Universidad de Valladolid

FACULTAD DE CIENCIAS

TRABAJO FIN DE GRADO

Grado en Matemáticas

Introducción al análisis p-ádico

Autora: Natalia Becoechea Baños

Tutor: Alberto F. Boix

Curso 2023-3024

Índice

0. Resumen e introducción

0.1. Resumen y abstract

RESUMEN En este trabajo nos centraremos en los aspectos más básicos del análisis p-ádico, haciendo hincapié de vez en cuando en las diferencias con el análisis sobre el cuerpo de los reales. Comenzaremos introduciendo las normas no Arquimedianas y algunas de sus propiedades. A continuación construiremos a través de sucesiones de Cauchy el completado de $\mathbb{R}$ para una norma cualquiera, para posteriormente definir la norma p-ádica y el cuerpo de los números p-ádicos.
Sobre este cuerpo definiremos algunas operaciones sencillas que nos permitirán presentar un primer resultado importante: el ***Lema de Hensel*** [5, Teorema 1.39], del cual deduciremos algunos resultados de carácter algebraico sobre $\mathbb{Z}_p$. El siguiente gran teorema que veremos es el ***Teorema de Ostrowski*** [7, 2.4 Generalized Absolute Values on the Rational Field], donde se prueba que toda norma no trivial sobre $\mathbb{Q}$ es equivalente a alguna norma p-ádica (incluyendo $p = \infty$).
Seguidamente introduciremos algunos conceptos básicos de la topología p-ádica que nos ayudarán a visualizar lo abstracto de la distancia p-ádica y sus diferencias con la topología real. Finalmente estudiaremos el análisis sobre $\mathbb{Q}_p$ sin profundizar demasiado; trataremos las sucesiones y series centrándonos en las propiedades que no existen en $\mathbb{R}$, para posteriormente introducir las funciones p-ádicas. El estudio de estas nos permitirá definir la derivación, dando paso a enunciar los últimos teoremas sobre $\mathbb{R}$ y así ver que no pueden existir resultados similares en $\mathbb{Q}_p$.
ABSTRACT In this project we will focus on the most basic aspects of p-adic analysis, emphasizing from time to time the differences with the analysis on $\mathbb{R}$. We will begin by introducing non-Archimedean norms and some of their properties. Next we will construct using Cauchy sequences the completion of $\mathbb{R}$ for any norm, to later define the p-adic norm and the field of p-adic numbers. Secondly we will define some simple operations that will allow us to present an important result:***Hensel's Lemma*** [5, Theorem 1.39], from which we will deduce some algebraic results about $\mathbb{Z}_p$.
The next important theorem we will see is ***Ostrowski's Theorem*** [7, 2.4], where we prove that every non-trivial norm over $\mathbb{Q}$ is equivalent to some p-adic norm (including $p = \infty$). Next we will introduce some basic concepts of p-adic topology that will help us visualize the abstractness of the p-adic distance and its differences with real topology. Finally we will study analysis on $\mathbb{Q}_p$ without going too deep; we will talk about sequences and series focusing on the properties that do not exist in $\mathbb{R}$ to later introduce the p-adic functions. The study of these will allow us to define the derivation, leading to stating the last theorems about $\mathbb{R}$ and thus seeing that similar results cannot exist in $\mathbb{Q}_p$.

0.2. Introducción

Los números p-ádicos aparecieron por primera vez en el año 1897 de la mano del matemático alemán Kurt Hensel, y aunque en un principio se estudiaron como herramienta para llevar las técnicas utilizadas en las series de potencias a la teoría de números, pronto se vio que su interés iba mucho más allá.
Se observó que aplicándoles una cierta métrica estos obtenían una estructura de cuerpo y que este era además completo. Por otro lado se podía llegar a ellos a través de los números racionales mediante equivalencias de series de Cauchy, lo que favoreció su estudio desde un punto de vista analítico.
Desde entonces los números p-ádicos han tenido un papel importante en áreas de la Teoría de números y de la Geometría algebraica, siendo utilizados principalmente en demostraciones más como herramienta que como objeto de estudio en sí.
Así aparecen en textos académicos como ***On the Rationality of the Zeta Function of an Algebraic Variety***[3] o en teoremas importantes como el ***Principio de Hessel-Monkovski*** [8].
Por lo general la teoría de los números p-ádicos no se estudia en el grado, comprensible teniendo en cuenta el tiempo y la cantidad de materia que se debe impartir.
Sin embargo considero que los números p-ádicos son un área de gran interés, pues permiten observar más de cerca algunas particularidades que surgen de las propiedades de su norma y su estructura, y que muchas veces se estudian únicamente de forma teórica sin ver ningún ejemplo práctico.
Lo poco intuitivos que resultan es precisamente lo que los hace tan interesantes; el juego entre "cerca" y "lejos" que sugieren me parece especialmente estimulante para alumnos del grado en matemáticas. Considero que además no es un tema especialmente complejo, por lo que resultaría asequible ver una breve introducción como material adicional en alguna materia del grado (resalto que sea **breve**, viendo por ejemplo sólo los conceptos de las dos primeras secciones que engloba este texto).

Personalmente he disfrutado mucho del proceso de escritura de este trabajo; siento que no sólo he aprendido teoría de números p-ádicos, sino que he abierto la puerta a otras formas de observar las matemáticas. Como estudiante del grado en matemáticas estas no eran sólo una herramienta, sino un fin en sí mismas, y considero que los númerps p-ádicos son un bonito ejemplo de ello.

1. Números p-ádicos

1.1. Espacios normados y normas no arquimedianas

Para presentar al principal protagonista de este trabajo, el cuerpo de los números p-ádicos, vamos a introducir primero unas definiciones y lecciones básicas sobre los cuerpos normados, que resultan necesarias para nuestro objetivo.

Definición 1.1. Sea M un conjunto no vacío. La función $d : M \times M \longrightarrow \mathbb{R}_{\geq 0}$ decimos que es una *métrica* en M si cumple:

1. *Positividad:* $d(x, y) \geq 0 \ \forall x, y \in M$
2. *d es no degenerada:* $d(x, y) = 0 \Leftrightarrow x = y$
3. *Simetría:* $d(x, y) = d(y, x) \ \forall x, y \in M$
4. *Desigualdad triangular:* $d(x, y) \leq d(x, z) + d(z, y) \ \forall x, y, z \in M$

A la función d también se la llama *función distancia.*
Al par (M, d) se le denomina *espacio métrico.*

Definición 1.2. Sea (x_n) una sucesión de elementos de (M, d); es una *sucesión de Cauchy* si para todo $\epsilon > 0$ existe $n_0 \in \mathbb{N}$ tal que si $n, m \in \mathbb{N}$ son tales que $n, m > n_0$ entonces $d(x_n, x_m) < \epsilon$. Si toda sucesión de Cauchy de M converge en M diremos que M es un *espacio completo.* Si la serie converge hacia 0 diremos que es una *sucesión nula.*

Definición 1.3. Sea F un cuerpo. Una norma sobre F es una aplicación $\|\cdot\| : F \longrightarrow \mathbb{R}_{\geq 0}$ que cumple:

1. *(Positividad)* $\|x\| \geq 0$.
2. *(No degenerada):* $\|x\| = 0 \Leftrightarrow x = 0$
3. *(Propiedad multiplicativa):* $\|xy\| = \|x\|\|y\| \ \ \forall x, y \in F$
4. *Desigualdad triangular:* $\|x + y\| \leq \|x\| + \|y\|$

Al par $(F, \|\cdot\|)$ lo denominaremos *cuerpo normado*

***Observación* 1.** Vamos a denotar por n al elemento que resulta de aplicar $n \cdot 1$ al elemento unidad del cuerpo F:

$$n \cdot 1 = \underbrace{1 + 1 + ... + 1}_{\text{n veces}} \in F$$

No distinguiremos la notación entre este elemento n y el número natural n, pero serán diferenciables por el contexto.

Proposición 1.4. Algunas propiedades de una norma sobre un cuerpo son:

1. $\|1\| = \|-1\|$
2. $\|x\| = \|-x\|$
3. $\|x \pm y\| \geq |\|x\| - \|y\||$
4. $\|x - y\| \leq \|x\| + \|y\|$
5. $\|\frac{x}{y}\| = \frac{\|x\|}{\|y\|}$
6. $\|n\| \leq n \ \forall n \in \mathbb{N}$

Demostración

1. Utilizando la tercera condición de la definición tenemos que $\|1\| = \|\pm 1 \cdot \pm 1\| = \|\pm 1\|^2 \Rightarrow \|\pm 1\| = 1$
2. A partir de lo anterior: $\|-x\| = \|(-1)x\| = 1\|x\| = \|x\|$
3. $\|y\| = \|(x+y) - x\| \leq \|x+y\| + \|x\|$ por la desigualdad triangular y la propiedad anterior, y deducimos que $\|y\| - \|x\| \leq \|x+y\|$. De igual manera escribimos $\|x\| = \|(x+y) - y\| \leq \|x+y\| + \|y\|$ y deducimos que $\|x\| - \|y\| \leq \|x+y\|$. Entonces tenemos
$$-\|x+y\| \leq \|y\| - \|x\| \leq \|x+y\|$$
y por lo tanto $\|x+y\| \geq |\|y\| - \|x\||$.
Razonando igual, pero escribiendo $\|x\| = \|(x-y)+y\|$ obtenemos la desigualdad para $\|x-y\|$.
4. Podemos escribir $\|x-y\| = \|x+(-y)\| \leq \|x\| + \|y\|$ utilizando 2. y la desigualdad triangular.
5. $\|x\| = \|y\frac{x}{y}\| = \|y\|\|\frac{x}{y}\|$
6. Por inducción: para n=1 sabemos que se cumple por el primer apartado.
Suponemos que se cumple para $n-1$, veamos que se cumple para n: tenemos que $\|n\| = \|(n-1)+1\| \leq \|n-1\| + \|1\| \leq (n-1)+1 = n$ por la hipótesis de inducción. □

Una norma $\|\cdot\|$ en un cuerpo induce una métrica en él mismo: si definimos $d(x,y) = \|x-y\|$ es sencillo comprobar que cumple las propiedades de una métrica:

I. Se deduce directamente de la positividad de la norma

II. Tenemos que $d(x,y) = \|x-y\| = \|y-x\|$ pues $(x-y) = -(y-x)$.

III. $d(x,y) = \|x-y\| = \|(x-z)+(z-y)\| \leq \|x-z\| + \|z-y\| = d(x,z) + d(y,z)$

Definición 1.5. Una norma sobre un cuerpo F se llama *no Arquimediana* si satisface la desigualdad del triángulo fuerte

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

Si **no** la satisface diremos que es una *norma Arquimediana*

***Observación* 2.** La desigualdad del triángulo fuerte implica la desigualdad triangular, pero no viceversa.

La métrica inducida por una norma no Arquimediana se denomina *ultra-métrica*, y su respectivo espacio métrico un *espacio ultramétrico*.

Definición 1.6. Diremos que dos métricas d_1, d_2 sobre un cuerpo F son *equivalentes* si una sucesión es de Cauchy para d_1 si y sólo si es de Cauchy para d_2. Diremos que dos normas $\|\cdot\|_1, \|\cdot\|_2$ son *equivalentes* si las distancias que inducen son equivalentes. Lo denotaremos $\|\cdot\|_1 \sim \|\cdot\|_2$

La siguiente proposición caracteriza a las normas no Arquimedianas a partir de la norma de los números enteros.

Proposición 1.7. Las siguientes afirmaciones son equivalentes:

I. $\|\cdot\|$ es no Arquimediana.

II. $\|n\| \leq 1 \ \ \forall n \in \mathbb{N}$

Demostración
i* $\Rightarrow$ *ii: Por inducción:
Para $n = 1$: $\|1\| = 1 \leq 1$.
Suponemos que se cumple para todo $k \leq n-1$.Vemos que podemos escribir $\|n\| = \|(n-1)+1\| \leq \text{máx}\{\|n-1\|, \|1\|\} = 1$, donde hemos utilizado la hipótesis de inducción y la desigualdad del triángulo fuerte.
ii* $\Rightarrow$ *i: Tenemos que:
$\|x+y\|^n = \|(x+y)^n\| = \|\sum_{k=0}^n \binom{n}{k} x^k y^{n-k}\| \leq \sum_{k=0}^n \|\binom{n}{k}\| \|x^k\| \|y^{n-k}\| \leq \sum_{k=0}^n \|x\|^k \|y\|^{n-k} \leq$

$(n+1)\,\text{máx}\{\|x\|\|y\|\}^n$ donde hemos utilizado la desigualdad triangular en la primera desigualdad, y la hipótesis de ***ii*** en la penúltima. Luego para cada entero n tenemos que

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

y haciendo tender n a infinito obtenemos que

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

que es lo que queríamos probar.□
Esta proposición resume la principal diferencia entre una norma Arquimediana y una no Arquimediana, que podemos reescribir de la siguiente manera:

Corolario 1.8. Sobre un cuerpo F, una norma es Arquimediana si y sólo si cumple la *Propiedad Arquimediana:* dados $x, y \in F, x \neq 0$, existe un entero positivo n tal que $\|nx\| > \|y\|$.

Demostración
Si una norma cumple la Propiedad Arquimediana, dados $x, y \in F$ tales que $\|y\| > \|x\|$, existe un n entero positivo tal que $\|xn\| > \|y\|$, luego $\|n\| > \frac{\|y\|}{\|x\|} > 1$, luego es una norma Arquimediana.
Viceversa, si tenemos una norma Arquimediana, entonces existe un entero positivo n tal que $\|n\| > 1$, luego si consideramos n^k para $k \in \mathbb{N}$ tenemos que $\lim_{k\to\infty} n^k = \infty$. Entonces para cierto $k \in \mathbb{N}, \|n^k\| > \frac{\|y\|}{\|x\|}$ y por lo tanto $\|n^k x\| > \|y\|$.□

Proposición 1.9. Si dos elementos a y x de un cuerpo ultra-métrico F satisfacen la desigualdad $\|x-a\| < \|a\|$ entonces $\|a\| = \|x\|$

Demostración
Podemos escribir $\|x\| = \|(x-a)+a\| \leq \text{máx}\{\|x-a\|, \|a\|\} = \|a\|$ por hipótesis, luego $\|x\| \leq \|a\|$.
Por otro lado, $\|a\| = \|(a-x)+x\| \leq \text{máx}\{\|a-x\|, \|x\|\}$, donde si $\|x-a\| > \|x\|$ tendríamos que $\|a\| \leq \|x-a\|$ por la desigualdad que hemos visto antes, lo cual entra en contradicción con la hipótesis. Por lo tanto $\|x-a\| \leq \|x\|$ y utilizando la desigualdad del triángulo fuerte tenemos que $\|a\| \leq \|x\|$.
Concluimos que $\|x\| = \|a\|$.□

***Observación* 3.** La proposición anterior se puede reescribir como: dados $a, b \in F$ un cuerpo ultra-métrico, entonces si $\|a\| > \|b\|$ se tiene que $\|a+b\| = \|a\|$.

A continuación veremos dos proposiciones acerca de las normas no Arquimedianas. La primera resulta de especial interés, puesto que es una propiedad que entra en contraste con la situación que se da en los números reales.

Proposición 1.10. Si $\|\cdot\|$ es una norma no Arquimediana en un cuerpo F entonces cualquier punto de la bola abierta $B(a,r) = \{x : \|x-a\| < r\}$ es su centro. Es decir, dado $b \in B(a,r)$ se tiene que $B(a,r) = B(b,r)$. Esto también se da en bolas cerradas.

Demostración
Sea $b \in B(a,r)$, es decir $\|b-a\| < r$. Consideramos $c \in B(a,r)$,$\|c-a\| < r$, entonces $\|c-b\| = \|(c-a)+(a-b)\| \leq \text{máx}\{\|c-a\|, a-b\} < r$, luego $c \in B(b,r)$.
Ahora, si $c \in B(b,r)$,$\|c-b\| < r$, luego $\|c-a\| = \|(c-b)+(b-a)\| \leq \text{máx}\{\|c-b\|, \|b-a\|\} < r$, luego $c \in B(a,r)$. Concluimos que $B(a,r) = B(b,r)$.□

Proposición 1.11. Dos normas equivalentes $\|\cdot\|_1, \|\cdot\|_2$ en un cuerpo F son o bien ambas Arquimedianas o bien ambas no Arquimedianas.

Demostración
Vamos a ver que si ambas normas son equivalentes, entonces dado un elemento $x \in F$:

$i)\|x\|_1 < 1 \Leftrightarrow \|x\|_2 < 1$
$ii)\|x\|_1 > 1 \Leftrightarrow \|x\|_2 > 1$
$iii)\|x\|_1 = 1 \Leftrightarrow \|x\|_2 = 1$

Probaremos primero i: Supongamos que $\|x\|_1 < 1$ y $\|x\|_2 \geq 1$. Si consideramos la sucesión de Cauchy (x^n) sabemos que $\lim_{n\to\infty} \|x^n\|_1 = \lim_{n\to\infty} \|x\|_1^n = 0$ porque $\|x\|_1 < 1$, luego (x^n) converge y por tanto es de Cauchy para $\|\cdot\|_1$.
Por otro lado, consideramos $\epsilon = \|x-1\|_2 > 0$, porque si $\|x-1\|_2 = 0$ significaría que x=1, y necesariamente entonces $\|x\|_1 = 1$, lo cual no sucede. Entonces $\|x^{n+1} - x^n\|_2 = \|x\|_2^n \|x-1\|_2 \geq \|x-1\|_2 = \epsilon > \frac{\epsilon}{2}$. Luego para la sucesión (x^n) no se cumple la condición de Cauchy con la norma $\|\cdot\|_2$.
Llegamos por lo tanto a un absurdo, puesto que habíamos supuesto que $\|\cdot\|_1 \sim \|\cdot\|_2$. Por lo tanto, si $\|x\|_1 < 1$ entonces $\|x\|_2 < 1$. La demostración en el otro sentido es exactamente igual, y por lo tanto queda demostrado i.
Para probar ii utilizamos x^{-1}:
$\|x\|_1 > 1 \Leftrightarrow \|x^{-1}\|_1 < 1 \Leftrightarrow \|x^{-1}\|_2 < 1 \Leftrightarrow \|x\|_2 > 1$.
A partir de ambas equivalencias se deduce iii,y utilizando la proposición 1.7 concluimos la demostración.□

1.2. Completitud

La completitud es la propiedad que tienen algunos espacios métricos de que toda sucesión de Cauchy converge hacia algún elemento del espacio. Existe un proceso para obtener espacios métricos completos a partir de espacios que no lo son; la complección. Un ejemplo muy utilizado es el de los números reales, pues estos se obtienen a partir de la complección aplicada al espacio métrico $\mathbb{Q}$ con la distancia Euclídea usual, derivada del valor absoluto.

Teorema 1.12 (**Teorema de completitud**). *Todo cuerpo métrico (M, d) puede completarse, es decir: existe un cuerpo métrico $(\hat{M}, D)$ que cumple:*

1. *$\hat{M}$ es completo respecto de la métrica D.*
2. *$\hat{M}$ contiene un subconjunto $\hat{M}_0$ isométrico a M.*
3. *$\hat{M}_0$ es denso en $\hat{M}$.*

La siguiente subsección se centrará en la demostración de este teorema, que se hace de forma constructiva: para un cuerpo métrico cualquiera construimos su complección.
A continuación vamos a presentar otra forma de ver la complección de $\mathbb{Q}$ para obtener $\mathbb{R}$, que puede ayudarnos a comprender mejor el significado de completitud:
Todo número real puede escribirse como una fracción decimal infinita de la forma

$$a = \sum_{k=m}^{\infty} a_k 10^{-k} \text{con } m \in \mathbb{Z} \text{ y } a_k \in \{0, 1, 2, 3, , 4, 5, 6, 7, 8, 9\} \tag{1}$$

Esta representación es única, a no ser que $a_k = 0 \ \forall k > n$ para cierto $n \in \mathbb{N}$ y $a_n \neq 0$, en cuyo caso podemos escribir $a = \sum_{k=m}^{\infty} a'_k 10^{-k}$ donde $a_k = a'_k$ para $k < n$,$a'_n = a_n - 1$ y $a'_k = 9 \ \forall k > n$.
No es difícil construir una sucesión de Cauchy de números racionales que no converge en $\mathbb{Q}$: podemos tomar por ejemplo la sucesión de las sumas parciales de la fracción decimal infinita de $\sqrt[2]{2}$. Por lo tanto $\mathbb{Q}$ no es completo con la distancia Euclídea.
En la siguiente proposición aparecerá por primera vez en este texto el concepto de espacio cerrado, por lo que se vuelve necesario hacer previamente una observación:

***Observación* 4.** Una métrica induce siempre en el espacio sobre el que está definida una topología, que es la que consideraremos a partir de ahora. Además, un subconjunto de un espacio métrico hereda su misma métrica.
Aunque aparecerá mas adelante recordamos que un espacio métrico A es cerrado si $A = \overline{A}$, donde $\overline{A}$ denota la adherencia de A.

Proposición 1.13. Sea M un espacio métrico completo y X un subconjunto de M. Entonces X es completo si y sólo si es cerrado en M. En particular, la adherencia de X en M se puede tomar como su completado.

Demostración
$\Rightarrow$Si X es completo: tomamos $x_0 \in \bar{X}$, por definición de adherencia existirá una sucesión (x_n) en X que converge hacia x_0. Entonces (x_n) converge y por lo tanto es de Cauchy, y como X es completo, en particular converge en X. Puesto que el límite es único tenemos que $x_0 \in X$.

