UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

Cálculo diferencial p-ádico

TESIS

Que para obtener el título de

Matemático

PRESENTA

Martín Guarneros Martínez

DIRECTOR DE TESIS

M. en C. Adrián Zenteno Gutiérrez

Ciudad Universitaria, septiembre 2016.

1. Datos del alumno:
   Guarneros
   Martínez
   Martín
   Universidad Nacional Autónoma de México, Facultad de Ciencias
   Matemáticas
   079231192

2. Datos del tutor:
   M. en C.
   Adrián
   Zenteno
   Gutiérrez

3. Datos del propietario 1:
   Dr.
   Santiago
   López de Medrano
   Sánchez

4. Datos del propietario 2:
   Dr.
   Santiago Alberto
   Verjovsky
   Solá

5. Datos del suplente 1:
   Dr.
   Timothy Mooney
   Gendron
   Thornton

6. Datos del suplente 2:
   M. en C.
   Julio César
   Galindo
   López

7. Datos del trabajo escrito:
   Cálculo diferencial p-ádico
   116 p.
   2016

Índice general

Agradecimientos y dedicatoria

Agradezco y dedico esta tesis a todos los que me han acompañado en la vida:

Mis creadores Concepción y Martín por darme la vida.

Mis criadores Carmen (q.e.p.d.) y Juan (q.e.p.d.) por haberme mantenido con vida.

Mi abuela Josefa (q.e.p.d.) por protegerme.

Mis hermanos José Luis (q.e.p.d.), Juan Carlos, Verónica *et. al.*

Carlos Eduardo (q.e.p.d.) por estar conmigo.

Mis amigas Angélica Benita, Claudia y Ruth por su acompañamiento.

Mi Maestro Adrián Zenteno por su ejemplo, motivación, entusiasmo, respeto y paciencia.

El Maestro Julio César Galindo por su apoyo.

Mi *alma mater* Universidad Nacional Autónoma de México.

Mis motivadores: Agustín, "La Polla", Kalimán, César Alejandro y Bruce Lee (q.e.p.d).

Lo único que se necesita es que toméis la decisión.
De vosotros depende...
llegó el final de la Eternidad,
-Y el comienzo del Infinito.

Isaac Asimov, *The End of Eternity* (1995)

$\mathbb{R}$ *is like the Sun, and the p-adics are like the stars.*
The Sun blocks out the stars during the day,
and humans are asleep at night and don't see the stars,
even though they are just as important.

Kazuya Kato

Introducción

El matemático alemán KURT HENSEL introdujo los números p-ádicos en Hensel (1897). Su objetivo era poder disponer de los métodos de las expansiones en series de potencias en la teoría de números; específicamente al buscar soluciones a ecuaciones diofánticas. Esta idea surgió al observar que los números se comportan y pueden considerarse como funciones sobre un espacio topológico. El campo de los números p-ádicos, nos provee una manera alternativa de hacer Cálculo.

El objetivo principal de este trabajo es presentar la construcción y las propiedades básicas del campo de los números p-ádicos y el Cálculo diferencial en él.

En la primera parte se revisará el concepto de valor absoluto en general. Caracterizaremos un valor absoluto no arquimediano que induce la ultramétrica que da la estructura de espacio ultramétrico a los números p-ádicos. Definiremos la función de valuación p-ádica que define tal valor absoluto.

Recordamos las propiedades de las sucesiones de Cauchy porque los números p-ádicos aparecen como dichas sucesiones.

Mediante el procedimiento de completación del campo de los números racionales, usando el valor absoluto p-ádico; obtendremos el campo de los números p-ádicos.

Mostramos la aritmética básica y la topología de los números p-ádicos. En el mundo p-ádico, por ejemplo, todos los "triángulos" son isósceles, las bolas son simultáneamente abiertas y cerradas y cada punto de una bola puede considerarse como su centro.

El campo de los números p-ádicos es totalmente disconexo, completo con respecto al valor absoluto p-ádico y localmente compacto. Es un espacio topológico.

Podemos hablar de límites p-ádicos; punto de acumulación; continuidad, funciones continuas y uniformemente continuas y localmente constantes. Revisamos la interpolación p-ádica y las condiciones para que una función de variable p-ádica pueda interpolarse. Todo lo cual es tratado en la segunda parte.

Cabe notar que en el contexto p-ádico los teoremas como el del valor medio y el de la función inversa no funcionan. Para tratar de reparar esta situación se introduce la noción de función estrictamente diferenciable.

En la tercera parte se desarrolla el concepto clave fundamental para el presente trabajo; la derivada en el campo de los números p-ádicos y sus reglas. Se presentarán las series formales de potencias además de las funciones logaritmo y exponencial p-ádicas con sus propiedades.

En la última parte se presentarán las antiderivadas p-ádicas.

Las referencias básicas serán Gouvêa (1997), Hensel (1897), Katok (2007), Mahler (1981) y Robert (2000).

Capítulo 1

El campo de los números p-ádicos $\mathbb{Q}_p$

El objetivo de este capítulo es presentar al protagonista de este trabajo; el *campo de los números p-ádicos*, $\mathbb{Q}_p$. Revisamos el valor absoluto en general; el concepto de valuación, el valor absoluto p-ádico y el procedimiento de completación que culmina en la definición precisa del campo $\mathbb{Q}_p$.

Este campo puede construirse a partir de los números racionales $\mathbb{Q}$; como su *completación* con respecto a un valor absoluto. En el caso de $\mathbb{Q}_p$, este valor absoluto depende de un número primo p, y difiere drásticamente del valor absoluto usual utilizado para construir $\mathbb{R}$. Sin embargo, en ambos casos, la completación produce un *campo normado* ya sea $\mathbb{R}$ o $\mathbb{Q}_p$.

1.1. Valores absolutos sobre $\mathbb{Q}$

Empecemos por definir un *valor absoluto* y exploremos las posibilidades de dicha definición.

Definición 1.1.1. Sea $\mathbb{K}$ un *campo* (ver A.2). Un *valor absoluto* sobre $\mathbb{K}$ es una función: $|\cdot|\colon \mathbb{K} \to \mathbb{R}_{\geqslant 0}$ que satisface:

(I) $|x| = 0$ si, y sólo si $x = 0$,

(II) $|xy| = |x||y|$ para todo $x, y \in \mathbb{K}$, y

(III) $|x+y| \leqslant |x| + |y|$ para todo $x, y \in \mathbb{K}$ (*desigualdad del triángulo*).

Ejemplo 1.1.1.

1. El valor absoluto *trivial* está definido como la función $|\cdot|_{\text{triv}}\colon \mathbb{Q} \to \{0,1\}$ tal que:

$$|x|_{\text{triv}} = \begin{cases} 0 & \text{si } x = 0; \\ 1 & \text{si } x \neq 0. \end{cases}$$

2. El valor absoluto *usual* (*clásico* o *al infinito*) en el campo $\mathbb{Q}$ de los números racionales está definido como la función $|\cdot|_\infty\colon \mathbb{Q} \to \mathbb{R}_{\geqslant 0}$ tal que:

$$|x|_\infty = \begin{cases} x & \text{si } x \geqslant 0; \\ -x & \text{si } x < 0. \end{cases}$$

Definición 1.1.2. Diremos que un valor absoluto es *no arquimediano* si cumple la *"desigualdad fuerte del triángulo"*

$$|x+y| \leqslant \text{máx}\{|x|,|y|\} \quad \text{para todo } x,y \in \mathbb{K};$$

en caso contrario, diremos que es *arquimediano*.

Ejemplo 1.1.2.

- El valor absoluto trivial es no arquimediano. Ya que; si $x = y = 1$ entonces

$$|x+y|_{\text{triv}} = |2|_{\text{triv}} = 1 \leqslant 1 = \text{máx}\{1,1\} = \text{máx}\{|1|_{\text{triv}}, |1|_{\text{triv}}\} = \text{máx}\{|x|_{\text{triv}}, |y|_{\text{triv}}\}.$$

- El valor absoluto usual es arquimediano. En efecto; si $x = y = 1$ entonces

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

Observemos que para cualquier valor absoluto sobre un campo $\mathbb{K}$ tenemos:

(a) $|1| = |-1| = 1$. Ya que $|1| = |\pm 1 \cdot \pm 1| = |\pm 1|^2$ entonces $|\pm 1| = 1$.

(b) Si $x \in \mathbb{K}$ y $|x^n| = 1$ entonces $|x| = 1$. Notemos que si $\lambda^n = 1$ entonces, por (a), $\lambda = 1$.

(c) $|-x| = |x|$ para todo $x \in \mathbb{K}$. Ya que $|-x| = |(-1)\cdot x| = 1 \cdot |x|$.

(d) Si $\mathbb{K}$ es un campo finito, entonces $|\cdot|$ es trivial. Ya que en un campo finito con q elementos, tenemos que $x^{q-1} = 1$ siempre que $x \neq 0$, y aplicando (b) mostramos que cualquier valor absoluto debe ser entonces trivial.

Diremos que dos valores absolutos $|\cdot|_1$ y $|\cdot|_2$ definidos sobre el mismo campo $\mathbb{K}$, son *equivalentes* si existe $c > 0$ tal que $|x|_1 = |x|_2^c$ para todo $x \in \mathbb{K}$.

PROPOSICIÓN 1.1.1. *Un valor absoluto $|\cdot|$ sobre $\mathbb{Q}$ es no arquimediano si, y sólo si,* $\sup\{|n|\colon n \in \mathbb{Z}\} = 1$.

Demostración. Supongamos que $\sup\{|n|\colon n \in \mathbb{Z}\} = c$, con $1 < c < \infty$. Entonces debe existir $m \in \mathbb{Z}$ tal que $|m| > 1$ implica que $|m^k| = |m|^k$ crece con k, por lo que $\sup\{|n|\colon n \in \mathbb{Z}\} = \infty$. ■

COROLARIO 1.1.1. *Las siguientes afirmaciones son equivalentes:*

(a) Un valor absoluto $|\cdot|$ sobre $\mathbb{Q}$ es no arquimediano.

(b) $|n| \leqslant 1$, para todo $n \in \mathbb{Z}$.

Demostración.
Probamos $(a) \implies (b)$ por inducción:

Sabemos que $|1| = 1 \leqslant 1$.

Supongamos que $|k| \leqslant 1$ para todo $k \in \{1, \cdots, n-1\}$; probemos que $|n| \leqslant 1$:

Observemos que $|n| = |(n-1)+1| \leqslant \text{máx}\{|n-1|, |1|\} = 1$.

A partir de la desigualdad $|1| = 1 \leqslant 1$ y el supuesto de inducción, tenemos $|n| \leqslant 1$ para todo $n \in \mathbb{N}$. Dado que $|-n| = |n|$, concluimos que $|n| \leqslant 1$ para todos los enteros $n \in \mathbb{Z}$.

Recíprocamente, para $(b) \implies (a)$, tenemos que

$$|x+y|^n = |(x+y)^n|$$

por el teorema del binomio:

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

ya que $\binom{n}{k}$ es un entero

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

entonces

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

Por lo tanto

$$|x+y|^n \leqslant (n+1)[\text{máx}\{|x|, |y|\}]^n.$$

Así, para cada entero n tenemos que

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

Ya que el límite $\lim\limits_{n\to\infty} \sqrt[n]{n+1} = 1$ y haciendo que n tienda a ∞, obtenemos:

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

que es la desigualdad fuerte del triángulo; y, por la definición 1.1.2, $|\cdot|$ es no arquimediano. ■

1.2. Valuaciones

A continuación mostramos una función de valuación específica necesaria para definir el valor absoluto mediante el cual construiremos $\mathbb{Q}_p$.

Tomemos $\mathbb{Q}$ y elijamos un primo $p \in \mathbb{Z}$. Por el *teorema fundamental de la Aritmética* (Gauss, 1986, teorema 16), cualquier entero $n \in \mathbb{Z}$ puede ser escrito de manera única como $n = p^v n'$, con $p \nmid n'$.

Dado que v está determinado por p y n; tiene sentido definir una función $v_p \colon \mathbb{Q} \to \mathbb{Z}$ estableciendo $v = v_p(n)$, i.e., $v_p(n)$ es simplemente la multiplicidad de p visto como un divisor de n. Formalmente:

Definición 1.2.1. Dado p un primo; la *valuación p-ádica* $v_p(x)\colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$, es el único entero tal que $x = p^{v_p(x)}x'$, con $p \nmid x'$ para todo $x \in \mathbb{Q}^\times$ y $v_p(0) = \infty$.

Algunos autores definen una *valuación p-ádica*[1] como la función dada por

$v_p\colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$

$$x \mapsto v_p(x) = \begin{cases} \text{máx}\{n \in \mathbb{Z}\colon p^n | x\} & \text{si } x \neq 0; \\ \infty & \text{si } x = 0 \text{ (Convención).} \end{cases}$$

PROPOSICIÓN 1.2.1. *Para todo $x, y \in \mathbb{Q}^\times$, la valuación p-ádica v_p cumple lo siguiente:*

1. $v_p(xy) = v_p(x) + v_p(y)$.
2. $v_p(x+y) \geqslant \text{mín}\{v_p(x), v_p(y)\}$.

Demostración. Sean $x, y \in \mathbb{Q}^\times; v_p(x) = a, v_p(y) = b, x = p^a x', y = p^b y', p \nmid x', p \nmid y'$

1. $xy = p^a p^b x' y' = p^{(a+b)}(xy)'$ entonces $v_p(xy) = a + b = v_p(x) + v_p(y)$.
2. $x + y = p^a x' + p^b y'$. Sin pérdida de generalidad, supongamos que $a \leqslant b$, entonces tenemos que

$$x + y = p^a \left(x' + p^{(b-a)} y' \right).$$

donde $x' + p^{(b-a)}y'$ puede ser divisible por p; por lo tanto $v_p(x+y) \geqslant p^a$, entonces

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

Ejemplo 1.2.1. Algunas valuaciones p-ádicas:

- $v_7(98) = 2$, dado que 98 se factoriza como $2 \cdot 7^{\mathbf{2}}$.
- $v_{13}(1963) = 1$, dado que 1963 se factoriza como $13^{\mathbf{1}} \cdot 151$.
- $v_2\left(\frac{1}{2}\right) = -1$, dado que $\frac{1}{2}$ se factoriza como $2^{-\mathbf{1}}$.

1.3. Valor absoluto p-ádico

Mostraremos al valor absoluto p-ádico como la función crucial del presente trabajo. Con él completaremos al campo $\mathbb{Q}$ para construir al campo $\mathbb{Q}_p$. Recordemos que nuestro objetivo principal es mostrar los conceptos del cálculo diferencial en el campo $\mathbb{Q}_p$.

[1] también llamada valuación aditiva, orden de x en p o valuación exponencial p-ádica.

Definición 1.3.1. El *valor absoluto p-ádico* $|\cdot|_p$ sobre $\mathbb{Q}$ es una función $|\cdot|_p\colon \mathbb{Q}\to\mathbb{R}_{\geqslant 0}$ tal que:

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

PROPOSICIÓN 1.3.1. *El valor absoluto p-ádico, $|\cdot|_p$, es un valor absoluto no arquimediano de $\mathbb{Q}$.*

Demostración. Veamos que $|\cdot|_p$ cumple las propiedades de un valor absoluto no arquimediano:

1. $|0|_p=0$; por definición.
2. $|xy|_p=p^{-v_p(xy)}=p^{-(v_p(x)+v_p(y))}=p^{-v_p(x)}p^{-v_p(y)}=|x|_p|y|_p$. Por proposición 1.2.1 inciso (1).
3. Por la proposición 1.2.1 inciso (2), tenemos que:

$$\begin{aligned}|x+y|_p&=p^{-v_p(x+y)}\\&\leqslant \text{máx}\{p^{-v_p(x)},p^{-v_p(y)}\}\end{aligned}$$

Por lo tanto : $|x+y|_p=\text{máx}\{|x|_p,|y|_p\}$. ■

Observación 1.3.1. A diferencia de un valor absoluto arquimediano sobre $\mathbb{Q}$; dados dos números $a,b\in\mathbb{Q}$ con $|a|_p<|b|_p$, no podemos encontrar siempre un tercer número $c\in\mathbb{Q}$ tal que $|a|_p<|c|_p<|b|_p$. En particular $|\cdot|_p$ sólo toma valores en $\{p^k\colon k\in\mathbb{Z}\}\cup\{0\}$, es decir, $|\cdot|_p$ tiene imagen discreta.

Ejemplo 1.3.1.

- Si $a=\dfrac{1}{p}$ y $b=\dfrac{1}{p^2}$, entonces tenemos que $a<b$; $|a|_p=p<p^2=|b|_p$ y no hay un c tal que $a<c<b$ y $|a|_p<|c|_p<|b|_p$.
- El valor absoluto p-ádico no respeta el orden usual lineal de $\mathbb{Q}$.

$$|2|_2=\frac{1}{2}<1 \text{ y } |4|_2=\frac{1}{4}<1;\ \text{sin embargo, } |3|_2=1,\ \text{aún cuando } 2<3<4.$$

- Algunos valores absolutos p-ádicos:
  - $\left|-\dfrac{128}{7}\right|_2=\left|-\dfrac{2^7}{7}\right|_2=2^{-7}=\dfrac{1}{128}$
  - $|-13.23|_3=\left|-13-\dfrac{23}{100}\right|_3=\left|-\dfrac{1323}{100}\right|_3=\left|-\dfrac{3^3\cdot 49}{100}\right|_3=3^{-3}=\dfrac{1}{27}$
  - $|9!|_3=|9\cdot 8\cdot 7\cdot 6\cdot 5\cdot 4\cdot 3\cdot 2|_3=\left|3^4\cdot 8\cdot 7\cdot 2\cdot 5\cdot 4\cdot 2\right|_3=3^{-4}=\dfrac{1}{81}$
  - Si $\alpha=\dfrac{140}{297}=2^2\cdot 5\cdot 7\cdot 3^{-3}\cdot 11^{-1}$, tenemos:
    $|\alpha|_2=\dfrac{1}{4}$; $|\alpha|_3=27$; $|\alpha|_5=\dfrac{1}{5}$; $|\alpha|_7=\dfrac{1}{7}$; $|\alpha|_{11}=11$ y $|\alpha|_{13}=1$

TEOREMA 1.3.1 (Fórmula del Producto). *Para todo $x \in \mathbb{Q}^\times$, y un número primo p:*

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

donde el producto se toma sobre todos los primos $p = 2,3,5,7,\ldots$

Demostración. De acuerdo al teorema fundamental de la Aritmética podemos escribir cualquier entero positivo n en la forma $n = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$ donde p_i son números primos distintos. Si q es algún número primo, $q \neq p_i$ entonces $|x|_q = 1$, así el producto infinito $\prod_{p\leqslant\infty} |x|_p$ contiene sólo una cantidad finita de términos diferentes de uno. Al multiplicar $|x|_\infty$ y $|x|_{p_i} = p_i^{-a_i}$ obtenemos el resultado deseado. Por la propiedad multiplicativa del valor absoluto, la fórmula del producto es válida para cualquier número racional diferente de cero. ■

COROLARIO 1.3.1. *Para cualquier número primo p y cualquier $n \in \mathbb{N}, |n|_p \geqslant \frac{1}{n}$.*

Demostración. Al combinar la fórmula del producto y el hecho de que para cada número primo $q, |n|_q \leqslant 1$ (corolario 1.1.1) obtenemos

$$\begin{aligned} |n|_\infty \prod_q |n|_q &= 1 \\ n \cdot |n|_p \prod_{p,q\neq p} |n|_q &= 1 \\ n|n|_p &\geqslant 1 \\ |n|_p &\geqslant \frac{1}{n} \end{aligned}$$

■

Esta fórmula establece una relación cercana entre los valores absolutos de $\mathbb{Q}$; por ejemplo, dice que si conocemos todos, excepto uno de los valores absolutos de un número $x \in \mathbb{Q}$, entonces podemos determinar el que falta. [2]

Mayores detalles sobre lo visto en esta sección pueden encontrarse en Murty (2008).

1.4. Completaciones

El campo de los números reales $\mathbb{R}$ se obtiene a partir de los racionales $\mathbb{Q}$ mediante un procedimiento llamado *completación*. El cual puede aplicarse a cualquier *espacio métrico* (Katok, 2007, teorema 1.1).

El campo $\mathbb{Q}_p$ de los números p-ádicos puede construirse a partir del campo $\mathbb{Q}$ de la misma manera. La clave para esto es remplazar el valor absoluto ordinario por el valor absoluto p-ádico $|\cdot|_p$ con respecto al cual, la serie que representa a un número p-ádico converge. Los números p-ádicos aparecen de modo usual como *sucesiones de Cauchy* de números racionales. Esta aproximación fue propuesta por el matemático húngaro JÓZSEF KÜRSCHÁK (1864-1933).

Recordatorio de análisis.

[2] Esto es útil para definir el anillo de adeles (véase (Goldfeld and Hundley, 2011, pp. 7)) asociados al campo $\mathbb{Q}$, que es una pieza clave en la teoría de números moderna. Este punto está fuera del alcance del presente trabajo.

Definición 1.4.1. Sean $\mathbb{K}$ un campo y $|\cdot|$ un valor absoluto sobre $\mathbb{K}$. Una sucesión $\{a_n\}$ en $\mathbb{K}$ se dice que es:

- *Acotada* si existe una constante $C > 0$ tal que $|a_n| \leqslant C$ para todo n;
- *Nula* si $\lim_{n\to\infty} |a_n| = 0$, i.e., para cualquier $\varepsilon > 0$ hay un N tal que para todo $n > N, |a_n| < \varepsilon$;
- De *Cauchy* si $\lim_{n,m\to\infty} |a_n - a_m| = 0$, i.e., para todo $\varepsilon > 0$ hay un N tal que para todos $n, m > N$ tenemos $|a_n - a_m| < \varepsilon$;
- *Convergente* a $a \in \mathbb{K}$ (escribimos $\lim_{n\to\infty} a_n = a$) si $\lim_{n\to\infty} |a_n - a| = 0$, i.e., para todo $\varepsilon > 0$ hay un N tal que para todo $n > N, |a_n - a| < \varepsilon$.

Empecemos por discutir las sucesiones de Cauchy en un campo $\mathbb{K}$.

Un campo $\mathbb{K}$ se llama *completo* con respecto a $|\cdot|$ si para toda sucesión de Cauchy $\{x_n\}$ con elementos en $\mathbb{K}$ se cumple que $\lim_{n\to\infty} \{x_n\} \in \mathbb{K}$.

LEMA 1.4.1. *Una sucesión $\{x_n\}$ de números racionales es una sucesión de Cauchy respecto a un valor absoluto no arquimediano $|\cdot|_p$ si $\lim_{n\to\infty} |x_{n+1} - x_n|_p = 0$.*

Demostración.

$$\begin{aligned}
|x_m - x_n|_p &= |x_{n+r} - x_n|_p \\
&\leqslant |x_{n+r} - x_{n+r-1} + x_{n+r-1} - x_{n+r-2} + x_{n+r-2} - x_{n+r-3} + \cdots + x_{n+1} - x_n|_p \\
&\leqslant \text{máx}\{|x_{n+r} - x_{n+r-1}|_p, |x_{n+r-1} - x_{n+r-2}|_p, |x_{n+r-2} - x_{n+r-3}|_p, \ldots, |x_{n+1} - x_n|_p\} \\
&\leqslant \text{máx}\{p^{-n}, p^{-n}, p^{-n}, \ldots, p^{-n}\} \\
&\leqslant p^{-n}
\end{aligned}$$

Por lo tanto $\lim_{n\to\infty} |x_m - x_n|_p = \lim_{n\to\infty} p^{-n} = 0$ ■

LEMA 1.4.2. *$\mathbb{Q}$ no es completo con respecto a $|\cdot|_p$.*

Demostración. Necesitamos construir una sucesión de Cauchy en $\mathbb{Q}$ que no tenga un límite en $\mathbb{Q}$. Para ello sólo requerimos encontrar una cadena de soluciones módulo p^n de una ecuación que no tenga solución en $\mathbb{Q}$.

Supongamos que $p \neq 2$ es un número primo. Elegimos un entero $a \in \mathbb{Z}$ tal que:

- a no es un cuadrado en $\mathbb{Q}$;
- p no divide a a;
- a es un residuo cuadrático módulo p, i.e., la congruencia $x^2 \equiv a \pmod{p}$ tiene una solución.

Ahora construimos la sucesión de Cauchy:

- Elegimos x_0 que sea cualquier solución de $x_0^2 \equiv a \pmod{p}$;
- Elegimos x_1 tal que $x_1 \equiv x_0 \pmod{p}$ y $x_1^2 \equiv a \pmod{p^2}$;

- En general, elegimos x_n tal que

$$x_n \equiv x_{n-1} \text{ mód } p^n \quad \text{y} \quad x_n^2 \equiv x_{n-1} \text{ mód } p^{n+1}.$$

Cuando $p \neq 2$ tales sucesiones existen siempre que el elemento inicial x_0 exista. Ahora verifiquemos que efectivamente es una sucesión de Cauchy:

De la construcción tenemos que

$$|x_{n+1} - x_n| = |\lambda p^{n+1}| \leqslant p^{-(n+1)} \to 0;$$

por lo tanto, por el lema 1.4.1, la sucesión $\{x_n\}$ es de Cauchy.

Por otro lado,

$$|x_n^2 - a| = |\mu p^{n+1}| \leqslant p^{-(n+1)} \to 0.$$

Así que, si existiera el límite, tendría que ser una raíz cuadrada de a. Dado que a no es un cuadrado, no puede haber tal límite, lo cual muestra que $\mathbb{Q}$ no es completo respecto a $|\cdot|_p$. ■

Por lo tanto necesitamos completar a $\mathbb{Q}$.

TEOREMA 1.4.1. *Si $\mathscr{C}_p(\mathbb{Q})$ es el conjunto de todas las sucesiones de Cauchy de elementos de $\mathbb{Q}$, i.e.,*

$$\mathscr{C}_p(\mathbb{Q}) = \Big\{\{x_n\} \colon \{x_n\} \textit{ es una sucesión de Cauchy con respecto a } |\cdot|_p\Big\},$$

entonces $\big(\mathscr{C}_p(\mathbb{Q}), +, \cdot\big)$ tiene una estructura de anillo con unidad, donde

a) La suma está dada por $\{x_n\} + \{y_n\} = \{x_n + y_n\}$,

b) El producto está dado por $\{x_n\}\{y_n\} = \{x_n y_n\}$ y

c) La unidad es la sucesión $\mathbf{1} = \{1, 1, \ldots\}$

Lo cual se sigue de la suma y el producto en $\mathbb{Q}$.

Demostración. Primero probemos que la suma y el producto de dos sucesiones de Cauchy es también de Cauchy: Sean $\{x\}, \{y\} \in \mathscr{C}_p(\mathbb{Q})$ y $\varepsilon > 0$. Elijamos N_1 tal que $|x_n - x_m| < \frac{\varepsilon}{2}$ para $n, m \geqslant N_1$. Elijamos N_2 tal que $|y_n - y_m| < \frac{\varepsilon}{2}$ para $n, m \geqslant N_2$. Entonces, para $N = \text{máx}\{N_1, N_2\}$, tenemos

$$|(x_n + y_n) - (x_m + y_m)|_p \leqslant |x_n - x_m|_p + |y_n - y_m|_p < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon,$$

para $n, m \geqslant N$. Así, la suma de dos sucesiones de Cauchy es también de Cauchy.

Ahora sea K tal que $|x_n|_p \leqslant K, |y_n|_p \leqslant K$ para todo n (esto es claro a partir de la propiedad de Cauchy). Luego, dado $\varepsilon > 0$, elegimos M_1 tal que para todo $n, m \geqslant M_1$, tenemos $|x_n - x_m| \leqslant \frac{\varepsilon}{2K}$. Sea M_2 tal que $|y_n - y_m|_p \leqslant \frac{\varepsilon}{2K}$ para todo $n, m \geqslant M_2$. Para $M = \text{máx}\{M_1, M_2\}$ y $n, m \geqslant M$, tenemos

$$|x_n y_n - x_m y_m|_p \leqslant |x_n|_p |y_n - y_m|_p + |y_m|_p |x_m - x_n|_p < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Así, el producto de dos sucesiones de Cauchy es también de Cauchy. Por lo tanto $\mathscr{C}_p(\mathbb{Q})$ es cerrado bajo sumas y productos. Los otros axiomas de anillo se siguen de la suma y el producto en $\mathbb{Q}$:

1. Asociatividad con respecto a la suma:

$$\{x_n\}+\big(\{y_n\}+\{z_n\}\big)=\{x_n\}+\{y_n+z_n\}=\{x_n+y_n+z_n\}=\{x_n+y_n\}+\{z_n\}=\big(\{x_n+y_n\}\big)+\{z_n\}.$$

2. Neutro para la suma. Sea $\mathbf{0}=\{0\}=\{0,0,\ldots\}$:

$$\{x_n\}+\mathbf{0}=\{x_n\}+\{0\}=\{x_n+0\}=\{x_n\}=\{0+x_n\}=\{0\}+\{x_n\}=\mathbf{0}+\{x_n\}.$$

3. La unidad para el producto. Sea $\mathbf{1}=\{1\}=\{1,1,\ldots\}$

$$\{x_n\}\{1\}=\{x_n\cdot 1\}=\{x_n\}=\{1\cdot x_n\}=\{1\}\{x_n\}.$$

4. Inverso para el producto. Si $\{x_n\}\neq\{0\}$, entonces $\{x_n\}^{-1}=\left\{\dfrac{1}{x_n}\right\}$:

$$\{x_n\}\{x_n\}^{-1}=\{x_n\}\left\{\frac{1}{x_n}\right\}=\left\{\frac{x_n}{x_n}\right\}=\{1\}=\left\{\frac{x_n}{x_n}\right\}=\left\{\frac{1}{x_n}\right\}\{x_n\}=\{x_n\}^{-1}\{x_n\}.$$

5. Distributividad:

$$\{x_n\}\big(\{y_n\}+\{z_n\}\big)=\{x_n\}\{y_n+z_n\}=\big\{x_n(y_n+z_n)\big\}=\{x_ny_n+x_nz_n\}=\{x_ny_n\}+\{x_nz_n\}.$$

Por lo tanto $\big(\mathscr{C}_p(\mathbb{Q}),+,\cdot\big)$ es un anillo con unidad. ■

La suma y el producto de dos sucesiones nulas es una sucesión nula. Es claro que dada una sucesión nula $\{x_n\}$ y una sucesión de Cauchy $\{y_n\}\in\mathscr{C}_p(\mathbb{Q}),\{x_n\}\{y_n\}$ es una sucesión nula. Por lo tanto el conjunto de las sucesiones nulas

$$\mathscr{N}_p(\mathbb{Q})=\Big\{\{x_n\}\colon x_n\to 0,n\to\infty\Big\}=\Big\{\{x_n\}\colon \lim_{n\to\infty}|x_n|_p=0\Big\}$$

forma un *ideal* (véase A.2) de $\mathscr{C}_p(\mathbb{Q})$.

Para $x\in\mathbb{Q}$, la sucesión $\{x\}=\{x,x,\ldots\}$ es ciertamente la sucesión constante de Cauchy asociada a x.

LEMA 1.4.3. *La aplicación que envía x a la sucesión $\{x\}$ es una inclusión de $\mathbb{Q}$ en $\mathscr{C}_p(\mathbb{Q})$.*

Demostración. Sea $i\colon\mathbb{Q}\to\mathscr{C}_p(\mathbb{Q})$ definida por $i(x)=\{x\}$. i es un homomorfismo de anillos. Usemos el teorema 1.4.1 para x,y elementos de $\mathbb{Q}$,

- $i(cx)=\{cx\}=c\{x\}=ci(x)$ para todo $c\in\mathbb{Q}$.
- $i(x+y)=\{x+y\}=\{x\}+\{y\}=i(x)+i(y)$.

Veamos que el homomorfismo i es una inclusión. Para esto:

$$\ker i=\{x\in\mathbb{Q}\colon i(x)=0\}=\{x\in\mathbb{Q}\colon\{x\}=0\}=\{0\}=0.$$

Así concluimos que i es inyectiva y por tanto, una inclusión. ■

Diferentes sucesiones de Cauchy pueden tener el mismo límite. Por lo que tenemos que eliminar esta ambigüedad.

LEMA 1.4.4. *$\mathcal{N}_p(\mathbb{Q})$ es un* ideal máximo *(ver A.2) de $\mathcal{C}_p(\mathbb{Q})$.*

Demostración. Sea $\{x_n\} \in \mathcal{C}_p(\mathbb{Q})$ tal que $\{x_n\} \notin \mathcal{N}_p(\mathbb{Q})$. Sea $\mathcal{I}$ el *ideal generado* (ver A.2) por $\{x_n\}$ y $\mathcal{N}_p(\mathbb{Q})$. Por demostrar $\mathcal{I} = \mathcal{C}_p(\mathbb{Q})$.

Veamos que $\{1\} \in \mathcal{I}$ ya que cualquier ideal que contiene a la unidad, debe contener el anillo completo.

Dado que $\{x_n\}$ no tiende a 0 y es sucesión de Cauchy; eventualmente debe estar lejos de cero, esto es, debe existir un número $c > 0$ y un entero N tal que $|x_n| \geqslant c > 0$ siempre que $n \geqslant N$. En particular $x_n \neq 0$ para $n \geqslant N$. Podemos definir una nueva sucesión $\{y_n\}$ estableciendo $y_n = 0$ si $n < N$ y $y_n = \frac{1}{x_n}$ si $n \geqslant N$.

Verifiquemos que $\{y_n\}$ es una sucesión de Cauchy:

Si $n \geqslant N$ tenemos

$$|y_{n+1} - y_n| = \left| \frac{1}{x_{n+1}} - \frac{1}{x_n} \right| = \frac{|x_{n+1} - x_n|}{|x_n x_{n+1}|} \leqslant \frac{|x_{n+1} - x_n|}{c^2} \text{ tiende a } 0$$

Por lo tanto, $\{y_n\} \in \mathcal{C}_p(\mathbb{Q})$ porque $|\cdot|$ es no arquimediano.

Notemos que:

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

Es decir, $\{x_n\}\{y_n\} = \underbrace{0,0,\ldots,0}_{\text{núm finito}},\underbrace{1,1,1,\ldots}_{\text{núm infinito}}$

$\{1\} = 1,1,\ldots$ entonces $\{1\} - \{x_n\}\{y_n\} \in \mathcal{N}_p(\mathbb{Q})$ por lo que $\{1\} = \{x_n\}\{y_n\}$; por lo tanto $\{1\} \in \mathcal{I}$. Entonces $\mathcal{I} = \mathcal{C}_p(\mathbb{Q})$. Y por lo tanto $\mathcal{N}_p(\mathbb{Q})$ es un ideal máximo. ■

Como $\mathcal{N}_p(\mathbb{Q})$ es ideal máximo de $\mathcal{C}_p(\mathbb{Q})$ entonces $\mathcal{C}_p(\mathbb{Q})/\mathcal{N}_p(\mathbb{Q})$ es campo (lema A.2.1).

Definición 1.4.2. El *campo de los números p-ádicos* $\mathbb{Q}_p$ se define como el cociente

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

Observemos que dos sucesiones constantes diferentes nunca difieren por un elemento de $\mathcal{N}_p(\mathbb{Q})$ (su diferencia es justo otra sucesión constante), entonces la inclusión $\mathbb{Q} \hookrightarrow \mathcal{C}_p(\mathbb{Q}) \to \mathbb{Q}_p$ se preserva al pasar al cociente, la cual envía a $x \in \mathbb{Q}$ a la clase de equivalencia de la sucesión constante $\{x\}$. Es decir, se tiene la inclusión $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$.

Ahora vamos a mostrar otras formas equivalente de construir a los números p-ádicos.

Sea $p \in \mathbb{N}$ un primo. Mostraremos que el campo de los números p-ádicos es equivalente a la completación de $\mathbb{Q}$ con respecto a $|\cdot|_p$ y sus elementos son clases de equivalencia de sucesiones de Cauchy. Para un $a \in \mathbb{Q}_p$ y una sucesión de Cauchy $\{a_n\}$ representando a a, definimos el valor absoluto de a como $|a|_p = \lim_{n\to\infty} |a_n|_p$.

LEMA 1.4.5. *Sea $\{x_n\} \in \mathcal{C}_p(\mathbb{Q}), \{x_n\} \notin \mathcal{N}_p(\mathbb{Q})$. La sucesión de números reales $\{|x_n|_p\}$ es eventualmente estacionaria, i.e. existe un entero N tal que $|x_n|_p = |x_m|_p$ siempre que $m,n > N$.*

Demostración. Dado que $\{x_n\}$ es sucesión de Cauchy que no tiende a cero, podemos encontrar c y N_1 tal que, $n > N_1$ implica $|x_n|_p \geqslant c > 0$.

Por otro lado, hay otro entero N_2 para el que $n, m > N_2$ implica $|x_n - x_m| < c$.

Se quiere que ambas condiciones sean verdaderas al unísono, así que se establece $N = \text{máx}\{N_1, N_2\}$. Entonces se tiene que $n, m \geqslant N$ implica $|x_n - x_m| < \text{máx}\{|x_n|, |x_m|\}$, de donde $|x_n| = |x_m|$ por la propiedad no arquimediana. ■

Notamos que el valor absoluto p-ádico de $x \in \mathbb{Q}_p$ sólo toma valores en $\{p^k : k \in \mathbb{Z}\}$. Si $|x|_p = p^k \neq 0$ entonces, por el lema 1.4.5, para cada sucesión de Cauchy que represente a x hay un N tal que $|x_n|_p = p^k$ para $n > N$.

LEMA 1.4.6. *Sea $x \in \mathbb{Q}$ con $|x|_p \leqslant 1$. Entonces, para cualquier i hay un único entero $\alpha \in \{0, 1, \ldots, p^i - 1\}$ tal que $|x - \alpha|_p \leqslant p^{-i}$.*

Demostración. Sea $\dfrac{a}{b}$ con a, b primos relativos. Dado que

$$|x|_p = p^{-v_p(a)+v_p(b)} \leqslant 1,$$

tenemos que $v_p(b) = 0$, esto es, b y p^i son primos relativos para cualquier i. Podemos entonces encontrar enteros m y n tales que $np^i + mb = 1$. Para $\alpha = am$ tenemos

$$\begin{aligned} |\alpha - x|_p &= \left|am - \frac{a}{b}\right|_p = \left|\frac{a}{b}\right|_p |mb - 1|_p \\ &\leqslant |mb - 1|_p = |np^i|_p = |n|_p p^{-i} \\ &\leqslant p^{-i} \end{aligned}$$

Hay exactamente un múltiplo cp^i de p^i tal que $cp^i + \alpha \in \{0, 1, \ldots, p^i - 1\}$ y se tiene

$$|cp^i + \alpha - x|_p \leqslant \text{máx}\{|\alpha - x|_p, |cp^i|_p\} \leqslant \text{máx}\{p^{-i}, p^{-i}\} = p^{-i}.$$ ■

PROPOSICIÓN 1.4.1. *Sea $x \in \mathbb{Q}$ con $|x|_p \leqslant 1$. Entonces hay exactamente una sucesión de Cauchy $\{x_n\}$ que representa a x, tal que, para cualquier i:*

1. $0 \leqslant x_i < p^i$;
2. $x_i \equiv x_{i+1} \pmod{p^i}$.

