UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

NÚMEROS *P*-ÁDICOS

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

MATEMÁTICO

P R E S E N T A :

MANUEL HERNÁNDEZ HERNÁNDEZ

DIRECTOR DE TESIS:
DR. SERGEY ANTONYAN
2015

Ciudad Universitaria, D. F.

1. Datos del alumno
Hernández
Hernández
Manuel
66494134
Universidad Nacional Autónoma de México
Facultad de Ciencias
Matemáticas
101001539

2. Datos del tutor
Dr.
Sergey
Antonyan

3. Datos del sinodal 1
Dr.
Hugo Alberto
Rincón
Mejía

4. Datos del sinodal 2
Mat.
Julio César
Guevara
Bravo

5. Datos del sinodal 3
Dra.
Natalia
Jonard
Pérez

6. Datos del sinodal 4
Dr.
Fidel
Casarrubias
Segura

7. Datos del trabajo escrito
Números *p*-ádicos
51 p
2015

Índice general

Introducción

Para cada número primo p los números p-ádicos forman un campo $\mathbb{Q}_p$ que extiende al campo de los números racionales $\mathbb{Q}$. Una posible construcción es definir una métrica en $\mathbb{Q}$, distinta de la métrica usual definida por el valor absoluto, y observar que el espacio métrico resultante no es completo. Al considerar la completación de este espacio, la forma de la métrica nos permite extender las operaciones del campo $\mathbb{Q}$ y obtener nuevamente un campo que es precisamente $\mathbb{Q}_p$.

Los números p-ádicos fueron definidos por primera vez por Kurt Hensel en 1905 para trabajar con distintas representaciones de los números algebraicos. Desde entonces han tenido aplicaciones en la teoría de números permitiendo utilizar las técnicas de las series de potencias, por ejemplo fueron utilizados en la demostración de Andrew Wiles del último teorema de Fermat.

Otro lugar donde han aparecido los números p-ádicos es en la solución de la conjetura de Hilbert-Smith, que puede considerarse una generalización del quinto problema de Hilbert o una mejor formulación del mismo. La conjetura de Hilbert-Smith afirma que si G es un grupo topológico localmente compacto y actúa continua y efectivamente en una variedad topológica conexa y de dimensión finita, entonces G debe ser un grupo de Lie. Se ha logrado demostrar que los únicos posibles contrajemplos son los enteros p-ádicos $\mathbb{Z}_p$, para algún primo p, que son subgrupos de $\mathbb{Q}_p$, es decir, que para demostrar la conjetura bastaría demostrar que para todo primo p, $\mathbb{Z}_p$ no puede actuar continua y efectivamente en una variedad topológica conexa de dimensión finita.

Además de las aplicaciones mencionadas anteriormente se ha desarrollado el análisis p-ádico como una rama propia de las matemáticas.

El objetivo de esta tesis es presentar una construcción de los números p-ádicos y algunas propiedades de los mismos. Como dijimos anteriormente la construcción de los números p-ádicos es a partir de la completación de un espacio métrico, por ello en el capítulo 1 se estudia el caso general de la completación de un espacio métrico para tenerla en cuenta en el caso concreto que estudiaremos más adelante.

En el capítulo 2 se estudia un tipo especial de métricas definidas en un campo, en particular la norma p-ádica en $\mathbb{Q}$, que permiten extender la estructura de campo a la completación del espacio y así se construye el campo de los números p-ádicos. Finalmente se encuentra una expresión de los números p-ádicos que es similar a las expresiones decimales de los reales.

En el capítulo 3 se presentan los algoritmos para hacer las operaciones en el campo $\mathbb{Q}_p$ a partir de la expresión mencionada en el párrafo anterior y se utilizan para encontrar la forma en que se expresan los enteros y los racionales dentro de $\mathbb{Q}_p$. A continuación se presenta el subanillo de enteros p-ádicos $\mathbb{Z}_p$ y se estudian algunas propiedades algebraicas de $\mathbb{Z}_p$ y $\mathbb{Q}_p$ estableciendo la analogía con $\mathbb{Z}$ y $\mathbb{Q}$. Por último, se estudian algunas propiedades topológicas de $\mathbb{Z}_p$ y $\mathbb{Q}_p$, en particular que $\mathbb{Z}_p$ es candidato para contraejemplo de la conjetura de Hilbert-Smith, es decir, que $\mathbb{Z}_p$ es un grupo topológico compacto, pero no es un grupo de Lie.

Capítulo 1

Completación de un espacio métrico

En este capítulo presentaremos una forma general de completar un espacio métrico, es decir, que dado un espacio métrico (X, d), construiremos un espacio métrico completo $(\overline{X}_d, \rho)$ en el que (X, d) pueda ser encajado isométricamente como un subconjunto denso. También veremos una condición para que dos métricas distintas en un mismo conjunto induzcan completaciones equivalentes.

1.1. La construcción

La idea de la construcción es la siguiente: un espacio métrico no es completo cuando existen sucesiones de Cauchy que no son convergentes, que basicamente son "sucesiones convergentes sin límite", es decir, que al espacio le hacen falta algunos puntos en los cuales converjan esas sucesiones.

Así, por cada sucesión de Cauchy no convergente, debemos agregar un punto al espacio, pero como para cada punto existe una infinidad de sucesiones convergentes a él, entonces tenemos que hacer una identificación de las sucesiones de Cauchy que "tienen el mismo límite". Por último extendemos la métrica de la única forma posible.

Empezamos dando algunas definiciones básicas.

Definición 1.1.1. *Sea X un conjunto. Una métrica en X es una función $d\colon X \times X \to [0, \infty)$ que para cualesquiera x, y, z en X cumple:*

1. $d(x, y) = 0 \Leftrightarrow x = y$,
2. $d(x, y) = d(y, x)$,

3. $d(x,z) \leq d(x,y) + d(y,z)$.

En tal caso al par (X,d) *se le llama espacio métrico.*

Definición 1.1.2. *Una sucesión* $(x_n)_{n\in\mathbb{N}}$ *de elementos de* X*, se dice que es convergente a un elemento* $x \in X$ *en* (X,d)*, si para cada número positivo* ε *existe un natural* N *tal que para cualquier* $n \geq N$ *se cumple que* $d(x_n,x) < \varepsilon$.

A x *se le llama límite de la sucesión y se denota simplemente por* $\lim_{n\to\infty} x_n = x$ *cuando no hay ambigüedad respecto a la métrica que se está usando.*

Definición 1.1.3. *Una sucesión* $(x_n)_{n\in\mathbb{N}}$ *de elementos de* X*, es una sucesión d-Cauchy, si para todo número positivo* ε *existe* $N \in \mathbb{N}$ *tal que para cualesquiera* $n, m \geq N$ *se tiene que* $d(x_n,x_m) < \varepsilon$.

Un resultado inmediato es que toda sucesión convergente es d-Cauchy.

Proposición 1. *Toda sucesión convergente en* (X,d) *es d-Cauchy.*

Demostración. Sea $(x_n)_{n\in\mathbb{N}}$ una sucesión convergente en (X,d) y sea $x \in X$ su límite. Para cualquier número positivo ε existe un natural N tal que si $n \geq N$ se cumple que $d(x_n,x) < \frac{\varepsilon}{2}$.

Considerando dos naturales $n, m \geq N$ tenemos que:

$$d(x_n,x_m) \leq d(x_n,x) + d(x,x_m) < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon,$$

por lo tanto la sucesión es d-Cauchy. □

Sin embargo el recíproco no es cierto como lo muestra el siguiente ejemplo.

Ejemplo 2. *Consideremos el intervalo semiabierto de reales* $(0,1]$ *con la métrica definida por el valor absoluto* $d(x,y) = |x-y|$ *y en este espacio la sucesión* $x_n = \frac{1}{n}$*. Esta sucesión es d-Cauchy, pero no tiene límite.*

Definición 1.1.4. *Se dice que un espacio métrico* (X,d) *es completo si para toda sucesión d-Cauchy* $(x_n)_{n\in\mathbb{N}}$ *existe un elemento* $x \in X$ *tal que* $\lim_{n\to\infty} x_n = x$.

Ahora, partiendo de un espacio métrico (X,d) consideremos el conjunto de todas las sucesiones d-Cauchy en X y en él definimos la siguiente relación:

$$(x_n)_{n\in\mathbb{N}} \sim (y_n)_{n\in\mathbb{N}} \Leftrightarrow d(x_n,y_n) \to 0 \text{ cuando } n \to \infty,$$

la cual es una relación de equivalencia. Definimos al conjunto $\overline{X}_d$ como el cociente del conjunto de sucesiones d-Cauchy en X bajo esta relación y denotaremos por $\overline{(x_n)}_{n\in\mathbb{N}}$ a la clase de equivalencia de una sucesión d-Cauchy $(x_n)_{n\in\mathbb{N}}$.

Puesto que nuestra idea es que $\overline{(x_n)}_{n\in\mathbb{N}}$ sea el "límite" de la sucesión $(x_n)_{n\in\mathbb{N}}$, la única forma en que podemos definir la distancia entre dos elementos de $\overline{X}_d$, para que extienda a la métrica d, es la siguiente:

$$\rho(\overline{(x_n)}_{n\in\mathbb{N}}, \overline{(y_n)}_{n\in\mathbb{N}}) = \lim_{n\to\infty} d(x_n, y_n).$$

A continuación demostraremos que esta distancia está bien definida.

Considerando dos elementos de $\overline{X}_d$, tomemos una sucesión representante de cada uno, $(x_n)_{n\in\mathbb{N}}$ y $(y_n)_{n\in\mathbb{N}}$, y consideramos la sucesión de números reales $(d(x_n, y_n))_{n\in\mathbb{N}}$. De la desigualdad del triángulo se sigue que

$$|d(x_n, y_n) - d(x_m, y_m)| \leq d(x_n, x_m) + d(y_n, y_m),$$

y como las sucesiones $(x_n)_{n\in\mathbb{N}}$ y $(y_n)_{n\in\mathbb{N}}$ son d-Cauchy, entonces la sucesión $(d(x_n, y_n))_{n\in\mathbb{N}}$ es una sucesión de Cauchy con la métrica usual en $\mathbb{R}$, que debe de ser convergente, ya que $\mathbb{R}$ es completo, así que el límite usado en nuestra definición existe.

Para mostrar que nuestra definición no depende de los representantes que elegimos, consideremos otros dos representantes $(x_n)_{n\in\mathbb{N}} \sim (x'_n)_{n\in\mathbb{N}}$, $(y_n)_{n\in\mathbb{N}} \sim (y'_n)_{n\in\mathbb{N}}$ y la siguiente desigualdad:

$$d(x'_n, y'_n) \leq d(x'_n, x_n) + d(x_n, y_n) + d(y_n, y'_n),$$

donde todos los sumandos son términos de sucesiones convergentes, de manera que al tomar el límite cuando $n \to \infty$ obtenemos que

$$\begin{aligned} \lim_{n\to\infty} d(x'_n, y'_n) &\leq \lim_{n\to\infty} d(x'_n, x_n) + \lim_{n\to\infty} d(x_n, y_n) + \lim_{n\to\infty} d(y_n, y'_n) \\ &= \lim_{n\to\infty} d(x_n, y_n). \end{aligned}$$

Análogamente se obtiene la otra desigualdad y por tanto ambos límites son iguales.

Por lo anterior nuestra distancia está bien definida y a partir de propiedades simples de límites se puede verificar que cumple la definición de métrica. Con lo anterior queda demostrado el siguiente teorema.

Teorema 3. *El par $(\overline{X}_d, \rho)$ es un espacio métrico.*

Ahora mostraremos que este espacio métrico cumple con las propiedades deseadas, es decir, que es completo y que (X, d) se puede encajar isométricamente como subconjunto denso.

Lo primero que debemos hacer es identificar nuestro espacio original con un subconjunto del nuevo espacio. Como una sucesión constante es d-Cauchy y converge al término constante, entonces identificaremos a cada elemento $x \in X$, con la clase de equivalencia de la sucesión constante cuyos términos son el elemento x.

Con base en lo mencionado, si $(x_n)_{n\in\mathbb{N}}$ y $(y_n)_{n\in\mathbb{N}}$ son sucesiones constantes con $x_n = x$ y $y_n = y$, para toda $n \in \mathbb{N}$, se tiene que

$$\rho(\overline{(x_n)}_{n\in\mathbb{N}}, \overline{(y_n)}_{n\in\mathbb{N}}) = \lim_{n\to\infty} d(x_n, y_n) = \lim_{n\to\infty} d(x, y) = d(x, y),$$

lo que quiere decir que nuestra identificación es un encaje isométrico.

Consideremos un elemento $\overline{(x_n)}_{n\in\mathbb{N}}$ de $\overline{X}_d$ y a la sucesión de clases de equivalencia $(\overline{(x_{kn})}_{n\in\mathbb{N}})_{k\in\mathbb{N}}$, donde $x_{kn} = x_k$ para toda n.

Ahora observemos que esta sucesión converge al elemento que tomamos en $\overline{X}_d$. Para ello consideremos un real positivo ε, y escojamos un natural N tal que para cualesquiera números naturales k y n mayores que N se tiene que $d(x_n, x_k) < \frac{\varepsilon}{2}$. Entonces, al considerar una k mayor que N tenemos que:

$$\rho(\overline{(x_n)}_{n\in\mathbb{N}}, \overline{(x_{kn})}_{n\in\mathbb{N}}) = \lim_{n\to\infty} d(x_n, x_{kn}) = \lim_{n\to\infty} d(x_n, x_k) \leq \frac{\varepsilon}{2} < \varepsilon,$$

ya que $d(x_n, x_k) < \frac{\varepsilon}{2}$ para toda n mayor que N, entonces concluimos que al encajar el espacio X en $\overline{X}_d$ su imagen es un subconjunto denso.

Tenemos el siguiente teorema.

Teorema 4. *Existe una isometría $i : X \to \overline{X}_d$ tal que $i(X)$ es un subconjunto denso de $\overline{X}_d$.*

Por último debemos demostrar que el espacio $(\overline{X}_d, \rho)$ es completo. Para ello consideremos una sucesión ρ-Cauchy en $\overline{X}_d$, $(\overline{(x_{kn})}_{n\in\mathbb{N}})_{k\in\mathbb{N}}$, y encontremos un límite para esta sucesión.

Como cada $(x_{kn})_{n\in\mathbb{N}}$ es una sucesión d-Cauchy, entonces para cada k existe un natural $N(k)$ tal que $d(x_{kn}, x_{km}) \leq \frac{1}{k}$, siempre que $n, m \geq N(k)$.

Podemos elegir los naturales $N(k)$ de forma que $N(k+1) > N(k)$, para toda k y consideremos la sucesión $(x_{kN(k)})_{k\in\mathbb{N}}$ en X. Luego, para cualquier real positivo ε existe un natural N_1 tal que $\rho(\overline{(x_{jn})}_{n\in\mathbb{N}}, \overline{(x_{kn})}_{n\in\mathbb{N}}) < \frac{\varepsilon}{3}$, si $j, k \geq N_1$. Sea N un natural tal que $N \geq \text{máx}\{N_1, \frac{3}{\varepsilon}\}$, así para $j, k \geq N$, y considerando cualquier $n \geq \text{máx}\{N(j), N(k)\}$, se tiene que

$$\begin{aligned} d(x_{jN(j)}, x_{kN(k)}) &\leq d(x_{jN(j)}, x_{jn}) + d(x_{jn}, x_{kn}) + d(x_{kn}, x_{kN(k)}) \\ &\leq \tfrac{1}{j} + d(x_{jn}, x_{kn}) + \tfrac{1}{k}, \end{aligned}$$

y al tomar el límite cuando $n \to \infty$ se obtiene

$$\begin{aligned} d(x_{jN(j)}, x_{kN(k)}) &\leq \tfrac{1}{j} + \rho(\overline{(x_{kn})}_{n\in\mathbb{N}}, \overline{(x_{jn})}_{n\in\mathbb{N}}) + \tfrac{1}{k} < \tfrac{1}{N} + \tfrac{\varepsilon}{3} + \tfrac{1}{N} \\ &\leq \tfrac{\varepsilon}{3} + \tfrac{\varepsilon}{3} + \tfrac{\varepsilon}{3} = \varepsilon, \end{aligned}$$

y así la sucesión $(x_{kN(k)})_{k\in\mathbb{N}}$ es d-Cauchy.

Con lo anterior, proponemos a $\overline{(x_{kN(k)})}_{k\in\mathbb{N}}$ como límite de la sucesión.

Para cada $\varepsilon > 0$ existe un natural N tal que $d(x_{kN(k)}, x_{nN(n)}) < \frac{\varepsilon}{2}$ si $k, n \geq N$. Entonces, si $k > \text{máx}\{N, \frac{2}{\varepsilon}\}$ y además consideramos un natural $n > \text{máx}\{N, N(k)\}$ entonces tenemos que

$$d(x_{kn}, x_{nN(n)}) \leq d(x_{kn}, x_{kN(k)}) + d(x_{kN(k)}, x_{nN(n)}) < \frac{1}{k} + \frac{\varepsilon}{2}.$$

Al hacer tender n a infinito obtenemos

$$\rho(\overline{(x_{kn})}_{n\in\mathbb{N}}, \overline{(x_{nN(n)})}_{n\in\mathbb{N}}) = \lim_{n\to\infty} d(x_{kn}, x_{nN(n)}) \leq \frac{1}{k} + \frac{\varepsilon}{2} < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Concluimos que $\overline{(x_{nN(n)})}_{n\in\mathbb{N}}$ es el límite de la sucesión $(\overline{(x_{kn})}_{n\in\mathbb{N}})_{k\in\mathbb{N}}$ y por lo tanto hemos demostrado el siguiente teorema.

Teorema 5. *El espacio métrico $(\overline{X}_d, \rho)$ es completo.*

Observación 6. *Al final de la prueba anterior, para demostrar que el límite de la sucesión $(\overline{(x_{kn})}_{n\in\mathbb{N}})_{k\in\mathbb{N}}$ es $\overline{(x_{nN(n)})}_{n\in\mathbb{N}}$, únicamente utilizamos el hecho de que la sucesión $(x_{nN(n)})_{n\in\mathbb{N}}$ es d-Cauchy, así como la forma en que elegimos a los naturales $N(k)$.*

En el caso en que nuestro espacio métrico original (X, d) ya fuera completo, cada sucesión d-Cauchy, que es convergente, está relacionada con la sucesión constante en la que cada término es su límite. De esta forma podemos identificar el espacio X con todo el espacio $\overline{X}_d$, por lo que obtenemos el espacio original.

1.2. Métricas equivalentes

Definición 1.2.1. *Decimos que dos métricas d_1 y d_2 en X son equivalentes si cada sucesión de elementos de X es d_1-Cauchy si y sólo si es d_2-Cauchy.*

Veamos que esta definición es más fuerte que pedir que dos métricas definan la misma convergencia, recordando que esto es equivalente a que definan la misma topología.