$\Leftarrow$Suponemos que X es cerrado: Sea (x_n) una sucesión de Cauchy de elementos de X. Como M es completo tenemos que existe $x \in M$ tal que (x_n) converge hacia x. Por definición de adherencia tenemos entonces que $x \in \bar{X}$, y puesto que X es cerrado, $x \in X$. Por lo tanto (x_n) converge en X, y concluimos que X es completo.$\square$

***Ejemplo* 1.14.** Cualquier intervalo abierto de la recta real es un espacio métrico cuyo completado es su adherencia. En particular para cualquier subconjunto abierto de $\mathbb{R}$ su completado es su adherencia. Sin embargo al contrario no se cumple: $\mathbb{Q}$ no es abierto en $\mathbb{R}$, pero $\bar{\mathbb{Q}} = \mathbb{R}$ que sí es su completado ya que para todo número real existe una sucesión de racionales que converge hacia él.

1.3. Construcción del completado de un cuerpo normado

En esta sección veremos cómo completar un cuerpo normado en el caso general. Consideramos $(\mathbb{K}, \|\cdot\|)$ un cuerpo normado, sea $C\mathbb{K}$ el conjunto de todas las sucesioness de Cauchy de $\mathbb{K}$. Definimos una suma y un producto de sucesiones de Cauchy de la siguiente manera: sean $(a_n), (b_n)$ elementos de $C\mathbb{K}$ entonces

- $(a_n) + (b_n) = (a_n + b_n)$
- $(a_n)(b_n) = (a_n b_n)$

Veamos que estas operaciones son internas en $C\mathbb{K}$:
Sean $\varepsilon > 0, N, M \in \mathbb{N}$ tales que para todo $n, m > N$, $\|a_n - a_m\| < \frac{\varepsilon}{2}$ y para todo $n, m > M$, $\|b_n - b_m\| < \frac{\varepsilon}{2}$.
Entonces para todo $n, m > max\{N, M\}$ tenemos que $\|(a_n + b_n) - (a_m + b_m)\| =$
$\|(a_n - a_m) + (b_n - b_m)\| \leq \|a_n - a_m\| + \|b_n - b_m\| < \epsilon$.
Por otro lado $\|a_n b_n - a_m b_m\| = \|a_n b_n - a_n b_m + a_n b_m - a_m b_m\| = \|a_n(b_n - b_m) + b_n(a_n - a_m)\| <$
$\|a_n\|\frac{\varepsilon}{2} + \|b_n\|\frac{\varepsilon}{2} = \frac{\varepsilon}{2}(\|a_n\| + \|b_n\|)$, donde esto lo hemos visto para un $\varepsilon > 0$ cualquiera. Luego tanto $(a_n + b_n)$ como $(a_n b_n)$ son sucesiones de Cauchy. $\square$

Definición 1.15. Sean $(a_n), (b_n)$ dos elementos de $C\mathbb{K}$, diremos que son *equivalentes* si $\lim_{n\to\infty} \|a_n - b_n\| = 0$.

Consideramos la aplicación $\mathbb{K} \longrightarrow C\mathbb{K}$

$$a \longrightarrow \hat{a} = (a, a, \ldots)$$

que envía los elementos de $\mathbb{K}$ a sucesiones constantes, que son por lo tanto de Cauchy. Mediante este monomorfismo podemos ver $\mathbb{K}$ sumergido en $C\mathbb{K}$.
Entonces $\hat{1} = (0, 0, \ldots)$, $\hat{0} = (0, 0, \ldots)$ son los elementos neutros de $C\mathbb{K}$ para el producto y la suma respectivamente.

***Observación* 5.** De esta manera hemos visto que $C\mathbb{K}$ es un anillo conmutativo con unidad. Sin embargo no es un cuerpo, puesto que contiene infinitos divisores de 0:
$(0, 1, 0, 0, \ldots)(1, 0, 1, 1, \ldots) = \hat{0}$.

Por ello consideramos el conjunto $\mathbf{N} = \{(a_n) \in C\mathbb{K} / \lim_{n\to\infty} \|a_n\| = 0\}$ de todas las sucesiones de Cauchy de $\mathbb{K}$ nulas.

Proposición 1.16. $\mathbf{N}$ es un ideal maximal en $C\mathbb{K}$.

Demostración
Primero veamos que $(\mathbf{N}, +)$ es un grupo: consideramos $(a_n), (b_n)$ elementos de $C\mathbb{K}$. Sea $\varepsilon > 0$ y $N, M \in \mathbb{N}$ tales que para todo $n > N, \|a_n\| < \frac{\varepsilon}{2}$ y para todo $m > M, \|b_n\| < \frac{\varepsilon}{2}$. Entonces para todo $k > \text{máx}\{N, M\}$ tenemos que $\|a_k + b_k\| \leq \|a_k\| + \|b_k\| < \varepsilon$ por la desigualdad triangular. Luego $(\mathbf{N}, +)$ es cerrado para la suma. Observamos que el inverso de (a_n) es $(-a_n)$, que es también nula ($\|a_n\| = \|-a_n\|$) y es obvio que $\hat{0} \in C\mathbb{K}$.
En segundo lugar veamos que si $(x_n) \in C\mathbb{K}$ y $(a_n) \in \mathbf{N}$ entonces $(x_n b_n) \in N$: sabemos que toda serie de Cauchy está acotada, luego existe $C > 0$ tal que $\|x_n\| < C$ para todo $n \in \mathbb{N}$. Ahora, sea $\varepsilon > 0$ existe $N \in \mathbb{N}$ tal que $\forall n > N, \|a_n\| < \frac{\varepsilon}{C}$. Entonces $\forall n > N \ \|a_n x_n\| < \frac{\varepsilon}{C} C = \varepsilon$, luego $(a_n x_n) \in \mathbf{N}$.
Por lo tanto $\mathbf{N}$ es in ideal sobre $C\mathbb{K}$, veamos ahora que es maximal: para ello veremos que si consideramos un elemento $(a_n) \in C\mathbb{K} \setminus \mathbf{N}$ y consideramos el ideal $(\mathbf{N}, (a_n))$, entonces $\hat{1} \in (\mathbf{N}, (a_n))$ y por lo tanto tendríamos que $(\mathbf{N}, (a_n)) = C\mathbb{K}$, luego $\mathbf{N}$ sería maximal.
Puesto que (a_n) no es nula sabemos que existe $C > 0$ y $N \in \mathbb{N}$ tal que $\forall n > N \ \|a_n\| \geq C$. Entonces dado $\varepsilon > 0$ para n y m lo suficientemente grandes tenemos que

$$\left\| \frac{1}{\|a_n\|} - \frac{1}{\|a_m\|} \right\| = \left\| \frac{a_m - a_n}{a_n a_m} \right\| \leq \frac{\varepsilon}{C^2}$$

Si definimos entonces la sucesión (b_n) como

$$b_n = \begin{cases} 1 & \text{si } a_n = 0 \\ \frac{1}{a_n} & \text{si } a_n \neq 0 \end{cases} \tag{2}$$

acabamos de ver que es una serie de Cauchy. Definimos ahora una sucesión nula de la siguiente manera:

$$x_n = \begin{cases} 1 & \text{si } a_n = 0 \\ 0 & \text{si } a_n \neq 0 \end{cases} \tag{3}$$

Por cómo están definidas tenemos que $1 = a_n b_n + x_n \ \ \forall n \in \mathbb{N}$ y como $a_n b_n$ y $x_n \in (\mathbf{N}, (a_n))$, tenemos que $\hat{1} \in (\mathbf{N}, (a_n))$. $\square$
Podemos entonces definir $\hat{\mathbb{K}} = C\mathbb{K}/\mathbf{N}$ el cociente de ambos espacios, que será un cuerpo por ser $\mathbf{N}$ maximal. ([2] Capítulo 1, Prime ideals and maximal ideals).
Definimos entonces una norma sobre $\hat{\mathbb{K}}$:

Definición 1.17. Sea $a \in \hat{\mathbb{K}}$, definimos

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

donde $a = (a_n) + \mathbf{N}$. La definición de esta norma surge de manera natural, al querer considerar una aplicación con las propiedades de la norma y que sea continua.

***Observación* 6.** Vamos a denotar la norma sobre $\hat{\mathbb{K}}$ de la misma manera que denotamos la norma sobre $\mathbb{K}$. Que se trata de una u otra será deducible por el contexto.

Proposición 1.18. $\|\cdot\|$ es una norma y está bien definida en $\hat{\mathbb{K}}$

Demostración
Veamos que la norma no depende del representante de la clase: sean $(a_n), (b_n) \in C\mathbb{K}$ de la misma clase, es decir, $(a_n) = (b_n) + (c_n)$ donde (c_n) es una sucesión nula. Entonces
$\lim_{n\to\infty} \|a_n\| = \lim_{n\to\infty} \|b_n + c_n\| \leq \lim_{n\to\infty} \|b_n\|$
$\lim_{n\to\infty} \|b_n\| = \lim_{n\to\infty} \|a_n - c_n\| \leq \lim_{n\to\infty} \|a_n\|$
donde hemos usado que $\lim_{n\to\infty} \|c_n\| = 0$, y concluimos que $\lim_{n\to\infty} \|a_n\| = \lim_{n\to\infty} \|b_n\|$.
Ahora debemos ver que la definición tiene sentido, es decir, que el límite existe: tenemos que $|\|a_n\| - \|a_m\|| \leq \|a_n - a_m\|$ por la propiedad 3 de la norma, lo que implica que la sucesión $(\|a_n\|)$ de números reales es de Cauchy, y por ser $\mathbb{R}$ un espacio completo el límite de las normas existe.
Por definición, los elementos de norma cero son las sucesiones nulas, que son justamente la clase de $\hat{0}$.
Además, sean $a, b \in \hat{\mathbb{K}}$ tenemos que $\|ab\| = \lim_{n\to\infty} \|a_n b_n\| = (\lim_{n\to\infty} \|a_n\|)(\lim_{n\to\infty} \|b_n\|) = \|a\|\|b\|$ (la separación del límite del producto en el producto de los límites puede hacerse porque $\lim_{n\to\infty} \|a_n\|$ siempre existe en $\mathbb{R}$ y es $\|a\|$. Lo mismo para b).
Por último $\|a + b\| = \lim_{n\to\infty} \|a_n + b_n\| \leq \lim_{n\to\infty} (\|a_n\| + \|b_n\|) = \|a\| + \|b\|$.$\square$

***Observación* 7.** Antes hemos visto que mediante una aplicación podíamos considerar $\mathbb{K}$ sumergido en $C\mathbb{K}$. De igual manera vamos a ver $\mathbb{K}$ como subespacio de $\hat{\mathbb{K}}$, puesto que la única sucesión constante nula es $\hat{0}$.

Teorema 1.19. *El cuerpo normado* $(\hat{\mathbb{K}}, \|\cdot\|)$ *es completo, y* $\mathbb{K}$ *es denso en* $\hat{\mathbb{K}}$.

Demostración

Veamos primero que $\mathbb{K}$ es denso en $\hat{\mathbb{K}}$: tomamos $a \in \hat{\mathbb{K}}$, que es de la forma $a = (a_n) + \mathbf{N}$ donde (a_n) es un representante de su clase de equivalencia a. Consideramos $(\hat{a}_n)$, que es una sucesión de sucesiones constantes $\hat{a}_n = (a_n, a_n, \ldots)$. Entonces si denotamos por $[\hat{a}_n]$ a la clase de equivalencia de $\hat{a}_n$ (es decir, todas las sucesiones de Cauchy en $\mathbb{K}$ cuyo límite es a_n) tenemos que $([\hat{a}_n])$ es una sucesión de elementos de $\mathbb{K}$ visto como subespacio de $\hat{\mathbb{K}}$. Entonces tenemos que

$$\lim_{n\to\infty} \|[\hat{a}_n] - a\| = \lim_{n\to\infty} (\lim_{m\to\infty} \|a_n - a_m\|) = \lim_{m,n\to\infty} \|a_n - a_m\| = 0$$

Observemos que en el primer límite lo que hemos tomado ha sido la norma sobre $\hat{\mathbb{K}}$, y que simplemente aplicamos la definición de esta norma.($\|[\hat{a}_n]\| = \|a_n\|$ por definición).Además el límite es 0 por ser (a_n) de Cauchy.

Hemos encontrado por lo tanto una sucesión de elementos de $\mathbb{K}$ que converge hacia a, luego $\mathbb{K}$ es denso en $\hat{\mathbb{K}}$.

Ahora, sea (A_n) una sucesión de Cauchy de elementos de $\hat{\mathbb{K}}$: como $\mathbb{K}$ es denso en $\hat{\mathbb{K}}$ para cada A_n existe un elemento $[\hat{a}_n] \in \mathbb{K}$ tal que

$$\|A_n - [\hat{a}_n]\| < \frac{1}{n}$$

luego $(A_n - [\hat{a}_n])$ es una sucesión de $\hat{\mathbb{K}}$ nula, y por tanto de Cauchy. Podemos escribir

$$([\hat{a}_n]) = (A_n) - (A_n - [\hat{a}_n])$$

como resta de dos sucesiones de Cauchy, luego $([\hat{a}_n])$ es una sucesión de Cauchy en $\hat{\mathbb{K}}$ y entonces

$$\|[\hat{a}_n] - [\hat{a}_m]\| = \|a_n - a_m\| < \epsilon \text{ para } n, m \text{ suficientemente grandes}$$

Luego (a_n) es de Cauchy. Aquí de nuevo estamos utilizando la definición de la norma sobre $\hat{\mathbb{K}}$.

Denotamos por a a la clase de equivalencia de la sucesión (a_n). Ya hemos visto que $\lim_{n\to\infty} \|[\hat{a}_n] - a\| = 0$ y que $\lim_{n\to\infty} \|A_n - [\hat{a}_n]\| = 0$ por definición. Luego $(a - [\hat{a}_n])$ y $(A_n - [\hat{a}_n])$ son series nulas, y por lo tanto su diferencia también lo es:

$(a - A_n) = (a - [\hat{a}_n]) - ([\hat{a}_n] - A_n)$, concluimos que $(a - A_n)$ es una sucesión nula en $\hat{\mathbb{K}}$.

Por lo tanto $\lim_{n\to\infty} \|a - A_n\| = 0$, luego $\lim_{n\to\infty} A_n = a$ y en conclusión (A_n) converge en $\hat{\mathbb{K}}$.□

Hemos demostrado de forma constructiva el teorema 1.12.

Definición 1.20. Al cuerpo $\hat{\mathbb{K}}$ se le denomina *completado de* $\mathbb{K}$ respecto de la norma $\|\cdot\|$

A continuación veremos en forma de proposición que las operaciones en $\mathbb{K}$ se extienden por continuidad sobre $\hat{\mathbb{K}}$

Proposición 1.21. Sean $([\hat{a}_n]), ([\hat{b}_n])$ sucesiones de Cauchy de $\mathbb{K} \subset \hat{\mathbb{K}}$. Entonces

- $\lim_{n\to\infty}[\hat{a}_n + \hat{b}_n] = \lim_{n\to\infty}[\hat{a}_n] + \lim_{n\to\infty}[\hat{b}_n]$
- $\lim_{n\to\infty}[\hat{a}_n\hat{b}_n] = (\lim_{n\to\infty}[\hat{a}_n])(\lim_{n\to\infty}[\hat{b}_n])$

Demostración
En la demostración anterior hemos visto que:
$\lim_{n\to\infty}[\hat{a}_n] = [(a_n)]$
$\lim_{n\to\infty}[\hat{b}_n] = [(b_n)]$
y entonces $\lim_{n\to\infty}[\hat{a}_n + \hat{b}_n] = [(a_n + b_n)] = [(a_n) + (b_n)] = [(a_n)] + [(b_n)]$ y
$\lim_{n\to\infty}[\hat{a}_n\hat{b}_n] = [(a_n b_n)] = [(a_n)(b_n)] = [(a_n)][(b_n)]$. □

1.4. El cuerpo de los números p-ádicos

Presentamos en esta subsección el principal objeto de estudio de este trabajo: el cuerpo de los números p-ádicos.

Definición 1.22. Sea $p \in \mathbb{N}$ un número primo. Para $0 \neq x \in \mathbb{Q}$ definimos *el orden p-ádico* de x como

$$ord_p(x) = \begin{cases} \text{máx}\{n \in \mathbb{N} \text{ tal que } p^n \text{ divide a } x\} & \text{si } x \in \mathbb{Z} \\ ord_p(a) - ord_p(b) & \text{si } x = \frac{a}{b}; b \neq 0, \text{ y } a, b \in \mathbb{Z} \end{cases} \tag{4}$$

Entonces definimos la *norma p-ádica* de x como

$$|x|_p = \begin{cases} p^{-ord_p(x)} & \text{si } x \neq 0 \\ 0 & \text{si } x = 0 \end{cases} \tag{5}$$

***Observación* 8.** Si $n_0 = ord_p(x)$ para $x \in \mathbb{Z}$, entonces $p^n \mid x$ para todo $n \leq n_0$

Veamos que cumple las propiedades de una norma:

1. La positividad se cumple por definición (la potencia de un número positivo es siempre estrictamente positiva)

2. Que es no degenerada también es sencillo de ver a partir de la definición por la razón anterior.

3. Multiplicatividad: Sean $x, y \in \mathbb{Q}$, $|xy|_p = p^{ord_p(xy)}$ donde $x = (xy)\frac{1}{y}$ lo que implica que $ord_p(x) = ord_p(xy) - ord_p(y)$, luego $ord_p(xy) = ord_p(x) + ord_p(y)$ y por tanto $p^{-ord_p(xy)} = p^{-ord_p(x)}p^{-ord_p(y)} = |x|_p|y|_p$.

4. Desigualdad triangular: Supongamos que $x, y \neq 0$(en caso contrario es trivial). Supongamos que $x = \frac{a}{b}, y = \frac{c}{d}$ con $a, b, c, d \in \mathbb{Z}$, entonces $x + y = \frac{ad+bc}{bd}$ y $ord_p(x + y) = ord_p(ad + bc) - ord_p(bd)$. Veamos primero que para $a, b \in \mathbb{Z}$ se tiene que $ord_p(a + b) \geq \text{mín}\{ord_p(a), ord_p(b)\}$:
Sea $n_0 = \text{mín}\{ord_p(a), ord_p(b)\}$, entonces $p^{n_0} \mid a$ y $p^{n_0} \mid b$, y por lo tanto $p^{n_0} \mid (a+b)$, luego $ord_p(a + b) \geq n_0$
Entonces

$$
\begin{aligned}
&ord_p(x + y) = ord_p(ad + bc) - ord_p(bd) \geq \\
&\geq \text{mín}\{ord_p(ad), ord_p(bc)\} - ord_p(b) - ord_p(d) = \\
&= \text{mín}\{ord_p(a) + ord_p(d), ord_p(c) + ord_p(b)\} - ord_p(b) - ord_p(d) = \\
&= \text{mín}\{ord_p(a) - ord_p(b), ord_p(c) - ord_p(d)\} = \text{mín}\{ord_p(x), ord_p(y)\} \\
&|x + y|_p = p^{-ord_p(x+y)} \leq p^{-\text{mín}\{ord_p(x), ord_p(y)\}} = \\
&p^{\text{máx}\{-ord_p(x), -ord_p(y)\}} = \text{máx}\{p^{-ord_p(x)}, p^{-ord_p(y)}\} = \\
&\text{máx}\{|x|_p, |y|_p\} \leq |x|_p + |y|_p
\end{aligned}
$$

Concluimos que $|\cdot|_p$ es una norma bien definida, y además no Arquimediana. □.

Proposición 1.23. $|\cdot|_p$ es una norma no Arquimediana.

A partir de ahora p será siempre un número primo.

***Observación* 9.** Sean p_1, p_2 dos primos distintos, las normas $|\cdot|_{p_1}, |\cdot|_{p_2}$ no son equivalentes: basta considerar la sucesión $x_n = (\frac{p_1}{p_2})^n$ para la cual
$ord_{p_1}(x_n) = ord_{p_1}(p_1^n) - ord_{p_1}(p_2^n) = n - 0 = n$, luego $|x_n|_{p_1} \xrightarrow{n\to\infty} 0$ y
$ord_{p_2}(x_n) = ord_{p_2}(p_1^n) - ord_{p_2}(p_2^n) = -n$ luego $|x_n|_{p_2} \xrightarrow{n\to\infty} \infty$.
x_n es de Cauchy para $|\cdot|_{p_1}$ pero no para $|\cdot|_{p_2}$

Por la forma en la que está definida la norma p-ádica, esta sólo puede tomar valores distintos en un conjunto discreto de la forma $\{p^n; n \in \mathbb{Z}\} \cup \{0\}$. En particular esto implica que, al contrario de lo que sucede con la norma Euclídea en $\mathbb{Q}$, dados dos números $a, b \in \mathbb{Q}$ con $|a|_p < |b|_p$, no siempre podremos encontrar otro elemento $c \in \mathbb{Q}$ tal que $|a|_p < |c|_p < |b|_p$.

Definición 1.24. Sea $p \in \mathbb{N}$ un número primo. El *cuerpo de los números p-ádicos* $\mathbb{Q}_p$ se define como la compleción de $\mathbb{Q}$ respecto de la norma $|\cdot|_p$, y sus elementos son clases de equivalencia de series de Cauchy.

