantor no contiene ningún intervalo de conjuntos cerrados esto equivale a no ser denso. Esta propiedad topológica del conjunto de Cantor cuya demostración se encuentra en los libros básicos de topología.

Por otra parte, los espacios $\mathbb{Z}_p$ y $\mathbb{Z}_2$ son homeomorfos para cualquier primo p. Esta demostración, usa lemas propios del conjunto de Cantor que no se tratarán en este trabajo. Esta prueba se pueden encontrar en la referencia bibliográfica [7].

4. Análisis p-ádico básico

Como ya se ha reiterado, el campo de los números p-ádicos es análogo al campo de los números reales: De hecho, como se mencionó anteriormente, $\mathbb{R}$ y $\mathbb{Q}_p$ son terminaciones de $\mathbb{Q}$, por lo tanto contienen a $\mathbb{Q}$ como un subconjunto denso. Así mismo $\mathbb{Q}_p$ es locamente compacto y $\mathbb{R}$ también lo es; y ninguno de ellos es algebraicamente cerrado.

Estas similitudes sugieren que gran parte de lo que se suele hacer en $\mathbb{R}$ se puede extender a $\mathbb{Q}_p$. El objetivo de esta sección es examinar que forma toman las ideas del análisis real en el contexto p-ádico. Aunque existen ciertas diferencias notables, para empezar, $\mathbb{R}$ es un campo ordenado: hay una idea bien definida de « mas grande » que es bien compatible con las operaciones. Esto no es cierto para $\mathbb{Q}_p$ como mostró en la sección 3.1. Además $\mathbb{R}$ cumple la propiedad Arquimediana, mas precisamente el valor absoluto, a diferencia de $\mathbb{Q}_p$ donde la norma es no-arquimediana. Mas aún, $\mathbb{R}$ es conexo, mientras que $\mathbb{Q}_p$ es totalmente disconexo como se probó en el teorema 68 . Esto significa, por ejemplo, que no hay una idea clara de un intervalo en $\mathbb{Q}_p$ o cualquiera análogo a la noción de una curva. Son estos contrastes los que harán la diferencia entre el análisis real y el p-ádico.

En esta sección se mostrará el análisis p-ádico incluyendo conceptos tales como convergencia, sucesiones, series y otros tópicos conocidos en el análisis real pero ahora en el contexto de los números p-ádicos con la norma establecida para este conjunto.

4.1. Sucesiones y series

Se comenzará estudiando las propiedades de convergencia básicas de sucesiones y series. El hecho más importante, ya mencionado, es que $\mathbb{Q}_p$ es un campo completo, de modo de cada sucesión de Cauchy es convergente. Además todos los axiomas que se tiene para el valor absoluto en $\mathbb{R}$ siguen siendo validos para $\mathbb{Q}_p$. Por lo tanto, la mayoría de los teoremas básicos en el contexto p-ádico mantienen las pruebas algo similares. Además el hecho de que se tiene la propiedad no-arquimediana, introduce ciertas diferencias respecto al caso real. Quizás la más importante de tales diferencias es el hecho de que en un contexto no-arquimediano es más fácil comprobar la propiedad de Cauchy.

Teorema 72. *Una sucesión (a_n) en $\mathbb{Q}_p$ es una sucesión de Cauchy, y por lo tanto convergente, si y solo si satisface*

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

Demostración. Este es el Teorema 31 que fue definido para $\mathbb{Q}$ usando la norma p-ádica, pero cuya prueba claramente solo utiliza el hecho de que es no-arquimediana, y por lo tanto funciona igual para las sucesiones en $\mathbb{Q}_p$ □

La teoría de las sucesiones y sus propiedades de convergencia es casi idéntica a la teoría sobre $\mathbb{R}$ excepto por el Teorema 72.

Además considérese una serie $\sum_{i=1}^{\infty} a_i$ en $\mathbb{Q}_p$, se dice que esta serie *converge* si la sucesión de sus sumas parciales $S_n = \sum_{i=1}^{n} a_i$ converge en $\mathbb{Q}_p$ y *converge absolutamente* si $\sum_{i=1}^{\infty} \| a_i\|_p$ converge (en $\mathbb{R}$).

Ejemplo 73. Tomando la sucesión cuyo n-ésimo termino es $a_n = 1+p+p^2+\ldots+p^{n-1}$ entonces se tiene

$$\| a_{n+k} - a_n\|_p = \left\| p^n + p^{n+1} + \ldots p^{n+k-1} \right\|_p$$

$$\left\| p^n \left(1 + p^n + \ldots + p^{k-1}\right) \right\|_p = \frac{1}{p^n}$$

Para cada $\varepsilon > 0$ se puede seleccionar un m tal que $p^m \geq \frac{1}{\varepsilon}$ de este modo si $n > M$ se tiene que $\| a_{n+k} - a_n\|_p < \frac{1}{p^m} \leq \varepsilon$ por lo tanto (a_n) es una sucesión de Cauchy y por lo tanto convergente al número $a = \frac{1}{1-p} \in \mathbb{Q}$ por tanto

$$\lim_{n\to\infty} \left(1 + p + p^2 + \ldots + p^{n-1}\right) = \frac{1}{1-p}$$

claramente esta sucesión no converge en $\mathbb{R}$.