Ejemplo 7. *Una vez más consideremos el conjunto de reales positivos $\mathbb{R}^+$ y las métricas $d_1(x, y) = |x - y|$ y $d_2(x, y) = |x - y| + |\frac{1}{x} - \frac{1}{y}|$. Primero veamos que ambas métricas definen la misma convergencia.*

Como $d_1 \leq d_2$ tenemos que si una sucesión converge en $(\mathbb{R}^+, d_2)$ debe converger también en $(\mathbb{R}^+, d_1)$. Por otro lado consideremos una sucesión $(x_n)_{n\in\mathbb{N}}$ convergente a x en $(\mathbb{R}^+, d_1)$. Como la función $f : \mathbb{R}^+ \to \mathbb{R}^+$ definida

por $f(x) = \frac{1}{x}$ es una función continua con la métrica d_1, tenemos que la sucesión $(\frac{1}{x_n})_{n\in\mathbb{N}}$ converge a $\frac{1}{x}$ en $(\mathbb{R}^+, d_1)$.

Así, al considerar un número positivo ε, existen naturales N_1 y N_2 tales que $|x_n - x| < \frac{\varepsilon}{2}$, siempre que $n \geq N_1$, y $|\frac{1}{x_n} - \frac{1}{x}| < \frac{\varepsilon}{2}$, si $n \geq N_2$. De esta manera llamamos $N = \max\{N_1, N_2\}$ y tenemos que si $n \geq N$, entonces $d(x_n, x) < \varepsilon$.

Por lo tanto ambas métricas definan la misma convergencia. A continuación consideremos la sucesión $x_n = \frac{1}{n}$, esta sucesión es d_1-Cauchy. Sin embargo, no es d_2-Cauchy, pues para cualquier natural N tenemos que $d_2(x_N, x_{N+1}) > 1$.

La siguiente proposición muestra que si dos métricas cumplen nuestra definición de equivalencia, entonces ambas métricas definen la misma convergencia.

Proposición 8. *Si dos métricas en X, d_1 y d_2, son equivalentes, entonces una sucesión de elementos de X, $(x_n)_{n\in\mathbb{N}}$, converge a un elemento x de X con la métrica d_1 si y sólo si converge a x con la métrica d_2.*

Demostración. Supongamos que $(x_n)_{n\in\mathbb{N}}$ converge a x con la métrica d_1 y consideremos la sucesión $(y_n)_{n\in\mathbb{N}}$ definida por

$$y_n = \begin{cases} x_{\frac{n}{2}} & \text{si } n \text{ es par} \\ x & \text{si } n \text{ es impar.} \end{cases}$$

Esta sucesión también es convergente a x con la métrica d_1 y por tanto es d_1-Cauchy, lo cual, según nuestra hipótesis, implica que es una sucesión d_2-Cauchy.

Como la subsucesión $(y_{2n-1})_{n\in\mathbb{N}}$ es constante, entonces es convergente a x con la métrica d_2 y por tanto toda la sucesión $(y_n)_{n\in\mathbb{N}}$ converge a x con la métrica d_2 al igual que la subsucesión $(y_{2n})_{n\in\mathbb{N}}$. Pero esta subsucesión es la sucesión original, por lo que podemos concluir que la sucesión $(x_n)_{n\in\mathbb{N}}$ converge a x con la métrica d_2.

La otra implicación es análoga. □

Cabe señalar que cuando el espacio métrico es completo con una métrica, en consecuencia también lo es con cualquier métrica equivalente. Comprobar que dos métricas son equivalentes cuando con ambas se obtiene un espacio completo, se reduce a comprobar que la convergencia es igual con ambas métricas.

Veamos qué pasa al completar un espacio métrico con dos métricas equivalentes.

Teorema 9. *Si d_1 y d_2 son métricas equivalentes para X, entonces las completaciones $\overline{X}_{d_1}$ y $\overline{X}_{d_2}$ son homeomorfas, de manera que el homeomorfismo y los correspondientes encajes de X hacen conmutar el siguiente diagrama:*

$$\begin{array}{ccc} \overline{X}_{d_1} & \rightleftarrows & \overline{X}_{d_2} \\ \uparrow & \nearrow & \\ X & & \end{array}$$

De hecho $\overline{X}_{d_1} = \overline{X}_{d_2}$ y el homeomorfismo es la identidad.

Demostración. Consideremos un espacio X y dos métricas equivalentes en él, d_1 y d_2, lo primero que debemos probar es que los conjuntos $\overline{X}_{d_1}$ y $\overline{X}_{d_2}$ coinciden.

Por definición de métricas equivalentes los conjuntos de sucesiones d_1-Cauchy y sucesiones d_2-Cauchy coinciden, ahora únicamente hace falta probar que la relación de equivalencia inducida por ambas métricas en este conjunto es la misma. Para ello demostraremos el siguiente lema.

Lema 10. *Si $(x_n)_{n\in\mathbb{N}}$ y $(y_n)_{n\in\mathbb{N}}$ son sucesiones d_1-Cauchy tales que $\lim_{n\to\infty} d_1(x_n, y_n) = 0$, entonces $\lim_{n\to\infty} d_2(x_n, y_n) = 0$.*

Demostración. Considerando la sucesión $(z_n)_{n\in\mathbb{N}}$ dada por

$$z_n = \begin{cases} x_k & \text{si } n = 2k \\ y_k & \text{si } n = 2k-1. \end{cases}$$

Afirmamos que $(z_n)_{n\in\mathbb{N}}$ es una sucesión d_1-Cauchy.

Sea $N_1 \in \mathbb{N}$ tal que si $j, k \geq N_1$, entonces se tiene que $d_1(x_j, x_k) < \frac{\varepsilon}{2}$; sea N_2 un natural tal que si $j, k \geq N_2$, tenemos que $d_1(y_j, y_k) < \frac{\varepsilon}{2}$ y sea $N_3 \in \mathbb{N}$ tal que si $k \geq N_3$, se cumple que $d_1(x_k, y_k) < \frac{\varepsilon}{2}$.

Consideremos $N = \text{máx}\{2N_1, 2N_2, 2N_3\}$, sean $n, m \geq N$ y analizemos los 3 casos en que ambos, n y m, sean pares; ambos sean impares o que tengan distinta paridad.

$[n = 2j, m = 2k]$ En tal caso tenemos que $j, k \geq N_1$ y por tanto

$$d_1(z_n, z_m) = d_1(x_j, x_k) < \frac{\varepsilon}{2} < \varepsilon.$$

$[n = 2j-1, m = 2k-1]$ En este caso se tiene que $j, k > N_2$ lo que implica que

$$d_1(z_n, z_m) = d_1(y_j, y_k) < \frac{\varepsilon}{2}.$$

$[n = 2j-1, m = 2k]$ Tenemos que $j, k \geq N_2$ y que $k \geq N_3$ y así tenemos que

$$d_1(z_n, z_m) = d_1(y_j, x_k) \leq d_1(y_j, y_k) + d_1(y_k, x_k) < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Concluimos que la sucesión es d_1-Cauchy y por lo tanto es d_2-Cauchy, así que dado cualquier real positivo ε existe un natural N, tal que si $n, m \geq N$ se tiene que $d_2(z_n, z_m) < \varepsilon$, en particular para cualquier $k \geq N$, poniendo $n = 2k$ y $m = 2k - 1$ se cumple $n, m \geq N$ y esto implica que

$$d_2(x_k, y_k) = d_2(z_n, z_m) < \varepsilon,$$

lo cual demuestra el lema.

□

Por último, para ver que al completar el espacio con ambas métricas la identidad resulta un homeomorfismo, debemos mostrar que si una sucesión converge con una métrica entonces converge con la otra métrica.

Si llamamos ρ_1 a la métrica inducida por d_1 y ρ_2 a la métrica inducida por d_2, y consideramos una sucesión ρ_1-convergente, $(\overline{(x_{kn})}_{n\in\mathbb{N}})_{k\in\mathbb{N}}$, entonces podemos construir una sucesión creciente de naturales $N(k)$, tales que si $n, m \geq N(k)$, se dará lugar a que se cumpla simultáneamente que $d_1(x_{kn}, x_{km}) \leq \frac{1}{k}$ y $d_2(x_{kn}, x_{km}) \leq \frac{1}{k}$.

Lo anterior es posible porque para cada natural k, la sucesión $(x_{kn})_{n\in\mathbb{N}}$ es tanto d_1-Cauchy como d_2-Cauchy, entonces podemos construir dos sucesiones $N_1(k)$ y $N_2(k)$ como en la demostración del teorema 5, una para que se cumple la primera desigualdad y otra para que se cumple la segunda desigualdad. La sucesión $N(k) = N_1(k) + N_2(k)$ cumple las propiedades deseadas.

Por ser $(\overline{(x_{kn})}_{n\in\mathbb{N}})_{k\in\mathbb{N}}$ ρ_1-convergente, sabemos que es ρ_1-Cauchy, eso nos garantiza, por lo hecho en la sección anterior, que la sucesión $(x_{kN(k)})_{n\in\mathbb{N}}$ es d_1-Cauchy y que $\overline{(x_{kN(k)})}_{n\in\mathbb{N}}$ es el límite de $(\overline{(x_{kn})}_{n\in\mathbb{N}})_{k\in\mathbb{N}}$ con la métrica ρ_1.

Pero la sucesión $(x_{kN(k)})_{n\in\mathbb{N}}$ también es d_2-Cauchy y esto junto con la forma en la que elegimos a los naturales $N(k)$, basta para asegurar que la sucesión $(\overline{(x_{kn})}_{n\in\mathbb{N}})_{k\in\mathbb{N}}$ converge a $\overline{(x_{kN(k)})}_{n\in\mathbb{N}}$ con la métrica ρ_2, como se señaló en la observación 6. Con esto queda demostrado que ambas métricas son equivalentes. □

Capítulo 2

Los números p-ádicos

2.1. La norma p-ádica

Definición 2.1.1. *Una norma en un campo F es una función $\|\cdot\|: F \to [0,\infty)$ tal que para todo x, y en F cumple lo siguiente:*

1. $\|x\| = 0 \Leftrightarrow x = 0$,
2. $\|x \cdot y\| = \|x\| \cdot \|y\|$,
3. $\|x + y\| \leq \|x\| + \|y\|$.

Algunas de propiedades básicas de una norma sobre un campo están dadas en la siguiente proposición.

Proposición 11. *Si 1 es el neutro multiplicativo del campo F, -1 su inverso aditivo, x un elemento cualquiera del campo, y $\|\cdot\|$ es una norma sobre F, entonces*

1. $\|x^n\| = \|x\|^n$,
2. $\|1\| = 1$,
3. $\|-1\| = 1$,
4. $\|\frac{1}{x}\| = \frac{1}{\|x\|}$, *si* $x \neq 0$.

Demostración.

(1) La demostración es por inducción, para $n = 2$ es la propiedad 2 de la definición de norma cuando $x = y$. Ahora suponiendo que $\|x^n\| = \|x\|^n$, tenemos que $\|x^{n+1}\| = \|x^n \cdot x\| = \|x\|^n\|x\| = \|x\|^{n+1}$.

(2) $\|1\| = \|1 \cdot 1\| = \|1\|\|1\|$ y como $1 \neq 0$ tenemos que $\|1\| = 1$.

(3) $1 = \|1\| = \|(-1)^2\| = \|-1\|^2$, entonces como $\|-1\| \geq 0$ se tiene que $\|-1\| = 1$.

(4) $1 = \|1\| = \|x \cdot \frac{1}{x}\| = \|x\|\|\frac{1}{x}\|$ y despejando obtenemos que $\|\frac{1}{x}\| = \frac{1}{\|x\|}$. □

Si definimos $d(x, y) = \|x - y\|$, entonces d es una métrica sobre el campo. Así, una norma es el tipo de métrica sobre un campo que se acopla bien con las operaciones del campo. Además, diremos que dos normas son equivalentes cuando las métricas que inducen son equivalentes.

Ejemplo 12. *La norma trivial se define como*

$$\|x\| = \begin{cases} 0 & si\ x = 0 \\ 1 & si\ x \neq 0 \end{cases}$$

e induce la métrica discreta en F.

Ejemplo 13. *El valor absoluto usual define una norma en $\mathbb{R}$ o en $\mathbb{Q}$.*

La compatibilidad que proporciona una norma entre la estructura de campo y la métrica que induce en el campo, se muestra en la siguiente proposición.

Proposición 14. *En un campo con la métrica inducida por una norma, la suma, resta e inversión aditiva son continuas y la inversión multiplicativa es continua en el subconjunto de los elementos distintos de* 0.

Demostración. Demostraremos únicamente que la multiplicación es continua para hacer notar que la demostración es idéntica a la que se haría en el caso para la continuidad de la multiplicación en $\mathbb{R}$ al igual que para las demás operaciones.

Sean x y y elementos de F y sea ε un número positivo. Consideremos un natural fijo N tal que $\|x\| < N$ y $\|y\| < N$, entonces si x_1 y y_1 son elementos de F tales que $\|x - x_1\| < \text{mín}\{\frac{\varepsilon}{2N}, 1\}$ y $\|y - y_1\| < \frac{\varepsilon}{2(N+1)}$, observando que $\|x_1\| = \|x_1 - x + x\| \leq \|x_1 - x\| + \|x\| < 1 + N$, tenemos que

$$\begin{aligned} \|x \cdot y - x_1 \cdot y_1\| &= \|x \cdot y - x_1 \cdot y + x_1 \cdot y - x_1 \cdot y_1\| \\ &\leq \|(x - x_1)\|\|y\| + \|x_1\|\|(y - y_1)\| \\ &< \frac{\varepsilon}{2N} \cdot N + (N + 1) \cdot \frac{\varepsilon}{2(N+1)} = \varepsilon. \end{aligned}$$

□

Ahora definiremos una familia de normas en $\mathbb{Q}$.

Sea p un número primo y sea a un entero distinto de cero. Ahora definimos al ordinal p-ádico de a, denotado por $ord_p a$ como el entero no negativo m tal que $p^m \mid a$ y $p^{m+1} \nmid a$. Otra forma de interpretar $ord_p a$ es el número de veces que aparece el primo p en la factorización en primos de a.

Nótese la siguiente propiedad tipo logaritmo de ord_p:

$$ord_p ab = ord_p a + ord_p b.$$

Si se tiene el caso de que $x = \frac{a}{b}$ es un racional distinto de 0, entonces podemos definir el ordinal p-ádico de x como $ord_p x = ord_p a - ord_p b$, y si $x = \frac{c}{d}$ es otra expresión de x, se tendrá que $ad = bc$ y por lo tanto $ord_p a + ord_p d = ord_p b + ord_p c$. Así $ord_p a - ord_p b = ord_p c - ord_p d$, por lo que $ord_p x$ queda bien definido.

Ahora ya podemos definir la norma p-ádica en $\mathbb{Q}$ como sigue.

Definición 2.1.2. *Definimos la norma p-ádica como la función* $|\cdot|_p \colon \mathbb{Q} \to [0, \infty)$ *dada por*

$$|x|_p = \begin{cases} \frac{1}{p^{ord_p x}} & si\ x \neq 0 \\ 0 & si\ x = 0 \end{cases}$$

Ejemplo 15.

1. $\frac{50}{15} = \frac{2 \cdot 5^2}{3 \cdot 5}$, $ord_5 \frac{50}{15} = ord_5(2 \cdot 5^2) - ord_5(3 \cdot 5) = 2 - 1 = 1$, $|\frac{50}{15}|_5 = 5^{-1}$.
2. *Para cualquier primo p y entero n, $ord_p(p^n) = n$, $|p^n|_p = p^{-n}$.*
3. *Para cualquier primo p si a y b son enteros primos relativos de p, entonces $ord_p(\frac{a}{b}) = 0$ y $|\frac{a}{b}|_p = 1$.*
4. *Sean a y b son enteros tales que $|a - b|_p \leq p^{-n}$ para algún natural n, entonces, $p^n | a - b$.*

   Es decir, que existe algún entero c, tal que $a - b = c \cdot p^n$. Lo anterior nos dice que dos enteros son "cercanos" según la norma p-ádica cuando su diferencia es un múltiplo de una potencia "grande" de p.

Demostraremos ahora que $|\cdot|_p$ efectivamente es una norma.

Proposición 16. $|\cdot|_p$ *es una norma sobre* $\mathbb{Q}$.

Demostración.
(1) Es claro por la definición.

(2) Hay que observar que la propiedad tipo logaritmo de ord_p también es válida en $\mathbb{Q}$

$$\begin{aligned} ord_p(\tfrac{a}{b} \cdot \tfrac{c}{d}) &= ord_p(ac) - ord_p(bd) = ord_p a - ord_p b + ord_p c - ord_p d \\ &= ord_p \tfrac{a}{b} + ord_p \tfrac{c}{d} \end{aligned}$$

de donde podemos obtener que

$$|x \cdot y|_p = p^{-ord_p x \cdot y} = p^{-ord_p x - ord_p y} = p^{-ord_p x} p^{-ord_p y} = |x|_p |y|_p.$$

(3) En el caso en que $x = 0$, $y = 0$ ó $x + y = 0$ la desigualdad del triángulo se cumple de forma trivial, así que supondremos que los tres son distintos de cero, digamos que $x = \frac{a}{b}$, $y = \frac{c}{d}$ y $x + y = \frac{ad+bc}{bd}$. De forma que $ord_p(x + y) = ord_p(ad + bc) - ord_p b - ord_p d$. Notemos que $ord_p(ad + bc) \geq$ mín$\{ord_p ad, ord_p bc\}$ y por lo tanto

$$\begin{aligned} ord_p(x+y) &\geq \text{mín}\{ord_p a + ord_p d, ord_p b + ord_p c\} - ord_p b - ord_p d \\ &= \text{mín}\{ord_p a - ord_p b, ord_p c - ord_p d\} \\ &= \text{mín}\{ord_p x, ord_p y\}. \end{aligned}$$

La desigualdad anterior implica

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

□

En la demostración anterior podemos observar que esta norma cumple una propiedad mucho más fuerte que la desigualdad del triángulo.

A una norma $\|\cdot\|$ que cumple $\|x + y\| \leq \text{máx}\{\|x\|, \|y\|\}$ la llamaremos norma no arquimediana, pues esta propiedad es equivalente a que el conjunto $\{n \cdot 1 : n \in \mathbb{N}\}$ sea acotado, es decir, que el conjunto $\{\|n \cdot 1\| : n \in \mathbb{N}\}$ sea un subconjunto acotado superiormente de $\mathbb{R}$, donde entendemos que $n \cdot 1$ es el neutro multiplicativo del campo sumado consigo mismo n veces.