La extensión se hace particularizando lo que hemos visto en la subsección anterior. De igual manera podemos considerar $\mathbb{Q}$ sumergido en $\mathbb{Q}_p$:

$$\mathbb{Q} \longrightarrow \mathbb{Q}_p \tag{6}$$

$$a \longrightarrow \hat{a} = [(a, a, \ldots)] \text{ clase de equivalencia de}$$

una sucesión de Cauchy constante.
Podemos escribir
$\mathbb{Q}_p = \{\mathbf{a} = (a_n) + N$, donde (a_n) es una serie de de elementos de $\mathbb{Q}$ de Cauchy para $|\cdot|_p\}$ y N es el conjunto de las series de elementos de $\mathbb{Q}$ nulas para $|\cdot|_p$. Una vez que tenemos el espacio, definimos sobre él una norma como hicimos para un espacio genérico:

Definición 1.25. Sea $a \in \mathbb{Q}_p$ y (a_n) una sucesión de Cauchy de elementos de $\mathbb{Q}$ que pertenezca a la clase de equivalencia de a ; $a = (a_n) + N$. Entonces

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

***Observación* 10.** Hacemos un abuso de notación, pues denotaremos la norma p-ádica sobre $\mathbb{Q}$ de la misma manera que esta nueva norma que acabamos de definir sobre $\mathbb{Q}_p$.

Al definir esta norma observamos un suceso que no ocurre con la norma euclídea: $|\cdot|_p$ toma en $\mathbb{Q}_p$ los mismos valores que toma en $\mathbb{Q}$. Esto es debido a que el conjunto de valores que puede adquirir esta norma es un conjunto discreto, $\{p^n; n \in \mathbb{Z}\} \cup \{0\}$.
En particular esto significa que dado $a \in \mathbb{Q}_p$ con $|a|_p \neq 0$, $|a|_p = p^k, k \in \mathbb{Z}$, para cualquier serie de Cauchy (a_n) que represente a a existe un $N \in \mathbb{N}$ tal que para todo $n > N$,
$|a_n|_p = p^k$.
Vamos a introducir a continuación dos proposiciones y un teorema que nos harán comprender mejor la forma que tienen los elementos de $\mathbb{Q}_p$, de una forma un poco menos abstracta.

Proposición 1.26. Sean $0 \neq d_{-m} < p$ y $0 \leq d_i < p$ enteros, $i > -m$ con $m \in \mathbb{N}$. Consideramos la serie

$$a := d_{-m}p^m + d_{-m+1}p^{-m+1} + \ldots + d_{-1}p^{-1} + d_0 + d_1 p + d_2 p^2 + \ldots \tag{7}$$

Entonces las sumas parciales de esta serie forman una sucesión de Cauchy cuyo límite es a. En consecuencia a es un elemento de $\mathbb{Q}_p$.

Demostración
Sea $\varepsilon > 0$, dados $k, n \in \mathbb{Z}$ con $k > n > m$ tenemos que $|\sum_{i=-m}^{k} d_i p^i - \sum_{i=-m}^{n} d_i p^i|_p = |\sum_{i=n+1}^{k} d_i p^i|_p \leq \text{máx}_{n<i\leq k} |d_i p^i|_p = \text{máx}_{n<i\leq k}\, p^{-i}$, luego basta tomar $N \in \mathbb{Z}$ tal que

$p^{-N} < \varepsilon$ y tomando $k > n > N$ tenemos que $|\sum_{-m}^{k} d_i - \sum_{-m}^{n} d_i p^i|_p < p^{-N} < \varepsilon$.□

Por lo tanto cada serie de la forma (7) representa un elemento de $\mathbb{Q}_p$. Los siguientes dos resultados prueban que también se cumple el recíproco: para todo elemento de $\mathbb{Q}_p$ existe una única serie de Cauchy de la forma (7) que lo represente, a la que llamaremos *forma canónica.*

***Observación* 11.** Si a es un elemento de $\mathbb{Q}_p$, a denota la clase de equivalencia de todas las sucesiones de Cauchy que convergen hacia a en $\mathbb{Q}_p$.

Proposición 1.27. Sea $x \in \mathbb{Q}$ con $|x|_p \leq 1$. Entonces para todo natural i existe un único entero $\alpha \in \{0, 1, \ldots, p^i - 1\}$ tal que $|x - \alpha|_p \leq p^{-i}$

Demostración
Sea $x = \frac{a}{b}$ donde $a, b \in \mathbb{Z}$ son primos relativos, en particular esto implica que si $ord_p(a) > 0$ entonces $ord_p(b) = 0$. Puesto que $|x|_p = p^{-ord_p(a)+ord_p(b)} \leq 1$ necesariamente $ord_p(b) = 0$, es decir, p^i no divide a b para ningún $i \in \mathbb{N}$. Aplicando la identidad de Bezout sabemos que existen enteros $m, n \in \mathbb{Z}$ tales que $np^i + mb = 1$. Tomando $\alpha = ma$ tenemos que:
$|\alpha - x|_p = |am - \frac{a}{b}|_p = |\frac{a}{b}|_p |mb - 1|_p \leq |np^i|_p = |n|_p p^{-i} \leq p^{-i}$ donde hemos utilizado la hipótesis y la caracterización de las normas no arquimedianas. Puesto que el conjunto $\{0, 1, \ldots, p^i - 1\}$ tiene exactamente p^i elementos hay un único múltiplo de p^i, cp^i tal que $cp^i + \alpha \in \{0, 1, \ldots, p^i - 1\}$, luego $|cp^i + \alpha - x|_p \leq \text{máx}\{|\alpha - x|_p, |p^i|_p\} \leq \text{máx}\{p^{-i}, p^{-i}\} = p^{-i}$.
□

Teorema 1.28. *Cada clase de equivalencia $a \in \mathbb{Q}_p$ tal que $|a|_p \leq 1$ tiene exactamente una sucesión de Cauchy (a_i) que la represente y que cumpla:*

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

II. $a_i \equiv a_{i+1} \pmod{p^i}$ *para* $i = 1, 2, \ldots$

Demostración
Sea (b_i) una sucesión de Cauchy que represente a a. Queremos encontrar una sucesión equivalente que satisfaga I y II. Ya sabemos que $|b_i|_p \xrightarrow{i \to \infty} |a|_p \leq 1$, luego sabemos que a partir de cierto i_0 $|b_i|_p \leq 1 \ \forall i \geq i_0$. Renombrando subíndices si es necesario podemos considerar una nueva serie (b_i) tal que $|b_i| \leq 1 \ \forall i \in \mathbb{N}$. Para cada $j = 1, 2, \ldots$ sea $N(j)$ un entero positivo tal que $|b_i - b_{i'}|_p \leq p^{-j} \ \forall i, i' > N(j)$, y podemos tomar $N(j) \geq j$(por ser (b_i) de Cauchy).
Entonces por la proposición anterior sabemos que existen enteros $0 \leq a_j < p^{-j}$ tales que $|a_j - b_{N(j)}| \leq p^{-j}$ para cada $j = 1, 2, \ldots$ Obtenemos entonces una sucesión (a_j) que satisface la condición de Cauchy: $|a_{j+1} - a_j|_p = |a_{j+1} - b_{N(j+1)} + b_{N(j+1)} - b_{N(j)} + b_{N(j)} - a_j|_p \leq$

máx$\{|a_{j+1} - b_{N(j+1)}|_p, |b_{N(j+1)} - b_{N(j)}|_p, |b_{N(j)} - a_j|_p\} \leq p^{-j}$.
De aquí se deduce también la condición II del teorema: $|a_j - a_{j+1}|_p = p^{-ord_p(a_j - a_{j+1})} \leq p^{-j}$ y por definición de orden tenemos que máx$\{n \in \mathbb{N}/p^n | (a_j - a_{j+1}\} \geq j$ donde $j = 1, 2, \ldots$.
Además, esta sucesión (a_i) es equivalente a (b_i): para cada j tomamos $i \geq N(j) \geq j$ y hacemos $|a_i - b_i|_p = |a_i - a_j - b_{N(j)} + b_{N(j)} - b_i|_p \leq$ máx$\{|a_i - a_j|_p, |a_j - b_{N(j)}|_p, |b_{N(j)} - b_i|\} \leq p^{-j}$, luego haciendo tender $j \to \infty$ obtenemos que $|a_i - b_i|_p \to 0$
Finalmente probamos la unicidad: sea (c_n) otra sucesión de Cauchy que represente a a y que satisface I y II, y supongamos que $(a_n) \neq (c_n)$. En particular existirá un $i_0 \in \mathbb{N}$ tal que $a_{i_0} \neq c_{i_0}$, y puesto que ambos están entre 0 y $p-1$ tenemos que $a_{i_0} \not\equiv c_{i_0} \ (mod\ p^i)$. No es difícil comprobar que si $a_i \equiv a_{i+1} \ (mod\ p^i)$ entonces $a_i \equiv a_j \ (mod\ p^i)\ \forall j \geq i$:por inducción sobre n para $j = i + n$ y utilizando la propiedad II. Luego tenemos que para todo $j \geq i_0$ $a_j \equiv a_{i_0} \not\equiv c_{i_0} \equiv c_j \ (mod\ p^{i_0})$, lo cual significa que $p^{i_0} \nmid (a_j - c_j)$ y por lo tanto
$|a_j - c_j|_p > \frac{1}{p^{i_0}}$ para todo $j \geq i_0$, y esto implica que $(a_i) \nsim (c_i)$.□.

Dado $a \in \mathbb{Q}_p$ con $|a|_p \leq 1$, si (a_i) es la sucesión de representantes del teorema anterior entonces podemos escribir cada término en base p:

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

donde $d_i \in \{0, 1, \ldots, p-1\}$, y puesto que $a_i \equiv a_{i+1} \ (mod\ p^i)$ tendremos que a_{i+1} se escribe

$$a_{i+1} = d_0 + d_1 p^1 + \ldots + d_p p^i$$

Por lo tanto el elemento a queda representado por la serie $a = \sum_{n=0}^{\infty} d_n p^n$ y podemos pensar en él como un *número* escrito en base p. También podremos escribir entonces

$$a = \ldots d_n \ldots d_2 d_1 d_0 \tag{8}$$

A esta última forma de representar a la denominaremos *extensión p-ádica canónica.*
Si $|a|_p > 1$ podemos considerar un nuevo elemento $a' = ap^m$ donde $|a|_p = p^m$, escribir su forma canónica y después dividir todos los elementos de la serie por $|a|_p$, obteniendo así

$$a = \frac{a'}{|a|_p} = \sum_{n=-m}^{\infty} d_n p^n \tag{9}$$

que es justo la foma (7).
La extensión p-ádica que vimos en (8) se escribe entonces

$$a = \cdots a_2 a_1 a_0 . a_{-1} \cdots a_{-m} \tag{10}$$

A continuación vamos a ver la relación que existe entre la representación canónica de un elemento de $\mathbb{Q}_p$ y su norma: el orden de un elemento p-ádico es el primer índice no nulo en su forma canónica.

Proposición 1.29. Sea $a = \sum_{n=0}^{\infty} d_n p^n$ un número p-ádico, con $d_n = 0$ para $n < n_0$ y $d_{n_0} \neq 0$, entonces $|a|_p = p^{-n_0}$. Si $a = \sum_{n=-m}^{\infty} d_n p^n$ con $d_{-m} \neq 0$ entonces $|a|_p = p^m$

Demostración
Por la definición de la norma en $\mathbb{Q}_p$ sabemos que $|a|_p$ es el límite de de la sucesión de normas de las sumas parciales de su forma canónica ($|a_i|_p$), y que llegado a un punto esta sucesión se estabiliza
Para $a = \sum_{n=0}^{\infty} d_n p^n$ tenemos que para todo $i > n_0$, $|a_i|_p = |d_{n_0} p^{n_0} + d_{n_0+1} p^{n_0+1} + \ldots + d_{i-1} p^{i-1}|_p \leq \text{máx}\{|d_{n_0} p^{n_0}|_p, |d_{n_0+1} p^{n_0+1} + \ldots + d_{i-1} p^{i-1}|_p\} = p^{-n_0}$ donde hemos utilizado la desigualdad del triángulo fuerte y que $|d_k| = 1$ para todo k ($0 \leq d_k < p$). Y puesto que por otro lado $p^{n_0} | a_i \ \forall i > n_0$, tenemos que $|a|_p = p^{-n_0}$
Para $a = \sum_{n=-m}^{\infty} d_n p^n$ se razona exactamente igual, y llegamos a que $|a_i| = p^m$.□

***Observación* 12.** La afirmación de que la representación de los números p-ádicos es única no es algo que se pueda dar por hecho, por ejemplo, para la representación de los números reales en base 10. Como ya vimos en (1), el número 1.000...=0.999... tiene dos representaciones.

A continuación introduciremos una nueva estructura contenida en $\mathbb{Q}_p$: el anillo de los enteros p-ádicos.

Definición 1.30. Un número p-ádico a diremos que es un *entero p-ádico* si en su forma canónica únicamente presenta potencias no negativas de p. Al conjunto de todos estos elementos lo denotaremos por $\mathbb{Z}_p$.
En particular, puesto que $|a|_p \leq 1 \Leftrightarrow p^{-ord_p(a)} \leq 1 \Leftrightarrow ord_p(a) \geq 0$ y utilizando la proposición anterior, tenemos que $\mathbb{Z}_p = \{a \in \mathbb{Q}_p / |a|_p \leq 1\}$.

Que $\mathbb{Z}_p$ es un anillo se deduce directamente de las propiedades de las operaciones definidas sobre $\mathbb{Q}_p$ que veremos más adelante.

Presentamos ahora un teorema que nos da una propiedad muy interesante de los números p-ádicos, y que utilizaremos para después ver una versión del teorema de Bolzano-Weierstrass cuya demostración será muy sencilla a partir de este resultado:

Teorema 1.31. *Toda sucesión de números enteros p-ádicos contiene una parcial (subsucesión) convergente*

Demostración

Sea (x_n) una sucesión de $\mathbb{Z}_p$, para cada término de la sucesión escribimos su extensión canónica

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

Observemos que para cada dígito de esta expresión existe sólo un número finito de posibilidades: $a_i^k \in \{0, 1, 2, \ldots, p-1\}$. Por lo tanto, eligiendo $b_0 \in \{0, 1, \ldots, p-1\}$ existe una subsucesión $(x_{0,k})$ de (x_k) tal que el último dígito de cada elemento de la subsucesión es b_0. De igual manera, para el penúltimo dígito de los elementos de $(x_{0,k})$ existe un número finito de posibilidades, luego elegimos $b_1 \in \{0, 1, \ldots, p-1\}$ y tomamos una subsucesión $(x_{1,k})$ de $(x_{0,k})$ tal que el penúltimo y último dígito de todos sus elementos son $b_1 b_0$.
Recurrentemente construimos una sucesión de sucesiones $((x_{n,k}))$ tal que todos los elementos de $(x_{n,k})$ tienen como últimos dígitos $b_n \cdots b_1 b_2$ para unos $b_n, \ldots, b_1, b_0 \in \{0, 1, \ldots, p-1\}$:

$$\begin{aligned}
(x_{0,k}) &= x_{0,1}, x_{0,2}, \ldots, x_{0,k} \ldots \\
(x_{1,k}) &= x_{1,1}, x_{1,2}, \ldots, x_{1,k} \ldots \\
&\cdots \\
(x_{n,k}) &= x_{n,1}, x_{n,2}, \cdots, x_{n,k} \ldots
\end{aligned}$$

Puesto que cada sucesión es subsucesión de la anterior, todos los elementos $(x_{n,k})$ son subsucesión de la sucesión original (x_k). En particular si tomamos la sucesión de los elementos de la diagonal $(x_{j,j})$, esta converge a $\ldots, b_n, \ldots, b_2, b_1, b_0$, y es también subsucesión de (x_k), por lo que queda probado el resultado.□

Enunciamos ahora la versión del teorema de Bolzano-Weierstrass para números p-ádicos.

Teorema 1.32 (**Teorema de Bolzano-Weierstrass**). *Toda sucesión acotada de $\mathbb{Q}_p$ contiene una parcial (subsucesión) convergente.*

Demostración

Sea (a_n) una sucesión acotada de $\mathbb{Q}_p$, podemos suponer que existe $m \in \mathbb{Z}$ tal que $|a_n|_p \leq p^m \ \forall n \in \mathbb{N}$. Por lo tanto multiplicando cada elemento de (a_n) por p^{-m} obtenemos una sucesión de elementos de norma ≤ 1, es decir, de enteros p-ádicos. Por el teorema anterior sabemos entonces que $(p^{-m} a_n)$ contiene una subsucesión convergente, y multiplicando esta por p^m obtenemos una subsucesión convergente de (a_n).□

2. Operaciones aritméticas en $\mathbb{Q}_p$ y Lema de Hensel

2.1. Operaciones. La extensión p-ádica de un número racional

Comenzamos definiendo unas operaciones sobre $\mathbb{Q}_p$, que se podrán restringir a $\mathbb{Z}_p$ teniendo en cuenta que en la representación canónica de enteros p-ádicos solo hay potencias positivas de p.
Veremos que los algoritmos son similares a los que encontramos en $\mathbb{R}$ pero que gracias a las propiedades de los números p-ádicos resultan más sencillas.

Definición 2.1. Sean $a = \sum_{n=-m}^{\infty} a_n p^n$, $b = \sum_{n=-k}^{\infty} b_n p^n$ elementos de $\mathbb{Q}_p$ tales que $a_{-m} \neq 0$ y $b_{-k} \neq 0$. Podemos suponer que $m \geq k$. Definimos la *suma* de números p-ádicos como

$$a + b := \sum_{n=-m}^{\infty} (a_n + b_n)p^n = \sum_{n=-m}^{\infty} c_n \text{ con } b_n \neq 0 \text{ para } n < -k \tag{11}$$

Debemos tener en cuenta que lo que obtenemos puede no ser la forma canónica de la suma: si $a_n = p - 1$ y $b_n = 1$ tendríamos que $c_n = p$ y obtendríamos un término de la forma pp^n.

Ilustramos la suma de números p-ádicos con un ejemplo sencillo.

***Ejemplo* 2.2.** Sea $p = 7$, entonces $9 = 2{\cdot}7^0{+}1{\cdot}7^1{+}0{\cdot}7^2{+}\ldots$ y $12 = 5{\cdot}7^0{+}1{\cdot}7^1{+}0{\cdot}7^2{+}\ldots$. Luego $9, 12 \in \mathbb{Q}_p$ son $9 = \ldots 012$ y $12 = \ldots 015$ y la suma es

$$\begin{array}{rccc} & 0 & 1 & 2 \\ + & 0 & 1 & 5 \\ \hline & 0 & 3 & 0 \end{array}$$

donde $0 \cdot 7^2 + 3 \cdot 7^1 + 0 \cdot 7^0 = 21 = 9 + 12$. Haciendo la suma de esta manera sí se obtiene la extensión p-ádica. Observamos que el método es similar a la suma decimal pero cambiando la base, utilizando también un sistema de llevadas.

Definición 2.3. Sean a y b elementos de $\mathbb{Q}_p$ como en la definición anterior. Definimos el *producto* de números p-ádicos como

$$a \cdot b := \sum_{n=-m-k}^{\infty} c_n p^n \text{ donde } c_{-m-k+l} = \sum_{i=0}^{l} a_{-m+l-i} b_{-k+i} \tag{12}$$

De nuevo, así definida la operación el resultado no tiene por qué ser la forma canónica del producto.

Vemos un ejemplo de producto de números p-ádicos.

***Ejemplo* 2.4.** Utilizamos los números del ejemplo anterior:

$$\begin{array}{cccc} & 0 & 1 & 2 \\ \times & 0 & 1 & 5 \\ \hline & & 0 & 6 & 3 \\ + & 0 & 1 & 2 & \\ \hline & & 2 & 1 & 3 \end{array}$$

donde $2 \cdot 7^2 + 1 \cdot 7^1 + 3 \cdot 7^0 = 98 + 7 + 3 = 108 = 9 \cdot 12$. Observamos que al igual que pasaba con la suma, el algoritmo del producto es como el de los números enteros pero tomando como base el primo p.

Vemos ahora una proposición que justifica que $\mathbb{Z}_p$ no es un cuerpo.

Proposición 2.5. Un entero p-ádico $a = \cdots a_1 a_0$ tiene inverso en $\mathbb{Z}_p$ para el producto si y sólo si $a_0 \neq 0$.

Demostración
$\Rightarrow$ Si $a_0 = 0$: supongamos que existe $b \in \mathbb{Z}_p$ tal que $a \cdot b = 1$. Entonces $a \cdot b = \sum_{n=0}^{\infty} c_n p^n$ donde $c_0 = a_0 b_0$ y debe cumplirse que al igualar coeficientes con 1, $c_0 = 1$. Pero $a_0 = 0$, luego $c_0 = 0$ y llegamos a un absurdo.
$\Leftarrow$ Sea $b = \sum_{n=-k}^{\infty} b_n p^n$ el inverso multiplicativo de a en $\mathbb{Q}_p$ y $a_0 \neq 0$. Entonces $a \cdot b = \sum_{n=-k}^{\infty} c_n p^n = 1$, e igualando coeficientes con 1 obtenemos que $c_{-k} = a_0 b_{-k} = 0$ y por hipótesis concluimos que $b_{-k} = 0$.
Si $k > 1$ comparamos los coeficientes de p^{-k+1} llegando a que $c_{-k+1} = a_1 b_{-k} + a_0 b_{-k+1} = 0$, luego $b_{-k+1} = 0$.
El proceso se repite k veces hasta llegar a que $c_0 = a_k b_{-k} + a_{k-1} b_{-k+1} + \ldots + a_0 b_0 = 1$ concluyendo por tanto que $b_n = 0 \ \forall n < 0$ y que $b_0 \neq 0$. Luego $b \in \mathbb{Z}_p$. $\square$
Por lo tanto sí que hay elementos en $\mathbb{Z}_p$ que tienen inverso para el producto, sin embargo $\mathbb{Z}_p$ no es cuerpo:

Corolario 2.6. $p \in \mathbb{Z}_p$ no tiene inverso multiplicativo en $\mathbb{Z}_p$, $p = 0 \cdot p^0 + 1 \cdot p^1$.

