USC
UNIVERSIDADE
DE SANTIAGO
DE COMPOSTELA

FACULTADE DE MATEMÁTICAS

Trabajo Fin de Grado

Números p-ádicos

Pablo López Somoza

2018/2019

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

GRADO DE MATEMÁTICAS

Trabajo Fin de Grado

Números p-ádicos

Pablo López Somoza

Febrero, 2019

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Trabajo propuesto

Área de Conocimiento: Álgebra
Título: Números p-ádicos
Breve descripción del contenido
Los números p-ádicos fueron introducidos por el matemático alemán Kurt Hensel. La principal motivación de Hensel fue la analogía entre el anillo de los enteros $\mathbb{Z}$, junto con su cuerpo de fracciones $\mathbb{Q}$, y el anillo de polinomios $\mathbb{C}[X]$, con coeficientes complejos, junto con su cuerpo de fracciones $\mathbb{C}(X)$. El objetivo es introducir los enteros p-ádicos $\mathbb{Z}_p$ usando expansiones p-ádicas y el límite inverso; los números p-ádicos $\mathbb{Q}_p$ usando expansiones. También se introducirá la valoración p-ádica y el valor absoluto p-ádico. Finalmente, se estudiará la fórmula producto que relaciona el valor absoluto de $\mathbb{Q}$ con los valores absolutos p-ádicos, la definición formal de $\mathbb{Q}_p$ como completación de $\mathbb{Q}$ y el estudio de ideales y unidades de $\mathbb{Z}_p$. La motivación de este trabajo es conocer los números p-ádicos.

Índice general

Resumen

En matemáticas, hay números de todos los tipos: enteros, racionales, reales, complejos, p-ádicos, ... En este trabajo estudiaremos los números p-ádicos, los cuales fueron introducidos por el matemático alemán Kurt Hensel. Estos números son menos conocidos que los otros, pero tienen un papel muy importante en la teoría de números y en otras partes de las matemáticas.

A parte de la definición de número p-ádico, estudiaremos diferentes valores absolutos en diversos cuerpos. Estos valores absolutos tendrán una serie de propiedades que también cumplirá el valor absoluto p-ádico. Pero el cuerpo de los números racionales $\mathbb{Q}$ no será completo con este valor absoluto p-ádico, por lo que tendremos que construir un cuerpo más grande que sea completo con este valor absoluto. Este nuevo cuerpo será precisamente el cuerpo de los números p-ádicos. Una vez construido y definidas un par de propiedades, veremos como trabajar con algunos elementos de este cuerpo así como con los enteros p-ádicos.

Abstract

In mathematics, there are numbers of various types: integers, rationals, reals, complexes, p-adics, ... In this project we will study the p-adic numbers, which were introduced by the German mathematician Kurt Hensel. These numbers are less known than the others, but they have a very important role in number theory and other parts of mathematics.

Apart from the definition of a p-adic number, we will study different absolute values in different fields. These absolute values will have a series of properties that will also have the p-adic absolute value. However, the field of rational numbers $\mathbb{Q}$ will not be complete with respect to this p-adic absolute value, so we will have to build a larger field that is complete with this absolute value. This new field will precisely be the field of the p-adic numbers. Once we have constructed it and we have given some properties, we will see how to work with some elements of this field, as well as with the p-adic integers.

Introducción

Como todo en matemáticas, los números p-ádicos también tuvieron un principio.

Durante el siglo pasado, los números p-ádicos y el análisis p-ádico han desempeñado un papel importante en la teoría moderna de números. Su importancia radica en como permite expresar de manera natural las congruencias entre números enteros en términos de distancias, de esta manera podemos usar métodos del análisis para estudiar problemas de congruencias.

Hay varias formas de abordar el estudio de los números p-ádicos. Una es la forma original, estudiándolos como series de Laurent. Esta es la más antigua, ya que fue así como nacieron estos números. Otra manera de estudiarlos es usando la teoría de valores absolutos. Por último, también pueden ser estudiados mediante el uso de límites proyectivos. Cada una de ellas tendrá ventajas y desventajas.

Fueron introducidos por primera vez por el matemático alemán Kurt Hensel en 1987, donde los describe como series de potencias de Laurent, en analogía, como el mismo dice apenas iniciado su trabajo, entre los resultados de la teoría de funciones algebraicas en una variable y de los números algebraicos.

En 1910, Ernst Steinitz publicó su trabajo fundamental sobre teoría de cuerpos, citando a los números p-ádicos como su mayor motivación. En ese mismo año, gracias a los trabajos de Maurice Fréchet, Frigyes Riesz y otros, las ideas topológicas se vuelven mas claras, esto permite tener un mejor entendimiento de los números p-ádicos. Aún así, en este trabajo nos basaremos en los aspectos analíticos y algebraicos de los números p-ádicos.

En 1912, Kürschák define los valores absolutos. Esta nueva definición permite interpretar $\mathbb{Q}_p$ en términos de espacios métricos y topológicos. Hensel, a su vez, publicó varios trabajos y libros, en los que simplificó las teorías de divisibilidad en números algebraicos usando los números p-ádicos. Sin embargo, Hensel no usó la definición de Kürschák sobre valoraciones, pero introdujo límites y probó la completitud de $\mathbb{Q}_p$ sin mencionar las valoraciones. En 1917, Ostrowski enuncia el teorema de valores absolutos en $\mathbb{Q}$.

En 1921, Helmut Hasse propone y prueba en su tesis doctoral, el Principio Local-Global para estudiar la existencia o no de soluciones en $\mathbb{Q}$ de una ecuación diofántica a partir del estudio de las soluciones de la ecuación en $\mathbb{Q}_p$ para cada $p \leq \infty$.

Durante los años 1920 a 1935, se desarrolla la teoría completa de valores absolutos, gracias a los aportes de Deuring, Schmidt y Krull entre otros.

Actualmente, los números p-ádicos son utilizados en muchas áreas de la matemáticas, como son teoría de números, geometría algebraica, topología algebraica, análisis funcional, ecuaciones diferenciales y sistemas dinámicos. También son utilizados en física.

El contenido de este trabajo se divide en tres capítulos estructurados de la siguiente forma.
En el Capítulo 1, vemos la analogía de Hensel, la cual fue una de las principales motivaciones de sus estudios. Esta analogía se basa en la relación entre el anillo de enteros $\mathbb{Z}$ con su cuerpo de fracciones $\mathbb{Q}$, y la relación entre el anillo de polinomios con coeficientes complejos $\mathbb{C}[X]$ con su cuerpo de fracciones $\mathbb{C}(X)$. Continuaremos este capítulo con el desarrollo de los números racionales como series de Laurent en potencias del primo p y definiremos la expansión p-ádica de un número racional. A continuación, resolveremos congruencias módulo p^n y veremos como representar sus soluciones en diagramas en forma de árbol. Todo esto nos servirá para dar una idea general de lo que son los números p-ádicos, sin llegar a definir en ningún momento el cuerpo de los números p-ádicos. Por último, veremos un par de ejemplos relacionados con el análisis matemático y los cambios que obtenemos en algunos resultados al utilizar números p-ádicos.

Empezaremos el Capítulo 2 definiendo y viendo las propiedades de los valores absolutos. Una propiedad muy importante será la que nos indica si un valor absoluto es arquimediano o no. Definiremos el concepto de valoración p-ádica, el cual será, junto con otras propiedades, fundamental para definir el valor absoluto p-ádico. Una vez definido este, veremos que cumple todas las propiedades que definen un valor absoluto y veremos que es no arquimediano. Así, tendremos un valor absoluto para cada primo p, incluyendo el $+\infty$. Daremos también una caracterización directa para saber si un valor absoluto es arquimediano o no. Finalmente, veremos una serie de definiciones.

Por último, el Capítulo 3 contendrá algunos de los resultados más importantes de este trabajo. Empezaremos estudiando valores absolutos en el cuerpo $\mathbb{Q}$. Destacarán resultado como el Teorema de Ostrowski o la Fórmula del Producto. A continuación, nos basaremos en el hecho de que el cuerpo $\mathbb{Q}$ no es completo respecto al valor absoluto usual, pero

construiremos un cuerpo nuevo que si que será una buena completación de $\mathbb{Q}$. Definiremos el cuerpo de los números p-ádicos utilizando algunos conceptos del análisis matemático. Una vez definido el cuerpo de los números p-ádicos, tendremos un apartado dedicado a la aritmética p-ádica. Por último, daremos un par de pinceladas del Lema de Hensel y el Teorema de Hasse-Minkowski, así como del estudio de soluciones locales y globales de ecuaciones.

Capítulo 1

Preliminares

En este capítulo, nos basaremos en el libro [4].

1.1. La analogía de Hensel

Los números p-ádicos fueron estudiados por Ernst Eduard Kummer aunque fueron introducidos por primera vez por su discípulo Kurt Hensel. La principal motivación de Hensel era la analogía entre el anillo de enteros $\mathbb{Z}$ con su cuerpo de fracciones $\mathbb{Q}$, así como la analogía entre el anillo de polinomios con coeficientes complejos $\mathbb{C}[X]$, con su cuerpo de fracciones $\mathbb{C}(X)$. Recordemos que un elemento $f(X) \in \mathbb{C}(X)$ es una "función racional", es decir, un cociente de dos polinomios

$$f(X) = \frac{P(X)}{Q(X)},$$

con $P(X), Q(X) \in \mathbb{C}(X), Q(X) \neq 0$; de manera similar, cualquier número racional $x \in \mathbb{Q}$ es un cociente de dos enteros

$$x = \frac{a}{b},$$

con $a, b \in \mathbb{Z}, b \neq 0$. Además, las propiedades de los dos anillos son muy similares, tanto $\mathbb{Z}$ como $\mathbb{C}[X]$ son anillos de factorización única, es decir, cualquier entero de $\mathbb{Z}$ puede expresarse únicamente como un producto de primos salvo unidades, y cualquier polinomio de $\mathbb{C}[X]$ puede expresarse únicamente como

$$P(X) = a(X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n)$$

donde a y $\alpha_1, \alpha_2, \ldots, \alpha_n$ son números complejos. El motivo principal de la analogía que Hensel estudiaba era este, que los primos $p \in \mathbb{Z}$ son análogos a los polinomios lineales $X - \alpha \in \mathbb{C}[X]$.

Hensel se dio cuenta de que esta analogía va un poco más allá. Supongamos que tenemos un polinomio $P(X)$ y un $\alpha \in \mathbb{C}$ arbitrario. Así, podemos escribir su polinomio de Taylor del siguiente modo:

$$P(X) = a_0 + a_1(X-\alpha) + a_2(X-\alpha)^2 + \cdots + a_n(X-\alpha)^n = \sum_{i=0}^{n} a_i(X-\alpha)^i$$

con $a_i \in \mathbb{C}$. Esto también funciona para los enteros (nos restringiremos de momento a los positivos): dados un entero positivo m y un primo p arbitrarios, podemos escribir este entero "en base p", y obtenemos que

$$m = a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n = \sum_{i=0}^{n} a_i p^i$$

con $a_i \in \mathbb{Z}$ y $0 \leq a_i \leq p-1$.

La razón por la que estas expansiones son importantes es que nos dan información "local" sobre los polinomios y sobre los enteros. La expansión de un polinomio cualquiera en potencias de $(X-\alpha)$ nos muestra si $P(X)$ se anula en α, y con que orden. Análogamente, la expansión de un entero cualquiera "en base p" nos muestra si es divisible por ese primo p, y con que orden. Para verlo de manera más visual, pongamos un ejemplo. Cogemos el entero 72 y el primo $p = 3$, y ponemos en "base p" el entero 72 y esto nos da lo siguiente:

$$72 = 0 + 0 \times 3 + 2 \times 3^2 + 2 \times 3^3,$$

lo cual nos muestra que 72 es divisible por 3^2.

Veamos ahora que ocurre con los polinomios y sus cocientes. Tomemos $f(X) \in \mathbb{C}(X)$ y $\alpha \in \mathbb{C}$. Conociendo como son los elementos de $\mathbb{C}(X)$ y teniendo en cuenta que siempre podemos expandir un polinomio, tenemos que

$$f(X) = \frac{P(X)}{Q(X)} = a_{n_0}(X-\alpha)^{n_0} + a_{n_0+1}(X-\alpha)^{n_0+1} + \cdots = \sum_{i \geq n_0} a_i(X-\alpha)^i.$$

La expansión anterior es justamente la serie de Laurent de un polinomio, y en nuestro caso puede ser más fácil obtenerla mediante divisiones entre las expansiones de $P(X)$ y $Q(X)$. Aún así, obtener la serie de Laurent para un polinomio no es tan sencillo como obtener la expansión en "base p" de cualquier entero, ya que para la igualdad

$$f(X) = \frac{P(X)}{Q(X)} = \sum_{i \geq n_0} a_i(X-\alpha)^i,$$

puede haber diferentes situaciones:

- Podemos tener $n_0 < 0$, es decir, la serie comienza con un exponente negativo. Esto significa que α es una raíz de $Q(X)$ y no de $P(X)$ y que la multiplicidad de α como raíz de $Q(X)$ es mayor que la de $P(X)$. En este caso, diremos que $f(X)$ tiene un polo en α, de orden $-n_0$.
- La expansión puede ser no finita. De hecho, solo será finita si al expandir $f(X) = P(X)/Q(X)$ en potencias menores, $Q(X)$ resulta ser una potencia de $(X - \alpha)$.

Ejemplo 1.1. Tomemos la función racional

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

y miremos sus expansiones para diferentes α. Si $\alpha = 0$, tenemos

$$\frac{X}{X-1} = -X - X^2 - X^3 - \cdots$$

lo cual demuestra que $f(0) = 0$ con multiplicidad uno. Para $\alpha = 1$, tenemos

$$\frac{X}{X-1} = \frac{1 + X - 1}{X-1} = (X-1)^{-1} + 1$$

lo cual nos muestra que existe un polo de orden uno en $\alpha = 1$ (y también da un ejemplo de expansión finita). Por último, si cogemos $\alpha = 2$, donde no hay ningún polo y ningún cero, tenemos que

$$\frac{X}{X-1} = 2 - (X-2) + (X-2)^2 - (X-2)^3 + \cdots .$$

Hemos visto que cualquier función racional se puede extender a series de este tipo, en potencias de $(X - \alpha)$. Más adelante veremos que los ideales generados por los elementos de la forma $(X - \alpha)$ son exactamente los ideales primos del anillo $\mathbb{C}[X]$. Aún así, no todas las series provienen de una función racional. De hecho algunas series como la del $\sin(X)$, o la de la e^X no pueden ser expansiones de ninguna función racional.