Ahora se calculará otro límite en $\mathbb{Q}_p$.

Ejemplo 74. Hallar $\lim_{n\to+\infty} 2^{3^n}$ en $\mathbb{Q}_3$

Usando la función de Euler se tiene que $\Phi\left(3^{n+1}\right) = 3^{n+1} - 3^n = 3^n.2$ por el teorema de Euler como $(2, 3^{n+1}) = 1$ entonces $2^{\Phi\left(3^{n+1}\right)} \equiv 1 \left(mod\, 3^{n+1}\right)$ por lo tanto

$$2^{3^n.2} \equiv 1 \left(mod\, 3^{n+1}\right)$$

de ahí que

$\left(2^{3^n}\right)^2 - 1 \equiv 0\,(mod\,3^{n+1})$ por diferencia de cuadrados se tiene que

$$\left(2^{3^n}+1\right)\left(2^{3^n}-1\right) \equiv 0\left(mod\,3^{n+1}\right)$$

Luego como $\left(3^{n+1}, 2^{3^n}-1\right) = 1$ en efecto $2^k \equiv 1\,(mod\,3)$ si k es par y $2^k \equiv 2\,(mod\,3)$ si k es impar. Por tanto $2^{3^n}+1 \equiv 0\,(mod\,3^{n+1})$ además

$$\left\|2^{3^n}+1\right\|_p = \left\|\,k.\,3^{n+1}\right\| \leq \left\|3^{n+1}\right\|_p$$

de ahí que

$$\left\|2^{3^n}+1\right\|_3 \leq \left\|3^{n+1}\right\|_p = \frac{1}{3^{n+1}}$$

finalmente $\frac{1}{3^{n+1}} \to 0$ cuando $n \to \infty$ por lo tanto $\lim\limits_{n\to\infty} 2^{3^n}+1 = 0$ en $\mathbb{Q}_3$ es decir, $\lim\limits_{n\to\infty} 2^{3^n} = -1$ en $\mathbb{Q}_3$

Proposición 75. *Si la serie $\sum \|\,a_i\|_p$ converge en $\mathbb{R}$, entonces $\sum a_i$ converge en $\mathbb{Q}_p$*

Demostración. Sea $\sum \|\,a_i\|_p$ convergente, por tanto es una sucesión de Cauchy, es decir, para algún $\varepsilon > 0$ existe un entero N tal que para todo n, m con $m > n > N$ entonces

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

Por la desigualdad triangular

$$\|\,S_m - S_N\|_p = \left\|\sum_{i=n+1}^{m} a_i\right\|_p \leq \sum_{i=n+1}^{m} \|\,a_i\|_p < \varepsilon$$

lo que implica que (S_n) es de Cauchy y así la serie $\sum a_i$ converge en $\mathbb{Q}_p$. □

En análisis real existen series que convergen, pero no convergen absolutamente, por ejemplo la serie $\sum\limits_{n=1}^{\infty} \frac{(-1)}{n}$ converge a $-ln\,(2)$, pero la serie armónica $\sum\limits_{n=1}^{\infty} \frac{1}{n}$ diverge. El siguiente resultado muestra que esto no puede suceder en $\mathbb{Q}_p$.

Como se espera algo mejor en $\mathbb{Q}_p$, de hecho, el siguiente resultado es una consecuencia de el Teorema 72 y permite identificar cuando una serie es convergente.

Teorema 76. *Una serie $\sum\limits_{n=1}^{\infty} a_n$ con $a_n \in \mathbb{Q}_p$ converge en $\mathbb{Q}_p$ si y solo si $\lim\limits_{n\to\infty} a_n = 0$,*

en ese caso

$$\left\| \sum_{n=1}^{\infty} a_n \right\|_p \leq \max_n \| a_n \|_p$$

Demostración. La serie converge si y solo si la sucesión de sumas parciales $S_n = \sum_{i=1}^{n} a_i$ converge. Pero $a_n = S_{n+1} - S_n$. Del Teorema 72 se deduce que a_n tiende a 0 si y solo si la serie converge. Ahora supóngase que $\sum_{n=1}^{\infty} a_n$ converge. Si $\sum_{n=1}^{\infty} a_n = 0$ no hay nada que demostrar. Si no, ya que $a_n \to 0$ se tiene que existe un entero N tal que

$$\left\| \sum_{n=1}^{\infty} a_n \right\|_p = \left\| \sum_{n=1}^{N} a_n \right\|_p$$

y

$$max \left\{ \| a_n \|_p : 1 \leq n \leq N \right\} = \max_n \| a_n \|_p$$

por la desigualdad triangular

$$\left\| \sum_{n=1}^{N} a_n \right\|_p \leq max \left\{ \| a_n \|_p : 1 \leq n \leq N \right\} = \max_n \| a_n \|_p$$

lo que completa la prueba. □

Así para verificar que la serie en $\mathbb{Q}_p$ converge es suficiente verificar que $\lim_{n\to\infty} a_n = 0$. Esto significa que la convergencia de las series en $\mathbb{Q}_p$ es más fácil de manejar que la convergencia en los reales o complejos. Esta proposición es falsa en $\mathbb{R}$. El ejemplo mas obvio de una serie en $\mathbb{R}$ cuyo término general tiende a 0 , pero que no es convergente es la serie armónica $\sum \frac{1}{n}$.