Demostración. Sea $\{c_n\}$ una sucesión de Cauchy que representa a x. Dado que $|c_n|_p$ tiende a $|x|_p \leqslant 1$, hay un N tal que $|c_n|_p \leqslant 1$ para cualquier $n > N$. Mediante el remplazo de los primeros N elementos se puede encontrar una sucesión de Cauchy equivalente tal que $|b_n|_p \leqslant 1$ para cualquier n.

Ahora, para cada $j = 1, 2, \ldots$, sea $N(j) \geqslant j$ y $|b_i - b_{i'}|_p \leqslant p^{-j}$, para todo $i, i' \geqslant N(j)$. Del lema 1.4.6, se sabe que para cualquier j se pueden encontrar enteros $x_j \in \{0, 1, \ldots, p^i - 1\}, 0 \leqslant x_j < p^j$ (condición de x) tal que $|x_j - b_{N(j)}|_p \leqslant p^{-j}$.

Estos x_j también satisfacen la condición (2.); en efecto:

$$\begin{aligned}|x_{j+1}-x_j|_p &= |x_{j+1}-b_{N(j+1)}+b_{N(j+1)}-b_{N(j)}+b_{N(j)}-x_j|_p\\ &\leqslant \text{máx}\{|x_{j+1}-b_{N(j+1)}|_p, |b_{N(j+1)}-b_{N(j)}|_p, |b_{N(j)}-x_j|_p\}\\ &\leqslant \text{máx}\{p^{-j-1}, p^{-j}, p^{-j}\}\\ &= p^{-j}\end{aligned}$$

Esta sucesión es equivalente a $\{b_n\}$; si para cualquier j se toma $i \geqslant N(j)$

$$\begin{aligned}|x_i-b_i|_p &= |x_i-x_j+x_j-b_{N(j)}+b_{N(j)}-b_i|_p\\ &\leqslant \text{máx}\{|x_i-x_j|_p, |x_j-b_{N(j)}|_p, |b_{N(j)}-b_i|_p\}\\ &\leqslant \text{máx}\{p^{-j}, p^{-j}, p^{-j}\}\\ &= p^{-j}\end{aligned}$$

Así, $|x_i-b_i|_p$ tiende a 0 cuando i tiende a ∞.

Ahora, para mostrar la unicidad: Sea $\{d_n\}$ otra sucesión de Cauchy satisfaciendo las condiciones del lema 1.4.6 y la condición (2.) y sea $\{x_n\} \neq \{d_n\}$; esto es, para algún i_0, $x_{i_0} \neq d_{i_0}$. Dado que x_{i_0} y d_{i_0} están entre 0 y p^{i_0}; $x_{i_0} \not\equiv d_{i_0}$ mód p^{i_0}. A partir de la condición (2.) tenemos, para $i > i_0, x_i = x_{i_0} \neq d_{i_0} \equiv d_i$ mód p^{i_0}, esto es $x_i \not\equiv d_i$ mód p^{i_0} y por lo tanto $|x_i - d_i| > p^{-i_0}$ y entonces no converge a cero y $\{x_n\}$ y $\{d_n\}$ no serían equivalentes (lo que es una contradicción). ■

Para $x \in \mathbb{Q}_p$ con $|x|_p \leqslant 1$ se puede escribir la sucesión de Cauchy $\{x_n\}$ que representa a x a partir de la proposición previa como:

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

para $d_i \in \{0, 1, \ldots, p-1\}$ y x está representado por la serie convergente

$$x = \sum_{i=0}^{\infty} d_i p^i, \tag{1.1}$$

la cual puede pensarse como un *número escrito en base p* que al extenderlo queda

$$x = \cdots d_n \cdots d_1 d_0.$$

Si $x \in \mathbb{Q}_p$ con $|x|_p = p^m > 1$ entonces $x' = xp^m$ satisface $|x'|_p = p^m p^{-m} = 1$ y podemos escribir entonces

$$x = x' p^{-m} = p^{-m} \sum_{i=0}^{\infty} c_i p^i = \sum_{i=-m}^{\infty} d_i p^i,$$

con $d_{-m} = c_0 \neq 0, x$ se convierte en una fracción en base p con un número finito de dígitos después del punto y que extiende infinitamente a la izquierda

$$x = \cdots d_n \cdots d_1 d_0 . d_{-1} d_{-2} \cdots d_{-m}.$$

Este modo de escribir $x \in \mathbb{Q}_p$ como un número escrito en base p que se mantiene expandiéndose a la izquierda se llama expansión p-ádica de x. Para $d_i \in \{0,1,\ldots,p-1\}$,

$$x = \begin{cases} \cdots d_n \cdots d_1 d_0 & \text{si } |x|_p \leqslant 1; \\ \cdots d_n \cdots d_1 d_0 . d_{-1} d_{-2} \cdots d_{-m} & \text{si } |x|_p > 1 \text{ y } d_{-m} \neq 0 \end{cases}$$

Así tenemos que:

$$\mathbb{Q}_p = \left\{ \sum_{i=-m}^{\infty} d_i p^i : d_i \in \mathbb{Z} \right\}.$$

PROPOSICIÓN 1.4.2. *Sean $d_{-m} \neq 0$ y $0 \leqslant d_i < p$ enteros. Entonces las sumas parciales de la serie*

$$x = d_{-m}p^{-m} + d_{-m+1}p^{-m+1} + \cdots + d_{-1}p^{-1} + d_0 + d_1 p + d_2 p^2 + \cdots$$

forman una sucesión de Cauchy y por lo tanto x es un elemento de $\mathbb{Q}_p$.

Demostración. Sea $\varepsilon > 0$. Entonces podemos encontrar $N \in \mathbb{N}$ tal que $p^{-N} < \varepsilon$, y para $n,k > N$, sin pérdida de generalidad $k > n$; se tiene:

$$\left| \sum_{i=-m}^{k} d_i p^i - \sum_{i=-m}^{n} d_i p^i \right| = \left| \sum_{i=n+1}^{k} d_i p^i \right|$$

$$\leqslant \text{máx}\{|d_{n+1}|_p, \ldots, |d_k p^k|_p\}$$

$$\leqslant p^{-N}$$

Entonces

$$\left| \sum_{i=-m}^{k} d_i p^i - \sum_{i=-m}^{n} d_i p^i \right| < \varepsilon$$

■

1.5. Caracterizaciones de $\mathbb{Q}_p$

Hay diferentes maneras de caracterizar a $\mathbb{Q}_p$; a continuación esbozamos dos de ellas.

1. Como *límites proyectivos* (también llamados límites inversos): Para cada $n \geqslant 1$, $A_n = \mathbb{Z}/p^n\mathbb{Z}$ es el anillo de clases de enteros mód p^n. Un elemento de A_n define, por multiplicación por p, un elemento de A_{n-1}; así obtenemos un homomorfismo $\phi_n : A_n \to A_{n-1}$, cuyo núcleo es $p^{n-1}A_n$. Es decir:

$$\phi_n : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^{n-1}\mathbb{Z}$$

La sucesión

$$\ldots \to A_n \to A_{n-1} \to \ldots \to A_2 \to A_1$$

forma un sistema proyectivo indexado por los enteros positivos. Entonces el anillo de los enteros p-ádicos $\mathbb{Z}_p$ es el límite proyectivo del sistema (A_n, ϕ_n):

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

Un elemento de $\mathbb{Z}_p = \varprojlim(A_n, \phi_n)$ es una sucesión $x = \{\ldots, x_n, \ldots, x_1\}$ con $x_n \in A_n$ y $\phi_n(x_n) = x_{n-1}$ si $n \geqslant 2$. La suma y el producto en $\mathbb{Z}_p$ se definen coordenada a coordenada. Observemos que $\mathbb{Z}_p$ es un subanillo del producto $\prod_{n\geqslant 1} A_n$.

Si damos a A_n la *topología discreta*[3] y a $\prod_{n\geqslant 1} A_n$, la *topología producto*[4], el anillo $\mathbb{Z}_p$ hereda una topología que lo convierte en espacio *compacto* (dado que es un cerrado en un producto de espacios compactos). Finalmente, el campo de los números p-ádicos $\mathbb{Q}_p$ es el *campo de fracciones* (Dummit, 2004, 7.5) del anillo $\mathbb{Z}_p$:

$$\mathbb{Q}_p = \mathrm{Frac}(\mathbb{Z}_p) = S^{-1}\mathbb{Z}_p,$$

donde S es el conjunto multiplicativo $\mathbb{Z}_p \setminus \{0\}$.

Para más detalles véase Serre (1973).

2. Como *series de potencias*: Si p es un número primo fijo. Un entero p-ádico es una serie formal infinita

$$f = a_0 + a_1 p + a_2 p^2 + \cdots \qquad \text{donde } 0 \leqslant a_i < p, \text{ para todo } i = 0, 1, 2, \ldots$$

El conjunto de los enteros p-ádicos es $\mathbb{Z}_p$.

Cada $f \in \mathbb{Z}_p$ define una sucesión de clases residuales

$$\bar{s}_n = f \text{ mód } p^n \in \mathbb{Z}/p^n\mathbb{Z}, \quad n = 1, 2, \ldots,$$

Si $a_0, a_1, a_2, \ldots \in \{0, 1, \ldots, p-1\}$ son coeficientes únicos, la sucesión de números

$$s_n = a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1} p^{n-1}, \quad n = 1, 2, \ldots,$$

define el entero p-ádico y su *expansión p-ádica* es

$$\sum_{\nu=0}^{\infty} a_\nu p^\nu \in \mathbb{Z}_p.$$

Si p es un primo, $m \in \mathbb{Z}$ y $0 \leqslant a_\nu < p$ llamamos *número p-ádico* a:

$$\sum_{\nu=-m}^{\infty} a_\nu p^\nu = a_{-m} p^{-m} + \cdots + a_{-1} p^{-1} + a_0 + a_1 p + \cdots.$$

Para más detalles sobre lo tratado en esta sección véase Deitmar (2010) y Neukirch (1999).

[3] Si X es un conjunto, $\tau = 2^X$ es la topología discreta, i.e., consideramos cualquier subconjunto de X como un conjunto abierto. Es equivalente a declarar que cada punto x pertenece X un subconjunto abierto.

[4] La topología producto (de Tychonoff) sobre $\prod X_i$ se obtiene tomando como base conjuntos abiertos de la forma $\prod U_i$, donde $U_i \subset X_i$ (i finito).

1.6. Cálculos aritméticos en $\mathbb{Q}_p$

Notemos que todo entero positivo admite un desarrollo p-ádico, con p un primo (escritura en base p). Veamos algunos cálculos numéricos.

Ejemplo 1.6.1.

- Para los enteros negativos: expresemos -1 en $\mathbb{Q}_p$:

$$\begin{aligned}
-1 &= (p-1)-p \\
&= (p-1)+[(p-1)-p]\,p \\
&= (p-1)+(p-1)p+p^2 \\
&= (p-1)+(p-1)p+[(p-1)-p]\,p^2 \\
&= (p-1)+(p-1)p+(p-1)p^2-p^3 \\
&\vdots \\
&= (p-1)+(p-1)p+(p-1)p^2\cdots+(p-1)p^{n-1}-p^n
\end{aligned}$$

  Por lo tanto,

$$-1=\sum_{i=0}^{\infty}(p-1)p^i.$$

- Para números racionales: expresemos $\dfrac{2}{3}$ en $\mathbb{Q}_5$: Con $m_0=2, n=3$ y $p=5$ construimos la sucesión de m_i y a_i:

$$\begin{aligned}
m_0 &= a_0 n + m_1 p, \\
2 &= 3a_0 + 5m_1, \\
a_0 = 4, &\quad m_1 = -2,
\end{aligned}$$

$$\begin{aligned}
m_1 &= a_1 n + m_2 p, \\
-2 &= 3a_1 + 5m_2 \\
a_1 = 1, &\quad m_2 = -1,
\end{aligned}$$

$$\begin{aligned}
m_2 &= a_2 n + m_3 p, \\
-1 &= 3a_2 + 5m_3 \\
a_2 = 3, &\quad m_3 = -2.
\end{aligned}$$

  Tenemos $m_3 = m_1$ así que tendremos un periodo de longitud 2 después del rango 1. Por lo tanto

$$\frac{2}{3} = \ldots\boxed{31}31314.$$

La mecánica de suma, resta, producto y división de números p-ádicos es muy parecida a las operaciones correspondientes sobre decimales. La única diferencia es que el "acarreo", (el "llevar", la "multiplicación larga") va de izquierda a derecha en lugar de derecha a izquierda. Aquí hay unos ejemplos en $\mathbb{Q}_7$:

1. Una suma:

$$\begin{array}{r} 2\times 7^{-1}+0\times 7^{0}+3\times 7^{1}+2\times 7^{2}+\cdots \\ -4\times 7^{-1}+0\times 7^{0}+5\times 7^{1}+1\times 7^{2}+\cdots \\ \hline 5\times 7^{-1}+0\times 7^{0}+1\times 7^{1}+4\times 7^{2}+\cdots \end{array}$$

2. Un producto:

$$\begin{array}{r} 3\times 7^{0}+6\times 7+2\times 7^{2}+\cdots \\ -4\times 7^{0}+5\times 7+1\times 7^{2}+\cdots \\ \hline 5\times 7^{0}+4\times 7+4\times 7^{2}+\cdots \\ 1\times 7+4\times 7^{2}+\cdots \\ 3\times 7^{2}+\cdots \\ \hline 5\times 7^{0}+5\times 7+4\times 7^{2}+\cdots \end{array}$$

3. Expresemos $-\dfrac{1}{7}$ en $\mathbb{Q}_5$:

   A partir de $5^6 \equiv 1$ mód 7 (Fermat), y $\dfrac{(5^6-1)}{7} = 2232$, tenemos

$$\begin{aligned} -\frac{1}{7} &= \frac{2232}{1-5^6} \\ &= \frac{2+1\cdot 5+4\cdot 5^2+2\cdot 5^3+3\cdot 5^4}{1-5^6} \\ &= (21423)(1+5^6+5^{12}+\cdots) \\ &= \mathbf{214230}\,214230\,214230\,214230\ldots \\ &= 3+3\cdot 5^1+0\cdot 5^2+2\cdot 5^3+\cdots \end{aligned}$$

   Por lo tanto: $-\dfrac{1}{7} = 330214\,230214\,230214\,230214\,230214\ldots$

4. Una división en $\mathbb{Q}_7$:

$$
\begin{array}{rl|llll}
 & & & & 5\cdot 7^0 & +1\cdot 7+6\cdot 7^2\cdots \\ \hline
3+5\cdot 7+1\cdot 7^2+\cdots &) & 1+ & 2\cdot 7+ & 4\cdot 7^2 & +\cdots \\
 & & 1+ & 6\cdot 7+ & 1\cdot 7^2 & +\cdots \\ \hline
 & & & 3\cdot 7+ & 2\cdot 7^2 & +\cdots \\
 & & & 3\cdot 7+ & 5\cdot 7^2 & +\cdots \\ \hline
 & & & & 4\cdot 7^2 & +\cdots \\
 & & & & 4\cdot 7^2 & +\cdots \\ \hline
\end{array}
$$

5. Calculemos $\sqrt{6}$ en $\mathbb{Q}_5$:

   Queremos encontrar una sucesión de dígitos 5-ádicos $a_0, a_1, \ldots, \quad 0 \leqslant a_i \leqslant 4$ tales que

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

   De lo anterior obtenemos $a_0^2 \equiv 1 \text{ mód } 5$; lo que implica que $a_0 = 1$.

   Si $a_0 = 1$, entonces

$$2a_1 \cdot 5 \equiv 1 \cdot 5 \text{ mód } 5^2; \text{ entonces } 2a_1 \equiv 1 \text{ mód } 5; \text{ entonces } a_1 = 3$$

   En el siguiente paso tenemos:

$$1 + 1 \cdot 5 \equiv \left(1 + 3 \cdot 5 + a_2 \cdot 5^2\right)^2 \equiv 1 + 1 \cdot 5 + 2a_2 \cdot 5^2 \text{ mód } 5^3,$$

   lo cual implica que $2a_2 \equiv 0 \text{ mód } 5$ y, por tanto, $a_2 = 0$.

   Así, obtenemos la serie

$$a = 1 + 3 \cdot 5 + 0 \cdot 5^2 + \cdots$$

   donde cada a_i después de a_0 está determinado de manera única.

   Si elegimos $a_0 = 4$, entonces obtenemos la solución

$$-a = 4 + 1 \cdot 5 + 4 \cdot 5^2 + 0 \cdot 5^3 + \cdots$$

   Lo cual indica que $a \in \mathbb{Q}_p$ siempre tiene exactamente dos raíces cuadradas en $\mathbb{Q}_p$, si tiene alguna.

6. Tratemos de calcular $\sqrt{7}$ en $\mathbb{Q}_5$:

   Si tenemos

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

   seguimos que $a_0^2 \equiv 2 \text{ mód } 5$. Al verificar los posibles valores de $a_0 = 1, 2, 3, 4$; vemos que es imposible. Es decir, 7 no tiene raíz cuadrada en $\mathbb{Q}_5$.

7. Cálculo de $\sqrt{-1}$ en $\mathbb{Q}_5$:

   Buscamos $\sqrt{-1}|_{\mathbb{Q}_5} = \sum_{i\geqslant 0} a_i 5^i$ con $0 \leqslant a_i \leqslant 4$.

   Debemos tener

$$\left(\sum_{i\geqslant 0} a_i 5^i\right) \times \left(\sum_{i\geqslant 0} a_i 5^i\right) = -1$$

   es decir:

$$a_0^2 + (2a_0a_1)5 + (a_1^2 + 2a_2a_0)5^2 + \cdots = -1.$$

   Lo que da las siguientes condiciones:

$$\begin{aligned} a_0^2 &\equiv -1(5), \\ a_0^2 + (2a_0a_1)5 &\equiv -1(5^2), \\ a_0^2 + (2a_0a_1)5 + (a_1^2 + 2a_2a_0)5^2 &\equiv -1(5^3), \\ &\cdots \end{aligned}$$

   o, para los primeros 3 coeficientes $(a_0, a_1, a_2) \in [0,4]$:

$$\begin{aligned} a_0^2 &\equiv -1(5), \\ a_0^2 + 10a_0a_1 &\equiv -1(25), \\ a_0^2 + 10a_0a_1 + 25a_1^2 + 50a_2a_0 &\equiv -1(125), \end{aligned}$$

   o:

$$\begin{aligned} a_0^2 &\equiv -1(5), \\ a_0^2 + 10a_0a_1 &\equiv -1(25), \\ (a_0 + 5a_1)^2 + 50a_0a_2 &\equiv -1(125). \end{aligned}$$

   Calculamos los valores de a_0^2 en $\mathbb{Z}/5\mathbb{Z}$:

a_0	0	1	2	3	4
a_0^2	0	1	4	4	1

   así que $a_0 = 2$ o $a_0 = 3$.

   (a) Consideremos el caso $a_0 = 2$. Para encontrar a_1 resolvemos:

$$\begin{aligned} a_0^2 + 10a_0a_1 &\equiv -1(25), \\ 4 + 20a_1 &\equiv -1(25) \\ 20a_1 &\equiv -5(25). \end{aligned}$$

   Calculamos los valores de $20a_1$ en $\mathbb{Z}/25\mathbb{Z}$:

a_1	0	1	2	3	4
$20a_1$	0	20	15	10	5

hay una única solución $a_1 = 1$. Para encontrar a_2 resolvemos:

$$\begin{aligned}(a_0+5a_1)^2+50a_0a_2 &\equiv -1(125),\\ (2+5)^2+100a_2 &\equiv -1(125)\\ 100a_2 &\equiv -50(125).\end{aligned}$$

Calculamos los valores de $100a_2$ en $\mathbb{Z}/125\mathbb{Z}$:

a_2	0	1	2	3	4
$100a_2$	0	100	75	50	25

hay una única solución $a_2 = 1$. Mostremos que los $a_i's$ son soluciones del sistema

$$(a_0+5a_1+\cdots+5^{k-2}a_{k-2})^2+2(5^{k-1})a_0a_{k-1} \equiv -1(5^k), \quad \text{para todo } k>1. \tag{1.2}$$

Sabemos que $\left(\sum_{i\geqslant 0} a_i\right)^2 = -1$ o $\sum_{s=0}\left(\sum_{i+j=s} a_ia_j\right)5^s = -1$; así que tenemos las relaciones:

$$\sum_{s=0}^{s=k-1}\left(\sum_{i+j=s} a_ia_j\right)5^s = -1(5^k), \quad k>1.$$

Por otro lado, tenemos que

$$\begin{aligned}(a_0+5a_1+\cdots+5^{k-2}a_{k-2})^2 &= \sum_{0\leqslant(i,j\leqslant k-2)} a_ia_j5^{i+j},\\ &= \sum_{s=0}^{2(k-2)}\left(\sum_{\substack{i+j=s\\(i,j)\leqslant k-2}} a_ia_j\right)5^s,\\ &\equiv \sum_{s=0}^{k-1}\left(\sum_{\substack{i+j=s\\(i,j)\leqslant k-2}} a_ia_j\right)5^s \text{ mód } 5^k,\\ &\equiv \sum_{s=0}^{k-1}\left(\sum_{i+j=s} a_ia_j\right)5^s - 2a_0a_{k-1}5^{k-1} \text{ mód } 5^k,\\ &\equiv -1-2a_0a_{k-1} \text{ mód } 5^k.\end{aligned}$$

lo que prueba la afirmación. Mostremos que el sistema (1.2) tiene solución única $\{a_k\}_{k\in\mathbb{N}}$, dados a_0 y a_1. Dicho sistema es equivalente a :

$$\begin{aligned}&(a_0+5a_1+\cdots+5^{k-3}a_{k-3})^2+(5^{k-2}a_{k-2})^2\\ &\qquad+2(a_0+5a_1+\cdots+5^{k-3}a_{k-3})(5^{k-2}a_{k-2})+2(5^{k-1})a_0a_{k-1} \equiv -1(5^k),\\ &\qquad\qquad\text{para todo } k>1.\end{aligned}$$

Si, y sólo si $\left[\text{con } S_{k-1} = 2(a_1 + \cdots + 5^{k-2}a_{k-3})a_{k-2}\right]$

$$-1 + 5^{k-1}S_{k-1} - 2(5^{k-2})a_0a_{k-2} + 2(a_0)(5^{k-2}a_{k-2}) + 2(5^{k-1})a_0a_{k-1} \equiv -1(5^k), \quad \text{para todo } k > 1$$

si, y sólo si, $-1 + 5^{k-1}S_{k-1} - 2(5^{k-1})a_0a_{k-1} \equiv -1(5^k)$, para todo $k > 1$.
Esto nos lleva a solucionar las ecuaciones lineales para $k = 1, \ldots$ con $X = a_{k-1}$:

$$5^{k-1}S_{k-1} - 2(5^{k-1})a_0X \equiv 0(5^k).$$

Para cada $k \geqslant 1$, si $\alpha = 2a_0$ y $\beta = S_{k-1}$, a_{k-1} es solución de

$$\alpha X + \beta = 0, \quad X \in \mathbb{Z}/5\mathbb{Z}.$$

tiene solución única porque $\mathbb{Z}/5\mathbb{Z}$ es un campo y $\alpha \neq 0$. Esta es $X = -\frac{\beta}{\alpha}$. Así que, al resolver recursivamente las ecuaciones lineales para todos los valores de k, obtenemos la solución única $\{a_k\}_{k\in\mathbb{N}}$:

$$\sqrt{-1}|_{\mathbb{Q}_5} = \ldots 212.$$

(b) El mismo proceso en (a) se aplica para encontrar la única raíz cuadrada de -1 en $\mathbb{Q}_5$ cuando $a_0 = 3$.

Observación 1.6.1. La existencia $\sqrt{a}|_{\mathbb{Q}_p}$ depende del valor de $a \in \mathbb{Q}_p$ y del primo p. Hay raíces cuadradas en algún $\mathbb{Q}_p$ que no están en $\mathbb{R}$ y viceversa .

1.7. Topología de $\mathbb{Q}_p$

Un punto importante de un valor absoluto es que nos proporciona una noción de "tamaño". Y podemos medir distancias entre números al dotar a nuestro campo de una *métrica*. Con ello podemos definir conjuntos abiertos y cerrados y así determinar la *topología* del campo.

Definición 1.7.1. Sea $\mathbb{K}$ un campo, $|\cdot|$ un valor absoluto en $\mathbb{K}$. La función distancia o *métrica* inducida por el valor absoluto es la función $d(x,y)$, entre dos elementos $x, y \in \mathbb{K}$ dada por:

$$d\colon \mathbb{K} \times \mathbb{K} \to \mathbb{R}_{\geqslant 0} \quad ; \quad d(x,y) = |x-y|.$$

La cual cumple las siguientes propiedades para cualesquiera $x, y, z \in \mathbb{K}$:

1. $d(x,y) \geqslant 0$, $\quad d(x,y) = 0$ si, y sólo si, $x = y$.
2. $d(x,y) = d(y,x)$.
3. $d(x,z) \leqslant d(x,y) + d(y,z)$ $\quad$ (*desigualdad del triángulo*) .

Así, $\big(\mathbb{K}, d(x,y)\big)$ es un *espacio métrico*.

Todo valor absoluto $|\cdot|$ induce una métrica sobre $\mathbb{K}$ lo que nos permite referirnos al campo normado $(\mathbb{K}, |\cdot|)$ como un *espacio métrico*.

Observación 1.7.1. A la métrica inducida por un valor absoluto no arquimediano se le llama *ultramétrica* y al correspondiente espacio, *espacio ultramétrico*.

Definición 1.7.2. Sean (X,d_1) y (Y,d_2) dos espacios métricos. Una función f de X en Y.

- f es *continua en el punto* $a \in X$ si para cada $\varepsilon > 0$ existe un $\delta > 0$ tal que $d_2\big(f(x),f(a)\big) < \varepsilon$ siempre que $d_1(x,a) < \delta$.
- f es *continua* si es continua en cada punto de su dominio.
- f es continua en un subconjunto A de su dominio si la función restringida $f|_A$ es continua.

Definición 1.7.3. Sea X un conjunto:

1. Una *topología* en X es una colección τ de subconjuntos de X con las siguientes propiedades:
   a) $\emptyset \in \tau$ y $X \in \tau$.
   b) Si $V_i \in \tau$ para $i = 1,2,\ldots,n$ entonces $\bigcap_{i=1}^{n} V_i \in \tau$.
   c) Si $\{V_i\}$ es una colección arbitraria de elementos de τ (finita, numerable o no numerable), entonces $\bigcup_{\alpha} V_\alpha \in \tau$.
2. Si τ es una topología en X, entonces se dice que X es un *espacio topológico*, y los elementos de τ se denominan *conjuntos abiertos* en X.

Observación 1.7.2.

1. Al fijar $x_0, y_0 \in \mathbb{K}$ para todo $\varepsilon > 0$, existe $\delta > 0$ tal que siempre que $d(x,x_0) < \delta$ y $d(y,y_0) < \delta$, tenemos que $d(x+y, x_0+y_0) < \varepsilon$. Es decir, la suma es una función continua.
2. Fijemos $x_0, y_0 \in \mathbb{K}$. Para todo $\varepsilon > 0$, existe $\delta > 0$ tal que siempre que $d(x,x_0) < \delta$ y $d(y,y_0) < \delta$, tenemos que $d(xy, x_0y_0) < \varepsilon$. Es decir, la multiplicación es una función continua.
3. Fijemos $x_0 \in \mathbb{K}, x_0 \neq 0$. Para todo $\varepsilon > 0$, existe $\delta > 0$ tal que siempre que $d(x,x_0) < \delta$, tenemos que $x \neq 0$ y $d\big(\frac{1}{x}, \frac{1}{x_0}\big) < \varepsilon$. Es decir, tomar inversos es una función continua.

Esto muestra que la métrica $d(x,y)$ convierte a $\mathbb{K}$ en un *campo topológico*. El hecho de que un valor absoluto sea no arquimediano puede expresarse en términos de la métrica:

LEMA 1.7.1. *Sea* $|\cdot|$ *un valor absoluto en el campo* $\mathbb{K}$. *Entonces* $|\cdot|$ *es no arquimediano si, y sólo si, para todo* $x,y,z \in \mathbb{K}$, *se cumple la* desigualdad ultramétrica*:*

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

Demostración. Sean $x,y,z \in \mathbb{K}$, entonces podemos escribir $|x-y| = |x-z+z-y|$, luego $|x-y| = |(x-z)+(z-y)|$; por la propiedad no arquimediana: $|x-y| \leqslant \text{máx}\{|x-z|,|z-y|\}$; entonces $d(x,y) \leqslant \text{máx}\{d(x,z),d(z,y)\}$.

Recíprocamente: Supongamos que se cumple $d(x,y) \leqslant \text{máx}\{d(x,z),d(z,y)\}$; sin pérdida de generalidad sean $y = y_1, z = 0$. Entonces la desigualdad es $d(x,-y_1) \leqslant \text{máx}\{d(x,0),d(0,-y_1)\}$. De ahí $|x+y_1| \leqslant \text{máx}\{|x|,|y_1|\}$ que es la propiedad no arquimediana. Entonces $|\cdot|$ es un valor absoluto no arquimediano. ■

Los espacios ultramétricos tienen propiedades curiosas, y las exploraremos en el resto de esta sección. El punto principal es que una vez que tenemos una manera de medir distancias; podemos hacer geometría. Dado que nuestro modo de medir distancias es un poco extraño, la geometría es también algo extraña. (Khrennikov and Nilson, 2004, cap. 2).

LEMA 1.7.2 (Principio de dominación)**.** *Sea $\mathbb{K}$ un campo y sea $|\cdot|$ un valor absoluto no arquimediano en $\mathbb{K}$. Si $x,y \in \mathbb{K}$ y $|x| \neq |y|$, entonces*

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

Demostración. Intercambiando x y y si fuera necesario; podemos suponer que $|x| > |y|$.

Sabemos que

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

Por otro lado, $x = (x+y)-y$, así que

$$|x| \leqslant \text{máx}\{|x+y|,|y|\}.$$

Dado que sabemos que $|x| > |y|$, esta desigualdad se cumple sólo si

$$\text{máx}\{|x+y|,|y|\} = |x+y|.$$

Esto da la desigualdad inversa $|x| \leqslant |x+y|$, y de ella, al usar la primera desigualdad, concluimos que $|x| = |x+y|$. ■

El siguiente resultado es importante de aquí en adelante:

COROLARIO 1.7.1. *En un espacio ultramétrico, todos los* "triángulos" *son isósceles.*

Demostración. Sean x,y y z elementos de un espacio ultramétrico (los vértices de nuestro "triángulo"). Las longitudes de los lados del "triángulo" son las distancias

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

Como $(x-y)+(y-z) = (x-z)$. Entonces por el lema 1.7.2 tenemos que si $|x-y|_p \neq |y-z|_p$, entonces $|x-z|_p$ es igual al mayor de los dos. Por lo tanto, en cualquier caso, dos de los "lados" son iguales. De ahí que todo triángulo sea isósceles en el mundo no arquimediano. ■

Este es un resultado más bien poco intuitivo. El trasfondo es el siguiente: veamos el caso donde $x,y \in \mathbb{Z}$. Digamos que $v_p(x) = n$ y $v_p(y) = m$, así que

$$x = p^n x'\,; \qquad y = p^m y'\,; \qquad p \nmid x'y'.$$

traduciendo a valores absolutos, tenemos

$$|x|_p = p^{-n} \qquad \text{y} \qquad |y|_p = p^{-m}.$$

Tenemos $|x|_p > |y|_p$ cuando $n < m$; digamos que $m = n+\varepsilon$, con $\varepsilon > 0$. Entonces

$$x+y = p^n x' + p^{n+\varepsilon} y' = p^n (x' + p^\varepsilon y').$$

Ahora, dado que $p \nmid x'$, tenemos $p \nmid (x' + p^\varepsilon y')$, y por lo tanto $v_p(x+y) = n$ lo que significa que $|x+y|_p = p^{-n} = |x|_p$, como establece el lema 1.7.2.

Por otro lado, supongamos que $|x|_p = |y|_p$; es decir, $n = m$. Entonces tenemos

$$x+y = p^n (x' + y')$$

con $p \nmid x'$ y $p \nmid y'$ y es perfectamente posible que $p|(x'+y')$. Si es así, lo más que podemos decir es que $v_p(x+y) \geqslant n = \text{mín}\{v_p(x), v_p(y)\}$, lo cual se traduce como

$$|x+y|_p \leqslant \text{máx}\big\{|x|_p, |y|_p\big\} = |x|_p = |y|_p.$$

Notamos que, en cualquier caso, dos de los tres valores absolutos $|x|_p, |y|_p$ y $|x+y|_p$ son iguales.

Observemos que en los espacios métricos, más importantes que los triángulos, son las "bolas" o "discos". Estos también se convierten en algo extraño en los espacios ultramétricos.

Definición 1.7.4. Sea $\mathbb{Q}_p$ el campo de los números p-ádicos con valor absoluto $|\cdot|_p$. Sea $a \in \mathbb{Q}_p$ un elemento y $r \in \mathbb{R}_{>0}$ un número real.

- La *bola abierta* de radio r y centro a es el conjunto

$$B(a,r) = \{x \in \mathbb{Q}_p \colon d(x,a) < r\} = \{x \in \mathbb{Q}_p \colon |x-a|_p < r\}.$$

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

$$\overline{B}(a,r) = \{x \in \mathbb{Q}_p \colon d(x,a) \leqslant r\} = \{x \in \mathbb{Q}_p \colon |x-a|_p \leqslant r\}.$$

- La *esfera* de radio r y centro a es el conjunto

$$S(a,r) = \{x \in \mathbb{Q}_p \colon d(x,a) = r\} = \{x \in \mathbb{Q}_p \colon |x-a|_p = r\}.$$

Las bolas abiertas siempre son los conjuntos abiertos, y las bolas cerradas siempre son conjuntos cerrados con cualquier valor absoluto, arquimediano o no arquimediano.

PROPOSICIÓN 1.7.1. *La* esfera $S(a,r)$ *es un conjunto abierto en* $\mathbb{Q}_p$.

Demostración. Sea $x \in S(a,r), \varepsilon < r$. Mostraremos que $B(x,\varepsilon) \subset S(a,r)$.
Si $y \in B(x,\varepsilon)$, entonces $|x-y|_p < |x-a|_p = r$ de donde $|x-y|_p = |x-a|_p = r$; lo que significa exactamente que $y \in S(a,r)$. ■

PROPOSICIÓN 1.7.2. *La esfera $S(a,r)$ es simultáneamente abierta y cerrada.*

Demostración. Sabemos que $S(a,r)$ es abierta por la proposición anterior.
Sabemos que $\overline{B}(a,r)$ es cerrada, y dado que $B(a,r)$ es abierta, su complemento, $\{x \in \mathbb{Q}_p : |x-a|_p \geqslant r\}$ es cerrado. Pero $S(a,r)$ es la intersección de estos dos conjuntos cerrados y por tanto es cerrado. ■

PROPOSICIÓN 1.7.3. *Sea el campo $\mathbb{Q}_p$ con su valor absoluto no arquimediano $|\cdot|_p$.*

1. *Si $b \in B(a,r)$, entonces $B(a,r) = B(b,r)$; es decir, cada punto contenido en una bola abierta, es un centro de dicha bola.*

2. *Si $b \in \overline{B}$, entonces $\overline{B}(a,r) = \overline{B}(b,r)$, es decir, cada punto contenido en una bola cerrada es un centro de dicha bola.*

3. *El conjunto $B(a,r)$ es, al mismo tiempo, abierto y cerrado.*

4. *Si $r \neq 0$, el conjunto $\overline{B}(a,r)$ es, al mismo tiempo, abierto y cerrado.*

5. *Si $a,b \in \mathbb{Q}_p$ y $r,s \in \mathbb{R}_{\geqslant 0}$, tenemos $B(a,r) \cap B(b,s) \neq \emptyset$ si, y sólo si, $B(a,r) \subset B(b,s)$ o $B(a,r) \supset B(b,s)$, es decir, dos bolas abiertas cualquiera son al mismo tiempo disjuntas o contenidas una en la otra.*

6. *Si $a,b \in \mathbb{Q}_p$ y $r,s \in \mathbb{R}_{\geqslant 0}$, tenemos $\overline{B}(a,r) \cap \overline{B}(b,s) \neq \emptyset$ si, y sólo si $\overline{B}(a,r) \subset \overline{B}(b,s)$ o $\overline{B}(a,r) \supset \overline{B}(b,s)$, es decir, dos bolas cerradas cualquiera son al mismo tiempo disjuntas y contenidas una en la otra.*

Demostración. Sean $a,b \in \mathbb{Q}_p$ con valor absoluto no arquimediano $|\cdot|_p$ y $r \in \mathbb{R}_{\geqslant 0}$

1. Por definición $b \in B(a,r)$ si, y sólo si, $|b-a|_p < r$. Ahora, tomando cualquier x para el que $|x-a|_p < r$, la propiedad no arquimediana nos dice que

$$|x-b|_p \leqslant \text{máx}\{|x-a|_p, |b-a|_p\} < r,$$

así que $x \in B(b,r)$; esto muestra que $B(a,r) \subset B(b,r)$. Intercambiando a y b

$$|x-a|_p \leqslant \text{máx}\{|x-b|_p, |a-b|_p\} < r,$$

así que $x \in B(a,r)$; esto muestra que $B(b,r) \subset B(a,r)$. Por lo tanto $B(a,r) = B(b,r)$.

2. Por definición $b \in \overline{B}(a,r)$ si, y sólo si, $|b-a|_p \leqslant r$. Ahora, tomando cualquier x para el que $|x-a|_p \leqslant r$, la propiedad no arquimediana nos dice que

$$|x-b|_p \leqslant \text{máx}\{|x-a|_p, |b-a|_p\} \leqslant r,$$

así que $x \in \overline{B}(b,r)$; esto muestra que $\overline{B}(a,r) \subset \overline{B}(b,r)$. Intercambiando a y b

$$|x-a|_p \leqslant \text{máx}\{|x-b|_p, |a-b|_p\} \leqslant r,$$

así que $x \in \overline{B}(a,r)$; esto muestra que $\overline{B}(b,r) \subset \overline{B}(a,r)$. Por lo tanto $\overline{B}(a,r) = \overline{B}(b,r)$.