Ahora bien, desde el punto de vista algebraico tenemos dos cuerpos: el cuerpo $\mathbb{C}(X)$ de todas las funciones racionales, y el que contiene todas las series de Laurent en potencias de $(X - \alpha)$, que denotaremos por $\mathbb{C}((X - \alpha))$. La aplicación

$$f(X) \mapsto \text{expansión sobre } (X - \alpha)$$

define la inclusión de cuerpos

$$\mathbb{C}(X) \hookrightarrow \mathbb{C}((X - \alpha)).$$

Obviamente, hay infinitas inclusiones de este tipo (una para cada α), y cada una de ellas contiene información "local" sobre como se comportan cada una de las funciones racionales cuando se aproximan a α.

La elección de α es análoga a la elección de un número primo p. Como ya hemos visto, conocemos el desarrollo de un entero m en "base p":

$$m = a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n$$

con $a_i \in \mathbb{Z}$, $0 \leq a_i \leq p-1$. Como en el caso de los polinomios, esto es una expresión finita.

Para pasar de enteros positivos a racionales positivos, simplemente hacemos lo mismo que en el otro caso, es decir, expandimos ambos numerador y denominador en potencias de p, y luego dividimos. Lo único con lo que tendremos que tener cuidado es "arrastrar" las potencias de p. La suma de dos de nuestros a_i, por ejemplo, puede ser más grande que p. Veamos el siguiente ejemplo para entenderlo mejor.

Ejemplo 1.2. Tomamos el número primo $p = 3$, y el número racional positivo $a/b = 24/17$. Desarrollamos ambos enteros 24 y 17 en base $p = 3$ y obtenemos

$$a = 24 = 0 + 2 \times 3 + 2 \times 3^2 = 2p + 2p^2$$

y

$$b = 17 = 2 + 2 \times 3 + 1 \times 3^2 = 2 + 2p + 2p^2.$$

Para no confundirnos y ya que $p = 3$, escribimos ambos desarrollos en función de p. Una vez hecho esto, dividimos formalmente y llegamos a que

$$\frac{a}{b} = \frac{24}{17} = \frac{2p + 2p^2}{2 + 2p + 2p^2} = p + p^3 + 2p^5 + p^7 + p^8 + 2p^9 + \cdots$$

Para comprobar que esta última igualdad es correcta, la multiplicamos por el desarrollo de 17 en base $p = 3$. Hay que tener en cuenta que $p = 3$ y que $p^3 + 2p^3 = 3p^3 = p \cdot p^3 = p^4$, y así con las sucesivas potencias. Dicho esto, tenemos que

$$\begin{aligned}
&(2 + 2p + p^2)(p + p^3 + 2p^5 + p^7 + p^8 + 2p^9 + \cdots) \\
&= 2p + 2p^2 + \underbrace{p^3 + 2p^3} + 2p^4 + p^5 + 4p^5 + 4p^6 + 2p^7 + 2p^7 + 2p^8 + 2p^8 + p^9 + 2p^9 + 4p^9 \cdots \\
&= 2p + 2p^2 + \underbrace{p^4 + 2p^4} + p^5 + 4p^5 + 4p^6 + 2p^7 + 2p^7 + 2p^8 + 2p^8 + p^9 + 2p^9 + 4p^9 + \cdots \\
&= 2p + 2p^2 + \underbrace{p^5 + p^5 + 4p^5} + 4p^6 + 2p^7 + 2p^7 + 2p^8 + 2p^8 + p^9 + 2p^9 + 4p^9 + \cdots \\
&= 2p + 2p^2 + \underbrace{2p^6 + 4p^6} + 2p^7 + 2p^7 + 2p^8 + p^9 + 2p^9 + 4p^9 + \cdots \\
&= 2p + 2p^2 + \underbrace{2p^7 + +2p^7 + 2p^7} + 2p^8 + 2p^8 + p^9 + 2p^9 + 4p^9 + \cdots \\
&= 2p + 2p^2 + \underbrace{2p^8 + 2p^8 + 2p^8} + p^9 + 2p^9 + 4p^9 + \cdots \\
&= \cdots \\
&= 2p + 2p^2.
\end{aligned}$$

Las potencias de p desaparecen "hacia la derecha", dejándonos solo $2p + 2p^2$.

Este proceso siempre funciona. Por lo tanto, para cada primo p, podemos escribir cualquier número racional a/b (positivo, de momento) de la siguiente forma

$$x = \frac{a}{b} = \sum_{n \geq n_0} a_n p^n.$$

En la igualdad anterior, el índice puede cambiar. Tenemos que $n_0 \geq 0$ si y solo si $p \nmid b$, y $n_0 > 0$ si y solo si $p \nmid b$ y $p \mid a$. De hecho, el número n_0 (que juega un papel parecido al orden de un cero o polo) muestra la "multiplicidad" de p en a/b, y podemos expresar x de la siguiente forma

$$x = p^{n_0} \frac{a_1}{b_1} \text{ con } p \nmid a_1 b_1.$$

Queda por ver ahora cómo conseguir el desarrollo de los números racionales negativos. Como nuestras series en potencias de p pueden ser multiplicadas, llegará con conocer el desarrollo para -1, el cual no es difícil de obtener. Para cualquier primo p, tenemos que

$$-1 = (p-1) + (p-1)p + (p-1)p^2 + (p-1)p^3 + \cdots .$$

Para ver que esto es correcto, le sumamos 1 al desarrollo y vemos que da 0:

$$\begin{aligned}
&\underbrace{1 + (p-1)} + (p-1)p + (p-1)p^2 + (p-1)p^3 + \cdots \\
=&\underbrace{p + (p-1)p} + (p-1)p^2 + (p-1)p^3 + \cdots \\
=&\underbrace{p^2 + (p-1)p^2} + (p-1)p^3 + \cdots \\
=&\cdots \\
=&0.
\end{aligned}$$

Una vez desarrollado todo esto, cabe destacar que lo más importante es que todo número racional x puede ser escrito como una "cola finita de una serie de Laurent en potencias de p", es decir

$$x = a_{n_0} p_{n_0} + a_{n_0+1}\, p_{n_0+1} + \cdots$$

("cola finita" se refiere al hecho de que la serie es finita hacia la izquierda, e infinita hacia la derecha). Nosotros llamaremos a esto la expansión p-ádica de x. Si x es un entero positivo, este expansión es en realidad su desarrollo en "base p".
Nótese que la expansión p-ádica de un número es única, mientras que la expansión decimal de un real no tiene por qué serlo. Por ejemplo, en [1], podemos ver

$$0.999\ldots = 1.000\ldots = 1.$$

Al igual que pasaba con $\mathbb{C}((X-\alpha))$, el conjunto de todas las colas finitas de las series de Laurent en potencias de p (es decir, de todas las expansiones p-ádicas) es también un cuerpo. Lo denotaremos como $\mathbb{Q}_p$, y lo llamaremos el cuerpo de los números p-ádicos. Como ocurría antes, podemos decir que la aplicación

$$x \mapsto \text{expansión } p\text{-ádica de } x$$

nos da la inclusión de cuerpos

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

Aunque no hemos visto que $\mathbb{Q}_p$ es estrictamente mayor que $\mathbb{Q}$, esto lo veremos más adelante.

Por el momento, hemos definido número p-ádico como una cola finita de una serie de Laurent en potencias de p. Esta no es la verdadera definición. En el Capítulo 3, veremos la correcta y construiremos el cuerpo $\mathbb{Q}_p$. Esta construcción será parecida a la del cuerpo de los números reales. Por ahora, a pesar de cual sea la definición de número p-ádico, lo más importante es que estas series deben converger, luego las potencias p^n deben hacerse más pequeñas a medida que n crece.

1.2. Resolución de congruencias módulo p^n

Los "números p-ádicos" que acabamos de construir están muy relacionados con la resolución de congruencias de potencias de módulo p. Veamos algunos ejemplos de esto.

Ejemplo 1.3. Empecemos por el caso más fácil, una ecuación que tiene soluciones en $\mathbb{Q}$

$$X^2 = 25.$$

Queremos resolverla módulo p^n para todo n, es decir, resolver las congruencias

$$X^2 \equiv 25 \ (\text{mód } p^n).$$

Nuestra ecuación sigue teniendo soluciones enteras: $X = \pm 5$. Esto automáticamente nos da una solución de la congruencia para cada n, concretamente $X \equiv \pm 5 \ (\text{mód } p^n)$ para todo n.

Ahora bien, intentemos entender estas soluciones desde el punto de vista p-ádico. Para hacer esto, tomamos $p = 3$. Reescribimos nuestras soluciones usando representantes de clases de los residuos entre 0 y $3^n - 1$ para las soluciones módulo 3^n.

La primera solución, $X = 5$, nos da:

$$\begin{aligned} X &\equiv 2 \text{ (mód 3)} \\ X &\equiv 5 = 2 + 3 \text{ (mód 9)} \\ X &\equiv 5 = 2 + 3 \text{ (mód 27)} \\ &\dots \end{aligned}$$

lo cual no cambia más, y esto nos da la expansión 3-ádica de esta solución $X = 5$:

$$X = 5 = 2 + 1 \times 3.$$

Para $X = -5$, realizamos el mismo proceso que antes. Sin embargo, los resultados que obtenemos son más interesantes ya que en esta ocasión

$$\begin{aligned} X &\equiv -5 \equiv 1 \text{ (mód 3)} \\ X &\equiv -5 \equiv 4 = 1 + 3 \text{ (mód 9)} \\ X &\equiv -5 \equiv 22 = 1 + 3 + 2 \times 9 \text{ (mód 27)} \\ X &\equiv -5 \equiv 76 = 1 + 3 + 2 \times 9 + 2 \times 27 \text{ (mód 81)} \\ &\dots \end{aligned}$$

Como antes, esto nos da la expansión 3-ádica de la solución $X = -5$, la cual es infinita:

$$X = -5 = 1 + 1 \times 3 + 2 \times 3^2 + 2 \times 3^3 + 2 \times 3^4 + \cdots$$

Cabe destacar que los dos sistemas de soluciones son "coherentes", en el sentido de que cuando consideramos, por ejemplo, $X = 76$ (la cual es solución módulo 3^4) y la reducimos a módulo 3^3, tenemos $X = 22$ (la cual es solución módulo 3^3).

La coherencia de estos dos sistemas de soluciones nos permite enunciar la siguiente definición:

Definición 1.4. Sea p un número primo, diremos que una sucesión de enteros α_n tales que $0 \leq \alpha_n \leq p^n - 1$ es coherente si, para todo $n \geq 1$, tenemos

$$\alpha_{n+1} \equiv \alpha_n \text{ (mód } p^n).$$

Si necesitamos enfatizar la elección del primo p, diremos que la sucesión es p-ádicamente coherente.

En todos estos problemas, podemos representar nuestras dos sucesiones coherentes de soluciones como ramas de un árbol, como vemos en la Figura 1.1. En este caso, es obvio que ambas sucesiones son coherentes puesto que son soluciones en $\mathbb{Z}$ (76 es congruente con 22 porque ambos son congruentes con -5). Lo importante es la conexión entre la expresión de las raíces como una sucesión coherente y la obtención de su expansión p-ádica.

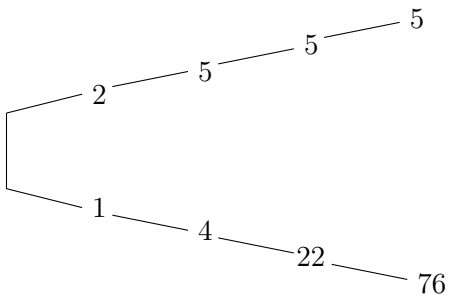


Figura 1.1: Soluciones de $X^2 \equiv 25 \pmod{3^n}$

Veamos ahora un ejemplo un poco más interesante, puesto que la ecuación que vamos a considerar ahora no tiene raíces racionales.

Ejemplo 1.5. Sea el sistema de congruencias

$$X^2 \equiv 2 \pmod{7^n}, \quad n = 1, 2, 3, \ldots$$

Para $n = 1$, las soluciones son $X \equiv 3 \pmod 7$ y $X \equiv 4 \equiv -3 \pmod 7$. Para encontrar las soluciones para $n = 2$, es decir, las soluciones módulo 7^2, utilizaremos el hecho de que las reducciones de sus soluciones módulo 7 tienen que ser soluciones para $n = 1$, es decir, soluciones módulo 7. Por eso, cogemos $X = 3 + 7k$ y $X = 4 + 7k$ y lo resolvemos para k:

$$\begin{aligned} (3 + 7k)^2 &\equiv 2 \pmod{49} \\ 9 + 42k &\equiv 2 \pmod{49} \end{aligned}$$

(al desarrollar el cuadrado de $(3 + 7k)^2$, es obvio que el sumando $(7k)^2$ es congruente con cero, por eso no lo ponemos)

$$\begin{aligned} 7 + 42k &\equiv 0 \pmod{49} \\ 1 + 6k &\equiv 0 \pmod 7 \\ k &\equiv 1 \pmod 7. \end{aligned}$$

Así, para este primer caso en el que $X = 3 + 7k$, y una vez obtenido el valor al que es congruente k, tenemos que la solución es $X \equiv 10 \pmod{49}$.
De manera análoga para la otra ecuación $X = 4+7k$, obtenemos la solución $X \equiv 39 \equiv -10 \pmod{49}$.

Como dijimos antes, estas soluciones pueden ser representadas como ramas de un árbol, como vemos en la Figura 1.2.

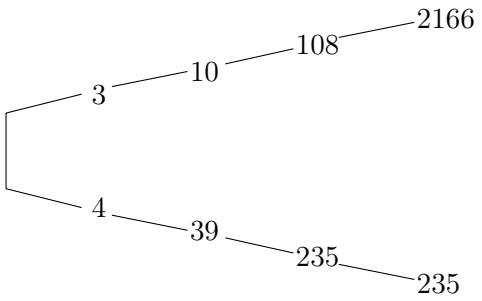


Figura 1.2: Soluciones de $X^2 \equiv 2$ (mód 7^n)

Aunque ya hemos visto dos ejemplos en los que hemos calculado las soluciones de las ecuaciones y las hemos representado en un diagrama en forma de árbol, no podemos predecir a priori cuales serán las soluciones que aparecerán. Lo único que podemos hacer es convencernos de que este proceso de cálculo de soluciones puede ser tan largo como queramos. El hecho de que uno pueda seguir calculando raíces indefinidamente muestra que hay dos sucesiones coherentes de soluciones que son infinitas:

$$x_1 = (3, 10, 108, 2166, \dots)$$

y

$$x_2 = (4, 39, 235, 235, \dots) = (-3, -10, -108, -2166, \dots) = -x_1.$$

Podemos expandir cada número en un sucesión 7-ádica. El hecho de obtener una sucesión coherente significa que la expansión de cada raíz se corresponde con el truncamiento de la expansión de la siguiente.

$$\begin{aligned} 3 &= 3 \\ 10 &= 3 + 1 \times 7 \\ 108 &= 3 + 1 \times 7 + 2 \times 49. \end{aligned}$$

Lo que realmente hemos obtenido, es la expresión de dos números 7-ádicos:

$$x_1 = 3 + 1 \times 7 + 2 \times 49 + 6 \times 343 + \cdots$$

y

$$x_2 = 4 + 5 \times 7 + 4 \times 49 + 0 \times 343 + \cdots = -x_1.$$

Como comentamos antes, no estamos intentando conseguir un patrón para saber como construir estos números. Lo único que estamos mostrando con estos ejemplos es que este proceso de obtención de raíces puede ser tan largo como queramos. Es como buscar la

expansión decimal de la raíz cuadrada de 2, nos podemos acercar tanto como queramos, pero no podemos predecir cual será la expansión.