Proposición 17. *Sea $\|\cdot\|$ una norma en un campo F. Entonces, $\|\cdot\|$ es no arquimediana si y sólo si existe un número positivo M, tal que $\|n \cdot 1\| \leq M$ para todo natural n.*

Demostración. Primero veamos que en un campo con una norma no arquimedeana para cualquier natural n sucede que $\|n \cdot 1\| \leq 1$, esto lo demostraremos por inducción. Cuando no haya ambigüedad en lugar de $n \cdot 1$ escribiremos simplemente n.

Para $n = 1$ ya demostramos que $\|1\| = 1$.

Ahora supongamos que $\|n\| \leq 1$, entonces $\|n+1\| \leq \text{máx}\{\|n\|, \|1\|\} = 1$.

Por lo tanto se cumple la propiedad para cualquier natural, es decir, que el conjunto $\{n \cdot 1 : n \in \mathbb{N}\}$ está acotado.

Ahora supongamos que el conjunto $\{n \cdot 1 : n \in \mathbb{N}\}$ está acotado y demostremos que la norma $\|\cdot\|$ debe ser no arquimediana.

Si $\|n\| > 1$ para alguna n, la sucesión $\|n^k\| = \|n\|^k$ tiende a infinito cuando k tiende a infinito, lo cual contradice la hipótesis. Por lo tanto $\|n\| \leq 1$ para toda n.

Sean x, y elementos del campo, N un natural y observemos que

$$\begin{aligned}\|x+y\|^N &= \|(x+y)^N\| = \|\sum_{k=0}^{N}\tbinom{N}{k}x^{N-k}y^k\| \leq \sum_{k=0}^{N}\|\tbinom{N}{k}\|\|x\|^{N-k}\|y\|^k \\ &\leq \sum_{k=0}^{N}\|x\|^{N-k}\|y\|^k \leq \sum_{k=0}^{N}(\text{máx}\{\|x\|,\|y\|\})^N \\ &= (N+1)(\text{máx}\{\|x\|,\|y\|\})^N.\end{aligned}$$

Si sacamos raíz N-ésima obtenemos $\|x+y\| \leq \sqrt[N]{N+1}(\text{máx}\{\|x\|,\|y\|\})$, y al tomar el límite cuando N tiende a infinito nos da la desigualdad buscada: $\|x+y\| \leq \text{máx}\{\|x\|,\|y\|\}$. Así queda demostrada la equivalencia que justifica el nombre que le hemos dado a este tipo de normas. □

Volviendo a los racionales, para todo primo p el espacio métrico $(\mathbb{Q}, |\cdot|_p)$ resulta no ser completo, la demostración la dejaremos para la siguiente sección por simplicidad y para no repetir esfuerzos. Así como al completar a los racionales con el valor absoluto usual obtenemos los números reales, $\mathbb{R}$, al completar a los racionales con las normas p-ádicas obtendremos distintos espacios a los que llamaremos números p-ádicos y denotaremos por $\mathbb{Q}_p$.

El siguiente teorema nos asegura que no hay más formas de completar a los racionales con una norma.

Teorema 18 (Ostrowski)**.** *Toda norma $\|\cdot\|$ no trivial sobre $\mathbb{Q}$ es equivalente al valor absoluto usual $|\cdot|$ o a la norma p-ádica $|\cdot|_p$ para algún primo p.*

Demostración. Caso 1. Si existe un entero positivo n tal que $\|n\| > 1$.

Sea $n_0 = \text{mín}\{n \in \mathbb{Z}^+ : \|n\| > 1\}$, como $\|1\| = 1$ entonces $n_0 > 1$ y por lo tanto existe un real positivo α tal que $\|n_0\| = n_0^\alpha$.

Consideremos cualquier entero positivo n y expresémoslo en base n_0

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

donde cada a_i es un entero tal que $0 \leq a_i < n_0$ y $a_s \neq 0$.

Como $0 \leq a_i < n_0$ entonces $\|a_i\| \leq 1$ para toda i, además teniendo en cuenta que $n_0^s \leq n$, podemos acotar la norma de n de la siguiente forma:

$$\begin{aligned}\|n\| &\leq \|a_0\| + \|a_1 n_0\| + \|a_2 n_0^2\| + \cdots + \|a_s n_0^s\| \\ &= \|a_0\| + \|a_1\|n_0^\alpha + \|a_2\|n_0^{2\alpha} + \cdots + \|a_s\|n_0^{s\alpha} \\ &\leq 1 + n_0^\alpha + n_0^{2\alpha} + \cdots + n_0^{s\alpha} \\ &= n_0^{s\alpha}(1 + n_0^{-\alpha} + n_0^{-2\alpha} + \cdots + n_0^{-s\alpha}) \\ &\leq n^\alpha[\sum_{i=0}^{\infty}(\tfrac{1}{n_0^\alpha})^i].\end{aligned}$$

Observemos que la serie de reales es convergente pues $0 < \frac{1}{n_0^\alpha} = \frac{1}{\|n_0\|} < 1$.

De forma que $\|n\| \leq Cn^{\alpha}$ para todo entero positivo n, donde la constante positiva $C = \sum_{i=0}^{\infty} (\frac{1}{n_0^{\alpha}})^i$ no depende de n.

Considerando números naturales de la forma n^N obtenemos

$$\|n\|^N \leq Cn^{N\alpha},$$

tomando raíz N-ésima

$$\|n\| \leq C^{\frac{1}{N}} n^{\alpha}$$

y por último si tomamos el límite cuando $N \to \infty$ obtenemos que

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

para todo entero positivo n.

Por otro lado considerando que $\|n_0^{s+1}\| = \|n + n_0^{s+1} - n\| \leq \|n\| + \|n_0^{s+1} - n\|$ y que $n_0^{s+1} > n \geq n_0^s$ podemos obtener la otra desigualdad de la siguiente forma:

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

donde la constante $C' = 1 - (1 - \frac{1}{n_0})^{\alpha}$ es positiva.

Procediendo de igual modo obtenemos que $\|n\| \geq n^{\alpha}$ y por lo tanto que $\|n\| = n^{\alpha}$, para todo entero positivo n.

De las propiedades de norma se sigue que $\|-n\| = \|n\|$ y que $\|\frac{n}{m}\| = \frac{\|n\|}{\|m\|}$, y utilizando ambas propiedades podemos llegar a que $\|x\| = |x|^{\alpha}$, para todo racional x.

Por último, es claro que una sucesión será $|\cdot|$-Cauchy si y sólo si es $\|\cdot\|$-Cauchy, por ser $\alpha > 0$, lo que concluye la demostración en este caso.

Caso 2. Si $\|n\| \leq 1$ para todo entero positivo n.

Si para todo n entero positivo sucede que $\|n\| = 1$, entonces utilizando las propiedades de norma al igual que al final de la demostración del primer caso, obtenemos que $\|x\| = 1$, para todo racional $x \neq 0$ y por lo tanto la norma sería trivial, una contradicción.

Así pues sea $n_0 = \text{mín}\{n \in \mathbb{Z}^+ : \|n\| < 1\}$, supongamos que $n_0 = n_1 n_2$ con $1 < n_1, n_2 < n_0$, en tal caso tendríamos que $\|n_1\| = \|n_2\| = 1$ y por tanto que $\|n_0\| = \|n_1\|\|n_2\| = 1$ lo cual es una contradicción. Por lo tanto n_0 es un número primo, al cual llamaremos p.

Consideremos un primo $q \neq p$ y supongamos que $\|q\| < 1$, entonces existe un natural N tal que $\|q^N\| = \|q\|^N < \frac{1}{2}$, también existe un natural

M tal que $\|p^M\| < \frac{1}{2}$. Pero además p^M y q^N son primos relativos y por lo tanto existen enteros m y n tales que $1 = mp^M + nq^N$ lo cual implica que

$$\begin{aligned} 1 &= \|mp^M + nq^N\| \leq \|mp^M\| + \|nq^N\| \\ &= \|m\|\|p^M\| + \|n\|\|q^N\| \leq \|p^M\| + \|q^N\| \\ &< \tfrac{1}{2} + \tfrac{1}{2} = 1, \end{aligned}$$

y esto es una contradicción. De aquí concluimos que $\|q\| = 1$ para todo primo $q \neq p$.

Ahora para calcular la norma de cualquier entero positivo a, lo factorizamos en primos

$$a = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$$

y utilizando las propiedades de norma y la definición de $ord_p a$ obtenemos que

$$\|a\| = \|p_1\|^{b_1} \|p_2\|^{b_2} \cdots \|p_r\|^{b_r} = \|p\|^{ord_p a},$$

ya que todos los demás factores son 1.

Como $\|p\| < 1$, existe un real positivo α tal que $(\frac{1}{p})^\alpha = \|p\|$ y por lo tanto $\|a\| = |a|_p^\alpha$ para todo entero positivo. Al igual que en el caso 1 esto implica que la igualdad es válida para todos los racionales y que por lo tanto esta norma es equivalente a la norma p-ádica, $|\cdot|_p$.

□

Como trabajaremos con normas no arquimedianas nos detendremos un momento a estudiar algunas propiedades de ellas.

Propiedad de los triángulos isósceles

Sean x y y elementos de un campo F con una norma no arquimediana $\|\cdot\|$. Sabemos que $\|x+y\| \leq \text{máx}\{\|x\|, \|y\|\}$. Ahora supongamos que $\|x\| < \|y\|$, entonces tenemos que $\|x + y\| \leq \|y\|$. Por otro lado tenemos que $\|y\| = \|(x+y) - x\| \leq \text{máx}\{\|x+y\|, \|x\|\}$, pero sabemos que $\|y\| \not\leq \|x\|$, por lo que se debe cumplir que $\|y\| \leq \|x + y\|$ y por lo tanto $\|x + y\| = \|y\|$.

Entonces podemos concluir que $\|x+y\| \leq \text{máx}\{\|x\|, \|y\|\}$ y se cumple la igualdad cuando $\|x\| \neq \|y\|$, esto lo podemos expresar diciendo que **todos los triángulos son isósceles**.

Centro de un disco

Sea $a \in F$, $r > 0$ y denotemos el disco con centro en a y radio r como $D_r(a) = \{x \in F : \|x - a\| < r\}$. Sea $b \in D_r(a)$, si $x \in D_r(a)$ entonces $\|x - a\| < r$. Además

$$\|x - b\| = \|(x - a) + (a - b)\| \leq \text{máx}\{\|x - a\|, \|a - b\|\} < r$$

y por lo tanto $x \in D_r(b)$. Esto quiere decir que $D_r(a) \subseteq D_r(b)$, la otra contención es análoga, por lo tanto $D_r(a) = D_r(b)$, lo cual quiere decir que **cualquier punto en el disco puede tomarse como centro del mismo**.

Caracterización de sucesciones de Cauchy

Otra propiedad importante es una que caracteriza cuándo una sucesión es de Cauchy. Sabemos que en general no es suficiente que la distancia entre términos consecutivos tienda a cero para que una sucesión sea de Cauchy, pero en el caso de una norma no arquimediana sí lo es.

En efecto, sea $(x_n)_{n\in\mathbb{N}}$ una sucesión de elementos de F tal que $\|x_n - x_{n+1}\| \to 0$ cuando $n \to \infty$. Entonces, para todo $\varepsilon > 0$, existe un natural N tal que $\|x_n - \ x_{n+1}\| < \ \varepsilon$, siempre que $n \geq N$. Sean $j, k \geq N$ y supongamos que $j < k$, entonces tenemos que

$$\begin{aligned} \|x_j - x_k\| &= \|(x_j - x_{j+1}) + (x_{j+1} - x_{j+2}) + \cdots + (x_{k-1} - x_k)\| \\ &\leq \text{máx}\{\|x_j - x_{j+1}\|, \|x_{j+1} - x_{j+2}\|, \ldots, \|x_{k-1} - x_k\|\} \\ &< \varepsilon, \end{aligned}$$

y por lo tanto la sucesión es de Cauchy.

Convergencia de series

Una serie $\sum_{n=1}^{\infty} a_n$ es una suma infinita, formalmente una pareja ordenada $((a_n)_{n\in\mathbb{N}}, (s_n)_{n\in\mathbb{N}})$ de sucesiones en F tales que $s_n = \sum_{i=1}^{n} a_i$, a $(a_n)_{n\in\mathbb{N}}$ le llamamos el término general de la serie y a $(s_n)_{n\in\mathbb{N}}$ la sucesión de sumas parciales. Decimos que la serie es convergente si la sucesión de sumas parciales es convergente, y al límite le llamamos el valor de la serie.

En general no basta que el término general de una serie tienda a cero para que la serie converja, por ejemplo la serie $\sum_{n=1}^{\infty} \frac{1}{n}$ no converge en $\mathbb{R}$.

Con la caracterización de sucesiones de Cauchy podemos asegurar que en un campo completo con una norma no arquimediana una serie converge si y sólo si el término general tiende a cero. Lo anterior sucede ya que la diferencia entre términos consecutivos de la sucesión de sumas parciales es precisamente el término general de la serie, es decir que la sucesión de sumas parciales es una sucesión de Cauchy si y sólo si el término general de la serie tiende a cero.

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

Como dijimos en la sección anterior, llamaremos números p-ádicos a los elementos del espacio métrico que obtenemos al completar $\mathbb{Q}$ con la norma

p-ádica, y que queda denotado por $\mathbb{Q}_p$. Si $x \in \mathbb{Q}$ y no hay lugar a confusión, entonces denotaremos a la clase de equivalencia de la sucesión constante $(x)_{n\in\mathbb{N}}$ simplemente como x, pero ahora considerado como un elemento de $\mathbb{Q}_p$.

Veamos cómo se extiende la norma p-ádica a $\mathbb{Q}_p$. Consideremos un elemento $a = \overline{(a_n)}_{n\in\mathbb{N}} \in \mathbb{Q}_p$, observando la sucesión de normas tenemos dos casos:

i) Si $(a_n)_{n\in\mathbb{N}} \sim (0)_{n\in\mathbb{N}}$, por definición de la relación de equivalencia tenemos que $|a_n - 0|_p \to 0$ cuando $n \to \infty$.

ii) Si $(a_n)_{n\in\mathbb{N}} \nsim (0)_{n\in\mathbb{N}}$, significa que $|a_n|_p$ no converge a 0, es decir, que existe un real positivo ε_0 tal que dado cualquier natural N existe otro natural $k \geq N$ tal que $|a_k|_p \geq \varepsilon_0$. Por otro lado como la sucesión es de Cauchy, existe un natural N tal que para cualesquiera dos naturales $n, m \geq N$ se tiene que $|a_n - a_m|_p < \varepsilon_0$.

Fijemos un natural $k \geq N$ tal que $|a_k|_p \geq \varepsilon_0$. Considerando cualquier natural $n \geq N$ observemos que

$$|a_n|_p = |(a_n - a_k) + a_k|_p \leq \text{máx}\{|a_n - a_k|_p, |a_k|_p\},$$

como $|a_n - a_k|_p < \varepsilon_0$ y $|a_k|_p \geq \varepsilon_0$ es claro que $|a_n - a_k|_p \neq |a_k|_p$, y por la propiedad de que todos los triángulos son isósceles podemos concluir que $|a_n|_p$ tiene el valor constante $|a_k|_p$ para todo $n \geq N$.

En cualquier caso tenemos que la sucesión de normas es convergente y definiremos la norma p-ádica de a como $|a|_p = \lim\limits_{n\to\infty} |a_n|_p$. La norma está bien definida pues si consideramos otro representante $(a'_n)_{n\in\mathbb{N}}$ tendríamos que

$$|a'_n|_p = |(a'_n - a_n) + a_n|_p \leq \text{máx}\{|a'_n - a_n|_p, |a_n|_p\},$$

y al tomar el límite cuando n tiende a infinito, como $|a'_n - a_n| \to 0$, obtenemos que $\lim\limits_{n\to\infty} |a'_n|_p \leq \lim\limits_{n\to\infty} |a_n|_p$. Siendo la otra desigualdad análoga, concluimos que ambos límites son iguales.

Todo lo anterior ya estaba garantizado según lo estudiado en el capítulo anterior referente a completar espacios métricos, pues $|a|_p$ es simplemente la distancia entre los elementos a y 0 de $\mathbb{Q}_p$, pero la demostración en este caso concreto nos indica que en $\mathbb{Q}_p$ los posibles valores para la distancia entre dos puntos son los mismos que ya había en $\mathbb{Q}$ con la norma p-ádica, es decir $\{p^n | n \in \mathbb{Z}\} \cup \{0\}$.

Un caso muy distinto a lo que pasaba al completar $\mathbb{Q}$ con el valor absoluto y obtener $\mathbb{R}$ donde pasábamos de todos los racionales no negativos, una cantidad numerable, a todos los reales no negativos, una cantidad no numerable.

Ahora extenderemos la estructura de campo de $\mathbb{Q}$ a $\mathbb{Q}_p$. Si $a = \overline{(a_n)}_{n\in\mathbb{N}}$ y $b = \overline{(b_n)}_{n\in\mathbb{N}}$ son elementos de $\mathbb{Q}_p$ definimos la suma y la multiplicación de la siguiente manera:

$$\overline{(a_n)}_{n\in\mathbb{N}} + \overline{(b_n)}_{n\in\mathbb{N}} = \overline{(a_n + b_n)}_{n\in\mathbb{N}},$$

$$\overline{(a_n)}_{n\in\mathbb{N}} \cdot \overline{(b_n)}_{n\in\mathbb{N}} = \overline{(a_n \cdot b_n)}_{n\in\mathbb{N}}.$$

Hay que verificar que estén bien definidas las operaciones. Consideremos otros dos representantes $(a'_n)_{n\in\mathbb{N}} \sim (a_n)_{n\in\mathbb{N}}$ y $(b'_n)_{n\in\mathbb{N}} \sim (b_n)_{n\in\mathbb{N}}$, entonces

$$|(a_n+b_n)-(a'_n+b'_n)|_p = |(a_n-a'_n)+(b_n-b'_n)|_p \leq \text{máx}\{|a_n-a'_n|_p, |b_n-b'_n|_p\}$$

y como ambas expresiones tienden a cero, obtenemos que

$$\lim_{n\to\infty} |(a_n + b_n) - (a'_n + b'_n)|_p = 0,$$

por otro lado

$$\begin{aligned} |a_n \cdot b_n - a'_n \cdot b'_n|_p &= |a_n \cdot b_n - a_n \cdot b'_n + a_n \cdot b'_n - a'_n \cdot b'_n|_p \\ &= |a_n(b_n - b'_n) + b'_n(a_n - a'_n)|_p \\ &\leq \text{máx}\{|a_n|_p|b_n - b'_n|_p, |b'_n|_p|a_n - a'_n|_p\}, \end{aligned}$$

estas expresiones tienden a $|a|_p \lim_{n\to\infty} |b_n - b'_n|_p$ y $|b|_p \lim_{n\to\infty} |a_n - a'_n|_p$ y ambos son 0, por lo que $\lim_{n\to\infty} |a_n \cdot b_n - a'_n \cdot b'_n|_p = 0$.