3. La bola abierta $B(a,r)$ es un conjunto abierto en cualquier espacio métrico (Cualquier $x \in B(a,r)$ está en $B(a,r)$ que está contenido en $B(a,r)$). Para ver que es cerrado, mostraremos que su complemento

$$C = \{x \in \mathbb{Q}_p : |x-a|_p \geqslant r\}$$

es abierto. Pero $C = S(a,r) \cup D$, donde

$$D = \{x \in \mathbb{Q}_p : |x-a|_p > r\}.$$

El conjunto D es abierto (esto es verdadero en cualquier espacio métrico). Para ver esto, sea $y \in D$. Entonces $|y-a|_p = r_1 > r$. Afirmamos que la bola abierta $B(y, r_1 - r)$ está contenida en D. En efecto, si no fuera así, entonces habría un $x \in B(y, r_1 - r)$ tal que $|x-a|_p \leqslant r$. Pero, por la desigualdad ultramétrica,

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

una contradicción. La proposición ahora se sigue porque la unión de dos abiertos es un abierto.

4. Ahora recordemos que un punto $x \in \mathbb{Q}_p$ es un *punto frontera* del conjunto $A \subset \mathbb{Q}_p$ si cualquier bola abierta centrada en x contiene puntos que están en A y puntos que no están en A, y un conjunto A es cerrado si, y sólo si, contiene a todos sus puntos frontera. Se sigue de (3) que $S(a,r)$ no es una frontera de la bola abierta $B(a,r)$. En efecto, (3) implica inmediatamente que $B(a,r)$ no tiene frontera. Y, por supuesto, la bola cerrada

$$\begin{aligned} \overline{B}(a,r) &= \{x \in \mathbb{Q}_p : |x-a|_p \leqslant p^n\} \\ &= \{x \in \mathbb{Q}_p : |x-a|_p \leqslant p^{n+1}\} \\ &= B(a, p^{n+1}) \end{aligned}$$

no es la cerradura de la bola abierta. De lo anterior se sigue que todos las afirmaciones probadas para bolas abiertas se cumplen para bolas cerradas en $\mathbb{Q}_p$.

5. Si una bola está contenida en la otra, tienen una intersección no vacía. Para probar la dirección contraria, asumamos que $r \leqslant s$ y $y \in B(a,r) \cap B(b,s)$. Por (2), tenemos $B(a,r) = B(y,r)$ y $B(b,s) = B(y,s)$, y se sigue la inclusión.

6. Si una bola está contenida en la otra, tienen una intersección no vacía. Para probar la dirección contraria, asumamos que $r \leqslant s$ y $y \in \overline{B}(a,r) \cap \overline{B}(b,s)$. Por (1), tenemos $\overline{B}(a,r) = \overline{B}(y,r)$ y $\overline{B}(b,s) = \overline{B}(y,s)$, y se sigue la inclusión. ■

El conjunto de bolas en $\mathbb{R}$ es no numerable dado que el conjunto de todos los posibles números reales positivos es no numerable (*Teorema de Cantor* (Haaser and Sullivan, 1991, cap. 1, proposición 6.1)); lo mismo es verdadero para el conjunto de centros a de radio ρ como para el conjunto de todas las bolas $B(a,\rho)$ en $\mathbb{R}$. El siguiente resultado, completamente diferente, se cumple para el conjunto de bolas en $\mathbb{Q}_p$.

PROPOSICIÓN 1.7.4. *El conjunto de todas las bolas en $\mathbb{Q}_p$ es numerable.*

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

$$a=\sum_{n=-m}^{\infty}a_np^n,$$

y sea

$$a_0=\sum_{n=-m}^{s}a_np^n,$$

Claramente, a_0 es un número racional, y $|a-a_0|_p<p^{-s}$, es decir, $a_0\in B(a,p^{-s})$, entonces

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

Aquí, ambos centros y el radio vienen de conjuntos numerables. Por lo tanto, el conjunto que se produce de todos los pares (a_0,s) es también numerable así como el conjunto de todas las bolas en $\mathbb{Q}_p$. ■

PROPOSICIÓN 1.7.5. *Un entero p-ádico tiene un inverso multiplicativo en $\mathbb{Z}_p$ si, y sólo si $|a|_p=1$.*

Demostración. Para un elemento $a\in\mathbb{Z}_p\setminus\{0\}$; su inverso $a^{-1}\in\mathbb{Q}_p$ verifica $|a^{-1}|_p|a|_p=1$.
Como $|a|_p\leqslant 1$, entonces $|a^{-1}|_p\leqslant 1$, si, y sólo si $|a|_p=1$. ■

Esto es, el subgrupo de unidades $\mathbb{Z}_p^{\times}$ coincide con $S(0,1)$. i.e.,

$$\mathbb{Z}_p^{\times}=\{x\in\mathbb{Z}_p\colon\ |x|_p=1\}=S(0,1) \tag{1.3}$$

Definición 1.7.5. *A* es un anillo *local* si tiene un único ideal máximo M. i.e., si, y sólo si los no invertibles de A forman un ideal.

PROPOSICIÓN 1.7.6. *El anillo $\mathbb{Z}_p$ tiene un único ideal máximo, $p\mathbb{Z}_p=\mathbb{Z}_p\setminus\mathbb{Z}_p^{\times}$.*

Demostración. Notemos el homomorfismo natural φ del anillo $\mathbb{Z}_p$ al campo finito $\mathbb{Z}/p\mathbb{Z}$, dado por $\varphi:\mathbb{Z}_p\to\mathbb{Z}/p\mathbb{Z}$:

$$a=a_0+a_1p+a_2p^2+\cdots\mapsto\varphi(a)=a_0\ \text{mód}\ p.$$

En efecto:

- φ es homomorfismo. Sean $a,b\in\mathbb{Z}_p$:
  - $\varphi(a+b)=(a_0+b_0)\ \text{mód}\ p=a_0\ \text{mód}\ p+b_0\ \text{mód}\ p=\varphi(a)+\varphi(b)$;
  - $\varphi(a\cdot b)=(a_0\cdot b_0)\ \text{mód}\ p=(a_0\ \text{mód}\ p)\cdot(b_0\ \text{mód}\ p)=\varphi(a)\cdot\varphi(b)$;
  - $\varphi(1)=1\ \text{mód}\ p=1$.
- φ es suprayectivo ya que cualquier $a\in\mathbb{Z}_p$ puede expresarse como $a_0\ \text{mód}\ p=\varphi(a)$.
- Para encontrar $\ker(\varphi)$, el núcleo de φ, partamos de la definición:

$$\ker(\varphi)=\{a\in\mathbb{Z}_p\colon\ \varphi(a)=0\}=\{a\in\mathbb{Z}_p\colon\ a_0=0\}$$

Si $b \in \ker(\varphi)$, tenemos

$$\varphi(b) = 0 = b_0 \text{ mód } p,$$

entonces

$$b = 0 + b_1 p + b_2 p^2 + \cdots = p(b_1 + b_2 p + \cdots) = pb'$$

donde $b' \in p\mathbb{Z}_p$. Por tanto

$$\ker(\varphi) = p\mathbb{Z}_p.$$

Ya que $p\mathbb{Z}_p$ es núcleo de un homomorfismo de anillos, es ideal. (véase (1) de teorema A.2.1).
Dado que para $x \in p\mathbb{Z}_p, |x|_p \leqslant \dfrac{1}{p}$, tenemos que $p\mathbb{Z}_p$ es justamente el complemento de las unidades de $\mathbb{Z}_p$:

$$p\mathbb{Z}_p = \mathbb{Z}_p \setminus \mathbb{Z}_p^\times$$

Además hemos probado que se tiene el isomorfismo $\mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}_p/p\mathbb{Z}_p$.
Por la definición 1.7.5, observamos que $\mathbb{Z}_p$ es un anillo local y $p\mathbb{Z}_p \subset \mathbb{Z}_p$ es su ideal máximo. ■

Luego

$$\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus p\mathbb{Z}_p. \tag{1.4}$$

Tenemos por la ecuación (1.3)

$$\mathbb{Z}_p^\times = S(0,1) = \{x \in \mathbb{Z}_p \colon |x|_p = 1\}.$$

Hemos probado que $p\mathbb{Z}_p$, visto como subgrupo de $\mathbb{Z}_p$, es de índice p en $\mathbb{Z}_p$. Y dada la ecuación (1.4), tenemos la siguiente descomposición de $\mathbb{Z}_p^\times$ en clases laterales disjuntas:

$$\mathbb{Z}_p^\times = (1 + p\mathbb{Z}_p) \cup (2 + p\mathbb{Z}_p) \cup \cdots \cup \big((p-1) + p\mathbb{Z}_p\big). \tag{1.5}$$

Ilustramos lo anterior en la siguiente figura para $p = 5$. La esfera $\mathbb{Z}_5^\times$ es una unión de cuatro bolas abiertas. La bola central representa el ideal máximo $5\mathbb{Z}_5$ del anillo $\mathbb{Z}_5$.

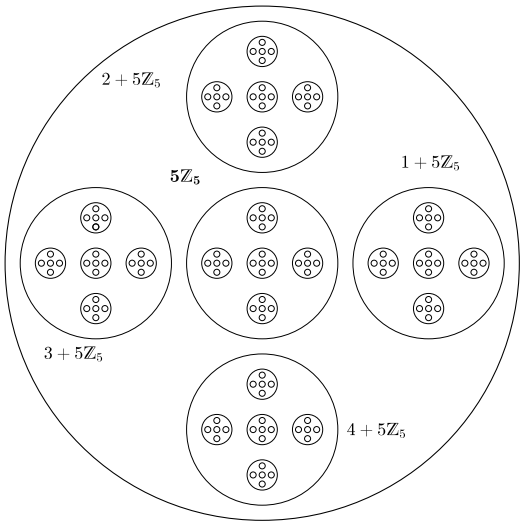

Figura 1.1: $\mathbb{Z}_5$

Observación 1.7.3. Notemos que, como en la proposición 1.7.6, tenemos morfismos $\varphi_k\colon \mathbb{Z}_p \to \mathbb{Z}/p^k\mathbb{Z}$, para toda k; dados por $\sum_{n=0}^{\infty} a_n p^n \mapsto \sum_{\nu=0}^{k-1} a_\nu p^\nu$ cuyo núcleo es el ideal $p^k\mathbb{Z}_p$.

En efecto, φ es homomorfismo de anillos y es suprayectivo ya que para todo $a \in \mathbb{Z}_p$, $\varphi_k(a)$ puede escribirse como $\sum_{\nu=0}^{k-1} a_\nu p^\nu$. Además, vemos que

$$\ker(\varphi_k) = \{a \in \mathbb{Z}_p\colon\ \varphi_k(a) = 0\} = \left\{ \sum_{n=0}^{\infty} a_n p^n\colon\ a_i = 0, i = 0, \ldots, k-1 \right\}$$
$$= \left\{ \sum_{n=k}^{\infty} a_n p^n \right\} = \left\{ p^k \sum_{\nu=0}^{\infty} a_\nu p^\nu \right\} = p^k\mathbb{Z}_p.$$

entonces el núcleo de φ_k es $\ker(\varphi_k) = p^k\mathbb{Z}_p$.

Definición 1.7.6.

- Un subconjunto K en un espacio métrico (X,d) se llama *compacto* si cualquier cubierta de K constituida por conjuntos abiertos, contiene una subcubierta finita.
- Un subconjunto K en un espacio métrico (X,d) se llama *secuencialmente compacto* si cada sucesión infinita de puntos en K contiene una subsucesión convergente a un punto en K.

De modo similar se definen espacio métrico *compacto* y *secuencialmente compacto*.

De acuerdo al *Teorema de Heine-Borel* (Rudin, 1988, teorema 2.41) estas dos propiedades son equivalentes para espacios métricos, y para $\mathbb{R}^n$ son equivalentes a la propiedad de ser cerrado y acotado.

Una propiedad útil es que una sucesión anidada de conjuntos compactos no vacíos tiene una intersección compacta no vacía.

TEOREMA 1.7.1. *Cada sucesión infinita de enteros p-ádicos tiene una subsucesión convergente.*

Demostración. Recordamos que una subsucesión $\{x_{n_k}\}$ de una sucesión $\{x_k\}$ está dada por por una sucesión de enteros positivos $\{n_k\}$ tales que $n_1 < n_2 < n_3 \cdots$.

Sea $\{x_k\}$ una sucesión en $\mathbb{Z}_p$. Cada expansión canónica de cada término es

$$x_k = \ldots a_2^k a_1^k a_0^k.$$

Dado que sólo hay una cantidad finita de posibilidades para los dígitos a_0^k (a saber, $0, 1, 2, \ldots, p-1$), podemos encontrar $b_0 \in \{0, 1, \ldots, p-1\}$ y una subsucesión infinita de $\{x_k\}$, denotada por $\{x_{0k}\}$, tal que el primer dígito de todos los x_{0k} es siempre b_0. El mismo ardid produce $b_1 \in \{0, 1, \ldots, p-1\}$ y una subsucesión $\{x_{1k}\}$ de $\{x_{0k}\}$ para la que los primeros dos dígitos son $b_1 b_0$.

Este procedimiento puede continuarse, y obtenemos $b_0, b_1, b_2, \ldots$ junto con una sucesión de subsucesiones

$$x_{00}, x_{01}, x_{02}, \ldots, x_{0s}, \ldots,$$
$$x_{10}, x_{11}, x_{12}, \ldots, x_{1s}, \ldots,$$
$$x_{20}, x_{21}, x_{22}, \ldots, x_{2s}, \ldots,$$
$$\ldots \qquad \ldots$$

tal que cada sucesión es una subsucesión de la precedente, y tales que cada elemento de la fila $(j+1)$-ésima empieza con $b_j \dots b_1 b_0$.

Para cada $j = 0, 1, \dots$ tenemos

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

Por lo tanto la sucesión diagonal $x_{00}, x_{11}, \dots$ es aún una subsucesión de la sucesión original, y obviamente converge a $\dots b_3 b_2 b_1 b_0$. ■

LEMA 1.7.3. *$\mathbb{Z}_p$ es secuencialmente compacto.*

Demostración. Por el teorema 1.7.1, $\mathbb{Z}_p$ cumple la definición 1.7.6. ■

Por lo tanto, $\mathbb{Z}_p$ es compacto, y así, también cualquier bola en $\mathbb{Q}_p$. Lo cual implica que el espacio $\mathbb{Q}_p$ es localmente compacto.

TEOREMA 1.7.2. *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 $\mathbb{Z}_p$, digamos a, la sucesión misma, que converge en $\mathbb{Q}_p$ por su completez, debe converger a a. Esto prueba la completez de $\mathbb{Z}_p$. ■

En consecuencia, podemos asociar un nuevo campo completo $\mathbb{Q}_p$ para cada número primo $p < \infty$. Así ha surgido una familia infinita de campos además del campo $\mathbb{Q}$:

$$\mathbb{Q}_2,\ \mathbb{Q}_3,\ \mathbb{Q}_5,\ \mathbb{Q}_7,\ \mathbb{Q}_{11},\ \mathbb{Q}_{13}, \dots$$

TEOREMA 1.7.3. *El conjunto $\mathbb{N}$ es denso en $\mathbb{Z}_p$.*

Demostración. Sea $x = \dots a_2 a_1 a_0 \in \mathbb{Z}_p$. Para todo $n \in \mathbb{N}$, definimos

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

Entonces $x_n \in \mathbb{N}$ y $|x - x_n|_p < p^{-n}$, y se cumple la afirmación. ■

Observación 1.7.4. Este resultado nos avisa que $\mathbb{Z}$ es denso en $\mathbb{Z}_p$.

Definición 1.7.7. X es un espacio topológico *disconexo* si puede ser representado como la unión de subconjuntos abiertos disjuntos no vacíos. Equivalentemente, no puede representarse como la unión de dos subconjuntos cerrados disjuntos no vacíos. De lo contrario X se llama *conexo* .

Por ejemplo, cualquier intervalo en $\mathbb{R}$ es conexo.

Un subconjunto C de X es conexo si es un espacio conexo con la topología inducida por X.

X es totalmente disconexo si los únicos subconjuntos conexos de X son el conjunto vacío y los puntos $\{a\}, a \in X$.

Contrario a lo que ocurre en $\mathbb{R}$, tenemos el siguiente resultado:

TEOREMA 1.7.4. *El espacio $\mathbb{Q}_p$ es totalmente disconexo.*

Demostración. Mostramos que para cualquier elemento $a \in \mathbb{Q}_p$, su componente conexa $A \subset \mathbb{Q}_p$ es igual a $\{a\}$.

Sea $a \in A$ y supongamos que $\{a\} \neq A$. Para cada $n \in \mathbb{N}$, hay un conjunto

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

que es una vecindad abierta y cerrada de a y $B(a, p^{-n}) \cap A \neq A$. Entonces tenemos

$$A = \Big(B(a, p^{-n}) \cap A\Big) \cup \Big(\big(\mathbb{Q}_p \setminus B(a, p^{-n})\big) \cap A\Big)$$

que es una unión ajena de dos subconjuntos abiertos y no vacíos.

Por lo tanto A no es conexo, lo cual es una contradicción. ■

Para mayores detalles sobre lo tratado en este capítulo puede consultarse Dunne (2011), Goldfeld and Hundley (2011), Gouvêa (1997) y Koblitz (1984).

Capítulo 2

Funciones p-ádicas

El campo de los números p-ádicos es un objeto que en varios aspectos es análogo al campo de los números reales: por ejemplo $\mathbb{Q}_p$ es un campo completo con respecto al valor absoluto p-ádico, localmente compacto y no es algebraicamente cerrado.

Todas estas similitudes sugieren que mucho de lo que usualmente se hace en $\mathbb{R}$ puede extenderse a $\mathbb{Q}_p$, en particular, las estructuras básicas del cálculo deberían aplicarse. En este capítulo tratamos el concepto de límite p-ádico y la noción de continuidad. Además, al final del capítulo estudiamos el concepto de interpolación p-ádica el cual nos permitirá construir funciones continuas a partir de una sucesión de números p-ádicos.

2.1. Límites p-ádicos

Antes de continuar veamos qué significa ser un punto de acumulación en $\mathbb{Z}_p$.

El subgrupo $\mathbb{Z}_p$ es una bola cerrada de radio 1 (proposición 1.7.5). Como la función valor absoluto p-ádico, $|\cdot|_p$ sólo toma valores en $\{p^k : k \in \mathbb{Z}\}$, entonces el conjunto $\mathbb{Z}_p$ es también una bola de radio α para cualquier $1 < \alpha < p$, así

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x| < \alpha\}.$$

Por lo tanto, $\mathbb{Z}_p$ es una vecindad abierta del cero, i.e., un subgrupo abierto. Ya que $\mathbb{Z}_p$ es secuencialmente compacto (lema 1.7.3), cada sucesión de Cauchy $\{x_j\}$ tiene un punto de acumulación en $\mathbb{Z}_p$.

En efecto, consideremos el subgrupo $p\mathbb{Z}_p$. Para todo $k \in \mathbb{N}$ el homomorfismo de grupos

$$\varphi : \mathbb{Z}_p \to \mathbb{Z}/p^k\mathbb{Z}, \quad \text{dado por} \quad \sum_{n=0}^{\infty} a_n p^n \to \sum_{\nu=0}^{k-1} a_\nu p^\nu.$$

φ es suprayectivo y tiene núcleo $p^k\mathbb{Z}_p$ (véase observación 1.7.3).

Así el *índice* $[\mathbb{Z} : p^k\mathbb{Z}_p]$ iguala al *orden* $\mathrm{ord}(\mathbb{Z}/p^k\mathbb{Z}) = p^k$. Consideremos el caso $k = 1$. En la descomposición en *clases laterales* disjuntas (ver A.1), dada por la ecuación (1.5) , $\mathbb{Z}_p = \bigcup_{i=1}^{p} (a_i + p\mathbb{Z}_p)$ existe una clase lateral que contiene a $\{x_j\}$ para una infinidad de $j \in \mathbb{N}$. De esta infinidad, hay una infinidad para los que $\{x_j\}$ se encuentra en la misma clase de módulo $p^2\mathbb{Z}_p$ y así sucesivamente. Esta sucesión descendente de clases

laterales tiene la forma

$$a+p^k\mathbb{Z}_p=\{x\in\mathbb{Z}_p\colon |x-a|_p\leqslant p^{-k}\}=\overline{B}(a,p^{-k}),$$

entonces son bolas cerradas en la métrica p-ádica cuyos radios tienden a cero. La intersección de estas bolas contiene un elemento por completez.

Así que hay un elemento $x\in\mathbb{Z}_p$ tal que para todo $n\in\mathbb{N}$; $x_j\equiv x$ mód p^n para una infinidad de j. Esto significa que x es un *punto de acumulación* en $\mathbb{Z}_p$.

Consideremos a $\mathbb{Q}_p$ con su valor absoluto $|\cdot|_p$. Al reemplazar el valor absoluto ordinario con el valor absoluto p-ádico en la definición familiar de límite, obtenemos la siguiente

Definición 2.1.1. Sea $D\subseteq\mathbb{Q}_p$ y $f\colon D\to\mathbb{Q}_p$ una función definida en D. Decimos que el *límite p-ádico* de $f(x)$ es L, cuando x tiende a x_0, si para cada $\varepsilon>0$, existe un $\delta>0$ tal que si $0<|x-x_0|_p<\delta$, entonces $|f(x)-L|_p<\varepsilon$, para todo $x\in D$. Lo denotamos $\lim\limits_{x\to x_0} f(x)=L$.

Tenemos la notación alternativa: $f(x)\to L$ cuando $x\to x_0$ $\big(f(x)$ tiende a L cuando x tiende a $x_0\big)$.

LEMA 2.1.1. *Sean* $x,x_0,y,y_0\in D\subseteq\mathbb{Q}_p$.

1. *Si* $|x-x_0|_p<\frac{\varepsilon}{2}$ y $|y-y_0|_p<\frac{\varepsilon}{2}$, *entonces* $|(x+y)-(x_0-y_0)|_p<\varepsilon$.
2. *Si* $|x-x_0|_p<\text{mín}\left\{1,\frac{\varepsilon}{2(|y_0|_p+1)}\right\}$ y $|y-y_0|_p<\frac{\varepsilon}{2(|x_0|_p+1)}$, *entonces* $|xy-x_0y_0|_p<\varepsilon$.
3. *Si* $y_0\neq 0$ y $|y-y_0|_p<\text{mín}\left\{\frac{|y_0|_p}{2},\frac{\varepsilon|y_0|_p^2}{2}\right\}$ *entonces* $y\neq 0$ y $\left|\frac{1}{y}-\frac{1}{y_0}\right|_p<\varepsilon$.

Demostración.

1. $|(x+y)-(x_0+y_0)|_p=|(x-x_0)+(y-y_0)|_p<|x-x_0|_p+|y-y_0|_p<\dfrac{\varepsilon}{2}+\dfrac{\varepsilon}{2}=\varepsilon.$

2. Dado que $|x-x_0|_p<1$ tenemos $|x|_p-|x_0|_p\leqslant|x-x_0|_p<1$, así que $|x|_p<1+|x_0|_p$. Entonces

$$\begin{aligned}|xy-x_0y_0|_p&=|xy+xy_0-xy_0-x_0y_0|_p\\&=|x(y-y_0)+y_0(x-x_0)|_p\\&\leqslant|x(y-y_0)|_p+|y_0(x-x_0)|_p\\&\leqslant|x|_p|y-y_0|_p+|y_0|_p|x-x_0|_p\\&<(1+|x_0|_p)\cdot\frac{\varepsilon}{2(|x_0|_p+1)}+|y_0|_p\cdot\frac{\varepsilon}{2(|y_0|_p+1)}\\&<\frac{\varepsilon}{2}+\frac{\varepsilon}{2}=\varepsilon.\end{aligned}$$

3. Tenemos $|y|_p-|y_0|_p\leqslant|y-y_0|_p<\frac{|y_0|_p}{2}$, así $|y|_p>\frac{|y_0|_p}{2}$. En particular, $y\neq 0$ y $\frac{1}{|y|_p}<\frac{2}{|y_0|_p}$. Entonces

$$\left|\frac{1}{y}-\frac{1}{y_0}\right|_p=\frac{|y_0-y|_p}{|y|_p|y_0|_p}<\frac{2}{|y_0|_p}\cdot\frac{1}{|y_0|_p}\cdot\frac{\varepsilon|y_0|_p^2}{2}=\varepsilon.$$

■

TEOREMA 2.1.1. *Sea $D \subseteq \mathbb{Q}_p$ y $f,g\colon D \to \mathbb{Q}_p$ funciones definidas en D. Sea x_0 un punto de acumulación de $D_{f\circ g}$ [el símbolo $\circ$ denota cualquiera de las operaciones binarias elementales (suma, resta, producto, división)]. Supongamos que existen los límites finitos $\lim_{x\to x_0} f(x) = A$, $\lim_{x\to x_0} g(x) = B$ y $B \neq 0$. Entonces*

1. $\lim_{x\to x_0} f(x) = c, \quad$ *con $f(x) = c$ una función constante,*
2. $\lim_{x\to x_0} \big(f(x)+g(x)\big) = A+B,$
3. $\lim_{x\to x_0} \big(f(x)\cdot g(x)\big) = A\cdot B,$
4. $\lim_{x\to x_0} \dfrac{1}{g(x)} = \dfrac{1}{B},$

Demostración.

1. Debemos demostrar que para cada $\varepsilon > 0$, existe un $\delta > 0$ tal que $|f(x)-c|_p = |0-0|_p = 0 < \varepsilon$ siempre que $0 < |x-x_0|_p < \delta$. Para este caso nos sirve cualquier $\delta > 0$ ya que $f(x)-c = 0$.

2. La hipótesis implica que para cada $\varepsilon > 0$ hay $\delta_1, \delta_2 > 0$ tales que, para toda $x \in D$,
   si $0 < |x-x_0|_p < \delta_1$ entonces $|f(x)-A|_p < \frac{\varepsilon}{2}$ y si $0 < |x-x_0|_p < \delta_2$ entonces $|g(x)-B|_p < \frac{\varepsilon}{2}$.
   Dado que $\frac{\varepsilon}{2} > 0$. Tomamos $\delta = \text{mín}\{\delta_1,\delta_2\} > 0$ entonces $0 < |x-x_0|_p < \delta$ (luego menor que δ_1 y menor que δ_2). Ahora usando la parte (1) del lema 2.1.1:

   $$|\big(f(x)+g(x)\big) - (A+B)|_p = |f(x)-A+g(x)-B|_p \leqslant |f(x)-A|_p + |g(x)-B|_p < \frac{\varepsilon}{2}+\frac{\varepsilon}{2} = \varepsilon.$$

   Así tenemos $\lim_{x\to x_0} \big(f(x)+g(x)\big) = A+B$.

3. Usamos la parte (2) del lema 2.1.1. Si $\varepsilon > 0$ hay $\delta_1, \delta_2 > 0$ tales que, para toda $x \in D$,

   si $0 < |x-x_0|_p < \delta_1$, entonces $|f(x)-A|_p < \text{mín}\left\{1, \dfrac{\varepsilon}{2(|B|_p+1)}\right\}$ y

   si $0 < |x-x_0|_p < \delta_2$, entonces $|g(x)-B|_p < \dfrac{\varepsilon}{2(|A|_p+1)}$.

   Sea $\delta = \text{mín}\{\delta_1,\delta_2\} > 0$, si $|x-x_0|_p < \delta$, entonces

   $|f(x)-A|_p < \text{mín}\left\{1, \dfrac{\varepsilon}{2(|B|_p+1)}\right\}$ y $|g(x)-B|_p < \dfrac{\varepsilon}{2(|A|_p+1)}$.

   Por el lema 2.1.1, $\lim_{x\to x_0} \big(f(x)\cdot g(x)\big) = A\cdot B$.

4. Finalmente, si $\varepsilon > 0$ hay un $\delta > 0$ tal que, para toda $x \in D$,

   si $0 < |x-x_0|_p < \delta_1$, entonces $|g(x)-B|_p < \text{mín}\left\{\dfrac{|B|_p}{2}, \dfrac{\varepsilon|B|_p^2}{2}\right\}$.

De acuerdo al inciso (3) del lema 2.1.1, significa que $g(x) \neq 0$ para que $\left(\frac{1}{g}\right)(x)$ tenga sentido y que

$$\left|\left(\frac{1}{g}\right)(x) - \frac{1}{B}\right|_p < \varepsilon. \qquad \blacksquare$$

Observación 2.1.1. Los siguientes resultados pueden probarse como corolarios del teorema 2.1.1:

- $\lim_{x\to x_0}\big(f(x)-g(x)\big) = A - B$;
- $\lim_{x\to x_0} \frac{f(x)}{g(x)} = \frac{A}{B}, \quad B \neq 0$;
- $\lim_{x\to x_0} h\big(f(x)\big) = h(A), \quad h(t)$ continua;
- $f(x) \leqslant g(x)$ entonces $A \leqslant B$;
- Si $A = B$ y $f(x) \leqslant h(x) \leqslant g(x)$ entonces $\lim_{x\to x_0} h(x) = A$.

2.2. Sucesiones y series

En esta sección vamos a estudiar las propiedades básicas de convergencia de sucesiones y series en $\mathbb{Q}_p$. El hecho más importante es que $\mathbb{Q}_p$ es un espacio métrico completo (véase teorema 1.7.2); de ahí la convergencia de toda sucesión de Cauchy en este campo.

Consideremos la serie $\sum_{i=1}^{\infty} a_i$ en $\mathbb{Q}_p$. Decimos que converge si sus sumas parciales $S_n = \sum_{i=1}^{n} a_i$ convergen en $\mathbb{Q}_p$ y converge *absolutamente* si $\sum_{i=1}^{n} |a_i|_p$ converge (en $\mathbb{R}$).

PROPOSICIÓN 2.2.1. *Si la serie $\sum |a_i|_p$ converge en $\mathbb{R}$, entonces $\sum a_i$ converge en $\mathbb{Q}_p$.*

Demostración. Dado que $\sum |a_i|_p$ converge, la sucesión de sus sumas parciales es de Cauchy, i.e., para cualquier $\varepsilon > 0$ existe un entero N tal que para todo n, m que satisfagan $m > n > N$, tenemos $\sum_{i=n+1}^{m} |a_i|_p < \varepsilon$.
Por la desigualdad triangular, $|S_m - S_n|_p = \left|\sum_{i=n+1}^{m} a_i\right|_p \leqslant \sum_{i=n+1}^{m} |a_i|_p < \varepsilon$, lo cual implica que $\{S_n\}$ es de Cauchy y así, la serie $\sum a_i$ converge en $\mathbb{Q}_p$. $\blacksquare$

LEMA 2.2.1. *Si $\lim_{n\to\infty} a_n = a \in \mathbb{Q}_p$ entonces: o bien $\lim_{n\to\infty} |a_n|_p = 0$ o existe un entero N tal que $|a_n|_p = |a|_p$ para todo $n \geqslant N$.*

Demostración. Esto se cumple ya que el valor absoluto p-ádico sólo toma valores discretos en el conjunto $\{p^n, n \in \mathbb{Z}\} \cup \{0\}$. $\blacksquare$

Una consecuencia de la proposición 2.2.1 es la siguiente

PROPOSICIÓN 2.2.2. *(*Principio de dominación para series convergentes*)*
Una serie $\sum_{n=1}^{\infty} a_n$ con $a_n \in \mathbb{Q}_p$ converge en $\mathbb{Q}_p$ si, y sólo si $\lim_{n\to\infty} a_n = 0$, en cuyo caso $\left|\sum_{n=1}^{\infty} a_n\right|_p \leqslant \max_n |a_n|_p$.

Demostración. La serie $\sum_{n=1}^{\infty} a_n$ converge si, y sólo si, la sucesión de sumas parciales $S_n = \sum_{i=1}^{n} a_i$ converge. Pero $a_n = S_{n+1} - S_n$. Se sigue de la proposición 2.2.1 que la serie converge si, y sólo si, a_n tiende a 0.

Ahora suponemos que $\sum_{n=1}^{\infty} a_n$ converge. Si $\sum_{n=1}^{\infty} a_n = 0$, no hay nada que probar. Si no, para cualquier suma parcial tenemos

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

por la desigualdad fuerte del triángulo, y para un N suficientemente grande tenemos

$$\max_{i \leqslant n \leqslant N} |a_n|_p \leqslant \max_{n} |a_n|_p$$

dado que a_n tiende a 0, y

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

por el lema 2.2.1 se tiene la desigualdad requerida. ■

Observación 2.2.1. Notemos que la proposición 2.2.1 es *falsa* en $\mathbb{R}$. El ejemplo clásico es la serie armónica $\sum \frac{1}{n}$ con $n \in \mathbb{Z}^+$ cuyo término general tiende a 0, pero que no converge. Otros ejemplos son $\sum \frac{\log n}{n}$ y $\sum_p \frac{1}{p}$ con p primo.

Definición 2.2.1. Una serie $\sum_{n=0}^{\infty} a_n$ converge *incondicionalmente* si ante cualquier reordenamiento de sus términos también converge.

La convergencia incondicional implica convergencia ordinaria. En $\mathbb{Q}_p$ lo inverso también es verdadero.

TEOREMA 2.2.1. *Si la serie $\sum_{n=0}^{\infty} a_n$ con $a_n \in \mathbb{Q}_p$ converge, entonces también converge incondicionalmente.*

Demostración. Supongamos que ε sea un número real arbitrario y N sea un entero tales que para cualquier $n > N$ tengamos $|a_n|_p < \varepsilon, |a'_n|_p < \varepsilon$, y

$$\left| \sum_{n=0}^{\infty} a_n - \sum_{n=0}^{N} a_n \right|_p < \varepsilon. \tag{2.1}$$

Convengamos que $S = \sum_{n=1}^{N} a_n$ y $S' = \sum_{n=1}^{N} a'_n$, y denotemos mediante S_1 y S'_1, respectivamente, las sumas de todos los términos de S para los que $|a_n|_p > \varepsilon$, y de todos los términos de S' para los cuales $|a'_n|_p > \varepsilon$. Observamos que S_1 y S'_1 tienen los mismos términos (porque estamos considerando sólo los términos con peso mayor que ε en la serie); de ahí que $S_1 = S'_1$. La suma S difiere de S_1 por los términos que satisfacen $|a_n|_p < \varepsilon$, y S' de S'_1 por los términos que satisfacen $|a'_n|_p < \varepsilon$. Por lo tanto, $|S - S_1|_p < \varepsilon$ y $|S' - S'_1|_p < \varepsilon$. Combinando esto con la desigualdad (2.1), obtenemos

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

Dado que ε tiende a 0 y N tiende a ∞, vemos que la serie $\sum_{n=1}^{\infty} a'_n$ converge y

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

■

Observación 2.2.2. En análisis real, el resultado correspondiente (Rudin, 1988, teoremas 3.54 y 3.55) sólo es verdadero si una serie converge absolutamente. Si una serie converge, pero no absolutamente, al reordenar sus términos podemos cambiar su suma y hasta hacerla convergente .

Contrariamente a los resultados anteriores tenemos el siguiente resultado que es válido para $\mathbb{R}$ y para $\mathbb{Q}_p$:

PROPOSICIÓN 2.2.3. *Existe una serie $\sum_{n=1}^{\infty} a_n$ en $\mathbb{Q}_p$ que converge pero no converge absolutamente.*

Demostración. Consideremos los siguientes términos consecutivos de la serie:

$$1, \underbrace{p, \ldots, p}_{p \text{ veces}}, \underbrace{p^2, \ldots, p^2}_{p^2 \text{ veces}}, \underbrace{p^3, \ldots, p^3}_{p^3 \text{ veces}}, \ldots$$

Estos términos tienden a 0; de ahí que la serie converge. Sin embargo,

$$\sum_{n=1}^{\infty} |a_n|_p = 1 + p \cdot p^{-1} + p^2 \cdot p^{-2} + p^3 \cdot p^{-3} + \cdots = \infty. \qquad \blacksquare$$

El siguiente resultado se refiere al cambio en el orden al sumar en series dobles, un tema sutil en el caso real.

TEOREMA 2.2.2. *Consideremos los números p-ádicos $b_{ij} \in \mathbb{Q}_p, i, j = 1, 2, \ldots,$ tales que para cualquier $\varepsilon > 0$ existe un entero $N = N(\varepsilon)$, tal que siempre que* $\max(i, j) \geqslant N$ *se cumple que $|b_{ij}| < \varepsilon$. Entonces las series*

$$\sum_i \left(\sum_j b_{ij} \right) \quad y \quad \sum_j \left(\sum_i b_{ij} \right)$$

convergen, y sus sumas son iguales.

Demostración. Por la proposición 2.2.2, la series internas $\sum_j b_{ij}$ y $\sum_i b_{ij}$ convergen (la primera para todas las i y la segunda para todas las j). Además, para todo $i \geqslant N$ tenemos

$$\left| \sum_j b_{ij} \right|_p \leqslant \max_j |b_{ij}|_p < \varepsilon,$$

y, para toda $j \geqslant N$, tenemos

$$\left| \sum_i b_{ij} \right|_p < \varepsilon.$$

Esto quiere decir que ambas series dobles convergen. Para verificar que sus sumas son iguales, escribimos

$$\left| \sum_{i=1}^{\infty} \left(\sum_{j=1}^{\infty} b_{ij} \right) - \sum_{i=1}^{N} \left(\sum_{j=1}^{N} b_{ij} \right) \right|_p = \left| \sum_{i=1}^{N} \left(\sum_{j=N+1}^{\infty} b_{ij} \right) + \sum_{i=N+1}^{\infty} \left(\sum_{j=1}^{\infty} b_{ij} \right) \right|_p < \varepsilon,$$

lo cual es ser cierto para toda ε sólo si las series son iguales. $\blacksquare$

2.3. Funciones continuas y uniformemente continuas en $\mathbb{Q}_p$

Aquí estudiaremos la noción de continuidad en el campo $\mathbb{Q}_p$. Empecemos por recordar algunas definiciones de funciones continuas entre espacios métricos.

Sean (X,d) y (Y,ρ) dos espacios métricos y una función $f\colon X \to Y$. Decimos que f es *continua* si para cada conjunto abierto $V \subset Y$ su imagen inversa $f^{-1}(V)$ es un conjunto abierto en X. Además f es *abierta* si para cada conjunto abierto U en X su imagen $f(U)$ es abierta en Y. Asimismo f es *homeomorfismo* si es continua y biyectiva con inversa continua. También f es *continua en el punto* x si para cada vecindad A de $f(x)$ en Y su imagen inversa $f^{-1}(A)$ contiene una vecindad de x. Y, finalmente f es *uniformemente continua* si para cada $\varepsilon > 0$ existe una $\delta > 0$ tal que $d(x_1,x_2) < \delta$ implica que $\rho\big(f(x_1),f(x_2)\big) < \varepsilon$.