En cualquier caso, hemos encontrado dos números 7-ádicos, y ambos son raíces de la ecuación $X^2 = 2$ en $\mathbb{Q}_7$.

Por todo esto, hemos visto que la relación entre resolver congruencias módulo potencias de p cada vez más grandes, y resolver la correspondiente ecuación en $\mathbb{Q}_p$, es muy parecida. De hecho, esta es una de las razones por las cuales el uso de métodos p-ádicos es muy importante en la teoría de números.

1.3. Otros ejemplos

En esta sección daremos un par de ejemplos que mostrarán la importancia y la gran utilidad de trabajar con números p-ádicos en diversos contextos.

Ejemplo 1.6. Consideramos la ecuación $X = 1 + 3X$. La solución de esta es obvia. Sin embargo, consideraremos este como un problema de punto fijo, es decir, como un problema en el que tendremos que encontrar para una función $f(x)$ una solución del tipo $f(x) = x$. Estos problemas de punto fijo, se resuelven normalmente iterando, empezando en un valor arbitrario inicial, y calculando $f(x)$ una y otra vez hasta que nos acerquemos al punto fijo. En este caso, tomamos $x_0 = 1$ como punto inicial e iteramos, por lo que obtenemos $x_{n+1} = 1 + 3x_n$. Así, nos queda

$$\begin{aligned} x_0 &= 1, \\ x_1 &= 1 + 3x_0 = 1 + 3, \\ x_2 &= 1 + 3x_1 = 1 + 3 + 3^2, \\ &\cdots \\ x_n &= 1 + 3x_{n-1} = 1 + 3 + 3^2 + \cdots + 3^n. \end{aligned}$$

En $\mathbb{R}$, esto es una serie divergente, aunque también es una sucesión de sumas parciales de una serie geométrica, y sabemos que su suma para $|a| < 1$ es

$$1 + a + a^2 + a^3 + \cdots = \frac{1}{1-a}$$

Así, usando el mismo razonamiento para nuestra serie

$$1 + 3 + 3^2 + \cdots + 3^n$$

llegamos a que

$$1 + 3x_{n-1} = 1 + 3 + 3^2 + \cdots + 3^n = \frac{1}{1-3} = -\frac{1}{2}$$

lo cual, sorprendentemente, es correcto.

Sin embargo, aunque lo anterior funciona y nos da un resultado correcto, no se puede hacer. Mientras que la serie es divergente en $\mathbb{R}$, nada nos dice que no podamos considerar esta serie en $\mathbb{Q}_3$ (ya que los elementos están en $\mathbb{Q}$, y este está contenido en $\mathbb{R}$ y en $\mathbb{Q}_3$). Por eso, como la consideramos en $\mathbb{Q}_3$, tenemos que la serie es convergente, y converge al número 3-ádico

$$1 + 3 + 3^2 + \cdots + 3^n + \cdots .$$

Una vez comprobada la convergencia de la serie, podemos ver, usando el mismo argumento que en $\mathbb{R}$, que su suma es igual a $-1/2$.

Obviamente, resolver de esta forma ecuaciones lineales como estas es extraño, pero lo más curioso es que la serie considerada era divergente al pensar en ella como serie de números reales. Sin embargo, al considerarla en otro cuerpo, como el cuerpo de los números p-ádicos, pasó a ser convergente. De hecho, veremos en el siguiente capítulo que hay un valor absoluto en $\mathbb{Q}_3$ (en general en $\mathbb{Q}_p$), y este valor absoluto nos servirá para ver que algunos tipos de series como estas son convergentes.

Con lo que nos tenemos que quedar es que al introducir el cuerpo de los números p-ádicos, las cosas que en otro cuerpo pueden parecer obvias, pueden cambiar al considerarlas en otro cuerpo distinto que antes no usábamos. El ejemplo anterior es un buen ejemplo de como usar números p-ádicos simplifica algunos casos.
Veamos ahora otro ejemplo un poco más interesante. Muestra que utilizar conceptos p-ádicos permite demostrar de manera más sencilla cosas que son difíciles de demostrar.

Ejemplo 1.7. Tomamos $p = 2$, es decir, estamos en el cuerpo $\mathbb{Q}_2$ de los números 2-ádicos. Consideramos la serie (polinomio) de MacLaurin para el logaritmo de $1 + X$:

$$\log(1 + X) = X - \frac{X^2}{2} + \frac{X^3}{3} - \frac{X^4}{4} + \cdots$$

Como las potencias de 2 son "pequeñas" en $\mathbb{Q}_2$, resulta que sustituyendo $X = -2$ tenemos el logaritmo de -1

$$\begin{aligned}\log(-1) = \log(1-2) &= -2 - \frac{(-2)^2}{2} + \frac{(-2)^3}{3} - \frac{(-2)^4}{4} + \cdots = -2 - \frac{2^2}{2} - \frac{2^3}{3} - \frac{2^4}{4} - \cdots \\ &= -\Big(2 + \frac{2^2}{2} + \frac{2^3}{3} + \frac{2^4}{4} + \cdots\Big).\end{aligned}$$

Esta serie es divergente en $\mathbb{R}$, pero convergente en $\mathbb{Q}_2$. Ahora bien, si la serie converge, debe converger a cero, por las propiedades usuales de los logaritmos, en concreto porque $\log(a)^b = b\log(a)$, con lo cual:

$$2\log(-1) = \log(-1)^2 = \log(1) = 0.$$

Esto significa que la suma parcial

$$2 + \frac{2^2}{2} + \frac{2^3}{3} + \frac{2^4}{4} + \cdots + \frac{2^n}{n}$$

se acerca más y más a cero a medida que n crece. Los términos en la expansión 2-ádica "desaparecen hacia la derecha", es decir, que la suma parcial, escrita en base 2, empieza con muchísimos ceros.

Lo que estos ejemplos nos muestran es que, usando métodos p-ádicos, y en particular, métodos de cálculo en un contexto p-ádico, podemos probar hechos sobre la multiplicidad de potencias de p.

Por último, resumimos la analogía entre las funciones complejas y los números p-ádicos en la Tabla 1.1, que podemos encontrar en [7]. Muchos de los conceptos definidos en ella serán trabajados en capítulos posteriores.

$\mathbb{C}$: espacio de puntos	$\mathcal{P} = \{p\}$: conjunto de primos
$\mathbb{C}[x]$: polinomios sobre $\mathbb{C}$	$\mathbb{Z}$: "polinomios" sobre $\mathcal{P}$
funciones analíticas en p_0 $f(x) = \sum_{i=0}^{\infty} a_i(x-p_0)^i$	$\mathbb{Z}_p$: enteros p-ádicos $n = \sum_{i=0}^{\infty} a_i p^i$
funciones meromorfas en p_0 $f(x) = \sum_{i=-k}^{\infty} a_i(x-p_0)^i$	$\mathbb{Q}_p$: números p-ádicos $n = \sum_{i=-k}^{\infty} a_i p^i$

Tabla 1.1: Funciones complejas versus los números p-ádicos

Capítulo 2

Fundamentos

Seguiremos en este capítulo tomando como referencia el libro [4]. El objetivo en este capítulo es empezar a elaborar unos fundamentos sólidos para la teoría que describimos en el Capítulo 1. La principal idea será la de introducir diferentes funciones que definan diferentes valores absolutos en el cuerpo de los números racionales. Esto nos dará una nueva forma de medir distancias. Una vez tengamos esto, lo utilizaremos para construir los números p-ádicos (los cuales serán construidos en el Capítulo 3).

Para construir los números p-ádicos, necesitamos empezar considerando el cuerpo de los números racionales $\mathbb{Q}$. Aunque el cuerpo más importante que tenemos que estudiar es $\mathbb{Q}$, en este capítulo estudiaremos valores absolutos en todo tipo de cuerpos, y después nos restringiremos a $\mathbb{Q}$.

Por tanto, tendremos un cuerpo arbitrario $\mathbb{K}$, y a partir de el, definiremos valores absolutos en $\mathbb{K}$. Empezaremos haciendo esto basándonos en las propiedades básicas que conocemos de los valores absolutos, y luego estudiaremos otras funciones con propiedades similares.

Una vez definidos nuestros nuevos valores absolutos, tendremos una nueva forma de medir el "tamaño" de los elementos de nuestro cuerpo. Para verlo mejor, daremos ejemplos.

2.1. Valores absolutos en un cuerpo

Sea $\mathbb{K}$ un cuerpo arbitrario. Empecemos definiendo un valor absoluto en $\mathbb{K}$.

Definición 2.1. Un valor absoluto en $\mathbb{K}$ es una función

$$|\cdot| : \mathbb{K} \longrightarrow \mathbb{R}^+$$

que verifica las siguientes propiedades:

(I) $|x| = 0$ si y solo si $x = 0$;

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

(III) $|x + y| \leq |x| + |y|$ para todo $x, y \in \mathbb{K}$.
Diremos que un valor absoluto en $\mathbb{K}$ es no arquimediano cuando satisface la siguiente condición adicional

(IV) $|x + y| \leq \text{máx}\{|x|, |y|\}$ para todo $x, y \in \mathbb{K}$;

en otro caso, diremos que el valor absoluto es arquimediano.

Notemos que la condición (IV) implica la condición (III), ya que $\text{máx}\{|x|, |y|\}$ es más pequeño que la suma $|x| + |y|$. Veremos después el motivo por el cual los valores absolutos no arquimedianos son importantes, y veremos que son bastante comunes. Veamos ahora un par de ejemplos:

Ejemplo 2.2. Cogemos $\mathbb{K} = \mathbb{Q}$, y tomamos el valor absoluto usual $|\ |$ definido por

$$|x| = \begin{cases} x & \text{si } x \geq 0, \\ -x & \text{si } x < 0. \end{cases}$$

Este es el valor absoluto definido en el cuerpo de los números reales $\mathbb{R}$, aplicado a $\mathbb{Q}$ a través de la inclusión $\mathbb{Q} \hookrightarrow \mathbb{R}$. Es fácil ver que este valor absoluto es arquimediano (cogemos $x = y = 1$ y la condición (IV) no se cumple). Este valor absoluto en $\mathbb{Q}$ se llamará valor absoluto en el infinito y se denotará por $|\ |_\infty$.

Ejemplo 2.3. Cogemos ahora $|x| = 1$ si $x \neq 0$ y $|0| = 0$. Esto funciona para cualquier cuerpo $\mathbb{K}$, y define un valor absoluto no arquimediano. Es conocido como el valor absoluto trivial.

A continuación introduciremos el ejemplo principal y más importante de este trabajo. Tomamos $\mathbb{K} = \mathbb{Q}$, y elegimos un primo $p \in \mathbb{Z}$. Cualquier entero $n \in \mathbb{Z}$ puede escribirse como $n = p^v n'$, con $p \nmid n'$, y esta representación es única. Como v está determinado por p y n, definimos una función v_p de la siguiente forma, $v_p(n) = v$. Vemos claramente que $v_p(n)$ indica la multiplicidad de p como divisor de n. Todo esto, se puede definir de una manera más formal de la siguiente forma:

Definición 2.4. Sea $p \in \mathbb{Z}$ un número primo fijado. Llamaremos valoración p-ádica en $\mathbb{Z}$ a la función

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

tal que para cada entero $n \in \mathbb{Z} - \{0\}$, $v_p(n)$ es el único entero positivo tal que

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

Extendemos v_p al cuerpo de los números racionales de la siguiente forma. Denotamos por $\mathbb{Q}^*$ a todos los enteros menos el cero. Si $x = a/b \in \mathbb{Q}^*$, entonces

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

Es conveniente establecer que $v_p(0) = +\infty$. La razón es que podemos dividir 0 por p, y el resultado es 0, lo cual podemos volver a dividir por p, y vuelve a dar 0, lo cual podemos dividir por p y así sucesivamente. Por eso establecemos que $v_p(0) = +\infty$.

De hecho, es fácil ver que la valoración p-ádica de cualquier $x \in \mathbb{Q}^*$ es de la forma

$$x = p^{v_p(x)} \cdot \frac{a}{b} \text{ con } p \nmid ab.$$

Las propiedades básicas de una valoración p-ádica v_p son las siguientes:

Lema 2.5. *Para todo $x, y \in \mathbb{Q}$, tenemos*

1. $v_p(xy) = v_p(x) + v_p(y)$;
2. $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$;

con el criterio habitual respecto a $v_p(0) = +\infty$.

Ahora bien, si comparamos la propiedad 2 de este lema con la propiedad (IV) de la definición de valores absolutos, vemos que son muy parecidas, excepto que el producto en la primera se ha convertido en una suma en la segunda, y que la desigualdad es en el otro sentido. Para que se parezcan más, podemos darle la vuelta cambiando el signo, y después convertir la suma en un producto poniendo un exponente. Todo esto nos sugiere lo siguiente:

Definición 2.6. Para cualquier $x \in \mathbb{Q}$, definimos el valor absoluto p-ádico como

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

Cabe destacar que la definición de $|0|_p$ concuerda con $v_p(0) = +\infty$ si interpretamos $p^{-\infty}$ de la única manera posible.

Proposición 2.7. *La función $|\ |_p$ es un valor absoluto no arquimediano en $\mathbb{Q}$.*

Demostración. Todo se sigue del Lema 2.3. En primer lugar, para ver que $|\ |_p$ es un valor absoluto, tenemos que mirar que cumple las tres propiedades que lo definen

1. Veamos que $|x|_p = 0$ si y solo si $x = 0$.
   Lo veremos por contrarrecíproco, si $x \neq 0$, entonces $|x|_p = p^{-v_p(x)} \neq 0$.
   Por otro lado, si $x = 0$, $|x|_p = |0|_p = 0$ por la definición de valor absoluto p-ádico.