Si $a'_n = a_{n+1}$ y $b'_n = b_{n+1}$, lo anterior nos dice que $(a_n + b_n)_{n\in\mathbb{N}}$ y $(a_n \cdot b_n)_{n\in\mathbb{N}}$ son sucesiones $|\cdot|_p$-Cauchy y que no importa qué representantes escojamos en la definición de las operaciones.

De la misma manera podemos definir $-a$ como la clase de equivalencia de $(-a_n)_{n\in\mathbb{N}}$, y si $a \neq 0$, teniendo en cuenta que a lo más una cantidad finita de términos pueden ser 0, podemos definir a^{-1} como la clase de equivalencia de la siguiente sucesión:

$$x_n = \begin{cases} a_n^{-1} & \text{si } a_n \neq 0 \\ 0 & \text{si } a_n = 0. \end{cases}$$

Para ver que a^{-1} está bien definido consideremos dos representantes de a, $(a_n)_{n\in\mathbb{N}}$ y $(a'_n)_{n\in\mathbb{N}}$, y dos términos a_n y a'_n distintos de cero y observemos que

$$|\frac{1}{a_n} - \frac{1}{a'_n}|_p = |\frac{a'_n - a_n}{a_n a'_n}|_p = \frac{|a'_n - a_n|_p}{|a_n a'_n|_p}.$$

Como a partir algún término todos los demás términos son distintos de cero tenemos que

$$\lim_{n\to\infty} |\frac{1}{a_n} - \frac{1}{a'_n}|_p = \frac{1}{|a|_p^2} \lim_{n\to\infty} |a'_n - a_n|_p = 0.$$

Ahora, como las operaciones se definieron término a término es fácil verificar que $\mathbb{Q}_p$ con estas operaciones forma un campo.

Veamos que la norma p-ádica efectivamente es una norma sobre el campo $\mathbb{Q}_p$:

1. Por la definición de la relación de equivalencia $\lim_{n\to\infty} |a_n|_p = |a|_p = 0$ si y sólo si $a = 0$.
2. $|ab|_p = \lim_{n\to\infty} |a_n b_n|_p = \lim_{n\to\infty} |a_n|_p |b_n|_p = \lim_{n\to\infty} |a_n|_p \lim_{n\to\infty} |b_n|_p = |a|_p |b|_p$
3. $|a+b|_p = \lim_{n\to\infty} |a_n+b_n|_p \leq \text{máx}\{\lim_{n\to\infty} |a_n|_p, \lim_{n\to\infty} |b_n|_p\} = \text{máx}\{|a|_p, |b|_p\}$

Toda la discusión anterior queda resumida en el siguiente teorema.

Teorema 19. $(\mathbb{Q}_p, |\cdot|_p)$ *es un campo con una norma no arquimediana completa.*

Ahora buscamos una representación para los números p-ádicos, mucho más util para trabajar con ellos sin tener que hacer referencia a clases de equivalencia de sucesiones de Cauchy, que tiene cierta similitud con la expansión decimal de los números reales.

Para ello necesitaremos el siguiente lema.

Lema 20. *Dado $x \in \mathbb{Q}$ tal que $|x|_p \leq 1$, para cada $i \in \mathbb{Z}^+$ existe un entero α tal que $|\alpha - x|_p \leq p^{-i}$. Aún más, podemos tomar al entero en el conjunto $\{0, 1, 2, \ldots, p^i - 1\}$.*

Demostración. Expresando $x = \frac{a}{b}$ donde a y b son primos relativos, buscamos aproximar a x con algún entero. Al ser a y b primos relativos y $|x|_p \leq 1$ tenemos que $p \nmid b$ y por lo tanto p^i y b son primos relativos, así que existen enteros m y n tales que $mb + np^i = 1$.

Según lo anterior mb es cercano a 1, lo que quiere decir que m es cercano a $\frac{1}{b}$ y por lo tanto am debería ser cercano a $x = \frac{a}{b}$, así que proponemos $\alpha = am$ y tenemos que

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

Ahora podemos sumar múltiplos de p^i hasta estar en el intervalo deseado, es decir, sea $\alpha' = \alpha + rp^i$ tal que $\alpha' \in \{0, 1, 2, \ldots, p^i - 1\}$ y en tal caso

$$|\alpha' - x|_p = |\alpha - x + rp^i|_p \leq \text{máx}\{|\alpha - x|_p, |rp^i|_p\} \leq p^{-i}.$$

□

Con el siguiente teorema lograremos dar la representación deseada a los números p-ádicos.

Teorema 21. *Sea $a \in \mathbb{Q}_p$ tal que $|a|_p \leq 1$, entonces a tiene un único representante, $(a_n)_{n\in\mathbb{N}}$, que cumple las siguientes propiedades:*

1. *$a_n \in \mathbb{Z}$ para todo natural n,*
2. *$0 \leq a_n < p^n$ para todo natural n,*
3. *$a_n \equiv a_{n+1}$ $(mod\ p^n)$ para todo natural n.*

Demostración. Sea $(b_n)_{n\in\mathbb{N}} \in a$ cualquier representante y para cada $n \in \mathbb{N}$ elegimos $N(n)$ tal que $|b_k - b_l|_p \leq \frac{1}{p^n}$ siempre que $k, l \geq N(n)$. Además elegimos las $N(n)$ de modo que formen una sucesión creciente.

Sean $k, l \geq N(1)$, entonces tenemos que

$$|b_k|_p \leq \text{máx}\{|b_l|_p, |b_k - b_l|_p\} \leq \text{máx}\{|b_l|_p, \frac{1}{p}\},$$

tomando el límite cuando $l \to \infty$

$$|b_k|_p \leq \text{máx}\{|a|_p, \frac{1}{p}\} \leq 1.$$

Utilizando el lema anterior podemos encontrar una sucesión de enteros $(a_n)_{n\in\mathbb{N}}$, tal que $0 \leq a_n < p^n$ y que además cumple que $|a_n - b_{N(n)}|_p \leq \frac{1}{p^n}$.

Afirmamos que esta sucesión es la buscada. Por la manera en que la elegimos cumple con las propiedades *1* y *2*. Por otro lado tenemos que

$$\begin{aligned} |a_{n+1} - a_n|_p &= |a_{n+1} - b_{N(n+1)} + b_{N(n+1)} - b_{N(n)} + b_{N(n)} - a_n|_p \\ &\leq \text{máx}\{|a_{n+1} - b_{N(n+1)}|_p, |b_{N(n+1)} - b_{N(n)}|_p, |b_{N(n)} - a_n|_p\} \\ &\leq \text{máx}\{\tfrac{1}{p^{n+1}}, \tfrac{1}{p^n}, \tfrac{1}{p^n}\} = \tfrac{1}{p^n}, \end{aligned}$$

y ya que $a_{n+1} - a_n$ es un entero, entonces se tiene que $p^n \mid (a_{n+1} - a_n)$, es decir, que $a_{n+1} \equiv a_n$ $(mod\ p^n)$. Por lo tanto, la sucesión cumple las tres propiedades.

Observemos que de la propiedad *3*, tenemos que $a_{n+1} \equiv a_{n+2}$ $(mod\ p^{n+1})$, entonces $a_{n+1} \equiv a_{n+2}$ $(mod\ p^n)$, y por la transitividad de las congruencias $a_n \equiv a_{n+2}$ $(mod\ p^n)$. Por inducción, podemos demostrar que $a_n \equiv a_m$ $(mod\ p^n)$ para cualquier natural $m \geq n$.

Falta ver que efectivamente $(a_n)_{n\in\mathbb{N}} \in a$. Para ello observemos que para cada $m \in \mathbb{N}$, si $n \geq N(m)$ entonces

$$\begin{aligned} |a_n - b_n|_p &= |a_n - a_m + a_m - b_{N(m)} + b_{N(m)} - b_n|_p \\ &\leq \text{máx}\{|a_n - a_m|_p, |a_m - b_{N(m)}|_p, |b_{N(m)} - b_n|_p\} \\ &\leq \text{máx}\{\tfrac{1}{p^m}, \tfrac{1}{p^m}, \tfrac{1}{p^m}\} = \tfrac{1}{p^m}, \end{aligned}$$

por lo tanto $|a_n - b_n|_p \to 0$ cuando n tiende a infinito, es decir, que $(a_n)_{n\in\mathbb{N}} \in a$.

Ahora supongamos que hay una sucesión $(a'_n)_{n\in\mathbb{N}}$ que cumple las propiedades *1*, *2* y *3*, y que existe un natural n_0 tal que $a_{n_0} \neq a'_{n_0}$. Como ambos términos están entre 0 y $p^{n_0} - 1$, significa que $a_{n_0} \not\equiv a'_{n_0}\ (mod\ p^{n_0})$.

Sin embargo, para cualquier $n \geq n_0$ tenemos que $a_n \equiv a_{n_0}\ (mod\ p^{n_o})$ y $a'_n \equiv\ a'_{n_0}\ (mod\ p^{n_0})$ esto implica que $a_n \not\equiv a'_n\ (mod\ p^{n_0})$, es decir que $|a_n - a'_n|_p > \frac{1}{p^{n_0}}$ para toda $n \geq n_0$. Por lo tanto $(a'_n)_{n\in\mathbb{N}} \notin a$, lo cual implica que $(a_n)_{n\in\mathbb{N}}$ es la única sucesión en a que cumple las tres propiedades.

□

Analicemos qué nos dice el teorema que acabamos de demostrar. Consideremos algún número p-ádico a de norma menor o igual que 1, y la sucesión $(a_n)_{n\in\mathbb{N}} \in a$ como en el teorema. Al entero a_n lo expresamos en base p de la siguiente forma, recordando que $0 \leq a_n < p^n - 1$:

$$a_n = b_0 + b_1 \times p + b_2 \times p^2 + \cdots + b_{n-1} \times p^{n-1},$$

con $b_i \in \{0, 1, \ldots, p-1\}$ para toda i.

Análogamente expresamos a_{n+1} en base p:

$$a_{n+1} = b'_0 + b'_1 \times p + b'_2 \times p^2 + \cdots + b'_{n-1} \times p^{n-1} + b_n \times p^n,$$

con $b'_i \in \{0, 1, \ldots, p-1\}$ para toda i.

Sin embargo observemos que $b_i = b'_i$ para toda $i \in \{0, 1, \ldots, n-1\}$ ya que $a_n \equiv a_{n+1}\ (mod\ p^n)$, lo cual quiere decir que al tomar la diferencia entre ambos números obtenemos un múltiplo de p^n.

Así que a queda determinado por la sucesión de enteros b_n y podemos escribir $a = \sum_{n=0}^{\infty} b_n \times p^n$, que en principio se podría considerar como simple notación, pero al pensar a los enteros $b_n \times p^n$ como elementos de $\mathbb{Q}_p$ obtenemos una serie cuyo término general tiende a cero, pues $|b_n \times p^n|_p \leq\ |p^n|_p = p^{-n}$, y al estar en un espacio métrico completo no arquimediano, significa que la serie es convergente, y además converge precisamente al elemento a.

También notemos que cualquier serie de la forma $\sum_{n=0}^{\infty} b_n \times p^n$, donde cada $b_n \in \{0, 1, \ldots, p-1\}$, es una serie que converge a un elemento $a = \overline{(a_n)}_{n\in\mathbb{N}} \in\ \mathbb{Q}_p$ con $|a|_p \leq 1$, donde $a_n = \sum_{j=0}^{n-1} b_j \times p^j$ forma una sucesión que cumple las condiciones del teorema.

Veamos que también podemos construir una expresión similar para los números p-ádicos con norma mayor que 1.

Sea $a \in \mathbb{Q}_p$ tal que $|a|_p > 1$, además consideremos a un natural m tal que $|p^m a|_p \leq 1$. A este número lo podemos expresar como serie $p^m a = \sum_{n=0}^{\infty} b'_n \times p^n$, de modo que $a = \sum_{n=0}^{\infty} b'_n \times p^{n-m}$ o, poniendo $b_n = b'_{n+m}$, $a = \sum_{n=-m}^{\infty} b_n \times p^n$.

Teorema 22. *Para cada $a \in \mathbb{Q}_p$ existe un entero m y una sucesión $(b_n)_{n=m}^{\infty}$ de enteros tales que $0 \leq b_n < p$ y $a = \sum_{n=m}^{\infty} b_n \times p^n$.*

Recíprocamente, sean m un entero y $(b_n)_{n=m}^{\infty}$ una sucesión de enteros tales que $0 \leq b_n < p$, entonces existe $a \in \mathbb{Q}_p$ tal que $a = \sum_{n=m}^{\infty} b_n \times p^n$.

A la serie del teorema anterior le llamaremos expansión p-ádica del número p-ádico a, al conjunto de enteros $\{0, 1, \ldots, p-1\}$ le llamaremos conjunto de dígitos y a b_n le llamaremos la cifra en la posición p^n.

De esta forma ya tenemos la expresión buscada para todos los números p-ádicos, que es muy similar a la expansión decimal de los reales con dos importantes diferencias, la primera es que los números p-ádicos sólo tienen una cantidad finita de cifras distintas de cero correspondientes a potencias negativas mientras que pueden tener una cantidad infinita de cifras distintas de cero correspondientes a potencias positivas.

La otra diferencia, aún más importante, es que la unicidad de la sucesión en el teorema 21 nos garantiza que esta expresión es única, salvo agregar ceros a la izquierda, para todos los números p-ádicos, a diferencia del problema con las colas de nueves en los números reales.

Podemos observar en esta representación de los números p-ádicos que $|\mathbb{Q}_p| = 2^{\aleph_0}$, lo que quiere decir que al completar $\mathbb{Q}$ con la norma p-ádica realmente agregamos algo, lo cual demuestra que $(\mathbb{Q}, |\cdot|_p)$ no es completo.

Capítulo 3

Propiedades de los números p-ádicos

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

Ahora que tenemos una representación adecuada veamos cómo podemos trabajar con los números p-ádicos a través de ella.

Empezaremos por analizar cómo medir la distancia entre dos números.

Sean $a, b \in \mathbb{Q}_p$ y consideremos sus expansiones, que siempre podemos suponer que empiezan en la misma posición, y agregando ceros de ser necesario,

$$a = a_m \times p^m + a_{m+1} \times p^{m+1} + \cdots$$
$$b = b_m \times p^m + b_{m+1} \times p^{m+1} + \cdots .$$

Si se tiene que $k = \text{mín}\{i \in \mathbb{Z} : i \geq m,\ a_i \neq b_i\}$, entonces tenemos que

$$a - b = p^k(a_k - b_k) + p^{k+1}(\sum_{i=k+1}^{\infty} a_i \times p^{i-k-1} - \sum_{i=k+1}^{\infty} b_i \times p^{i-k-1}),$$

y por la desigualdad del triángulo no arquimediana concluimos

$$|a-b|_p \leq \text{máx}\{|p^k(a_k - b_k)|_p, |p^{k+1}(\sum_{i=k+1}^{\infty} a_i \times p^{i-k-1} - \sum_{i=k+1}^{\infty} b_i \times p^{i-k-1})|_p\}.$$

Ahora, teniendo en cuenta que $a_k, b_k \in \{0, 1, \ldots, p-1\}$ y que $a_k \neq b_k$, tenemos que $|a_k - b_k|_p = 1$ y por lo tanto

$$|p^k(a_k - b_k)|_p = |p^k|_p |a_k - b_k|_p = p^{-k}.$$

Analicemos el otro término, con base en que cada una de las series empieza en potencias no negativas, la norma de cada una de las series es menor que 1 al igual que la norma de la resta de ambas series, entonces tenemos que

$$|p^{k+1}(\sum_{i=k+1}^{\infty} a_i \times p^{i-k-1} - \sum_{i=k+1}^{\infty} b_i \times p^{i-k-1})|_p \leq p^{-(k+1)} < p^{-k},$$

y por la propiedad de los triángulos isósceles inferimos que $|a-b|_p = p^{-k}$.

Observación 23. *Para saber qué tan separados están dos números p-ádicos tenemos que fijarnos cuál es la primera cifra en la que difieren.*

A continuación vamos a describir los algoritmos para realizar las operaciones del campo $\mathbb{Q}_p$ y describiremos explicitamente la forma de ir haciendo la operación, esto con el propósito de que sea más claro el procedimiento.

3.1.1. La Suma

Supongamos que queremos sumar n números $a^{(1)}, a^{(2)}, \ldots, a^{(n)} \in \mathbb{Q}_p$, considerando sus expansiones

$$a^{(i)} = b_m^{(i)} \times p^m + b_{m+1}^{(i)} \times p^{m+1} + \cdots,$$

cabe señalar que estamos agregando ceros en caso de ser necesario para conseguir que todos los números empiecen en la misma cifra. Ahora escribimos los números uno sobre otro, respetando las posiciones

$$\begin{array}{rl} & b_m^{(1)} \times p^m \ + \ b_{m+1}^{(1)} \times p^{m+1} \ + \ \cdots \\ & b_m^{(2)} \times p^m \ + \ b_{m+1}^{(2)} \times p^{m+1} \ + \ \cdots \\ + & \vdots \\ & b_m^{(n)} \times p^m \ + \ b_{m+1}^{(n)} \times p^{m+1} \ + \ \cdots \end{array}$$

Buscamos una cifra $c_m \in \{0, 1, \ldots, p-1\}$ y un entero $r_{m+1} \in \mathbb{Z}^+ \cup \{0\}$ tal que

$$b_m^{(1)} + b_m^{(2)} + \cdots + b_m^{(n)} = c_m + p \times r_{m+1}$$

y escribimos

$$
\begin{array}{rlllll}
 & & & r_{m+1} & & \\
 & b_m^{(1)} \times p^m & + & b_{m+1}^{(1)} \times p^{m+1} & + & \cdots \\
 & b_m^{(2)} \times p^m & + & b_{m+1}^{(2)} \times p^{m+1} & + & \cdots \\
+ & \vdots & & & & \\
 & b_m^{(n)} \times p^m & + & b_{m+1}^{(n)} \times p^{m+1} & + & \cdots \\
\hline
 & c_m \times p^m & & & &
\end{array}
$$

Suponiendo que ya hemos encontrado las cifras anteriores a la posición p^k para $k > m$, ahora buscamos una cifra $c_k \in \{0, 1, \ldots, p - 1\}$ y un entero $r_{k+1} \in \mathbb{Z}^+ \cup \{0\}$ tal que

$$r_k + b_k^{(1)} + b_k^{(2)} + \cdots + b_k^{(n)} = c_k + p \times r_{k+1},$$

y de esta forma obtenemos un número p-ádico $d = c_m \times p^m + c_{m+1} \times p^{m+1} + \cdots$.