En este contexto, se tiene la siguiente

Definición 2.3.1. Sea una función $f\colon \mathbb{Z}_p \to \mathbb{Q}_p$:

- f es *continua en el punto* $a \in \mathbb{Z}_p$ si

  $$\text{para todo } \varepsilon > 0, \text{ existe } \delta > 0 \text{ tal que } |x-a|_p < \delta \text{ implica } |f(x)-f(a)|_p < \varepsilon, \text{ para todo } x \in \mathbb{Z}_p.$$

- f es *continua* si es continua en todos los puntos $x \in \mathbb{Z}_p$.

- f es *uniformemente continua* si

  $$\text{para todo } \varepsilon > 0, \text{ existe } \delta > 0 \text{ tal que } |x-y|_p < \delta \text{ implica } |f(x)-f(y)|_p < \varepsilon, \text{ para todo } x,y \in \mathbb{Z}_p.$$

Definición 2.3.2. Sea que $E \subset \mathbb{Z}_p$, $f\colon E \to \mathbb{Q}_p$ y x_0 es un punto de acumulación de E. Diremos que $f(x)$ tiende a q cuando x tiende a x_0 (o que $\lim\limits_{x\to x_0} f(x) = q$) si existe un punto $q \in \mathbb{Q}_p$ con la siguiente propiedad: Para todo $\varepsilon > 0$ existe un $\delta > 0$ tal que $|f(x)-q|_p < \varepsilon$ para todos los puntos $x \in E$, para los cuales $0 < |x-x_0|_p < \delta$.

Lema 2.3.1. *Sea $E \subset \mathbb{Z}_p, f\colon E \to \mathbb{Q}_p$ y x_0 un punto de acumulación de E. Entonces*

$$\lim_{x\to x_0} f(x) = q \tag{2.2}$$

si, y sólo si

$$\lim_{n\to\infty} f(x_n) = q \tag{2.3}$$

para toda sucesión $\{x_n\}$ en E, tal que

$$x_n \neq x_0, \qquad \lim_{n\to\infty} x_n = x_0. \tag{2.4}$$

Demostración. Supongamos que se cumple (2.2). Elijamos $\{x_n\}$ en E, de modo que satisfaga (2.4). Sea que $\varepsilon > 0$ está dado, entonces existe $\delta > 0$, tal que $|f(x)-q|_p < \varepsilon$ si $x \in E$ y $0 < |x-x_0|_p < \delta$. Existe, además, un N tal que $n > N$ implica que $0 < |x_n - x_0|_p < \delta$. Así, para un $n > N$, tenemos $|f(x_n)-q|_p < \varepsilon$ lo que demuestra que se cumple (2.3).

Inversamente, supongamos que la ecuación (2.2) es falsa. Entonces existe algún $\varepsilon > 0$, tal que para todo $\delta > 0$ existe un punto $x \in E$ (dependiente de δ), para el cual $|f(x)-q|_p \geqslant \varepsilon$ pero $0 \leqslant |x-x_0|_p < \delta$. Al tomar $\delta_n = \frac{1}{n}$, $(n = 1,2,3,\ldots)$, hallamos una sucesión que satisface (2.4), para la cual (2.3) es falsa. ∎

Así que si f tiene un límite en x_0, este límite es único, por el lema (2.3.1) y porque si $\{x_n\}$ converge, el punto de convergencia es único.

Sea E un subconjunto de $\mathbb{Z}_p$, y sea $x_0 \in E$ un punto de acumulación de E. Listaremos algunas propiedades de las funciones continuas en E.

TEOREMA 2.3.1. *Sean* $f\colon E \to \mathbb{Q}_p$ *y* $g\colon E \to \mathbb{Q}_p$.

(1) f *es* continua *en* $x_0 \in E$ *si, y sólo si para cualquier sucesión* $\{x_n\}$*, que satisfaga* $\lim_{n\to\infty} x_n = x_0$*, tenemos*

$$\lim_{n\to\infty} f(x_n) = f(x_0).$$

(2) Si f *y* g *son continuas en* $x_0 \in E$*, entonces también lo son* $f+g, f-g$ *y* $f\cdot g$*. Si, además* $g(x_0) \neq 0$*, entonces* $\dfrac{f}{g}$ *también es continua en* x_0*.*

Demostración.

(1) se sigue al comparar las definiciones 2.3.1 y 2.3.2.

(2): en puntos aislados no hay nada qué probar. En puntos límites, la afirmación se sigue de las propiedades de límites y del inciso (1). ■

Ejemplo 2.3.1. Sea la función $f\colon \mathbb{N} \to \mathbb{Q}_p$ dada por la fórmula

$$f(x) = \frac{1}{x-c},$$

donde $c \in \mathbb{Z}_p$. Si $c \notin \mathbb{N}$, entonces el denominador no se anula en $\mathbb{N}$, y por teorema 2.3.1, f es continua en $\mathbb{N}$, pero no uniformemente continua. Sin embargo, f no está acotada en $\mathbb{N}$. En efecto, dado que c es un entero p-ádico, podemos encontrar elementos en $\mathbb{N}$ para los cuales $|x-c|_p$ es arbitrariamente pequeño, y de ahí que $|f(x)|_p$ es arbitrariamente grande. Si $c \in \mathbb{N}$, entonces f no es continua en el punto c.

Ejemplo 2.3.2. Sea $\{a_n\}$ una sucesión nula de enteros p-ádicos tales que $a_n \neq 0$ para todo n. A esta sucesión asociamos dos funciones $f_1\colon \mathbb{Z}_p \to \mathbb{Q}_p$ y $f_2\colon \mathbb{Z}_p \to \mathbb{Q}_p$ configuradas como sigue

$$f_1(x) = \begin{cases} a_x & \text{si } x \in \mathbb{N}, \\ 0 & \text{si } x \in \mathbb{Z}_p \setminus \mathbb{N} \end{cases} \qquad \text{y} \qquad f_2(x) = \begin{cases} a_x & \text{si } x \in \mathbb{N}, \\ 1 & \text{si } x \in \mathbb{Z}_p \setminus \mathbb{N} \end{cases}$$

Ambas, f_1 y f_2 son discontinuas en todos los puntos de $\mathbb{N}$. Para ver esto, tomemos $x \in \mathbb{N}$. Entonces

$$\lim_{n\to\infty} x + p^n = x \qquad \text{y} \qquad \lim_{n\to\infty} f_1(x+p^n) = \lim_{n\to\infty} a_{x+p^n} = 0.$$

Dado que la última es una subsucesión de una sucesión nula. Sin embargo, $f_1(x) = a_x \neq 0$, análogamente para f_2.

Probemos que f_1 es continua en todos los puntos $x \in \mathbb{Z}_p \setminus \mathbb{N}$. Efectivamente, tomamos cualquier sucesión $\{x_n\}$ que tienda a x, y sea $\{x_{r_n}\}$ su subsucesión contenida en $\mathbb{N}$. Entonces $\{a_{x_{r_n}}\}$ tiende a 0, por ser subsucesión de una sucesión nula, y de ahí que $f_1(x_n)$ tiende a 0.

La función $f_2(x)$ es discontinua en todos los puntos de $\mathbb{Z}_p$. Efectivamente, si $x \in \mathbb{Z}_p \setminus \mathbb{N}$, tomamos una sucesión $\{x_n\} \in \mathbb{N}$ tal que x_n tienda a n. Entonces $f(x_n) = a_{x_n}$ que tiende a 0, pero $f_2(x) = 1 \neq 0$.

Por el lema 1.7.3, $\mathbb{Z}_p$ es compacto, luego tenemos el siguiente resultado:

TEOREMA 2.3.2. *Toda función $f\colon \mathbb{Z}_p \to \mathbb{Q}_p$ continua en $\mathbb{Z}_p$ es uniformemente continua y acotada en $\mathbb{Z}_p$.*

Demostración. Sea $\varepsilon > 0$. Ya que f es continua, podemos asociar a cada punto $x \in \mathbb{Z}_p$ un número positivo $\varphi(x)$ tal que

$$x_0 \in \mathbb{Z}_p, |x-x_0|_p < \varphi(x) \quad \text{implica} \quad |f(x)-f(x_0)|_p < \frac{\varepsilon}{2}. \tag{2.5}$$

Sea $J(x)$ el conjunto de todas los $x_0 \in \mathbb{Z}_p$ para los que

$$|x-x_0|_p < \frac{1}{2}\varphi(x).$$

Dado que $x \in J(x)$, la colección de todos los conjuntos $J(x)$ es una cubierta abierta de $\mathbb{Z}_p$; y dado que $\mathbb{Z}_p$ es compacto, hay un conjunto finito de puntos $x_1, \ldots, x_n$ en $\mathbb{Z}_p$, tales que

$$\mathbb{Z}_p \subset J(x_1) \cup \cdots \cup J(x_n). \tag{2.6}$$

Establecemos

$$\delta = \text{mín}\{\varphi(x_1), \ldots, \varphi(x_n)\}.$$

Entonces $\delta > 0$ (este es un punto donde la finitud de la cubierta, inherente en la definición de compacidad, es esencial. El mínimo de un número finito de números positivos es positivo).

Ahora sea x_0 y x puntos de $\mathbb{Z}_p$, tales que $|x-x_0|_p < \delta$. Por (2.6), hay un entero $m, 1 \leqslant m \leqslant n$, tal que $x \in J(x_m)$: de ahí que

$$|x-x_m|_p < \frac{1}{2}\varphi(x_m),$$

y tenemos también

$$|x_0-x_m|_p \leqslant |x-x_0|_p + |x-x_m|_p < \delta + \frac{1}{2}\varphi(x_m) \leqslant \varphi(x_m).$$

Finalmente, (2.5) muestra, por lo tanto, que

$$|f(x)-f(x_0)|_p \leqslant |f(x)-f(x_m)|_p + |f(x_0)-f(x_m)|_p < \varepsilon. \qquad \blacksquare$$

El siguiente teorema nos será muy útil más adelante, especialmente para el caso en que $E = \mathbb{N}$; en ese caso, como lo vimos en el teorema 1.7.3, su cerradura $\overline{E}$ coincide con $\mathbb{Z}_p$.

TEOREMA 2.3.3. *Sea E un subconjunto de $\mathbb{Z}_p$ y sea $\overline{E}$ su cerradura. Sea $f : E \to \mathbb{Q}_p$ una función uniformemente continua en E. Entonces existe una única función $F\colon \overline{E} \to \mathbb{Q}_p$ uniformemente continua y acotada en $\overline{E}$ tal que*

$$F(x) = f(x) \ \ si \ \ x \in E.$$

Demostración. Sea $X \in \overline{E}$. Entonces existe una sucesión $\{x_n\}$ en E tal que

$$\{x_n\} \text{ tiende a } X \ \ \text{cuando} \ \ n \text{ tiende a } \infty. \tag{2.7}$$

(Sólo cuando $X \neq E$ es de interés) Sea f uniformemente continua en E. Elijamos dos enteros positivos s y $t(s)$ tales que:

$$|f(x)-f(x_0)|_p \leqslant p^{-s} \quad \text{si} \quad x, x_0 \in E \quad \text{y} \quad |x-x_0|_p \leqslant p^{-t}. \tag{2.8}$$

Dado que f es uniformemente continua en E, para cualquier entero s positivo existe otro entero positivo $t = t(s)$ tal que se satisface (2.8). Por (2.7) hay un entero $N = N(t)$ tal que

$$|x_n - X|_p \leqslant p^{-t} \quad \text{siempre que} \quad n \geqslant N.$$

Por lo tanto, para $n, m \geqslant N$ también tenemos

$$|x_m - x_n|_p = |(x_m - X) - (x_n - X)|_p \leqslant p^{-t},$$

y de ahí que, por (2.8),

$$|f(x_m) - f(x_n)|_p \leqslant p^{-s}.$$

Entonces $\{f(x_n)\}$ es una sucesión p-ádica de Cauchy, y como $\mathbb{Q}_p$ es completo, su límite $L = \lim_{n\to\infty} f(x_n) \in \mathbb{Q}_p$.

El límite no depende de que en la sucesión x_n tienda a x. Efectivamente, sea $\{x'_n\}$ otra sucesión tal que x'_n tiende a X. Entonces $\{x_n - x'_n\}$ será una sucesión nula, y por la continuidad uniforme de f, $\{f(x_n) - f(x'_n)\}$ también es una sucesión nula; pero esto implica además que

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

en consecuencia, la función $F : \overline{E} \to \mathbb{Q}_p$ dada por

$$F(X) = \lim_{n\to\infty} f(x_n)$$

está bien definida siempre que $X \in \overline{E}$ y $X = \lim_{n\to\infty} x_n$ y $x_n \in E$.

Ahora mostremos que la función F es uniformemente continua en $\overline{E}$. Sea X y X_0 dos puntos en $\overline{E}$ que satisfacen $|X - X_0|_p \leqslant p^{-t}$. Elijamos x y x_0 en E de modo que

$$\begin{aligned} |x - X|_p &\leqslant p^{-t}, \qquad |x_0 - X_0|_p \leqslant p^{-t}, \\ |f(x) - F(X)|_p &\leqslant p^{-s}, \qquad |f(x_0) - F(X_0)|_p \leqslant p^{-s}. \end{aligned}$$

Resulta que

$$|x - x_0|_p = |(x - X) + (X - X_0) - (x_0 - X_0)|_p \leqslant p^{-t};$$

entonces, por (2.8) tenemos $|f(x) - f(x_0)|_p \leqslant p^{-s}$. Por lo tanto,

$$|F(X) - F(X_0)|_p = \big|-\big(f(x) - F(X)\big) + \big(f(x) - f(x_0)\big) + \big(f(x_0) - F(X_0)\big)\big|_p \leqslant p^{-s},$$

que prueba la continuidad uniforme de F en $\overline{E}$.

Finalmente, F está acotada en $\overline{E}$. Efectivamente, de otra manera existiría una sucesión infinita $\{X_n\} \subset \overline{E}$ tal que

$$\lim_{n\to\infty} |F(X_n)|_p = \infty. \tag{2.9}$$

Dado que E y por consiguiente $\overline{E}$ son subconjuntos de un conjunto compacto $\mathbb{Z}_p$, existe una subsucesión $\{X_{r_n}\}$ tal que el límite

$$X_0 = \lim_{n\to\infty} X_{r_n}$$

existe. Ya que todos los puntos están en $\overline{E}$ y dado que $\overline{E}$ es un conjunto cerrado, tenemos $X_0 \in \overline{E}$. Ahora F es uniformemente continua en $\overline{E}$ y por tanto, continua en X_0. Sin embargo, esto implica que

$$\lim_{n\to\infty} F(X_{r_n}) = F(X_0),$$

lo opuesto a lo establecido en la ecuación (2.9).

Para probar la unicidad de F, suponemos que hay una segunda función F^* con las mismas propiedades. Entonces $F - F^*$ es uniformemente continua en $\overline{E}$ e idénticamente 0 en E. Dado que E es denso en $\overline{E}$; por continuidad $F - F^*$ es también idénticamente 0 en $\overline{E}$. ■

El siguiente resultado es similar al que se tiene en el análisis real.

TEOREMA 2.3.4. *Sea $E \subset \mathbb{Z}_p$. Si $\{f_n\}$ es una sucesión de funciones continuas en E y si f_n converge uniformemente a f en E, entonces f es continua en E.*

Demostración. Fijemos momentáneamente $x \in E$. Entonces $\{f_n\}_{n\geqslant 0}$ es una sucesión de Cauchy en $\mathbb{Z}_p$ y por eso converge. Denotemos $f(x) = \lim_{n\to\infty} f_n(x)$ como su límite. Esto define a la función $f\colon E \to \mathbb{Z}_p$. Tenemos que probar que esta función es continua. Pero para cada $\varepsilon > 0$ hay un $N = N_\varepsilon$ tal que

$$|f_m(y) - f_n(y)|_p \leqslant \sup_E\{|f_n(x) - f(x)|_p\} = |f_m - f_n| \leqslant \varepsilon \qquad (m,n \geqslant N, y \in E).$$

Si m tiende a ∞ inferimos que

$$|f(y) - f_n(y)|_p \leqslant \varepsilon, \qquad (n \geqslant N,\ y \in E),$$

y entonces

$$|f - f_n| = \sup_{y\in E}\{|f(y) - f_n(y)|_p\} \leqslant \varepsilon, \qquad (n \geqslant N).$$

Esto prueba que la sucesión $\{f_n\}_{\geqslant 0}$ converge *uniformemente* a f e implica la continuidad esperada. Para $a, y \in E$, escribimos

$$|f(y) - f(a)|_p \leqslant |f(y) - f_n(y)|_p + |f_n(y) - f_n(a)|_p + |f_n(a) - f(a)|_p;$$

de donde

$$|f(y) - f(a)|_p \leqslant \varepsilon + |f_n(y) - f_n(a)|_p + \varepsilon, \qquad (n \geqslant N).$$

Elijamos y fijemos un entero $n \geqslant N$. Si $a \in E$, la continuidad de la función f_n nos asegura que hay una vecindad V de a en E tal que $y \in V$ entonces

$$|f_n(y) - f_n(a)|_p \leqslant \varepsilon.$$

Esta desigualdad muestra que

$$|f(y) - f(a)|_p \leqslant 3\varepsilon \qquad (y \in V),$$

y de ahí que f es continua en cualquier punto $a \in E$. ■

Para mayores detalles sobre lo tratado en esta sección, véase Jacob and Evans (2016) y Schikhof (1984).

2.4. Funciones localmente constantes

Recordemos, de análisis real que si $f\colon (a,b) \to \mathbb{R}$ es una función continua; para cada $x \in (a,b)$ hay un $t > 0$ tal que $(x-t, x+t) \subseteq (a,b)$ y f es constante en $(x-t, x+t)$, i.e., f es *localmente constante*. Entonces f es constante en (a,b).

Lo anterior implica que no hay ejemplos interesantes de funciones localmente constantes en intervalos abiertos de $\mathbb{R}$. Sin embargo en el análisis p-ádico se tienen funciones localmente constantes no triviales. Aquí veremos algunas propiedades interesantes de dichas funciones.

Ejemplo 2.4.1. Ya que el espacio $\mathbb{Z}_p$ es totalmente disconexo (teorema 1.7.4), la *función característica* ξ de cualquier bola $U \in \mathbb{Z}_p$ dada por:

$$\xi_U(x) = \begin{cases} 0 & \text{si } x \in U, \\ 1 & \text{si } x \in \mathbb{Z}_p \setminus U, \end{cases}$$

es continua. Porque tanto la bola U como su complemento $\mathbb{Z}_p \setminus U$ son conjuntos abiertos.

Definición 2.4.1. Una función $f\colon \mathbb{Z}_p \to \mathbb{Q}_p$ es *localmente constante* si para todo $x \in \mathbb{Z}_p$ existe una vecindad abierta U_x de x; es decir, una bola de radio p^{-m} para algún $m \in \mathbb{N}$ centrada en x, $U_x = \{y \in \mathbb{Z}_p\colon |x-y|_p < p^{-m}\}$ tal que f es constante en U_x.

LEMA 2.4.1. *Las funciones localmente constantes son continuas.*

Demostración. Es claro por la definición 2.4.1 y el ejemplo 2.4.1 . ■

Ejemplo 2.4.2. Para $\alpha \in \mathbb{Z}_p$ tenemos la expansión p-ádica

$$\alpha = \alpha_0 + \alpha_1 p + \ldots + \alpha_n p^n + \ldots, \quad \text{con } \alpha_i \in \mathbb{Z}, \text{ y } 0 < \alpha_i \leqslant (p-1)$$

Definimos las funciones $f_n\colon \mathbb{Z}_p \to \mathbb{Q}_p$ por

$$f_n(\alpha) = \alpha_n, \text{ para todo } n.$$

Si remplazamos α por cualquier β con

$$|\beta - \alpha|_p < \frac{1}{p^n},$$

las f_n permanecen sin cambios y por lo tanto son localmente constantes. Y podemos extenderlas a todo $\mathbb{Q}_p$.

LEMA 2.4.2. *Sea $f\colon \mathbb{Z}_p \to \mathbb{Q}_p$ una función localmente constante. Entonces $\mathbb{Z}_p$ puede escribirse como la unión*

$$\mathbb{Z}_p = \bigcup_{i=1}^{k} U_{x_i}$$

finita de bolas disjuntas tales que la función f es constante en cada una de estas bolas. En particular, el conjunto $\{f(x)\colon x \in \mathbb{Z}_p\}$ de todos los valores que toma f en $\mathbb{Z}_p$ tienen sólo una cantidad finita de elementos distintos.

Demostración. Consideremos el conjunto de bolas U_x a partir de la definición de una función localmente constante. Esta forma una cubierta de $\mathbb{Z}_p$. Por compacidad de $\mathbb{Z}_p$, esta cubierta contiene una subcubierta finita $U_{x_1}, U_{x_2}, \ldots, U_{x_k}$. Además, por la proposición 1.7.3, inciso 5, sabemos que dos bolas en un espacio ultramétrico son disjuntas o contenidas una en la otra, así que si borramos todas las bolas que están dentro de otras bolas, obtenemos una cubierta finita de $\mathbb{Z}_p$ formada de bolas disjuntas. ■

PROPOSICIÓN 2.4.1. *Cualquier función localmente constante en $\mathbb{Z}_p$ es uniformemente continua.*

Demostración. Sea

$$\mathbb{Z}_p = \bigcup_{i=1}^{k} U_{x_i}$$

una partición de $\mathbb{Z}_p$ en bolas disjuntas como en el lema 2.4.2. Sea p^{-m_i} el radio de U_{x_i}, $i = 1,2,\ldots,k$, $m = \max\{m_i\}$ y $\delta = p^{-m}$. Probamos que para todo $\varepsilon > 0$ el δ elegido funciona. Supongamos que $|x-y|_p < \delta = p^{-m}$. Dado que $x \in U_{x_i}$ para algún i y cada punto de la bola es su centro (proposición 1.7.3), podemos suponer que $x = x_i$. Entonces $|x_i - y|_p < p^{-m_i}$ lo que significa que $f(y) = f(x_i) = f(x)$. ■

El conjunto $\mathbb{Z}_p$ contiene a $\mathbb{N}$ y a $\mathbb{Z}$ los cuales son densos en $\mathbb{Z}_p$ (teorema 1.7.3), así que algunas veces consideramos funciones de $\mathbb{N}$ a $\mathbb{Q}_p$, de $\mathbb{Z}$ a $\mathbb{Q}_p$, y más generalmente, de E a $\mathbb{Q}_p$ donde $E \subset \mathbb{Z}_p$ (teorema 2.3.3).

Definición 2.4.2. Sea $E \subset \mathbb{Z}_p$. Una función $f\colon E \to \mathbb{Q}_p$ se llama *escalonada* en E si existe un entero positivo t tal que

$$f(x) = f(x_0), \text{ para todo } x, x_0 \in E \text{ con } |x - x_0|_p \leqslant p^{-t}.$$

El entero más pequeño t para el que se cumple esta propiedad se llama *orden de* f.

Observación 2.4.1. Notamos que, a partir de la definición, que *una función escalonada es uniformemente continua y también localmente constante en E*.

Cualquier función localmente constante es una función escalonada en $\mathbb{Z}_p$ (o en cualquier otro conjunto compacto).

En análisis p-ádico, las funciones escalonadas tienen propiedades interesantes. Antes de enunciar algunas, veamos lo siguiente.

Construyamos una partición explícita de $E \subset \mathbb{Z}_p$ para un entero positivo t.

Sea $\mathbb{N}_t = \{0, 1, \ldots, p^t - 1\}$. Para cada $x \in \mathbb{Z}_p$ escribimos su expansión canónica:

$$x = x_0 + x_1 p + \ldots + x_{t-1} p^{t-1} + x_t p^t + \ldots$$

y sea

$$N_x = x_0 + x_1 p + \ldots + x_{t-1} p^{t-1} \tag{2.10}$$

Entonces $N_x \in \mathbb{N}_t$ y

$$|x - N_x|_p \leqslant p^{-t} \tag{2.11}$$

Para cada $N \in \mathbb{N}_t$ definimos $E(N) = E \cap U(N,t)$, donde

$$U(N,t) = \{x \in \mathbb{Z}_p \colon |x - N|_p \leqslant p^{-t} < p^{-t+1}\}.$$

Hemos visto que cualquier $x \in \mathbb{Z}_p$ pertenece a algún $U(N,t)$ y dado que para cualquier $N, M \in \mathbb{N}_t$ tenemos que $|N-M|_p > p^{-t}$, se sigue que las bolas $U(N,t)$ son ajenas. Por lo tanto:

$$E = \bigcup_{N=0}^{p^t-1} E(N)$$

y de aquí que $\{E(N)\}_{N\in\mathbb{N}_t}$ forman una partición de E.

TEOREMA 2.4.1. *Cualquier función escalonada sobre* $\mathbb{N}$ *o* $\mathbb{Z}_p$ *es* periódica.

Demostración. Sea $E = \mathbb{N}$ o $E = \mathbb{Z}_p$ y $f\colon E \to \mathbb{Q}_p$ una función escalonada de orden t. Consideremos la partición E:

$$E = \bigcup_{N=0}^{p^t-1} E(N)$$

Si $x, y \in E(N)$, por la desigualdad fuerte del triángulo tenemos que $|x-y|_p = |(x-N)+(N-y)|_p \leqslant p^{-t}$ y de ahí que $f(x) = f(y)$. Si $x \in E(N)$ entonces $x + p^t \in E(N)$. Por lo tanto

$$f(x+p^t) = f(x) \text{ para } x \in E,$$

lo que significa que f es periódica. ■

Observación 2.4.2. En análisis real las funciones continuas sobre intervalos cerrados pueden aproximarse uniformemente mediante funciones escalonadas. En análisis p-ádico también y las funciones escalonadas son continuas.

TEOREMA 2.4.2. *Sea* $E = \mathbb{N}$ *o* $E = \mathbb{Z}_p$. *Una función* $f\colon E \to \mathbb{Q}_p$ *es* uniformemente continua *en* E *si, y sólo si para cada entero positivo* s *existe otro entero positivo* $t = t(s)$ *y una función escalonada* $S\colon E \to \mathbb{Q}_p$ *de orden a lo más* t *tal que:*

$$|f(x) - S(x)|_p \leqslant p^{-s}, \quad \textit{para todo } x \in E \tag{2.12}$$

Demostración. Sea f uniformemente continua en E. Elijamos dos enteros positivos s y $t(s)$ tales que:

$$|f(x) - f(x_0)|_p \leqslant p^{-s} \quad \text{si} \quad x, x_0 \in E \quad \text{y} \quad |x - x_0|_p \leqslant p^{-t}. \tag{2.13}$$

Sea N_x como en la ecuación (2.10), y definamos una función $S\colon E \to \mathbb{Q}_p$ como

$$S(x) = f(N_x) \quad \text{si} \quad x \in E.$$

Entonces S es una función escalonada de orden a lo más t. Por (2.11) y (2.13),

$$|f(x) - S(x)|_p = |f(x) - f(N_x)|_p \leqslant p^{-s}.$$

Recíprocamente, supongamos que f y S satisfacen la desigualdad (2.12). Si x_0 satisface $|x - x_0| \leqslant p^{-t}$, entonces tenemos

$$S(x) = S(x_0); \qquad |f(x) - S(x)|_p \leqslant p^{-s}; \qquad |f(x_0) - S(x_0)|_p \leqslant p^{-s};$$

por lo tanto $$|f(x) - f(x_0)|_p = |\big(f(x) - S(x)\big) - \big(f(x_0) - S(x_0)\big)|_p \leqslant p^{-s},$$

lo que prueba que f es uniformemente continua. ■

2.5. Puntos de discontinuidad y el teorema de la categoría de Baire

La función f_1 del ejemplo 2.3.2 tiene una pariente cercana en el análisis real llamada *función de Riemann* $\mathscr{R} : \mathbb{R} \to \mathbb{R}$, definida por

$$\mathscr{R}(x) = \begin{cases} \dfrac{1}{q} & \text{si } x \neq 0,\ x \in \mathbb{Q},\ x = \dfrac{p}{q},\ (p,q) = 1, \\ 1 & \text{si } x = 0, \\ 0 & \text{si } x \notin \mathbb{Q}. \end{cases}$$

Esta función es continua en todos los puntos irracionales y discontinua en los racionales. La función f_2 del ejemplo 2.3.2 también tiene una análoga en análisis real

$$f(x) = \begin{cases} \dfrac{1}{q} & \text{si } x \neq 0,\ x \in \mathbb{Q},\ x = \dfrac{p}{q},\ (p,q) = 1, \\ 1 & \text{si } x = 0, \\ 1 & \text{si } x,\ x \notin \mathbb{Q}. \end{cases}$$

la cual es discontinua en todos los puntos de $\mathbb{R}$.

Otra función que es discontinua en todos los puntos de $\mathbb{R}$ es la función característica del conjunto de los números racionales o *función de Dirichlet*:

$$\xi_{\mathbb{Q}}(x) = \begin{cases} 1 & \text{si } x \in \mathbb{Q} \\ 0 & \text{si } x \notin \mathbb{Q}. \end{cases}$$

Una pregunta natural es: ¿Es posible construir una función real discontinua en todos los puntos irracionales y continua en todos los racionales, y de modo similar, una función p-ádica discontinua en todos los puntos de $\mathbb{Z}_p \setminus \mathbb{N}$ y continua en todos los puntos de $\mathbb{N}$? La respuesta es NO para ambas cuestiones. Esto se sigue del teorema de la categoría de Baire, el cual veremos en breve y que es válido para todos los espacios métricos completos.

En efecto, sea $\left(X, \rho\right)$ un espacio métrico. $\mathscr{G}$ denotará la familia de todos los subconjuntos abiertos en X, y $\mathscr{F}$, la familia de todos los subconjuntos cerrados en X. Por definición cada elemento en $\mathscr{F}$ es el complemento de un único elemento en $\mathscr{G}$ y viceversa. Recordemos que $\mathscr{G}$ es cerrado bajo uniones arbitrarias e intersecciones finitas, y $\mathscr{F}$ es cerrado bajo intersecciones arbitrarias y uniones finitas.

Definición 2.5.1. Un conjunto $A \subset X$ se llama de tipo $\mathscr{G}_\delta$ si puede representarse como una intersección numerable de conjuntos abiertos; un conjunto $A \subset X$ se llama de tipo $\mathscr{F}_\sigma$ si puede representarse como una unión numerable de conjuntos abiertos.

TEOREMA 2.5.1. *Supongamos que (X, ρ) y (Y, d) son dos espacios métricos y $f : X \to Y$ una aplicación cualquiera. Entonces el conjunto de todos los puntos donde f es continua es de tipo $\mathscr{G}_\delta$.*

Demostración. Sea $A \subset X$. Recordemos que la *oscilación* de f en A es el elemento del conjunto de los números reales extendidos $\mathbb{R} \cup \infty$ dado por

$$\omega(A) = \sup\Big\{ d\big(f(x), f(y)\big) : x, y \in A \Big\}.$$

Para $x_0 \in X$, la *oscilación de f en x_0* se define como $\omega(x_0) = \lim_{\delta \to 0} \omega\big(B(x_0, \delta)\big)$.

Observamos que si $f : X \to Y$, y $\varepsilon > 0$. Entonces el conjunto $W_\varepsilon = \{x \in X : \omega(x) < \varepsilon\}$ es abierto. En efecto, $x_0 \in W_\varepsilon$, entonces $\omega(x_0) < \varepsilon$. Esto significa que existe un $\delta > 0$ tal que para cualquier $x, y \in B(x_0, \delta)$ se cumple la desigualdad $d\big(f(x), f(y)\big) < \varepsilon_1$ para algún $\varepsilon_1 < \varepsilon$. Sea $z \in B\left(x_0, \frac{\delta}{2}\right)$. Si $z_1, z_2 \in B\left(z, \frac{\delta}{2}\right)$, entonces $z_1, z_2 \in B(z, \delta)$, y de ahí,

$$d\big(f(z_1, f(z_2)\big) < \varepsilon_1.$$

Esto muestra que $\omega\left(B\left(z, \frac{\delta}{2}\right)\right) \leqslant \varepsilon_1 < \varepsilon$. Así $\omega(z) < \varepsilon$, y W_ε es abierto.

Para concluir la prueba del teorema, observamos que

$$\{x : \omega(x) = 0\} = \bigcap_{n=1}^{\infty} W_{\frac{1}{n}} ;$$

Ya que f es continua en x_0 si, y sólo si $\omega(x_0) = 0$; el conjunto de continuidad de f es $\mathcal{G}_\delta$. ■

COROLARIO 2.5.1. *El conjunto de discontinuidad de cualquier función $f : X \to Y$ es de tipo $\mathcal{F}_\sigma$.*

Demostración. Sea $A \subset X$ el conjunto de continuidad de f, que es de tipo $\mathcal{G}_\delta$ por el teorema 2.5.1. Entonces, de acuerdo a la definición 2.5.1:

$$A = \bigcap_\alpha E_\alpha$$

El conjunto de discontinuidad de f, es el complemento de A en X;

$$A^c = X \setminus A = X \setminus \left(\bigcap_\alpha E_\alpha \right) = \left(\bigcap_\alpha E_\alpha \right)^c$$

De la teoría de los conjuntos recordemos el siguiente resultado (Rudin, 1988, teorema 2.22) :

$$\left(\bigcap_\alpha E_\alpha \right)^c = \bigcup_\alpha \left(E_\alpha^c \right)$$

Por lo tanto, el conjunto de discontinuidad de f es $\bigcup_\alpha \left(E_\alpha^c \right)$ que por la definición 2.5.1, de tipo $\mathcal{F}_\sigma$. ■

Definición 2.5.2. Un subconjunto $A \subset X$ se llama *denso* en X si su cerradura $\overline{A}$ coincide con X. Un subconjunto $A \subset X$ se llama *denso en ninguna parte* en X si $X \setminus \overline{A}$ es denso en X.

Observación 2.5.1. Se sigue inmediatamente de la definición 2.5.2 que un conjunto cerrado es denso en ninguna parte si, y sólo si, no contiene bola abierta alguna.

TEOREMA 2.5.2. *(Teorema de Baire).*

Si X es un espacio métrico completo, la intersección de toda colección numerable de subconjuntos abiertos densos de X es densa en X. En particular la intersección es no vacía (excepto en el caso trivial $X = \emptyset$).

Demostración. Supongamos que $E_1, E_2, \ldots$ son subconjuntos abiertos densos de X. Sea W un conjunto abierto en X.

Sea ρ la métrica de X; digamos

$$B(x,r) = \{y \in X : \rho(x,y) < r\}$$

y sea $\overline{B}(x,r)$ la cerradura de $B(x,r)$. [hay casos en los que $\overline{B}(x,r)$ *no* contiene a todos los y con $\rho(x,y) \leqslant r$].

Como E_1 es denso, $W \cap E_1$ es un conjunto abierto no vacío, y podemos, por lo tanto, encontrar x_1 y r_1 tales que

$$\overline{B}(x_1, r_1) \subset W \cap E_1 \quad \text{y} \quad 0 < r_1 < 1. \tag{2.14}$$

Si $n \geqslant 2$ y se han elegido x_{n-1} y r_{n-1}, la densidad de E_n muestra que $E_n \cup B(x_{n-1}, r_{n-1})$ no es vacío, y podemos, por consiguiente, encontrar x_n y r_n tales que

$$\overline{B}(x_n, r_n) \subset E_n \cap B(x_{n-1}, r_{n-1}) \quad \text{y} \quad 0 < r_n < \frac{1}{n}. \tag{2.15}$$

Por inducción este proceso genera una sucesión $\{x_n\}$ en X. Si $i > n$ y $j > n$, la construcción muestra que x_i y x_j están ambos en $B(x_n, r_n)$, de modo que $\rho(x_i, x_j) < 2r_n < \frac{2}{n}$, y, por tanto, $\{x_n\}$ es una sucesión de Cauchy. Como X es completo, existe un punto $x \in X$ tal que $x = \lim_{n\to\infty} x_n$.

Como x_i pertenece al conjunto cerrado $\overline{B}(x_n, r_n)$ si $i > n$, se deduce que x está en cada $\overline{B}(x_n, r_n)$, y (2.15) muestra que x está en cada E_n. Por (2.14), $x \in W$.

Por lo tanto $\bigcap E_n$ tiene un punto en W; $W \neq \emptyset$. ■

Tenemos el siguiente resultado:

TEOREMA 2.5.3. *Si (X, ρ) y (Y, d) dos espacios métricos y $E \subset X$ es un subconjunto denso numerable, entonces no hay funciones $f : X \to Y$ cuyo conjunto de continuidad es $X \setminus E$.*

Demostración. De acuerdo al corolario 2.5.1, es suficiente probar que el conjunto $X \setminus E$ no es de tipo $\mathcal{F}_\sigma$. Supongamos que

$$x \setminus E = \bigcup_{n=1}^{\infty} F_n,$$

donde todos los conjuntos F_n son cerrados. Entonces cada F_n es denso en ninguna parte ya que, de otra manera, por la definición de densidad, podría ser cerrado, tendría que contener una bola abierta, contradiciendo el hecho de que E es denso en X.

Ahora observamos que E es de tipo $\mathcal{F}_\sigma$ ya que es la unión de sus puntos, los cuales son cerrados y densos en ninguna parte en X. Así, tenemos expresado el espacio métrico completo X como la unión numerable de conjuntos densos en ninguna parte, lo cual contradice el teorema 2.5.2. ■

Ya que el conjunto de puntos racionales es numerable y denso en $\mathbb{R}$; tenemos inmediatamente del teorema 2.5.3, el siguiente resultado: No hay una función $f\colon \mathbb{R} \to \mathbb{R}$ que sea continua en todos los puntos racionales y discontinua en todos los puntos irracionales.