2. Veamos que $|xy|_p = |x|_p + |y|_p$ para todo $x, y \in \mathbb{Q}$.
   Por definición, tenemos que

   $$|xy|_p = p^{-v_p(xy)} = p^{-(v_p(x)+v_p(y))} = p^{-v_p(x)-v_p(y)} = p^{-v_p(x)}p^{-v_p(y)} = |x|_p + |y|_p$$

   utilizando el Lema 2.5.

3. Por último, tenemos que ver que $|x + y|_p \leq |x|_p + |y|_p$.
   Por el Lema 2.5, tenemos que $v_p(x + y) \geq \text{mín}\{v_p(x), v_p(y)\}$, lo cual es equivalente a, $-v_p(x + y) \leq -\text{mín}\{v_p(x), v_p(y)\}$, y podemos elevar p a estas potencias y nos queda, $p^{-v_p(x+y)} \leq p^{-\text{mín}\{v_p(x),v_p(y)\}}$. La desigualdad sigue cumpliéndose puesto que, $p^{-v_p(x+y)} = e^{-v_p(x+y)\log(p)}$ y $p^{-\text{mín}\{v_p(x),v_p(y)\}} = e^{-\text{mín}\{v_p(x),v_p(y)\}\log(p)}$, y la función exponencial es una función monótona creciente. Luego, hemos llegado a que

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

Luego, ya hemos probado que $|\ |_p$ es un valor absoluto. Nos queda ver que es no arquimediano, es decir que cumple la siguiente desigualdad

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

Vamos a demostrarlo, utilizando el Lema 2.5 y razonando igual que en la demostración de la tercera propiedad de valor absoluto tenemos que

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

Por lo tanto, $|\ |_p$ es un valor absoluto no arquimediano. □

Para tener una visión más global del valor absoluto p-ádico, es interesante darse cuenta de que cuanto más divisible por p sea un número n, más grande será su valoración p-ádica $v_p(n)$, y su valor absoluto $|n|_p$ será más pequeño (debido al signo menos del exponente). Por tanto, el valor absoluto p-ádico nos da una medida de como de divisible es un número por p.

La relación entre un valor absoluto no arquimediano y una función como la definida en el Lema 2.5 (funciones a las cuales llamaremos valoraciones) es muy grande. Uno puede

estudiar todos estos problemas tomando valores absolutos o valoraciones, pero nosotros nos basaremos en los valores absolutos.

Aunque el valor absoluto más importante para nosotros es el valor absoluto p-ádico, en otros cuerpos hay valores absolutos muy importantes.

El siguiente ejemplo que vamos a dar, muestra que esta teoría es muy general y que se puede aplicar en numerosos contextos. También nos sirve para entender mejor la analogía que estudió Hensel entre $\mathbb{Q}$ y los cuerpos de funciones racionales. Luego, sea $\mathbb{F}$ un cuerpo arbitrario (por ejemplo $\mathbb{C}$), y sea $\mathbb{F}(t)$ el cuerpo de funciones racionales sobre $\mathbb{F}$. Hay que recordar que los elementos del cuerpo $\mathbb{F}(t)$, son fracciones de la forma $f(t)/g(t)$ donde $f(t), g(t) \in \mathbb{F}[t]$ y $g(t) \neq 0$. Ahora definiremos una valoración para cada polinomio, y después definiremos un valor absoluto. Nos basaremos en el grado del polinomio y en el valor absoluto p-ádico, respectivamente.

Primero, para cualquier polinomio $f(t)$, definimos $v_\infty(f) = -\deg(f(t))$, y extendemos esto a fracciones racionales igual que hicimos antes, es decir,

$$\begin{aligned} v_\infty\Big(\frac{f}{g}\Big) &= v_\infty(f(t)) - v_\infty(g(t)) = -\deg(f(t)) - [-\deg(g(t))] \\ &= \deg(g(t)) - \deg(f(t)). \end{aligned}$$

Una vez definida esta valoración en este cuerpo, tenemos un valor absoluto no arquimediano justo como hicimos antes:

$$|f(t)|_\infty = e^{-v_\infty(f)}$$

para cualquier $f(t) \in \mathbb{F}(t)$.

Esta valoración no es la única que podemos tener en $\mathbb{F}(t)$. Como sabemos que $\mathbb{F}[t]$ es un dominio de factorización única, basta con coger un polinomio irreducible $p = p(t)$ y en vez de definir la valoración a partir del grado del polinomio, la podemos definir contando la multiplicidad de $p(t)$ como un factor. Luego, seguimos el mismo proceso que hicimos antes y obtendremos otro valor absoluto diferente.

Vamos ahora a trabajar con valores absolutos más generales y sus propiedades básicas, sin olvidarnos de estos ejemplos anteriores, y sobre todo, sin olvidarnos del valor absoluto p-ádico que acabamos de definir.

2.2. Propiedades básicas

En esta sección, $\mathbb{K}$ será un cuerpo arbitrario, y $|\ |$ un valor absoluto no trivial en $\mathbb{K}$, el cual podrá ser arquimediano o no arquimediano.

Lema 2.8. *Para cualquier valor absoluto $|\ |$ en cualquier cuerpo $\mathbb{K}$, tenemos*

(I) $|1| = 1$*;*

(II) *si* $x \in \mathbb{K}$ *y* $|x^n| = 1$*, entonces* $|x| = 1$*;*

(III) $|-1| = 1$*;*

(IV) *para cualquier* $x \in \mathbb{K}$*,* $|-x| = |x|$*;*

(V) *si* $\mathbb{K}$ *es un cuerpo finito, entonces* $|\ |$ *es trivial.*

Antes de enunciar el siguiente teorema, el cual nos dará una condición suficiente y necesaria para que un valor absoluto sea no arquimediano, recordaremos que para cualquier cuerpo $\mathbb{K}$, podemos definir una función $\mathbb{Z} \longrightarrow \mathbb{K}$ de la siguiente forma

$$n \mapsto \begin{cases} \underbrace{1+1+\cdots+1}_{n} & \text{si } n > 0, \\ 0 & \text{si } n = 0, \\ -\underbrace{(1+1+\cdots+1)}_{-n} & \text{si } n < 0. \end{cases}$$

Por ejemplo, si $\mathbb{Q} \subset \mathbb{K}$, esta función nos define la inclusión de $\mathbb{Z}$ en $\mathbb{Q}$. Sin embargo, si $\mathbb{K}$ es un cuerpo finito, la imagen es un subconjunto de $\mathbb{K}$, el cual tendrá un número primo de elementos.

Teorema 2.9. *Sea* $\mathbb{A} \subset \mathbb{K}$ *la imagen de* $\mathbb{Z}$ *en* $\mathbb{K}$*. Un valor absoluto* $|\ |$ *en* $\mathbb{K}$ *es no arquimediano si y solo si* $|a| \leq 1$ *para todo* $a \in \mathbb{A}$*. En particular, un valor absoluto en* $\mathbb{Q}$ *es no arquimediano si y solo si* $|n| \leq 1$ *para todo* $n \in \mathbb{Z}$*.*

Demostración. En primer lugar, supongamos que $|\ |$ es un valor absoluto no arquimediano y probemos que $|a| \leq 1$ para todo $a \in \mathbb{A}$.
Tenemos que $|\pm 1| = 1$, y como el valor absoluto es no arquimediano en $\mathbb{A}$, se cumple que $|x \pm y| \leq \text{máx}\{|x|, |y|\}$ para todo $x, y \in \mathbb{A}$, en particular, se cumple que

$$|a \pm 1| \leq \text{máx}\{|a|, |1|\}.$$

Por inducción, se sigue que $|a| \leq 1$ para todo $a \in \mathbb{A}$.

Veamos ahora la otra implicación: supongamos en este caso que $|a| \leq 1$ para todo $a \in \mathbb{A}$. Queremos demostrar que el valor absoluto es no arquimediano, es decir, que dados dos elementos cualesquiera $x, y \in \mathbb{K}$, tenemos que $|x + y| \leq \text{máx}\{|x|, |y|\}$. Si $y = 0$, la condición se cumple y ya hemos acabado. Si $y \neq 0$, podemos dividir toda la expresión por $|y|$, y vemos que la ecuación anterior es equivalente a esta otra

$$\left|\frac{x}{y} + 1\right| \leq \text{máx}\left\{\left|\frac{x}{y}\right|, 1\right\}.$$

Luego, solo tenemos que probar esta última desigualdad para ver que el valor absoluto es no arquimediano, es decir, tenemos que ver que

$$|x+1| \leq \text{máx}\{|x|, 1\}.$$

Sea m cualquier entero positivo. Tenemos que

$$\begin{aligned} |x+1|^m &= \Big|\sum_{k=0}^{m} \binom{m}{k} x^k\Big| \\ &\leq \sum_{k=0}^{m} \Big|\binom{m}{k}\Big| \, |x^k|. \end{aligned}$$

Por hipótesis, como $\binom{m}{k}$ es un entero, tenemos que $\left|\binom{m}{k}\right| \leq 1$. Luego

$$\begin{aligned} |x+1|^m &\leq \sum_{k=0}^{m} \Big|\binom{m}{k}\Big| \, |x^k| \\ &\leq \sum_{k=0}^{m} |x^k| = \sum_{k=0}^{m} |x|^k \\ &\leq (m+1)\,\text{máx}\{1, |x|^m\}. \end{aligned}$$

Para este último paso, hemos utilizado que el valor más alto que puede tomar $|x|^k$, para $k = 0, 1, 2, \ldots, m$, es $|x|^m$ si $|x| > 1$ o 1 en otro caso. De esta forma, hemos llegado a que

$$|x+1|^m \leq (m+1)\,\text{máx}\{1, |x|^m\}.$$

Aplicamos en ambos lados la raíz m-ésima y nos queda

$$|x+1| \leq \sqrt[m]{m+1}\,\text{máx}\{1, |x|\}.$$

Esta desigualdad se cumple para todo m, y sabemos que

$$\lim_{m\to\infty} \sqrt[m]{m+1} = 1.$$

Luego, si tomamos $m \to \infty$ tenemos

$$|x+1| \leq \text{máx}\{|x|, 1\},$$

lo cual era lo que queríamos demostrar. □

El teorema anterior nos muestra la diferencia entre los valores absolutos arquimedianos y no arquimedianos. De hecho, nos permite enunciar la siguiente propiedad:

Propiedad Arquimediana: Dados $x, y \in \mathbb{K}, x \neq 0$, existe un entero positivo n tal que $|nx| > |y|$.

Si nos fijamos en la propiedad arquimediana, vemos que está relacionada con el hecho de que existen enteros cuyos valores absolutos son muy grandes. Otra forma de decir esto es que la propiedad arquimediana es equivalente a que

$$\sup\{|n| : n \in \mathbb{Z}\} = +\infty.$$

Esto nos lleva a enunciar el siguiente corolario:

Corolario 2.10. *Un valor absoluto* $|\ |$ *es no arquimediano si y solo si* $\sup\{|n| : n \in \mathbb{Z}\} = 1$.

2.3. Álgebra

En esta sección veremos las relaciones entre los valores absolutos no arquimedianos y las estructuras algebraicas de los cuerpos en los que estamos trabajando.

Todo valor absoluto no arquimediano está relacionado con un subanillo del cuerpo $\mathbb{K}$, y este subanillo tiene unas propiedades muy interesantes.

Proposición 2.11. *Sea* $\mathbb{K}$ *un cuerpo, y sea* $|\ |$ *un valor absoluto no arquimediano en* $\mathbb{K}$. *El conjunto*

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

es un subanillo de $\mathbb{K}$. *Su subconjunto*

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

es un ideal de $\mathcal{O}$. *Además,* $\mathfrak{P}$ *es un ideal maximal de* $\mathcal{O}$, *y todo elemento del complementario* $\mathcal{O} - \mathfrak{P}$ *es invertible en* $\mathcal{O}$.

Demostración. $\mathcal{O}$ es un subanillo de $\mathbb{K}$ si y solo si dados dos elementos cualquiera $x, y \in \mathcal{O}$, $x - y \in \mathcal{O}$ y dados otros dos elementos arbitrarios $x, y \in \mathcal{O}, xy \in \mathcal{O}$. Para la primera de ellas, tenemos que como $x \in \mathcal{O},\ |x| \leq 1$, y como $y \in \mathcal{O},\ |y| \leq 1$ y por ser un cuerpo, existe el opuesto de y, el cual cumple que $|-y| \leq 1$. Además, tenemos que

$$|x - y| = |x + (-y)| \leq \text{máx}\{|x|, |-y|\} \leq 1$$

usando la tercera propiedad de un valor absoluto no arquimediano. Luego, $x - y \in \mathcal{O}$.
Veamos ahora la segunda condición para que sea subanillo. Como antes, $x, y \in \mathcal{O}$, por lo que se cumple que $|x| \leq 1$ y $|y| \leq 1$. Una vez tenemos esto

$$|xy| = |x||y| \leq 1 \cdot 1 = 1$$

usando la segunda propiedad de un valor absoluto no arquimediano. De aquí se sigue que $xy \in \mathcal{O}$.

Por tanto, $\mathcal{O}$ es un subanillo de $\mathbb{K}$.
Veamos ahora que $\mathfrak{P}$ es un ideal de $\mathcal{O}$. Para ver esto, tenemos que ver que $\mathfrak{P}$ es un subgrupo de $\mathcal{O}$ y que dados $x \in \mathcal{O}$ e $y \in \mathfrak{P}$, el producto $xy \in \mathfrak{P}$.
Es obvio que $\mathfrak{P}$ es un subgrupo de $\mathcal{O}$.
Como $x \in \mathcal{O},\ |x| \leq 1$, y como $y \in \mathfrak{P},\ |y| < 1$, entonces

$$|xy| = |x||y| \leq 1 \cdot |y| < 1 \cdot 1 = 1,$$

y así, $xy \in \mathfrak{P}$. Por tanto, $\mathfrak{P}$ es un ideal de $\mathcal{O}$.
Falta por ver que este ideal $\mathfrak{P}$ es maximal, lo cual es obvio ya que no existe ningún otro ideal mayor y distinto que $\mathfrak{P}$.
Veamos ahora que todos los elementos del complementario $\mathcal{O} - \mathfrak{P}$ son invertibles. Tenemos que

$$\mathcal{O} - \mathfrak{P} = \{x \in \mathbb{K} : |x| \leq 1\} - \{x \in \mathbb{K} : |x| < 1\} = \{x \in \mathbb{K} : |x| = 1\}.$$

Todos los elementos de este conjunto son elementos de $\mathbb{K}$ cuyo valor absoluto es igual a 1, y por ser $\mathbb{K}$ cuerpo, todos tienen inverso multiplicativo, por lo tanto, todo elemento de $\mathcal{O} - \mathfrak{P}$ es invertible. □

Los anillos que tienen un único ideal maximal y todos los elementos de su complementario son invertibles son los denominados anillos locales. La proposición anterior nos muestra como se relacionan los valores absolutos no arquimedianos en un cuerpo arbitrario $\mathbb{K}$ y los subanillos de $\mathbb{K}$. Vamos a dar ahora una serie de definiciones:

Definición 2.12. Sea $\mathbb{K}$ un cuerpo cualquiera y sea $|\ |$ un valor absoluto no arquimediano. El subanillo

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

se llama el anillo de valoración de $|\ |$. El ideal

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

se llama el ideal de valoración de $|\ |$. El cociente

$$\kappa = \mathcal{O}/\mathfrak{P}$$

se llama el cuerpo de residuos de $|\ |$.