Consideremos las aproximaciones

$$a_k^{(i)} = b_m^{(i)} \times p^m + b_{m+1}^{(i)} \times p^{m+1} + \cdots + b_k^{(i)} \times p^k$$

$$d_k = c_m \times p^m + c_{m+1} \times p^{m+1} + \cdots + c_k \times p^k$$

que son racionales no negativos, y observamos que el algoritmo descrito antes, si se lleva hasta la obtención de la cifra en la posición p^k, es el algoritmo usual de suma de racionales no negativos con expansión finita, pero en base p,

$$
\begin{array}{rlllllllll}
 & & & r_{m+1} & & r_{m+2} & & & r_k & r_{k+1} \\
 & b_m^{(1)} \times p^m & + & b_{m+1}^{(1)} \times p^{m+1} & + & b_{m+2}^{(1)} \times p^{m+2} & + & \cdots + & b_k^{(1)} \times p^k & \\
 & b_m^{(2)} \times p^m & + & b_{m+1}^{(2)} \times p^{m+1} & + & b_{m+2}^{(2)} \times p^{m+2} & + & \cdots + & b_k^{(2)} \times p^k & \\
+ & \vdots & & & & & & & & \\
 & b_m^{(n)} \times p^m & + & b_{m+1}^{(n)} \times p^{m+1} & + & b_{m+2}^{(n)} \times p^{m+2} & + & \cdots + & b_k^{(n)} \times p^k & \\
\hline
 & c_m \times p^m & + & c_{m+1} \times p^{m+1} & + & c_{m+2} \times p^{m+2} & + & \cdots + & c_k \times p^k &
\end{array}
$$

De esta manera

$$a_k^{(1)} + a_k^{(2)} + \cdots + a_k^{(n)} = d_k + r_{k+1} \times p^{k+1}$$

y por lo tanto

$$|(a_k^{(1)} + a_k^{(2)} + \cdots + a_k^{(n)}) - d_k|_p \leq p^{-(k+1)}.$$

Así, al tomar el límite cuando $k \to \infty$, obtenemos que

$$d = a^{(1)} + a^{(2)} + \cdots + a^{(n)}.$$

Cabe señalar que si queremos conocer el número d hasta la posición p^k es suficiente conocer las cifras de $a^{(1)}, a^{(2)}, \ldots, a^{(n)}$ hasta esa misma posición.

3.1.2. La Resta

Ahora vamos a calcular $a-c$ con $a, c \in \mathbb{Q}_p$, partiendo de sus expansiones

$$a = b_m \times p^m + b_{m+1} \times p^{m+1} + \cdots,$$

$$c = d_m \times p^m + d_{m+1} \times p^{m+1} + \cdots.$$

De manera análoga al algoritmo de la suma escribimos a encima de c respetando las posiciones

$$\begin{array}{rl} & b_m \times p^m \ + \ b_{m+1} \times p^{m+1} \ + \ \cdots \\ - & d_m \times p^m \ + \ d_{m+1} \times p^{m+1} \ + \ \cdots \\ \hline \end{array}$$

Para encontrar la primera cifra consideramos dos casos:
si $b_m \geq d_m$, entonces $e_m = b_m - d_m$ y sea $r_{m+1} = 0$,
si $b_m < d_m$, entonces $e_m = b_m + p - d_m$ y sea $r_{m+1} = 1$.

En cualquier caso observemos que $e_m \in \{0, 1, \ldots, p-1\}$ y escribimos

$$\begin{array}{rl} & \quad\ r_{m+1} \\ & b_m \times p^m \ + \ b_{m+1} \times p^{m+1} \ + \ \cdots \\ - & d_m \times p^m \ + \ d_{m+1} \times p^{m+1} \ + \ \cdots \\ \hline & e_m \times p^m \end{array}$$

Suponiendo que hemos encontrado las cifras anteriores a la posición p^k con $k > m$, podemos encontrar la siguiente cifra como sigue:
si $b_k - r_k \geq d_k$, entonces $e_k = (b_k - r_k) - d_k$ y $r_{k+1} = 0$,
si $b_k - r_k < d_k$, entonces $e_k = (b_k - r_k) + p - d_k$ y $r_{k+1} = 1$.

En cualquier caso $e_k \in \{0, 1, \ldots, p-1\}$ y de esta forma vamos obteniendo un número p-ádico $f = e_m \times p^m + e_{m+1} \times p^{m+1} + \cdots$.

Consideremos las aproximaciones

$$a_k = b_m \times p^m + b_{m+1} \times p^{m+1} + \cdots + b_k \times p^k,$$

$$c_k = d_m \times p^m + d_{m+1} \times p^{m+1} + \cdots + d_k \times p^k,$$

$$f_k = e_m \times p^m + e_{m+1} \times p^{m+1} + \cdots + e_k \times p^k,$$

las cuales son racionales no negativos. Ahora cortamos el algoritmo descrito anteriormente hasta la obtención de la cifra en la posición p^k y lo comparamos con el algoritmo usal en base p para restar c_k a $a_k + r_{k+1} \times p^{k+1}$, observando que $a_k + r_{k+1} \times p^{k+1} \geq c_k$,

$$
\begin{array}{rl}
 & \overset{r_{m+1}}{b_m \times p^m} + b_{m+1} \times p^{m+1} + \overset{r_{m+2}}{b_{m+2} \times p^{m+2}} + \cdots + \overset{r_k}{b_k \times p^k} + \overset{r_{k+1}}{r_{k+1} \times p^{k+1}} \\
- & d_m \times p^m + d_{m+1} \times p^{m+1} + d_{m+2} \times p^{m+2} + \cdots + d_k \times p^k \\
\hline
 & e_m \times p^m + e_{m+1} \times p^{m+1} + e_{m+2} \times p^{m+2} + \cdots + e_k \times p^k + 0 \times p^{k+1}
\end{array}
$$

Notemos que $a_k + r_{k+1} \times p^{k+1} - c_k = f_k$ y por lo tanto

$$|(a_k - c_k) - f_k|_p \leq p^{-(k+1)}$$

y al tomar el límite cuando $k \to \infty$ obtenemos que $f = a - c$.

Hacemos notar que, al igual que en el caso de la suma, para encontrar las cifras hasta la posición p^k de f únicamente necesitamos conocer a y c hasta esa posición.

3.1.3. El Producto

Para el caso de la multiplicación de dos números $a, c \in \mathbb{Q}_p$, primero consideraremos el caso más sencillo en que uno de los números tiene tan sólo una cifra. Así, si las expansiones son

$$a = b_m \times p^m + b_{m+1} \times p^{m+1} + \cdots,$$

$$c = d_n \times p^n,$$

escribimos uno encima del otro, y en este caso no importa en qué posición comiencen,

$$
\begin{array}{rl}
 & b_m \times p^m \ + \ b_{m+1} \times p^{m+1} \ + \ \cdots \\
\times & d_n \times p^n \\
\hline
\end{array}
$$

Buscamos $f_s \in \{0, 1, \ldots, p-1\}$ y $r_{s+1} \in \mathbb{Z}^+ \cup \{0\}$ tal que

$$b_m \times d_n = f_s + r_{s+1} \times p$$

y escribimos

$$
\begin{array}{rl}
 & \overset{r_{s+1}}{b_m \times p^m} \ + \ b_{m+1} \times p^{m+1} \ + \ b_{m+2} \times p^{m+2} \ + \ \cdots \\
\times & d_n \times p^n \\
\hline
 & f_s \times p^s
\end{array}
$$

donde $s = n + m$.

Suponiendo que hemos encontrado las cifras anteriores a la posición p^k con $k > s$, buscamos $f_k \in \{0, 1, \ldots, p-1\}$ y $r_{k+1} \in \mathbb{Z}^+ \cup \{0\}$ tales que

$$b_{k-n} \times d_n + r_k = f_k + r_{k+1} \times p.$$

Continuando de esta manera encontramos el número p-ádico

$$e = \ f_s \times \ p^s + \ f_{s+1} \times \ p^{s+1} + \ \cdots .$$

Una vez más consideraremos las aproximaciones

$$a_k = b_m \times p^m + b_{m+1} \times p^{m+1} + \cdots + b_k \times p^k,$$

$$e_k = f_s \times p^s + f_{s+1} \times p^{s+1} + \cdots + f_k \times p^k.$$

El algoritmo hasta la obtención de la cifra en la posición p^k se escribe

$$\begin{array}{rlllllllll}
 & & & r_{s+1} & & r_{s+2} & & & r_k & r_{k+1} \\
 & b_m \times p^m & + & b_{m+1} \times p^{m+1} & + & b_{m+2} \times p^{m+2} & + \cdots + & b_{k-n} \times p^{k-n} & & \\
\times & d_n \times p^n & & & & & & & & \\
\hline
 & f_s \times p^s & + & f_{s+1} \times p^{s+1} & + & f_{s+2} \times p^{s+2} & + \cdots + & f_k \times p^k & &
\end{array}$$

y coincide con el algoritmo usual en base p de la multiplicación en los racionales. Esto nos dice que $a_{k-n} \times c = e_k + r_{k+1} \times p^{k+1}$, por lo tanto

$$|a_{k-n} \times c - e_k|_p \leq p^{-(k+1)}.$$

Al tomar el límite obtenemos que $a \times c = e$.

Para el caso general en que c es cualquier número p-ádico cuya expansión es

$$c = d_n \times p^n + d_{n+1} \times p^{n+1} + \cdots$$

escribimos a encima de c y vamos multiplicando cada cifra de c por a, usando el algoritmo del caso anterior, y escribiendo los resultados abajo respetando las posiciones

$$\begin{array}{rlllllll}
 & b_m \times p^m & + & b_{m+1} \times p^{m+1} & + & b_{m+2} \times p^{m+2} & + & \cdots \\
\times & d_n \times p^n & + & d_{n+1} \times p^{n+1} & + & d_{n+2} \times p^{n+2} & + & \cdots \\
\hline
 & f_s^{(n)} \times p^s & + & f_{s+1}^{(n)} \times p^{s+1} & + & f_{s+2}^{(n)} \times p^{s+2} & + & \cdots \\
 & & & f_{s+1}^{(n+1)} \times p^{s+1} & + & f_{s+2}^{(n+1)} \times p^{s+2} & + & \cdots \\
 & & & & & f_{s+2}^{(n+2)} \times p^{s+2} & + & \cdots \\
 & & & & & & & \ddots \\
\hline
\end{array}$$

donde $s = n + m$ y

$$a \times d_i \times p^i = e^{(i)} = f_{m+i}^{(i)} \times p^{m+i} + f_{m+i+1}^{(i)} \times p^{m+i+1} + \cdots$$

De esta forma nos queda una suma infinita, sin embargo debido a que se va recorriendo la posición en que comienza cada sumando, podemos ir sumando sin problemas. Es decir, si queremos el resultado hasta la cifra en la posición p^k consideramos únicamente los primeros $k-s+1$ sumandos y los sumamos hasta la posición p^k. Como los siguientes sumandos comienzan después de la posición p^k, las cifras que obtuvimos de esta forma no serán modificadas.

Llamemos g al número p-ádico así obtenido cuya expansión es

$$g \;=\; h_s \times \; p^s + \; h_{s+1} \times \; p^{s+1} + \; \cdots$$

y g_k a la aproximación hasta la posicón p^k y multipliquemos los racionales no negativos a_{k-n} y c_{k-m} con el algoritmo usual en base p. Obtenemos entonces lo siguiente:

$$\begin{array}{cccccccccc}
 & b_m \times p^m & + & b_{m+1} \times p^{m+1} & + \cdots + & b_{k-n} \times p^{k-n} & & \\
\times & d_n \times p^n & + & d_{n+1} \times p^{n+1} & + \cdots + & d_{k-m} \times p^{k-m} & & \\
\hline
 & f_s^{(n)} \times p^s & + & f_{s+1}^{(n)} \times p^{s+1} & + \cdots + & f_k^{(n)} \times p^k & + & \cdots \\
 & & & f_{s+1}^{(n+1)} \times p^{s+1} & + \cdots + & f_k^{(n+1)} \times p^k & + & \cdots \\
 & & & & \ddots & \vdots & & \\
 & & & & & f_k^{(k-m)} \times p^k & + & \cdots \\
\hline
 & h_s \times p^s & + & h_{s+1} \times p^{s+1} & + \cdots + & h_k \times p^k & + & \cdots
\end{array}$$

El resultado coincidiría hasta la posición p^k, es decir, que para algún entero no negativo r se cumple que $a_{k-n} \times c_{k-m} = g_k + r \times p^{k+1}$. Por lo tanto se cumple que

$$|(a_{k-n} \times c_{k-m}) - g_k|_p \leq p^{-(k+1)},$$

y al tomar el límite obtenemos que $a \times c = g$.

Recalcamos que para obtener el número g hasta la posición p^k necesitamos el número a hasta la posición p^{k-n} y el número c hasta la posición p^{k-m}.

3.1.4. La División

Por último, para dividir un número $a \in \mathbb{Q}_p$ entre otro número $c \in \mathbb{Q}_p \setminus \{0\}$ cuyas expansiones son

$$a = b_m \times p^m + b_{m+1} \times p^{m+1} + \cdots,$$

$$c = d_n \times p^n + d_{n+1} \times p^{n+1} + \cdots,$$

con $d_n \neq 0$ escribimos a dentro de la "casita" y c afuera

$$d_n \times p^n + d_{n+1} \times p^{n+1} + \cdots \;\big|\; \overline{b_m \times p^m \;+\; b_{m+1} \times p^{m+1} \;+\; \cdots}$$

Buscamos una cifra h_s tal que $h_s \times d_n \equiv b_m \; (mod\ p)$, donde $s = m - n$, que siempre existe pues $d_n \neq 0$ y p es un primo. Escribimos $h_s \times p^s$ arriba de la casita, lo multiplicamos por c, lo escribimos debajo de a y hacemos la resta.

Si llamamos $e^{(0)} = f_m \times p^m + f_{m+1} \times p^{m+1} + \cdots = (h_s \times p^s) \times c$ y $a^{(1)} = b^{(1)}_{m+1} \times p^{m+1} + b^{(1)}_{m+2} \times p^{m+2} + \cdots = a - e^{(0)}$, la forma en que escogimos la cifra h_s nos garantiza que $b_m = f_m$ y por lo tanto $|a^{(1)}|_p \leq p^{-(m+1)}$

$$d_n \times p^n + d_{n+1} \times p^{n+1} + \cdots \;\Big|\; \begin{array}{l} \overline{h_s \times p^s} \\ b_m \times p^m + b_{m+1} \times p^{m+1} + \cdots \\ \underline{f_m \times p^m + f_{m+1} \times p^{m+1} + \cdots} \\ \qquad b^{(1)}_{m+1} \times p^{m+1} + b^{(1)}_{m+2} \times p^{m+2} + \cdots \end{array}$$

Suponiendo que hemos encontrado las cifras anteriores a la posición p^k con $k > s$, buscamos una cifra h_k tal que $h_k \times d_n \equiv b^{(k-s)}_{n+k} \; (mod\ p)$ y llamamos

$$e^{(k-s)} = f^{(k-s)}_{n+k} \times p^{n+k} + f^{(k-s)}_{n+k+1} \times p^{n+k+1} + \cdots = (h_k \times p^k) \times c$$

y

$$a^{(k-s+1)} = b^{(k-s+1)}_{n+k+1} \times p^{n+k+1} + b^{(k-s+1)}_{n+k+2} \times p^{n+k+2} + \cdots = \; a^{(k-s)} - \; e^{(k-s)}.$$

Por la forma en que elegimos la cifra h_k tenemos que $f^{(k-s)}_{n+k} = b^{(k-s)}_{n+k}$ y por lo tanto $|a^{(k-s+1)}|_p \leq \; p^{-(k+n+1)}$

$$d_n \times p^n + d_{n+1} \times p^{n+1} + \cdots \;\Big|\; \begin{array}{l} \overline{h_s \times p^s \;+ h_{s+1} \times p^{s+1} \;+ \cdots \qquad\qquad + h_k \times p^k} \\ b_m \times p^m + b_{m+1} \times p^{m+1} + \cdots \\ \underline{f_m \times p^m + f_{m+1} \times p^{m+1} + \cdots} \\ \qquad b^{(1)}_{m+1} \times p^{m+1} + b^{(1)}_{m+2} \times p^{m+2} + \cdots \\ \qquad \underline{f^{(1)}_{m+1} \times p^{m+1} + f^{(1)}_{m+1} \times p^{m+1} + \cdots} \\ \qquad\qquad \ddots \\ \qquad\qquad\qquad \begin{array}{l} b^{(k-s)}_{n+k} \times p^{n+k} + b^{(k-s)}_{n+k+1} \times p^{n+k+1} \;+ \cdots \\ \underline{f^{(k-s)}_{n+k} \times p^{n+k} + f^{(k-s)}_{n+k+1} \times p^{n+k+1} \;+ \cdots} \\ \qquad b^{(k-s+1)}_{n+k+1} \times p^{n+k+1} + \cdots \end{array} \end{array}$$

De esta forma obtenemos un número p-ádico $g = h_s \times p^s + h_{s+1} \times p^{s+1} + \cdots$ y si llamamos g_k a la aproximación hasta la posición p^k tenemos que

$$g_k \times c = \sum_{i=s}^{k} (h_i \times p^i) \times c = \sum_{i=s}^{k} e^{(i-s)}$$

así que

$$\begin{aligned} a - g_k \times c &= a - e^{(0)} - \sum_{i=s+1}^{k} e^{(i-s)} = a^{(1)} - e^{(1)} - \sum_{i=s+2}^{k} e^{(i-s)} \\ &= \cdots = a^{(k-s)} - e^{(k-s)} = a^{(k-s+1)} \end{aligned}$$

Por lo tanto $|a - (g_k \times c)|_p \leq p^{-(k+n+1)}$ y al tomar el límite obtenemos que $a = g \times c$, o equivalentemente que $g = \frac{a}{c}$.

En nuestro algoritmo podemos observar que para encontrar g hasta la posición p^k únicamente necesitamos conocer a hasta la posición p^{n+k} y c hasta la posición p^{2n+k-m}.

Observemos algunas diferencias entre estos algoritmos y los correspondientes algoritmos en el campo de los números reales.

Estos algoritmos se aplican directamente a cualesquiera números p-ádicos, a diferencia de los números reales, donde si consideramos dos números $a, b \in \mathbb{R}$ y queremos obtener $a + b$, suponiendo que $a > 0$, $b < 0$ y $|a| < |b|$, debemos usar el algoritmo de resta para obtener $|b| - |a|$ y al resultado ponerle un signo negativo.