Definición 77. Una serie $\sum_{n=1}^{\infty} a_n$ converge *incondicionalmete* si para cualquier reordenamiento de los términos $a_n \to a'_n$ la serie $\sum_{n=0}^{\infty} a'_n$ también converge.

Obviamente, la convergencia incondicional implica convergencia ordinaria. En $\mathbb{Q}_p$, sin embargo, lo contrario también es cierto.

Teorema 78. *Si* $\sum_{n=1}^{\infty} a_n$ *converge en* $\mathbb{Q}_p$ *entonces converge incondicionalmente, y la suma no depende del reordenamiento.*

Demostración. Sea ε un número real arbitrario y N un número entero tal que para cualquier $n > N$ se tiene $\| a_n \|_p < \varepsilon$, $\| a'_n \|_p < \varepsilon$ y

$$\left\| \sum_{n=1}^{\infty} a_n - \sum_{n=1}^{N} a_n \right\|_p < \varepsilon \quad (1)$$

Sea $S = \sum_{n=1}^{N} a_n$ y $S' = \sum_{n=1}^{N} a'_n$ y denote por S_1 la suma de todos los términos de S para los que $\| a_n \|_p > \varepsilon$, y por S'_1 la suma de todos los términos de S' para los que $\| a'_n \|_p > \varepsilon$. Es claro que S_1 y S'_1 tienen los mismos términos por lo tanto $S_1 = S'_1$. La suma S difiere de S_1 por los términos que satisfacen que $\| a_n \|_p < \varepsilon$, y S' de S'_1 por los términos que satisfacen $\| a'_n \|_p < \varepsilon$. Por lo tanto $\| S - S_1 \| < \varepsilon$ y $\| S' - S'_1 \| < \varepsilon$, de modo que $\| S - S' \| < \varepsilon$. Combinando esto con (1), se obtiene

$$\left\| \sum_{n=1}^{\infty} a_n - \sum_{n=1}^{N} a'_n \right\|_p < \varepsilon$$

tomando $\varepsilon \to 0$ y $N \to \infty$, se puede notar que la serie $\sum_{n=1}^{\infty} a'_n$ converge y

$$\sum_{n=1}^{\infty} a_n = \sum_{n=1}^{\infty} a'_n$$

□

Esto difiere del resultado del análisis real, donde reordenar los términos de una serie puede cambiar su convergencia o su suma; una condición necesaria y suficiente para que una serie convergente siga siéndolo y tenga la misma suma, después de sufrir una permutación de términos es la condición de convergencia absoluta. El teorema 78 es aún mas sorprendente porque, al igual que en el caso real, el siguiente resultado se mantiene.

Teorema 79. *Existe una serie* $\sum_{n=1}^{\infty} a_n$ *en* $\mathbb{Q}_p$ *que converge pero no converge absolutamente.*

Demostración. Considere los siguientes términos consecutivos de la serie: 1; p repetido p veces; p^2 repetido p^2 veces; etc. Estos terminos tienden a 0, por lo tanto, la serie es convergente. Sin embargo

$$\sum_{n=1}^{\infty} \| a_n \|_p = 1 + p.p^{-1} + p^2.p^{-2} + \ldots = \infty$$

lo que se deseaba. □

4.2. Series de potencias p-ádicas

Una serie de potencias formal es una expresión de la forma

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

donde $a_n \in \mathbb{Q}_p$ y x es una variable. El conjunto de todas las series de potencia en x con coeficientes en el campo F se denota por $F[[\cdot]]$.

Dado $a_n \in \mathbb{Q}_p$, considerando la correspondiente serie de potencias numérica $f(x)$ por $f(x) = \sum_{n=0}^{\infty} a_n x^n$. Ya se sabe que converge si y solo si $\| a_n x^n \|_p \to 0$

Al igual que en el caso de Arquímediano (serie de potencia sobre $\mathbb{R}$), se define el radio de convergencia por

$$r = \frac{1}{lim\, sup \sqrt[n]{\| a_n \|_p}}$$

Cabe recordar que *lim sup* de una sucesión es el extremo superior de el conjunto de puntos de esta sucesión. Por lo tanto, en el caso $0 < r < \infty$, para algún $C > \frac{1}{r}$ solo hay un número finito de $\sqrt[n]{\| a_n \|_p}$ mayores que C.

A continuación se establece el conjunto de valores para los cuales la serie converge, a partir del radio de convergencia, como se tiene de manera habitual.

Proposición 80. *Supóngase que* $0 < r < \infty$ *entonces la serie* $\sum_{n=0}^{\infty} a_n x^n$ *converge si* $\|x\|_p < r$ *y diverge si* $\|x\|_p > r$.