Recordemos que $\kappa = \mathcal{O}/\mathfrak{P}$ es un cuerpo, ya que estamos cocientando un anillo por un ideal maximal y esto siempre da un cuerpo.

Por todo esto, muchos valores absolutos están relacionados con propiedades algebraicas de los anillos de valoración a los que están asociados. Veamos ahora que pasa si consideramos el valor absoluto p-ádico.

Proposición 2.13. *Sea $\mathbb{K} = \mathbb{Q}$ y sea $|\ | = |\ |_p$ el valor absoluto p-ádico. Entonces:*

(I) el anillo de valoración asociado es $\mathcal{O} = \mathbb{Z}_{(p)} = \{a/b \in \mathbb{Q} : p \nmid b\}$,

(II) el ideal de valoración es $\mathfrak{P} = p\mathbb{Z}_{(p)} = \{a/b \in \mathbb{Q} : p \nmid b \text{ y } p \mid a\}$,

(III) el cuerpo de residuos es $\kappa = \mathbb{F}_p$ (cuerpo con p elementos).

Demostración. Como ya vimos, el valor absoluto p-ádico se define de la siguiente forma

$$\left|\frac{a}{b}\right| = p^{-v} \text{ cuando } \frac{a}{b} = p^v \frac{a_1}{b_1} \text{ con } p \nmid a_1 b_1.$$

Luego, está claro que $a/b \in \mathcal{O}$ si y solo si $v \geq 0$ y tenemos que $p \nmid b$.
Análogamente, $a/b \in \mathfrak{P}$ si y solo si $v > 0$, y en este caso $p \nmid b$ y $p \mid a$.
El cuerpo de residuos $\kappa = \mathcal{O}/\mathfrak{P}$ es $\kappa = \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}$, el cual es un cuerpo de p elementos con p clases de equivalencia, igual a $\mathbb{F}_p$. □

Capítulo 3

Los números p-ádicos

Seguimos la línea del libro [4]. En los capítulos anteriores, discutimos algunas de las propiedades básicas de los valores absolutos, vimos una propiedad para diferenciar los valores absolutos arquimedianos de los no arquimedianos, los cuales definimos en una serie de cuerpos arbitrarios distintos. Una vez hecho todo esto, podemos aplicar todos los resultados anteriores al cuerpo más interesante desde el punto de vista de este trabajo, el cuerpo de los números racionales $\mathbb{Q}$. A su vez, extenderemos todos estos resultados a otros cuerpos como el formado por extensiones finitas de $\mathbb{Q}$.

3.1. Valores absolutos en $\mathbb{Q}$

En el capítulo anterior, ya hemos visto un par de ejemplos de valores absolutos en el cuerpo $\mathbb{Q}$. Lo siguiente que tendremos que hacer es demostrar que los ejemplos que hemos visto son en realidad los únicos valores absolutos que podremos considerar en $\mathbb{Q}$. Para ello, veremos que se tienen que cumplir una serie de propiedades para que dos valores absolutos distintos sean equivalentes. Por último, veremos como se comportan todos los valores absolutos de $\mathbb{Q}$ aritméticamente.

Empezaremos recordando los valores absolutos definidos en $\mathbb{Q}$ que ya hemos visto en el capítulo anterior:

- el valor absoluto trivial;
- el valor absoluto $|\ |_\infty$, el cual denominamos valor absoluto en el infinito;
- el valor absoluto p-ádico $|\ |_p$. En este caso, hay que tener en cuenta que existe uno distinto para cada primo p.

El caso del valor absoluto trivial es el que menos nos interesa. Los otros dos si que son más importantes. En realidad, estos dos últimos se pueden considerar como uno solo, ya que podemos escribir ambos valores absolutos de la forma $|\ |_p$ con p cualquier primo o $p = \infty$. De utilizar esta notación, estamos considerando el ∞ como el número primo más grande en $\mathbb{Z}$, y nos referiremos a él como el "primo infinito". Como no puede ser de otra forma, a su correspondiente valor absoluto lo denominaremos el valor absoluto ∞-ádico. El motivo de utilizar esta notación en lugar de diferenciar ambos valores absolutos es simplemente por comodidad, ya que en muchos resultados podremos usar afirmaciones como "$|\ |_p$ para todo primo $p \leq \infty$."

Antes de enunciar el principal teorema de esta sección, definiremos un par de conceptos que nos serán de gran utilidad para muchos resultados de este capítulo.

Definición 3.1. Dos valores absolutos $|\ |_1$ y $|\ |_2$ en un cuerpo $\mathbb{K}$ son equivalentes si definen la misma topología en $\mathbb{K}$, es decir, si todo conjunto abierto respecto a una de las topologías, es también abierto respecto a la otra.

Puesto que cuesta ver que dos valores absolutos son equivalentes mediante el uso de esta definición, enunciamos el siguiente lema:

Lema 3.2 ([4])**.** *Sean $|\ |_1$ y $|\ |_2$ dos valores absolutos en el cuerpo $\mathbb{K}$. Son equivalentes:*

1. *$|\ |_1$ y $|\ |_2$ son valores absolutos equivalentes;*
2. *para cualquier $x \in \mathbb{K}$, tenemos que $|x|_1 < 1$ si y solo si $|x|_2 < 1$;*
3. *existe un número real positivo α tal que para cada $x \in \mathbb{K}$ se cumple que*

$$|x|_1 = |x|_2^{\alpha}.$$

Antes de ver el teorema más importante de esta sección, veamos un ejemplo de dos valores absolutos equivalentes.

Ejemplo 3.3. Para cualquier $c \in \mathbb{R}, c > 1$, la ecuación $|x| = c^{-v_p(x)}$ define un valor absoluto no arquimediano en $\mathbb{Q}$. Además, este valor absoluto es equivalente al valor absoluto p-ádico $|\ |_p$.
Veamos primero que este valor absoluto así definido es no arquimediano. Para ello, utilizaremos el Teorema 2.9. Tenemos que ver entonces que $|x| \leq 1$ para todo $x \in \mathbb{Q}$. Sabemos que $|x| = c^{-v_p(x)}$ y tenemos que $c > 1$, luego $\frac{1}{c} < 1$. Elevando ambos lados, la desigualdad se conserva, luego $(\frac{1}{c})^{v_p(x)} < 1^{v_p(x)}$. Así, tenemos que $\frac{1}{c^{v_p(x)}} < 1$ de donde se sigue que $c^{-v_p(x)} < 1$, con lo que llegamos a que $|x| < 1$ para todo $x \in \mathbb{Q}$. Luego, este valor absoluto en $\mathbb{Q}$ así definido $|x| = c^{-v_p(x)}$ es no arquimediano.

Veamos ahora que $|x| = c^{-v_p(x)}$ es equivalente al valor absoluto p-ádico $|\ |_p$. Vamos a ver que son equivalentes viendo que existe un número real α tal que para cada $x \in \mathbb{Q}$ se cumple que $|x|_p = |x|^\alpha$.
Tomamos α tal que $c^\alpha = p$. Tenemos que $|x|_p = p^{-v_p(x)} = c^{\alpha(-v_p(x))} = c^{-v_p(x)\alpha} = |x|^\alpha$. Por tanto, este valor absoluto así definido $|x| = c^{-v_p(x)}$ es equivalente al valor absoluto p-ádico $|\ |_p$.

Teorema 3.4. ***(Ostrowski)*** *Todo valor absoluto no trivial en $\mathbb{Q}$ es equivalente a uno de los valores absolutos $|\ |_p$, donde p puede ser un número primo cualquiera o $p = \infty$.*

Demostración. Sea $|\ |$ un valor absoluto no trivial en $\mathbb{Q}$. Tenemos que considerar dos casos diferentes:

(I) Supongamos que $|\ |$ es arquimediano. En este caso, queremos ver que este valor absoluto es equivalente al valor absoluto "usual" que hemos definido anteriormente, es decir, al valor absoluto ∞-ádico $|\ |_\infty$.
Sea n_0 el último entero positivo tal que $|n_0| > 1$ (si no hay ningún elemento que lo cumpla, $|\ |$ sería no arquimediano, ya que un valor absoluto $|\ |$ es no arquimediano si y solo si $\sup\{|n| : n \in \mathbb{Z}\} = 1$).
Podemos encontrar un número real positivo α tal que $|n_0| = n_0^\alpha$. Para este α, vamos a probar que para todo $x \in \mathbb{Q}$, $|x| = |x|_\infty^\alpha$. Como hemos visto anteriormente, sabemos que llega con ver que esto se cumple para los enteros positivos, con lo cual, veremos si se cumple que $|n| = n^\alpha$.
Para $n = n_0$, se cumple.
Veamos ahora si se cumple en general. Cogemos un entero arbitrario n, y lo escribimos en "base n_0". Luego tenemos

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

con $0 \leq a_i \leq n_0 - 1$ y $a_k \neq 0$. Además, es importante ver que k cumple que $n_0^k \leq n < n_0^{k+1}$, lo cual nos dice que k es de la forma

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

donde $\lfloor x \rfloor$ denota la parte entera (esta igualdad anterior es fácil de ver si le aplicamos logaritmos a la desigualdad $n_0^k \leq n < n_0^{k+1}$). Una vez desarrollado n en su "base n_0", tomamos valores absolutos

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

Como n_0 es el entero más pequeño cuyo valor absoluto es $|n_0| > 1$, y tenemos que $0 \leq a_i \leq n_0 - 1$, llegamos a que $|a_i| \leq 1$ para $i = 0, 1, \ldots, k$. Por tanto,

$$|n| \leq 1 + n_0^{\alpha} + n_0^{2\alpha} + \cdots + n_0^{k\alpha} = n_0^{k\alpha}\Big(1 + n_0^{-\alpha} + n_0^{-2\alpha} + \cdots + n_0^{-k\alpha}\Big)$$
$$\leq n_0^{k\alpha} \sum_{i=0}^{\infty} n_0^{-i\alpha} = n_0^{k\alpha}\, \frac{n_0^{\alpha}}{n_0^{\alpha} - 1}.$$

Si tomamos $C = \frac{n_0^{\alpha}}{n_0^{\alpha}-1}$ (el cual es un número positivo), tenemos que

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

usando que $n_0^k \leq n < n_0^{k+1}$. Esta fórmula se cumple para todo n puesto que hemos tomado un n arbitrario, luego podemos tomar un entero de la forma n^N y obtenemos

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

Cogiendo raíces N-ésimas, tenemos que

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

Por último, cuando $N \longrightarrow \infty$, $\sqrt[N]{C} \longrightarrow 1$, con lo cual tenemos que

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

Veamos ahora la otra desigualdad. Para ello, volvemos a escribir n en su "base n_0".

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

Como $n_0^{k+1} > n \geq n_0^k$, tenemos lo siguiente

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

y pasándolo al otro lado obtenemos

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

Para esta última desigualdad hemos utilizado que $n_0^{(k+1)\alpha} \leq |n| + |n_0^{k+1} - n|$, de donde sacamos que $|n_0^{k+1} - n| \geq n_0^{(k+1)\alpha} - |n|$ y $n_0^{(k+1)\alpha} - |n| \geq (n_0^{k+1} - n)^{\alpha}$ puesto que añades más términos a la resta.
Ahora bien, como $n \geq n_0^k$

$$|n| \geq n_0^{(k+1)\alpha} - (n_0^{k+1} - n)^{\alpha} = n_0^{(k+1)\alpha}\Big(1 - \Big(1 - \frac{1}{n_0}\Big)^{\alpha}\Big) = C' n_0^{(k+1)\alpha} > C' n^{\alpha},$$

siendo $C' = \left(1 - \left(1 - \frac{1}{n_0}\right)^{\alpha}\right) > 0$. Igual que hicimos antes, hemos llegado a que

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

y como hemos tomado un número arbitrario n, podemos tomar un número de la forma n^N.

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

Tomamos raíces N-ésimas

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

y cuando $N \longrightarrow \infty$, $\sqrt[N]{C'} \longrightarrow 1$. Luego, llegamos a que

$$|n| > n^{\alpha}.$$

Como hemos visto, se cumplen ambas desigualdades, es decir, se cumple que $|n| = n^{\alpha}$. Por tanto, el valor absoluto $|\ |$ es equivalente al valor absoluto usual ∞-ádico $|\ |_{\infty}$.

(II) Supongamos ahora que $|\ |$ es un valor absoluto no arquimediano. En este caso, veremos que este valor absoluto $|\ |$ es equivalente al valor absoluto p-ádico $|\ |_p$. Por ser no arquimediano, tenemos que $|n| \leq 1$ para todo $n \in \mathbb{Z}$.
Como $|\ |$ es un valor absoluto no trivial, existe $n_0 \in \mathbb{Z}$ entero más pequeño tal que $|n_0| < 1$.
Lo primero que vamos a ver es que n_0 es primo.
Supongamos que $n_0 = a \cdot b$, con $a, b < n_0$ y $|n_0| < 1$. Esto no puede ocurrir, luego n_0 es primo.
Tomamos por tanto $n_0 = p$, y vamos a ver que $|\ |$ es equivalente al valor absoluto p-ádico.
El próximo paso es ver que si $n \in \mathbb{Z}$ no es divisible por p, entonces $|n| = 1$. Si dividimos n por p, podemos escribir n como sigue

$$n = rp + s,$$

con $0 < s < p$ y $r \in \mathbb{Z}$. Como p es el entero más pequeño tal que $|p| \leq 1$ por construcción, tenemos que $|s| = 1$. También tenemos que $|rp| < 1$, porque $|r| \leq 1$ (ya que $|\ |$ es no arquimediano). Como $|\ |$ es no arquimediano, se sigue que $|n| = 1$.
Por último, dado cualquier $n \in \mathbb{Z}$, el cual podemos escribirlo como $n = p^v n'$ con $p \nmid n'$. Entonces

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

donde $c = |p|^{-1} > 1$. Por tanto, hemos probado que $|\ |$ es equivalente al valor absoluto p-ádico.