Definición 2.7. Denotemos por $\mathbb{Z}_p^*$ a los elementos de $\mathbb{Z}_p$ que son invertibles para el producto en $\mathbb{Z}_p$, y lo llamaremos *Grupo de las unidades p-ádicas.*

***Observación* 13.** Ya vimos que $\mathbb{Z}_p = \{a \in \mathbb{Q}_p / |a|_p \leq 1\}$, y sabemos que el orden p-ádico de un número es el primer índice no nulo en su forma canónica, luego
$a \in \mathbb{Z}*_p \Leftrightarrow a_0 \neq 0 \Leftrightarrow ord_p(a) = 0 \Leftrightarrow |a|_p = 1$. Entonces $\mathbb{Z}_p^* = \{a \in \mathbb{Q}_p / |a|_p = 1\}$

Para el teorema que veremos a continuación conviene recordar que $\mathbb{Q} \subset \mathbb{Q}_p$ mediante la aplicación (6).

Teorema 2.8. *Una expansión canónica de la forma* (10) *representa un número racional si y sólo si hacia la izquierda es periódica a partir de algún punto.*

Demostración

$\Rightarrow$ Sea $x \in \mathbb{Q}_p$, supongamos que su expansión p-ádica es periódica a partir de algún dígito. Multiplicando si hiciera falta por alguna potencia de p hasta que $\|x\|_p \leq 1$ y restando un entero, podemos suponer que $x \in \mathbb{Z}_p$ y que es de la forma

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

Es decir, nos quedamos con la parte periódica.

Si consideramos $a = x_0 + x_1 p + \ldots + x_{k-1}p^{k-1}$ este es un entero racional. Podemos escribir entonces $x = a(1 + p^k + p^{2k} + \ldots) = a\sum_{n=0}^{\infty} p^{nk} = a\frac{1}{1-p^k}$.

Luego x es un número racional (por ser producto de un entero por un racional). Las operaciones que pudieran haberse realizado al principio no alteran la naturaleza del x original.

$\Leftarrow$ Supongamos ahora que tenemos un número racional de la forma

$$\frac{a}{b} = \sum_{i=0}^{\infty} x_i p^i \in \mathbb{Z}_p \tag{13}$$

Podemos suponer que a y b son primos entre sí (la fracción está reducida al máximo) luego b y p son primos entre sí ($ord_p(a) \geq ord_p(b)$ y a y b primos entre sí, luego si $ord_p(a) > 0 \Rightarrow ord_p(b) = 0$).

Como $mcd(b, p^n) = 1$ por la igualdad de Bezout sabemos que existen enteros c_n, d_n tales que $1 = c_n b + d_n p^n$. Multiplicando a ambos lados por a obtenemos $a = ac_n b + ad_n p^n$.

Sumando a ac_n un múltiplo de p^n, sp^n de forma que $0 \leq A_n = ac_n + sp^n \leq p^n - 1$ tenemos que $a = A_n b + r_n p^n$ con r_n entero. Dividiendo a ambos lados por b llegamos a

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

y despejando obtenemos $r_n = \frac{(a - A_n b)}{p^n}$ y puesto que $0 \leq A_n \leq p^n - 1$ tenemos que $\frac{a-(p^n-1)b}{p^n} \leq r^n \leq \frac{a}{p^n}$. Haciendo $n \to \infty$ llegamos a

$$-b \leq r^n \leq 0$$

y concluimos que a partir de n lo suficiente grande n_0, r_n toma sólo un número finito de valores (r_n es entero). Podemos escribir

$$\tfrac{a}{b} = A_n + p^n \tfrac{r_n}{b} = A_{n+1} + p^{n+1}\tfrac{r_{n+1}}{b}$$

Luego $A_{n+1} - A_n = p^n(\frac{r_n - pr_{n+1}}{b})$, que es entero por ser resta de enteros, luego puesto que $mcd(b, p^n) = 1$ deducimos que $\frac{r_n - pr_{n+1}}{b}$ es un entero.

Entonces $A_n \equiv A_{n+1}\ (mod\ p^n)$ y además $|p^n(\frac{r_n - pr_{n+1}}{b})|_p \leq p^{-n}$, donde hemos utilizado que $ord_p(b) = 0$. Deducimos por tanto que (A_n) es la sucesión de Cauchy de sumas

parciales de una serie.
Vamos a ver que esta serie es precisamente (13). Tenemos que

$$|A_n - \frac{a}{b}|_p = |p^n \frac{r_n}{b}|_p \leq |p^n|_p = p^{-n} \xrightarrow{n\to\infty} 0$$

luego $\frac{a}{b}$ es el límite de (A_n).
Ahora, hemos construido (A_n) de forma que cumple las dos condiciones del teorema (1.28) y es una serie de Cauchy representante de la clase de equivalencia de $\frac{a}{b}$. Luego (A_n) es la sucesión de sumas parciales de la representación p-ádica canónica de $\frac{a}{b}$ (13).
Entonces $A_{n+1} = A_n + x_n p^n$ donde $x_n = \frac{r_n - r_{n+1}p}{b} \Rightarrow r_n = x_n b + r_{n+1}p$. Como para n lo suficientemente grande r_n sólo toma un número finito de valores, existe un índice m y un entero positivo P tales que $r_m = r_{m+P}$ y por lo tanto

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

Puesto que $mcd(b, p^n) = 1$ deducimos que p divide a $(x_m - x_{m+P})$, pero tanto x_m como $x_{m+P} \in \{0, 1, \ldots, p-1\}$, luego $(x_m - x_{m+P}) = 0 \Rightarrow x_m = x_{m+P}$. Sustituyendo en $r_m = r_{m+P}$ obtenemos que también $r_{m+1} = r_{m+P+1}$.
Recurrentemente concluimos que

$$r_n = r_{n+P}$$
$$x_n = x_{n+P} \ \forall n > m.$$

Hacemos una última observación: hemos comenzado el teorema suponiendo que $\frac{a}{b} \in \mathbb{Z}_p$. De no ser así, tendríamos que $\frac{a}{b} = \sum_{n=-m}^{\infty} x_n p^n$ con $x_{-m} \neq 0$, en cuyo caso $|\frac{a}{b}|_p = p^m$, luego es suficiente con considerar $\frac{p^m a}{b}$ pues $|\frac{p^m a}{b}|_p = 1$.□

2.2. Lema de Hensel

Una vez vistas las operaciones aritméticas en $\mathbb{Q}_p$ resulta inevitable darse cuenta de las similitudes que existen entre $\mathbb{Z}_p$ y el cuerpo finito de p elementos $\mathbb{F}_p$. Un ejemplo sería los elementos que tienen inverso para el producto: en $\mathbb{F}_p$ todos los elementos menos el $\bar{0}$ (es decir, los múltiplos de p) tienen inverso. En $\mathbb{Z}_p$ los elementos tienen inverso si y sólo si $a_0 \neq 0$, es decir, todos aquellos que no son múltiplos de p. En esta sección trataremos de profundizar un poco más en esa relación, y para ello comenzamos presentando el siguiente lema:

Teorema 2.9 (**Lema de Hensel**). *Consideramos un polinomio de coeficientes en $\mathbb{Z}_p$, $P(x) = c_0 + c_1 x + \ldots + c_n x^n$ con derivada $P'(x) = c_1 + 2c_2 x + \ldots + n c_n x^{n-1}$. Supongamos que existe $a_0 \in \mathbb{F}_p$ tal que $P(a_0) \equiv 0 \pmod{p}$ y $P'(a_0) \not\equiv 0 \pmod{p}$. Entonces existe un único entero p-ádico a tal que $P(a) = 0$ y $a \equiv a_0 \pmod{p}$.*

Demostración

Construiremos el elemento a del enunciado dando su forma p-ádica canónica $a = \sum_{n=0}^{\infty} b_n p^n$ inductivamente sobre k de la siguiente manera:

Para $k = 0$ tomamos b_0 como a_0, luego es claro que $P(b_0) \equiv 0 \ (mod \ p)$ por las hipótesis del enunciado.

Supongamos que ya tenemos $b_0, b_1, \ldots, b_k \in \{0, 1, \ldots, p-1\}$ tales que $a_k = b_0 + b_1 p + \ldots + b_k p^k$ de forma que $P(a_k) \equiv 0 \ (mod \ p^{k+1})$ y $a_k \equiv a_0 \ (mod \ p)$.

Veamos que tenemos entonces a_{k+1}: sea $a_{k+1} = a_k + b_{k+1} p^{k+1}$ para algún b_{k+1} que vamos a determinar.

Evaluamos

$$P(a_{k+1}) = P(a_k + b_{k+1} p^{k+1}) =$$
$$\sum_{i=0}^{n} c_i (a_k + b_{k+1} p^{k+1})^i =$$
$$c_0 + \sum_{i=1}^{n} c_i (a_k^i + i a_k^{i-1} b_{k+1} p^{k+1} + \text{términos divisibles por } p^{k+2}) \equiv$$
$$P(a_k) + b_{k+1} p^{k+1} P'(a_k) \ (mod \ p^{k+2})$$

Puesto que $P(a_k) \equiv 0 \ (mod \ p^{k+1})$ por la hipótesis de inducción, podemos escribir

$$P(a_{k+1}) \equiv \alpha_{k+1} p^{k+1} + b_{k+1} p^{k+1} P'(a_k) = p^{k+1}(\alpha_{k+1} + P'(a_k) b_{k+1}) \ (mod \ p^{k+2}).$$

Imponiendo que $P(a_{k+1}) \equiv 0 \ (mod \ p^{k+2})$ llegamos a

$$\alpha_{k+1} + b_{k+1} P'(a_k) \equiv 0 \ (mod \ p)$$

y de aquí podemos despejar b_{k+1} teniendo en cuenta que como $a_k \equiv a_0 \ (mod \ p)$ se cumple $P'(a_k) \equiv P'(a_0) \not\equiv 0 \ (mod \ p)$, luego concluimos que

$$b_{k+1} \equiv -\frac{\alpha_{k+1}}{P'(a_k)} \ (mod \ p) \tag{14}$$

y obtenemos a_{k+1} tal que $P(a_{k+1}) \equiv 0 \ (mod \ p^{k+2})$ y $a_{k+1} \equiv a_0 \ (mod \ p)$. Por lo tanto $P(a) \equiv 0 \ (mod \ p^k)$ para todo k, y concluimos que $P(a) = 0$ y que $a \equiv a_0 \ (mod \ p)$. □

***Observación* 14.** En la demostración anterior se utiliza un método similar al método de Newton; recordemos que este método consistía en buscar una raíz real de un polinomio $f(x)$ de coeficientes reales. Se partía de una raíz aproximada a_0 tal que $f'(a_0) \neq 0$ y se construía una sucesión de elementos (a_n) tales que $f'(a_n) \neq 0$ siguiendo

$$a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)} \tag{15}$$

que no es muy diferente de la fórmula (14)

$$b_{k+1}p^{k+1} \equiv -\frac{\alpha_{k+1}p^{k+1}}{P'(a_k)} \equiv -\frac{P(a_k)}{P'(a_k)} \ (mod\ p^{k+2})$$

La convergencia de esta sucesión (a_n) sin embargo dependía del polinomio y de la primera aproximación tomada a_0.
En el caso p-ádico la convergencia, como hemos visto en el lema de Hensel, está garantizada.

Utilizamos ahora el lema de Hensel para la obtención de raíces en los enteros p-ádicos.

Proposición 2.10. Un polinomio de coeficientes enteros (en $\mathbb{Z}[x]$) tiene una raíz en $\mathbb{Z}_p$ si y sólo si tiene una raíz entera módulo p^k para cualquier $k \geq 1$

Demostración
$\Rightarrow$ Denotamos por $P(x)$ el polinomio de coeficientes enteros, y suponemos que $a \in \mathbb{Z}_p$ es raíz suya: $P(a) = 0$. Por el teorema 1.28 sabemos que existe una única sucesión de enteros $\{a_1, a_2, \ldots\}$ donde $a_k = b_0 + b_1 p + \ldots + b_{k-1}p^{k-1}$, tal que $a \equiv a_k \ (mod\ p^k)$. Entonces $P(a_k) \equiv P(a) \ (mod\ p^k)$ y $P(a) = 0$ implica $P(a_k) \equiv 0 \ (mod\ p^k)$ para todo k.
$\Leftarrow$ Supongamos ahora que existen $a_k \in \mathbb{Z}$ con $k \geq 1$ tales que $P(a_k) \equiv 0 \ (mod\ p^k)$. Podemos considerar $\mathbb{Z} \subset \mathbb{Q}_p$ utilizando el mismo morfismo que usamos para $\mathbb{Q}$, y a partir de ahí es sencillo ver que $\mathbb{Z} \subset \mathbb{Z}_p$. Luego aplicando el teorema (1.31) sabemos que (a_n) contiene una parcial (a_{k_i}) convergente $\lim_{i\to\infty} a_{k_i} = a$ para cierto $a \in \mathbb{Z}_p$. Veamos que este a es raíz de P: por la proposición 1.21 sabemos que la suma del límite es el límite de la suma, y lo mismo para el producto, luego $P(a) = P(\lim_{i\to\infty} a_{k_i}) = \lim_{i\to\infty} P(a_{k_i})$. Por otro lado $P(a_{k_i}) \equiv 0 \ (mod\ p^{k_i}) \Rightarrow$ por lo que $\lim_{i\to\infty} P(a_{k_i}) = 0$. Luego $P(a) = 0$.□

***Observación* 15.** Una consecuencia inmediata de este teorema es que si un polinomio de coeficientes enteros no tiene ninguna raíz módulo p, entonces no tiene ninguna raíz en $\mathbb{Z}_p$. Por otro lado, por el lema de Hensel, si tiene una raíz simple módulo p, entonces tiene una raíz simple en $\mathbb{Z}_p$.

Proposición 2.11. Un entero a no divisible por p tiene una raíz cuadrada en $\mathbb{Z}_p$ $(p \neq 2)$ si y sólo si a tiene una raíz cuadrada módulo p.

Demostración
Para ver que a tiene una raíz cuadrada en $\mathbb{Z}_p$ debemos ver que $P(x) = x^2 - a$ tiene raíz en $\mathbb{Z}_p$. Observemos que $P'(x) = 2x$.
$\Leftarrow$ Supongamos que existe $a_0 \in \{1, 2, \ldots, p-1\}$ tal que $a \equiv a_0^2 \ (mod\ p)$. Es decir, $P(a_0) \equiv 0 \ (mod\ p)$, pero $P'(a_0) = 2a_0 \not\equiv 0 \ (mod\ p)$, luego por el lema de Hensel la

solución de $P(x) = 0$ existe en $\mathbb{Z}_p$.
$\Rightarrow$ Si $P(x)$ no tuviera raíces $(mod\ p)$ por el teorema anterior no tiene raíces en $\mathbb{Z}_p$, y en consecuencia a no tiene raíces en $\mathbb{Z}_{|}$.$\square$

***Ejemplo* 2.12.** Si consideramos $\sqrt{2}$ es sencillo ver que $\sqrt{2} \in \mathbb{Z}_7$, pues $2 \equiv 9 = 3^2\ (mod\ 7)$. Podemos utilizar el método de Newton tomando como primera raíz aproximada $x_0 = 3$, y utilizando la fórmula de recurrencia (15) que podemos escribir en este caso como $x_{n+1} = \frac{x_n^2+2}{2x_n}$ vamos obteniendo una expresión decimal que se aproxima al valor de $\sqrt{2}$:

$$x_1 = \frac{3^2+2}{2\cdot 3} = \frac{11}{6}$$
$$x_2 = \frac{\frac{121}{36}+2}{\frac{11}{3}} = \frac{579}{11\cdot 36} = \frac{193}{132}$$
$$x_3 = \frac{9516804}{6725664} \approx 1{,}41499\ldots$$

Un ejemplo similar a este se puede encontrar en el siguiente url:
`https://math.stackexchange.com/questions/88488/square-roots-in-the-p-adics`

2.3. Algunas propiedades algebraicas de los enteros p-ádicos

Así como antes hemos hecho un pequeño hincapié en las similitudes de $\mathbb{Z}_p$ y $\mathbb{F}_p$, vamos ahora a profundizar brevemente en las diferencias que existen entre $\mathbb{Z}$ y $\mathbb{Z}_p$.
Sabemos que $\mathbb{Z}$ es un anillo conmutativo con unidad: presenta dos operaciones internas,$+$ y $\cdot$, para ambas cumple conmutatividad y asociatividad, existen inverso y neutro para la suma y el producto es distributivo con respecto de la suma.
Veremos primero un par de definiciones básicas.

Definición 2.13. Un subconjunto I de un anillo R se denomina *ideal* si I es subgrupo de R para la suma, y para todo $x \in I, r \in R$ se tiene que $x \cdot r \in I$. Un ideal se dice *maximal* si no está contenido en ningún otro.

Definición 2.14. Un anillo conmutativo sin divisores de cero se denomina un *dominio de integridad.*

Proposición 2.15. $\mathbb{Z}_p$ es un anillo conmutativo. De hecho es un dominio de integridad.

Demostración
Que $\mathbb{Z}_p$ es un anillo conmutativo se deduce de las propiedades de la suma y el producto

sobre $\mathbb{Z}$:

- $a+b=\sum_{n=0}^{\infty}(a_n+b_n)p^n=\sum_{n=0}^{\infty}(b_n+a_n)p^n=b+a$
- $(a+b)+c=\sum_{n=0}^{\infty}[(a_n+b_n)+c_n]p^n=\sum_{n=0}^{\infty}[a_n+(b_n+c_n)]p^n=a+(b+c)$
- $ab=\sum_{n=0}^{\infty}d_np^n=\sum_{n=0}^{\infty}(\sum_{i=0}^{n}a_{n-i}b_i)p^n=\sum_{n=0}^{\infty}(\sum_{i=0}^{n}a_ib_{n-i})p^n=ba$
- $(ab)c=(\sum_{n=0}^{\infty}d_np^n)c=\sum_{n=0}^{\infty}e_np^n$ donde $e_n=\sum_{l=0}^{n}d_{n-l}c_l=\sum_{l=0}^{n}(\sum_{i=0}^{n-l}a_{(n-l)-i}b_i)c_l$

y haciendo el cambio $k=n-l$

$e_n=\sum_{k=0}^{n}(\sum_{i=0}^{k}a_{k-i}b_i)c_{n-k}=\sum_{k=0}^{n}a_k(\sum_{i=0}^{n-k}b_ic_{(n-k)-i})=\sum_{k=0}^{n}a_kw_{n-k}$ luego tenemos que

$(ab)c=(\sum_{n=0}^{\infty}d_np^n)c=a(\sum_{n=0}^{\infty}w_np^n)=a(bc)$

- $(a+b)c=\sum_{n=0}^{\infty}(a_n+b_n)c=\sum_{n=0}^{\infty}(\sum_{i=0}^{n}(a_{n-i}+b_{n-i})c_i)p^n=\sum_{n=0}^{\infty}(\sum_{i=0}^{n}a_{n-i}c_i+\sum_{i=0}^{n}b_{n-i}c_i)p^n$

$=\sum_{n=0}^{\infty}(\sum_{i=0}^{n}a_{n-i}c_i)p^n+\sum_{n=0}^{\infty}(\sum_{i=0}^{n}b_{n-i}c_i)p^n=ac+bc$

Luego $\mathbb{Z}_p$ es un anillo conmutativo que además tiene unidad $1\in\mathbb{Z}\subset\mathbb{Z}_p$. Ahora, $\mathbb{Z}_p\subset\mathbb{Q}_p$ que sabemos que es un cuerpo, luego no tiene divisores de cero y en consecuencia $\mathbb{Z}_p$ tampoco.□

Recordemos que $\mathbb{F}_p$ es el cuerpo finito de p elementos, y que este es único salvo isomorfismos. Dado $a\in\mathbb{Z}_p$, la aplicación

$$a=\sum_{n=0}^{\infty}a_np^n\longrightarrow a_0$$

define un epimorfismo de anillos $\mathbb{Z}_p\longrightarrow\mathbb{F}_p$ que denominaremos *reducción módulo p*.
Es claro que es una aplicación sobreyectiva y su núcleo es

$$\{a\in\mathbb{Z}_p \text{ tal que } a_0=0\}=\{\sum_{n=1}^{\infty}a_np^n \text{ con } a_n\in\{0,1,2,\ldots,p-1\}\}=\{p\sum_{n=0}^{\infty}a_{n+1}p^n\}=p\mathbb{Z}_p$$

Por el Primer teorema de isomorfía tenemos que $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$ que es un cuerpo. Por lo tanto puesto que $\mathbb{Z}_p$ es un dominio de integridad, podemos deducir que $p\mathbb{Z}_p$ es un ideal maximal.

Corolario 2.16. El anillo $\mathbb{Z}_p$ tiene un único ideal maximal, y este es $p\mathbb{Z}_p$.

Demostración
Si existiera otro ideal maximal I, como $p\mathbb{Z}_p$ también es maximal debe existir $a \in I$ tal que $a \notin p\mathbb{Z}_p$. En particular existirá $a^{-1} \in \mathbb{Z}_p$, luego como I es ideal $1 = aa^{-1} \in I$, lo que implica que $I = \mathbb{Z}_p$. $\square$

***Observación* 16.** No es difícil comprobar que $\mathbb{Z}_p = p\mathbb{Z}_p \cup \mathbb{Z}_p^*$ es una partición de $\mathbb{Z}_p$.