Otra diferencia es que al trabajar con números con expansión infinita, los algoritmos en los números reales van aproximando el resultadoen el sentido de convergencia, pero no en el sentido de ir obteniendo las cifras definitivas, por ejemplo al sumar los números $0.333\ldots$ y $0.666\cdots$ las aproximaciones nos van dando 9 en todas las cifras decimales mientras el resultado es 0 en todas las cifras decimales. Como vimos, con nuestros algoritmos p-ádicos vamos obteniendo las cifras del resultado.

Trabajando con los números p-ádicos si hemos utilizado nuestro algoritmo para obtener n cifras y ahora queremos obtener la siguiente cifra podemos retomar los cálculos que habíamos hecho para las n cifras ya obtenidas, esto no es posible en los reales, debido a que los algoritmos se trabajan empezando por las cifras menos significativas, exceptuando el algoritmo de la división.

3.2. $\mathbb{Z}$ y $\mathbb{Q}$ dentro de $\mathbb{Q}_p$

En esta sección describiremos cómo son las expansiones p-ádicas correspondientes a los enteros y a los racionales.

Los enteros positivos son simplemente los números p-ádicos cuya expansión es finita y no tienen cifras correspondientes a potencias negativas, pues su expansión es la correspondiente a la base p. Para encontrar la forma de los enteros negativos utilizaremos el algoritmo de la resta.

Sea $a \in \mathbb{Z}^+$ con expansión p-ádica $a = b_k \times p^k + b_{k+1} \times p^{k+1} + \cdots + b_n \times p^n$ con $b_k \neq 0$ y $k \geq 0$, podemos escribir al 0 de la siguiente manera:

$$0 = c_k \times p^k + c_{k+1} \times p^{k+1} + \cdots \text{donde cada } c_i = 0.$$

Podemos encontrar $-a$ como el resultado de restarle a a 0 siguiendo el algoritmo descrito en la sección anterior. Como $c_k < b_k$ llamemos $d_k = p - b_k$ y $r_{k+1} = 1$, ahora $c_{k+1} - r_{k+1} = -1 < b_{k+1}$, por lo tanto $d_{k+1} = p - 1 - b_{k+1}$ y $r_{k+2} = 1$. De la misma forma podemos ver que todas los siguientes residuos r_i van a ser 1 y $d_i = p - 1 - b_i$, de forma que para $i > n$ tenemos que $d_i = p - 1$.

$$\begin{array}{rccccc}
 & {\scriptstyle 1} & & {\scriptstyle 1} & & {\scriptstyle 1} \\
 & 0 \times p^k & +0 \times p^{k+1} & +0 \times p^{k+2} & +\cdots+0 \times p^n & +0 \times p^{n+1} \\
- & b_k \times p^k & +b_{k+1} \times p^{k+1} & +b_{k+2} \times p^{k+2} & +\cdots+b_n \times p^n & \\
\hline
 & (p-b_k) \times p^k & +(p-1-b_{k+1}) \times p^{k+1} & +(p-1-b_{k+2}) \times p^{k+2} & +\cdots+(p-1-b_n) \times p^n & +(p-1) \times p^{n+1}
\end{array}$$

De hecho con un argumento casi idéntico podemos ver que si un número p-ádico cualquiera a tiene expansión $a = \sum_{i=k}^{\infty} b_i \times p^i$ con $b_k \neq 0$ entonces la expansión de $-a$ será $-a = (p - b_k) \times p^k + \sum_{i=k+1}^{\infty} (p - 1 - b_i) \times p^i$.

Por lo tanto **los enteros negativos son los números p-ádicos cuya expansión no tiene cifras correspondientes a potencias negativas y a partir de un momento todas sus cifras son $p - 1$.**

Para encontrar cómo es la expansión de un número racional consideremos $x = \frac{a}{b} \in \mathbb{Q} \setminus \mathbb{Z}$ con $a \in \mathbb{Z}$ y $b \in \mathbb{Z}^+$ y dividamos a entre b.

Observando el algoritmo de la división, como x no es entero la expansión del cociente no es finita, por lo cual a los diferentes residuos les restamos múltiplos de b, que son de hecho cada vez más grandes, por lo cual eventualmente el residuo tendrá que ser un entero negativo, es decir que sus cifras serán todas $p - 1$ a partir de un momento.

Consideremos los distintos múltiplos de b: $1 \times b, 2 \times b, \ldots, (p-1) \times b$; todos son enteros positivos y por lo tanto tienen una cantidad finita de cifras distintas de cero, llamemos n a la máxima cantidad de cifras entre la primera cifra distinta de cero y la última cifra distinta de cero en estos números.

Analicemos cómo van siendo los distintos residuos, sin tomar en cuenta la posición sino únicamente la sucesión de cifras. Partiendo de un residuo

que ya es un entero negativo podemos asegurar que después de m cifras todas sus cifras son $p-1$ para alguna $m \geq n$.

Al siguiente paso restaremos un múltiplo de b, es decir un número con a lo más m cifras, esta resta en el peor de los casos podría llegar a afectar la primera cifra después de las m, con lo cual el nuevo residuo tendría $m+1$ cifras antes de que todas sean $p-1$, sin embargo, debido a la forma del algoritmo, la primera cifra debe cancelarse, es decir que en realidad el nuevo residuo tendrá una vez más a lo más m cifras antes de que todas sean $p-1$.

Como únicamente hay p^m sucesiones de cifras de esta forma, en algún paso se debe repetir algún residuo, lo cual causará que a partir de ese momento se genere una sucesión periódica de cifras en el cociente.

Recíprocamente, si consideramos un número p-ádico cuya expansión sea eventualmente periódica

$$a = b_n \times p^n + \cdots + b_m \times p^m + c_1 \times p^{m+1} + \cdots + c_r \times p^{m+r} + c_1 \times p^{m+r+1} + \cdots + c_r \times p^{m+2r} + \cdots$$

Llamamos

$$A = b_n + b_{n+1} \times p + \cdots + b_m \times p^{m-n} \in \mathbb{Z}$$

y

$$B = c_1 + c_2 \times p + \cdots + c_r \times p^{r-1} \in \mathbb{Z}$$

entonces tenemos que

$$a = A \times p^n + B \times \sum_{k=0}^{\infty} p^{m+kr+1}.$$

Observemos que $\sum_{k=0}^{s} p^{kr} = \frac{1-p^{(s+1)r}}{1-p^r}$, ya que es una igualdad general y además $|p^{(s+1)r}|_p = p^{-(s+1)r} \to 0$ cuando s tiende a infinito, entonces $\sum_{k=0}^{\infty} p^{kr} = \frac{1}{1-p^r}$.

Podemos concluir que

$$a = A \times p^n + B \times p^{m+1} \times (\frac{1}{1-p^r}) \in \mathbb{Q}.$$

Por lo tanto, **los racionales son exactamente los números p-ádicos cuya expansión es eventualmente periódica**, de manera similar a lo que sucede en los reales, y así se puede demostrar que $\mathbb{Q}_p \setminus \mathbb{Q}$ es denso en $\mathbb{Q}_p$.

3.3. Los enteros p-ádicos $\mathbb{Z}_p$

Denotemos $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$. Este subespacio recibe el nombre de enteros p-ádicos, que también puede verse como el conjunto de los números p-ádicos que no tienen cifras correspondientes a potencias negativas, es claro que $\mathbb{Z}$ es denso en $\mathbb{Z}_p$. De hecho, $\mathbb{Z}_p$ es la completación de $\mathbb{Z}$ con la norma p-ádica. La demostración de la afirmación anterior es el teorema 21.

En esta sección vamos a estudiar algunas propiedades algebraicas de $\mathbb{Z}_p$ y $\mathbb{Q}_p$, siempre teniendo en cuenta la analogía con $\mathbb{Z}$ y $\mathbb{Q}$. Para estudiar algunos de los conceptos que serán mencionados a lo largo de esta sección así como las propiedades análogas de $\mathbb{Z}$ y $\mathbb{Q}$ se pueden ver en [3].

$\mathbb{Z}_p$ es un anillo, pues es cerrado bajo la suma, el producto y la inversión aditiva, lo cual puede comprobarse a través de los algoritmos o simplemente notando que si $x, y \in \mathbb{Z}_p$, entonces

$$|x + y|_p \leq \text{máx}\{|x|_p, |y|_p\} \leq 1,$$

$$|xy|_p = |x|_p|y|_p \leq 1,$$

y

$$|-x|_p = |x|_p \leq 1.$$

A partir de $\mathbb{Z}_p$ podemos recuperar $\mathbb{Q}_p$ como su campo de fracciones, al igual que $\mathbb{Q}$ es el campo de fracciones de $\mathbb{Z}$.

Recordemos que $|\frac{1}{x}|_p = \frac{1}{|x|_p}$, por lo tanto la única forma de que un entero p-ádico x tenga inverso multiplicativo en $\mathbb{Z}_p$ es que $|x|_p = 1$, es decir que $\mathbb{Z}_p^\times = \{x \in \mathbb{Z}_p : |x|_p = 1\}$ son las unidades en los enteros p-ádicos, o equivalentemente los enteros p-ádicos cuya cifra en la posición p^0 es distinta de cero, mientras que en $\mathbb{Z}$ las únicas unidades son 1 y -1.

Sea $p^n\mathbb{Z}_p = \{p^n x : x \in \mathbb{Z}_p\} = \{x \in \mathbb{Z}_p : |x|_p \leq p^{-n}\}$, estos subanillos de $\mathbb{Z}_p$ son ideales ordenados por la contención de forma que $p^m\mathbb{Z}_p \subset p^n\mathbb{Z}_p$ si $n < m$. A continuación veremos que son los únicos ideales de $\mathbb{Z}_p$.

Proposición 24. *$\mathbb{Z}_p$ es un dominio de ideales principales, es decir que todos sus ideales están generados por un elemento.*

Demostración. Sea I un ideal en $\mathbb{Z}_p$ y $p^{-n} = \text{máx}\{|a|_p : a \in I\}$, el máximo existe ya que los posibles valores de la norma p-ádica están acotados en $\mathbb{Z}_p$ y son discretos, salvo el 0. Entonces claramente $I \subseteq p^n\mathbb{Z}_p$. Ahora sea $a \in I$ tal que $|a|_p = p^{-n}$, entonces $p^{-n}a \in \mathbb{Z}_p^\times$ que es un grupo multiplicativo, de forma que existe $x \in \mathbb{Z}_p$ tal que $p^{-n}ax = 1$ o equivalentemente $ax = p^n$, pero al ser I un ideal tenemos que $ax \in I$ y por lo tanto $p^n\mathbb{Z}_p \subseteq I$.

□

Sean $x, y \in \mathbb{Z}_p$, escribiremos $x \equiv y \ (mod\ p^n)$ si $|x-y|_p \leq p^{-n}$, o equivalentemente si $x - y \in p^n\mathbb{Z}_p$ (o que x y y coinciden en sus cifras hasta la posición p^{n-1}). Esto define una relación de equivalencia.

Observación 25. *Se cumplen las siguientes propiedades:*

1. *Si* $x \equiv y \ (mod\ p^n)$ *y* $z \in \mathbb{Z}_p$ *entonces* $x + z \equiv y + z \ (mod\ p^n)$
2. *Si* $x \equiv y \ (mod\ p^n)$ *y* $z \in \mathbb{Z}_p$ *entonces* $xz \equiv yz \ (mod\ p^n)$
3. *Si* $x \equiv y \ (mod\ p^n)$ *y* $z \in \mathbb{Z}_p^\times$ *entonces* $\frac{x}{z} \equiv \frac{y}{z} \ (mod\ p^n)$
4. $xp \equiv yp \ (mod\ p^{n+1}) \Leftrightarrow x \equiv y \ (mod\ p^n)$

ya que

(1) $|(x+z)-(y+z)|_p = |x-y|_p \leq p^{-n}$.
(2) $|xz - yz|_p = |x-y|_p|z|_p \leq |x-y|_p \leq p^{-n}$.
(3) *Por 2, ya que* $\frac{1}{z} \in \mathbb{Z}_p$.
(4) $|xp - yp|_p = |x-y|_p p^{-1} \leq p^{-(n+1)} \Leftrightarrow |x-y|_p \leq p^{-n}$.

Si $x, y \in \mathbb{Z}$ recuperamos la noción de congruencia usual, además los cocientes bajo esta relación en $\mathbb{Z}$ y $\mathbb{Z}_p$ son isomorfos ${}^{\mathbb{Z}_p}\!/_{p^n\mathbb{Z}_p} \cong {}^{\mathbb{Z}}\!/_{p^n\mathbb{Z}}$.

Llamaremos $\mathbb{Z}_p[x]$ y $\mathbb{Q}_p[x]$ a los anillos de polinomios con coeficientes en $\mathbb{Z}_p$ y $\mathbb{Q}_p$ respectivamente. Veamos que la irreducibilidad de un polinomio con coeficientes enteros p-ádicos es equivalente en ambos anillos, al igual que sucede con $\mathbb{Z}$ y $\mathbb{Q}$.

Teorema 26. *Sea* $f(x) \in \mathbb{Z}_p[x]$ *entonces, existen dos polinomios no constantes* $g(x), h(x) \in \mathbb{Q}_p[x]$ *tales que* $f(x) = g(x)h(x)$ *si y sólo si existen polinomios no constantes* $\bar{g}(x), \bar{h}(x) \in \mathbb{Z}_p[x]$ *tales que* $f(x) = \bar{g}(x)\bar{h}(x)$.

Demostración. Sean $f(x) \in \mathbb{Z}_p[x]$ y $g(x), h(x) \in \mathbb{Q}_p[x]$, $f(x) = \sum_{i=0}^{n+m} a_i x^i$, $g(x) = \sum_{i=0}^{n} b_i x^i$,$h(x) = \sum_{i=0}^{m} c_i x^i$ con $n, m > 0$, tales que $f(x) = g(x)h(x)$.

Sean r, s, i_0, j_0 tales que $p^r = |b_{i_0}|_p = \text{máx}\{|b_i|_p : i = 0, \ldots, n\}$ y $p^s = |c_{j_0}|_p = \text{máx}\{|c_j|_p : j = 0, \ldots, m\}$, escogiendo i_0 y j_0 mínimos. Entonces tenemos que $p^r g(x), p^s h(x) \in \mathbb{Z}_p[x]$ y además

$$|a_{i_0+j_0}|_p = |\sum_{i+j=i_0+j_0} b_i c_j|_p \leq \text{máx}\{|b_i c_j|_p : i + j = i_0 + j_0\} = p^{r+s}.$$

Observemos que si $i < i_0$ entonces $|b_i c_j|_p < p^r |c_j|_p \leq p^{r+s}$ y si $i > i_0$ esto implica que $j < j_0$ y en tal caso $|b_i c_j|_p < |b_i|_p p^s \leq p^{r+s}$, es decir que la norma máxima se alcanza en tan sólo uno de los sumandos lo cual implica que la desigualdad en realidad es una igualdad. De aquí concluimos que

$$1 \geq |a_{i_0+j_0}|_p = p^{r+s},$$

es decir que $r+s \leq 0$ y por lo tanto $p^{-(r+s)} \in \mathbb{Z}$ y $p^{-s}g(x) \in \mathbb{Z}_p[x]$.

De esta forma podemos escribir $f(x) = (p^{-s}g(x))(p^s h(x))$ como producto de polinomios no constantes en $\mathbb{Z}_p[x]$. Es decir que si un polinomio en $\mathbb{Z}_p[x]$ no es irreducible en $\mathbb{Q}_p[x]$, tampoco es irreducible en $\mathbb{Z}_p[x]$. La otra implicación es inmediata ya que todo polinomio con coeficientes en $\mathbb{Z}_p$ es un polinomio con coeficientes en $\mathbb{Q}_p$.

□

Consideremos el caso en que el coeficiente principal de $f(x)$ es una unidad de $\mathbb{Z}_p$, es decir que $|a_{n+m}|_p = 1$, pero $1 = |a_{n+m}|_p = |b_n c_m|_p \leq p^{r+s}$ y como $r+s \leq 0$, debe cumplirse que $r+s=0$, $|b_n|_p = p^r$ y $|c_m|_p = p^s$, por lo tanto los coeficientes principales de $p^{-s}g(x)$ y $p^r h(x)$ están en $\mathbb{Z}_p^\times$.

Sea $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}_p[x]$ con $a_n \in \mathbb{Z}_p^\times$ y sea $\alpha \in \mathbb{Q}_p$ una raíz de $f(x)$. Entonces $f(x) = g(x)(x-\alpha)$ y por la discusión anterior $f(x)$ se puede factorizar como producto de polinomios en $\mathbb{Z}_p[x]$, con coeficientes principales en $\mathbb{Z}_p^\times$ que son los mismos polinomios tan sólo multiplicados por un escalar y por lo tanto tienen las mismas raíces. Digamos que $f(x) = \bar{g}(x)(c_1 x + c_0)$ con $c_1 \in \mathbb{Z}_p^\times$, entonces la raíz de este polinomio debe ser $\alpha = -\frac{c_0}{c_1} \in \mathbb{Z}_p$.

Es decir que para un polinomio con coeficientes en $\mathbb{Z}_p$, cuyo coeficiente principal es una unidad (en particular si el polinomio es mónico), todas sus raíces en $\mathbb{Q}_p$ son enteros p-ádicos. Lo anterior es análogo a lo que sucede con los polinomios mónicos con coeficientes enteros cuyas raíces racionales son enteros.

El siguiente teorema nos da un método bastante general para encontrar raíces de polinomios con coeficientes en $\mathbb{Z}_p$.

Teorema 27 (Lema de Hensel)**.** *Sea $f(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n$ un polinomio con coeficientes en $\mathbb{Z}_p$ y $f'(x) = c_1 + 2c_2 x + \cdots + n c_n x^{n-1}$ su derivada. Si $a_0 \in \mathbb{Z}_p$ cumple que $f(a_0) \equiv 0 \ (mod\ p)$ y $f'(a_0) \not\equiv 0 \ (mod\ p)$ entonces existe un único $a \in \mathbb{Z}_p$ tal que $a \equiv a_0 \ (mod\ p)$ y $f(a) = 0$.*

Demostración. Vamos a contruir una sucesión de enteros que aproximen la raíz que buscamos en $\mathbb{Z}_p$, $a_1, a_2, \ldots$ que cumplan

1. $f(a_k) \equiv 0 \ (mod\ p^{k+1})$
2. $a_k \equiv a_{k-1} \ (mod\ p^k)$
3. $0 \leq a_k < p^{k+1}$

Para $k=1$ Sea $b_0 \in \{0, 1, \ldots, p-1\}$ tal que $a_0 \equiv b_0 \ (mod\ p)$. Para que se cumplan las condición 2 y 3 necesitamos que $a_1 = b_0 + b_1 \times p$ para algún $b_1 \in \{0, 1, \ldots, p-1\}$.