□

Este teorema es la principal razón por la cual pensamos en el valor absoluto usual $|\ |_\infty$ (o la inclusión de cuerpos de la que proviene $\mathbb{Q} \hookrightarrow \mathbb{R}$) como un tipo de elemento "primo" de $\mathbb{Q}$. Sin embargo, no hay que olvidar que lo más importante que dice el teorema es que todo valor absoluto de $\mathbb{Q}$ está asociado a un primo p que puede ser finito o infinito.

Proposición 3.5. *(Fórmula del Producto) Para cualquier $x \in \mathbb{Q}^*$, tenemos que*

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

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

Demostración. Está claro que solo lo tenemos que probar para los enteros positivos x. Sea x un entero positivo, el cual podemos factorizar como producto de primos, es decir, lo expresamos de la siguiente forma: $x = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}$. Entonces tenemos

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

Por tanto, el producto de los tres tipos de valores absolutos nos da 1, ya que en el primer caso es igual a 1 y en los siguientes se van anulando uno a uno para $i = 1, 2, \ldots, k$. □

Esta Fórmula del Producto nos muestra una relación entre los diferentes valores absolutos de $\mathbb{Q}$. Esto nos permite saber cuánto vale el valor absoluto de un número $x \in \mathbb{Q}$ siempre que tengamos el valor de todos los restantes elementos. Esto es muy importante en numerosas aplicaciones. Esto último, también funciona con cada una de las inclusiones sobre las que se define cada uno de los valores absolutos que tenemos en $\mathbb{Q}$, es decir, para cada primo p, tenemos un valor absoluto, y para cada valor absoluto, tenemos una inclusión de cuerpos. Aún así, para definir esto de una forma más formal, tenemos que trabajar en diferentes extensiones de $\mathbb{Q}$.

3.2. Completaciones

En esta sección, vamos a construir los diferentes cuerpos p-ádicos $\mathbb{Q}_p$. Un factor que debemos tener en cuenta a la hora de construir estos cuerpos, es que todos los valores absolutos que tenemos en $\mathbb{Q}$ son igual de importantes. Antes de empezar a construirlos, vamos a mencionar una serie de conceptos topológicos que serán importantes para la construcción.

Definición 3.6. Sea $\mathbb{K}$ un cuerpo arbitrario y $|\ |$ un valor absoluto en $\mathbb{K}$.

(I) Se dice que una sucesión de elementos $x_n \in \mathbb{K}$ es una sucesión de Cauchy si para todo $\varepsilon > 0$, existe un M tal que $|x_n - x_m| < \varepsilon$ para todo $m, n \geq M$.

(II) Se dice que el cuerpo $\mathbb{K}$ es un cuerpo completo respecto a $|\ |$ si toda sucesión de Cauchy de elementos de $\mathbb{K}$ tiene límite.

(III) Se dice que un subconjunto $S \subset \mathbb{K}$ es un subconjunto denso en $\mathbb{K}$ si para todo elemento de $\mathbb{K}$ y para toda bola abierta con centro los elementos de $\mathbb{K}$, contiene un elemento de S. Es decir, si para todo $x \in \mathbb{K}$ y todo $\varepsilon > 0$ tenemos

$$B(x, \varepsilon) \cap S \neq \emptyset.$$

Antes de seguir, vamos a ver un par de ejemplos de sucesiones de Cauchy.

Ejemplo 3.7 ([1])**.** Consideremos la sucesión $a_n = 1 + p + p^2 + \cdots + p^{n-1}$. Veamos si es una sucesión de Cauchy

$$\begin{aligned} |a_{n+k} - a_n|_p &= \left|1 + p + p^2 + \cdots + p^{n+k-1} - (1 + p + p^2 + \cdots + p^{n-1})\right|_p \\ &= \left|p^n + p^{n+1} + \cdots + p^{n+k-1}\right|_p = \left|p^n(1 + p + p^2 + \cdots + p^{k-1})\right|_p \\ &= p^{-n} = \frac{1}{p^n}. \end{aligned}$$

Para cada $\varepsilon > 0$, escogemos un M para el cual $p^M \geq 1/\varepsilon$, por lo que si $n > M$, tenemos que

$$|a_{n+k} - a_n| < \frac{1}{p^M} \leq \varepsilon.$$

Por lo tanto, (a_n) es una sucesión de Cauchy. De hecho, esta sucesión tiene límite respecto de $|\ |_p$. Cogemos $a = \frac{1}{1-p} \in \mathbb{Q}$, luego $a_n = \frac{p^n - 1}{p-1}$, por lo tanto

$$\left|a_n - \frac{1}{1-p}\right|_p = \left|\frac{p^n}{p-1}\right|_p = p^{-n} = \frac{1}{p^n}.$$

Luego, para $\varepsilon > 0$, tenemos que

$$\left|a_n - \frac{1}{1-p}\right|_p < \varepsilon$$

siempre que $n > M$ como antes. Escribiremos $\lim_{n\to\infty}^{(p)}$ para referirnos al límite de la sucesión. En este caso tenemos que

$$\lim_{n\to\infty}^{(p)} (1 + p + p^2 + \cdots + p^{n-1}) = \frac{1}{1-p}.$$

La razón por la que hemos definido estos conceptos es que para el valor absoluto arquimediano $|\ |_\infty$, tenemos que existe una inclusión $\mathbb{Q} \hookrightarrow \mathbb{R}$ de $\mathbb{Q}$ en el cuerpo $\mathbb{R}$, y que tiene las siguientes propiedades:

- el valor absoluto $|\ |_\infty$ se extiende a $\mathbb{R}$;
- $\mathbb{R}$ es un cuerpo completo respecto a la métrica dada por el valor absoluto $|\ |_\infty$;
- $\mathbb{Q}$ es denso en $\mathbb{R}$.

Todas estas propiedades anteriores se pueden resumir diciendo que el cuerpo $\mathbb{R}$ es una completación de $\mathbb{Q}$ respecto al valor absoluto $|\ |_\infty$. De hecho, $\mathbb{R}$ es el cuerpo más pequeño que contiene a $\mathbb{Q}$ y que es completación de él respecto a este valor absoluto. Esto es así porque, cualquier cuerpo en estas condiciones tiene que incluir el límite de cualquier sucesión de Cauchy de elementos de $\mathbb{Q}$, y como $\mathbb{Q}$ es denso en $\mathbb{R}$, cualquier elemento de $\mathbb{R}$ es límite de una sucesión de Cauchy.

En esta sección intentaremos construir para cada uno de los valores absolutos de $\mathbb{Q}$ una completación, de la misma forma que hicimos para el valor absoluto $|\ |_\infty$. Esta completación será parecida a la que hemos hecho con $\mathbb{R}$. Queremos ver que para cada primo p, existe un cuerpo en el cual podemos extender su valor absoluto p-ádico, y este cuerpo será una completación respecto a este valor absoluto, y en el cual $\mathbb{Q}$ es denso.

A partir de ahora, consideraremos $|\ | = |\ |_p$ como el valor absoluto p-ádico para algún primo p. Lo primero en lo que nos tenemos que fijar es que la caracterización de las sucesiones de Cauchy en un valor absoluto no arquimediano es más sencilla.

Lema 3.8. *Una sucesión (x_n) de números racionales es una sucesión de Cauchy respecto a un valor absoluto no arquimediano $|\ |$ si y solo si se cumple que*

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

Demostración. Si $m = n + r > n$, tenemos que

$$\begin{aligned} |x_m - x_n| &= |x_{n+r} - x_{n+r-1} + x_{n+r-1} - x_{n+r-2} + \cdots + x_{n+1} - x_n| \\ &\leq \text{máx}\{|x_{n+r} - x_{n+r-1}|, |x_{n+r-1} - x_{n+r-2}|, \ldots, |x_{n+1} - x_n|\}. \end{aligned}$$

Esta última desigualdad se debe a que es valor absoluto es no arquimediano. Una vez calculado el máximo y aplicando límites en ambos lados, llegamos a que $\lim_{n\to\infty} |x_{n+1} - x_n| = 0$, como queríamos probar. □

Esta última caracterización de las sucesiones de Cauchy solo funciona cuando el valor absoluto que consideramos es no arquimediano.

Lema 3.9. *El cuerpo $\mathbb{Q}$ de los números racionales no es completo respecto a cualquiera de sus valores absolutos no triviales.*

Demostración. Por el teorema de Ostrowski, tenemos que ver que $\mathbb{Q}$ no es completo respecto a ningún valor absoluto $|\ |_p$ para $p \leq \infty$.
Para el caso de $|\ |_\infty$, consideramos la sucesión $x_{n+1} = \frac{x_n}{2} + \frac{1}{x_n}$ para $n > 1$ y $x_0 = 2$. Veamos que el límite de esta sucesión es $\sqrt{2}$.
Aplicando la desigualdad de media aritmética y geométrica $\frac{x+y}{2} \geq \sqrt{xy}$, tenemos que

$$x_{n+1} = \frac{x_n}{2} + \frac{1}{x_n} = \frac{x_n + \frac{2}{x_n}}{2} \geq \sqrt{x_n \frac{2}{x_n}} = \sqrt{2}.$$

Por otro lado, como x_n es un número racional, tenemos que $x_n > \sqrt{2}$. De aquí se sigue que

$$x_n > \sqrt{2} \Longleftrightarrow \frac{1}{x_n} < \frac{1}{\sqrt{2}}.$$

Multiplicando esta última por 2, mantenemos el sentido de la desigualdad y llegamos a que

$$\frac{2}{x_n} < \frac{2}{\sqrt{2}} = \sqrt{2},$$

y así tenemos que $\frac{2}{x_n} < \sqrt{2}$. Entonces

$$x_n + x_n > x_n + \sqrt{2}$$

de donde, despejando, se obtiene

$$x_n > \frac{x_n + \sqrt{2}}{2}.$$

Así, tenemos que

$$x_{n+1} = \frac{x_n + \frac{2}{x_n}}{2} < \frac{x_n + \sqrt{2}}{2} < x_n$$

con lo cual hemos visto que $x_{n+1} < x_n$, es decir, tenemos una función monótona decreciente y acotada inferiormente, luego es convergente. De aquí deducimos que el límite de esta sucesión de números racionales es $\sqrt{2}$, y $\sqrt{2} \notin \mathbb{Q}$, con lo cual $\mathbb{Q}$ no es completo respecto a este valor absoluto.
Tomamos ahora $|\ | = |\ |_p$ para algún primo p. Tenemos que construir una sucesión en $\mathbb{Q}$ cuyo límite no está en $\mathbb{Q}$. Necesitamos encontrar una sucesión de soluciones módulo p^n de una ecuación que no tiene soluciones en $\mathbb{Q}$.
Consideremos ahora $p \neq 2$. Tomamos un entero $a \in \mathbb{Z}$ tal que

- a no es un cuadrado en $\mathbb{Q}$;

- p no divide a a;
- a es un residuo cuadrático módulo p, es decir, la congruencia $X^2 \equiv a \pmod{p}$ tiene solución.

Tomamos cualquier cuadrado en $\mathbb{Z}$ y le añadimos un múltiplo de p para encontrar un a. Ahora podemos construir de la siguiente forma una sucesión de Cauchy respecto de $|\ |_p$:

- cogemos cualquier solución x_0 tal que $x_0^2 \equiv a \pmod{p}$;
- tomamos x_1 tal que $x_1 \equiv x_0 \pmod{p}$ y $x_1^2 \equiv a \pmod{p^2}$;
- en general, tomamos x_n tal que

$$x_n \equiv x_{n-1} \pmod{p^n}$$

y

$$x_n^2 \equiv a \pmod{p^{n+1}}.$$

Tenemos que ver si esta sucesión es de Cauchy, luego

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

lo cual muestra utilizando el Lema 3.8, que es una sucesión de Cauchy. Por otro lado, tenemos que

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

por lo que el límite, de existir, tiene que ser la raíz cuadrada de a. Pero como a no es un cuadrado, no puede existir límite.
Por tanto, $\mathbb{Q}$ no es completo respecto a $|\ |_p$.
Para el caso $p = 2$, hacemos lo mismo que en el caso de $p \neq 2$, pero en este caso tomamos raíces cúbicas en lugar de raíces cuadradas, es decir, tomamos a de tal forma que no es un cubo en $\mathbb{Q}$, y que la congruencia $X^3 \equiv a \pmod{2}$ tiene solución. Y realizamos el mismo proceso que en el otro caso.
Por tanto, hemos probado que $\mathbb{Q}$ no es completo respecto a ningún valor absoluto $|\ |_p$ para $p \leq \infty$. □

Luego como $\mathbb{Q}$ no es completo, hay que construirle una completación, es decir, tenemos que añadirle todos los límites de todas las sucesiones de Cauchy. Para ello, primero definiremos una serie de conceptos:

Definición 3.10. Sea $|\ | = |\ |_p$ un valor absoluto no arquimediano en $\mathbb{Q}$. Denotamos por $\mathcal{C}$, o $\mathcal{C}_p(\mathbb{Q})$, para recalcar el valor de p y $\mathbb{Q}$, al conjunto de todas las sucesiones de Cauchy de elementos de $\mathbb{Q}$:

$$\mathcal{C} = \mathcal{C}_p(\mathbb{Q}) = \{(x_n) : (x_n) \text{ es una sucesión de Cauchy respecto de } |\ |_p\}.$$

Proposición 3.11. *$\mathcal{C}$ tiene estructura de anillo conmutativo con las operaciones*

$$(x_n) + (y_n) = (x_n + y_n),$$
$$(x_n) \cdot (y_n) = (x_n y_n).$$

Demostración. Probemos primero que $(\mathcal{C}, +, \cdot)$ es un anillo. Para ello veremos una serie de propiedades que nos definirán primero la existencia de un grupo, y posteriormente el anillo.

1. Dados dos elementos $(x_n), (y_n) \in (\mathcal{C}, +)$, su suma $(x_n) + (y_n) = (x_n + y_n) \in (\mathcal{C}, +)$.

2. La operación $+$ es asociativa, es decir, para todo $(x_n), (y_n), (z_n) \in (\mathcal{C}, +)$ se cumple que

$$\begin{aligned}((x_n) + (y_n)) + (z_n) &= (x_n + y_n) + (z_n) = (x_n + y_n + z_n) \\ &= (x_n) + (y_n + z_n) = (x_n) + ((y_n) + (z_n)).\end{aligned}$$

3. Existe un elemento neutro (0) para la suma, es decir, para todo $(x_n) \in (\mathcal{C}, +)$, existe un elemento neutro tal que

$$(x_n) + (0) = (x_n + 0) = (x_n).$$

4. Existe un elemento simétrico para la suma, es decir, para todo $(x_n) \in (\mathcal{C}, +)$, existe un elemento $(-x_n) \in (\mathcal{C}, +)$ tal que

$$(x_n) + (-x_n) = (x_n - x_n) = (0)$$
$$(x_n) + (-x_n) = (-x_n) + (x_n).$$

   Así, $(\mathcal{C}, +)$ es un grupo.