Demostración. Primero, si $\|x\|_p < r$, sea $\|x\|_p = (1-\varepsilon) r$. Entonces

$$\| a_n x^n \|_p = \left(r \sqrt[n]{\| a_n \|_p} \right)^n (1-\varepsilon)^n$$

puesto que hay un número finito n para el cual

$$\sqrt[n]{\| a_n \|_p} > \frac{1}{r - \varepsilon \frac{r}{2}}$$

se tiene

$$\lim_{n\to\infty} \| a_n x^n \|_p \leq lim \left(\frac{(1+\varepsilon) r}{\left(1 - \frac{1}{2}\varepsilon\right) r} \right)^n = \lim_{n\to\infty} \left(\frac{1-\varepsilon}{1 - \frac{1}{2}\varepsilon} \right)^n = 0$$

Del mismo modo, si $\|x\|_p > r$, escribiendo $\|x\|_p = (1+\varepsilon)\, r$. Entonces

$$\| a_n x^n \|_p = \left(r \sqrt[n]{\| a_n \|_p} \right)^n (1+\varepsilon)^n$$

ya que hay un número infinito n para el cual

$$\sqrt[n]{\| a_n \|_p} > \frac{1}{r + \varepsilon \frac{r}{2}}$$

entonces

$$\underset{n\to\infty}{lim\, sup} \| a_n x^n \|_p \geq lim \left(\frac{(1+\varepsilon)\, r}{\left(1+\frac{1}{2}\varepsilon\right) r} \right)^n = \underset{n\to\infty}{lim} \left(\frac{1+\varepsilon}{1+\frac{1}{2}\varepsilon} \right)^n \neq 0$$

□

¿Qué sucede con el límite en $\| x \|_p = r$? En el caso Arquímediano ($\mathbb{R}$ o $\mathbb{C}$) el comportamiento en el límite del intervalo de convergencia puede ser bastante complicado. Por ejemplo, la serie de potencias logarítmica habitual $Log\,(1+x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n}$ tiene radio de convergencia 1. Si $|x| = 1$, en el caso que $x = -1$ diverge, y converge (no absolutamente) para $x = 1$.

En el caso no-Arquímediano, la respuesta es la misma para todos los puntos de $\|x\|_p = r$. Esto es debido a que la serie converge si y solo si $\| a_n x^n \|_p \to 0$ y esto depende solo de la norma $\|x\|_p$, no del valor específico de x.

Tomando el mismo ejemplo $\sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n}$ entonces $\| a_n \|_p = p^{v_p(n)}$ y como $v_p(n)$ es un entero positivo por lo tanto $p^{v_p(n)} \geq 1$ y de ahí que $\underset{n\to\infty}{lim} \sqrt[n]{\| a_n \|_p} = 1$

La serie converge para $\|x\|_p < 1$ y diverge para $\|x\|_p > 1$. Si $\|x\|_p = 1$, $\| a_n x^n \|_p = p^{v_p(n)} \geq 1$ por lo tanto, la serie diverge.

Lema 81. *Todo* $f(x) \in \mathbb{Z}_p [[x]]$ *converge en* $\left\{ x \in \mathbb{Q}_p \mid \|x\|_p < 1 \right\}$

Demostración. Sea $\|x\|_p < 1$ y $f(x) = \sum_{n=0}^{\infty} a_n x^n$. Dado que para cualquier $n \geq 0$ $\| a_n \|_p \leq 1$, se sigue que $\| a_n x^n \|_p \leq \| x \|_p^n \to 0$ cuando $n \to \infty$, así que la serie converge.

□

Sea $a \in \mathbb{Z}_p$ fijo, entonces

$$f_a(x) = \sum_{n=0}^{\infty} \binom{a}{n} x^n \in \mathbb{Z}_p[[x]]$$

donde

$$\binom{a}{n} = \frac{a(a-1)\dots(a-n+1)}{n!} \quad \text{y} \quad f_a(x) = (1+x)^a$$

Lema 82. *Si $a \in \mathbb{Z}_p$, $n \geq 0$, entonces $\binom{a}{n} \in \mathbb{Z}_p$*

Demostración. Para cada $n \geq 0$ considere

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

Como cualquier polinomio, P_n define una función continua $\mathbb{Q}_p \to \mathbb{Q}_p$. Si m, n son enteros positivos, $\binom{m}{n} \in \mathbb{N}$, entonces para $a \in \mathbb{N}$ se tiene

$$P_n(a) = \binom{a}{n} \in \mathbb{N}$$

Así la función P_n de $\mathbb{N} \to \mathbb{N}$ es continua. Por continuidad, se asigna la clausura de $\mathbb{N}$ en la clausura de $\mathbb{N}$. Se ha visto en la demostración del Teorema 65 que $\mathbb{N}$ es denso en $\mathbb{Z}_p$; esto significa que $P_n : \mathbb{Z}_p \to \mathbb{Z}_p$ □

El siguiente resultado es similar a uno en el análisis real.