De los resultados anteriores se llega a una conclusión interesante que potencia las diferencias entre $\mathbb{Z}$ y $\mathbb{Z}_p$: así como en $\mathbb{Z}$ tenemos un ideal maximal $m\mathbb{Z}$ para cada número primo m, hemos visto que en $\mathbb{Z}_p$ existe sólo uno.

Definición 2.17. Un *dominio de ideales principales* es un dominio de integridad donde todos los ideales son principales, es decir; están generados por un único elemento.

Veremos ahora el último resultado de la sección.

Proposición 2.18. El anillo de $\mathbb{Z}_p$ es un dominio de ideales principales. De hecho sus ideales son (0) y $p^k\mathbb{Z}_p$ para todo $k \in \mathbb{N}$

Demostración
Consideremos $I \neq (0)$ un ideal en $\mathbb{Z}_p$, y sea $0 \neq a \in I$ un elemento de norma máxima en I, que podemos encontrar puesto que la norma p-ádica sólo toma valores discretos.
Supongamos que $|a|_p = p^{-k}$ para $k \in \mathbb{N}$. Entonces $c = ap^{-k}$ es una unidad p-ádica. Ahora, podemos escribir $p^k = ac^{-1} \in I$, luego $(p^k) = p\mathbb{Z}_p \subset I$.
Por otro lado, dado $b \in I$ se tiene que $|b|_p = p^{-m} \leq p^{-k}$ y escribimos
$b = p^m c' = p^k p^{m-k} c' \in p^k\mathbb{Z}_p$ donde $c' = bp^{-m}$. Se da entonces que $I \subset p^k\mathbb{Z}_p$ y concluimos que $I = p^k\mathbb{Z}_p$.$\square$

3. Teorema de Ostrowski

Ya hemos visto que sobre $\mathbb{Q}$ podemos definir una norma p-ádica para cada p primo $|\cdot|_p$ y la norma del valor absoluto $|\cdot|$, y que a partir de cada una de ellas obtenemos una completación del espacio distinta.
¿Son estas las únicas normas no triviales que podemos definir sobre $\mathbb{Q}$? El Teorema de Ostrowski demuestra que toda norma no trivial definida sobre $\mathbb{Q}$ será equivalente a cierta norma p-ádica $|\cdot|_p$ ó a la norma del valor absoluto $|\cdot|$.
Obviaremos, como hemos hecho hasta ahora, la norma trivial, pues es únicamente equivalente a sí misma.

3.1. Teorema de Ostrowski

Podemos entender el Teorema de Ostrowski como un resultado para clasificar las normas sobre $\mathbb{Q}$ en Arquimedianas y no Arquimedianas, dependiendo de si son equivalentes a $|\cdot|$ ó a $|\cdot|_p$ para cierto primo p.
Primero veremos una proposición esencial para la demostración que presentaremos del teorema.

Proposición 3.1. Sean $\|\cdot\|_1$ y $\|\cdot\|_2$ dos normas no triviales definidas sobre un cuerpo F. Entonces $\|\cdot\|_1 \sim \|\cdot\|_2$ si y sólo si existe un real positivo α tal que

$$\|x\|_2 = \|x\|_1^\alpha \ \forall x \in F$$

Demostración
$\Rightarrow$ Si $\|\cdot\|_1 \sim \|\cdot\|_2$, sea $a \in F$ con $\|a\|_1 \neq 1$. Reemplazando a por a^{-1} si fuera necesario podemos asumir que $\|a\|_1 < 1$. Definimos

$$\alpha := \frac{\log \|a\|_2}{\log \|a\|_1}$$

Puesto que las normas son equivalentes tenemos que $\|a\|_2 < 1$, luego ambos logaritmos son negativos y $\alpha > 0$. Veamos que es el α que buscamos:
Sea $x \in F$ tal que $\|x\|_1 < 1$ y consideramos el conjunto

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

Para todo $r \in S_1$ tenemos que $\|x\|_1^m < \|a\|_1^n$ luego $\|\frac{x^m}{a^n}\|_1 < 1$.
Como $\|\cdot\|_1 \sim \|\cdot\|_2$ también $\|\frac{x^m}{a^n}\|_2 < 1$. Podemos probar lo mismo intercambiando los papeles de $\|\cdot\|_1$ y $\|\cdot\|_2$ y considerando

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

se llega a la conclusión de que $S_1 = S_2$ (si $r \in S_1 \Rightarrow r \in S_2$ y si $r \in S_2 \Rightarrow r \in S_1$)
Tomando logaritmos podemos reescribir $\|x\|_1^r < \|a\|_1$ y $\|x\|_2^r < \|a\|_2$ como

$$r > \frac{\log \|a\|_1}{\log \|x\|_1}, \qquad r > \frac{\log \|a\|_2}{\log \|x\|_2}$$

pues todos los logaritmos son negativos.

En consecuencia se tiene que

$$\frac{\log \|a\|_1}{\log \|x\|_1} = \frac{\log \|a\|_2}{\log \|x\|_2} \tag{16}$$

pues de no ser así existiría un $r_0 \in S_1 \setminus S_2$ (o viceversa) y ya hemos visto que $S_1 = S_2$. Luego de (16) deducimos que

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

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

Para $\|x\|_1 > 1$ se deduce tomando x^{-1}, pues $\|x^{-1}\|_1 = \frac{1}{\|x\|_1} < 1 \Rightarrow \|x^{-1}\|_2 < 1$ (por ser ambas normas equivalentes) luego $\|x^{-1}\|_2 = \|x^{-1}\|_1^\alpha$ y concluimos que $\|x\|_2 = \|x\|_1^\alpha$.

Para $\|x\|_1 = 1$ es obvio, pues al ser equivalentes las normas $\|x\|_2 = 1$.

$\Leftarrow$ Supongamos que existe $\alpha > 0$ tal que $\forall x \in F \ \|x\|_2 = \|x\|_1^\alpha$, y sea (a_n) una sucesión de Cauchy para $\|\cdot\|_1$. Dado $\varepsilon > 0$ existe $N \in \mathbb{N}$ tal que $\forall n, m > N \ \|a_n - a_m\|_1 < \varepsilon^{\frac{1}{\alpha}}$, luego $\|a_n - a_m\| < \varepsilon$ para todo $n, m > N$ y concluimos que (a_n) es de Cauchy para $\|\cdot\|_2$. Intercambiando los papeles de $\|\cdot\|_1$ y $\|\cdot\|_2$ y tomando (a_n) con $\|a_n - a_m\|_2 < \varepsilon^\alpha$ se concluye la demostración.$\square$

Podemos ahora presentar el teorema que da nombre a esta sección.

Teorema 3.2 (**Teorema de Ostrowski**). *Toda norma no trivial $\|\cdot\|$ sobre $\mathbb{Q}$ es equivalente a $|\cdot|_p$ para algún primo p o a la norma absoluta $|\cdot|$. De hecho si $\|\cdot\|$ es Arquimediana será equivalente a esta última.*

Demostración

Supongamos primero que $\|\cdot\|$ es Arquimediana, en cuyo caso existe un entero positivo n tal que $\|n\| > 1$. Tomamos n_0 el menor de los n que cumple esta condición; podemos escribir entonces $\|n_0\| = {n_0}^\alpha$ para cierto $\alpha \in \mathbb{R}^+$ (la función $f(x) = {n_0}^x$ es continua y su imagen es $(0, \infty)$).

Escribimos cada entero positivo n en base n_0:

$$n = a_0 + a_1 n_0 + a_2 n_o^2 + \ldots + a_s n_0^s \text{ con } a_i \in \mathbb{Z}, \ \leq a_i < n_0 \text{ para } 0 \leq i \leq s \text{ y } a_s \neq 0$$

Tomando normas llegamos a que

$$\|n\| \leq \|a_0\| + \|a_1\|\|n_0\| + \ldots + \|a_s\|\|n_0\|^s$$

donde como $a_i < n_0$, por cómo hemos elegido n_0 tenemos que $\|a_i\| \leq 1$. Luego

$$\|n\| \leq 1 + n_0^\alpha + n_0^{2\alpha} + \ldots + n_0^{s\alpha} = n_0^\alpha(1 + n_0^{-\alpha} + \ldots + n_0^{-s\alpha}) \leq n_0^{s\alpha}(\sum_{i=0}^{\infty}(\frac{1}{n_0^\alpha})^i)$$

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

pues $n \geq n_0^s$.
Denominando $C = \sum_{i=0}^{\infty}(\frac{1}{n_0^\alpha})^i$ que es constante obtenemos que $\|n\| \leq Cn^\alpha$ para todo n entero positivo.
Sustituyendo en todo el razonamiento anterior n por n^N para $N \in \mathbb{N}$ llegamos a que

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

y haciendo $N \to \infty$ concluimos que

$$\|n\| \leq n^\alpha \tag{17}$$

Probamos ahora la desigualdad contraria: observemos que $n_0^{(s+1)\alpha} > n \geq n_0^s$ y puesto que

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

llegamos a que

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

pues por (17) tenemos que $\|n_0^{s+1} - n\| \leq (n_0^{s+1} - n)^\alpha$. Entonces

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

y como $n_0^s \leq n < n_0^{s+1}$ tenemos que $1 \leq n_0^{s+1} - n \leq n_0^{s+1} - n_0^s$ y por lo tanto

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

Igual que antes, sustituyendo en el razonamiento n por n^N para $N \in \mathbb{N}$ llegamos a

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

y haciendo $N \to \infty$ concluimos que

$$\|n\| \geq n^\alpha$$

Luego $\|n\| = n^\alpha \ \forall n \in \mathbb{N}$, y utilizando la multiplicatividad de la norma deducimos que $\|x\| = |x|^\alpha \ \forall x \in \mathbb{Q}$. Por la proposición anterior concluimos que $\|\cdot\| \sim |\cdot|$.

Supongamos ahora que $\|\cdot\|$ es no Arquimediana, es decir, que $\forall n \in \mathbb{N}\ \|n\| \leq 1$. Puesto que $\|\cdot\|$ es no trivial podemos encontrar n_0 el menor de los n tales que $\|n\| < 1$.
Por cómo lo hemos elegido n_0 debe ser un número primo; si $n_0 = n_1 n_2$ con $n_1, n_2 < n_0$ entonces $\|n_1\| = \|n_2\| = 1$ y $\|n_0\| = \|n_1\|\|n_2\| = 1$.
Denotamos $p := n_0$. Veamos primero que si $n \in \mathbb{N}$ no es divisible por p entonces $\|n\| = 1$: si $n = kp + s$ con $0 < s < p$ entonces $\|s\| = 1$ y $\|kp\| < 1$ (pues $\|p\| < 1$). Por tanto $\|n - s\| = \|kp\| < 1 = \|s\|$ y por la proposición 1.9 concluimos que $\|n\| = \|s\| = 1$.
Ahora, dado $n \in \mathbb{N}$ divisible por p podemos escribir $n = p^v n'$ con n' no divisible por p. Observemos que de esta manera $v = ord_p(n)$. Entonces $\|n\| = \|p\|^v \|n'\| = \|p\|^v$ pues $p \not| n'$.
Como $\|p\| < 1$ existe $\alpha \in \mathbb{R}^+$ tal que $\|p\| = (\frac{1}{p})^\alpha$, es decir:

$$\|n\| = (\frac{1}{p})^{v\alpha} = (p^{-v})^\alpha = |n|_p^\alpha$$

Utilizando la multiplicatividad de la norma deducimos la fórmula anterior para todo $x \in \mathbb{Q}$, y por la proposición anterior concluimos que $\|\cdot\| \sim |\cdot|_p$ y queda demostrado el teorema.□

***Observación* 17.** Sabemos que sobre $\mathbb{R}$ todas las normas son equivalentes; no es así en $\mathbb{Q}$. De hecho vimos en la observación (9) que para primos distintos sus respectivas normas no son equivalentes.

3.2. Consecuencias del Teorema de Ostrowski

Veamos primero un resultado que establece una relación entre las normas p-ádicas y la norma absoluta definidas sobre $\mathbb{Q}$, que por el Teorema de Ostrowski establece una relación entre todas las normas definidas sobre $\mathbb{Q}$.

Proposición 3.3 (Fórmula del producto). Para todo $x \in \mathbb{Q} \setminus \{0\}$ se cumple que

$$|x| \prod_{p \text{ primo}} |x|_p = 1$$

Demostración
Lo probamos para enteros positivos, y el caso para x racional se deduce de la multiplicatividad de la norma. Sea $n \in \mathbb{N}$ podemos escribirlo como $n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$ donde p_i son primos distintos. Si q es primo tal que $q \neq p_i$ para $i = 1, 2, \ldots, s$ entonces $|x|_q = 1$, luego en la fórmula del producto sólo hay un número finito de términos distintos de 1. Entonces

$$|n| \prod_{p \text{ primo}} |n|_p = |n| \prod_{i=1}^{s} |n|_{p_i} = |n| \prod_{i=1}^{s} p_i^{-a_i} = |p_1|^{a_1} \cdots |p_s|^{a_s} |p_1|^{-a_1} \cdots |p_s|^{-a_s} = 1$$

y el resultado queda probado. □

Corolario 3.4. Para cualquier primo p y cualquier $n \in \mathbb{N}$ se tiene que $|n|_p \geq \frac{1}{n}$.

Demostración
Dados p primo y $n \in \mathbb{N}$, como $|\cdot|_q$ es no Arquimediana para todo primo q sabemos que $|n|_q \leq 1$. Entonces

$$|n| \prod_{q \text{ primo}} |n|_q = 1 \Rightarrow n|n|_p \prod_{q \text{ primo } q \neq p} |n|_q = 1 \Rightarrow n|n|_p \geq 1 \Rightarrow |n|_p \geq \frac{1}{n} \square$$

Presentamos a continuación dos proposiciones que son consecuencia del Teorema de Ostrowski.

Proposición 3.5. Si $\|\cdot\|_1, \|\cdot\|_2$ son dos normas no equivalentes sobre $\mathbb{Q}$ entonces para cada par de números racionales s, t existe una sucesión (a_n) de racionales tal que $\lim_{n\to\infty} \|s - a_n\|_1 = 0$ y $\lim_{n\to\infty} \|t - a_n\|_2 = 0$.

Demostración
Primero vamos a ver lo siguiente: si $(\frac{p^n}{p^n+q^n})$ es una sucesión donde p y q son primos con $p < q$ entonces:

- $\lim_{n\to\infty} \frac{p^n}{p^n+q^n} = 0$ en $(\mathbb{Q}, |\cdot|)$.
- $|\frac{p^n}{p^n+q^n}|_p \leq p^{-n} \frac{1}{||p^n|_p - |q^n|_p|} = p^{-n} \frac{1}{1-p^{-n}} = \frac{1}{p^n-1}$ luego $\lim_{n\to\infty} \frac{p^n}{p^n+q^n} = 0$ en $(\mathbb{Q}, |\cdot|_p)$.
- $|\frac{p^n}{p^n+q^n} - 1|_q = |\frac{q^n}{q^n+p^n}|_q \leq q^{-n} \frac{1}{||q^n|_q - |p^n|_q|} = \frac{1}{q^n-1}$ luego $\lim_{n\to\infty} \frac{p^n}{q^n+p^n} = 1$ en $(\mathbb{Q}, |\cdot|_q)$.

Sin pérdida de generalidad podemos suponer, por el Teorema de Ostrowski, que $\|\cdot\|_1 \sim |\cdot|$ ó $\|\cdot\|_1 \sim |\cdot|_p$ para algún primo p y que $\|\cdot\|_2 \sim |\cdot|_q$ para algún primo q.
Es decir, existen $\alpha_1, \alpha_2 \in \mathbb{R}^+$ tales que $\|\cdot\|_1 = |\cdot|_p^{\alpha_1}$ y $\|\cdot\|_2 = |\cdot|_q^{\alpha_2}$. Por lo tanto es suficiente con encontrar una sucesión (a_n) tal que $\lim_{n\to\infty} |s - a_n|_p = 0$ y $\lim_{n\to\infty} |t - a_n|_q = 0$. Consideramos 3 casos:

- **Caso 1**: p y q son primos con $p < q$. Entonces definimos $a_n = t\frac{p^n}{p^n+q^n} + s\frac{q^n}{p^n+q^n}$, y tenemos $s - a_n = s(1 - \frac{q^n}{p^n+q^n}) - t\frac{p^n}{p^n+q^n} = (s-t)\frac{p^n}{p^n+q^n} \xrightarrow{n\to\infty} 0$ en $(\mathbb{Q}, |\cdot|_p)$ y
  $t - a_n = t(1 - \frac{p^n}{p^n+q^n}) - s\frac{q^n}{p^n+q^n} = (t-s)\frac{q^n}{p^n+q^n} \xrightarrow{n\to\infty} 0$ en $(\mathbb{Q}, |\cdot|_q)$.
- **Caso 2**: $p = \infty$ y $q > 2$. Definimos $a_n = t\frac{2^n}{2^n+q^n} + s\frac{q^n}{2^n+q^n}$ y tenemos
  $s - a_n = (s-t)\frac{2^n}{2^n+q^n} \xrightarrow{n\to\infty} 0$ en $(\mathbb{Q}, |\cdot|)$ y
  $t - a_n = (t-s)\frac{q^n}{2^n+q^n} \xrightarrow{n\to\infty} 0$ en $(\mathbb{Q}, |\cdot|_q)$.

- **Caso 3** $p = \infty$ y $q = 2$. Definimos $a_n = t\frac{1}{1+2^n} + s\frac{2^n}{1+2^n}$ y tenemos $s - a_n = (s-t)\frac{1}{1+2^n} \xrightarrow{n\to\infty} 0$ en $(\mathbb{Q}, |\cdot|)$ y
  $t - a_n = (t-s)\frac{2^n}{1+2^n} \xrightarrow{n\to\infty} 0$ en $(\mathbb{Q}, |\cdot|_2)$

En todos los casos la sucesión construida cumple lo requerido.□

Proposición 3.6. Para cada primo p existe una sucesión (a_n) de $\mathbb{Q}$ tal que $\lim_{n\to\infty} |a_n|_p = 1$ y $\lim_{n\to\infty} a_n = 0$ en $(\mathbb{Q}, |\cdot|)$ y $(\mathbb{Q}, |\cdot|_q)$ para q primo distinto de p.

Demostración

Sea L_k el producto de los k primeros primos. Entonces si tomamos un primo p que será el primo i-ésimo, para $k > i$ consideramos

$$|L_k^k L_{k^2}^{-1}|_p = \frac{|L_k^k|_p}{|L_{k^2}|_p} = \frac{p^{-k}}{p^{-1}} \xrightarrow{k\to\infty} 0$$

Además

$$L_k^k L_{k^2}^{-1} = \frac{L_k^k}{L_{k^2}} = \frac{(p_1 p_2 \cdots p_k)^k}{p_1 \cdots p_k p_{k+1} \cdots p_{k^2}} = \frac{(p_1 \cdots p_k)^{k-1}}{p_{k+1} \cdots p_{k^2}}$$

Ahora, $p_{jk+1} \cdots p_{(j+1)k} > 2p_1 \cdots p_k$ para $j = 1, 2, \cdots k$ y $k > 1$, luego tenemos que

$$L_k^k L_{k^2}^{-1} = \frac{(p_1 \cdots p_k)^{k-1}}{p_{k+1} \cdots p_{k^2}} < \frac{(p_1 \cdots p_k)^{k-1}}{(2p_1 \cdots p_k)^{k-1}} = \frac{1}{2^{k-1}} \xrightarrow{k\to\infty} 0$$

Por lo tanto $\lim_{k\to\infty} L_k^k L_{k^2}^{-1} = 0$ en $(\mathbb{Q}, |\cdot|)$, y si consideramos $a_k = p^{k-1} L_k^k L_{k^2}^{-1}$ como $|p^{k-1}|_p = p^{1-k}$ se tienen las dos primeras peticiones que hemos hecho a (a_n).

Ver la última sin embargo no tiene complicación, pues para todo primo $q \neq p$ existirá un k lo suficientemente grande a partir del cual q dividirá a L_k y tendremos que

$$\lim_{k\to\infty} |a_k|_q = \lim_{k\to\infty} \frac{q^{-k}}{q^{-1}} = 0$$

y la demostración queda terminada.□

Para terminar la sección nos planteamos lo siguiente: es claro que si un polinomio tiene raíces en $\mathbb{Q}$ estas están también en $\mathbb{R}$ y $\mathbb{Q}_p$ para cualquier primo p, de lo cual deducimos que si existe un primo p para el cual el polinomio no tiene raíces en $\mathbb{Q}_p$ entonces este polinomio tampoco tendrá raíces en $\mathbb{Q}$.

Motivada por lo anterior nos surge la siguiente duda: si un polinomio tiene alguna raíz en $\mathbb{R}$ y en $\mathbb{Q}_p$ para todo primo p ¿es esta una raíz del polinomio en $\mathbb{Q}$?

A esta condición se la conoce como ***Principio de Hasse*** y existe una colección de polinomios que sí que la cumplen, aunque no son todos. No profundizaremos demasiado en este tema, pero de manera ilustrativa veremos a continuación un ejemplo de polinomio que cumple dicho principio.

Proposición 3.7. Un número $x \in \mathbb{Q} \setminus \{0\}$ tiene raíz cuadrada en $\mathbb{Q}$ si y sólo si la tiene en $\mathbb{Q}_p$ para $p \leq \infty$ primo.

Demostración

$\Rightarrow$ Obvio, pues $\mathbb{Q} \subset \mathbb{Q}_p$ para todo p primo y $p = \infty$.