5. La operación $+$ es conmutativa, es decir, para todo $(x_n), (y_n) \in (\mathcal{C}, +)$, se cumple que

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

   Por tanto, $(\mathcal{C}, +)$ es un grupo conmutativo.

6. Dados dos elementos $(x_n), (y_n) \in (\mathcal{C}, +, \cdot)$, su producto $(x_n) \cdot (y_n) = (x_n \cdot y_n) \in (\mathcal{C}, +, \cdot)$.

7. La operación $\cdot$ es asociativa, es decir, para todo $(x_n), (y_n), (z_n) \in (\mathcal{C}, \cdot)$ se cumple que

$$\begin{aligned}((x_n) \cdot (y_n)) \cdot (z_n) &= (x_n \cdot y_n) \cdot (z_n) = (x_n \cdot y_n \cdot z_n) \\ &= (x_n) \cdot (y_n \cdot z_n) = (x_n) \cdot ((y_n) \cdot (z_n)).\end{aligned}$$

8. Existe un elemento neutro para la operación $\cdot$, y este elemento es distinto que el neutro para la operación $+$. Así, existe un elemento (1) tal que

$$((x_n) \cdot (1)) = (x_n \cdot 1) = (x_n).$$

9. La operación $\cdot$ es distributiva respecto de $+$, es decir, para todo $(x_n), (y_n), (z_n) \in (\mathcal{C}, +, \cdot)$, tenemos que

$$\begin{aligned}x_n \cdot (y_n + z_n) &= (x_n \cdot y_n) + (x_n \cdot z_n), \\ (x_n + y_n) \cdot (z_n) &= (x_n \cdot z_n) + (y_n \cdot z_n).\end{aligned}$$

   Por lo tanto, $(\mathcal{C}, +, \cdot)$ es un anillo.

10. La operación $\cdot$ es conmutativa, es decir, dados $(x_n), (y_n) \in (\mathcal{C}, +, \cdot)$ se cumple que

$$(x_n) \cdot (y_n) = (x_n \cdot y_n) = (y_n \cdot x_n) = (y_n) \cdot (x_n).$$

    Por tanto, $(\mathcal{C}, +, \cdot)$ es un anillo conmutativo, como queríamos probar.

□

Proposición 3.12. *El anillo $\mathcal{C}$ no es un cuerpo, puesto que no todos los elementos distintos de cero son invertibles respecto a la segunda operación. De hecho, $\mathcal{C}$ contiene divisores de cero, es decir, elementos distintos de cero cuyo producto es cero.*

Puesto que queremos encontrar una completación de $\mathbb{Q}$, tenemos que ver si este anillo $\mathcal{C}$ es un buen candidato, luego comprobaremos si este anillo contiene al cuerpo de los números racionales $\mathbb{Q}$. Para ver esto, nos llega con tomar un número cualquiera $x \in \mathbb{Q}$. La sucesión

$$x, x, x, x, \ldots$$

es una sucesión de Cauchy. De hecho, la llamaremos la sucesión constante asociada a x y la denotaremos por (x). Una vez vista la construcción de esta sucesión, podemos enunciar el siguiente lema.

Lema 3.13. *La aplicación que lleva al número racional x en su sucesión constante (x), es decir, la aplicación $x \mapsto (x)$, induce la inclusión del cuerpo $\mathbb{Q}$ en el anillo $\mathcal{C}$.*

Demostración. Es obvio por como hemos construido la sucesión constante (x). □

A pesar de como hemos definido el anillo $\mathcal{C}$, en él no se encuentran todos los límites de todas las sucesiones de Cauchy. Y es que dos sucesiones de Cauchy diferentes cuyos términos se aproximan más y más, deberían tener el mismo límite, pero estas sucesiones son diferentes elementos de $\mathcal{C}$. Una manera de solucionar este problema es pasar al cociente, es decir, dos sucesiones diferentes que deberían tener el mismo límite, las pasamos al cociente y las identificamos con un mismo elemento del cociente. De esta forma, son iguales. Veamos cómo y por qué cocientamos a $\mathcal{C}$. Es fácil ver que los términos de dos sucesiones que deben tener el mismo límite tienen que ser cada vez más próximos, es decir, la diferencia de los términos de las sucesiones tiende a cero. Así, empezaremos definiendo el conjunto de las sucesiones nulas, es decir las que tienden a cero.

Definición 3.14. Definimos $\mathcal{N} \subset \mathcal{C}$ como el ideal

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

de todas las sucesiones que tienden a cero respecto al valor absoluto $|\ |_p$. A estas sucesiones las llamaremos sucesiones nulas.

Ejemplo 3.15 ([1])**.** Consideramos el anillo $\mathbb{Q}$ y el valor absoluto p-ádico $|\ |_p$, tenemos que $a_n = p^n$. Luego

$$|p^n|_p = \frac{1}{p^n} \longrightarrow 0 \quad \text{cuando } n \longrightarrow \infty$$

con lo cual, $\lim_{n\to\infty}{}^{(p)}\, a_n = 0$. Por lo tanto, esta sucesión es nula respecto al valor absoluto p-ádico.

Ejemplo 3.16 ([1])**.** Tomamos $a_n = (1+p)^{p^n} - 1$ y consideramos el mismo valor absoluto que en el ejemplo anterior. Luego, para $n = 1$

$$\begin{aligned}
|a_1|_p &= \left|(1+p)^p - 1\right|_p \\
&= \left|\binom{p}{0} + \binom{p}{1}p + \binom{p}{2}p^2 + \cdots + \binom{p}{p}p^p - 1\right| \\
&= \left|1 + \binom{p}{1}p + \binom{p}{2}p^2 + \cdots + \binom{p}{p-1}p^{p-1} + p^p - 1\right| \\
&= \frac{1}{p^2}.
\end{aligned}$$

Esto pasa ya que para $1 \leq k \leq p-1$, tenemos que

$$v_p\binom{p}{k} = 1;$$

por tanto sacaremos de cada elemento un p^2 y por la definición de valor absoluto p-ádico, obtendremos ese resultado.
Razonando de manera similar, tenemos que para n se cumple que

$$|a_n|_p = \frac{1}{p^{n+1}}.$$

Vemos que cuando $n \longrightarrow \infty$, $|a_n|_p \longrightarrow 0$, luego esta sucesión es nula respecto al valor absoluto p-ádico.

Antes de seguir, veamos que $\mathcal{N}$ es un ideal de $\mathcal{C}$.

- $\mathcal{N}$ es un subgrupo de $\mathcal{C}$.
- Para todo elemento $(x_n) \in \mathcal{C}$, el cual es una sucesión de Cauchy respecto de $|\ |_p$, y para todo elemento $(y_n) \in \mathcal{N}$, el cual es una sucesión de Cauchy tal que $y_n \longrightarrow 0$, tenemos que

  $$(x_n) \cdot (y_n) \longrightarrow 0,$$

  es decir, que $(x_n)(y_n) \in \mathcal{N}$.

Por tanto, $\mathcal{N}$ es un ideal de $\mathcal{C}$.

Lema 3.17. *$\mathcal{N}$ es un ideal maximal de $\mathcal{C}$.*

Demostración. Sea $(x_n) \in \mathcal{C}$ una sucesión de Cauchy que no tienda a cero (es decir, que no pertenece a $\mathcal{N}$), y sea $\mathcal{I}$ el ideal generado por (x_n) y $\mathcal{N}$. Veremos que este ideal $\mathcal{I}$ es todo $\mathcal{C}$. Para ello, nos llega con ver que el elemento unidad (1) (la sucesión constante 1) es un elemento de $\mathcal{I}$. Una vez visto esto, es obvio que $\mathcal{I}$ es todo $\mathcal{C}$ porque cualquier ideal que contenga el elemento unidad, tiene que ser igual al anillo entero. Como (x_n) no tiende a cero y es una sucesión de Cauchy, su límite debe alejarse de cero, es decir, debe existir un número $c > 0$ y un entero N tal que $|x_n| \geq c > 0$ si $n \geq N$. En particular, tenemos que $x_n \neq 0$ para $n \geq N$, y podemos definir otra sucesión (y_n) tomando $x_n = 0$ si $n < N$ y $y_n = 1/x_n$ si $n \geq N$. Veamos ahora que esta nueva sucesión (y_n) es una sucesión de Cauchy. Esto es obvio puesto que si $n \geq N$, tenemos que

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

lo cual demuestra que $(y_n) \in \mathcal{C}$ porque $|\ |$ es no arquimediano. Fijémonos ahora en que

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

La sucesión producto $(x_n)(y_n)$ tiene un número finito de ceros y está seguida por un número infinito de unos. En particular, si restamos esta sucesión a la sucesión constante (1), obtenemos

$$(1) - (x_n\, y_n) \in \mathcal{N}.$$

Esto muestra que la sucesión constante (1) puede escribirse como un múltiplo de (x_n) más un elemento de $\mathcal{N}$, luego la sucesión unidad (1) pertenece al ideal $\mathcal{I}$, como queríamos probar. □

Identificaremos sucesiones que difieren en elementos de $\mathcal{N}$ y que deben tener el mismo límite. Esto lo haremos cocientando el anillo $\mathcal{C}$ por el ideal maximal $\mathcal{N}$. Al cocientar un anillo por un ideal maximal obtenemos un cuerpo.

Definición 3.18. Definimos el cuerpo de los números p-ádicos como el cociente del anillo $\mathcal{C}$ por su ideal maximal $\mathcal{N}$ y lo denotaremos por:

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

Cabe destacar que dos sucesiones constantes diferentes nunca difieren en un elemento de $\mathcal{N}$ (su diferencia es justamente otra sucesión constante). Así, podemos definir la inclusión de cuerpos

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

tal que a cada $x \in \mathbb{Q}$, le asociamos su clase de equivalencia de la sucesión constante (x).

Si nos fijamos en lo que hemos obtenido hasta ahora, vemos que hemos construido un cuerpo, en el cual $\mathbb{Q}$ está incluido. Veamos ahora si este puede ser una completación del cuerpo de los números racionales $\mathbb{Q}$. Para ello, este debe de cumplir una serie de propiedades:

- $|\ |_p$ extiende el cuerpo $\mathbb{Q}$ a $\mathbb{Q}_p$;
- $\mathbb{Q}_p$ es un cuerpo completo respecto a la métrica dada por el valor absoluto p-ádico $|\ |_p$;
- $\mathbb{Q}$ es denso en $\mathbb{Q}_p$.

Lo primero que vamos a comprobar, es si el valor absoluto $|\ |_p$ extiende $\mathbb{Q}$ a $\mathbb{Q}_p$. Para ello, enunciamos el siguiente lema.

Lema 3.19. *Sea $(x_n) \in \mathcal{C}, (x_n) \notin \mathcal{N}$. La sucesión de números reales $|x_n|_p$ es una sucesión estacionaria, es decir, existe un número entero N tal que $|x_n|_p = |x_m|_p$ siempre que $m, n \geq N$.*

Demostración. Como (x_n) es una sucesión de Cauchy que no tiende a cero, podemos tomar un c y un N_1 tales que

$$n \geq N_1 \Longrightarrow |x_n| \geq c > 0.$$

Por otra parte, también existe un entero N_2 para el cual si

$$n, m \geq N_2 \Longrightarrow |x_n - x_m| < c.$$

Como queremos que ambas condiciones se cumplan, tomamos $N = \text{máx}\{N_1, N_2\}$. Así tenemos lo siguiente

$$n, m \geq N \Longrightarrow |x_n - x_m| < \text{máx}\{|x_n|, |x_m|\},$$

lo cual nos da que $|x_n| = |x_m|$ por la propiedad no arquimediana. □

Definición 3.20. Si λ es un elemento de $\mathbb{Q}_p$, y (x_n) es cualquier sucesión de Cauchy que representa a λ, definimos

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

Esto tiene sentido debido a que hemos definido $\mathbb{Q}_p$ como un cociente. Cada elemento que pertenece a él se representa con una clase de equivalencia determinada, es decir con una sucesión de Cauchy perteneciente a $\mathcal{C}$ y por una sucesión de Cauchy que pertenece a $\mathcal{N}$. Por eso, cuando pasamos a calcular $|\lambda|_p$ con $\lambda \in \mathbb{Q}_p$, tiene sentido que sea igual al límite cuando n tiende a infinito de la sucesión que representa a ese λ y la otra sucesión se va a cero. Por lo tanto, nos queda solo que $|\lambda|_p = \lim_{n\to\infty} |x_n|_p$ (en este caso, el representante de λ es la sucesión (x_n)).

Esta definición $|\lambda|_p = \lim_{n\to\infty} |x_n|_p$ no depende del representante elegido, es decir, en lugar de tomar la sucesión (x_n) como representante del elemento $\lambda \in \mathbb{Q}_p$, podemos tomar la sucesión $(\tilde{x}_n)$, la cual es equivalente a (x_n), puesto que ambas están en la misma clase de equivalencia. Es decir, ambas tienen el mismo límite en el cociente, luego tenemos que $\lim_{n\to\infty} |x_n|_p = \lim_{n\to\infty} |\tilde{x}_n|_p$.

Proposición 3.21. *Sea $\lambda \in \mathbb{Q}_p$. Tenemos que $|\lambda|_p = 0$ si y solo si $\lambda = 0$.*

Demostración. Empecemos viendo que si $|\lambda|_p = 0$, entonces $\lambda = 0$. Como $|\lambda|_p = 0$, tenemos que $\lim_{n\to\infty} |x_n|_p = 0$, y sabemos que $(x_n) \in \mathcal{C}$ pero $(x_n) \notin \mathcal{N}$, luego (x_n) es una sucesión constante de ceros, y por tanto, λ tiene que ser igual a cero.

Si $\lambda = 0$, tomamos como representante una sucesión que tiende a cero, es decir, tomamos una sucesión (x_n) tal que $\lim_{n\to\infty} |x_n|_p = 0$, y por definición, se cumple que $|\lambda|_p = \lim_{n\to\infty} |x_n|_p$, luego $|\lambda|_p = 0$. □

Proposición 3.22. *La aplicación*

$$\begin{aligned} |\ |_p : \mathbb{Q}_p &\longrightarrow \mathbb{R}^+ \\ \lambda &\longmapsto |\lambda|_p \end{aligned}$$

define un valor absoluto no arquimediano.

Demostración. Es obvio puesto que $|\ |_p$ define un valor absoluto no arquimediano sobre $\mathbb{Q}$ y tenemos que $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$. □

Todo esto implica que hemos definido un valor absoluto en $\mathbb{Q}_p$ el cual extiende el valor absoluto p-ádico en $\mathbb{Q}$. Lo único que nos queda por ver es que el conjunto de valores absolutos es el mismo en ambos cuerpos.