COROLARIO 2.5.2. *No hay una función $f\colon \mathbb{Z}_p \to \mathbb{Q}_p$ que sea continua en todos los puntos de $\mathbb{N}$ y discontinua en todos los puntos de $\mathbb{Z}_p \setminus \mathbb{N}$.*

Demostración. Del teorema 1.7.3, $\mathbb{N}$ es denso en $\mathbb{Z}_p$. El resultado se sigue del teorema 2.5.3. ■

2.6. Interpolación p-ádica

Sea $a_1, a_2, \ldots$ una sucesión en $\mathbb{Q}_p$; la cual puede considerarse como una función $f\colon \mathbb{N} \to \mathbb{Q}_p$ dada por $f(n) = a_n$. Dado que $\mathbb{N}$ es un subconjunto denso de $\mathbb{Z}_p$, el teorema 2.3.3 implica que existe a lo más una función *continua* $F\colon \mathbb{Z}_p \to \mathbb{Q}_p$ tal que $F(n) = f(n)$ para todo $n \in \mathbb{N}$. Si tal función existe, decimos que $\{a_n\}$ *puede ser interpolada*. (Por supuesto, una definición similar puede darse para sucesiones bilaterales $\ldots a_{-1}, a_0, a_1, \ldots$ y sucesiones tales como $a_0, a_1, \ldots$).

Si $f(n) = a_n$ es uniformemente continua en $\mathbb{N}$, se sigue directamente del teorema 2.3.3 que puede ser interpolada. A la inversa, supongamos que $f(n) = a_n$ pueda interpolarse a una función continua $F\colon \mathbb{Z}_p \to \mathbb{Q}_p$. Entonces F es uniformemente continua en $\mathbb{Z}_p$ por el teorema 2.3.2, también en $\mathbb{N}$. Entonces una sucesión $a_1, a_2, \ldots$ en $\mathbb{Q}_p$ puede interpolarse si, y sólo si, para cada ε hay un N tal que

$$|n-m|_p \leqslant p^{-N} \quad \text{implica que} \quad |a_n - a_m|_p < \varepsilon. \tag{2.16}$$

No es necesario considerar todos los enteros n, m para los cuales $|n-m|_p \leqslant p^{-N}$; es suficiente verificar (2.16) sólo para n, m que difieran por una potencia grande de p. Más precisamente, tenemos el siguiente resultado.

PROPOSICIÓN 2.6.1. *Sea $\{a_n\}, n \in \mathbb{N}$, una sucesión en $\mathbb{Q}_p$. Son equivalentes:*

(1) $\{a_n\}$ puede interpolarse;

(2) la función $f\colon \mathbb{N} \to \mathbb{Q}_p$ dada por $f(n) = a_n$ es uniformemente continua;

(3) para todo $\varepsilon \geqslant 0$ hay un N tal que

$$n = m + p^N \quad \textit{implica que} \quad |a_n - a_m|_p < \varepsilon. \tag{2.17}$$

Demostración. De la discusión anterior se desprende que (1) y (2) son equivalentes.

Mostremos la equivalencia de (2) y (3). Si $f(n) = a_n$ es uniformemente continua, entonces para cualquier $\varepsilon > 0$ hay un N para el cual se cumple (2.16). En particular se mantiene para $n = m + p^N$ ya que lo último implica que $|n-m|_p \leqslant p^{-N}$.

Mostremos que la condición (2.17) implica continuidad uniforme. Dado $\varepsilon > 0$, vamos a encontrar un N que cumpla (2.17). Sea $n, m \in \mathbb{N}$ que satisfagan $|n-m|_p \leqslant p^{-N}$. Entonces $n-m$ es divisible por p^N, así que $n = m + bp^N$ para algún $b \in \mathbb{N}$. Tenemos

$$a_n - a_m = \sum_{j=1}^{b} \left(a_{m+jp^N} - a_{m+(j-1)p^N} \right).$$

Nuestra condición (2.17) implica que el valor absoluto p-ádico de cada sumando es menor que ε. Por la desigualdad fuerte del triángulo, $|a_n - a_m|_p < \varepsilon$. ■

La siguiente proposición muestra que en cierto sentido la continuidad uniforme de la sucesión $\{a_n\}$ es una propiedad opuesta a ser una sucesión de Cauchy y nos proporciona muchos ejemplos de sucesiones que *no* son uniformemente continuas, que por lo tanto, no pueden ser interpoladas.

PROPOSICIÓN 2.6.2. *Si $\{a_n\}$ en $\mathbb{Q}_p$ es una sucesión de Cauchy no constante, entonces $\{a_n\}$ no puede ser interpolada.*

Demostración. Supongamos que $\{a_n\}$ pueda ser interpolada a una función continua $f\colon \mathbb{Z}_p \to \mathbb{Q}_p$ de modo que $f(n) = a_n$. Ya que $\mathbb{N}$ es denso en $\mathbb{Z}_p$, para cualquier $x \in \mathbb{Z}_p \setminus \mathbb{N}$ hay una sucesión de enteros $\{n_k\}$ que convergen a x. La sucesión $\{a_n\}$ es de Cauchy y por tanto converge a algún límite $c \in \mathbb{Q}_p$. Por lo tanto, a_{n_k} converge al mismo límite, y por continuidad tenemos $f(x) = \lim\limits_{k\to\infty} a_{n_k} = c$. Además, ya que $\mathbb{Z}_p \setminus \mathbb{N}$ es también denso en $\mathbb{Z}_p$, para todo $n \in \mathbb{N}$ existe una sucesión $\{x_k\} \in \mathbb{Z}_p \setminus \mathbb{N}$ tal que $n = \lim\limits_{k\to\infty} x_k$. ya probamos que $f(x_k) = c$. Pero entonces $a_n = f(n) = \lim\limits_{k\to\infty} f(x_k) = c$, i.e., $\{a_n\}$ es una sucesión constante; lo que es una contradicción. ■

PROPOSICIÓN 2.6.3. *Cualquier polinomio $P(x)$ con coeficientes en $\mathbb{Q}_p$ es una función uniformemente continua en cualquier subconjunto $E \subset \mathbb{Z}_p$.*

Demostración. Se sigue de que, en virtud del teorema 2.3.2, $f(x) = c$ y $f(x) = x$ son uniformemente continuas en cualquier $E \subset \mathbb{Z}_p$; además de que la suma, diferencia, y producto de dos funciones uniformemente continuas a partir de cualquier subconjunto $E \subset \mathbb{Z}_p$ a $\mathbb{Q}_p$ es uniformemente continua. ■

Definición 2.6.1. Sea $n \in \mathbb{N}$ y $x \in \mathbb{Z}_p$. Se define el *coeficiente binomial* p-ádico como

$$\binom{x}{n} = \frac{x(x-1)\cdots(x-n+1)}{n!}.$$

LEMA 2.6.1. *Si $x \in \mathbb{Z}_p$, $n \geqslant 0$, entonces $\binom{x}{n} \in \mathbb{Z}_p$.*

Demostración. Para cada $n \in \mathbb{N}$ consideremos

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

P_n, como cualquier polinomio, define una aplicación continua $\mathbb{Q}_p \to \mathbb{Q}_p$. Sea $x \in \mathbb{Z}_p$. Existe una sucesión $\{x_m\} \in \mathbb{N}$ tal que $x = \lim\limits_{m\to\infty} x_m$, y por la continuidad de $P_n(x)$, tenemos

$$\lim_{m\to\infty} \binom{x_m}{n} = \binom{x}{n}.$$

Dado que cada $\binom{x_m}{n}$ es un entero racional, tenemos que $\left|\binom{x_m}{n}\right|_p \leqslant 1$. De ahí que,

$$\left|\binom{x}{n}\right|_p = \lim_{m\to\infty} \left|\binom{x_m}{n}\right|_p \leqslant 1, \quad \text{i.e.,} \quad \binom{x}{n} \in \mathbb{Z}_p.$$ ■

COROLARIO 2.6.1. *La sucesión* $\{P_n(x)\} \in \mathbb{Q}_p$ *es uniformemente continua en* $\mathbb{Z}_p$

Demostración. Dado que $P_n(x) = \binom{x}{n}$ es un polinomio con coeficientes racionales, por la proposición 2.6.3 tenemos que es una función uniformemente continua en $\mathbb{Z}_p$. ■

Ahora veremos los exponentes p-ádicos. Nuestro objetivo es encontrar para qué enteros p-ádicos $a \in \mathbb{Z}_p$ la sucesión $1, a, a^2, a^3, \ldots$ puede interpolarse para producir una función "exponencial" continua $f(x) = a^x$.

Definición 2.6.2. Para todo $x \in \mathbb{Z}_p$ el límite $\lim_{n\to\infty} x^{p^n}$ existe y se denota por $\operatorname{sgn}_p(x)$ que es la *función signum*.

TEOREMA 2.6.1. *La función signum tiene las siguientes propiedades:*

(a) $\operatorname{sgn}_p(x)$ *depende sólo del primer dígito* x_0 *en la expansión p-ádica de x;*

(b) $\operatorname{sgn}_p(xy) = \operatorname{sgn}_p(x) \cdot \operatorname{sgn}_p(y)$*;*

(c) $\operatorname{sgn}_p(x) = 0$ *si* $x_0 = 0$ *y si es una raíz* $(p-1)$*-ésima de la unidad si* $x_0 \neq 0$*.*

Demostración. Sea $x_0 \in \{1, 2, \ldots p-1\}$. Primero mostremos que la sucesión $\{x^{p^n}\}$ converge. Por el Teorema de Euler-Fermat (Apostol, 1984, teorema 5.17),

$$x_0^{\varphi(p^n)} \equiv 1 \text{ mód } p^n,$$

donde φ es la función φ de Euler[1]. Observemos que, como p es primo, tenemos $\varphi(p^n) = p^n - p^{n-1}$. Así,

$$x_0^{p^n - p^{n-1}} \equiv 1 \text{ mód } p^n, \qquad x_0^{p^n} \equiv x_0^{p^{n-1}} \text{ mód } p^n,$$

y de ahí

$$\left| x_0^{p^n} - x_0^{p^{n-1}} \right|_p \leqslant \frac{1}{p^n}.$$

Dado que $1/p^n$ tiende a 0 cuando n tiende a ∞, la sucesión $\{x_0^{p^n}\}$ es de Cauchy, y por la completez de $\mathbb{Z}_p$ (lema 1.7.2), converge a un límite en $\mathbb{Z}_p$, el cual denotamos por

$$\operatorname{sgn}_p(x_0) = \lim_{n\to\infty} x_0^{p^n}.$$

El límite existe para $x_0 = 0$. Así, $\operatorname{sgn}_p(x)$ está definida para $x_0 \in \{0, 1, 2, \ldots, p-1\}$ con $\operatorname{sgn}_p(0) = 0$. Ahora mostramos que el límite existe para todo $x \in \mathbb{Z}_p$ y está definido por el primer dígito x_0 de x.

Para esto necesitamos ver que si $x \in \mathbb{Z}_p$, con su primer dígito x_0, entonces tenemos $|x^p - x_0^p|_p \leqslant p^{-1}|x - x_0|_p$. Si $x = x_0 + \alpha$, con $|\alpha|_p \leqslant p^{-1}$. Entonces

$$\begin{aligned} x^p - x_0^p &= \binom{p}{1} x_0^{p-1}\alpha + \binom{p}{2} x_0^{p-2}\alpha^2 + \cdots + \binom{p}{p}\alpha^p \\ &= (x - x_0)\left(\binom{p}{1} x_0^{p-1} + \binom{p}{2} x_0^{p-1}\alpha + \cdots + \binom{p}{p}\alpha^{p-1} \right). \end{aligned}$$

[1] Para un entero positivo m, $\varphi(m)$ es igual al número de enteros menores a m y primos relativos a m.

Dado que $\left|\binom{p}{j} x_0^{p-j}\alpha^{j-1}\right|_p \leqslant p^{-1}$ para $j \geqslant 1$; por la desigualdad fuerte del triángulo: $|x^p - x_0^p|_p \leqslant p^{-1}|x-x_0|_p$.

Aplicando lo anterior, obtenemos

$$\left|x^{p^n} - x_0^{p^n}\right|_p \leqslant p^{-1}\left|x^{p^{n-1}} - x_0^{p^{n-1}}\right|_p \leqslant \cdots \leqslant p^{-n}\,|x-x_0|_p\,,$$

lo que implica que $\lim\limits_{n\to\infty} x^{p^n}$ existe y es igual a $\lim\limits_{n\to\infty} x_0^{p^n}$. Así hemos definido $\operatorname{sgn}_p(x)$ para todo $x \in \mathbb{Z}_p$, y se satisface la propiedad (a) del teorema.

La propiedad (b) se sigue a partir de la propiedad de los límites:

$$\operatorname{sgn}_p(xy) = \lim_{n\to\infty}(xy)^{p^n} = \lim_{n\to\infty}\left(x^{p^n}\right)\left(y^{p^n}\right) = \lim_{n\to\infty} x^{p^n} \lim_{n\to\infty} y^{p^n} = \operatorname{sgn}_p(x)\cdot\operatorname{sgn}_p(y).$$

Resta mostrar que si $x_0 \in \{1,2,\ldots,p-1\}$, entonces $\operatorname{sgn}_p(x)$ es una raíz $(p-1)$-ésima de la unidad. Usando la propiedad (b) y el Pequeño Teorema de Fermat[2](Apostol, 1984, teorema 5.18), obtenemos

$$\operatorname{sgn}_p^{p-1}(x_0) = \operatorname{sgn}_p\left(x_0^{p-1}\right) = \operatorname{sgn}_p(1) = 1.$$

Los valores de $\operatorname{sgn}_p(x)$ son entonces soluciones de la ecuación $y^p - y = 0$. Ya que $\mathbb{Q}_p$ es un campo, esta ecuación no puede tener más que p soluciones en $\mathbb{Q}_p$ y de ahí, en $\mathbb{Z}_p$. Por consiguiente, las únicas soluciones de esta ecuación son los valores de la función signum. ■

TEOREMA 2.6.2. *La sucesión $1, a, a^2, \ldots$ puede interpolarse si, y sólo si, $a \in 1 + p\mathbb{Z}_p$.*

Demostración. Se sigue del teorema 2.6.1 que

(1) $\lim\limits_{n\to\infty} a^{p^n} = 1$ si, y sólo si

(2) $a \in 1 + p\mathbb{Z}_p$.

Ahora usamos la proposición 2.6.1. La sucesión $1, a, a^2, \ldots$ puede interpolarse si, y sólo si $|a^{j+p^n} - a^j|_p$ tiende a 0 uniformemente en j. Notemos que si $|a|_p < 1$, entonces la sucesión $\{a_n\}$ tiende a 0; de ahí que es una sucesión de Cauchy no constante y por la proposición 2.6.2 no puede ser interpolada. Así podemos asumir que $|a|_p = 1$. Entonces

$$|a^{j+p^n} - a^j|_p = |a|_p^j |a^{p^n} - 1|_p = |a^{p^n} - 1|_p,$$

el cual tiende a 0 uniformemente en j si, y sólo si, (1), y de ahí se cumple (2). ■

Las propiedades de la función

$$a^x = \lim_{n\to\infty} a^n, \quad x \in \mathbb{Z}_p,\ a \in 1 + p\mathbb{Z}_p,$$

serán probadas al final de esta sección (teorema 2.6.5) usando la teoría de interpolación de series de Mahler que a continuación desarrollaremos.

[2]El cual es el Teorema de Euler para $n = p$.

Definición 2.6.3. Si $f\colon \mathbb{N} \to \mathbb{Q}_p$ una sucesión de números p-ádicos.

$$f(n) = \sum_{n=-m}^{\infty} a_n p^n \quad \in \mathbb{Q}_p$$

Entonces:

(1) Los *coeficientes de interpolación* de f están definidos como las siguientes sucesiones de sumas finitas:

$$a_n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} f(n-k) = \sum_{k=0}^{n} \binom{n}{k} f(k). \tag{2.18}$$

(2) La *serie de interpolación* de f, denotada por f^*, está definida por la fórmula

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

PROPOSICIÓN 2.6.4. *Cada función $f\colon \mathbb{N} \to \mathbb{Q}_p$ admite una y sólo una representación*

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

como una serie de interpolación.

Demostración. Para probar que $f^*(x) = f(x)$ para todo $x \in \mathbb{N}$, usaremos la siguiente identidad:

$$\sum_{k=0}^{x-j} (-1)^k \binom{x-j}{k} = (1-1)^{x-j} = \begin{cases} 1 & \text{si} \quad j = k \\ 0 & \text{si} \quad 0 \leqslant j < x. \end{cases} \tag{2.19}$$

Ya que para todo $x \in \mathbb{N}$ el coeficiente binomial $\binom{x}{n} = 0$, la serie infinita para f^*

$$f^*(x) = \sum_{n=0}^{x} a_n \binom{x}{n}.$$

Al sustituir el valor del coeficiente a_n, obtenemos

$$f^*(x) = \sum_{n=0}^{x} \left(\sum_{k=0}^{n} (-1)^k \binom{n}{k} f(n-k) \right) \binom{x}{n}.$$

Al usar $j = n-k$, reescribimos $f^*(x)$ en la forma

$$f^*(x) = \sum_{j=0}^{x} f(j) \sum_{k=0}^{j+k} (-1)^k \binom{j+k}{k} \binom{x}{j+k}. \tag{2.20}$$

Sin embargo,

$$\binom{j+k}{k}\binom{x}{j+k} = \frac{(j+k)!}{k!(j+k-k)!}\cdot\frac{x!}{(j+k)!\big(x-(j+k)\big)!} = \frac{1}{k!j!}\cdot\frac{x!}{\big((x-j)-k\big)!}\cdot\frac{(x-j)!}{(x-j)!}$$

$$= \frac{x!}{j!(x-j)!}\cdot\frac{(x-j)!}{(x-j)!(x-j-k)!} = \binom{x}{j}\binom{x-j}{k}.$$

Al sustituir lo anterior en la fórmula (2.20) y si usamos (2.19), obtenemos

$$f^*(x) = \sum_{j=0}^{x} f(j)\sum_{k=0}^{j+k}(-1)^k\binom{x}{j}\binom{x-j}{k} = \sum_{j=0}^{x} f(j)\binom{x}{j}(1-1)^{x-j} = f(x)$$

si $x \in \mathbb{N}$. Para probar la unicidad, asumamos que f admite un segundo desarrollo para todo $x \in \mathbb{N}$,

$$f(x) = \sum_{n=0}^{\infty} a'_n\binom{x}{n}$$

como una serie de interpolación con coeficientes diferentes a'_n. Entonces, si establecemos para $n \in \mathbb{N}$

$$b_n = a_n - a'_n,$$

tendríamos

$$\sum_{n=0}^{\infty} b_n\binom{x}{n} = 0$$

idénticamente para $x \in \mathbb{N}$. Probaremos que $b_n = 0$ para todo $n \in \mathbb{N}$. Pues de otro modo habría al menos un índice n tal que $b_n \neq 0$ y por lo tanto habrá el menor n con esta propiedad. Pero entonces, si elegimos $x = n$, obtenemos

$$b_n\binom{n}{n} = b_n = 0,$$

lo que contradice la elección de n. ■

Ahora empecemos otra vez con una función $f\colon \mathbb{N} \to \mathbb{Q}_p$ con serie de interpolación

$$f^*(x) = \sum_{n=0}^{\infty} a_n\binom{x}{n}. \tag{2.21}$$

Sabemos que la serie (2.21) converge uniformemente en $\mathbb{Z}_p$ si, y sólo si, sus términos tienden a 0 uniformemente en $x \in \mathbb{Z}_p$, i.e.,

$$\lim_{n\to\infty} a_n\binom{x}{n} = 0. \tag{2.22}$$

El siguiente resultado nos da una condición necesaria y suficiente más simple para convergencia uniforme de la serie de interpolación.

TEOREMA 2.6.3. *La serie* $f^*(x) = \sum_{n=0}^{\infty} a_n\binom{x}{n}$ *converge uniformemente en* $\mathbb{Z}_p$ *si, y sólo si* $\{a_n\}$ *es una sucesión nula.*

Demostración. Supongamos que la serie $f^*(x) = \sum_{n=0}^{\infty} a_n \binom{x}{n}$ converge uniformemente en $\mathbb{Z}_p$. Entonces para todo entero positivo s existe un $N > 0$ tal que para cualquier $n > N$

$$\left| a_n \binom{x}{n} \right|_p \leqslant p^{-s}.$$

Para $x = n + p^r$, donde $r \in \mathbb{Z}_p$, tenemos $\lim_{r\to\infty} x = n$, y ya que $\binom{x}{k}$ es un polinomio en x y por lo tanto una función continua, concluimos que

$$\lim_{r\to\infty} \binom{x}{n} = \binom{n}{n} = 1,$$

por lo tanto $|a_n|_p \leqslant p^s$. Por lo que $\{a_n\}$ es una sucesión nula. Por el contrario, por el corolario 2.6.1,

$$\left| \binom{x}{n} \right|_p \leqslant 1.$$

Que $\{a_n\}$ sea una sucesión nula implica que la ecuación (2.22) tenga $x \in \mathbb{Z}_p$; de ahí que la serie de interpolación converge uniformemente en $\mathbb{Z}_p$. ■

El siguiente teorema pertenece a KURT MAHLER [quien da cuatro diferentes demostraciones en Mahler (1981)]. Aquí reproducimos la prueba en Ranko Bojanic (1974) que depende de estimaciones recursivas de los coeficientes de interpolación.

TEOREMA 2.6.4 (Mahler)**.** *Sea $f\colon \mathbb{N} \to \mathbb{Q}_p$ una función uniformemente continua. Entonces su serie de interpolación $f^*(x) = \sum_{n=0}^{\infty} a_n \binom{x}{n}$ converge uniformemente a una función uniformemente continua en $\mathbb{Z}_p$.*

Demostración. Por la proposición 2.6.4

$$f(x) = f^*(x) = \sum_{n=0}^{\infty} a_n \binom{x}{n}, \tag{2.23}$$

para todo $x \in \mathbb{N}$, donde a_n son los coeficientes definidos por la fórmula (2.18). Si y es otro número natural, la función $f_y(x) = f(x+y)$ es una función en $\mathbb{N}$ y como tal tiene coeficientes de interpolación $a_n(y)$ definidos por la fórmula

$$a_n(y) = \sum_{k=0}^{n} (-1)^k \binom{n}{k} f(n-k+y) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(k+y). \tag{2.24}$$

Entonces

$$f(x+y) = \sum_{n=0}^{\infty} a_n(y) \binom{x}{n} = \sum_{n=0}^{x} a_n(y) \binom{x}{n}. \tag{2.25}$$

Ahora derivaremos los valores explícitos de los coeficientes $a_n(y)$. Usamos la identidad

$$\binom{x+y}{m} = \sum_{n=0}^{m} \binom{x}{n} \binom{y}{m-n}$$

y la serie de interpolación para $f(x)$, obtenemos

$$f(x+y) = \sum_{m=0}^{\infty} a_m \binom{x+y}{m} = \sum_{m=0}^{\infty} a_m \sum_{n=0}^{m} \binom{x}{n}\binom{y}{m-n}$$

$$= \sum_{n=0}^{\infty} \binom{x}{n} \sum_{m=n}^{\infty} a_m \binom{y}{m-n} = \sum_{n=0}^{\infty} \binom{x}{n} \sum_{k=0}^{\infty} a_{n+k} \binom{y}{k}$$

a partir de lo cual, por la unicidad de las series de interpolación (proposición 2.6.4), obtenemos la expresión

$$a_n(y) = \sum_{k=0}^{\infty} a_{n+k} \binom{y}{k}. \tag{2.26}$$

Al comparar (2.24) y (2.25), obtenemos la identidad

$$\sum_{k=0}^{\infty} a_{n+k} \binom{y}{k} = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(k+y).$$

Ya que f es uniformemente continua, para todo $s > n$ podemos encontrar un t tal que

$$x = y + p^t \quad \text{entonces} \quad |f(x) - f(y)|_p \leqslant p^{-s}.$$

Ya que $\mathbb{N}$ es un subconjunto del conjunto compacto $\mathbb{Z}_p$, por el teorema 2.3.3, f es acotada, y podemos asumir sin pérdida de generalidad que

$$|f(x)|_p \leqslant 1.$$

A partir de (2.18), (2.23) y ya que los coeficientes binomiales están en $\mathbb{Z}_p$, así como $(-1)^n$, podemos establecer las siguientes desigualdades:

$$\max_{0\leqslant n\leqslant x} |a_n|_p \leqslant \max_{0\leqslant n\leqslant x} |f(n)|_p \quad \text{y} \quad \max_{0\leqslant n\leqslant x} |f(n)|_p \leqslant \max_{0\leqslant n\leqslant x} |a_n|_p.$$

Al igualarlas y haciendo tender n al infinito, obtenemos que

$$\sup_{n\in\mathbb{N}} |a_n|_p = \sup_{n\in\mathbb{N}} |f(n)|_p.$$

De ahí, $|a_n|_p \leqslant 1$. Ahora al aplicar el corolario 2.5.1 con $y = p^t$, tenemos

$$\sum_{k=0}^{p^t} a_{n+k} \binom{p^t}{k} = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(k+p^t)$$

$$= a_n + \sum_{k=1}^{p^t-1} a_{n+k} \binom{p^t}{k} + a_{n+p^t}$$

Al sustituir $a_n = \displaystyle\sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(k)$ en la última ecuación, obtenemos:

$$a_{n+p^t} = -\sum_{k=1}^{p^t-1} a_{n+k} \binom{p^t}{k} + \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} \big(f(k+p^t) - f(k)\big).$$

Dado que cada coeficiente binomial en la primera suma es divisible entre p, por la desigualdad fuerte del triángulo,

$$|a_{n+p^t}|_p \leqslant \text{máx}\{pp^{-1}|a_{n+1}|_p, p^{-1}|a_{n+2}|_p, \ldots, p^{-1}|a_{n+p^t-1}|_p, p^{-s}\}.$$

Concluimos que si $m \geqslant p^t$, entonces

$$|a_m|_p \leqslant p^{-1}.$$

Ahora establezcamos otra estimación, basada en la previa y asumiendo que $m \geqslant p^t$,

$$|a_{m+p^t}|_p \leqslant \text{máx}\{p^{-1}|a_{m+1}|_p, p^{-1}|a_{m+2}|_p, \ldots, p^{-1}|a_{m+p^t-1}|_p, p^{-s}\}.$$

Sin embargo, dado que ya encontramos que $|a_m|_p \leqslant p^{-1}$, concluimos que los términos con índice mayor que $2p^t$ tienen valor absoluto a lo más p^{-2}. Repetimos el proceso hasta que tengamos el estimado

$$|a_n|_p \leqslant p^{-s} \quad \text{si} \quad n \geqslant sp^t.$$

Ya que s puede elegirse arbitrariamente grande, $\{a_n\}$ es una sucesión nula. De ahí que, por el teorema 2.6.3, la serie de interpolación

$$\sum_{n=0}^{\infty} a_n \binom{x}{n}$$

converge uniformemente en $\mathbb{Z}_p$. Ya que los términos de esta serie son polinomios en x y por ello funciones continuas, se sigue del teorema 2.3.4 que la serie es continua en $\mathbb{Z}_p$ y por tanto, uniformemente continua en este conjunto compacto. ■

En el contexto p-ádico, una consecuencia del teorema anterior es el análogo al Teorema de Aproximaciones de Weierstrass (Rudin, 1976, teorema 7.26):

COROLARIO 2.6.2. *Cualquier función uniformemente continua $f : \mathbb{N} \to \mathbb{Q}_p$ (o $F : \mathbb{Z}_p \to \mathbb{Q}_p$) puede aproximarse uniformemente por polinomios.*

Demostración. Es suficiente probar la afirmación para la función F. Ya que f, la restricción de F a $\mathbb{N}$, será también uniformemente continua. Probamos en el teorema 2.6.4 que la serie de interpolación para f, $\sum_{n=0}^{\infty} a_n \binom{x}{n}$, converge uniformemente en $\mathbb{Z}_p$ a una función uniformemente continua que extiende a f y por unicidad en el teorema 2.3.3, debe ser igual a F. Sin embargo, esto significa que las sumas parciales

$$\sum_{n=0}^{N} a_n \binom{x}{n}$$

convergen uniformemente a F cuando N tiende a infinito. El resultado se tiene ya que cada suma parcial es un polinomio. ■

Como una aplicación de la teoría de las series de interpolación, estudiaremos la función a^x como una interpolación de la sucesión $1, a, a^2, a^3, \ldots$.

TEOREMA 2.6.5. *La función a^x tiene las siguientes propiedades: para todo $x, y \in \mathbb{Z}_p$ y cualquier $a \in 1 + p\mathbb{Z}_p$*

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

(2) $a^x \in 1 + p\mathbb{Z}_p$,

(3) $a^{x+y} = a^x a^y$,

(4) $a^{-x} = (a^x)^{-1}$.

Demostración.

(1) La función a^x es uniformemente continua en $\mathbb{Z}_p$ y por lo tanto puede representarse por una serie de interpolación. Los coeficientes de interpolación a_n están dados por la fórmula

$$a_n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} a^{n-k} = (1-a)^n;$$

por lo tanto

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

(2) Reescribimos $a^x = 1 + \sum_{n=1}^{\infty} (1-a)^n \binom{x}{n}$, y dado que para $n > 0$, $(1-a)^n \in p\mathbb{Z}_p$, entonces $a^x \in 1 + p\mathbb{Z}_p$.

(3) Mediante la fórmula de suma (2.25),

$$a^{x+y} = \sum_{k=0}^{\infty} a_{n+k} \binom{y}{k} = \sum_{k=0}^{\infty} (a-1)^{n+k} \binom{y}{k} = (a-1)^n a^y,$$

donde los coeficientes $a_n(y)$ están dados por la fórmula (2.26):

$$a_n(y) = \sum_{k=0}^{\infty} a_{n+k} \binom{y}{k} = \sum_{k=0}^{\infty} (a-1)^{n+k} \binom{y}{k} = (a-1)^n a^y,$$

Y así, obtenemos $a^{x+y} = a^x a^y$.

(4) Tomemos $y = -x$:

Por un lado tenemos que $a^{x-x} = a^0 = 1$; por otro lado, si usamos la propiedad (3): $a^{x-x} = a^x a^{-x}$, entonces $a^x a^{-x} = 1$. Por lo tanto $a^{-x} = \dfrac{1}{a^x} = (a^x)^{-1}$. ■

Mayores detalles de lo visto en este capítulo en (Katok, 2007, cap. 2 y 4).

Capítulo 3

Cálculo diferencial p-ádico

El objetivo de este capítulo es estudiar la noción de derivada en el contexto p-ádico, que es pieza clave en el presente trabajo. Así como la teoría de series infinitas, que usamos para construir funciones p-ádicas diferenciables en $\mathbb{Q}_p$.

Al final del capítulo revisamos las funciones logaritmo y exponencial p-ádicas.

3.1. La derivada p-ádica

La derivada de una función p-ádica es análoga a la del análisis real, excepto que ahora el límite en su definición se entiende en el sentido p-ádico.

Un resultado útil es el siguiente

LEMA 3.1.1. *Si p un número primo y $n \in \mathbb{N}$, entonces, tenemos el siguiente límite en $\mathbb{Q}_p$,*

$$\lim_{n\to\infty} p^n = 0.$$

Demostración. Tenemos que $\left\{p^n\mathbb{Z}_p\right\}_{n=0}^{\infty}$ es una base de vecindades de p^n y de 0. Por lo tanto ambos están contenidos en cada una de las bolas $p^n\mathbb{Z}_p$ abiertas cada vez más pequeñas mientras n crece. Es decir, que para toda $\varepsilon > 0$ existe $N \in \mathbb{N}$ tal que $|p^n - 0|_p < \varepsilon$ para toda $n \geqslant N$. Entonces p^n tiende a cero. ■

Observación 3.1.1. Sea $y \in \mathbb{Q}$, sabemos que $|y|_p = p^{-n} = \dfrac{1}{p^n}$, para algún $n \in \mathbb{Z}$. Tenemos que $|y|_p$ tiende a cero, si, y sólo si n tiende a ∞.

Definición 3.1.1. Sea $U \subset \mathbb{Q}_p$ un conjunto abierto, y sea $f\colon \mathbb{Q}_p \to \mathbb{Q}_p$ una función. Decimos que f es *diferenciable* en un punto de acumulación $x \in U$ (sección 2.1) si existe el siguiente *límite p-ádico.*

$$f'(x) = \lim_{|y|_p\to 0} \frac{f(x+y) - f(x)}{y}$$

o equivalentemente, por la observación 3.1.1:

$$f'(x) = \lim_{n\to\infty} \frac{f(x+p^n) - f(x)}{p^n}.$$

Si existe $f'(x)$ para cada $x \in U$, decimos que f es diferenciable en U, y escribimos $f'(x)\colon U \to \mathbb{Q}_p$ para la función que a cada $x \in U$ le asocia $f'(x)$, la cual llamaremos *derivada* de f.

LEMA 3.1.2. *Las funciones diferenciables son continuas en $\mathbb{Q}_p$.*

Demostración. Supongamos que f es diferenciable en el punto $a \in \mathbb{Q}_p$. Entonces existe $f'(a)$:
Por definición:

$$f'(a) = \lim_{|y|_p \to 0} \frac{f(a+y) - f(a)}{y};$$

entonces

$$f'(a) \cdot \lim_{|y|_p \to 0} y = \frac{\lim\limits_{|y|_p \to 0} f(a+y) - f(a)}{\lim\limits_{|y|_p \to 0} y} \cdot \lim_{|y|_p \to 0} y$$

$$0 = \lim_{|y|_p \to 0} f(a+y) - f(a);$$

de ahí que

$$f(a) = \lim_{|y|_p \to 0} f(a+y);$$

si $x = a+y$; $y = x-a$

$$f(a) = \lim_{|x-a|_p \to 0} f(x)$$

es decir, por el lema 3.1.1

$$f(a) = \lim_{x \to a} f(x),$$

Por lo tanto f es continua en a. ■

Reglas de derivación p-ádica

Las conocidas reglas del análisis real (véase Spivak (2008)) sobre las derivadas de una suma, diferencia, producto, cociente o composición de dos funciones; tienen sus análogos para funciones de variable p-ádica. Además, las pruebas son esencialmente las mismas, excepto que los límites reales deben reemplazarse por los límites p-ádicos.

TEOREMA 3.1.1. *Sean $f, g\colon \mathbb{Z}_p \to \mathbb{Q}_p$ dos funciones que en algún punto $x \in \mathbb{Z}_p$ tienen las derivadas $f'(x)$ y $g'(x)$, respectivamente. Entonces,*

1. *La derivada de una función constante $f(x) = c$ es $f'(x) = 0$,*
2. *La derivada de una función identidad $f(x) = x$ es $f'(x) = 1$,*
3. *La derivada de $(f+g)(x)$ es $f'(x) + g'(x)$,*
4. *La derivada de $(f \cdot g)(x)$ es $f'(x)g(x) + f(x)g'(x)$,*
5. *La derivada de $\left(\frac{f}{g}\right)(x)$ es $\frac{f'(x)g(x) - f(x)g'(x)}{g^2(x)}$.*
6. *La derivada de $f(x) = x^n$, para algún $n \in \mathbb{N}$ es $f'(x) = nx^{n-1}$.*

Demostración.

1. Por definición: $f'(x) = \lim\limits_{|y|_p \to 0} \dfrac{f(x+y)-f(x)}{y} = \lim\limits_{|y|_p \to 0} \dfrac{c-c}{y} = 0.$

2. Por definición: $f'(x) = \lim\limits_{|y|_p \to 0} \dfrac{f(x+y)-f(x)}{y} = \lim\limits_{|y|_p \to 0} \dfrac{x+y-x}{y} = \lim\limits_{|y|_p \to 0} \dfrac{y}{y} = 1.$

3. Por definición

$$\begin{aligned}(f+g)'(x) &= \lim_{|y|_p \to 0} \frac{(f+g)(x+y)-(f+g)(x)}{y} \\ &= \lim_{|y|_p \to 0} \frac{f(x+y)+g(x+y)-f(x)-g(x)}{y} \\ &= \lim_{|y|_p \to 0} \frac{f(x+y)-f(x)+g(x+y)-g(x)}{y} \\ &= \lim_{|y|_p \to 0} \frac{f(x+y)-f(x)}{y} + \lim_{|y|_p \to 0} \frac{g(x+y)-g(x)}{y} \\ &= f'(x)+g'(x).\end{aligned}$$

   Así, $(f+g)'(x) = f'(x)+g'(x)$.

4. Por definición

$$\begin{aligned}(fg)'(x) &= \lim_{|y|_p \to 0} \frac{(fg)(x+y)-(fg)(x)}{y} \\ &= \lim_{|y|_p \to 0} \frac{f(x+y)g(x+y)-f(x)g(x)}{y} \\ &= \lim_{|y|_p \to 0} \frac{\big(f(x+y)-f(x)+f(x)\big)g(x+y)-f(x)g(x)}{y} \\ &= \lim_{|y|_p \to 0} \frac{\big(f(x+y)-f(x)\big)g(x+y)+f(x)g(x+y)-f(x)g(x)}{y} \\ &= \lim_{|y|_p \to 0} \frac{\big(f(x+y)-f(x)\big)g(x+y)+f(x)\big(g(x+y)-g(x)\big)}{y} \\ &= \lim_{|y|_p \to 0} g(x+y)\frac{f(x+y)-f(x)}{y} + \lim_{|y|_p \to 0} f(x)\frac{g(x+y)-g(x)}{y} \\ &= \lim_{|y|_p \to 0} g(x+y) \lim_{|y|_p \to 0} \frac{f(x+y)-f(x)}{x} + f(x) \lim_{|y|_p \to 0} \frac{g(x+y)-g(x)}{y} \\ &= g(x)f'(x)+f(x)g'(x).\end{aligned}$$

   Asi, $(fg)'(x) = g(x)f'(x)+f(x)g'(x)$.

5. Suponiendo que $g(x) \neq 0$ y por continuidad de g en x, también $g(x+y) \neq 0$ para todo $|y|_p$ suficientemente pequeño. Por definición,

$$\begin{aligned}
\left(\frac{f}{g}\right)'(x) &= \lim_{|y|_p \to 0} \frac{\left(\frac{f}{g}\right)(x+y) - \left(\frac{f}{g}\right)(x)}{y} \\
&= \lim_{|y|_p \to 0} \frac{\frac{f(x+y)}{g(x+y)} - \frac{f(x)}{g(x)}}{y} \\
&= \lim_{|y|_p \to 0} \frac{g(x)f(x+y) - f(x)g(x+y)}{g(x+y)g(x)y} \\
&= \lim_{|y|_p \to 0} \frac{g(x)f(x+y) - g(x)f(x) + f(x)g(x) - f(x)g(x+y)}{g(x+y)g(x)y} \\
&= \lim_{|y|_p \to 0} \frac{g(x)\big(f(x+y) - f(x)\big) - f(x)\big(g(x+y) - g(x)\big)}{g(x+y)g(x)y} \\
&= \frac{1}{g(x)} \lim_{|y|_p \to 0} \frac{1}{g(x+y)} \left(g(x)\frac{f(x+y) - f(x)}{y} - f(x)\frac{g(x+y) - g(x)}{y} \right) \\
&= \frac{1}{g(x)g(x)} \left(g(x) \lim_{|y|_p \to 0} \frac{f(x+y) - f(y)}{y} - f(x) \lim_{|y|_p \to 0} \frac{g(x+y) - g(x)}{y} \right) \\
&= \frac{1}{g^2(x)} \big(g(x)f'(x) - f(x)g'(x) \big) \\
&= \frac{g(x)f'(x) - f(x)g'(x)}{g^2(x)}.
\end{aligned}$$

   Así, $\left(\frac{f}{g}\right)'(x) = \frac{g(x)f'(x) - f(x)g'(x)}{g^2(x)}$.