$\Leftarrow$ Supongamos que $x = \frac{a}{b}$ para $a, b \in \mathbb{Z}$ con $mcd(a, b) = 1$. Como x es cuadrado de algún número en $\mathbb{Q}_p$ para todo p primo y $p = \infty$ en particular será positivo. Además, si $m = ord_p(x)$ sabemos que podemos escribir

$$x = p^m v_p = y_p^2 = (p^s u_p)^2 \text{ donde } v_p, u_p \in \mathbb{Z}_p^*$$

para y_p la raíz cuadrada p-ádica de x, $s = ord_p(y_p)$, luego necesariamente $ord_p(x)$ es par (recordemos que p no divide a las unidades p-ádicas).

Ahora, por definición de x y de orden p-ádico tenemos que $ord_p(x) = ord_p(a) - ord_p(b)$, y como a y b no tienen divisores en común tenemos que para todo p primo $ord_p(a)$ es par y $ord_p(b) = 0$ o viceversa. Si un número es entero positivo podemos escribir su factorización en números primos

$$a = \prod_{p<\infty \text{ primo}} p^{ord_p(a)}$$

e igual para b. Nos queda entonces que x es de la forma

$$x = \frac{p_1^{2k_1} p_2^{2k_2} \cdots p_n^{2k_n}}{q_1^{2j_1} q_2^{2j_2} \cdots q_s^{2j_s}} = (\frac{p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}}{q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s}})^2$$

y queda terminada la demostración.□

4. Topología en $\mathbb{Q}_p$

Sobre $\mathbb{Q}_p$ hemos definido una norma $|\cdot|_p$, y en consecuencia tenemos una métrica a partir de la cual podemos definir una topología. En esta sección veremos propiedades únicas de $\mathbb{Q}_p$ como espacio topológico y daremos por conocidas definiciones y propiedades básicas de la topología real.

4.1. Conceptos y propiedades elementales

$\mathbb{Q}_p$ es similar a $\mathbb{R}$ en muchos aspectos; ambos son espacios normados que contienen a $\mathbb{Q}$ como subconjunto denso, luego ambos son separables, y son por supuesto completos. Sin embargo existen diferencias interesantes que encontraremos al examinar $\mathbb{Q}_p$ como espacio topológico.

Definición 4.1. Definimos en $\mathbb{Q}_p$ la *bola abierta de centro* $a \in \mathbb{Q}_p$ *y radio* $r>0$ como

$$B(a,r) = \{x \in \mathbb{Q}_p \text{ tales que } |a-x|_p < r\}$$

Notemos que como $|\cdot|_p$ sólo toma valores discretos de la forma $\{p^n; n \in \mathbb{Z}\} \cup \{0\}$ basta con que consideremos $r = p^n, n \in \mathbb{Z}$.

Presentamos ahora la definición general de topología en términos de $\mathbb{Q}_p$.

Definición 4.2. Una topología sobre $\mathbb{Q}_p$ es un subconjunto τ de $\mathcal{P}(\mathbb{Q}_p)$ (partes de $\mathbb{Q}_p$) que cumple:

1. $\emptyset, \mathbb{Q}_p \in \tau$
2. Sea $\{A_i; i \in I\} \subset \tau$ un subconjunto arbitrario de τ, entonces $\cup_{i\in I} A_i \in \tau$
3. Sean $A_1, A_2, \ldots, A_n \in \tau$, entonces $\cap_{i=1}^n A_i \in \tau$.

Si τ es una topología sobre $\mathbb{Q}_p$, a los conjuntos de $\mathbb{Q}_p$ que están en τ se les llama *abiertos* de $\mathbb{Q}_p$ para τ. Dado $A \subset \mathbb{Q}_p$, diremos que es un conjunto *cerrado* si $A^c \in \tau$.

Consideraremos en $\mathbb{Q}_p$ la topología usual τ_u, derivada de la métrica dada por la norma $|\cdot|_p$.

Definición 4.3. Dado $U \subset \mathbb{Q}_p$, definimos en $\mathbb{Q}_p$ la topología usual

$$U \in \tau_u \Leftrightarrow \ \forall x \in U \text{ existe } n \in \mathbb{Z} \text{ tal que } B(x,p^n) \subset U$$

***Observación* 18.** Puesto que hemos definido la topología usual en $\mathbb{Q}_p$ de la misma manera en la que se define la topología usual en $\mathbb{R}$, mediante bolas abiertas, la demostración de que τ_u es una topología es idéntica a la que se realiza en $\mathbb{R}$.

Sean $a \in \mathbb{Q}_p$, $r = p^n, n \in \mathbb{Z}$, consideramos la esfera en $\mathbb{Q}_p$ de centro a y radio r:

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

Se nos presenta entonces la primera diferencia con la topología real usual que conocemos:

Proposición 4.4. La esfera $S(a,r)$ en $\mathbb{Q}_p$ es un conjunto abierto para lo topología usual.

Demostración
Sea $x \in S(a,r)$, tomamos $0 < \varepsilon < r$, veremos que $B(x,\varepsilon) \subset S(a,r)$. Sea $y \in B(x,\varepsilon)$, luego $|x-y|_p < \varepsilon < r = |x-a|_p$. Como $|\cdot|_p$ es una norma no Arquimediana, por la proposición (1.9) como $|x-y|_p = |(y-a)-(x-a)|_p < |x-a|_p$ se concluye que $|y-a|_p = |x-a|_p = r$ y por lo tanto $y \in S(a,r)$.□

Esto contrasta con las esferas en $\mathbb{R}^n$, que son claramente conjuntos cerrados. Esta propiedad trae consigo resultados sorprendentes, como el que sigue.

Proposición 4.5. Las bolas abiertas en $\mathbb{Q}_p$ son conjuntos abiertos y cerrados (en τ_u).

Demostración
Consideramos $B(a,r)$; que es abierta se deduce de la definición que hemos dado de conjuntos abiertos en τ_u.
Para ver que es cerrada veremos que su complementario

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

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

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

Como ya sabemos que $S(a,r)$ es abierto, basta ver que D también lo es. Sea $y \in D$, entonces $|y-a|_p = r_1 > r$. Entonces la bola abierta $B(y, r_1 - r)$ está contenida en D, pues de no ser así existiría $x \in B(y, r_1 - r)$ tal que $|x-a|_p \leq r$, y por la desigualdad triangular tendríamos que $r_1 = |y-a|_p = |(a-x)+(x-y)|_p \leq |a-x|_p + |x-y|_p < r + (r_1 - r) = r_1$, que es un absurdo.□

Recordamos la siguiente definición:

Definición 4.6. Un punto x de un conjunto $A \subset \mathbb{Q}_p$ se dice *punto frontera* si para toda bola abierta centrada en x $B(x,r)$ se tiene que $B(x,r) \not\subset A$ y $B(x,r) \cap A \neq \emptyset$. El conjunto de todos los puntos frontera de A se denomia *frontera* y se denota por $Fr(A)$.

Proposición 4.7. Si un conjunto A es cerrado entonces $Fr(A) \subset A$.

Demostración
Sea $x \in Fr(A)$, luego dado $r > 0$ $B(x,r) \not\subset A$ y $B(x,r) \cap A \neq \emptyset$, lo que en particular implica que $B(x,r) \not\subset A^c$. A es cerrado, luego A^c es abierto y por lo tanto $x \notin A^c$. Concluimos que $x \in A$. □

De la proposición anterior podemos deducir que $S(a,r)$ no es la frontera de $B(a,r)$, pues $B(a,r)$ es cerrado y $S(a,r) \not\subset B(a,r)$. De hecho podemos deducir algo más fuerte: $B(a,r)$ no tiene ninguna frontera. Si la tuviera esta debería estar contenida en $B(a,r)$ por ser cerrada, pero como también es abierta para todos sus puntos existe una bola abierta centrada en ellos contenida en $B(a,r)$, luego ninguno de sus puntos está en la frontera.
Es decir; si $x \notin B(a,r)$ existe $\varepsilon > 0$ tal que $B(x,\varepsilon) \cap B(a,r) = \emptyset$.
Dicho de otra manera: un punto $x \in \mathbb{Q}_p$ está en $B(a,r)$ o está "separado"de ella.

***Observación* 19.** Nos damos cuenta del siguiente fenómeno: si consideramos la bola cerrada de centro $a \in \mathbb{Q}_p$ y radio $r = p^n, n \in \mathbb{Z}$ denotada por $\bar{B}(a,r)$ tenemos que

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

Por lo tanto la bola cerrada $\bar{B}(a,r)$ es también un conjunto abierto y cerrado que carece de frontera.
A partir de ahora diremos simplemente *bola centrada en a y de radio r* para referirnos a $B(a,r)$.

Presentamos ahora una colección de proposiciones que entran en contraste con las propiedades de las bolas en $\mathbb{R}^n$.

Proposición 4.8. Si $b \in B(a,r)$ entonces $B(a,r) = B(b,r)$. En otras palabras; todos los puntos de la bola son su centro.

Demostración
Como $|\cdot|_p$ es no Arquimediana el resultado se deduce de la proposición (1.10).□

Proposición 4.9. Dos bolas en $\mathbb{Q}_p$ tienen intersección no vacía si y sólo si una esta contenida dentro de la otra.

Demostración
Sean $B(a,r), B(b,s)$ dos bolas en $\mathbb{Q}_p$. Si una está contenida en la otra obviamente la intersección no es vacía. Ahora, si la intersección no es vacía: supongamos que $r \leq s$

y que $y \in B(a,r) \cap B(b,s)$. Entonces por la proposición anterior $B(a,r) = B(y,r)$ y $B(b,s) = B(y,s)$, y como $B(y,r) \subset B(y,s)$ se concluye que $B(a,r) \subset B(b,s)$. $\square$

Proposición 4.10. La esfera $S(a,r)$ es abierta y cerrada.

Demostración
Ya hemos visto que es abierta, luego sólo queda probar que es cerrada. Sabemos que $\bar{B}(a,r)$ es cerrada, y como $B(a,r)$ es abierta su complementario $\{x \in \mathbb{Q}_p; |x-a|_p \geq r\}$ es cerrado. Podemos escribir $S(a,r) = \bar{B}(a,r) \cap \{x \in \mathbb{Q}_p; |x-a|_p\}$, es decir, como intersección finita de cerrados, luego cerrado.$\square$

Sabemos que $\mathbb{R}$ es un conjunto no numerable; de hecho el intervalo $(0,1)$ contiene un infinito no numerable de elementos. Por lo tanto el conjunto de bolas abiertas en $\mathbb{R}$ resulta ser también un conjunto infinito no numerable. No es así en $\mathbb{Q}_p$.

Proposición 4.11. El conjunto de bolas en $\mathbb{Q}_p$ es numerable.

Demostración
Consideramos una bola abierta en $\mathbb{Q}_p$, $B(a,p^{-s})$ con $a \in \mathbb{Q}_p$ y $s \in \mathbb{Z}$. Escribimos a en su forma canónica

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

Tomamos $a_0 = \sum_{n=-m}^{|s|} a_n p^n$ que sabemos por el Teorema (2.8) que es un número racional, y además $|a_0 - a|_p < p^{-s}$.
Entonces como $a_0 \in B(a,p^{-s})$ por la Proposición (4.8) tenemos que $B(a,p^{-s}) = B(a_0,p^{-s})$. Hemos visto que toda bola en $\mathbb{Q}_p$ puede expresarse como una bola de centro racional y radio de la forma p^{-s} con $s \in \mathbb{Z}$, y puesto que tanto los racionales como los enteros son conjuntos finitos numerables el conjunto de bolas en $\mathbb{Q}_p$ también lo es.$\square$

***Observación* 20.** Podemos escribir entonces $\mathbb{Z}_p = \bar{B}(0,1) = \bar{B}(0,p^0) = B(0,p)$ y $\mathbb{Z}_p^* = S(0,1)$.

4.2. Compacidad y conexidad

Comenzaremos esta sección introduciendo algunas definiciones básicas

Definición 4.12. Un subconjunto A de un espacio métrico se dice que es *secuencialmente compacto* si para toda sucesión infinita de elementos de A existe una subsucesión convergente a un punto de A.

Un subconjunto A de un espacio métrico se dice que es *compacto* si todo recubrimiento por abiertos de A contiene un subrecubrimiento finito.
Un subconjunto A de un espacio métrico se dice que es *localmente compacto* si $\forall a \in A$ cada entorno de a contiene un conjunto compacto entorno de a.
De igual manera se definen la compacidad, la compacidad local y secuencial para espacios métricos.

No lo demostraremos, pero el Teorema de Heine-Borel-Lebesgue asegura que que un espacio métrico sea compacto y sea secuencialmente compacto son equivalentes.
Ya hemos visto por el Teorema (1.31) que $\mathbb{Z}_p$ es secuencialmente compacto, y por el Teorema (1.32) también lo es cualquier bola en $\mathbb{Q}_p$. En consecuencia obtenemos el siguiente teorema, cuya demostración se deduce directamente de lo anterior:

Teorema 4.13. *$\mathbb{Z}_p$ es un conjunto compacto y el espacio $\mathbb{Q}_p$ es localmente compacto.*

***Observación* 21.** $\mathbb{Q}_p$ no es secuencialmente compacto, por lo tanto no es compacto. Tomamos por ejemplo la sucesión

Resulta de interés la siguiente proposición:

Proposición 4.14. $\mathbb{Z}_p$ es completo.

Demostración
Dada (a_n) una sucesión de Cauchy en $\mathbb{Z}_p$, por ser sucesión en $\mathbb{Z}_p$ sabemos que contiene una subsucesión convergente hacia un elemento $a \in \mathbb{Z}_p$.
Por otro lado (a_n) es una sucesión en $\mathbb{Q}_p$, que es completo, luego converge en $\mathbb{Q}_p$, y como $a \in \mathbb{Z}_p$ en particular converge en $\mathbb{Z}_p$, luego $\mathbb{Z}_p$ es completo.□

***Observación* 22.** No es difícil comprobar que $\mathbb{N}$ es un conjunto denso en $\mathbb{Z}_p$: dado $x \in \mathbb{Z}_p$ basta considerar la sucesión dada por las sumas parciales de la forma canónica de x. Luego $\mathbb{Z}_p$ tiene un subconjunto denso y numerable, y es por lo tanto separable.

Hemos visto que $\mathbb{Z}_p$ tiene más características similares a $\mathbb{R}$ de lo que podía parecer en un principio: ambos espacios son completos y separables.
Presentamos ahora la definición de espacio conexo a partir de la de espacio disconexo.

Definición 4.15. Un espacio topológico X es *disconexo* si existen subconjuntos abiertos no vacíos A y B tales que $A \cup B = X$ y $A \cap B = \emptyset$. Un espacio métrico será *conexo* si no es disconexo.
Un subconjunto de X es conexo si lo es para la topología inducida.
Un espacio topológico X es *totalmente disconexo* si los únicos subconjuntos conexos de X son el vacío y los puntos $\{a\}, a \in X$.

***Ejemplo* 4.16.** Obviamente el conjunto de los números reales $\mathbb{R}$ es conexo, como también lo es cualquier intervalo de la recta real. Por otro lado si en $\mathbb{R}$ consideramos la topología usual, cualquier conjunto numerable es totalmente disconexo.

En contraste con el ejemplo anterior presentamos el siguiente teorema:

Teorema 4.17. *$\mathbb{Q}_p$ es un espacio totalmente disconexo*

Demostración
Sea $A \subset \mathbb{Q}_p$ un subconjunto tal que $A \neq \emptyset$ y $A \neq \{a\}$ para $a \in \mathbb{Q}_p$. Consideramos la bola de centro a y radio p^{-n} para $n \in \mathbb{N}$: $B(a, p^{-n}) = \{x \in \mathbb{Q}_p; |a - x|_p < p^{-n}\}$. Como $A \neq \{a\}$ existirá $n \in \mathbb{N}$ tal que $B(a, p^{-n}) \cap A \neq A$, luego

$$A = (B(a, p^{-n}) \cap A) \cup (B^c(a, p^{-n}) \cap A)$$

donde $B(a, p^{-n})$ y su complementario son ambos abiertos no vacíos y disjuntos, luego A es disconexo.□

La esencia de la demostración anterior está en que en $\mathbb{Q}_p$ las bolas son abiertas y cerradas.

5. Análisis en $\mathbb{Q}_p$

Esta sección servirá de introducción al siguiente capítulo, para el cual resultan necesarias unas bases del análisis en los números p-ádicos.

5.1. Sucesiones y series

En este apartado estudiaremos las sucesiones y series en $\mathbb{Q}_p$. Encontraremos diferencias notables con las sucesiones y las series en los números reales, a las que haremos referencia de vez en cuando.
Comenzaremos caracterizando las sucesiones de Cauchy en $\mathbb{Q}_p$

Teorema 5.1. *Una sucesión (a_n) en $\mathbb{Q}_p$ es de Cauchy, y por tanto convergente, si y sólo si*

$$\lim_{n\to\infty} |a_{n+1} - a_n|_p = 0 \tag{18}$$

Demostración
Si (a_n) es de Cauchy entonces $\lim_{m,n\to\infty} |a_m - a_n|_p = 0$. En particular si consideramos m=n+1 obtenemos $\lim_{n\to\infty} |a_{n+1} - a_n|_p = 0$. Esto se cumple para series de Cauchy en cualquier espacio métrico.
Ahora, supongamos que $\lim_{n\to\infty} |a_{n+1} - a_n|_p = 0$, luego para cada $\varepsilon > 0$ existe N>0 tal que $\forall n > N$ se tiene que $|a_{n+1} - a_n|_p < \varepsilon$.
Consideramos $m > n > N$ y calculamos $|a_m - a_m|_p$:

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

donde hemos utilizado que $|\cdot|_p$ es una norma no Arquimediana (desigualdad del triángulo fuerte). □

***Observación* 23.** La segunda implicación no es cierta en general. De hecho no lo es en aquellos espacios métricos con métrica Arquimediana. $(\mathbb{R}, \|\cdot\|)$ es uno de ellos: un ejemplo de sucesión que no cumple esta implicación es $(log(n))$. Esta sucesión sí cumple que $\lim_{n\to\infty} \|log(n+1) - log(n)\| = \lim_{n\to\infty} \|log(\frac{n+1}{n})\| = |log(1)|_p = 0$, sin embargo $\lim_{n\to\infty} log(n) = \infty$, luego no converge y por lo tanto no es de Cauchy.

Definición 5.2. Sea $\sum_{n=0}^{\infty} a_n$ una serie en $\mathbb{Q}_p$. Diremos que la serie *converge* si lo hace su sucesión de sumas parciales $S_n = \sum_{k=0}^{n} a_k$ en $\mathbb{Q}_p$.
Diremos que *converge absolutamente* si la serie $\sum_{n=0}^{\infty} |a_n|_p$ converge en $\mathbb{R}$.

La convergencia absoluta es un concepto más fuerte que la convergencia simple:

Proposición 5.3. Si la serie $\sum_{n=0}^{\infty} a_n$ converge absolutamente entonces converge en $\mathbb{Q}_p$.

Demostración
Que $\sum_{n=0}^{\infty} a_n$ converja absolutamente quiere decir que la sucesión $\sum_{n=0}^{\infty}|a_n|_p$ converge en $\mathbb{R}$. En particular que su sucesión de sumas parciales es de Cauchy, luego dado $\varepsilon > 0$ existe N natural tal que $\forall n, m > N$ con $m > n > N$ se cumple que

$$\|\sum_{i=0}^{m}|a_i|_p - \sum_{i=0}^{n}|a_i|_p\| = \sum_{i=n+1}^{m}|a_i|_p < \varepsilon$$

Entonces por la desigualdad triangular tenemos que

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

lo cual implica que (S_n) es de Cauchy, luego converge. Por lo tanto la serie $\sum_{n=0}^{\infty} a_n$ converge en $\mathbb{Q}_p$. □

A continuación presentamos la propiedad más fuerte que tienen las series en $\mathbb{Q}_p$, de la que carecen las series de números reales.

Proposición 5.4. Una serie $\sum_{n=0}^{\infty} a_n$ de números p-ádica converge en $\mathbb{Q}_p$ si y sólo si $\lim_{n\to\infty}|a_n|_p = 0$, en cuyo caso

$$|\sum_{n=0}^{\infty} a_n|_p \leq \max_n |a_n|_p$$

Demostración
La serie $\sum_{n=0}^{\infty} a_n$ converge si y sólo si lo hace la sucesión de sumas parciales (S_n). Pero $a_n = S_n - S_{n-1}$, y por el teorema (5.1) la sucesión (S_n) converge si y sólo si $\lim_{n\to\infty}|S_n - S_{n-1}|_p = \lim_{n\to\infty}|a_n|_p = 0$. Concluimos que $\sum_{n=0}^{\infty} a_n$ converge si y sólo si $\lim_{n\to\infty}|a_n|_p = 0$.
Ahora supongamos que $\sum_{n=0}^{\infty} a_n$ converge:
Si $\sum_{n=0}^{\infty} a_n = 0$ es obvio que $|\sum_{n=0}^{\infty} a_n|_p \leq \max_n |a_n|_p$.
En caso de no ser así, por la desigualdad del triángulo fuerte tenemos que para cada suma parcial S_N

$$|\sum_{n=0}^{N} a_n|_p \leq \max_{1\leq n\leq N}|a_n|_p$$

y puesto que $|a_n|_p \longrightarrow 0$ sabemos que para N lo suficientemente grande se cumple que

$$\max_{1\leq n\leq N}|a_n|_p = \max_n |a_n|_p$$

Conviene recordar que en la norma p-ádica, puesto que esta toma sólo valores discretos, las sucesiones de normas se estabilizan a partir de un punto. Es decir, si $c_n \longrightarrow c$ entonces $|c_n|_p \longrightarrow |c|_p$, luego existe N_0 lo suficientemente grande tal que $|c_n|_p = |c|_p$ para todo $n > N_0$.
Por lo tanto aplicando esto y teniendo en cuenta que $S_n \longrightarrow \sum_{i=0}^{\infty} a_i$ tenemos que para un N lo suficientemente grande

$$|\sum_{n=0}^{\infty} a_n|_p = |\sum_{n=0}^{N} a_n|_p \leq \max_{1\leq n\leq N} |a_n|_p = \max_n |a_n|_p$$

y queda terminada la demostración. □

***Observación* 24.** Sabemos que esta proposición no se cumple en $\mathbb{R}$. El ejemplo más conocido es el de la serie armónica $\sum_{n=01}^{\infty} \frac{1}{n}$, pero podemos encontrar muchos más, como la serie de *Bertrand* $\sum_{n=1}^{\infty} \frac{1}{n\sqrt{log(n)}}$.