Lema 83. *Sea $f(x) = \sum a_n x^n$, $a_n \in \mathbb{Q}_p$ una serie p-ádica cuya región de convergencia es una bola abierta y cerrada $D \subset \mathbb{Q}_p$. Entonces $f : D \to \mathbb{Q}_p$ es una función continua en D.*

Demostración. Se mostrará que f es continua en cualquier $x \in D$, $x \neq 0$.

Sea $\|x - x'\|_p < \delta$, donde $\delta < \|x\|_p$ será elegido después. Entonces $\|x\|_p = \|x'\|_p$ por la propiedad del triángulo isósceles. Se tiene

$$\|f(x) - f(x')\|_p = \left\| \sum_{n=0}^{\infty} (a_n x^n - a_n x'^n) \right\|_p \leq \max_n \|a_n x^n - a_n x'^n\|_p$$

$$= \max_n \left(\| a_n \|_p \left\| (x - x') \left(x^{n-1} + x^{n-2}x' + \ldots + x'^{n-1} \right) \right\|_p \right)$$

pero

$$\left\| (x - x') \left(x^{n-1} + x^{n-2}x' + \ldots + x'^{n-1} \right) \right\|_p \leq \max_{1 \leq i \leq n} \left\| x^{n-i} x'^{i-1} \right\|_p = \|x\|_p^{n-1}$$

ya que $\|x\|_p = \| x'\|_p$. Por lo tanto

$$\| f(x) - f(x') \|_p \leq \max_n \left(\| x - x' \|_p \| a_n \|_p \|x\|_p^{n-1} \right) < \frac{\delta}{\|x\|_p} \max_n \left(\| a_n \|_p \|x\|_p^n \right)$$

Como $\| a_n x^n \|_p$ esta limitado cuando $n \to \infty$, se obtiene $\| f(x) - f(x') \|_p < \varepsilon$ para un adecuado δ.

Note que si $x = 0$; $f(x) = a_n x^n$, se tendrá radio de convergencia $r = 0$ y entonces $f(x)$ solo converge en $x = 0$. □

El siguiente resultado permite relacionar el radio convergencia de una serie de potencias y de su derivada, de la misma manera como se tiene en $\mathbb{R}$.

Proposición 84. *El radio de convergencia de la serie de potencias*

$$f(x) = \sum_{n=0}^{\infty} a_n x^n \in \mathbb{Q}_p [[x]]$$

y de su derivada formal

$$Df(x) = \sum_{n=0}^{\infty} n a_n x^{n-1}$$

son iguales, es decir, $r_f = r_{Df}$

Demostración. Para algún $n \in \mathbb{N}$ se tiene $\|n\|_p \leq 1$. Entonces

$$r_{Df} = \limsup_{n \to \infty} \| n a_n \|_p^{\frac{1}{n-1}} = \limsup_{n \to \infty} \| n a_n \|_p^{\frac{1}{n}} = r_{Df} = \limsup_{n \to \infty} \| a_n \|_p^{\frac{1}{n}} = r_f$$

□

El siguiente ejemplo muestra que el comportamiento de la serie de potencias y su derivada en el límite de la región de convergencia puede ser diferente. La serie de potencias $f(x) = \sum_{n=0}^{\infty} x^{p^n}$ tiene radio de convergencia igual a 1 y diverge para $\|x\|_p = 1$,

mientras que su derivada $Df(x) = \sum_{n=0}^{\infty} p^n x^{p^n-1}$ converge para $\|x\|_p = 1$, ya que la serie $\sum_{n=0}^{\infty} p^n$ converge.

4.3. Algunas funciones elementales

En esta sección, el objetivo es utilizar series de potencias de funciones p-ádicas que son análogas a las funciones clásicas. Comenzando con las versión p-ádica de las funciones exponencial y logarítmica. En contraste con el caso Arquímediano, el logaritmo posee mejores propiedades de convergencia.

Iniciando con la serie de potencias para el logaritmo. Sea la serie

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

Dado que sus coeficientes son números racionales, es un elemento de $\mathbb{Q}[[x]]$. Se ha visto que la serie de potencias correspondiente en $\mathbb{Q}_p$, que se denotará por $Ln_p(1+x)$ para no confundirlo con el logaritmo en base p , y llamado *logaritmo* $p-$*ádico*, este converge para $\|x\|_p < 1$, como se vio en el comentario posterior a la Proposición 80. El primer paso hacia la comprensión, por supuesto, es calcular su radio de convergencia. Antes de saltar en el cálculo límite, sin embargo, hay que señalar otro contraste. En el caso clásico, todos los números enteros en los denominadores ayudan a la convergencia, ya que tienden a hacer que los términos de las series sean más pequeños. En el caso de p-ádico, esto se invierte: números enteros en el denominador no cambian el valor absoluto (cuando no son divisibles por p) o hacerlo más grande (cuando es divisible por p). Lo que salva la convergencia en el caso de esta serie es que "en general" n no es demasiado divisible por p. Así $Ln_p(1+x)$ define una función en la bola abierta $B(0,1)$ de radio 1 y centro 0.