6. Procedemos por inducción sobre n.

   Para $n = 1$: Por (2): $f'(x^1) = f'(x) = 1 = 1(x)^{1-1}$.

   Suponemos $f'(x) = nx^{n-1}$ para todo $n \in \mathbb{N}$.

   Sea $g(x) = x^{n+1}$, que podemos expresar como $g(x) = x^n \cdot x$.

   Por (4): $g'(x) = (x^n)(1) + x(nx^{n-1}) = x^n + nx^n = (n+1)x^{(n+1)-1}$

   Es decir, $g'(x) = (n+1)x^{(n+1)-1}$, que es el caso para $n+1$. ■

TEOREMA 3.1.2 (Regla de la cadena)**.** *Sean $f\colon \mathbb{Z}_p \to \mathbb{Q}_p, g\colon \mathbb{Z}_p \to \mathbb{Z}_p$ funciones diferenciables en los puntos $g(x), x \in \mathbb{Z}_p$. La derivada de una función compuesta $h = f(g)$ está dada $h'(x) = f'\big(g(x)\big)g'(x)$.*

Demostración. Notemos que hemos supuesto que g mapea a $\mathbb{Z}_p$ en sí mismo para que esté definida la función composición,

$$h(x) = f\big(g(x)\big) \quad \text{para} \quad x \in \mathbb{Z}_p$$

Distinguimos dos casos:

1. Puede existir una sucesión infinita $\{y_n\}$ de puntos distintos de $\mathbb{Z}_p$ con el límite x tales que

$$g(y_n) = g(x) \qquad (n = 1,2,3,\ldots),$$

y por lo tanto también

$$h(y_n) = h(x) \qquad (n = 1,2,3,\ldots),$$

Por la existencia de $g'(x)$ esto sólo puede suceder si $g'(x) = 0$, y si h es diferenciable en x, se sigue que también $h'(x) = 0$.

2. En segundo lugar, si y tiende a x de forma tal que siempre $g(x) = g(y)$, entonces, por definición,

$$h'(x) = \lim_{|y|_p \to 0} \frac{h(x+y) - h(x)}{y}$$

$$= \lim_{|y|_p \to 0} \frac{f\big(g(x+y)\big) - f\big(g(x)\big)}{y} \cdot \frac{g(x+y) - g(x)}{g(x+y) - g(x)}$$

$$= \lim_{|y|_p \to 0} \frac{f\big(g(x+y)\big) - f\big(g(x)\big)}{g(x+y) - g(x)} \cdot \lim_{|y|_p \to 0} \frac{g(x+y) - g(x)}{y}$$

Por la existencia supuesta de $f'\big(g(x)\big)$ y $g'(x)$:

$$h'(x) = f'\big(g(x)\big)g'(x)$$

Este límite es 0 si $g'(x) = 0$; justo como encontramos para las sucesiones $\{y_n\}$ en el primer caso. ■

3.2. $\mathbb{Q}_p$ comparado con $\mathbb{R}$

Ciertos autores afirman que las derivadas son poco importantes en el contexto p-ádico, a diferencia de las integrales. (Gouvêa, 1997, pág. 87 párrafo 3). Una razón es que el teorema del valor medio, el cual es el eje de la teoría elemental de las funciones diferenciables en $\mathbb{R}$; falla en $\mathbb{Q}_p$. El teorema clásico dice que dados a y b en el dominio de una función diferenciable, existe un número ε "entre" a y b tal que

$$f(b) - f(a) = f'(\varepsilon)(b-a).$$

El problema en el mundo p-ádico es que la noción de "entre" no tiene sentido, dado que $\mathbb{Q}_p$ no es un campo ordenado. Sin embargo, recordemos que en $\mathbb{R}$ podemos redefinir la noción de "entre" diciendo que ε está entre a y b si tenemos que

$$\varepsilon = at + b(1-t) \text{ para } 0 \leqslant t \leqslant 1.$$

Concretamente, lo que el teorema del valor medio p-ádico debería decir es lo siguiente:

Si una función $f(x)$ es diferenciable con derivada continua en $\mathbb{Q}_p$, entonces, para cualesquiera dos números a,b en $\mathbb{Q}_p$, existe un elemento $\varepsilon \in \mathbb{Q}_p$ de la forma

$$\varepsilon = at + b(1-t) \text{ para algún } t, |t|_p \leqslant 1$$

para el cual tenemos

$$f(b)-f(a)=f'(\varepsilon)(b-a).$$

Sin embargo, el "teorema del valor medio p-ádico" como lo acabamos de establecer es falso. En efecto, veamos el siguiente

Ejemplo 3.2.1. Tomemos la siguiente función p-ádica: $f(x)=x^p-x, a=0, b=1$. Entonces $f'(x)=px^{p-1}-1$ y $f(a)=f(b)=0$. Si el teorema de valor medio fuera válido en el contexto p-ádico; éste implicaría que existe un ε de la forma anterior tal que $p\varepsilon^{p-1}-1=0$. Pero cualquier $\varepsilon=at+b(t-1)=(1-t)$ con $t\in\mathbb{Z}_p$ (lo que dice $|t|_p\leqslant 1$) debe pertenecer a $\mathbb{Z}_p$. Pero entonces $p\varepsilon^{p-1}-1$ es claramente una unidad en $\mathbb{Z}_p$ (pertenece a $1+\mathbb{Z}_p$); y por lo tanto no puede ser cero.

Asimismo, el teorema de la función inversa falla en $\mathbb{Q}_p$. Recordemos dicho teorema en el contexto real.

TEOREMA 3.2.1 (Teorema de la función inversa)**.** *Sea $U\subseteq\mathbb{R}$ abierto y sea $f\colon U\to\mathbb{R}$ de clase C^1 (f es continua con derivada continua). Si $f'(a)\neq 0$ para algún $a\in U$ entonces f es un difeomorfismo (aplicación biyectiva diferenciable con inversa diferenciable) en a.*

Tratando de imitar el caso real, el "teorema de la función inversa p-ádico" diría lo siguiente.

Sea $D\subseteq\mathbb{Q}_p$ abierto y sea $f\colon D\to\mathbb{Q}_p$ de clase C^1. Si $f'(x_0)\neq 0$ para algún $x_0\in D$ entonces f es un difeomorfismo (aplicación biyectiva diferenciable con inversa diferenciable) en x_0.

Sin embargo, tenemos el siguiente resultado.

PROPOSICIÓN 3.2.1. *Existe una aplicación continuamente diferenciable $f'\colon\mathbb{Z}_p\to\mathbb{Q}_p$ con derivada no nula en ninguna parte la cual no es inyectiva en ninguna vecindad de $0\in\mathbb{Z}_p$.*

Demostración. Para cada $n\in\mathbb{N}$, sea

$$B_n:=B(p^n,p^{-2n})=\left\{x\in\mathbb{Z}_p\colon |x-p^n|_p<p^{-2n}\right\}\subset\mathbb{Z}_p \tag{3.1}$$

Ya que $x\in B_n$ implica que $|x|_p=p^{-n}$ tenemos $B_n\cap B_m=\emptyset$ siempre que $n\neq m$. Definimos $f\colon\mathbb{Z}_p\to\mathbb{Q}_p$:

$$f(x)=\begin{cases}x-p^{2n} & \text{si } x\in B_n\\ x & \text{si } x\in\mathbb{Z}_p\setminus\bigcup\limits_{n\in\mathbb{N}}B_n.\end{cases}$$

Entonces $f(p^n)=p^n-p^{2n}$ ya que $p^n\in B_n$. Pero p^n-p^{2n} no pertenece a ningún B_m. Por lo tanto $f(p^n-p^{2n})=p^n-p^{2n}$ y f no es inyectiva en ninguna vecindad de $0\in\mathbb{Z}_p$.

En cuanto a la diferenciabilidad, consideremos $g(x):=x-f(x)$. Nuestro objetivo es mostrar que g' existe y se anula en todas partes en cuyo caso $g'(x)=1$. Para empezar, $g(x)$ es localmente constante en $\mathbb{Z}_p\setminus\{0\}$ y de ahí tenemos la derivada $g'(x)=0$ en $\mathbb{Z}_p\setminus\{0\}$. Resta verificar que $g'(0)=0$. Pero

$$\left|\frac{f(x)-f(0)}{x}\right|_p=\begin{cases}\dfrac{|p^{2n}|_p}{|x|_p}=p^n & x\in B_n\\ 0 & x\in\mathbb{Z}_p\setminus\bigcup\limits_{n\in\mathbb{N}}B_n,\end{cases}$$

de ahí la afirmación. ■

No obstante podemos encontrar ejemplos de funciones diferenciables interesantes.

Ejemplo 3.2.2. Sea $E \subset \mathbb{Z}_p$ un subconjunto sin puntos aislados y sea f una función localmente constante en E. Entonces para cada $a \in E$ existe un $\varepsilon > 0$ tal que si $x \in E$ satisface $|a-x|_p < \varepsilon$, entonces $f(x) = f(a)$. Así

$$\frac{f(x)-f(a)}{x-a} = 0 \qquad \text{si} \qquad |a-x|_p < \varepsilon;$$

de ahí que f, (que puede no ser constante) es diferenciable en E y $f'(a) = 0$ para todo $a \in E$.

Así, hay muchas funciones no constantes cuyas derivadas son idénticamente cero. Esto en contraste con el análisis real y con las funciones analíticas (funciones dadas por series de potencias).

Ejemplo 3.2.3. Sea $f(x) = \sum_{n=0}^{\infty} a_n x^n$, $x \in \mathbb{R}$, y sea E su región de convergencia. Efectivamente, si f' es idénticamente 0, entonces todas sus derivadas son idénticamente 0 y todos los coeficientes de la serie de potencias a_k se anulan para $k \geqslant 1$, así, $f(0) = a_0$, una constante.

El conjunto de funciones *pseudo-constantes*, i.e., $\{f\colon \mathbb{Z}_p \to \mathbb{Q}_p\colon f' = 0\}$, contiene funciones localmente constantes.

El siguiente resultado destruye la conjetura natural de que todas las funciones pseudo-constantes son localmente constantes.

LEMA 3.2.1. *Existe una función inyectiva (y por tanto, que no es localmente constante) $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ cuya derivada es cero.*

Demostración. Sea $x = \sum_{n=0}^{\infty} a_n p^n \in \mathbb{Z}_p$, y establezcamos $f(x)\colon \mathbb{Z}_p \to \mathbb{Z}_p$ como $f(x) = \sum_{n=0}^{\infty} a_n p^{2n}$, i.e.,

$$f\colon \sum_{n=0}^{\infty} a_n p^n \mapsto \sum_{n=0}^{\infty} a_n p^{2n}.$$

Ahora, si

$$x = \sum_{n=0}^{\infty} a_n p^n \in \mathbb{Z}_p \quad \text{y} \quad y = \sum_{n=0}^{\infty} b_n p^n \in \mathbb{Z}_p$$

satisfacen $|x-y|_p = p^{-j}$ para algún $j = 0,1,2,\ldots$, entonces

$$a_0 = b_0, a_1 = b_1, \ldots, a_{j-1} = b_{j-1}, \quad a_j \neq b_j,$$

y de ahí, $|f(x)-f(y)|_p = p^{-2j}$. Así tenemos

$$|f(x)-f(y)|_p = |x-y|_p^2, \quad \text{para todo } x,y \in \mathbb{Z}_p, \tag{3.2}$$

concluimos que f es inyectiva y

$$\left|\frac{f(x)-f(y)}{x-y}\right|_p = |x-y|_p \text{ tiende a 0 cuando } y \text{ tiende a } x,$$

i.e., f' es idénticamente 0. ■

En análisis real, las funciones continuamente diferenciables tienen derivadas continuas. Como vimos en la sección anterior; para las funciones p-ádicas no basta tener invertibilidad local. Una forma de solucionar este problema es con las funciones estrictamente diferenciables.

En lo que sigue $E \subset \mathbb{Q}_p$ será un conjunto no vacío sin puntos aislados.

Definición 3.2.1. Sea $f\colon E \to \mathbb{Q}_p$ y la diagonal $\Delta = \{(x,x)\colon x \in E\}$. El *primer cociente de diferencias* de f es la función

$$\Phi_1 f\colon E \times E \setminus \Delta \to \mathbb{Q}_p,$$

dada por

$$\Phi_1 f(x,y)\colon = \frac{f(x)-f(y)}{x-y}, \quad x,y \in E.$$

Decimos que f es *estrictamente diferenciable* en $a \in E$ si

$$\lim_{(x,y)\to(a,a)} \Phi_1 f(x,y)$$

existe y es igual a $f'(a)$. En otras palabras, f es estrictamente diferenciable en a si f es diferenciable en a y para toda $\varepsilon > 0$ existe una $\delta > 0$ tal que $|x-a|_p < \delta$ y $|y-a|_p < \delta,\ (x,y) \in E \times E \setminus \Delta$, implica

$$\left| \frac{f(x)-f(y)}{x-y} - f'(a) \right|_p < \varepsilon.$$

Decimos que f es estrictamente diferenciable en E si es estrictamente diferenciable en todo $a \in E$.

De lo anterior se sigue que cualquier función estrictamente diferenciable en E tiene derivada continua en E. Lo inverso no es cierto. Como lo vemos en el siguiente

Ejemplo 3.2.4. Sea la función $f\colon E \to \mathbb{Q}_p$ y B_n como en (3.1)

$$f(x) = \begin{cases} x - p^{2n} & \text{si } x \in B_n,\ n \in \mathbb{N}, \\ x & \text{si } x \in \mathbb{Z}_p \setminus \bigcup_n B_n. \end{cases}$$

entonces

$$\lim_{n\to\infty} \frac{f(p^n) - f(p^n - p^{2n})}{p^{2n}} = 0 \neq 1 = f'(0).$$

Ahora veamos la invertibilidad local para funciones p-ádicas diferenciables.

Definición 3.2.2. Una *isometría* de un espacio métrico (X,d) a otro espacio métrico (Y,ρ) es una aplicación $f\colon X \to Y$ que preserva distancias. Es decir, para cualesquiera $x_1, x_2 \in X$, $\rho\big(f(x_1), f(x_2)\big) = d(x_1,x_2)$.

Es claro que toda isometría f es una aplicación inyectiva ya que si $f(x) = f(y)$ entonces $d(x,y) = 0$.

PROPOSICIÓN 3.2.2. *Sea $E \subset \mathbb{Q}_p$, no vacío, sin puntos aislados, y sea $f\colon E \to \mathbb{Q}_p$ una función estrictamente diferenciable en algún $a \in E$. Si $f'(a) \neq 0$, entonces existe una vecindad U de a tal que*

$$|f(x)-f(y)|_p = |f'(a)|_p |x-y|_p, \quad x,y \in E \cap U,$$

En otras palabras, $\left(\dfrac{f}{f'}\right)(a)$ es una isometría *en (relativa a) una vecindad de a. En particular, f es inyectiva en una vecindad de a.*

Demostración. Por la definición de funciones estrictamente diferenciables, existe una $\delta > 0$ tal que $|x-a|_p < \delta$ y $|y-a|_p < \delta$, $x \neq y$, implica

$$\left| \frac{f(x)-f(y)}{x-y} - f'(a) \right|_p < |f'(a)|_p.$$

Ahora, por el corolario 1.7.1 tenemos,

$$\frac{|f(x)-f(y)|_p}{|x-y|_p} = |f'(a)|_p. \qquad \blacksquare$$

COROLARIO 3.2.1. *Si $f\colon E \to \mathbb{Q}_p$ estrictamente diferenciable en un punto $a \in E$ y si $f'(a) \neq 0$, entonces hay una vecindad U de a en la que f es inyectiva.*

Demostración. La prueba es inmediata, ya que todas las isometrías son inyectivas. $\blacksquare$

Observación 3.2.1. Sea $E \subset \mathbb{Z}_p$ y $\alpha > 0$. Una función $\mathbb{Z}_p \to \mathbb{Q}_p$ satisface una *condición Hölder de orden* α si existe una constante $M > 0$ tal que para todas $x, y \in E$ tenemos

$$|f(x)-f(y)|_p \leqslant M|x-y|_p^{\alpha}.$$

Cuando $\alpha = 1$, la condición de Hölder también se conoce como *condición de Lipschitz.*

Notemos que la función del lema 3.2.1 es Hölder de orden 2 por la ecuación (3.2).

PROPOSICIÓN 3.2.3. *Si una función f satisface una condición de Hölder de orden > 1, entonces $f' = 0$; en los casos:*

1. $f\colon I \subseteq \mathbb{R} \to \mathbb{R}$,
2. $f\colon \mathbb{Z}_p \to \mathbb{Q}_p$.

Demostración.

1. Para el caso real; podemos reescribir la condición de Hölder como

$$-M|x-y|^{\alpha} \leqslant f(x)-f(y) \leqslant -M|x-y|^{\alpha}$$

Por definición:

$$f'(y) = \lim_{x\to y} \frac{f(x)-f(y)}{x-y} = \lim_{x\to y^+} \frac{f(x)-f(y)}{x-y} \leqslant \lim_{x\to y^+} \frac{M|x-y|^{\alpha}}{x-y} = M \lim_{x\to y^+} \frac{(x-y)^{\alpha}}{x-y} = 0,$$

porque $\lim_{x\to y}\frac{(x-y)^\alpha}{x-y}=\lim_{x\to y}(x-y)^{\alpha-1}=0$ ya que $\alpha-1>0$.

De modo similar:

$$f'(y)=\lim_{x\to y}\frac{f(x)-f(y)}{x-y}=\lim_{x\to y^-}\frac{f(x)-f(y)}{x-y}\geqslant\lim_{x\to y^-}\frac{-M|x-y|^\alpha}{x-y}=(-M)\lim_{x\to y^-}\frac{(y-x)^\alpha}{x-y}=0$$

Porque $\lim_{x\to y^-}\frac{(y-x)^\alpha}{x-y}=(-1)^\alpha\lim_{x\to y}(x-y)^{\alpha-1}=0$ ya que $\alpha-1>0$. Por lo anterior, tenemos que para todo $y\in I$, $|f'(y)|=0$, es decir, $f'=0$.

2. Para el caso p-ádico tenemos:

$$|f(x)-f(y)|_p\leqslant M|x-y|_p^\alpha$$

de ahí que

$$\frac{|f(x)-f(y)|_p}{|x-y|_p}\leqslant M|x-y|_p^{\alpha-1}$$

entonces

$$\left|\frac{f(x)-f(y)}{x-y}\right|_p\leqslant M|x-y|_p^{\alpha-1}$$

al tomar límites

$$\lim_{|x-y|_p\to 0}\left|\frac{f(x)-f(y)}{x-y}\right|_p\leqslant M\lim_{|x-y|_p\to 0}|x-y|_p^{\alpha-1}$$

por lo tanto $f'=0$. ■

En análisis real, el Teorema de Rolle dice que si $f\colon[a,b]\to\mathbb{R}$ es continua y diferenciable en (a,b) y $f(a)=f(b)$, entonces existe un $\zeta\in(a,b)$ tal que $f'(\zeta)=0$. Sin embargo en el caso p-ádico, esta formulación del teorema de Rolle falla. En efecto, veamos el siguiente

Ejemplo 3.2.5. Sea $f\colon\mathbb{Z}_p\to\mathbb{Q}_p$ dada por

$$f(x)=x^p-x.$$

Tenemos $f(0)=0, f(1)=0, f'(x)=px^{p-1}-1$. Dado que $|f'(x)+1|_p\leqslant\frac{1}{p}$, i.e., $f'(x)\in p\mathbb{Z}_p-1$, se sigue que $f'(x)\neq 0$ para todo $x\in\mathbb{Z}_p$.

3.3. Series Formales de potencias p-ádicas

Las funciones expresadas mediante series de potencias son diferenciables (Rudin (1976), teorema 8.1) y como los números p-ádicos se pueden expresar de manera única como tales series (1.1). Tales series nos serán muy útiles para estudiar algunas funciones p-ádicas y su diferenciabilidad.

Definición 3.3.1. Una *serie formal de potencias* es una expresión de la forma

$$f(X)=\sum_{n=0}^{\infty}a_nX^n,$$

donde $a_n\in\mathbb{Q}_p$ y X es una indeterminada.

El conjunto de todas las series formales de potencias en X con coeficientes en $\mathbb{Q}_p$ se denota por $\mathbb{Q}_p\big[[X]\big]$.

Definición 3.3.2.

1. La suma de series formales de potencias p-ádicas es la aplicación

   $+ : \mathbb{Q}_p\big[[X]\big] \times \mathbb{Q}_p\big[[X]\big] \to \mathbb{Q}_p\big[[X]\big]$ dada por:

$$\left(\sum_{n=0}^{\infty} a_n X^n\right) + \left(\sum_{n=0}^{\infty} b_n X^n\right) = \sum_{n=0}^{\infty} (a_n + b_n) X^n,$$

2. El producto de series formales de potencias p-ádicas es la aplicación

   $\cdot : \mathbb{Q}_p\big[[X]\big] \times \mathbb{Q}_p\big[[X]\big] \to \mathbb{Q}_p\big[[X]\big]$ dada por:

$$\left(\sum_{n=0}^{\infty} a_n X^n\right) \cdot \left(\sum_{n=0}^{\infty} b_n X^n\right) = \sum_{n=0}^{\infty} \left(\sum_{i+j=n}^{\infty} a_i b_j\right) X^n.$$

TEOREMA 3.3.1. *$\left(\mathbb{Q}_p\big[[X]\big], +, \cdot\right)$ tiene una estructura de anillo donde:*

- *La identidad para $+$ es* $0 = \sum_{n=0}^{\infty} 0 \cdot X^n$,
- *el inverso para $+$ está dado por* $-f(X) = \sum_{n=0}^{\infty} (-a_n) X^n$, *y*
- *la identidad para $\cdot$ es* $1 = \sum_{n=0}^{\infty} e_n X^n$ *con* $e_0 = 1$ *y* $e_{i+1} = 0$.

Demostración. Consideremos $f(X), g(X), h(X) \in \mathbb{Q}_p\big[[X]\big]$ dadas por:

$$f(X) = \sum_{n=0}^{\infty} a_n X^n, \quad g(X) = \sum_{n=0}^{\infty} b_n X^n, \quad h(X) = \sum_{n=0}^{\infty} c_n X^n.$$

1. La operación $+$ es asociativa:

$$\begin{aligned}
\big(f(X)+g(X)\big)+h(X) &= \left(\left(\sum_{n=0}^{\infty} a_n X^n\right)+\left(\sum_{n=0}^{\infty} b_n X^n\right)\right)+\left(\sum_{n=0}^{\infty} c_n X^n\right)\\
&= \left(\sum_{n=0}^{\infty}(a_n+b_n)X^n\right)+\left(\sum_{n=0}^{\infty} c_n X^n\right)\\
&= \sum_{n=0}^{\infty}\big((a_n+b_n)+c_n\big)X^n\\
&= \sum_{n=0}^{\infty}\big(a_n+(b_n+c_n)\big)X^n\\
&= \left(\sum_{n=0}^{\infty} a_n X^n\right)+\left(\sum_{n=0}^{\infty}(b_n+c_n)X^n\right)\\
&= \left(\sum_{n=0}^{\infty} a_n X^n\right)+\left(\left(\sum_{n=0}^{\infty} b_n X^n\right)+\left(\sum_{n=0}^{\infty} c_n X^n\right)\right)\\
&= f(X)+\big(g(X)+h(X)\big).
\end{aligned}$$

   Entonces $\big(f(X)+g(X)\big)+h(X) = f(X)+\big(g(X)+h(X)\big)$.

2. Consideremos $0 = \sum_{n=0}^{\infty} 0\cdot X^n$. Entonces

$$\begin{aligned}
f(X)+0 &= \left(\sum_{n=0}^{\infty} a_n X^n\right)+\left(\sum_{n=0}^{\infty} 0\cdot X^n\right)\\
&= \sum_{n=0}^{\infty}(a_n+0)X^n\\
&= \sum_{n=0}^{\infty} a_n X^n\\
&= f(X)\\
&= \sum_{n=0}^{\infty}(0+a_n)X^n\\
&= \left(\sum_{n=0}^{\infty} 0\cdot X^n\right)+\left(\sum_{n=0}^{\infty} a_n X^n\right)\\
&= 0+f(X).
\end{aligned}$$

   Entonces $f(X)+0 = f(X) = 0+f(X)$. Así que 0 es la identidad para $+$.

3. Definamos $-f(X) \in \mathbb{Q}_p\big[[X]\big]$ de la siguiente manera: $-f(X) = \sum_{n=0}^{\infty}(-a_n)X^n$. Notemos que

$$f(X)+\big(-f(X)\big) = \left(\sum_{n=0}^{\infty} a_n X^n\right)+\left(\sum_{n=0}^{\infty}(-a_n)X^n\right)$$

$$\begin{aligned}
&= \sum_{n=0}^{\infty} (a_n - a_n) X^n \\
&= \sum_{n=0}^{\infty} 0 \cdot X^n \\
&= 0.
\end{aligned}$$

Así que $f(X) + \big(-f(X)\big) = 0$.

Análogamente:

$$\begin{aligned}
\big(-f(X)\big) + f(X) &= \left(\sum_{n=0}^{\infty} (-a_n) X^n \right) + \left(\sum_{n=0}^{\infty} a_n X^n \right) \\
&= \sum_{n=0}^{\infty} (-a_n + a_n) X^n \\
&= \sum_{n=0}^{\infty} 0 \cdot X^n \\
&= 0.
\end{aligned}$$

Así que $\big(-f(X)\big) + f(X) = 0$. Entonces $-f(X)$ es el inverso aditivo de $f(X)$ para la operación $+$.

4. La operación $+$ es conmutativa. En efecto:

$$\begin{aligned}
f(X) + g(X) &= \left(\sum_{n=0}^{\infty} a_n X^n \right) + \left(\sum_{n=0}^{\infty} b_n X^n \right) \\
&= \sum_{n=0}^{\infty} (a_n + b_n) X^n \\
&= \sum_{n=0}^{\infty} (b_n + a_n) X^n \\
&= \left(\sum_{n=0}^{\infty} b_n X^n \right) + \left(\sum_{n=0}^{\infty} a_n X^n \right) \\
&= g(X) + f(X).
\end{aligned}$$

Entonces $f(X) + g(X) = g(X) + f(X)$.

5. La operación $\cdot$ es asociativa:

$$\begin{aligned}
\big(f(X) \cdot g(X)\big) \cdot h(X) &= \left(\left(\sum_{n=0}^{\infty} a_n X^n \right) \cdot \left(\sum_{n=0}^{\infty} b_n X^n \right) \right) \cdot \left(\sum_{n=0}^{\infty} c_n X^n \right) \\
&= \left(\sum_{n=0}^{\infty} \left(\sum_{i+j=n}^{\infty} a_i b_j \right) X^n \right) \cdot \left(\sum_{n=0}^{\infty} c_n X^n \right) \\
&= \sum_{n=0}^{\infty} \left(\sum_{t+k=n}^{\infty} \left(\sum_{i+j=t}^{\infty} a_i b_j \right) c_k \right) X^n
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{n=0}^{\infty}\left(\sum_{t+k=n}^{\infty}\sum_{i+j=t}^{\infty} a_i b_j c_k\right) X^n \\
&= \sum_{n=0}^{\infty}\left(\sum_{i+j+k=n}^{\infty} a_i b_j c_k\right) X^n \\
&= \sum_{n=0}^{\infty}\left(\sum_{i+s=n}^{\infty}\left(\sum_{j+k=s}^{\infty} a_i b_j c_k\right)\right) X^n \\
&= \sum_{n=0}^{\infty}\left(\sum_{i+s=n}^{\infty} a_i\left(\sum_{j+k=s}^{\infty} b_j c_k\right)\right) X^n \\
&= \left(\sum_{n=0}^{\infty} a_n X^n\right)\cdot\left(\sum_{n=0}^{\infty}\left(\sum_{j+k=n}^{\infty} b_j c_k\right) X^n\right) \\
&= \left(\sum_{n=0}^{\infty} a_n X^n\right)\cdot\left(\left(\sum_{n=0}^{\infty} b_n X^n\right)\cdot\left(\sum_{n=0}^{\infty} c_n X^n\right)\right) \\
&= f(X)\cdot(g(X)\cdot h(X)).
\end{aligned}
$$

Entonces $\big(f(X)\cdot g(X)\big)\cdot h(X) = f(X)\cdot\big(g(X)\cdot h(X)\big)$.

6. La operación $\cdot$ se distribuye sobre la operación $+$ por la izquierda:

$$
\begin{aligned}
f(X)\cdot(g(X)+h(X)) &= \left(\sum_{n=0}^{\infty} a_n X^n\right)\cdot\left(\left(\sum_{n=0}^{\infty} b_n X^n\right)+\left(\sum_{n=0}^{\infty} c_n X^n\right)\right) \\
&= \left(\sum_{n=0}^{\infty} a_n X^n\right)\cdot\left(\sum_{n=0}^{\infty}(b_n+c_n) X^n\right) \\
&= \sum_{n=0}^{\infty}\left(\sum_{i+j=n}^{\infty} a_i(b_j+c_j)\right) X^n \\
&= \sum_{n=0}^{\infty}\left(\sum_{i+j=n}^{\infty} a_i b_j + a_i c_j)\right) X^n \\
&= \sum_{n=0}^{\infty}\left(\left(\sum_{i+j=n}^{\infty} a_i b_j\right)+\left(\sum_{i+j=n}^{\infty} a_i c_j\right)\right) X^n \\
&= \left(\sum_{n=0}^{\infty}\left(\sum_{i+j=n}^{\infty} a_i b_j\right) X^n\right)+\left(\sum_{n=0}^{\infty}\left(\sum_{i+j=n}^{\infty} a_i c_j\right) X^n\right) \\
&= \left(\sum_{n=0}^{\infty} a_n X^n\right)\cdot\left(\sum_{n=0}^{\infty} b_n X^n\right)+\left(\sum_{n=0}^{\infty} a_n X^n\right)\cdot\left(\sum_{n=0}^{\infty} c_n X^n\right) \\
&= f(X)\cdot g(X)+f(X)\cdot h(X).
\end{aligned}
$$

Por lo tanto $f(X)\cdot(g(X)+h(X)) = (f(X)\cdot g(X))+(f(X)\cdot h(X))$.

De modo similar, $\cdot$ se distribuye sobre $+$ por la derecha:

$$\begin{aligned}
\big(f(X)+g(X)\big)\cdot h(X) &= \left(\left(\sum_{n=0}^{\infty} a_n X^n\right)+\left(\sum_{n=0}^{\infty} b_n X^n\right)\right)\cdot\left(\sum_{n=0}^{\infty} c_n X^n\right)\\
&= \left(\sum_{n=0}^{\infty}(a_n+b_n)X^n\right)\cdot\left(\sum_{n=0}^{\infty} c_n X^n\right)\\
&= \sum_{n=0}^{\infty}\left(\sum_{i+j=n}^{\infty}(a_j+b_j)c_i\right)X^n\\
&= \sum_{n=0}^{\infty}\left(\sum_{i+j=n}^{\infty} a_j c_i + b_j c_i\right)X^n\\
&= \sum_{n=0}^{\infty}\left(\left(\sum_{i+j=n}^{\infty} a_j c_i\right)+\left(\sum_{i+j=n}^{\infty} b_j c_i\right)\right)X^n\\
&= \left(\sum_{n=0}^{\infty}\left(\sum_{i+j=n}^{\infty} a_j c_i\right)X^n\right)+\left(\sum_{n=0}^{\infty}\left(\sum_{i+j=n}^{\infty} b_j c_i\right)X^n\right)\\
&= \left(\sum_{n=0}^{\infty} a_n X^n\right)\cdot\left(\sum_{n=0}^{\infty} c_n X^n\right)+\left(\sum_{n=0}^{\infty} b_n X^n\right)\cdot\left(\sum_{n=0}^{\infty} c_n X^n\right)\\
&= \big(f(X)\cdot h(X)\big)+\big(g(X)\cdot h(X)\big).
\end{aligned}$$

Entonces $\big(f(X)+g(X)\big)\cdot h(X) = \big(f(X)\cdot h(X)\big)+\big(g(X)\cdot h(X)\big)$. Así, tenemos que $\mathbb{Q}_p\big[[X]\big]$ es un anillo.

7. Ya que $\mathbb{Q}_p$ es conmutativo, entonces tenemos que $\mathbb{Q}_p\big[[X]\big]$ es conmutativo.

$$\begin{aligned}
f(X)\cdot g(X) &= \left(\sum_{n=0}^{\infty} a_n X^n\right)\cdot\left(\sum_{n=0}^{\infty} b_n X^n\right)\\
&= \sum_{n=0}^{\infty}\left(\sum_{i+j=n}^{\infty} a_i b_j\right)X^n\\
&= \sum_{n=0}^{\infty}\left(\sum_{i+j=n}^{\infty} b_j a_i\right)X^n\\
&= \left(\sum_{n=0}^{\infty} b_n X^n\right)\cdot\left(\sum_{n=0}^{\infty} a_n X^n\right)\\
&= g(X)\cdot f(X).
\end{aligned}$$

Entonces $f(X)\cdot g(X) = g(X)\cdot f(X)$.

8. Definamos $1 = \sum_{n=0}^{\infty} e_n X^n$ con $e_0 = 1$ y $e_{i+1} = 0$. Entonces

$$f(X)\cdot 1 = \left(\sum_{n=0}^{\infty} a_n X^n\right)\cdot\left(\sum_{n=0}^{\infty} e_n X^n\right)$$

$$
\begin{aligned}
&= \sum_{n=0}^{\infty} \left(\sum_{n=i+j}^{\infty} a_i e_j \right) X^n \\
&= \sum_{n=0}^{\infty} a_n e_0 X^n \\
&= \sum_{n=0}^{\infty} a_n X^n \\
&= f(X) \\
&= \sum_{n=0}^{\infty} a_n X^n \\
&= \sum_{n=0}^{\infty} e_0 a_n X^n \\
&= \sum_{n=0}^{\infty} \left(\sum_{n=i+j}^{\infty} e_i a_j \right) X^n \\
&= \left(\sum_{n=0}^{\infty} e_n X^n \right) \cdot \left(\sum_{n=0}^{\infty} a_n X^n \right) \\
&= 1 \cdot f(X).
\end{aligned}
$$

Entonces $1 \cdot f(X) = f(X) = f(X) \cdot 1$. Es decir, $\mathbb{Q}_p[[X]]$ tiene una unidad y es 1. ■

Tomemos $x \in \mathbb{Q}_p$ y $f \in \mathbb{Q}_p\big[[X]\big]$ y consideremos la correspondiente serie numérica de potencias $f(x) = \sum_{n=0}^{\infty} a_n x^n$. Sabemos que ésta converge si, y sólo si, $|a_n x^n|_p$ tiende a 0. Así, si $r \geqslant 0$ denota un número real tal que $|a_n|_p r^n$ tiende a 0, entonces la serie $\sum_{n=0}^{\infty} a_n x^n$ converge al menos para $|x|_p \leqslant r$.

Definición 3.3.3. El *radio de convergencia* de una serie de potencias $f(X) = \sum_{n=0}^{\infty} a_n X^n$ con coeficientes en $\mathbb{Q}_p$ es el número real extendido $0 \leqslant r_f \leqslant \infty$ tal que $r_f = \sup\{r \geqslant 0 \colon |a_n|_p r^n \to 0\}$, donde los números reales extendidos se definen como $\mathbb{R} \cup \{\infty\}$.

Como en el caso arquimediano (series de potencias sobre $\mathbb{R}$ o $\mathbb{C}$); el radio de convergencia de una serie formal de potencias p-ádica puede calcularse mediante la *fórmula de Hadamard*; la cual está en la siguiente proposición.

PROPOSICIÓN 3.3.1. *El radio de convergencia de una serie de potencias* $f(X) = \sum_{n=0}^{\infty} a_n X^n$ *es*

$$r_f = \frac{1}{\limsup |a_n|_p^{1/n}}. \tag{3.3}$$

Demostración. Recordemos que límsup de una sucesión es la menor cota superior del conjunto de puntos límite de dicha sucesión. Puede ser calculada mediante la fórmula $\limsup x_n = \lim_{n\to\infty} \sup_{k \geqslant n} x_k$.

Si $|x|_p > r_f$ (que sólo es posible si $r_f < \infty$), tenemos

$$\limsup |x|_p |a_k|_p^{1/k} = |x|_p \lim_{n\to\infty} \sup_{k \geqslant n} |a_k|_p^{1/k} = |x|_p \cdot \frac{1}{r_f} > 1.$$

Por lo tanto, la sucesión decreciente $\sup_{k\geqslant n}|x|_p|a_k|_p^{1/k} > 1$ y para una cantidad infinita de valores k tenemos $|a_k|_p|x|_p^k > 1$. Se sigue que el término general $a_k x^k$ de la serie no tiende a 0; de ahí que la serie diverge.

Por otro lado, si $|x|_p < r_f$ (lo cual ocurre sólo si $r_f > 0$), entonces podemos elegir $r \in \mathbb{R}$ tal que $|x|_p < r < r_f$. Entonces

$$\lim_{n\to\infty}\sup_{k\geqslant n} r|a_k|_p^{1/k} = r\lim_{n\to\infty}\sup_{k\geqslant n}|a_k|_p^{1/k} < 1.$$

Por lo tanto existe un $N \in \mathbb{N}$ tal que

$$\sup_{k\geqslant N} r|a_k|_p^{1/k} < 1.$$

En consecuencia, para $k > N$ tenemos $|a_k|_p r^k < 1$ y

$$|a_k x^k|_p = |a_k|_p r^k\left(\frac{|x|_p}{r}\right)^k < \frac{|x|_p^k}{r^k} \text{ tiende a 0 cuando } k \text{ tiende a } \infty.$$

Así, el término general de la serie tiende a 0, y la serie converge. ■

¿Qué ocurre cuando $|x|_p = r$? En el caso arquimediano ($\mathbb{R}$ o $\mathbb{C}$) el comportamiento en la vecindad del intervalo o disco de convergencia puede ser muy complicado.

Ejemplo 3.3.1. La serie logarítmica usual de potencias

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

tiene radio de convergencia 1. Si $|x| = 1$, diverge para $x = -1$ y converge (no absolutamente) para $x = 1$.