Los términos de una serie se pueden reordenar, y en ocasiones esto puede llevar al cambio de carácter de la serie, pasando de ser convergente a no serlo o viceversa. Surge por lo tanto la siguiente definición:

Definición 5.5. Una serie $\sum_{n=0}^{\infty} a_n$ se dice que converge *incondicionalmente* si para cualquier reordenación de sus términos la serie sigue siendo convergente.

Teorema 5.6. *Si la serie de números p-ádicos $\sum_{n=0}^{\infty} a_n$ converge en $\mathbb{Q}_p$, entonces converge incondicionalmente y su suma no depende de la reordenación de sus términos.*

Demostración
Consideramos $\sum_{n=0}^{\infty} a'_n$ una reordenación de la serie. Como $\sum_{n=0}^{\infty} a_n$ converge sabemos que $a_n \longrightarrow \infty$, luego dado $\varepsilon > 0$ tomamos $N \in \mathbb{N}$ tal que para todo $n > N$ $|a_n|_p < \varepsilon, |a'_n|_p < \varepsilon$ y

$$|\sum_{n=0}^{\infty} a_n - \sum_{n=0}^{N} a_n|_p < \varepsilon$$

Sean $S = \sum_{n=0}^{N} a_n$ y $S' = \sum_{n=0}^{N} a'_n$, denotaremos por S_1 y S'_1 a las sumas $S_1 = \sum_{|a_n|_p>\varepsilon} a_n$ y $S'_1 = \sum_{|a'_n|_p>\varepsilon}$. Notemos que los términos de S_1 y S'_1 están en S y S' respectivamente. Además las sucesiones S_1 y S'_1 tienen los mismos términos, luego $S_1 = S'_1$, y por otro lado

$$|S - S_1|_p = |\sum_{|a_n|_p<\varepsilon, n<N} a_n|_p \leq \max\{|a_n|_p < \varepsilon, n < N\} < \varepsilon$$

$$|S' - S'_1|_p = |\sum_{|a'_n|_p<\varepsilon, n<N} a'_n|_p \leq \max\{|a'_n|_p < \varepsilon, n < N\} < \varepsilon$$

Luego $|S - S'|_p = |S - S_1 + S_1' - S'|_p \leq \text{máx}\{|S - S_1|_p, |S_1' - S'|_p\} < \varepsilon$, donde hemos usado que $S_1 = S_1'$.
Como $|\sum_{n=0}^{\infty} a_n - S|_p < \varepsilon$ tenemos que

$$|\sum_{n=0}^{\infty} a_n - S'|_p = |\sum_{n=0}^{\infty} a_n - S + S - S'|_p < \varepsilon$$

utilizando la desigualdad del triángulo fuerte.
Como hemos visto que se cumple para un $\varepsilon > 0$ cualquiera hacemos $\varepsilon \longrightarrow 0$, luego $N \longrightarrow \infty$, y por lo tanto $\sum_{n=0}^{\infty} a_n'$ converge y $\sum_{n=0}^{\infty} a_n' = \sum_{n=0}^{\infty} a_n$ como queríamos probar.□

Por supuesto para $\mathbb{R}$ este resultado no es cierto; el ***Teorema de reordenación de Riemann***[1] asegura que si una serie en $\mathbb{R}$ converge pero no absolutamente sus términos se pueden reordenar de forma que su suma sea un término prefijado cualquiera, o incluso que no converja. Es decir, en $\mathbb{R}$ el teorema anterior es cierto solamente si la serie converge absolutamente.
Ahora, si en $\mathbb{Q}_p$ todas las series que convergen lo hicieran absolutamente el teorema anterior no sería tan fuerte. Presentamos por ello el siguiente resultado:

Proposición 5.7. Existe al menos una serie en $\mathbb{Q}_p$ que converge pero no converge absolutamente.

Demostración
Consideramos la serie dada por 1,p repetido p veces, p^2 repetido p^2 veces,... donde $|p^n|_p = p^{-n} \xrightarrow{n\to\infty} 0$ luego por la proposición (5.4) la serie converge. Sin embargo

$$\sum_{n=0}^{\infty} |a_n|_p = 1 + pp^{-1} + p^2p^{-2} + \cdots = \infty$$

y la serie no converge absolutamente. □
Presentamos un último resultado relativo a las series de números p-ádicos, relacionado con el orden de sus términos.

Proposición 5.8. Dados números p-ádicos $b_{i,j}$, $i, j = 1, 2, \ldots$ tales que para cada $\varepsilon > 0$ existe un $N = N(\varepsilon)$ natural para el cual $\text{máx}(i, j) \leq N \Rightarrow |b_{i,j}|_p < \varepsilon$.
Entonces

$$\sum_{i,j=1}^{\infty} b_{i,j} = \sum_{i=1}^{\infty}(\sum_{j=1}^{\infty} b_{i,j}) = \sum_{j=1}^{\infty}(\sum_{i=1}^{\infty} b_{i,j}) < \infty$$

Demostración
Por la proposición (5.4) tanto $\sum_{i=1}^{\infty} b_{i,j}$ para j fijo como $\sum_{j=1}^{\infty} b_{i,j}$ para i fijo convergen.

Además para $i \geq N$ tenemos

$$|\sum_{j=1}^{\infty} b_{i,j}|_p \leq \max_j |b_{i,j}|_p < \varepsilon$$

y para $j \geq N$

$$|\sum_{i=1}^{\infty} b_{i,j}|_p \leq \max_i |b_{i,j}|_p < \varepsilon$$

luego $\sum_{i=1}^{\infty}(\sum_{j=1}^{\infty} b_{i,j})$ y $\sum_{j=1}^{\infty}(\sum_{i=1}^{\infty} b_{i,j})$ convergen.
Ahora

$$|\sum_{i=1}^{\infty}(\sum_{j=1}^{\infty} b_{i,j}) - \sum_{i=1}^{N}(\sum_{j=1}^{N} b_{i,j})|_p = |\sum_{i=1}^{N}(\sum_{j=N+1}^{\infty} b_{i,j}) + \sum_{i=N+1}^{\infty}(\sum_{j=1}^{\infty} b_{i,j})|_p \leq$$

$$\leq \max\{|\sum_{i=1}^{N}(\sum_{j=N+1}^{\infty} b_{i,j})|_p, |\sum_{i=N+1}^{\infty}(\sum_{j=1}^{\infty} b_{i,j})|_p\} \leq \max\{|\sum_{j=N+1, i\leq N}^{\infty} b_{i,j}|_p, |\sum_{j=1, i\geq N+1}^{\infty} b_{i,j}|_p\} < \varepsilon$$

De igual manera se prueba que

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

. Las desigualdades anteriores las hemos probado para un $\varepsilon > 0$ cualquiera, luego como $\sum_{i=1}^{N}(\sum_{j=1}^{N} b_{i,j}) = \sum_{j=1}^{N}(\sum_{i=1}^{N} b_{i,j})$ para todo $N \in \mathbb{N}$ tenemos que

$$\sum_{i=1}^{\infty}(\sum_{j=1}^{\infty} b_{i,j}) = \sum_{j=1}^{\infty}(\sum_{i=1}^{\infty} b_{i,j}) < \infty$$

como queríamos probar.□

5.2. Funciones p-ádicas

En esta sección introduciremos brevemente las funciones p-ádicas y algunos conceptos básicos de este tipo de funciones.

Definición 5.9. Una función $f : \mathbb{Z}_p \longrightarrow \mathbb{Q}_p$ es *continua en un punto* $a \in \mathbb{Z}_p$ si para cada $\varepsilon > 0$ existe $\delta > 0$ tal que si $|x - a|_p < \delta$ entonces $|f(x) - f(a)|_p < \varepsilon$ para todo $x \in \mathbb{Z}_p$.
La función $f : \mathbb{Z}_p \longrightarrow \mathbb{Q}_p$ es *continua* si lo es en todos los puntos de $\mathbb{Z}_p$.
La función $f : \mathbb{Z}_p \longrightarrow \mathbb{Q}_p$ es *uniformemente continua* si para todo $\varepsilon > 0$ existe $\delta > 0$ tal que si $|x - y|_p < \delta$ entonces $|f(x) - f(y)|_p < \varepsilon$ para todo $x, y \in \mathbb{Z}_p$.
Diremos que $f : \mathbb{Z}_p \longrightarrow \mathbb{Q}_p$ es *localmente constante* si para todo $x \in \mathbb{Z}_p$ existe un entorno U_x de x tal que f es constante en él.

***Observación* 25.** En $\mathbb{R}$ las únicas funciones localmente constantes son las constantes. En $\mathbb{Q}_p$ sin embargo no es así debido a las propiedades de la norma p-ádica. Por ejemplo, la función característica de cualquier bola en $\mathbb{Q}_p$ es localmente constante, pues tanto la bola como su complementario son abiertos.

Presentamos unas proposiciones relativa a esto.

Proposición 5.10. Las funciones localmente constantes son continuas.

Demostración
Si para cada x hay un entorno U_x tal que f es constante en él resulta obvio que f es continua en $\mathbb{Z}_p$. □

Proposición 5.11. Sea $f : \mathbb{Z}_p \longrightarrow \mathbb{Q}_p$ una función localmente constante. Entonces $\mathbb{Z}_p$ se puede escribir como la unión

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

donde U_{x_i} son las bolas disjuntas en las que f toma distintos valores. En particular el conjunto $\{f(x); x \in \mathbb{Z}_p\}$ tiene un número finito k de elementos distintos.

Demostración
Consideramos para cada $x \in \mathbb{Z}_p$ la bola U_x (entorno de x) en la que f es constante. Entonces este conjunto de bolas es un recubrimiento de $\mathbb{Z}_p$,que como es compacto tiene un subrecubrimiento finito $U_{x_1}, U_{x_2}, \ldots U_{x_m}$. Debemos recordar que por ser $\mathbb{Z}_p$ un espacio ultramétrico las bolas o son disjuntas o están contenidas una dentro de la otra. Suprimiendo las bolas que están contenidas en otras obtenemos un conjunto finito de bolas disjuntas $U_{x-1}, U_{x-2}, \ldots U_{x-k}$ que recubre $\mathbb{Z}_p$. □

***Observación* 26.** Si dada una función $f : \mathbb{Z}_p \longrightarrow \mathbb{Q}_p$ localmente constante tenemos la partición $\mathbb{Z}_p = \cup_{i=1}^{k} U_{x_i}$ no es difícil ver que entonces la función tiene la forma

$$f(x) = \sum_{i=1}^{k} f(x_i)\chi_{U_{x_i}}(x)$$

donde $\chi_{U_{x_i}}$ es la función característica de U_{x_i}. La similitud con las funciones simples en $\mathbb{R}$ es clara.

Corolario 5.12. Una función localmente constante en $\mathbb{Z}_p$ es uniformemente continua.

Demostración
Sea $\mathbb{Z}_p = \cup_{i=1}^{k} U_{x_i}$ la partición de $\mathbb{Z}_p$ de la proposición anterior, p^{-m_i} el radio de U_{x_i} para $i =$

$1, 2, \ldots, k$ y $m = \text{máx}_{1 \leq i \leq k}\{m_i\}$. Si consideramos $\delta = p^{-m}$ veremos que funciona para todo $\varepsilon > 0$: Sean $x, y \in \mathbb{Z}_p$ tales que $|x - y|_p < p^{-m}$, como $x \in U_{x_i}$ para algún i, y puesto que en espacios ultramétricos cualquier punto de la bola es su centro, podemos suponer que $x = x_i$. Entonces $|x_i - y|_p < p^{-m} \leq p^{-m_i}$, luego $f(x_i) = f(x) = f(y)$ y es obvio que $|f(x) - f(y)|_p < \varepsilon$. $\square$

Definición 5.13. Sea $E \subset \mathbb{Z}_p$. Una función $f : E \longrightarrow \mathbb{Q}_p$ se denomina *función paso* si existe un entero positivo t tal que

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

El entero más pequeño t que cumple esta propiedad se denomina *orden de f*.

De la definición deducimos que una función paso es localmente constante (luego uniformemente continua).
Para llegar a una propiedad sorprendente de las funciones paso es necesaria la construcción de la siguiente partición de $E \subset \mathbb{Z}_p$ para cada entero t.
Sea $t \in \mathbb{Z}$, consideramos $\mathbb{N}_t = \{1, 2, \ldots, p^t - 1\}$, para cada $x \in \mathbb{Z}_p$ escribiremos su extensión canónica

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

y tomamos $N_x = x_0 + x_1 p + \ldots + x_{t-1} p^{t-1} < p^t$. Entonces $N_x \in \mathbb{N}_t$ y $|x - N_x|_p \leq p^{-t}$.
Para cada $N \in \mathbb{N}_t$ escribimos $E(N) = E \cap U(N, t)$ donde

$$U(N, t) = \{x \in \mathbb{Z}_p; |x - N|_p \leq p^{-t}\}$$

Hemos visto entonces que todo $x \in \mathbb{Z}_p$ pertenece a algún $U(N, t)$, y como para $N, M \in \mathbb{N}_t$ tenemos que $|N - M|_p > p^{-t}$ ($N < p^t, M < p^t$, luego $|N - M| < p^t \Rightarrow |N - M|_p > p^{-t}$) las bolas $U(N, t), U(M, t)$ son disjuntas y por tanto

$$E = \cup_{N=0}^{p^t - 1} E(N) \text{ es una partición de } E$$

Presentamos entonces el siguiente teorema:

Teorema 5.14. *Toda función paso definida en un subconjunto $E = \mathbb{N}$ ó $\mathbb{Z}_p$ es periódica.*

Demostración
Sea $E = \mathbb{N}$ ó $\mathbb{Z}_p$ y $f : E \longrightarrow \mathbb{Q}_p$ una función paso de orden t, consideramos la partición de E dada antes. Dados $x, y \in E(N)$, $|x - y|_p = |(x - N) + (N - y)|_p \leq p^{-t}$ luego $f(x) = f(y)$. Observemos que si $x \in E(N)$ entonces $x + p^t \in E(N)$ luego $f(x) = f(x + p^t)$ para todo $x \in E$. $\square$

Así como en los números reales las funciones continuas se pueden aproximar por funciones simples, para los números p-ádicos sucede algo parecido. La diferencia radica en que en $\mathbb{Q}_p$ las funciones paso son continuas.

Teorema 5.15. *Sea $E = \mathbb{N}$ ó $\mathbb{Z}_p$, una función $f : E \longrightarrow \mathbb{Q}_p$ es uniformemente continua en E si y sólo si para cada entero positivo s existe otro entero $t = t(s)$ y una función paso $S : E \longrightarrow \mathbb{Q}_p$ de orden por lo menos t tal que*

$$|f(x) - S(x)|_p \leq p^{-s} \text{ para todo } x \in E \tag{19}$$

Demostración

Supongamos que existe S tal que se cumple (19), luego dado x_0 tal que $|x - x_0|_p \leq p^{-t}$ se cumple que $S(x) = S(x_0)$, $|f(x) - S(x)|_p \leq p^{-s}$ y $|f(x_0) - S(x_0)|_p \leq p^{-s}$. Entonces

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

para todo x, x_0 tales que $|x - x_0|_p \leq p^{-t}$, por lo que f es uniformemente continua.
Supongamos ahora que f es uniformemente continua en E, denotamos por s y $t = t(s)$ a dos enteros positivos tales que

$$|f(x) - f(x_0)|_p \leq p^{-s} \text{ para todo } x, x_o \in E \text{ tales que } |x - x_0|_p \leq p^{-t}$$

Sea N_x la truncación de hasta p^{t-1} de la extensión p-ádica canónica de x, y definimos la función $S : E \longrightarrow \mathbb{Q}_p$ por

$$S(x) = f(N_x) \text{ para } x \in E$$

Entonces S es una función de paso a lo sumo t (pues si $|x - x_0|_p \leq p^{-t}$ es claro que $N_x = N_{x_0}$). Además

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

pues $|x - N_x|_p \leq p^{-t}$ y por hipótesis f es uniformemente continua. □

Para finalizar esta sección vamos a enunciar dos teoremas relativos a la continuidad y continuidad uniforme. El primero de ellos es muy similar a uno existente en $\mathbb{R}$.

Teorema 5.16. *Sea E un subconjunto de $\mathbb{Z}_p$ y x_0 un punto de acumulación de E, es decir; existe una sucesión de elementos en E que converge hacia x_0.*
Sean $f : E \longrightarrow \mathbb{Q}_p$ y $g : E \longrightarrow \mathbb{Q}_p$:

1. *f es continua en x_0 si y sólo si para toda sucesión (x_n) en E tal que $\lim_{n\to\infty} x_n = x_0$ se tiene que*

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

2. *Si f y g son continuas en x_0 también son continuas $f + g$,$f - g$ y $f \cdot g$. Además, si $g(x_0) \neq 0$ entonces $\frac{f}{g}$ es continua también en x_0.*

Demostración

1. Si f es continua en x_0, dado $\varepsilon > 0$ existe $\delta > 0$ tal que para todo x tal que $|x-x_0|_p < \delta$ entonces $|f(x)-f(x_0)|_p < \varepsilon$. Como (x_n) converge hacia x_0 existe $N \in \mathbb{N}$ tal que para todo $n \geq N$ se tiene que $|x_0 - x_n|_p < \delta$, luego $|f(x_0) - f(x_n)|_p < \varepsilon$, y por tanto $\lim_{n\to\infty} f(x_n) = f(x_0)$.
   Para la implicación contraria utilizamos el contrarrecíproco: supongamos que f no es continua en x_0, luego existe un ε_0 tal que para todo $\delta > 0$, si $|x - x_0|_p < \delta$ entonces $|f(x) - f(x_0)|_p \geq \varepsilon_0$. Consideramos para cada $n \in \mathbb{N}$ los deltas $\delta_n = \frac{1}{n}$ y un elemento x_n de E tal que $|x_n - x_0|_p < d_n$. Obtenemos así una sucesión de E que converge hacia x_0, sin embargo $|f(x) - f(x_0)|_p \geq \varepsilon_0$, luego $\lim_{n\to\infty} f(x_n) \neq f(x_0)$, que es lo que queríamos probar.

2. La demostración es análoga al caso real.□

El segundo teorema presenta similitud con el ***Teorema de Heine*** (o Teorema de la continuidad uniforme) [1] del caso real, y dice lo siguiente:

Teorema 5.17. *Toda función $f : \mathbb{Z}_p \longrightarrow \mathbb{Q}_p$ continua en $\mathbb{Z}_p$ es uniformemente continua en $\mathbb{Z}_p$ y está acotada en $\mathbb{Z}_p$.*

Demostración

Supongamos que f no es uniformemente continua en $\mathbb{Z}_p$, luego existe $\varepsilon_0 > 0$ tal que para todo $\delta > 0$ existen x_δ, y_δ tales que $|x_\delta - y_\delta|_p < \delta$ y $|f(x_\delta) - f(y_\delta)|_p \geq \varepsilon_0$. Tomamos ε_0 y consideramos $\delta_n = \frac{1}{n}$ para todo $n \in \mathbb{N}$. Tenemos entonces dos sucesiones de números $(x_n), (y_n)$ tales que $|x_n - y_n|_p < \frac{1}{n}$ y $|f(x_n) - f(y_n)|_p \geq \varepsilon_0$.
Ahora, $\mathbb{Z}_p$ es compacto, luego dado $x_0 \in \mathbb{Z}_p$ existen subsucesiones $(x_{n_k}), (y_{n_k})$ que convergen a x_0. Además f es continua en x_0, luego $\lim_{n\to\infty} f(x_{n_k}) = f(x_0)$ y $\lim_{n\to\infty} f(y_{n_k}) = f(x_0)$. Pero $|f(x_{n_k}) - f(y_{n_k})|_p \geq \varepsilon_0$, llegamos a un absurdo, luego f es uniformemente continua en $\mathbb{Z}_p$. □

6. Análisis p-ádico comparado con el real: algunos resultados

En esta última sección nos centraremos en presentar algunos teoremas importantes existentes en $\mathbb{R}$ pero cuya versión p-ádica no existe. Para ello introducimos primero la siguiente definición:

Definición 6.1. Sea $X \subset \mathbb{Q}_p$ un subconjunto de $\mathbb{Q}_p$ y $a \in X$ un punto de acumulación de X. Una función $f : X \longrightarrow \mathbb{Q}_p$ es *diferenciable en* a si la derivada $f'(a)$ definida por

$$f'(a) := \lim_{x \to a} \frac{f(x) - f(a)}{x - a} \quad \text{existe.}$$

La función $f : X \longrightarrow \mathbb{Q}_p$ es *diferenciable en* X si $f'(a)$ existe para todo $a \in X$.

***Observación* 27.** Lo primero que debemos destacar es que por la forma en la que está definida, la diferenciabilidad de funciones p-ádicas en una variable equivale a la derivabilidad: este fenómeno se observa también en las funciones de una variable real.