De igual manera, se define la serie

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

que converge para $x \in B$ con $B(1,1) = \left\{ x \in \mathbb{Z}_p \mid \|x-1\|_p < 1 \right\} = 1 + p\mathbb{Z}_p$.

El siguiente teorema muestra que las propiedades para logaritmos que ya se conocen en $\mathbb{R}$ se mantienen en el caso p-ádico.

Teorema 85. *El logaritmo p-ádico satisface la propiedad fundamental*

$$Ln_p(xy) = Ln_p(x) + Ln_p(y)$$

Demostración. Para algún $x \in p\mathbb{Z}_p$, sea

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

Entonces, derivando esta serie de potencias se tiene

$$f'(x) = \sum_{n=0}^{\infty} (-1)^n x^n = \frac{1}{1+x}$$

Ahora fijando $y \in p\mathbb{Z}_p$ y defina

$$g(x) = Ln_p((1+x)(1+y)) = f(y + (1+y)x)$$

esta serie de potencias converge siempre que $\|x\|_p < 1$. Ahora usando la regla de la cadena para derivadas para calcula g' entonces

$$g'(x) = (1+y) f'(y + (1+y)x) = \frac{(1+y)}{1+y+(1+y)x} = \frac{1}{1+x} = f'(x)$$

ya que $f(x)$ y $g(x)$ son definidas por series de potencias que convergen para $\|x\|_p < 1$, entonces $g(x) = f(x) + c$ con $x = 0$ se tiene que $c = g(0) = f(y)$. Por lo tanto se mostró que $g(x) = f(x) + f(y)$ de ahí que

$$Ln_p((1+x)(1+y)) = Ln_p(1+x) + Ln_p(1+y)$$

y se ha demostrado la afirmación. □

Ahora considérese la serie de potencias

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

converge para todo $x \in \mathbb{R}$ debido a que los coeficientes $\frac{1}{n!}$ tienden muy rápidamente a 0 con respecto al valor absoluto usual. En el contexto p-ádico, por supuesto, esto cambia

drásticamente, ya que $\frac{1}{n!}$ tiende a 0, de manera que $\frac{1}{n!}$ es arbitrariamente grande a medida que n crece. Esto significa que no se podrá esperar tener un gran radio de convergencia. Para determinar cuál será ese radio, hay que saber exactamente qué tan rápido crecen los coeficientes $\frac{1}{n!}$, es decir, saber que tanto $n!$ es divisible por p. La serie de potencias correspondiente en $\mathbb{Q}_p$ se llama *exponencial* $p-$*ádica* y se denota por $exp_p(x)$.

Teorema 86. *La exponencial p-ádica* $exp_p(x)$ *converge en el disco*

$$D_p = \left\{ x \in \mathbb{Q}_p \mid \|x\|_p < r_p \right\}$$

donde $r_p = p^{\frac{-1}{p-1}}$ *y diverge en caso contrario.*

Demostración. En primer lugar se va a encontrar el radio de convergencia r_p de esta serie de potencias usando la definición que se dio anteriormente. Sea $a_n = \frac{1}{n!}$ como $v_p(n!) = \frac{n-S_n}{p-1}$ donde S_n es la suma de dígitos de n escritos en la base p, (esto se puede ver usando el hecho de que $(p-1)\sum_{k=1}^{\infty} \left[\!\left[\frac{n}{p^k}\right]\!\right]$ es equivalente a $n - S_n$.)

Entonces

$$\left\| \frac{1}{n!} \right\|_p = p^{\frac{n-S_n}{p-1}}$$

y además

$$r_p = \frac{1}{lim\, sup\ \sqrt[n]{\| a_n \|_p}}$$

se obtiene (utilizando el hecho de que r_p es una potencia de p) la relación

$$v_p(r_p) = lim\, inf\, \frac{1}{n} v_p(a_n) = lim\, inf\, \left(-\frac{n-S_n}{n(p-1)} \right) = -\frac{1}{p-1}$$

la última igualdad es válida dado que

$$\lim_{n\to\infty} -\frac{n-S_n}{n} = -1 + \lim_{n\to\infty} \frac{S_n}{n} = -1$$

y por lo tanto $r_p = p^{-\frac{1}{p-1}}$.

Ahora se verá lo que sucede cuando $\|x\|_p = p^{\frac{-1}{p-1}}$, es decir, cuando $v_p(x) = \frac{1}{p-1}$. Se puede escribir

$$v_p(a_n x^n) = -\frac{n-S_n}{p-1} + \frac{n}{p-1} = \frac{S_n}{p-1}.$$

Si $n = p^m$, entonces $S_n = 1$ y $v_p\left(a_{p^m}x^{p^m}\right) = \frac{1}{p-1}$, por lo tanto se tiene

$$\lim_{n\to\infty} \| a_n x^n \|_p \neq 0 \text{ para } \|x\|_p = p^{\frac{-1}{p-1}}$$

por lo tanto la serie diverge para $\|x\|_p = p^{\frac{-1}{p-1}}$. □

Observación 87. Si $p = 2$, el radio de convergencia es igual a $\frac{1}{2}$, por lo que $Ln_2(x)$ converge en $4\mathbb{Z}_2$. Si $p > 2$, el radio de convergencia es igual a $p^{\frac{-1}{p-1}}$ y como , $\frac{1}{p} < p^{\frac{-1}{p-1}} < 1$, por lo tanto $Ln_p(x)$ converge en $p\mathbb{Z}_p$.