Ahora observemos que

$$\begin{aligned} f(a_1) &= f(b_0 + b_1 \times p) = \sum_{i=0}^{n} c_i (b_0 + b_1 \times p)^i \\ &= \sum_{i=0}^{n} (c_i b_0^i + i c_i b_0^{i-1} b_1 p + O(p^2)) \\ &\equiv \sum_{i=0}^{n} c_i b_0^i + (\sum_{i=1}^{n} i c_i b_0^{i-1}) b_1 p \ (mod\ p^2) \\ &= f(b_0) + f'(b_0) b_1 p \end{aligned}$$

donde $O(p^2)$ se refiere a términos que son múltiplos de p^2.

Utilizando las propiedades de congruencias de la observación 25, como $b_0 \equiv a_0 \ (mod\ p)$ entonces $f(b_0) \equiv f(a_0) \ (mod\ p)$ y $f'(b_0) \equiv f'(a_0) \ (mod\ p)$, es decir que $f'(b_0) \in \mathbb{Z}_p^{\times}$.

Como $f(b_0) \equiv 0 \ (mod\ p)$, existe $\alpha_0 \in \{0, 1, \ldots, p-1\}$ tal que $f(b_0) \equiv \ \alpha_0 p \ (mod\ p^2)$, entonces para que se cumpla la condición 1

$$\begin{aligned} f(a_1) \equiv 0 \ (mod\ p^2) &\Leftrightarrow \alpha_0 p + f'(b_0) b_1 p \equiv 0 \ (mod\ p^2) \\ &\Leftrightarrow \alpha_0 + f'(b_0) b_1 \equiv 0 \ (mod\ p) \\ &\Leftrightarrow b_1 \equiv -\tfrac{\alpha_0}{f'(b_0)} \ (mod\ p) \end{aligned}$$

y esta última condición determina un único $b_1 \in \{0, 1, \ldots, p-1\}$.

Supongamos que ya encontramos $a_1, \ldots, a_{n-1}$ que cumplen las condiciones. Ahora buscamos a_n que debe tener la forma $a_n = a_{n-1} + b_n \times p^n$ para alguna $b_n \in \{0, 1, \ldots, p-1\}$.

Veamos que

$$\begin{aligned} f(a_n) &= f(a_{n-1} + b_n \times p^n) = \sum_{i=0}^{n} c_i (a_{n-1} + b_n \times p^n)^i \\ &= \sum_{i=0}^{n} (c_i a_{n-1}^i + i c_i a_{n-1}^{i-1} b_n p^n + O(p^{2n})) \\ &\equiv \sum_{i=0}^{n} c_i a_{n-1}^i + (\sum_{i=1}^{n} i c_i a_{n-1}^{i-1}) b_n p^n \ (mod\ p^{n+1}) \\ &= f(a_{n-1}) + f'(a_{n-1}) b_n p^n \end{aligned}$$

donde $O(p^{2n})$ son términos que son múltiplos de p^{2n}.

Como $f(a_{n-1}) \equiv 0 \ (mod\ p^n)$ debe existir $\alpha_{n-1} \in \{0, 1 \ldots, p-1\}$ tal que $f(a_{n-1}) \equiv \alpha_{n-1} p^n \ (mod\ p^{n+1})$, además $a_{n-1} \equiv a_0 \ (mod\ p)$ por lo que $f'(a_{n-1}) \equiv f'(a_0) \ (mod\ p)$ y $f'(a_{n-1}) \in \mathbb{Z}_p^{\times}$.

Para que se cumpla la condición 1 notemos que

$$\begin{aligned} f(a_n) \equiv 0 \ (mod\ p^{n+1}) &\Leftrightarrow \alpha_{n-1} p^n + f'(a_{n-1}) b_n p^n \equiv 0 \ (mod\ p^{n+1}) \\ &\Leftrightarrow \alpha_{n-1} + f'(a_{n-1}) b_n \equiv 0 \ (mod\ p) \\ &\Leftrightarrow b_n \equiv -\tfrac{\alpha_{n-1}}{f'(a_{n-1})} \ (mod\ p) \end{aligned}$$

una vez más, la última condición determina un único $b_n \in \{0, 1, \ldots, p-1\}$.

Sea $a = b_0 + b_1 \times p + b_2 \times p^2 + \cdots$, como $a \equiv a_n \ (mod\ p^{n+1})$, entonces $f(a) \equiv f(a_n) \equiv 0 \ (mod\ p^{n+1})$ para toda n, por lo tanto $f(a) = 0$.

La unicidad está garantizada en la construcción, pues en todo momento nos vimos forzados a una única opción en cada una de las cifras de a, a partir de a_0.

□

Obviamente, dependiendo de la elección de a_0 obtendremos distintas raíces en $\mathbb{Z}_p$, sin embargo notemos que por medio de este método no podemos obtener más de p raíces. Si $f(x)$ tiene más de p raíces distintas, entonces existen dos a, b tales que $a \equiv b \ (mod\ p)$ y en tal caso debe ocurrir que $f'(a) \equiv f'(b) \equiv 0 \ (mod\ p)$.

La siguiente generalización del Lema de Hensel, permite encontrar raíces simples de un polinomio cuando la derivada del polinomio evaluada en la raíz es congruente con 0 módulo p. La demostración es prácticamente igual y la omitiremos.

Teorema 28. *Sea $f(x) \in \mathbb{Z}_p[x]$ un polinomio con coeficientes enteros p-ádicos y M un entero no negativo. Sea $a_0 \in \mathbb{Z}_p$ tal que $f(a_0) \equiv 0 \ (mod\ p^{2M+1})$ y $f'(a_0) \equiv 0 \ (mod\ p^M)$, pero $f'(a_0) \not\equiv 0 \ (mod\ p^{M+1})$, entonces existe un único $a \in \mathbb{Z}_p$ tal que $f(a) = 0$ y $a \equiv a_0 \ (mod\ p^{M+1})$.*

Este teorema se puede aplicar para encontrar cualquier raíz simple, pues si a es una raíz simple $f'(a) \neq 0$ y por lo tanto debe existir algún entero no negativo M tal que $f'(a) \not\equiv 0 \ (mod\ p^{M+1})$, y en tal caso debemos aproximar la raíz módulo p^{2M+1} antes de poder aplicar el teorema. Para raíces múltiples hay que buscar las raíces de $f'(x)$.

Veamos ahora un ejemplo de cómo usar el Lema de Hensel. Sea $p > 2$ un primo y $a \in \mathbb{Q}_p \setminus \{0\}$ y estudiemos cuándo existe $\sqrt{a} \in \mathbb{Q}_p$.

Supongamos que $a = b^2$ y que $|a|_p = p^n$ y $|b|_p = p^m$, entonces debe ocurrir que $p^n = |b|_p^2 = p^{2m}$, es decir que $n = 2m$, de modo que una primera condición necesaria para la existencia de la raíz cuadrada de a es que su norma sea una potencia par de p.

Sea $c = p^n a \in \mathbb{Z}_p^\times$ y supongamos que $c = d^2$, entonces si llamamos $b = p^{-m} d$ tenemos que $b^2 = p^{-2m} d^2 = p^{-n} c = a$. Recíprocamente si $a = b^2$ y llamamos $d = p^m b$, entonces $d^2 = c$. Por lo cual basta analizar la existencia de raíces cuadradas para números en $\mathbb{Z}_p^\times$.

Sea $f(x) = x^2 - c \in \mathbb{Z}_p[x]$, notemos que cualquier raíz d de este polinomio debe estar en $\mathbb{Z}_p^\times$, y por lo tanto $f'(d) = 2d \not\equiv 0 \ (mod\ p)$. Es decir que si $d = e_0 + e_1 \times p + e_2 \times p^2 + \cdots \in \mathbb{Z}_p^\times$ es una raíz de $f(x)$, entonces

$e_0^2 - c = f(e_0) \equiv f(d) = 0 \ (mod\ p)$. De modo que la existencia de $\sqrt{c}$ es equivalente a la solubilidad de la congruencia $x^2 \equiv c \ (mod\ p)$. Queda demostrada la siguiente proposición.

Proposición 29. *Sea $p > 2$ un primo. Entonces, un número en $\mathbb{Q}_p$ tiene raíz cuadrada si y sólo si su norma es una potencia par de p y su primera cifra es congruente módulo p al cuadrado de alguna cifra.*

Observemos la siguiente tabla:

p	Cifras al cuadrado	Congruentes a
3	$1, 4$	1
5	$1, 4, 9, 16$	$1, 4$
7	$1, 4, 9, 16, 25, 36$	$1, 4, 2$
11	$1, 4, 9, 16, 25, 36, 49, 64, 81, 100$	$1, 4, 9, 5, 3$
13	$1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144$	$1, 4, 9, 3, 12, 10$
$\vdots$	$\vdots$	$\vdots$

Podemos decir por ejemplo que en $\mathbb{Q}_7$, los números cuya primera cifra sea $1, 4$ ó 2 y esté en una posición par tendrán raíz cuadrada, mientras que aquellos números cuya primera cifra sea $3, 5, 6$ ó que esté en una posición impar no tendrán raíz cuadrada.

Además recordando que $-1 = (p-1) + (p-1) \times p + (p-1) \times p^2 + \cdots$, podemos decir que $\sqrt{-1}$ existe en $\mathbb{Q}_5$ y en $\mathbb{Q}_{13}$, sin embargo no existe en $\mathbb{Q}_3, \mathbb{Q}_7$ ni en $\mathbb{Q}_{11}$.

A manera de ejercicio veamos cómo encontrar algunas cifras de $\sqrt{-1}$ en $\mathbb{Q}_5$ (recordemos que su expansión no puede ser periódica ya que no existe un racional que multiplicado por sí mismo dé como resultado -1).

Podemos empezar con 2 o con 3 ya que tanto 4 como 9 son congruentes módulo 5 a 4 que es la primera cifra de la expansión 5-ádica de -1. Empecemos con $b_0 = 2$, teniendo en cuenta que si empezáramos con 3 iríamos encontrando las cifras de la otra raíz cuadrada de -1.

$$\begin{aligned}
(2 + b_1 \times 5)^2 &\equiv 4 + 4b_1 \times 5 \equiv 4 + 4 \times 5 \ (mod\ 5^2) \\
&\Leftrightarrow 4b_1 \times 5 \equiv 4 \times 5 \ (mod\ 5^2) \\
&\Leftrightarrow 4b_1 \equiv 4 \ (mod\ 5) \\
&\Leftrightarrow b_1 \equiv 1 \ (mod\ 5)
\end{aligned}$$

$$\begin{aligned}
(2 + 1 \times 5 + b_2 \times 5^2)^2 &\equiv 4 + 4 \times 5 + (4b_2 + 1) \times 5^2 \ (mod\ 5^3) \\
&\equiv 4 + 4 \times 5 + 4 \times 5^2 \ (mod\ 5^3) \\
&\Leftrightarrow (4b_2 + 1) \times 5^2 \equiv 4 \times 5^2 \ (mod\ 5^3) \\
&\Leftrightarrow 4b_2 + 1 \equiv 4 \ (mod\ 5) \\
&\Leftrightarrow 4b_2 \equiv 3 \ (mod\ 5) \\
&\Leftrightarrow b_2 \equiv 4 \cdot 3 \equiv 2 \ (mod\ 5)
\end{aligned}$$

$$\begin{aligned}(2+1\times 5+2\times 5^2+b_3\times 5^3)^2 &\equiv 4+4\times 5+4\times 5^2+4b_3\times 5^3 \ (mod\ 5^4)\\ &\equiv 4+4\times 5+4\times 5^2+4\times 5^3 \ (mod\ 5^4)\\ &\Leftrightarrow 4b_3\times 5^3\equiv 4\times 5^3 \ (mod\ 5^4)\\ &\Leftrightarrow b_3\equiv 1 \ (mod\ 5)\end{aligned}$$

$$\begin{aligned}(2+1\times 5+2\times 5^2+1\times 5^3+b_4\times 5^4)^2 &\equiv 4+4\times 5+4\times 5^2+4\times 5^3+(4b_4+2)\times 5^4 \ (mod\ 5^5)\\ &\equiv 4+4\times 5+4\times 5^2+4\times 5^3+4\times 5^4 \ (mod\ 5^5)\\ &\Leftrightarrow (4b_4+2)\times 5^4\equiv 4\times 5^4 \ (mod\ 5^4)\\ &\Leftrightarrow 4b_4+2\equiv 4 \ (mod\ 5)\\ &\Leftrightarrow 4b_4\equiv 2 \ (mod\ 5)\\ &\Leftrightarrow b_4\equiv 4\cdot 2=8\equiv 3 \ (mod\ 5)\end{aligned}$$

Se puede continuar de esta manera para obtener la cantidad de cifras deseadas de

$$\sqrt{-1}=2+1\times 5+2\times 5^2+1\times 5^3+3\times 5^4+\cdots$$

o de

$$-\sqrt{-1}=3+4\times\ 5+3\times 5^2+4\times 5^3+2\times 5^4+\cdots$$

si hubieramos empezado con $b_0=3$.

A continuación veremos un criterio para verificar que un polinomio es irreducible.

Para ello consideremos la función $\varphi:\mathbb{Z}_p[x]\to {}^{\mathbb{Z}_p}/_{p\mathbb{Z}_p}[x]$ dada por

$$\varphi(a_0+a_1x+\cdots+a_nx^n)=\bar{a}_0+\bar{a}_1x+\cdots+\bar{a}_nx^n$$

donde $\bar{a}_i=a_i+p\mathbb{Z}_p$ es la clase de equivalencia de a_i en ${}^{\mathbb{Z}_p}/_{p\mathbb{Z}_p}$.

Recordando que los coeficientes de la suma de polinomios $f(x)+g(x)$ es la suma de los coeficientes de $f(x)$ y los de $g(x)$ y que los coeficientes del producto $f(x)g(x)$ son una suma de productos de coeficientes de $f(x)$ y $g(x)$, y como la proyección cociente es un homomorfismo de anillos, entonces φ es también un homomorfismo de anillos.

Teorema 30. *(Criterio de irreducibilidad de Eisenstein).*
Sea $f(x)=a_0+\ a_1x+\ \cdots+\ a_nx^n\in\ \mathbb{Z}_p[x]$ *tal que* $a_i\equiv 0\ (mod\ p)$ *para toda* $i\in\{0,1,\ldots,n-1\}$, $a_n\not\equiv 0\ (mod\ p)$ *y* $a_0\not\equiv 0\ (mod\ p^2)$. *Entonces* $f(x)$ *es irreducible en* $\mathbb{Q}_p[x]$.

Demostración. Basta demostrar que $f(x)$ es irreducible en $\mathbb{Z}_p[x]$.

Sean $g(x)=b_0+b_1x+\cdots+b_sx^s$ y $h(x)=c_0+c_1x+\cdots+c_rx^r$ polinomios en $\mathbb{Z}_p[x]$ tales que $f(x)=g(x)h(x)$, entonces $\bar{a}_nx^n=\varphi(f(x))=\ \varphi(g(x))\varphi(h(x))$.

Recordemos que si R es un dominio de factorización única, entonces $R[x]$ es un dominio de factorización única y como ${}^{\mathbb{Z}_p}/_{p\mathbb{Z}_p}$ es un campo, podemos

asegurar que todos los factores irreducibles de $\varphi(g(x))$ y de $\varphi(h(x))$ son de la forma ax.

Observemos que $gr(\varphi(g(x))) \leq s$, $gr(\varphi(h(x))) \leq r$ y además

$$gr(\varphi(g(x))) + gr(\varphi(h(x))) = gr(\varphi(f(x))) = n = r + s$$

donde gr es la función que a cada polinomio le asigna su grado. Entonces $gr(\varphi(g(x))) = s$ y $gr(\varphi(h(x))) = r$ y por lo tanto $\varphi(g(x)) = \bar{b}_s x^s$ y $\varphi(h(x)) = \bar{c}_r x^r$.

Así, si suponemos que $r, s > 0$ entonces $b_0 \equiv 0 \equiv c_0 \ (mod\ p)$ y por lo tanto $a_0 = b_0 c_0 \equiv 0 \ (mod\ p^2)$ lo que contradice nuestra hipótesis, entonces alguno de los polinomios $g(x)$ o $h(x)$ debe ser constante, es decir que $f(x)$ debe ser irreducible.

□

Una duda que podría surgir es si los espacios $\mathbb{Q}_p$ tienen o no la misma estructura algebraíca de campo para distintos primos p. A continuación veremos que esto nunca sucede, para ello vamos a estudiar cuántas raíces de la unidad hay en cada campo, es decir números que multiplicados por sí mismos algún número de veces den como resultado 1.

Sea $p > 2$ un primo y consideremos el polinomio $f(x) = x^p - x$, demostraremos que tiene sus p raíces en $\mathbb{Q}_p$. Una raíz es 0, las otras son las raíces $(p-1)$-ésimas de 1.

Sea $i \in \{0, 1, \ldots, p-1\}$, entonces $f'(i) = pi^{p-1} - 1 \equiv p - 1 \not\equiv 0 \ (mod\ p)$. Además, por el pequeño teorema de Fermat $i^p \equiv i \ (mod\ p)$, es decir que $f(i) \equiv 0 \ (mod\ p)$. Entonces por el lema de Hensel existen p raíces, $a_0, \ldots, a_{p-1}$, de $f(x)$ tales que $a_i \equiv i \ (mod\ p)$ para cada $i \in \{0, 1, \ldots, p-1\}$.

Ahora veamos que esas son todas las raíces de 1 en $\mathbb{Q}_p$. Notemos que cualquier raíz de 1 debe estar en $\mathbb{Z}_p^\times$.

Primero demostraremos que la única raíz de $x^p - 1$ en $\mathbb{Q}_p$ es 1. Considerando el polinomio $\frac{x^p-1}{x-1}$ y sustituyendo $x = y + 1$ tenemos que

$$\frac{x^p - 1}{x - 1} = \frac{(y+1)^p - 1}{y} = \frac{\sum_{k=0}^{p} \binom{p}{k} y^k - 1}{y} = \sum_{k=1}^{p} \binom{p}{k} y^{k-1}$$

y como $\binom{p}{k} \equiv 0 \ (mod\ p)$ para $k \in \{1, 2, \ldots, p-1\}$, $\binom{p}{p} = 1 \not\equiv 0 \ (mod\ p)$ y $\binom{p}{1} = p \not\equiv 0 \ (mod\ p^2)$, por el criterio de irreducibilidad de Eisenstein sabemos que $\sum_{k=1}^{p} \binom{p}{k} y^{k-1}$ es irreducible en $\mathbb{Q}_p[y]$.

Por lo tanto $\frac{x^p-1}{x-1}$ debe ser irreducible en $\mathbb{Q}_p[x]$, es decir que no existe ninguna raíz p-ésima de 1 en $\mathbb{Q}_p$, excepto 1.