Veremos ahora algunas propiedades de la derivada, que podemos encontrar también en $\mathbb{R}$.

Proposición 6.2.

- Las reglas de derivación para la suma, la resta, el producto, el cociente y la composición son idénticas a las que presenta $\mathbb{R}$.
- Toda función diferenciable es continua.

Demostración
La demostración de las reglas que aparecen en el primer punto es idéntica a la que se realiza en $\mathbb{R}$, y no la escribiremos.
Respecto al segundo punto; sabemos que para todo $\varepsilon > 0$ existe $\delta > 0$ tales que si $|x-a|_p < \delta$ entonces $|\frac{f(x)-f(a)}{x-a} - f'(a)|_p < \varepsilon$. Entonces $|f(x)-f(a)-(x-a)f'(a)|_p < \varepsilon|x-a|_p$ y al hacer $x \to a$ llegamos a que $\lim_{x \to a} |f(x) - f(a)|_p = 0$, luego f es continua en a. $\square$

Como consecuencia del primer punto de la proposición anterior deducimos que la derivada de un polinomio $P(x) = \sum_{i=0}^{n} a_i x^i$ es $P'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$.
Por otro lado hemos dado una definición de continuidad para funciones $f : \mathbb{Z}_p \longrightarrow \mathbb{Q}_p$ en términos de *épsilon* y *delta*. Presentamos ahora la definición topológica clásica de *función continua* para funciones $f : \mathbb{Q}_p \longrightarrow \mathbb{Q}_p$.

Definición 6.3. Una función $f : \mathbb{Q}_p \longrightarrow \mathbb{Q}_p$ diremos que es *continua* si para todo conjunto abierto $V \subset \mathbb{Q}_p$ tenemos que $f^{-1}(V)$ es también un subconjunto abierto.

6.1. Teorema de Rolle

El ***Teorema de Rolle*** [4] en el caso real se enuncia de la siguiente manera:

Teorema 6.4 (**Teorema de Rolle**). *Sea f una función real continua en un intervalo $[a,b]$ diferenciable en (a,b) con $f(a)=f(b)$. Entonces existe $c\in(a,b)$ tal que $f'(c)=0$.*

En el caso real este resultado nos parece muy intuitivo si tenemos en cuenta el significado de la derivada: la pendiente de la recta tangente a la función. ¿Existe un resultado similar en $\mathbb{Q}_p$?
Lo primero que debemos notar es que no hemos dotado a $\mathbb{Q}_p$ de un orden, luego no tendría sentido intentar enunciar algo similar en términos de intervalos. Sin embargo aunque excluyamos ese primer inconveniente, en $\mathbb{Q}_p$ no puede darse un resultado de esta naturaleza.

***Ejemplo* 6.5.** Consideramos la función $f:\mathbb{Z}_p\longrightarrow\mathbb{Q}_p$ dada por $f(x)=x^p-x$. Observamos que $f(0)=f(1)=0$ y que la función f es continua y derivable en $\mathbb{Z}_p$, con $f'(x)=px^{p-1}-1$. Luego para todo $x\in\mathbb{Z}_p$ tenemos que $f'(x)\in\mathbb{Z}_p-1$ luego $f'(x)\neq 0$.

***Observación* 28.** Cuando definimos la derivada utilizamos el concepto de límite, que se basa en una idea de "cercanía" o "aproximación" utilizando elementos como el *épsilon* arbitrariamente pequeño. En los números reales esta idea de "distancia natural" se apoya sobre la norma del valor absoluto, y es por eso que resulta mucho más intuitiva la distancia en $\mathbb{R}$.
En los números p-ádicos por el contrario la norma induce una distancia que nada tiene que ver con la "distancia natural" que fácilmente podemos visualizar, y es por eso que teoremas fundamentales e intuitivos como el de Rolle en $\mathbb{Q}_p$ simplemente no se cumplen.

En el análisis real, una consecuencia muy importante de este resultado es el ***Teorema del valor medio***.

6.2. Teorema del valor medio

Teorema 6.6 (**Teorema del valor medio**). *Sea f una función real continua en un intervalo $[a,b]$ y diferenciable en (a,b). Entonces para cada $x\neq y\in(a,b)$ existe $c\in(x,y)$ tal que*

$$f(y)-f(x)=f'(c)(y-x)$$

Por lo tanto si $f'(c)=0$ para todo $c\in(x,y)$ entonces es que $f(x)=f(y)$.

Al igual que sucedía con el Teorema de Rolle , el Teorema del valor medio tampoco va a tener equivalente en los números p-ádicos. Las funciones localmente constantes nos sirven de contraejemplo.

***Ejemplo* 6.7.** Consideramos un subconjunto $E \subset \mathbb{Z}_p$ cualquiera que no tenga puntos aislados, y sea $f : E \longrightarrow \mathbb{Q}_p$ una función localmente constante. Entonces para cualquier $a \in E$ existe $\varepsilon > 0$ tal que para todo $x \in E$ que cumple $|x - a|_p < \varepsilon$ se tiene que $f(x) = f(a)$. El cociente incremental queda

$$\frac{f(x) - f(a)}{x - a} = 0 \text{ para todo x} \in E \text{ tal que } |x - a|_p < \varepsilon$$

En consecuencia f es diferenciable en todo E y además $f'(a) = 0$ para todo $a \in E$. Sin embargo f no es constante.

En $\mathbb{R}$ no existen funciones no constantes que sí lo sean en un entorno de cada punto y que además sean continuas, pues por la noción de distancia en la recta de los números reales habría necesariamente un "salto".
Concluimos entonces que existen muchas funciones p-ádicas de derivada nula que no son constantes. Introducimos la siguiente definición.

Definición 6.8. Llamaremos funciones *pseudo-constantes* a aquellas funciones cuya derivada es cero: $\{f : \mathbb{Z}_p \longrightarrow \mathbb{Q}_p; f' = 0\}$.

Hemos visto que hay funciones localmente constantes que son pseudo-constantes (partíamos de un conjunto E sin puntos aislados). Veremos como último resultado que no todas las funciones pseudo-constantes son localmente constantes.

Proposición 6.9. Existe una función $f : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$ pseudo-constante que no es localmente constante.

Demostración
Vamos a construir la función f: sea $x \in \mathbb{Z}_p$ de la forma $x = \sum_{n=0}^{\infty} a_n p^n$, definimos

$$f(x) := \sum_{n=0}^{\infty} a_n p^{2n}$$

Tomamos dos números distintos $x = \sum_{n=0}^{\infty} a_n p^n$ e $y = \sum_{n=0}^{\infty} b_n p^n$, existe $j = 0, 1, 2, \ldots$ tal que $|x - y|_p = p^{-j}$. Es decir; $a_0 = b_0, a_1 = b_1, \ldots, a_j \neq b_j$ y por lo tanto $|f(x) - f(y)|_p = p^{-2j}$. En consecuencia

$$|f(x) - f(y)|_p = |x - y|_p^2 \text{ para todo } x, y \in \mathbb{Z}_p$$

Concluimos que f es inyectiva: si $x \neq y$ entonces $f(x) \neq f(y)$, luego f no es localmente constante, y además

$$\left|\frac{f(x) - f(y)}{x - y}\right|_p = |x - y|_p \xrightarrow{x \to y} 0$$

por lo que f' es idénticamente nula. □

A. p-ádicos en *Sage*

En esta sección explicaremos brevemente cómo implementar cálculos sencillos sobre el cuerpo de los números p-ádicos en ***Sage***. Como hemos visto a lo largo de este trabajo los números p-ádicos son representados mediante series infinitas de la forma

$$a = \sum_{n=-m}^{\infty} a_n p^n \tag{20}$$

Sin embargo esto requiere infinitos datos para cada número p-ádico, y al igual que sucede cuando trabajamos con números reales nos vemos obligados a conformarnos con una aproximación finita. Nos centraremos en ilustrar especialmente este hecho y sus efectos.
Desde un principio hemos trabajado con la forma canónica (20) de la cual podemos tomar una truncación finita que se aproxime a $a \in \mathbb{Q}_p$ tanto como queramos.
Tomando los términos hasta p^k para cierto $k \in \mathbb{N}$ tenemos que

$$a = a_{-n}p^{-n} + a_{-n+1}p^{-n+1} + \ldots + a_0 + a_1 p + \ldots + a_{k-1}p^{k-1} + O(p^k)$$

Diremos que k es la *precisión absoluta* de esta truncación, que denotaremos por *aproximación de precisión k*
Sabemos también que dado un número $x \in \mathbb{Q}_p$ existen $v \in \mathbb{Z}$ y $u \in \mathbb{Z}_p^*$ tales que $x = up^v$ (de hecho v es el orden de x). Por lo tanto tiene sentido pensar que para guardar un número p-ádico es suficiente con almacenar su orden v y una aproximación finita a $u \in \mathbb{Z}_p^*$. Surge de aquí la siguiente definición:

Definición A.1. Dado $x \in \mathbb{Q}_p$, la *precisión relativa* de una aproximación de x se define como su precisión absoluta menos el orden de x.

***Ejemplo* A.2.** Sea $a = \sum_{n=-m}^{\infty} a_n p^n$, su orden es $v = -m$ y $u = \sum_{n=0}^{\infty} a_{-m+n}p^n$. Si consideramos una aproximación de precisión absoluta k

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

su precisión relativa es $k - v = k + m$. Observemos que, tal y como esperamos, a mayor precisión absoluta menor es la diferencia entre a y su aproximación:

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

Sin embargo una gran precisión absoluta no garantiza que la aproximación sea buena; si tomamos por ejemplo un número p-ádico $b = \sum_{n=k}^{\infty} b_n p^n$ donde $k > 0$, tomar su

aproximación de precisión $k+1$ es tomar b_k, que es una aproximación mediocre.
Por otro lado para los p-ádicos de norma muy grande de la forma $c = \sum_{n=-k}^{\infty} c_n p^n$ una precisión absoluta no muy grande puede dar una aproximación relativamente buena.
Por eso es importante tener en cuenta la precisión relativa.

En ***Sage*** existen tres representaciones diferentes de $\mathbb{Z}_p$:

1. Con un *anillo de módulo fijo*
2. Con un *anillo de precisión absoluta acotada*
3. Con un *anillo de precisión relativa acotada*

Y una para $\mathbb{Q}_p$ mediante un *cuerpo de precisión relativa acotada.*

Anillo de módulo fijo

Esta es la forma más sencilla de proceder. Comenzamos tomando un $k \in \mathbb{N}$ como precisión absoluta y representaremos todos los enteros $\mathbb{Z}_p$ por sus truncaciones de precisión k:

$$a \in \mathbb{Z}_p, \;\; a = \sum_{n=0}^{k-1} a_n p^n, \;\; a_n \in \{0, 1, \ldots p-1\}$$

El cuerpo $\mathbb{Z}_p$ con el que trabajaremos será similar a $\mathbb{F}_{p^k}$. ***Sage*** tiene una función directa para crear $\mathbb{Z}_p$ de precisión k sin tener que construir paso a paso $\mathbb{F}_{p^k}$. Procedemos de la siguiente manera:

```
In:  K = Zp(7, prec = 20, type = 'fixed-mod', print_mode = 'series')
     K
Out: 7-adic Ring of fixed modulus 7^20
```

Una vez que lo tenemos definido podemos pedirle que nos muestre algún elemento concreto:

```
In:  a = K(89)
     a
Out: 5 + 5*7 + 7^2  #Nos muestra la forma 7-ádica de 89

In:  b = K(10^20)
     b
Out: 2 + 6*7 + 5*7^2 + 2*7^3 + 5*7^4 + 4*7^5 + 7^6 + 7^9 + 2*7^10 +
    6*7^11 + 7^12 + 6*7^13 + 5*7^14 + 3*7^15 + 7^16 + 3*7^17 + 5*7^18
    + 7^19   #Llega sólo hasta la precisión pedida
```

Comprobamos que, puesto que la forma 7-ádica de 10^{20} supera exponentes de orden $k = 20$ el elemento que nos devuelve no es exactamente la del número pedido:

```
In:  2 + 6*7 + 5*7^2 + 2*7^3 + 5*7^4 + 4*7^5 + 7^6 + 7^9 + 2*7^10 +
     6*7^11 + 7^12 + 6*7^13 + 5*7^14 + 3*7^15 + 7^16 + 3*7^17 +
     5*7^18 + 7^19
Out: 20290329092162747

In:  10^(20)-20290329092162747
Out: 99979709670907837253
```

Obviamente 10^{20} y la representación b que hemos tomado no son iguales, sin embargo sí lo son en $\mathbb{F}_7$, pues difieren en potencias de 7 de orden 20 o superior.

```
In:  K(99979709670907837253)
Out: 0

In:  c = 99979709670907837253
     c.factor()
Out: 7^21*179
```

Una vez visto esto podemos proceder a realizar algunas operaciones:

```
In:  a = K(2598)
     b = K(359)
     a
     b
     a+b
     a*b
Out: 1 + 4*7^2 + 7^4
     2 + 2*7 + 7^3
     3 + 2*7 + 4*7^2 + 7^3 + 7^4
     2 + 2*7 + 7^2 + 3*7^3 + 3*7^4 + 6*7^5 + 7^7 #el producto se realiza
     de la misma manera que vimos en el ejemplo 2.4
```

Cuando definimos un elemento en un cuerpo su precisión queda fijada, y aunque luego trabajemos sobre un cuerpo de mayor precisión esta no cambia:

```
In:  Z = Zp(7, prec = 30, type = 'fixed-mod', print_mode = 'series')
     Z
Out: 7-adic Ring of fixed modulus 7^30
```

```
#creamos un cuerpo auxiliar
In:  Z(8^21);
Out: 1 + 3*7^2 + 2*7^3 + 5*7^4 + 2*7^6 + 5*7^7 + 5*7^9 + 4*7^10 +
     2*7^11 + 7^12 + 7^13 + 6*7^14 + 7^16 + 7^18 + 4*7^19 + 3*7^20 +
     2*7^21 + 2*7^22

In:  a = K(8^21);a
Out: 1 + 3*7^2 + 2*7^3 + 5*7^4 + 2*7^6 + 5*7^7 + 5*7^9 + 4*7^10 +
     2*7^11 + 7^12 + 7^13 + 6*7^14 + 7^16 + 7^18 + 4*7^19

In:  7^18 + 3*7^19 + 3*7^20
Out: 275201898046865881

In:  b = K(275201898046865881);b
Out: 7^18 + 3*7^19

#Realizamos una operación en K
In:  a-b
Out: 1 + 3*7^2 + 2*7^3 + 5*7^4 + 2*7^6 + 5*7^7 + 5*7^9 + 4*7^10 +
     2*7^11 + 7^12 + 7^13 + 6*7^14 + 7^16 + 7^19

#Hacemos la misma operación sobre Z
In:  Z(a-b)
Out: 1 + 3*7^2 + 2*7^3 + 5*7^4 + 2*7^6 + 5*7^7 + 5*7^9 + 4*7^10 +
     2*7^11 + 7^12 + 7^13 + 6*7^14 + 7^16 + 7^19
#Aunque ahora Z sea un cuerpo de precisión 30, como a y b están en K
su precisión se reduce

In:  Z(8^21-275201898046865881)
Out: 1 + 3*7^2 + 2*7^3 + 5*7^4 + 2*7^6 + 5*7^7 + 5*7^9 + 4*7^10 +
     2*7^11 + 7^12 + 7^13 + 6*7^14 + 7^16 + 7^19 + 2*7^21 + 2*7^22
```

Utilizando este método, cuando realizamos una operación en la que debería haber una pérdida de precisión, el elemento resultante no refleja que la precisión ya no es absoluta. En ***Sage*** podemos dividir los números p-ádicos por unidades utilizando el comando // :

```
In:  g = K(8^21);g
     Z(8^21)
```

```
Out: 1 + 3*7^2 + 2*7^3 + 5*7^4 + 2*7^6 + 5*7^7 + 5*7^9 + 4*7^10 +
     2*7^11 + 7^12 + 7^13 + 6*7^14 + 7^16 + 7^18 + 4*7^19
     1 + 3*7^2 + 2*7^3 + 5*7^4 + 2*7^6 + 5*7^7 + 5*7^9 + 4*7^10 +
     2*7^11 + 7^12 + 7^13 + 6*7^14 + 7^16 + 7^18 + 4*7^19 + 3*7^20 +
     2*7^21 + 2*7^22

In: g//7
Out: 3*7 + 2*7^2 + 5*7^3 + 2*7^5 + 5*7^6 + 5*7^8 + 4*7^9 + 2*7^10 +
     7^11 + 7^12 + 6*7^13 + 7^15 + 7^17 + 4*7^18
#No se refleja la pérdida de precisión al dividir
```

Anillo de precisión absoluta acotada

Este tipo de representación de $\mathbb{Z}_p$ es similar a la anterior, pero cada elemento lleva el registro de su precisión, por lo que cuando se reduce al realizar alguna operación queda reflejado en el elemento.

```
In:  R = Zp(5, prec = 10, type = 'capped-abs', print_mode = 'series')
     R
Out: 5-adic Ring with capped absolute precision 10

In:  a = R(524);a
     b = R(125);b
     R(5^10)
Out: 4 + 4*5 + 4*5^3 + O(5^10)
     5^3 + O(5^10)
     O(5^10)

In:  a+b
     a-b
     a*b
     c = a//5;c
Out: 4 + 4*5 + 5^4 + O(5^10)
     4 + 4*5 + 3*5^3 + O(5^10)
     4*5^3 + 4*5^4 + 4*5^6 + O(5^10)
     4 + 4*5^2 + O(5^9) #Refleja la pérdida de precisión

In:  c+b
```

```
Out: 4 + 4*5^2 + 5^3 + O(5^9)
```

Anillos y cuerpos de precisión relativa acotada

Antes hemos hecho referencia a la importancia de la precisión relativa viendo un par de casos generales en los que la precisión absoluta no tenía gran importancia. Por eso en lugar de acotar la precisión absoluta hay casos en los que resulta más útil restringir la precisión relativa.

```
In:  K = Zp(7, prec = 10, type = 'capped-rel', print_mode = 'series')
     K
Out: 7-adic Ring with capped relative precision 10
```

Ahora la precisión absoluta cambia para elemento dependiendo de su expresión p-ádica

```
In:  a = K(488)
     a
     b = K(105)
     b
     c = K(7^2)
Out: 5 + 6*7 + 2*7^2 + 7^3 + O(7^10)
     7 + 2*7^2 + O(7^11)
     7^2 + O(7^12)
```

Este método funciona muy bien para el producto, ya que el menor orden del producto es la suma de los menores órdenes de los factores. Para la suma sin embargo no es así, ya que los términos de menor orden pueden cancelarse.

```
In:  a=K(7^4+2*7^12);a
     b=K(2+3*7^6);b
     c=K(6*7+7^3);c
     d=K(7+7^4);d
Out: 7^4 + 2*7^12 + O(7^14)
     2 + 3*7^6 + O(7^10)
     6*7 + 7^3 + O(7^11)
     7 + 7^4 + O(7^11)


In:  a*b
Out: 2*7^4 + 3*7^10 + 4*7^12 + O(7^14)#No desaparecen términos y la
precisión no cambia.
```

```
In:  a+b
Out: 2 + 7^4 + 3*7^6 + O(7^10) #El término 4*7^12 desaparece, pero la
precisión es la misma.

In:  c+d
Out: 7^2 + 7^3 + 7^4 + O(7^11) #La precisión relativa se reduce: 11-2=9
```

De manera similar podemos crear directamente un cuerpo de precisión relativa acotada, que hará las veces de $\mathbb{Q}_p$:

```
In:  Q = Qp(7, prec = 10, type = 'capped-rel', print_mode = 'series')
     Q
Out: 7-adic Field with capped relative precision 10

In:  c = 7^(-1)+2*7
     c
Out: 7^(-1)+2*7
```

Podemos realizar operaciones como la división de números p-ádicos:

```
In:  a = Q(488);a
     b = Q(105);b
     a/b
     Q(488/105)
Out: 5 + 6*7 + 2*7^2 + 7^3 + O(7^10)
     7 + 2*7^2 + O(7^11)
     5*7^-1 + 3 + 2*7 + 3*7^2 + 6*7^4 + 7^5 + 3*7^6 + 6*7^8 + O(7^9)
     5*7^-1 + 3 + 2*7 + 3*7^2 + 6*7^4 + 7^5 + 3*7^6 + 6*7^8 + O(7^9)
```

Referencias

[1] Tom M. Apostol. *Calculus. Vol. I: One-variable calculus, with an introduction to linear algebra.* Blaisdell Publishing Co. [Ginn and Co.], Waltham, Mass.-Toronto, Ont.-London, second edition, 1967.

[2] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra.* Addison-Wesley Series in Mathematics. Westview Press, Boulder, CO, economy edition, 2016. For the 1969 original see [MR0242802].

[3] Bernard Dwork. On the rationality of the zeta function of an algebraic variety. *Amer. J. Math.*, 82:631–648, 1960.

[4] John M. Howie. *Real analysis.* Springer Undergraduate Mathematics Series. Springer-Verlag London, Ltd., London, 2001.

[5] Svetlana Katok. *p-adic analysis compared with real*, volume 37 of *Student Mathematical Library.* American Mathematical Society, Providence, RI; Mathematics Advanced Study Semesters, University Park, PA, 2007.

[6] James R. Munkres. *Topology.* Prentice Hall, Inc., Upper Saddle River, NJ, second edition, 2000.

[7] Alain M. Robert. *A course in p-adic analysis*, volume 198 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 2000.

[8] J.-P. Serre. *A course in arithmetic*, volume No. 7 of *Graduate Texts in Mathematics.* Springer-Verlag, New York-Heidelberg, 1973. Translated from the French.