En el caso no arquimediano la situación es más simple. Ya que

- para $|x|_p < r$, la serie converge,
- para $|x|_p > r$, la serie diverge,
- y para $|x|_p = r$, la serie $\begin{cases}\text{converge} & \text{si } \lim_{n\to\infty}|a_n|_p r^n = 0\\ \text{diverge} & \text{si } \lim_{n\to\infty}|a_n|_p r^n > 0 \text{ o si el límite no existe.}\end{cases}$

De ahí que, la región de convergencia tenga la forma

$$|x|_p \leqslant r \quad \text{o} \quad |x|_p < r.$$

Notemos que, a diferencia del caso arquimediano, aquí podemos dar un criterio general para la convergencia también cuando $|x|_p = r$.

PROPOSICIÓN 3.3.2. *Sea $f(x) \in \mathbb{Q}_p[[X]]$ una serie de potencias p-ádica. El* dominio de convergencia *de $f(x)$ es una bola $D = \{x \in \mathbb{Q}_p : |x|_p \leqslant R\}$ para algún $R \in \{p^k, k \in \mathbb{Z}\} \cup \{0\} \cup \infty$, y la serie converge uniformemente en D.*

Demostración. Sea r_f el radio de convergencia de $f(X)$, sabemos que la serie converge en la bola abierta $D = \{|x|_p < r_f\}$ Como para los puntos x tales que $|x|_p = r_f$, la condición necesaria y suficiente para la convergencia es $|a_n x^n|_p \to 0$, la cual sólo depende del valor absoluto $|x|_p$, no del valor específico de x. Así, ya sea para todos los puntos con $|x|_p = r_f$ la serie converge, en cuyo caso $R = r_f$. O para todos los puntos con $|x|_p = r_f$ la serie diverge, en cuyo caso $R = \frac{1}{p} r_f$. Para $|x|_p \leqslant R$ tenemos

$$|a_n x^n|_p \leqslant |a_n R^n|_p \text{ tiende a } 0,$$

y se cumple la convergencia en D. ■

Ejemplo 3.3.2. Sea $\displaystyle\sum_{n=1}^{\infty} a_n x^n = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} x^n \in \mathbb{Q}_p\big[[X]\big]$. Entonces

$$|a_n|_p = p^{v_p(n)} \quad \text{y} \quad \lim_{n\to\infty} |a_n|_p^{1/n} = \lim_{n\to\infty} \left(p^{v_p(n)}\right)^{1/n} = 1.$$

En efecto, notemos que si $n > 1$, podemos escribir $n = p^{\alpha} n'$, donde $(p,n) = 1$. Entonces $v_p(n) = \alpha$ y, dado que $p^{\alpha} \leqslant n$, tenemos que $\alpha = \log_p(n)$; de ahí que $v_p(n) \leqslant \log_p(n)$. Así $\lim\limits_{n\to\infty} \frac{v_p(n)}{n} = 0$. Entonces $\lim\limits_{n\to\infty} p^{\frac{v_p(n)}{n}} = \lim\limits_{n\to\infty} p^0 = 1$.

La serie converge para $|x|_p < 1$ y diverge para $|x|_p > 1$. Si $|x|_p = 1$, $|a_n|_p = p^{v_p(n)} \geqslant 1$; de ahí que la serie diverge para tales x, y el dominio de convergencia de esta serie de potencias es $\{x \in \mathbb{Q}_p \colon |x|_p \leqslant p^{-1}\}$.

PROPOSICIÓN 3.3.3. *Cada $f(X) \in \mathbb{Z}_p\big[[X]\big]$ converge en $\{x \in \mathbb{Q}_p : |x|_p < 1\}$.*

Demostración. Sea $|x|_p < 1$ y $f(x) = \sum_{n=0}^{\infty} a_n x^n$. Dado que para cualquier $n \geqslant 0$, tenemos que $|a_n|_p \leqslant 1$, tenemos que $|a_n x^n|_p \leqslant |x|_p^n$ tiende a 0 cuando n tiende a ∞; de ahí que la serie converge. ■

Ejemplo 3.3.3. Sea $a \in \mathbb{Z}_p$ fijo. Entonces

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

La función $f_a(X) \colon = (1+X)^a$ está definida por la misma serie como su contraparte real y se llama *serie binomial p-ádica*.

Así, para cualquier $a \in \mathbb{Z}_p$, $f_a(X) \in \mathbb{Z}_p\big[[X]\big]$, y de ahí que converja para $|x|_p < 1$.

En particular, si $m \in \mathbb{Z}$, entonces $\binom{m}{n} \in \mathbb{Z}$.

PROPOSICIÓN 3.3.4. *Sea $f(x) = \sum a_n x^n \in \mathbb{Q}_p\big[[X]\big], a_n \in \mathbb{Q}_p$, una serie p-ádica cuya región de convergencia es una bola abierta y cerrada $D \subset \mathbb{Q}_p$. Entonces $f \colon D \to \mathbb{Q}_p$ es una función continua en D.*

Demostración. Probemos la continuidad en $x = 0$ de la serie de potencias $f(x) = \displaystyle\sum_{n=0}^{\infty} a_n x^n$ con un radio de convergencia positivo.

Escribimos

$$|f(x)-f(0)|_p = |x|_p \left| \sum_{n=0}^{\infty} a_{n+1}x^n \right|_p$$

y mostramos que la serie $\sum_{n=0}^{\infty} a_{n+1}x^n$ tiene el mismo radio de convergencia que la serie de potencias original.

Queremos probar que f es continua en cualquier $x \in D, x \neq 0$. Sea $|x-x'|_p < \delta$, donde $\delta < |x|_p$ se elegirá después. Entonces, por el corolario 1.7.1, $|x|_p = |x'|_p$.

Tenemos

$$\begin{aligned} |f(x)-f(x')|_p &= \left| \sum_{n=0}^{\infty} (a_n x^n - a_n x'^n) \right|_p \\ &\leqslant \max_n |a_n x^n - a_n x'^n|_p \\ &= \max_n (|a_n|_p |x-x'|_p |x^{n-1} + x^{n-2}x' + \cdots + x'^{n-1}|_p). \end{aligned}$$

Pero $$|x^{n-1} + x^{n-2}x' + \cdots + x'^{n-1}|_p \leqslant \max_{1 \leqslant i \leqslant n} |x^{n-i}x'^{i-1}|_p = |x|_p^{n-1}$$

Por lo tanto:
$$\begin{aligned} |f(x)-f(x')|_p &\leqslant \max_n (|x-x'|_p |a_n|_p |x|_p^{n-1}) \\ &< \frac{\delta}{|x|_p} \max_n (|a_n|_p |x|_p^n). \end{aligned}$$

dado que $|a_n x^n|_p$ está acotado cuando n tiende a ∞, obtenemos $|f(x)-f(x')|_p < \varepsilon$ para una δ adecuada. ■

Ahora revisaremos el comportamiento de la *derivada* en el contexto del análisis p-ádico.

Sean $f(X) = \sum_{n=0}^{\infty} a_n X^n$ una serie de potencias y $D_f(X)$ su derivada formal que, por teorema 3.1.1, es:

$$D_f(X) = \sum_{n=1}^{\infty} n a_n X^{n-1}.$$

PROPOSICIÓN 3.3.5. *El radio de convergencia de la serie de potencias,*

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

y el de su derivada formal,

$$D_f(X) = \sum_{n=1}^{\infty} n a_n X^{n-1}$$

son iguales, i.e., $r_f = r_{Df}$.

Demostración. Para cualquier $n \in \mathbb{N}$ tenemos $|n|_p \leqslant 1$. Entonces

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

Ejemplo 3.3.4. Mostremos que el comportamiento de las series de potencias y su derivada formal en la vecindad de la región de convergencia pueden diferir. 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 su derivada $Df(X) = \sum_{n=0}^{\infty} p^n X^{p^n-1}$ converge para $|x|_p = 1$ (dado que la serie $\sum_{n=0}^{\infty} p^n$ converge). Notemos, sin embargo, que la bola de convergencia de $Df(X)$ no es más pequeña que la de $f(X)$.

Ahora deberemos mostrar que justo como en los casos real y complejo, la serie formal de potencias $Df(X)$ efectivamente representa la derivada $f'(X)$ en la región de convergencia:

LEMA 3.3.1. *Sea $f(X) \in \mathbb{Q}_p\left[[X]\right]$ una serie de potencias y sea $Df(X)$ su derivada formal. Si $x \in \mathbb{Q}_p$ es tal que $f(x)$ converge, entonces $Df(x)$ también converge.*

Demostración. Se $|x|_p = r$. Entonces $f(x)$ converge si, y sólo si

$$\lim_{n\to\infty} a_n r^n = 0,$$

y $Df(x)$ converge si, y sólo si

$$\lim_{n\to\infty} |n|_p a_n r^{n-1} = 0. \qquad \blacksquare$$

PROPOSICIÓN 3.3.6. *Consideremos la serie de potencias*

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

y supongamos que $f(x) = \sum_{n=0}^{\infty} a_n x^n$ converge en una bola abierta $U \subset \mathbb{Q}_p$. Entonces $f(x)$ es diferenciable en U y para toda $x \in U$, tenemos

$$f'(X) = \sum_{n=0}^{\infty} n a_n X^{n-1}.$$

De modo más general, $f(x)$ tiene derivada de todos los órdenes en U las cuales están dadas por

$$f^{(k)}(x) = k! \sum_{n=0}^{\infty} \binom{n}{k} a_n x^{n-k}.$$

Los coeficientes de la serie de potencias original pueden expresarse como

$$a_k = \frac{f^k(0)}{k!}.$$

Demostración. La prueba clásica de este resultado (Rudin, 1976, Corolario del teorema 8.) se basa en el teorema del valor medio el cual no es válido en el caso p-ádico, como ya hemos visto en la sección 3.1, así que necesitamos una aproximación diferente. Sea $U = B(0, p^{n+1}) = \overline{B}(0, p^n)$ la bola (que es al mismo tiempo, abierta y cerrada) donde $f(x)$ converge. En vista de la observación 3.3.4 y el lema 3.3.1, $Df(x)$ también converge en U y la serie de potencias, converge uniformemente en la bola cerrada $\overline{B}(0, p^n)$ (proposición 3.3.2). Ahora sea $x \in U$. Para mostrar que

$$Df(x) = \lim_{h\to 0} \frac{f(x+h) - f(x)}{h}, \tag{3.4}$$

notamos primero que hay efectivamente elementos h que tienden a cero para los que $f(x+h)$ converge. Si $x=0$, cualquier h con $|h|_p \leqslant p^n$ funciona, y si $x \neq 0$, cualquier h con $|h|_p < |x|_p \leqslant p^n$ funciona debido a la desigualdad fuerte del triángulo, en particular, la expresión bajo el límite en la ecuación (3.4) tiene sentido. Expandamos $f(x+h)$ en la serie de potencias usando el teorema del binomio

$$\frac{f(x+h)-f(x)}{h} = \sum_{n=1}^{\infty} a_n \sum_{m=1}^{n} \binom{n}{m} x^{n-m} h^{m-1}. \tag{3.5}$$

Mostramos que la serie en (3.5) converge uniformemente en h. Un teorema estándar en análisis real (Rudin, 1976, teorema 7.12) implica que el límite es continuo en h; por lo tanto simplemente necesitamos establecer $h=0$ para obtener el resultado deseado. Por inducción se obtienen los resultados para derivadas superiores. ■

Ahora, supongamos que tenemos una función definida por una serie de potencias en algún disco. ¿Podemos extender la definición a una región más grande de algún modo "razonable"? En análisis real podíamos hacerlo; eligiendo un punto α dentro de la bola de convergencia, encontrando una nueva serie de potencias alrededor de α y así continuar nuestra función a la bola de convergencia de la nueva serie. Desafortunadamente, esto no funciona en el caso p-ádico como lo ilustra la siguiente resultado.

PROPOSICIÓN 3.3.7. *Sea*

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

y sea $\alpha \in D$, donde D es el disco de convergencia de f. Para $m \geqslant 0$, definimos

$$b_m = \sum_{n=0}^{\infty} \binom{n}{m} a_n \alpha^{n-m},$$

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

Entonces

1. *b_m converge para todo m, así b_m está bien definido para cualquier m;*
2. *$g(X)$ tiene el mismo disco de convergencia D;*
3. *$g(\lambda) = f(\lambda)$ para todo $\lambda \in D$.*

Demostración. Dado que $\alpha \in D$, para cada m tenemos

$$\left| \binom{n}{m} a_n \alpha^{n-m} \right|_p \leqslant |a_n \alpha^{n-m}|_p = |\alpha|_p^{-m} |a_n \alpha^n|_p \to 0,$$

dado que $\binom{n}{m} \in \mathbb{Z}$, y la serie $f(X)$ converge en α. Entonces b_m converge por la proposición 2.2.2, y se sigue (1). Ahora si $\lambda \in D$,

$$f(\lambda) = \sum_{n=0}^{\infty} a_n (\lambda - \alpha + \alpha)^n = \sum_{n=0}^{\infty} \sum_{m \leqslant n} \binom{n}{m} a_n \alpha^{n-m} (\lambda - \alpha)^m. \tag{3.6}$$

esto se ve como una suma parcial de $g(X)$, excepto que necesitamos re-arreglar sus términos. Para ello, debemos mostrar que la doble serie converge "uniformemente", i.e., satisface la condición del teorema 2.2.2. Así que pongamos esto dentro de una serie de potencias infinita en ambos índices: Sea

$$\beta_{n,m} = \begin{cases} \binom{n}{m} a_n \alpha^{n-m} (\lambda - \alpha)^m & \text{si } m \leqslant n, \\ 0 & \text{si } m > n. \end{cases}$$

Quisiéramos mostrar que $\beta_{m,n}$ tiende a 0 uniformemente en ambos índices. Esto es, queremos encontrar una N tal que si $m > N$ o $n > N$, entonces $|\beta_{m,n}|_p < \varepsilon$. Tenemos la siguiente estimación:

$$|\beta_{m,n}|_p = \left| \binom{n}{m} a_n \alpha^{n-m} (\lambda - \alpha)^m \right|_p \leqslant |a_n \alpha^{n-m} (\alpha - \lambda)^m|_p.$$

Podemos encontrar un punto $r_1 \in D$ tal que $r = |r_1|_p \geqslant \text{máx}\,(|\alpha|_p, |\lambda|_p)$. Entonces $|\alpha|_p^m \leqslant r^m$ por construcción, y

$$|\lambda - \alpha|_p^{n-m} \leqslant \text{máx}(|\alpha|_p, |\lambda|_p)^{n-m} \leqslant r^{n-m}$$

por construcción y por la propiedad no arquimediana; así

$$|\beta_{m,n}|_p = \left|a_n \alpha^{n-m} (\lambda - \alpha)^m\right|_p \leqslant |a_n|_p r^n.$$

lo cual tiende a cero cuando n tiende a ∞ independientemente de m, i.e., para todo $\varepsilon > 0$, existe N para todo $n > N, |\beta_{m,n}|_p < \varepsilon$. Ahora, si $m > N$, o bien $n \geqslant m$ implica $n > N$ implica que $|\beta_{m,n}|_p < \varepsilon$ o $n < m$ implica $\beta_{m,n} = 0$, así $|\beta_{m,n}|_p = 0 < \varepsilon$.

Así, podemos re-ordenar la suma en (3.6):

$$\begin{aligned} f(\lambda) &= \sum_{n=0}^{\infty} \sum_{m \leqslant n} \binom{n}{m} a_n a^{n-m} (\lambda - \alpha)^m = \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} \beta_{n,m} \\ &= \sum_{n=0}^{\infty} \sum_{m=0} \binom{n}{m} a_n a^{n-m} (\lambda - \alpha)^m = g(\lambda) \end{aligned}$$

Elegimos un λ arbitrario en D y encontramos que g converge en λ; así que g converge en todo D. Notemos que los papeles de f y g son simétricos, así empezando con g y construyendo f, vemos que f converge siempre que g lo hace. ■

Así, en contraste con el caso real o complejo, esto no nos da ningún nuevo dominio de definición. Para más detalles de los puntos tocados en esta sección véase Hasse (1980).

3.4. Logaritmo y Exponencial p-ádicos

En esta sección, nuestro objetivo es usar las series de potencias para definir funciones p-ádicas que son análogas a funciones clásicas. Mostramos las versiones p-ádicas de las funciones exponencial y logaritmo. En contraste con el caso arquimediano, el logaritmo tiene mejores propiedades de convergencia. Notemos el siguiente resultado,

LEMA 3.4.1. *Para cualquier entero positivo $n \in \mathbb{N}$, tenemos que su expansión en base p es:*

$$n = \sum_{i=0}^{k} a_i p^i$$

Si S_n es la suma de los dígitos de n escrito en base p; i.e., $S_n = a_0 + a_1 + \cdots + a_k$. Entonces

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

Demostración. Si $p > n$, tenemos $S_n = n$ y por lo tanto $\frac{n-S_n}{p-1} = 0$. Por supuesto esto es cierto ya que $p \nmid n!$ y por lo tanto $v_p(n!) = 0$. Ahora suponemos que $p \leqslant n$ y sea $n = \sum_{i=0}^{k} a_i p^i$ la expansión de n en base p. Para cualquier $1 \leqslant i \leqslant k$ hay exactamente

$$\left\lfloor \frac{n}{p^i} \right\rfloor - \left\lfloor \frac{n}{p^{i+1}} \right\rfloor$$

($\lfloor x \rfloor$ es la parte entera de x) números entre 1 y n tales que p^i es la mayor potencia de p que divide a cada uno. Así que obtenemos

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

Aquí se cumple la última ecuación porque para $i \geqslant 2$, cada término aparece dos veces en la suma, una vez con coeficiente i y una con coeficiente $-(i+1)$. Además, $\left\lfloor \frac{n}{p^{k+1}} \right\rfloor = 0$ por la definición de k.

Por otro lado tenemos que:

$$\begin{aligned}
\frac{n-S_n}{p-1} &= \frac{(a_0 + a_1 p + \cdots + a_k p^k) - (a_0 + a_1 + \cdots + a_k)}{p-1} \\
&= \frac{a_1(p-1) + a_2(p^2-1) + \cdots + a_k(p^k-1)}{p-1} \\
&= \sum_{i=1}^{k} a_i \left(\sum_{j=0}^{k-1} p^j \right) \\
&= \sum_{1 \leqslant j < i \leqslant k} a_i p^j \\
&= (a_1 + a_2 p + \cdots + a_k p^{k-1}) + (a_2 + a_3 p + \cdots + a_k p^{k-2}) + \cdots + a_k \\
&= \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{n}{p^k} \right\rfloor \\
&= \sum_{i=1}^{k} \left\lfloor \frac{n}{p^i} \right\rfloor
\end{aligned}$$

Por lo tanto

$$v_p(n!) = \frac{n - S_n}{p-1} \tag{3.7}$$

■

Empecemos con la serie formal de potencias para el logaritmo en análisis real:

$$\log(1+X) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{X^n}{n} = X - \frac{X^2}{2} + \frac{X^3}{3} - \frac{X^4}{4} + \cdots.$$

Dado que sus coeficientes son números racionales, $\log(1+X)$ es un elemento de $\mathbb{Q}\big[[X]\big]$. Hemos visto (ejemplo 3.3.2) que la correspondiente serie de potencias en $\mathbb{Q}_p$, la cual denotamos por $\ln_p(1+x)$ para no confundirla con el logaritmo en base p, y llamado el *logaritmo p-ádico*, converge para $|x|_p < 1$. (Reservaremos la notación $\log(1+x)$ para la serie de potencias numérica en $\mathbb{R}$.)

De modo similar, definimos la serie

$$\ln_p(x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{(x-1)^n}{n}, \quad \in \mathbb{Q}_p\big[[X]\big] \tag{3.8}$$

la cual converge para $x \in B\colon = \{x \in \mathbb{Z}_p\colon |x-1|_p < 1\} = 1 + p\mathbb{Z}_p$.

Notemos que, si $X = x-1$, entonces $\ln_p(x) = \ln_p\big(1+(x-1)\big)$. Así

$$\ln_p(x) = \ln_p(1+X) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{X^n}{n}, \quad \in \mathbb{Q}_p\big[[X]\big].$$

LEMA 3.4.2. *El logaritmo p-ádico converge para* $D = \{x \in \mathbb{Q}_p\colon |x|_p < 1\}$.

Demostración. Por definición, ecuación (3.8)

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

Por la ecuación (3.7)

$$\left|\frac{1}{n}\right|_p^{1/n} = p^{\dfrac{v_p(n)}{n}}$$

y

$$\limsup \left|\frac{1}{n}\right|_p^{1/n} = 1,$$

de ahí que el radio de convergencia de $\ln_p(x)$ es 1. ■

LEMA 3.4.3. *La función* $\ln_p$ *es diferenciable en* $1 + p\mathbb{Z}_p$*, además*

$$\ln_p'(x) = \frac{1}{x}$$

Demostración. La derivada de $\ln_p(x)$ está dada por:

$$\begin{aligned} \ln_p'(x) &= \left(\sum_{n=1}^{\infty} (-1)^{n+1} \frac{(x-1)^n}{n}\right)' = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{n(x-1)^{n-1}}{n} \\ &= \sum_{n=1}^{\infty} (-1)^{n-1} (x-1)^{n-1} \end{aligned}$$

Sea $k = n-1$ y por (Rade and Westergren, 2004, pp 185), tenemos:

$$\sum_{k=0}^{\infty} (-1)^k (x-1)^k = \frac{(-1)}{(-1)-(x-1)} = \frac{1}{x},$$

Por lo tanto

$$\ln_p'(x) = \frac{1}{x}.$$

■

PROPOSICIÓN 3.4.1. *Si $x, y \in 1+p\mathbb{Z}_p$, entonces el logaritmo p-ádico satisface la propiedad fundamental*

$$\ln_p\big((1+x)(1+y)\big) = \ln_p(1+x) + \ln_p(1+y).$$

Demostración. Sea t una indeterminada sobre $\mathbb{Z}_p$. Por el lema 3.4.3 tenemos:

$$\ln_p'(1+t) = \sum_{n=0}^{\infty} (-1)^n t^n = \frac{1}{1+t}.$$

En la composición $\ln_p\big((1+xt)(1+yt)\big)$. Mediante las reglas formales para diferenciación, tenemos:

$$\Big(\ln_p\big((1+xt)(1+yt)\big)\Big)' = \frac{\big((1+xt)(1+yt)\big)'}{(1+xt)(1+yt)}$$

$$= \frac{(1+xt)y + (1+yt)x}{(1+xt)(1+yt)}$$

$$= \frac{x}{1+xt} + \frac{y}{1+yt}$$

$$= \sum_{n=0}^{\infty} (-1)^n x^{n+1} t^n + \sum_{n=0}^{\infty} (-1)^n y^{n+1} t^n$$

$$= \sum_{n=0}^{\infty} (-1)^n (x^{n+1} + y^{n+1}) t^n.$$

Así,

$$\Big(\ln_p\big((1+xt)(1+yt)\big)\Big)' = \sum_{n=0}^{\infty} (-1)^n (x^{n+1} + y^{n+1}) t^n.$$

Por lo tanto, los coeficientes a_n en la serie de potencias $\ln_p\big((1+xt)(1+yt)\big) = \sum_{n=0}^{\infty} a_n t^n$ están determinados por las fórmulas $na_n = (-1)^{n-1}(x^n + y^n)$, para $n \geqslant 1$.

Dado que $\mathbb{Z}_p$ es de característica cero, concluimos que

$$\ln_p\big((1+xt)(1+yt)\big) = a_0 + \sum_{n=1}^{\infty} \frac{(-1)^{n-1}(x^n + y^n) t^n}{n}$$

$$= a_0 + \sum_{n=1}^{\infty} \frac{(-1)^{n-1} x^n t^n}{n} + \sum_{n=1}^{\infty} \frac{(-1)^{n-1} y^n t^n}{n}$$

$$= a_0 + \ln_p(1+xt) + \ln_p(1+yt)$$

con algún $a_0 \in \mathbb{Z}_p$. Al sustituir $t = 0$ tenemos $a_0 = 0$. Al remplazar $t = 1$ obtenemos la afirmación:

$$\ln_p\big((1+xt)(1+yt)\big) = \ln_p(1+x) + \ln_p(1+y)$$ ■

LEMA 3.4.4. *El logaritmo p-ádico cumple* $\ln_p(x^n) = n\ln_p(x)$

Demostración. Al aplicar la proposición 3.4.1:

$$\ln_p(x^n) = \ln_p(\underbrace{x\cdots x}_{n}) = \underbrace{\ln_p(x)+\cdots+\ln_p(x)}_{n} = n\ln_p(x). \qquad \blacksquare$$

Ahora consideramos la serie formal de potencias

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

La correspondiente serie numérica de potencias en $\mathbb{R}$ converge en todas partes. Ahora estudiaremos la serie de potencias correspondiente en $\mathbb{Q}_p$; se llama la *exponencial p-ádica* y la denotamos por $\exp_p(x)$.

TEOREMA 3.4.1. *La exponencial p-ádica* $\exp_p(x)$ *converge en el disco* $D_p = \{x \in \mathbb{Q}_p : |x|_p < r_p\}$, *donde* $r_p = p^{-1/(p-1)}$ *y diverge en cualquier otro caso.*

Demostración. Primero encontraremos el radio de convergencia r_p de esta serie de potencias usando la fórmula (3.3). Aquí $a_n = \dfrac{1}{n!}$, obtenemos

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

Usamos el hecho de que,

$$r_p = \frac{1}{\limsup |a_n|_p^{1/n}}$$

es una serie de p, obtenemos la relación,

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

La última igualdad es válida dado que,

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

Y así, $r_p = p^{-1/(p-1)}$. Ahora veamos qué sucede cuando $|x|_p = p^{-1/(p-1)}$, i.e., cuando $v_p(x) = 1/(p-1)$. Podemos 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 $v_p(a_{p^m} x^{p^m}) = \frac{1}{p-1}$; de ahí que tengamos

$$\lim_{n\to\infty} |a_n x^n|_p \neq 0 \quad \text{para} \quad |x|_p = p^{-1/(p-1)},$$

y la serie diverge para $|x|_p = p^{-1/(p-1)}$. $\blacksquare$

Ejemplo 3.4.1. Si $p = 2$, el radio de convergencia es igual a $\frac{1}{2}$; de ahí que $\exp_2(x)$ converge en $4\mathbb{Z}_2$.

Si $p > 2$, el radio de convergencia es igual a $p^{-1/(p-1)}$ el que no está entre los valores posibles del valor p-ádico y dado que $\frac{1}{p} < p^{-1/(p-1)} < 1$, $\exp_p(x)$ converge en $p\mathbb{Z}_p$.

Ejemplo 3.4.2. Sea $p = 2$. Entonces $-1 \in \{x \in \mathbb{Z}_2 : |x-1|_2 < 1\}$, dado que $|-1-1|_p = \frac{1}{2} < 1$. Por lo tanto el logaritmo 2-ádico $\ln_2(-1)$ puede calcularse usando la serie de potencias, digamos

$$\ln_2(-1) = \ln_2(1-2) = -\left(2 + \frac{2^2}{2} + \frac{2^3}{3} + \cdots\right).$$

Por otro lado, tenemos

$$0 = \ln_2(1) = \ln_2(-1) + \ln_2(-1) = 2\ln_2(-1);$$

de ahí que $\ln_2(-1) = 0$. Esto significa que cuando n tiende a ∞, la suma

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

se acerca cada vez más a cero en la norma 2-ádica, i.e.,

$$v_2\left(2 + \frac{2^2}{2} + \frac{2^3}{3} + \cdots + \frac{2^n}{n}\right)$$

es divisible por potencias cada vez más altas de 2. Más precisamente, para cualquier entero positivo M, existe un n tal que

$$2^M \left| v_2\left(2 + \frac{2^2}{2} + \frac{2^3}{3} + \cdots + \frac{2^n}{n}\right).\right.$$

Consideremos la región de convergencia de $\exp_p$,

$$D_p = \left\{x \in \mathbb{Z}_p : |x|_p < p^{-\frac{1}{p-1}}\right\}.$$

Hemos visto que si $p \neq 2$, entonces $D_p = p\mathbb{Z}_p$ y $D_2 = 4\mathbb{Z}_2$.

Antes de continuar estudiando la relación entre $\exp_p$ y $\ln_p$, necesitamos el siguiente resultado,

LEMA 3.4.5. *Para cualquier* $0 < |x|_p < r_p$ *y* $n \geqslant 2$

$$\left|\frac{x^n}{n}\right| \leqslant \left|\frac{x^n}{n!}\right|_p < |x|_p < r_p.$$

Demostración. Sea $n \in \mathbb{Z}, n \geqslant 1$ y $S_n \geqslant 1$ (la suma de los dígitos de n escrito en base p). Entonces

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

Por otro lado, dado que $v_p(n) \leqslant v_p(n!)$, obtenemos

$$|n|_p \geqslant |n!|_p \geqslant p^{-\frac{n-1}{p-1}} = r_p^{n-1}.$$

Por lo tanto

$$\left|\frac{x^n}{n}\right|_p \leqslant \left|\frac{x^n}{n!}\right|_p < \left(\frac{|x|_p}{r_p}\right)^{n-1} \cdot |x|_p < |x|_p < r_p$$

para $n \geqslant 2$ y $0 < |x|_p < r_p$. ■

Hay una propiedad formal más que quisiéramos que fuera verdadera también en el contexto p-ádico: el hecho que el logaritmo y la exponencial son inversos.

PROPOSICIÓN 3.4.2. *Las funciones*

$$\exp_p\colon D_p \to 1+D_p \quad y \quad \ln_p\colon 1+D_p \to D_p$$

son inversas una de la otra, i.e., si $x \in D_p$, entonces

$$\ln_p\big(\exp_p(x)\big) = x$$

y

$$\exp_p\big(\ln_p(1+x)\big) = 1+x.$$

Demostración. Considerando las correspondientes series formales de potencias, sabemos que las relaciones de la proposición se cumplen. Así que sólo tenemos que asegurar que las series de potencias involucradas convergen. En otras palabras, debemos mostrar que $\exp_p(x) \in 1+D_p$ y $\ln_p(1+x) \in D_p$ para cualquier $x \in D_p$. De la discusión anterior se concluye la convergencia. Al aplicar el lema 3.4.5 y la proposición 1.7.2 aplicada a series, tenemos

$$|\exp_p(x)-1|_p = \left|x+\sum_{n=2}^{\infty}\frac{x^n}{n!}\right|_p \leqslant |x|_p < r_p.$$

Por el lema 3.4.5, la desigualdad anterior se cumple porque todos los términos en la suma están a menos de $|x|_p$. Por lo tanto $\exp_p(x) \in 1+D_p$ y $\exp_p\colon D_p \to 1+D_p$.

El mismo argumento funciona para el logaritmo p-ádico. Sea $1+x \in 1+D_p$. Entonces

$$|\ln_p(1+x)|_p = \left|x+\sum_{n=2}^{\infty}(-1)^{n+1}\frac{x^n}{n}\right|_p = |x|_p < r_p.$$

Otra vez, la desigualdad anterior se cumple por el lema 3.4.5 y la proposición 1.7.2 para series. Así tenemos que $\ln_p(1+x) \in D_p$ para todo $x \in D_p$ y por lo tanto $\ln_p\colon 1+D_p \to D_p$ (ver la figura 3.1).

Se cumple la afirmación. ■

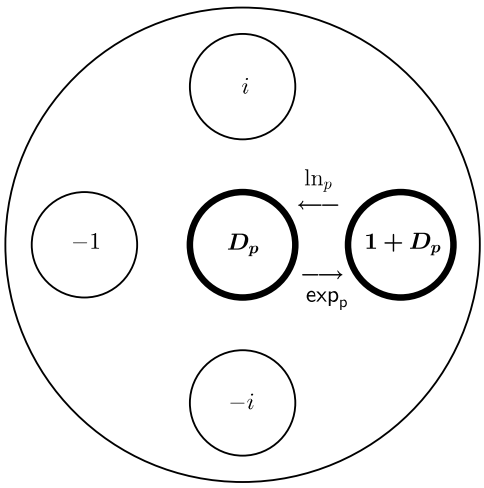

Figura 3.1: Exponencial y logaritmo p-ádicos en $\mathbb{Q}_5$.

PROPOSICIÓN 3.4.3. *Las funciones exponencial y logarítmica p-ádicas satisfacen las siguientes propiedades.*

(1) La función $\exp_p$ *es diferenciable en* D_p *y*

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

(2) $a^x = \exp_p\big(x\ln_p(a)\big)$,

(3) $(a^x)' = a^x \ln_p(a)$. *(Para* $p = 2$ *las igualdades* (2) *y* (3) *son ciertas sólo para* $a \in 1+4\mathbb{Z}_2$.*)*

Demostración.

1. Efectivamente, por la proposición 3.3.6,
$$\exp_p'(x) = \sum_{n=1}^{\infty} \frac{nx^{n-1}}{n!} = \sum_{n=1}^{\infty} \frac{x^{n-1}}{(n-1)!} = \exp_p(x).$$
2. Si $p \geqslant 3$, la función a la derecha converge para $a \in 1+p\mathbb{Z}_p$, pero si $p = 2$, sólo converge para $a \in 1+4\mathbb{Z}_2$. Para cualquier $n \in \mathbb{N}$ tenemos por la proposición 3.4.2:
$$\exp_p\big(n\ln_p(a)\big) = \exp_p\big(\ln_p(a^n)\big) = a^n,$$
i.e., las funciones coinciden en $\mathbb{N}$. El resultado se sigue de la unicidad de la serie de interpolación.
3. Esta propiedad se obtiene por diferenciación de la expresión para a^x en (3) al usar la proposición 3.4.3:
$$\begin{aligned} a^x &= \exp_p\big(\ln_p(a^x)\big) \\ &= \exp_p\big(x\ln_p(a)\big) \end{aligned}$$
Así:
$$\begin{aligned} (a^x)' &= \exp_p\big(x\ln_p(a)\big)\big(x\ln_p(a)\big)' \\ &= \exp_p\big(x\ln_p(a)\big)\big(\ln_p(a)\big) \\ &= a^x\big(\ln_p(a)\big) \end{aligned}$$
Por lo tanto,
$$(a^x)' = a^x\big(\ln_p(a)\big)$$
■

Observación 3.4.1. Notemos que la propiedad (2) de la proposición 3.4.3 implica, en particular, que $\exp_p(px) = (\exp_p p)^x$. Por el teorema 3.4.1 la serie definida por $\exp_p(x)$ diverge en $x = 1$. Sin embargo, la serie para $\exp_p(px)$ para $p \geqslant 3$ y $\exp_p(4x)$ para $p = 2$ son analíticas en $\mathbb{Z}_p$. En consecuencia, un número análogo a e no pertenece a $\mathbb{Q}_p$, pero e^p para $p \geqslant 3$ y e^4 para $p = 2$ sí pertenece a $\mathbb{Q}_p$. Así que e pertenece a una extensión algebraica de $\mathbb{Q}_p$ de grado 4 si $p = 2$ y de grado p si $p \geqslant 3$.

Justo como en el caso del logaritmo p-ádico, se preserva la propiedad formal de la exponencial en su contraparte p-ádica.

PROPOSICIÓN 3.4.4. *Si x, y pertenecen a D_p, la región de convergencia de la exponencial p-ádica. Tenemos* $\exp_p(x+y) = \exp_p(x)\exp_p(y)$.

Demostración. Del teorema 2.2.2 se sigue que

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

Por lo tanto, $\exp_p(x+y) = \exp_p(x)\exp_p(y)$ ■

Hemos refinado y hablado de las propiedades algebraicas de la exponencial y el logaritmo p-ádicos. Ahora veamos el siguiente resultado de teoría de grupos.

PROPOSICIÓN 3.4.5. *La exponencial p-ádica* $\exp_p$ *define un isomorfismo de grupos*

$$\exp_p : D_p \to 1 + D_p,$$

donde D_p es considerado como un grupo aditivo y $1+D_p$ como un grupo multiplicativo; el isomorfismo inverso es $\ln_p$.

Demostración. Verifiquemos que $1+D_p$ es un subgrupo multiplicativo de $\mathbb{Z}_p$. Esto se sigue del hecho de que D_p es un ideal en $\mathbb{Z}_p$: si $x, y \in D_p$, $x+y+xy \in D_p$ y por consiguiente $(1+x)(1+y) \in 1+D_p$. El resto es un corolario directo de las proposiciones 3.4.4 y 3.4.2. ■

Observación 3.4.2.

- $\ln_p$ da una correspondencia uno a uno entre los grupos $1+D_p$ y D_p, bajo la cual la imagen del producto es la suma de las imágenes. En particular $\ln_p$ es inyectiva.
- $1+D_p$ es el disco más grande en el que $\ln_p$ es inyectivo.
- Para $p \neq 2$, $1+D_p$ es el dominio de convergencia para $\ln_p$.
- Para $p = 2$; hemos visto en el ejemplo 3.4.2 que $|-1-1|_2 = \frac{1}{2}$, así, -1 está en $1+2\mathbb{Z}_2$, el dominio de $\ln_2$, pero no en $1+D_2 = 1+4\mathbb{Z}_2$, el dominio de $\exp_2$. Efectivamente, $\ln_2(1) = \ln_2(-1) = 0$, así, la inyectividad de $\ln_p$ se viola tan pronto como abandonamos $1+D_2$.

Este isomorfismo es análogo al caso real; en el que log y exp dan mutuamente isomorfismos inversos entre el grupo multiplicativo de números reales positivos y y el grupo aditivo de números reales.

COROLARIO 3.4.1. *El grupo multiplicativo* $1+D_p$ *es* libre de torsión*, i.e., no hay* $x \in 1+D_p, x \neq 1$*, tal que* $x^m = 1$ *para algún entero positivo m.*

Demostración. El grupo aditivo D_p es libre de torsión dado que en el campo $\mathbb{Q}_p$, la relación $my = 0$, donde $m \in \mathbb{Z}^+$ y $y \in \mathbb{Q}_p$, implica $y = 0$ y la afirmación se cumple. ■

Una propiedad interesante: la exponencial p-ádica es una isometría p-ádica. Para probarlo, necesitamos el siguiente

LEMA 3.4.6. *Para* $x \in D_p$ *tenemos*

1. $|\exp_p(x)|_p = 1$;
2. $|\ln_p(1+x)|_p = |x|_p$;
3. $|1-\exp_p(x)|_p = |x|_p$.