La siguiente proposición es la propiedad análoga a la que se tiene para la función exponencial en el caso real.

Proposición 88. *Se tiene que* $exp_p(x+y) = exp_p(x)\, exp_p(y)$ *si* $x, y \in D_p$, *la región de convergencia de la exponencial p-ádica.*

Demostración. Puesto que esto es cierto para las series formales, el resultado se sigue como en la demostración del Teorema 85. □

A continuación se establece la relación que existe entre las funciones *exponencial* $p-$*ádica* y *logaritmo* $p-$*ádico.*

Proposición 89. *Si* $x \in D_p = \left\{ \|x\|_p < p^{\frac{-1}{p-1}} \right\}$ *entonces* $\| exp_p(x) - 1 \|_p < 1$, *es decir,* $exp_p(x)$ *esta en el dominio de* $Ln_p(x)$ *y*

$$Ln_p(exp_p(x)) = x$$

Por otro lado, si $x \in D_p$

$$\| Ln_p(1+x) \|_p < p^{\frac{-1}{p-1}}$$

y

$$exp_p(Ln_p(1+x)) = 1 + x$$

Demostración. Las relaciones se derivan de las relaciones correspondientes para series formales, por tanto lo que se requiere es comprobar que todas las series involucradas convergen.

Si $x \in D_p$, entonces $exp_p(x)$ converge, y por el teorema 76

$$\| exp_p(x) - 1 \|_p \leq \max_n \left\| \frac{x^n}{n!} \right\|_p$$

como $v_p(n!) = \frac{n-S_n}{p-1}$ entonces

$$\left\| \frac{x^n}{n!} \right\|_p < p^{-\frac{n}{p-1}} p^{v_p(n!)} < p^{-\frac{n}{p-1}} p^{\frac{n}{p-1}} = 1.$$

Por lo tanto $\| exp_p(x) - 1\|_p < 1$. □

Para probar la segunda parte, se requiere una estimación para $v_p(n)$.

Lema 90. $v_p(n) - \frac{n}{p-1} \leq \frac{-1}{p-1}$

Demostración. Para $n = 1$ y $n = p$ se tiene la igualdad. Si $1 < n < p$, $v_p(n) = 0$ y se da la desigualdad estricta. Para $n > p$, se tiene la siguiente cota superior para $v_p(n)$ como $\lim_{n\to\infty} \sqrt[n]{p^{v_p(n)}} = 1$

$$v_p(n) \leq \frac{Logn}{Logp}$$

Entonces

$$\frac{n-1}{p-1} - v_p(n) \geq \frac{n-1}{p-1} - \frac{Logn}{Logp}$$

Sea

$$f(x) = \frac{x-1}{p-1} - \frac{Logx}{Logp}$$

Por tanto $f(p) = 0$ y $f'(x) > 0$ para $x > p$. Por lo tanto $f(x)$ es creciente, en particular, para $n > p$ entonces

$$\frac{n-1}{p-1} - \frac{Logn}{Logp} > 0$$

Usando esto y el hecho de que $\frac{n-1}{p-1} - v_p(n) \geq \frac{n-1}{p-1} - \frac{Logn}{Logp}$ se obtiene la desigualdad deseada. □

Continuando la demostración anterior, entonces para $x \in D_p$

$$\| Ln_p(1+x)\|_p \leq \max_n \left\| \frac{x^n}{n} \right\|_p$$

usando el lema anterior, se obtiene

$$\left\| \frac{x^n}{n} \right\|_p < p^{-\frac{n}{p-1}} p^{v_p(n)} \leq p^{-\frac{1}{p-1}}$$

luego $\| Ln_p(1+x)\|_p < p^{-\frac{1}{p-1}}$.

Ejemplo 91. Sea $p = 2$. Entonces $-1 \in \{ x \in \mathbb{Z}_2 \mid \| x - 1\|_2 < 1\}$.