Sea k un primo relativo de $p-1$ y supongamos que x^k-1 tiene alguna raíz distinta de 1. Si b_0 es la primera cifra de una de estas raíces, entonces $b_0^k \equiv 1 \ (mod\ p)$.

Como ${}^{\mathbb{Z}_p}\!/_{p\mathbb{Z}_p} \setminus \{0\}$ es un grupo multiplicativo cíclico de orden $p-1$, el orden de $\bar{b}_0$ debe ser un divisor de k y de $p-1$, y al ser primos relativos su orden es 1, es decir que $b_0 = 1$. Podemos concluir que la primera cifra de todas las raíces de x^k-1 es 1.

Ahora sea $r \in \mathbb{Z}^+$ y a una raíz de x^k-1 tal que

$$p^{-r} = |a-1|_p = \text{mín}\{|x-1|_p : x^k = 1, x \neq 1\},$$

escribimos $a = 1 + p^r c$ para alguna $c \in \mathbb{Z}_p^\times$ y consideremos a^p, que vuelve a ser una raíz k-ésima y $a^p \neq 1$ ya que $a \neq 1$.

Sin embargo observemos que $a^p = (1+p^r c)^p = 1 + p^{r+1}c + \sum_{i=2}^{p} \binom{p}{i} p^{ri} c^i$, entonces $|a^p - 1|_p = p^{-(r+1)} < |a-1|_p$ lo cual contradice nuestra elección de a.

Por lo tanto si k y $p-1$ son primos relativos, la única raíz k-ésima de 1 es precisamente 1.

Sea a una raíz k-ésima de 1, donde $k = nm$ y n es primo relativo con $p-1$, entonces $1 = a^k = a^{nm} = (a^m)^n$ y por lo tanto $a^m = 1$.

Juntando todo lo anterior, tan sólo nos resta analizar raíces k-ésimas de 1 donde k no tiene factores que sean primos relativos con $p-1$, en particular, como p y $p-1$ son primos relativos, debe cumplirse que $p \nmid k$.

Sea k un primo relativo de p, y observemos que cualquier raíz de x^k-1 también es una raíz de $f(x) = x^{k(p-1)} - 1$, ya que si $a^k = 1$ entonces $a^{k(p-1)} = (a^k)^{p-1} = 1^{p-1} = 1$.

Sea a una raíz de $f(x)$, entonces $f(a) = 0 \equiv 0 \ (mod\ p)$ y además notemos que $f'(a) = k(p-1)a^{k(p-1)-1} \not\equiv 0 \ (mod\ p)$, pero debe existir $i \in \{1, 2, \ldots, p-1\}$ tal que $a \equiv i \equiv a_i \ (mod\ p)$ y como $f(a_i) = 0$, por la unicidad en el lema de Hensel debe ocurrir que $a = a_i$ para alguna i, es decir que a debe ser una de las raíces $p-1$-ésimas de 1.

Podemos concluir que para $p > 2$, en $\mathbb{Q}_p$ hay exactamente $p-1$ raíces de 1, que son las raíces $(p-1)$-ésimas de 1.

Veamos ahora qué pasa en $\mathbb{Q}_2$.

Sabemos que 1 y $-1 = 1 + 1\times 2 + 1 \times 2^2 + 1 \times 2^3 + \cdots$, son raíces de 1, y supongamos que a es una raíz k-ésima distinta de 1 y -1 para alguna $k > 2$

y escojamos a de forma que $|a-1|_2 = p^{-r}$ sea mínima. Podemos escribir $a = 1 + c2^r$ para alguna $c \in \mathbb{Z}_2^\times$. Observemos que $a^2 = 1 + c2^{r+1} + c^2 2^{2r}$ es también una raíz k-esima de 1 y $|a^2 - 1|_2 \leq 2^{-(r+1)} < 2^{-r}$.

Como sólo pueden existir dos raíces cuadradas de 1, que son 1 y -1, entonces $a^2 \neq 1$ y además como $r + 1 \geq 2$, entonces la cifra de a^2 en la posición 2^1 es 0 y por lo tanto $a^2 \neq -1$, lo que contradice la elección de a. Podemos concluir que en $\mathbb{Q}_2$ las únicas raíces de 1 son 1 y -1.

Simplemente contando el número de raíces de 1 podemos observar que los campos $\mathbb{Q}_p$ para distintos primos p no son isomorfos, excepto quizá para los primos 2 y 3 donde tanto en $\mathbb{Q}_2$ y $\mathbb{Q}_3$ hay dos raíces de 1.

Para estos dos campos veamos un ejemplo sencillo. La expansión de 10 en $\mathbb{Q}_3$ es $10 = 1 + 0 \times 3 + 1 \times 3^2$ y revisando nuestra tabla podemos asegurar que existe una raíz cuadrada de 10 en $\mathbb{Q}_3$. Por otro lado en $\mathbb{Q}_2$ tenemos que $|10|_2 = 2^{-1}$, lo que implica que 10 no puede tener raíz cuadrada en $\mathbb{Q}_2$. Por lo tanto $\mathbb{Q}_2$ y $\mathbb{Q}_3$ no son isomorfos.

Teorema 31. *Sean p y q dos primos distintos. Entonces $\mathbb{Q}_p \ncong \mathbb{Q}_q$.*

3.4. Topología de $\mathbb{Q}_p$

Ahora estudiaremos un poco la topología de $\mathbb{Q}_p$. Un grupo topológico es un conjunto que tiene tanto estructura de grupo como de espacio topológico de forma que la operación de grupo y la inversión son funciones continuas, en particular un campo con la métrica inducida por una norma es un grupo topológico.

Los grupos topológicos son espacios con muchas propiedades, por ejemplo todo grupo topológico es homogéneo, es decir que para cualesquiera dos puntos x, y en el grupo, existe un homeomorfismo del grupo en sí mismo que manda x en y, es decir que la estructura topológica del espacio alrededor de uno u otro punto es indistinguible localmente. Para un mayor estudio de los grupos topológicos y sus propiedades que se aplican a $\mathbb{Q}_p$ se puede ver [7].

Cabe señalar en este contexto que en un campo con la métrica inducida por una norma las funciones que se obtienen de sumar una constante o de multiplicar por una constante distinta de cero son homeomorfismos.

Observemos que si $|x|_p < p^{n+1}$, como la norma no puede tomar ningún valor entre p^n y p^{n+1} se debe cumplir que $|x|_p \leq p^n$, por lo tanto

$$\{x \in \mathbb{Q}_p : |x|_p < p^{n+1}\} = \{x \in \mathbb{Q}_p : |x|_p \leq p^n\} = p^{-n}\mathbb{Z}_p.$$

Así una posible base para la topología de $\mathbb{Q}_p$ es $\{x + p^n\mathbb{Z}_p\}_{n\in\mathbb{Z}, x\in\mathbb{Q}_p}$ y cada uno de estos abiertos básicos es homeomorfo a $\mathbb{Z}_p$. Así tenemos que $\mathbb{Z}_p$ es abierto y cerrado en $\mathbb{Q}_p$. De hecho es compacto, como veremos a continuación.

Teorema 32. *$\mathbb{Z}_p$ es compacto.*

Demostración. Sea $(a_n)_{n\in\mathbb{N}}$ un sucesión de enteros p-ádicos y nos fijamos en la cifra en la posición p^0 de todos los términos y como solo hay p posibles cifras, debe existir una infinidad de términos que todos tengan la misma cifra en esta posición. Así tomamos una subsucesión $s_1 = (a_n^{(1)})_{n\in\mathbb{N}}$ tal que $a_n^{(1)} \equiv\ a_m^{(1)}\ (mod\ p)$ para todo n, m naturales.

Ahora, observando la cifra en la posición p^1 de los términos de la sucesión s_1, podemos tomar una subsucesión $s_2 = (a_n^{(2)})_{n\in\mathbb{N}}$, que también será subsucesión de la sucesión original, tal que $a_n^{(2)} \equiv a_m^{(2)}\ (mod\ p^2)$ para todo n, m naturales.

Continuando de esta forma podemos construir una infinidad de sucesiones $s_k =\ (a_n^{(k)})_{n\in\mathbb{N}}$ tales que:

1. s_{k+1} es una subsucesión de s_k,
2. $a_n^{(k)} \equiv a_m^{(k)}\ (mod\ p^k)$ para todo n, m naturales.

Consideremos la sucesión $s = (a_n^{(n)})_{n\in\mathbb{N}}$, que es una subsucesión de la sucesión original. Además como el término $a_k^{(k)}$ pertenece a la sucesión s_k y el término $a_{k+1}^{(k+1)}$ pertenece a la sucesión s_{k+1}, y por tanto a la sucesión s_k, se debe cumplir que $a_k^{(k)} \equiv a_{k+1}^{(k+1)}\ (mod\ p^k)$. Esto implica que s es una sucesión de Cauchy.

Como $\mathbb{Q}_p$ es un espacio métrico completo, s debe converger, y como $\mathbb{Z}_p$ es cerrado, el límite estará en $\mathbb{Z}_p$. Esto quiere decir que en $\mathbb{Z}_p$ cualquier sucesión tiene una subsucesión convergente, lo que en espacios métricos es equivalente a la compacidad.

□

Del hecho de que en cada punto existe una base local de conjuntos que son abiertos y cerrados a la vez, podemos concluir que los únicos subconjuntos conexos de $\mathbb{Q}_p$ son precisamente los conjuntos unitarios, es decir que $\mathbb{Q}_p$ es totalmente disconexo.

Todo subconjunto de $\mathbb{Q}_p$ también debe ser totalmente disconexo, en particular $\mathbb{Z}_p$ es totalmente disconexo. Analizando las expansiones p-ádicas de los números p-ádicos es fácil ver que $\mathbb{Z}_p$ no tiene puntos aislados, lo que junto con el hecho de que es un conjunto compacto y totalmente disconexo implica que es homeomorfo al conjunto de Cantor. La demostración de que todo espacio compacto, totalmente disconexo y sin puntos aislados es homeomorfo al conjunto de Cantor puede verse en [8].

Además podemos compactar el espacio $\mathbb{Q}_p$ agregando un punto al infinito, ∞ y haciendo que una base local para ∞ sea los conjuntos de la forma $\{\infty\} \cup \{x \in \mathbb{Q}_p : |x|_p > p^n\}$.

De esta forma el conjunto $\mathbb{Q}_p \cup \{\infty\}$ resulta ser compacto, además sigue siendo totalmente disconexo y perfecto, es decir que no tiene puntos aislados, con lo que podemos concluir que $\mathbb{Q}_p$ es homeomorfo al conjunto de Cantor menos un punto.

En la teoría de grupos topológicos son importantes lo subgrupos que son subconjuntos cerrados del espacio, veamos cómo son los subgrupos cerrados de $\mathbb{Q}_p$. Sea G un subgrupo cerrado no trivial de $\mathbb{Q}_p$. Tomemos algún elemento $a \in G \setminus \{0\}$ y digamos que la norma de a es $|a|_p = p^{-n}$.

Observemos que $p^k a \in G$ para cualquier $k \in \mathbb{N}$, ya que es la suma de p^k veces el elemento a consigo mismo, y además $|p^k a|_p = p^{-(k+n)}$. De forma que para cualquier $k \geq n$ existe $c \in G$ tal que $|c|_p = p^{-k}$. Además si d_k es la primera cifra distinta de cero de c, es decir que $c \equiv\ d_k \times\ p^k\ (mod\ p^{k+1})$, como p es un primo observemos que $d_k, 2d_k, \ldots, (p-1)d_k$ no pueden ser congruentes con 0 módulo p, sino que para cada $i \in \{1, \ldots, p-1\}$ debe existir $m \in \{1, \ldots, p-1\}$ tal que $md_k \equiv i\ (mod\ p)$.

Lo anterior quiere decir que para cualquier x cuya norma sea $|x|_p \leq p^{-k}$ con $k \geq n$ existe algún $y_k \in G$ tal que $x \equiv y_k\ (mod\ p^{k+1})$.

Ahora tenemos que $|x - y_k|_p \leq p^{-(k+1)}$ entonces existe $y_{k+1} \in G$ tal que $x - y_k \equiv y_{k+1}\ (mod\ p^{k+2})$, o lo que es lo mismo $x \equiv y_k + y_{k+1}\ (mod\ p^{k+2})$.

De esta forma para cualquier $N \geq k$ vamos tomando $y_k, y_{k+1}, \ldots, y_N \in G$ tales que $x \equiv \sum_{i=k}^{N} y_i\ (mod\ p^{N+1})$, de modo que $x = \sum_{i=k}^{\infty} y_i$, observando que $\sum_{i=k}^{N} y_i \in G$ para toda N y como G es cerrado podemos concluir que $x \in G$.

Por lo tanto $p^n\mathbb{Z}_p \subseteq G$, de forma que si G es acotado debe existir $r \in \mathbb{Z}$ tal que $G = p^r\mathbb{Z}_p$ y en caso de no ser acotado, entonces tenemos que $G = \mathbb{Q}_p$. Tenemos el siguiente teorema.

Teorema 33. *Los únicos subgrupos cerrados en $\mathbb{Q}_p$ son el total, el trivial y los grupos $p^n\mathbb{Z}_p$ con $n \in \mathbb{Z}$.*

Un grupo de Lie es un grupo topológico que además es una variedad, es decir, que como espacio topológico al rededor de cada punto es localmente homeomorfo a $\mathbb{R}^n$, para alguna n, y que tiene una estructura diferenciable, que hace que las operaciones del grupo no sean sólo continuas, sino que sean diferenciables. Una referencia para revisar esta definición con más detalle y estudiar algunos aspectos de los grupos de Lie es [13].

Veamos que $\mathbb{Z}_p$ no es un grupo de Lie. Supongamos que existe un abierto $U \subset \mathbb{Z}_p$ con $0 \in U$ tal que U es homeomorfa a $\mathbb{R}^n$ para alguna $n \geq 0$. Como $\mathbb{R}^n$ es conexo, entonces la componente de conexidad de 0 debe contener a U, pero, como $\mathbb{Z}_p$ es totalmente disconexo, la componente de conexidad de 0 es el conjunto $\{0\}$, y por lo tanto $U = \{0\}$.

Lo anterior implicaría que $\{0\}$ es un conjunto abierto y por lo tanto que la topología de $\mathbb{Z}_p$ es discreta, es decir que todos sus subconjuntos son abiertos, como esto no es el caso, entonces llegamos a una contradicción. Por lo tanto $\mathbb{Z}_p$ no es una variedad, y en particular no es un grupo de Lie.

Por último veamos una representación de $\mathbb{Z}_p$ como límite inverso de grupos finitos. Para estudiar más sobre límites inversos se puede ver [9].

Consideremos la sucesión inversa $\{{}^{\mathbb{Z}}/_{p^n\mathbb{Z}}, f_n : {}^{\mathbb{Z}}/_{p^{n+1}\mathbb{Z}} \to {}^{\mathbb{Z}}/_{p^n\mathbb{Z}}\}_{n\in\mathbb{N}}$, donde f_n es la proyección natural. Si $x \in \varprojlim\{{}^{\mathbb{Z}}/_{p^n\mathbb{Z}}, f_n\}_{n\in\mathbb{N}}$ significa que $x = (x_n)_{n\in\mathbb{N}}$ donde cada $x_n \in {}^{\mathbb{Z}}/_{p^n\mathbb{Z}}$ y $f_n(x_{n+1}) = x_n$.

Para cada $n \in \mathbb{N}$ podemos tomar un representante $a_n \in \{0, 1, \ldots, p^n - 1\}$ de x_n y $f(x_{n+1}) = x_n$ significa que $a_{n+1} \equiv a_n \ (mod\ p^n)$. Lo cual es exactamente una sucesión como la del Teorema 21 y reciprocamente cualquier sucesión como la del teorema da pie a un elemento único de $\varprojlim\{{}^{\mathbb{Z}}/_{p^n\mathbb{Z}}, f_n\}_{n\in\mathbb{N}}$.

Sólo falta ver la topología de $\varprojlim\{{}^{\mathbb{Z}}/_{p^n\mathbb{Z}}, f_n\}_{n\in\mathbb{N}}$, que es la heredada del producto $\prod_{n=1}^{\infty} {}^{\mathbb{Z}}/_{p^n\mathbb{Z}}$ en la que, como cada espacio es finito, las vecindades de un punto son los conjuntos de puntos que coinciden en una cantidad finita fija de coordenadas, lo cual en el límite inverso se convierte en que sean iguales hasta alguna coordenada, es decir que las primeras k cifras sean iguales, lo cual coincide con la topología de $\mathbb{Z}_p$, y por lo tanto $\mathbb{Z}_p \cong \varprojlim\{{}^{\mathbb{Z}}/_{p^n\mathbb{Z}}, f_n\}_{n\in\mathbb{N}}$.

Bibliografía

[1] Koblitz, Neal; *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Second Edition, Springer-Verlag New York Inc., USA, 1984.

[2] Niven, Ivan; Zuckerman, Herbet S.; Montgomery, Hugh L.; *An Introduction to the Theory of Numbers*, John Wiley and Sons, 5th edition, USA, 1991.

[3] Fraleigh, John B.; *Álgebra Abstracta Primer Curso*, Addison-Wesley Iberoamericana S.A., USA, 1987.

[4] Willard, Stephen; *General Topology*, Dover Publicationes Inc., USA, 2004.

[5] Wawrzyńczyk, Antoni; Delgado, Joaquín; *Introducción al Análisis*, Universidad Autónoma Metropolitana, Unidad Iztapalapa, México, 1993.

[6] Sagan, Hans; *Advanced Calculus: of Real-Valued Functions of a Real Variable and Vector-Valued Functions of a Vector Variable*, Houghton Mifflin Co, USA, 1974.

[7] Tkachenko, Mikhail; Villegas Silva, Luis Miguel; Hernández García, Constancio; Rendón Gómez, Oscar Jesús; *Grupos Topológicos*, Universidad Autónoma Metropolitana, Unidad Iztapalapa, México, 1997.

[8] Nadler, S.B.; *Continuum Theory: An Introduction*, Marcel Dekker, USA, 1992.

[9] Ingram, W.T.; *Inverse Limits*, Sociedad Matemática Mexicana, México, 2000.

[10] Hensel, Kurt; *Über eine Neue Begründung der Theorie der Algebraischen Zahlen*, Journal für die reine und angewandte Mathematik 128: 1-32, Alemania, 1905.

[11] Tao, Terence; *Hilbert's Fifth Problem and Related Topics*, Graduate Studies in Mathematics Vol. 153, American Mathematical Society, USA, 2014.

[12] Gouvêa, Fernando Q.; *A Marvelous Proof*, The American Mathematical Monthly Vol. 101 No. 3: 203-222, USA, 1994.

[13] Mimura, Mamoru; Toda, Hirosi; *Topology of Lie Groups, I and II*, Translations of Mathematical Monographs, American Mathematical Society, USA, 1991.