Demostración. Usamos las estimaciones del lema 3.4.5 y la ecuación (3.3) otra vez. En la serie

$$\exp_p(x) = 1 + x + \sum_{n=2}^{\infty} \frac{x^n}{n!}$$

el término de la norma maximal es 1. por lo tanto para $x \in D_p$, $|\exp_p(x)|_p = 1$. Dado que la serie

$$\exp_p(x) - 1 = x + \sum_{n=2}^{\infty} \frac{x^n}{n!}$$

el término de la normal maximal es x, obtenemos $|\exp_p(x) - 1|_p = |x|_p$.

De modo similar, dado que en la serie

$$\ln_p(1+x) = x + \sum_{n=2}^{\infty} (-1)^{n-1} \frac{x^n}{n!}$$

el término de la norma máxima es x, obtenemos $|\ln_p(1+x)|_p = |x|_p$. ■

COROLARIO 3.4.2. *Las aplicaciones*

$$\exp_p \colon D_p \to 1+D_p \quad y \quad \ln_p \colon 1+D_p \to D_p$$

son isometrías.

Demostración. Sean $x, y \in D_p$. Entonces

$$\begin{aligned} |\exp_p(x) - \exp_p(y)|_p &= |\exp_p(y)\big(\exp_p(x)\exp_p(-y) - 1\big)|_p \\ &= |\exp_p(y)|_p |\exp_p(x-y) - 1|_p \\ &= |\exp_p(x-y) - 1|_p \\ &= |x-y|_p, \end{aligned}$$

mostrando que la exponencial es una isometría. Ya que $\exp_p\big(\ln_p(1+x)\big) = 1+x$, tenemos

$$|\ln_p(1+x) - \ln_p(1+y)|_p = |(1+x)-(1-y)|_p = |x-y|_p,$$

que significa que el logaritmo también es una isometría. ■

Usaremos los logaritmos p-ádicos como una aplicación para determinar si las raíces (p^n)-ésimas de la unidad están en $\mathbb{Q}_p$.

Recordemos que en el caso real, las únicas raíces n-ésimas de la unidad contenidas en $\mathbb{R}$ son $\{1,-1\}$. Un fenómeno similar ocurre en el contexto p-ádico, como lo ilustra el siguiente resultado.

TEOREMA 3.4.2. *Ninguna de las raíces primitivas (p^n)-ésimas de la unidad están en $\mathbb{Q}_p$, excepto para $p=2$ y $n=1$.*

Demostración. Sea $p \neq 2$ y $x^{p^n} = 1$. Entonces debemos tener $|x|_p = 1$, i.e., $x \in \mathbb{Z}_p$, y para su primer dígito x_0 tenemos $x_0^{p^n} \equiv 1$ mód p. Sin embargo, el orden de cada elemento del grupo multiplicativo $(\mathbb{Z}/p\mathbb{Z})^\times$ debe dividir a su orden, $(p-1)$; así concluimos que $x_0 = 1$. Por lo tanto $x \in 1+p\mathbb{Z}_p$. Dado que $x^{p^n} = 1$, tenemos

$$0 = \ln_p(1) = \ln_p(x^{p^n}) = p^n \ln_p(x); \quad \text{de ahí que } \ln_p(x) = 0.$$

Pero, a partir de la inyectividad de $\ln_p$ en $1+p\mathbb{Z}_p$ (proposición 3.4.5) concluimos que $\ln_p(x) = 0$ si, y sólo si, $x = 1$, lo que implica que $x = 1$. Si $p = 2$, sin embargo, tenemos $\ln_2(-1) = \ln_2(1) = 0$ (ver ejemplo 3.4.2), y un argumento similar muestra que aunque $x = -1$ es una raíz no trivial de la unidad en $\mathbb{Q}_2$, ninguna raíz (2^n)-ésima de la unidad está en $\mathbb{Q}_2$ para $n > 1$. ■

Mayores detalles sobre los temas tocados en este capítulo se encuentran en Hasse (1980), Katok (2007), Koblitz (1984) y Mahler (1981). Un enfoque alternativo, al que hemos tomado para este tema, puede hallarse en Tran (1981).

Capítulo 4

Antiderivadas en $\mathbb{Q}_p$, Teorema de Dieudonné

El cálculo diferencial p-ádico es el objetivo principal del presente trabajo. Los temas de este capítulo están un poco fuera de dicho objetivo. Sin embargo los incluimos por ser de interés e importancia en su relación con $\mathbb{Q}_p$.

4.1. Antiderivadas

En análisis real, la antiderivación está conectada con la integración (de funciones continuas $f\colon \mathbb{R} \to \mathbb{R}$) por la fórmula

$$F(b) - F(a) = \int_a^b f(x)\,\mathrm{d}x \tag{4.1}$$

Donde F es una *antiderivada* de f. En el caso p-ádico, sin embargo, no sabemos si una 'integral' existe con propiedades similares[1]. Una conexión simple entre antiderivación e 'integración' como la dada en la ecuación (4.1) se pierde. En funciones p-ádicas se abordan los problemas de antiderivación e integración por separado. Aquí vamos a tratar la antiderivación.

Recordemos que una función f es diferenciable sobre un punto a de su dominio si $f'(a) :\ = \lim_{x\to a} \dfrac{f(x)-f(a)}{x-a}$ es finito. Luego f' es la *derivada* de f y f la *antiderivada* de f'.

Esta afirmación es verdadera si sustituimos $\mathbb{R}$ por $\mathbb{Q}_p$ o por un subconjunto X en $\mathbb{Q}_p$ sin puntos aislados.

Este resultado se conoce como *teorema de Dieudonné*, por el nombre del matemático francés JEAN-ALEXANDRE-EUGÈNE DIEUDONNÉ (1906-1992), uno de los iniciadores del proyecto Bourbaki y que hizo contribuciones importantes en diversos campos de las matemáticas, entre otros, análisis funcional, álgebra abstracta e historia de las matemáticas.

Consideremos las funciones $f\colon \mathbb{Z}_p \to \mathbb{Q}_p$. Diremos que F es una antiderivada de f y si g es otra función de $\mathbb{Z}_p \to \mathbb{Q}_p$ tal que $g' = 0$ entonces $F+g$ también es una antiderivada de f. De ahí que *si f tiene una antiderivada*

[1] En la literatura se han definido varias nociones que merecen el nombre de 'integral' p-ádica. Véase, por ejemplo, Deitmar (2010), Goldfeld and Hundley (2011), Murty (2002), Robert (2000) y Schikhof (1984).

entonces tiene 'muchas' en el sentido que *el conjunto de todas las antiderivadas de f es denso en el conjunto de funciones continuas $C(\mathbb{Z}_p, \mathbb{Q}_p)$.*

Veamos que dada una función continua $f\colon \mathbb{Z}_p \to \mathbb{Q}_p$ tiene antiderivada. Dado que no tenemos un análogo al teorema fundamental del cálculo, construiremos las antiderivadas en una forma muy diferente. Escribimos nuestra función f como una serie $\sum f_n$, donde las f_n son localmente constantes. Si ahora elegimos antiderivadas F_n para cada f_n, esperamos que $\sum F_n$ sea una antiderivada para f. Efectivamente, esto funcionará, aunque debemos tener cuidado al elegir las F_n.

Las antiderivadas, por supuesto, no son únicas ya que podemos añadir cualquier función $g \neq 0$ con $g' = 0$ para obtener alguna otra. En contraste a la situación en el cálculo real, donde todas las tales g tenían que ser constantes, el análisis p-ádico hay muchas más funciones cuya derivada es idénticamente 0, las funciones localmente constantes, por ejemplo. Pudiéramos pensar al principio que éstas son todas, pero no es el caso: consideremos a $g\colon \mathbb{Z}_p \to \mathbb{Q}_p$ definida por

$$g\left(\sum_{n=0}^{\infty} a_n p^n\right) :\ = \sum_{n=0}^{\infty} a_n p^{2n}.$$

Sean $x = \sum a_n p^n$, $y = \sum b_n p^n$. Si $x \neq y$, entonces hay un índice mínimo j tal que $a_j \neq b_j$. De ahí que

$$|x-y|_p = p^{-j} \quad \text{y} \quad |g(x)-g(y)|_p = p^{-2j},$$

la que podemos escribir como

$$|g(x)-g(y)|_p = |x-y|_p^2.$$

Entonces vemos que g' se anula en todo punto de $\mathbb{Z}_p$. Pero también se tiene que g es inyectiva y por lo tanto no es localmente constante.

Fijemos alguna notación: El (primer) *cociente de diferencias* $\Phi_1 f$ de f se define como

$$\Phi_1 f\colon \mathbb{Z}_p \times \mathbb{Z}_p \setminus \{(x,x)\colon x \in \mathbb{Z}_p \times \mathbb{Z}_p\} \to \mathbb{Q}_p, \qquad \Phi_1 f(s,t)\colon \frac{f(s)-f(t)}{s-t}.$$

Recordemos que se dice que f es una *función de clase C^1* (continuamente diferenciable o estrictamente diferenciable) si

$$\lim_{(x,y)\to(a,a)} \Phi_1 f(x,y) = f'(a) \text{ para todo } a \in \mathbb{Z}_p,$$

y escribiremos $C^1(\mathbb{Z}_p, \mathbb{Q}_p)$ para el conjunto de todas las funciones de clase C^1 definidas en $\mathbb{Z}_p$.

Lo primero es asegurarnos que dada una función continua siempre puede ser aproximada uniformemente por una suma de funciones localmente constantes.

Definición 4.1.1. $\|f\|_\infty = \sup_{x\in\mathbb{Z}_p} |f|_p$.

LEMA 4.1.1. *Si $f\colon \mathbb{Z}_p \to \mathbb{Q}_p$es una función continua, entonces hay funciones localmente constantes $f_n\colon \mathbb{Z}_p \to \mathbb{Q}_p$, tales que*

$$\lim_{N\to\infty} \left\| \sum_{n=1}^{N} f_n - f \right\|_\infty = 0.$$

Demostración. Sea $n \in \mathbb{N}$. A partir de la igualdad fuerte del triángulo decimos que

$$x \sim y \quad \text{si, y sólo si,} \quad |f(x) - f(y)|_p < \frac{1}{n}.$$

Esta relación es de equivalencia en $\mathbb{Z}_p$. Después de elegir un representante a_i para cada clase de equivalencia, definimos

$$g_n(x) := f(a_i), \quad \text{si } x \sim a_i.$$

Estas funciones son localmente constantes (lo cual es una consecuencia de la continuidad de f) y tenemos

$$|g_n(x) - f(x)|_p < \frac{1}{n}, \quad \text{para todo } x \in \mathbb{Z}_p.$$

Estamos interesados en una serie, así que establecemos

$$f_1 := g_1 \quad \text{y} \quad f_n := g_n - g_{n-1}, \quad \text{para} \quad n \geqslant 2.$$

Estas funciones aún son localmente constantes, y dado que

$$\left\| \sum_{n=1}^{N} f_n - f \right\|_\infty = \|g_N - f\|_\infty = \sup_{x \in \mathbb{Z}_p} |g_N(x) - f(x)|_p \leqslant \frac{1}{N},$$

hemos terminado. ∎

Nos interesa elegir buenas antiderivadas y el siguiente lema nos muestra cuales son las condiciones suficientes para dicha elección.

LEMA 4.1.2. *Sean $f_1, f_2, \ldots$ y f funciones continuas en $\mathbb{Z}_p$ tales que $\sum f_n$ converge uniformemente a f. Suponemos que cada f_n tiene una antiderivada continuamente diferenciable F_n tal que*

$$\text{máx}\left\{ \|F_n\|_\infty, \|\Phi_1 F_n\|_\infty \right\} \leqslant \|f_n\|_\infty$$

Entonces $\sum F_n$ converge uniformemente a $F := \sum_{n=1}^{\infty} F_n$ función de clase C^1, que es una antiderivada de f.

Demostración. Mostremos que $\sum F_n$ converge uniformemente. Dado que $\sum f_n$ converge uniformemente, sabemos que $\|f_n\|_\infty = 0$ y por el supuesto esto nos lleva a que $\lim \|F_n\|_\infty = 0$. Ya es claro ahora que $\sum F_n$ tiene que converger puntualmente a F, pero para $N \in \mathbb{N}$ aún tenemos que

$$\left\| \sum_{n=1}^{N} F_n - F \right\|_\infty + \left\| \sum_{n=N+1}^{\infty} F_n \right\|_\infty \leqslant \max_{n \geqslant N+1} \|F_n\|_\infty.$$

Este término se vuelve arbitrariamente pequeño y así $\sum F_n$ converge uniformemente a F y en consecuencia es continua.

Ahora mostremos que F es una función de clase C^1 y una antiderivada de f; en efecto, si $a \in \mathbb{Z}_p$ y $\varepsilon > 0$. Elegimos N tal que $\|f_n\|_\infty < \varepsilon$ para todo $n \geqslant N$. Entonces tenemos para todo $s, t \in \mathbb{Z}_p \times \mathbb{Z}_p, s \neq t$ y todo $n \geqslant N$:

$$|\Phi_1 F_n(s,t) - f_n(a)|_p \leqslant \text{máx}\{\|\Phi_1 F_n\|_\infty, \|f_n\|_\infty\} < \varepsilon.$$

Ahora, si $x, y \in \mathbb{Z}_p$ están suficientemente cerca de a, de tal manera que

$$|\Phi_1 F_n(x,y) - f_n(a)|_p < \varepsilon, \qquad \text{para } n = 1,2,\ldots,N,$$

eventualmente obtenemos

$$\begin{aligned} |\Phi_1 F_n(x,y) - f(a)|_p &= \left| \sum_{n=1}^{\infty} \Phi_1 F_n(x,y) - f_n(a) \right|_p \\ &\leqslant \sup_{n\in\mathbb{N}} |\Phi_1 F_n(x,y) - f_n(a)|_p \leqslant \varepsilon. \end{aligned}$$

Ya que ε fue arbitrario, F es continuamente diferenciable en a y $F'(a) = f(a)$. Esto es verdadero para cualquier $a \in \mathbb{Z}_p$. Así terminamos la prueba. ■

Ahora mostraremos que toda función localmente constante en $\mathbb{Z}_p$ tiene una antiderivada que satisface las condiciones del lema previo.

LEMA 4.1.3. *Sea $g\colon \mathbb{Z}_p \to \mathbb{Q}_p$ una función localmente continua. Entonces g tiene una antiderivada G continuamente diferenciable que satisface*

$$\max\{\|G\|_\infty, \|\Phi_1 G\|_\infty\} \leqslant \|g\|_\infty.$$

Demostración. Para un adecuado $n \in \mathbb{N}$, podemos escribir a g en la forma

$$g(x) = \sum_{m=0}^{p^n-1} \lambda_m \xi_{m+p^n\mathbb{Z}_p},$$

donde $\lambda_m \in \mathbb{Q}_p$ y $\xi_{m+p^n\mathbb{Z}_p}$ son las funciones características de $m + p^n\mathbb{Z}_p$, i.e.,

$$\xi_{m+p^n\mathbb{Z}_p}(x) = \begin{cases} 1, & \text{si } x \in m + p^n\mathbb{Z}_p, \\ 0, & \text{en otro caso.} \end{cases}$$

Una antiderivada de g está dada por

$$G(x) \colon = \sum_{m=0}^{p^n-1} \lambda_m (x-m) \xi_{m+p^n\mathbb{Z}_p},$$

donde G es una función de clase C^1.

Sea $x \in m + p^n\mathbb{Z}_p$ para algún m. Entonces $|x-m|_p \leqslant p^{-n}$ y de ahí

$$|G(x)|_p = |\lambda_m(x-m)|_p \leqslant |\lambda_m|_p.$$

Se sigue inmediatamente que $\|G\|_\infty \leqslant \max |\lambda_m|_p = \|g\|_\infty$.

Para mostrar la desigualdad

$$|\Phi_1 G(x,y)|_p \leqslant \|g\|_\infty \quad \text{para todo} \quad x, y \in \mathbb{Z}_p, x \neq y,$$

consideramos dos casos:

Primero, sean $x, y \in m + p^n\mathbb{Z}_p$, para algún m. Entonces

$$|\Phi_1 G(x,y)|_p = \left|\frac{G(x)-G(y)}{x-y}\right|_p = \left|\frac{\lambda_m(x,y)}{x-y}\right|_p = |\lambda_m|_p \leqslant \|g\|_\infty.$$

Segundo, sean $x \in m + p^n\mathbb{Z}_p$, $y \in m' + p^n\mathbb{Z}_p$, donde $m \neq m'$. Entonces $|x-m|_p \leqslant |x-y|_p$ y $|x-m'|_p \leqslant |x-y|_p$, y así

$$|\Phi_1 G(x,y)|_p = \left|\frac{G(x)-G(y)}{x-y}\right|_p = \left|\lambda_m \frac{x-m}{x-y} + \lambda_{m'}\frac{y-m'}{x-y}\right|_p \leqslant \|g\|_\infty.$$

Combinando ambos casos obtenemos $\|\Phi_1 G\|_\infty \leqslant \|g\|_\infty$, que es lo último que teníamos que mostrar. ■

Recordemos que una función es de clase C^1 si es continua con derivada continua.

TEOREMA 4.1.1 (DIEUDONNÉ)**.** *Toda función continua $f\colon \mathbb{Z}_p \to \mathbb{Q}_p$ tiene una antiderivada de clase C^1*

Demostración. Por el lema 4.1.1, sabemos que f puede escribirse como $f = \sum f_n$, donde f_n son funciones localmente constantes.

El lema 4.1.3 nos dice que cada f_n tiene una antiderivada $F_n \in C^1(\mathbb{Z}_p \to \mathbb{Q}_p)$, que satisface:

$$\text{máx}\{\|F_n\|_\infty, \|\Phi_1 F_n\|_\infty\} \leqslant \|f_n\|_\infty.$$

Luego aplicando el lema 4.1.2, el teorema queda probado. ■

Ejemplo 4.1.1. Consideremos la siguiente función en $\mathbb{Z}_p$:

$$f(x) \colon = \begin{cases} 0, & \text{si } x \neq 0 \\ 1, & \text{si } x = 0 \end{cases}$$

mostraremos que f tiene una antiderivada, dada por

$$F\left(\sum_{n=0}^{\infty} a_n p^n\right) \colon = \begin{cases} 0, & \text{si todo } a_n \text{ se anula,} \\ a_{n_0}p^{n_0} + \ldots + a_{2n_0}p^{2n_0}, & \text{en otro caso, donde } a_{n_0} \text{ es el coeficiente mínimo} \neq 0. \end{cases}$$

Sea $x = \sum_{n=n_0}^{\infty} a_n p^n$, donde $a_{n_0} \neq 0$. Cualquier $y \in \mathbb{Z}_p$ tal que $|x-y|_p < p^{-2n_0}$ debe tener los mismos primeros $2n_0$ coeficientes que x y por consiguiente $F(y) = F(x)$. Así, F es localmente constante en $\mathbb{Z}_p \setminus 0$ y tenemos $F'(x) = 0 = f(x)$ ahí. Resta ver la situación en 0: sea $y = \sum_{n=n_0}^{\infty} b_n p^n \neq 0$, donde $n_0 \neq 0$. Entonces

$$|\Phi_1 F(y,0) - 1|_p = \frac{|F(y)-y|_p}{|y|_p} = p^{n_0}\left|\sum_{n=2n_0+1}^{\infty} b_n p^n\right|_p \leqslant p^{-n_0-1}.$$

Esto se hace arbitrariamente pequeño si elegimos y bastante cerca de 0 y de ahí que $F'(0) = 1$.

Para más detalles de lo tratado en esta sección, véase Schikhof (1984).

4.2. Una muy breve reseña histórica

En Koblitz (1980) encontramos:

Hensel, *Kummer*	1850-1900	Introdujeron los números p-ádicos y desarrollaron sus propiedades básicas.
Kummer	1851	Acercamiento a congruencias para números de Bernoulli de modo *ad hoc*; sin usar números p-ádicos.
Minkowski	1884	Probó que una ecuación $a_1x_1^2+\cdots+a_nx_n^2=0$ (con a_i un racional), es resoluble en los números racionales si, y sólo si es resoluble en los reales y en los números p-ádicos para todos los primos p.
Tate	1950	Análisis de Fourier en grupos p-ádicos; dirigido a ver las interrelaciones de los números p-ádicos con funciones-L y con la teoría de representaciones.
Dwork	1960	Usó el análisis p-ádico para probar la racionalidad de la función zeta de una variedad algebraica definida sobre un campo finito, parte de las conjeturas de Weil .
Kubota, *Leopoldt*	1964	Interpretación de las congruencias de Kummer para números de Bernoulli usando la función zeta p-ádica.
Iwasawa, *Serre*, *Mazur*, *Manin*, *Katz*	1970's	Teorías p-ádicas para muchas funciones aritméticamente interesantes.
Dwork, *Grothendieck*	1970's-1980's	Ecuaciones diferenciales p-ádicas, cohomología p-ádica, cristales.
Scholze	2012	Espacios perfectoides en Scholze (2012a), Scholze (2012b) y Scholze (2014).

Bibliografía

Apostol, T. (1984). *Introducción a la teoría analítica de los números*. Editorial Reverté, S. A.

Bachman, G. (1964). *Introduction to p-adic Numbers and Valuation Theory*. Academic Press, New York.

Bojanic, R. (1974). A simple proof of Mahler's theorem on approximation of functions of p-adic variable by polynomials. *J. Number Theory*, 6:412–415.

Deitmar, A. (2010). *Automorphic Forms*. Universitext. Springer-Verlag, London.

Dummit, David S., F. R. M. (2004). *Abstract Algebra*. John Wiley & Sons, Inc., third edition.

Dunne, E. (2011). The p-adic numbers. Master thesis, Trinity College Dublin, Dublin.

Gauss, C. F. (1986). *Disquisitiones Arithmeticae*. Springer-Verlag, USA.

Goldfeld, D. and Hundley, J. (2011). *Automorphic representations and L-functions for the general linear group*, volume I. Cambridge University Press, New York.

Gouvêa, Fernando, Q. (1997). *P-adic numbers: An introduction*. Universitext. Springer-Verlag, New York, 2nd edition.

Haaser, N. B. and Sullivan, J. A. (1991). *Real analysis*. Dover Publications, Inc., New York.

Hasse, H. (1980). *Number Theory*. Springer-Verlag, Berlin.

Hensel, K. (1897). Über eine neue Begründung der Theorie der algebraischen Zahlen. *Journal Für Die Reine Und Angewandte Mathematik (Jahresbericht der Deutschen Mathematiker-Vereinigung | Jahresbericht der Deutschen Mathematiker)*, 6:83–88.

Herstein, I. N. (2002). *Álgebra moderna: Grupos, Anillos, Campos, teoría de Galois*. Trillas, 2nd edition. Coba, F. V. Trans.

Jacob, N. and Evans, K. P. (2016). *A course in analysis. Introductory Calculus. Analysis of functions of one variable*, volume I. World Scientific Publishing Co. Ltd., New York.

Katok, S. (2007). *p-adic analysis compared with real*, volume 37 of *Student Mathematical Library*. American Mathematical Society, Providence.

Khrennikov, A. Y. and Nilson, M. (2004). *P-adic Deterministic and Random Dynamics*. Springer-Science + Business media, B.V., Sweden.

Koblitz, N. (1980). *P-adic analysis : A short course on recent work*. Number 46 in London Mathematical Society Lecture Note. Cambridge, New York.

Koblitz, N. (1984). *P-adic numbers, p-adic analysis, and zeta-functions*. Springer-Verlag, New York, 2nd edition.

Mahler, K. (1981). *P-adic numbers and their functions*. Cambridge University Press, Cambridge, 2nd edition.

Murty, M. R. (2002). *Introduction to p-adic analytic number theory*, volume 27 of *Studies in Advanced Mathematics*. American Mathematical Society, International Press, Providence.

Murty, M. R. (2008). *Problems in Analytic Number Theory*. Number 206 in Graduate Texts in Mathematics. Springer, New York, 2nd edition.

Neukirch, J. (1999). *Algebraic Number Theory*. Number 322 in Grundlehren der mathematischen wissenschaften. Springer-Verlag, Heildelberg.

Rade, L. and Westergren, B. (2004). *Mathematics handbook for science and engineering*. Springer-Verlag, Berlin Heidelberg, 5th edition.

Robert, A. M. (2000). *A course in p-adic analysis*. Springer- Verlag, New York.

Rudin, W. (1976). *Principles of mathematical analysis*. McGraw-Hill International Editions, Singapore, 3rd edition.

Rudin, W. (1988). *Análisis real y complejo*. McGraw-Hill/Interamericana de España S.A., Madrid, tercera edition.

Schikhof, W. H. (1984). *Ultrametric calculus: An introduction to p-adic analysis*. Cambridge University Press, Cambridge.

Scholze, P. (2012a). Perfectoid spaces. *Publ. Math., Inst. Hautes Étud. Sci.*, (116):245–313.

Scholze, P. (2012b). Perfectoid spaces: A survey. *Current Developments in Math.*

Scholze, P. (2014). Perfectoid spaces and their applications. *Proc. of the ICM*.

Serre, J.-P. (1973). *A course in Arithmetic*. Springer-Verlag, New York.

Spivak, M. (2008). *Calculus*. Publish or Perish, Inc., Houston, 4th edition.

Tran, C. V. (1981). Studies in analysis over p-adic fields. Master's thesis, The University of Texas at El Paso, El Paso.

Apéndice A

Conceptos útiles

A.1. Grupos

Los conceptos enunciados a continuación se encuentran en Bachman (1964) y Schikhof (1984).

Grupo

Un conjunto G junto con una operación definida entre pares de elementos $a, b \in G$ (denotamos la operación por $a \cdot b$, o simplemente ab, y la llamamos *multiplicación*) la cual satisface los siguientes axiomas:

(1) Para todo $a, b \in G$, $a \cdot b \in G$ (cerradura).

(2) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (asociatividad).

(3) Existe un elemento *identidad* $\mathbf{1} \in G$ tal que $a \cdot \mathbf{1} = \mathbf{1} \cdot a = a$ para todo $a \in G$.

(4) Para cada elemento $a \in G$, existe un elemento *inverso* (de a), $a^{-1} \in G$ tal que $a \cdot a^{-1} = a^{-1} \cdot a = \mathbf{1}$.

Semigrupo

Un conjunto G que satisface sólo los dos primeros axiomas de grupo.

Grupo *conmutativo*

Un grupo G tal que, si para todo $a, b \in G$, $a \cdot b = b \cdot a$, entonces G

Grupo *abeliano*

En este caso, la operación se denota usualmente por $+$, y se escribe $a + b$ en lugar de ab. La identidad se escribe como 0, y el inverso de a como $-a$. Finalmente, escribimos $a - b$ en lugar de $a + (-b)$.

Grupo *finito*

Un grupo G que contiene un número finito de elementos. El orden de tal grupo, denotado por $|G|$ es el número de elementos de G.

Subgrupo

Un subconjunto H de un grupo G si

(1) $a, b \in H$ implica $ab \in H$;

(2) $\mathbf{1} \in H$;

(3) $a \in H$ implica $a^{-1} \in H$.

Orden de grupo

A partir del axioma de asociatividad para un grupo G se sigue que la ley asociativa se mantiene para cualquier numero finito de elementos, y, si $a_1, a_2, \ldots, a_n$ pertenecen a G, podemos escribir sin ambigüedades, $a_1 a_2 \cdots a_n$. Si todos los $a_i = a$, escribimos a^n, o na en el caso aditivo. Si para algún entero positivo n, $a^n = \mathbf{1}$, entonces decimos que a tiene orden *finito*, y el entero positivo más pequeño n es el *orden* de a y se denota $\text{ord}(a)$. Si a tiene orden finito, y si $a^k = \mathbf{1}$, entonces $\text{ord}(a)|k$.

$a \sim b$

Sea G un grupo y H un subgrupo de G. Definimos $a \sim b$ si, y sólo si, $a^{-1}b \in H$. Esta es una relación de equivalencia y $a \sim b$ si, y sólo si, $b \in aH$.

Clases laterales izquierdas

Los conjuntos de la forma aH con $a \in G$ un grupo. Tenemos que $aH = bH$, o aH y bH son disjuntos. Además, $G = \bigsqcup aH$, (la unión ajena).

Clases laterales derechas

Si $a \sim b$ si, y sólo si, $ba^{-1} \in H$; y se obtiene una descomposición de G en conjuntos de la forma Ha con $a \in G$. Tenemos que $Ha = Hb$, o Ha y Hb son disjuntos. Además, $G = \bigsqcup Ha$, (la unión ajena).

Teorema de Lagrange

El orden de un subgrupo H de un grupo finito G divide al orden de G.
Escribimos $[G:H] = \frac{|G|}{|H|}$ y $[G:H]$ es el *índice* de H en G. El orden de cualquier elemento de un grupo finito G divide al orden de G, y si $|G| = n$, entonces $a^n = 1$ para todo $a \in G$.

Grupo *cíclico*

Si existe un elemento a que pertenece al grupo G tal que cada $b \in G$ es de la forma a^m, para algún $m \in \mathbb{N}$, entonces G es un grupo *cíclico* y se dice que a es un *generador* de G; escribimos $G = [a]$.

Subgrupo *normal*	N subgrupo de G tal que $aNa^{-1} = N$ para todo $a \in G$. En el caso de un grupo abeliano, es claro que cada subgrupo es normal. Si N es un subgrupo normal de G, y si aN y bN son dos clases laterales izquierdas, entonces $(aN)(bN) = abN^2 = abN$.
Grupo *cociente*	El conjunto G/N de todas las clases laterales izquierdas aN, $a \in G$, donde N es un subgrupo normal de G, i.e., $aN \cdot bN = (aN)(bN) = abN$. Si G es un grupo finito, entonces $\lvert G/N\rvert = \frac{\lvert G\rvert}{\lvert N\rvert} = [G : N]$.
Homomorfismo de grupos	Sean G y G' dos grupos, $f\colon G \to G'$. f es un *homomorfismo de* G en G' si $f(ab) = f(a)f(b)$ para todo $a, b \in G$. Si además f es suprayectiva, entonces G' es una *imagen homomorfa* de G. Si f es un homomorfismo inyectivo y es suprayectiva, se llama *isomorfismo* y escribimos $G \simeq G'$. Un isomorfismo de un grupo en sí mismo es un *automorfismo*.
Homomorfismo *canónico* de grupos	El homomorfismo $f\colon G \to G/N$ tal que $f(a) = aN$ para todo $a \in G$; con G un grupo y N un subgrupo normal.
Núcleo o *kernel* de un homomorfismo de grupos	Un subgrupo normal $\ker(f)$ de G tal que $\ker(f) = \{a \in G\colon f(a) = \mathbf{1}'\}$, donde $f\colon G \to G'$ un homomorfismo, y $\mathbf{1}'$ es la identidad de G'.
Teorema fundamental de homomorfismos	Si $f\colon G \to G'$ es un homomorfismo de G sobre G', entonces $G' \simeq G/\ker(f)$.

A.2. Anillos e Ideales

Anillo *conmutativo*

Un conjunto A con dos operaciones, denotadas por $+$ y $\cdot$, definidas entre pares de elementos $a, b \in A$ que cumplen:

(1) A es un grupo abeliano con respecto a la operación $+$;

(2) A es un semigrupo con respecto a la operación $\cdot$;

(3) $a \cdot b = b \cdot a$ para todo $a, b \in A$;

(4) $a \cdot (b+c) = a \cdot b + a \cdot c$ para todo $a, b, c \in A$ (ley distributiva).

A partir de (4) se sigue que $a \cdot 0 = 0$ para todo $a \in A$.
En adelante omitimos la palabra conmutativo, entendemos que todos los anillos considerados son conmutativos.

Anillo con identidad

Un anillo A con un elemento $\mathbf{1} \in A$ tal que $a \cdot \mathbf{1} = a$ para todo $a \in A$.

Dominio entero

Un anillo A si $a \cdot b = 0$ implica que $a = 0$ o $b = 0$.

Unidad

Un elemento a del anillo A que tiene un inverso multiplicativo en A.

Ideal

Un subconjunto $\mathcal{I}$ de un anillo A que cumple:

(1) $a, b \in \mathcal{I}$ implica $a - b \in \mathcal{I}$;

(2) $a \in A$, $b \in \mathcal{I}$ implica $a \cdot b \in \mathcal{I}$.

Si $a \in \mathcal{I}$, un ideal, frecuentemente escribimos $a \equiv 0(\text{ mód } \mathcal{I})$.
Con respecto a la operación $+$, la condición (1) establece que el ideal, $\mathcal{I}$, es un subgrupo de A, y, dado que A es un grupo abeliano con respecto a $+$, $\mathcal{I}$ es un subgrupo normal.

Anillo cociente

El grupo cociente $A/\mathcal{I}$ de todas las clases laterales $a + \mathcal{I}$ donde $a \in A$. $A/\mathcal{I}$ puede considerarse como un anillo, donde la multiplicación se define, para $a_1, a_2 \in A$: $(a_1 + \mathcal{I}) \cdot (a_2 + \mathcal{I}) = a_1 \cdot a_2 + \mathcal{I}$,

Homomorfismo de anillos

Una aplicación $\varphi\colon A \to A'$ entre los anillos A y A'; tal que, para todo $a,b \in A\colon\ \varphi(1) = 1, \varphi(a+b) = \varphi(a) + \varphi(b)$, y $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$. Si φ es inyectiva y también suprayectiva, es un isomorfismo y A' es una *imagen isomorfa* de A. Denotamos esto por $A \simeq A'$. Un isomorfismo de un anillo sobre sí mismo es un *automorfismo*.

Núcleo o *kernel* de un homomorfismo de anillos

Un ideal $\ker(\varphi)$ del anillo A tal que $\ker(\varphi) = \{a \in A\colon\ \varphi(a) = 0'\}$, donde $\varphi\colon A \to A'$ es un homomorfismo y $0'$ es la identidad aditiva de A'.

Homomorfismo *canónico* de anillos

La función $\varphi\colon A \to A/\mathcal{I}$, donde $\mathcal{I}$ es un ideal de A, y $\varphi(a) = a + \mathcal{I}$.

Si $\varphi\colon A \to A'$ es un homomorfismo de A sobre A', entonces $A' \simeq A/\ker(\varphi)$.

Ideal *principal*

Si A es un anillo con identidad, entonces el conjunto $(a) = aA = \{ab\colon\ b \in A\}$ es un ideal que contiene a a y se llama *ideal principal* generado por a.
Todo ideal es un ideal principal en:

1. El anillo $\mathbb{Z}$;
2. El anillo $\mathbb{K}[X]$ de todos los polinomios en X con coeficientes en un campo $\mathbb{K}$.

Ideal *generado*

Si S es un subconjunto del anillo A, entonces el conjunto

$$(S) = \left\{ \sum_i a_i \cdot b_i\colon\ a_i \in A, b_i \in S \right\},$$

donde consideramos sólo las sumas finitas, es un ideal que contiene a S y se llama el ideal *generado* por S.

Ideal *primo*

Un ideal $\mathcal{I}$ en un anillo A tal que $A/\mathcal{I}$ es un dominio entero.

Ideal *máximo*

Un ideal $\mathscr{I}$ en un anillo A tal que $\mathscr{I} \neq A$ y si $\mathscr{J}$ es un ideal tal que $\mathscr{J} \supsetneq \mathscr{I}$, entonces $\mathscr{J} = A$.
Dado cualquier ideal distinto de A, donde A es un anillo con identidad, existe un ideal máximo que lo contiene (una consecuencia del Lema de Zorn).

Si A es un anillo con identidad y si $\mathscr{M}$ es un ideal máximo en A, entonces $\mathscr{M}$ es un ideal primo. Por otra parte, $A/\mathscr{M}$ es un campo. A la inversa, si $A/\mathscr{M}$ es un campo, entonces $\mathscr{M}$ es un ideal máximo.
Un campo $\mathbb{K}$, no tiene otros ideales además que $\mathbb{K}$ mismo y $\{0\}$. Entonces las únicas imágenes homomorfas de un campo son las triviales, donde enviamos todos los elementos a la unidad aditiva, o son imágenes isomorfas.

Elementos *asociados*

Sea A un anillo conmutativo con identidad. Si $a, b \in A$, entonces $b \neq 0$ *divide* a a, escrito $b|a$, si existe un elemento $c \in A$ tal que $a = b \cdot c$. Si $a|b$, y $b|a$, a y b son *asociados*.

Elemento *primo* o *irreducible*

Un elemento $a \in A$, tal que $b|a$ implica que b es una unidad de A o b es un asociado de a.

Anillo de fracciones

Sea A un anillo contenido en un campo $\mathbb{K}$ y $S \neq \emptyset$, un subconjunto de A tal que $0 \notin S$. El conjunto $\left\{\frac{a}{b} : a \in A, b \in S\right\}$ es un anillo, llamado *Anillo de fracciones* de A *por* S, que contiene a A y en el cual todos los elementos de S tienen inversos.

Dominio de ideales principales

A, un dominio entero (conmutativo) con identidad en el que cada ideal es principal.

Dominio de factorización única

A, un dominio entero (conmutativo) con identidad en el que cada elemento no-unidad y distinto de cero puede escribirse de manera única como un producto de primos excepto por el orden y multiplicación por unidades.

Dominio euclidiano

A un dominio entero (conmutativo) con identidad.
Si existe una función $\delta : A \to \mathbb{Z}$ tal que para $a, b \in A$

(a) $\delta(a) \geqslant 0$ y $= 0$ si, y sólo si, $a = 0$;

(b) $\delta(a \cdot b) = \delta(a) \cdot \delta(b)$;

(c) Si $b \neq 0$, existen $q, r \in A$ tales que $a = b \cdot q + r$, donde $\delta(r) < \delta(b)$.

Campo Un anillo $\mathbb{K}$ que además, $\mathbb{K} \setminus \{0\}$ es un grupo abeliano respecto a la operación $\cdot$.

LEMA A.2.1. *Dados A un anillo e $\mathcal{I}$ un ideal, $\mathcal{I}$ es máximo si, y sólo si, $A/\mathcal{I}$ es un campo.*

Demostración. Véase Herstein (2002). ■

TEOREMA A.2.1 (Primer teorema fundamental de isomorfismo de anillos)**.**

(1) *Si $\varphi : A \to S$ es un homomorfismo de anillos, entonces el núcleo de φ es un ideal de A, la imagen de φ es un subanillo de S y $A/\ker\varphi$ es isomorfo como anillo a $\varphi(A)$.*

(1) *Si $\mathcal{I}$ es cualquier ideal de A, entonces la aplicación*

$$A \to A/\mathcal{I} \quad \text{definida por} \quad a \mapsto a + \mathcal{I}$$

es un homomorfismo de anillos con núcleo $\mathcal{I}$ (este homomorfismo se llama la proyección natural *de A sobre $A/\mathcal{I}$). Así cada ideal es el núcleo de un homomorfismo de anillos y viceversa.*

Demostración. Véase Dummit (2004). ■