Dado que $\|-1 - 1\|_2 = \frac{1}{2} < 1$. Por lo tanto el logaritmo $2-$*ádico* $Ln_2(-1)$ se puede calcular mediante el uso de series de potencias, es decir,

$$Ln_2(-1) = Ln_2(1-2) = -\left(2 + \frac{2^2}{2} + \frac{2^3}{3} + \ldots\right)$$

Por otro lado, se tiene

$$0 = Ln_2(1) = Ln_2(-1) + Ln_2(-1) = 2Ln_2(-1)$$

por tanto $Ln_2(-1) = 0$. Esto significa que cuando $n \to \infty$, la suma

$$2 + \frac{2^2}{2} + \frac{2^3}{3} + \ldots + \frac{2^n}{n}$$

se acerca en la norma $2-$*ádica* a 0, es decir, es divisible por altas potencias de 2. Más precisamente, para cualquier M existe un n tal que

$$2^M \left(2 + \frac{2^2}{2} + \frac{2^3}{3} + \ldots + \frac{2^n}{n}\right)$$

Con esto finalizan las ideas que se querían presentar sobre los números p-ádicos y análisis p-ádico donde se mostró la fuerte analogía entre $\mathbb{R}$ y $\mathbb{Q}_p$ en cuanto a su construcción, pero se enunciaron también las diferencias más relevantes sobre todo en la convergencia. Como bien se dijo al inicio, se pretendía hacer una introducción a este conjunto de números; cabe decir que este conjunto es mucho más amplio, hay otros temas que requieren su profundización, por mencionar algunos de ellos: La teoría de las funciones L-p-ádicas que es una forma de usar métodos p-ádicos para estudiar cuestiones aritméticas , además trabajar con más detalle el Lema de Hensel para resolver ecuaciones diofánticas, así como el estudio de las funciones p-ádicas donde se ven conceptos análogos al cálculo clásico como lo es continuidad, diferenciabilidad, etc; así mismo es posible hacer análisis funcional p-ádico en parte por analogía con la teoría clásica. Los números p-ádicos, además de servir como una buena lista de curiosidades topológicas y rarezas de análisis funcional, se les ha encontrado aplicaciones en ramas tan dispares como el procesamiento de imágenes, la teoría de códigos o la teoría de cuerdas.

Conclusiones

En este trabajo de mostraron dos maneras de definir el conjunto de los números p-ádicos, la primera basada en los desarrollos en base p de un entero, y la segunda haciendo una paridad con la construcción de conjunto de los números reales, bajo el concepto de una nueva norma para generar el conjunto $\mathbb{Q}_p$ como la completación de $\mathbb{Q}$. A partir de esta segunda definición, se establece el análisis p-ádico, donde se puede notar que aunque existen similitudes con el caso real, hay muchas diferencias importantes, por ejemplo, la convergencia es mucho más fácil de manejar en $\mathbb{Q}_p$ que en $\mathbb{R}$ debido a la definición que se toma para sucesiones de Cauchy, y por supuesto a la propiedad no-arquimediana que se cumple para esta nueva norma.

Existen otras propiedades topológicas un tanto extrañas en este conjunto de números y donde la diferencia entre $\mathbb{R}$ y $\mathbb{Q}_p$ se hace más evidente. Además hay características no tan buenas para este conjunto, como es el hecho de no ser ordenado, esto significa, por ejemplo, que no hay una idea clara de un intervalo en $\mathbb{Q}_p$ o cualquiera análogo a la noción de una curva. Por otra parte, el comportamiento en cuanto a algunas funciones elementales varía, ya que en particular, la función exponencial en $\mathbb{R}$ tiene un buen comportamiento; mientras que en el caso p-ádico no ocurre los mismo, pues esta función queda definida en la bola $B\left(0, p^{\frac{-1}{p-1}}\right)$. Son estos contrastes los que hacen que la diferencia entre el análisis real y el p-ádico sea mas notable e interesante, a pesar de que estos conjuntos se obtuvieron de una construcción similar.

Bibliografía

[1] G. Bachman, George Introduction to p-adic numbers and valuation theory, Academic Press, New York-London, 1964

[2] A. J. Baker, An Introduction to p-adic Numbers and p-adic Analysis, Glasgow, 2002

[3] A. I. Borevich y I. R. Shafarevich, Number theory, Pure and Applied Mathematics, Vol. 20, Academic Press, New York-London, 1966

[4] A. García, Números p-ádicos, Universidad Nacional de Córdoba, Medina Allende,2008

[5] F. Q. Gouvêa, P-adic Numbers: An Introduction, Springer-Verlag Berlin Heidelberg New York, Second Edition, Universitext, 2000

[6] C. Ivorra, Teoría de Números, Autoedición, 2011. Disponible en https://www.uv.es/ivorra/Libros/Numeros.pdf

[7] S. Katok, Real and p-adic analysis, course notes, Deparmet of Mathematicas, The Pennsylvania State University, 2001

[8] N. Koblitz, P-adic Analysis, p-adic Analysis and Zeta-Functions, Springer-Verlag Berlin Heidelberg New York, Graduate texts in Mathematics, 1984

[9] R. Lafuente, Los Números p-ádicos y el Teorema de Hasse-Minkowski, La Plata-Argentina, 2008

[10] K. Mahler, P-adic Numbers and their Functions, Cambridge University Press, 1973

[11] J. I. Restrepo, Soluciones racionales a ecuaciones polinomiales: una aproximación al principio de Hasse, 2008.

[12] A. M. Robert, A Course in p-adic Analysis, Springer-Verlag Berlin Heidelberg New York, 2000

[13] W.H. Schikhof, Ultrametric Calculus, An Introduction to p-adic Analysis, Cambridge Studies in Adv. Math. 4, Cambridge University Press, 1984