Proposición 3.23. *Para cualquier $\lambda \in \mathbb{Q}_p$ con $\lambda \neq 0$, existe un $n \in \mathbb{Z}$, tal que $|\lambda|_p = p^{-n}$. Dicho de otra forma, la imagen de $\mathbb{Q}$ por $|\ |_p$ es la misma que la de $\mathbb{Q}_p$ por $|\ |_p$.*

Aún nos quedan por ver dos propiedades para afirmar que hemos obtenido una completación de cuerpos.

Proposición 3.24. *La imagen de $\mathbb{Q}$ por la inclusión $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ es un subconjunto denso de $\mathbb{Q}_p$.*

Demostración. Tenemos que ver que cualquier bola abierta centrada en el elemento $\lambda \in \mathbb{Q}_p$ contiene un elemento (de la imagen) de $\mathbb{Q}$, es decir, una sucesión constante. Fijamos un radio ε. Tenemos que ver que existe una sucesión constante que pertenece a la bola abierta $B(\lambda, \varepsilon)$.
Sea (x_n) una sucesión de Cauchy representando a λ, y sea ε' un número más pequeño que ε. Por la propiedad de Cauchy, existe un número $N \in \mathbb{N}$ tal que $|x_n - x_m| < \varepsilon'$ cuando $n, m \geq N$. Tomamos $y = x_N$ y consideramos la sucesión constante (y). Tenemos que

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

es decir, que $|\lambda - y| < \varepsilon$. Para ver esto, tenemos en cuenta que $\lambda - (y)$ es un representante de la sucesión $(x_n - y)$, y que hemos definido

$$|x_n - y| = \lim_{n\to\infty} |x_n - y|.$$

Pero para cualquier $n \geq N$ tenemos que

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

por lo que, al aplicar el límite, llegamos a que

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

con lo cual (y) pertenece a $B(\lambda, \varepsilon)$, como queríamos demostrar. □

Proposición 3.25. *Sean $x, y \in \mathbb{Q}_p$. Si $x \neq y$, entonces existe un número racional $c \in \mathbb{Q}$ tal que $|x - c|_p < |x - y|_p$.*

Demostración. Como $x, y \in \mathbb{Q}_p$, estos denotan a las clases de equivalencia de las sucesiones (x_n) e (y_n), luego tenemos que $x = [(x_n)]$ e $y = [(y_n)]$. Como $(x_n) \neq (y_n)$, tenemos que su diferencia $(x_n - y_n)$ no es una sucesión de Cauchy equivalente a la sucesión nula. También sabemos que $|[(x_n)] - [(y_n)]|_p = |[(x_n - y_n)]|_p > 0$, puesto que es igual a cero si y solo si $(x_n - y_n) = 0$ por definición de valor absoluto. Por tanto, existe un $n \in \mathbb{N}$ tal que $|x_n - y_n|_p \geq \varepsilon$ para todo $n \in \mathbb{N}$.
Por otro lado, para algún $M \in \mathbb{N}$, tenemos que $|x_n - x_m|_p < \frac{\varepsilon}{2}$ para todo $n, m \geq M$. Cogemos $c = x_{N+M}$. Así, para todo $n \geq N+M$, $|x_n - c|_p < \frac{\varepsilon}{2}$ y $|x_n - y_n|_p \geq \frac{\varepsilon}{2}$. Cambiando el signo en la primera de las dos anteriores desigualdades, obtenemos que $-|x_n - c|_p > -\frac{\varepsilon}{2}$. En particular,

$$|x_n - y_n|_p - |x_n - c|_p \geq \varepsilon - \frac{\varepsilon}{2} = \frac{\varepsilon}{2}.$$

Luego tenemos que $|x_n - c|_p < |x_n - y_n|_p$ y por lo tanto, llegamos a que $|x - c|_p < |x - y|_p$ como queríamos probar. □

Proposición 3.26. *Para todo p, el cuerpo $\mathbb{Q}_p$ es completo respecto al valor absoluto p-ádico $|\ |_p$, es decir, toda sucesión de Cauchy en $\mathbb{Q}_p$ converge a un elemento de $\mathbb{Q}_p$.*

Demostración. Sea (x_n) una sucesión de Cauchy en $\mathbb{Q}_p$. Si existen $x \in \mathbb{Q}_p$ y $N \in \mathbb{N}$ tales que $x_n = x$ para todo $n \geq N$, ya tendríamos todo probado, ya que $x_n \longrightarrow x$.
Supongamos entonces que no estamos en este caso. Para cada $n \in \mathbb{N}$, sea $n' \in \mathbb{N}$ el último natural tal que $n' > n$ y $x_n \neq x_{n'}$. Por la Proposición 3.25 para cada $n \in \mathbb{N}$ existe un $a_n \in \mathbb{Q}$ tal que $|x_n - a_n|_p < |x_n - x_{n'}|_p$.
Sea $\varepsilon > 0$, existe un $N \in \mathbb{N}$ tal que $|x_n - x_m|_p < \frac{\varepsilon}{3}$ para todo $n, m \geq N$. Por la desigualdad

triangular, tenemos

$$\begin{aligned}|a_n - a_m|_p &= |a_n - x_n + x_n - x_m + x_m - a_m|_p \\ &\leq |a_n - x_n|_p + |x_n - x_m|_p + |x_m - a_m|_p \\ &< |x_n - x_{n'}|_p + |x_n - x_m|_p + |x_m - x_{m'}|_p \\ &< \frac{\varepsilon}{3} + \frac{\varepsilon}{3} + \frac{\varepsilon}{3} = \varepsilon\end{aligned}$$

para todo $n, m \geq N$. Por lo tanto, (a_n) es una sucesión de Cauchy formada por números racionales, es decir, $(a_n) \in \mathbb{Q}$. Así, como sabemos que $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$, tenemos que $[(a_n)] \in \mathbb{Q}_p$ (la clase de equivalencia de la sucesión (a_n)).
Sea $\varepsilon > 0$, existe un $N \in \mathbb{N}$ tal que $|x_n - x_m|_p < \frac{\varepsilon}{3}$ y $|a_n - a_m|_p < \frac{\varepsilon}{3}$ para todo $n, m \geq N$. En particular, $|x_N - a_N|_p < \frac{\varepsilon}{3}$ y también $|a_N - [(a_m)]|_p \leq \frac{\varepsilon}{3}$ (en esta última, consideramos a_N como un elemento de $\mathbb{Q}_p$).
Usando otra vez la desigualdad triangular, tenemos

$$\begin{aligned}|x_n - [(a_m)]|_p &= |x_n - x_N + x_N - a_N + a_N - [(a_m)]|_p \\ &\leq |x_n - x_N|_p + |x_N - a_N|_p + |a_N - [(a_m)]|_p \\ &< \frac{\varepsilon}{3} + \frac{\varepsilon}{3} + \frac{\varepsilon}{3} = \varepsilon\end{aligned}$$

para todo $n \geq N$. Por lo tanto, hemos llegado a que $|x_n - [(a_m)]|_p < \varepsilon$ o, dicho de otra forma, que $x_n \longrightarrow [(a_m)] \in \mathbb{Q}_p$.
Por lo tanto, $\mathbb{Q}_p$ es completo respecto al valor absoluto p-ádico $|\ |_p$ para todo p. □

Una vez visto todo esto, podemos enunciar el siguiente teorema.

Teorema 3.27. *Para cada primo $p \in \mathbb{Z}$, existe un cuerpo $\mathbb{Q}_p$ con un valor absoluto no arquimediano $|\ |_p$, tal que:*

(I) existe una inclusión de cuerpos $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$, y el valor absoluto inducido por $|\ |_p$ en $\mathbb{Q}$ a través de esta inclusión es el valor absoluto p-ádico;

(II) la imagen de $\mathbb{Q}$ por esta inclusión es densa en $\mathbb{Q}_p$ (respecto al valor absoluto $|\ |_p$);

(III) $\mathbb{Q}_p$ es completo respecto al valor absoluto $|\ |_p$.

El cuerpo $\mathbb{Q}_p$ satisfaciendo (I),(II) y (III) es único salvo isomorfismos que conservan los valores absolutos.

Demostración. Lo único que nos falta para probar el teorema anterior es la unicidad. Para ello, consideramos otro cuerpo $\mathbb{K}$. Podemos pensar en la inclusión $\mathbb{Q} \hookrightarrow \mathbb{K}$ como una

función definida en un subconjunto denso de $\mathbb{Q}_p$. Como esta función tiene que conservar los valores absolutos de cualquier elemento de $\mathbb{Q}$, tiene que ser continua. Así, cualquier función continua definida en un subconjunto denso puede ser extendida únicamente en el cuerpo entero, por lo que tenemos una función $\mathbb{Q}_p \longrightarrow \mathbb{K}$ la cual es la única extensión continua de la inclusión de $\mathbb{Q}$ en $\mathbb{K}$. Es fácil ver ahora que es un isomorfismo que preserva los valores absolutos, y es único por construcción. □

3.3. Explorando $\mathbb{Q}_p$

En esta sección nos basaremos en las diferentes propiedades del cuerpo $\mathbb{Q}_p$ más que en como hemos construido este cuerpo. Algunas de sus propiedades más importantes serán:

- hay un valor absoluto $|\ | = |\ |_p$ en $\mathbb{Q}_p$, y $\mathbb{Q}_p$ es completo respecto de este valor absoluto;
- hay una inclusión $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ cuya imagen es densa en $\mathbb{Q}_p$, y la restricción del valor absoluto $|\ |_p$ en la imagen de $\mathbb{Q}$ coincide con el valor absoluto p-ádico;
- el conjunto de valores de $\mathbb{Q}$ y de $\mathbb{Q}_p$ bajo $|\ |_p$ es el mismo, en concreto, los dos conjuntos
$$\{x \in \mathbb{R}^+ : x = |\lambda|_p \text{ para algún } \lambda \in \mathbb{Q}\}$$
y
$$\{x \in \mathbb{R}^+ : x = |\lambda|_p \text{ para algún } \lambda \in \mathbb{Q}_p\}$$
son ambos iguales al conjunto $\{p^n : n \in \mathbb{Z}\} \cup \{0\}$ de potencias de p, junto con 0.

A partir de ahora, identificaremos $\mathbb{Q}$ como su imagen bajo la inclusión en $\mathbb{Q}_p$, es decir, pensaremos en $\mathbb{Q}$ como un subcuerpo de $\mathbb{Q}_p$.

Lema 3.28. *Para cada $x \in \mathbb{Q}_p$, $x \neq 0$, existe un entero $n \in \mathbb{Z}$ tal que $|x|_p = p^{-n}$.*

Otra forma de decir esto es en términos de la valoración p-ádica.

Lema 3.29. *Para cada $x \in \mathbb{Q}_p$, $x \neq 0$, existe un entero $v_p(x)$ tal que $|x|_p = p^{-v_p(x)}$. En otras palabras, la valoración p-ádica se extiende a $\mathbb{Q}_p$.*

Como hicimos antes, extendemos v_p a todos los $\mathbb{Q}_p$ teniendo en cuenta que $v_p(0) = +\infty$. Más adelante, describiremos los elementos de $\mathbb{Q}_p$ y podremos describir v_p de una manera más precisa.

Ahora empezaremos a estudiar la estructura de $\mathbb{Q}_p$. Sabemos que es un cuerpo con una valoración no arquimediana, por lo tanto, podemos considerar su anillo de valoración correspondiente.

Definición 3.30. El anillo de los enteros p-ádicos es el anillo de valoración

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

Como $\mathbb{Z}_p$ es la bola cerrada unitaria con centro 0, sabemos que $\mathbb{Z}_p$ es un conjunto cerrado en $\mathbb{Q}_p$, ya que toda bola cerrada lo es.

Proposición 3.31. *El anillo $\mathbb{Z}_p$ de los enteros p-ádicos es un anillo local cuyo ideal maximal es el ideal principal $p\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p < 1\}$. Además:*

(I) $\mathbb{Q} \cap \mathbb{Z}_p = \mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} : p \nmid b\}$.

(II) La inclusión $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ tiene una imagen densa. En particular, dados $x \in \mathbb{Z}_p$ y $n \geq 1$, existe un $\alpha \in \mathbb{Z}$, $0 \leq \alpha \leq p^n - 1$, tal que $|x - a| \leq p^{-n}$. El entero α con estas propiedades es único.

(III) Para cualquiera $x \in \mathbb{Z}_p$, existe una sucesión de Cauchy α_n, convergente a x, que es de la siguiente forma

- *$\alpha_n \in \mathbb{Z}$ satisfaciendo que $0 \leq \alpha_n \leq p^n - 1$;*
- *para todo n tenemos que $\alpha_n \equiv \alpha_{n-1} \pmod{p^{n-1}}$.*

La sucesión (α_n) con estas propiedades es única.

Demostración. Muchas de estas propiedades se siguen directamente de cosas que ya hemos probado. Para empezar, veamos que el anillo de valoración $\mathbb{Z}_p$ es un anillo local. Para ver que el ideal valoración está generado por p, utilizamos el Lema 3.28

$$|x| < 1 \Longrightarrow |x| \leq \frac{1}{p} \Longrightarrow \left|\frac{x}{p}\right| \leq 1 \Longrightarrow x \in p\mathbb{Z}_p.$$

Esto muestra que el ideal de valoración está contenido en $p\mathbb{Z}_p$, pero el ideal de valoración es un ideal maximal y $p\mathbb{Z}_p \neq \mathbb{Z}_p$. Veamos ahora las siguientes propiedades:

(I) Está claro que se cumple, porque ya sabíamos que $\mathbb{Z}_{(p)}$ era el anillo de valoración en $\mathbb{Q}$ correspondiente a la valoración p-ádica.

(II) Para ver esta segunda propiedad, elegimos un $x \in \mathbb{Z}_p$ y $n \geq 1$. Como $\mathbb{Q}$ es denso en $\mathbb{Q}_p$, uno puede encontrar un $a/b \in \mathbb{Q}$ suficientemente cerca de x tal que

$$\left|x - \frac{a}{b}\right| \leq p^{-n} < 1.$$

Lo que realmente tenemos que ver es que podemos elegir en realidad un entero. Pero para a/b, tendremos

$$\left|\frac{a}{b}\right| \leq \text{máx}\left\{|x|, \left|x - \frac{a}{b}\right|\right\} \leq 1,$$

lo cual nos dice que si $a/b \in \mathbb{Z}_{(p)}$, tenemos que $p \nmid b$. Ahora cabe recordar que por los teoremas elementales de congruencias, si $p \nmid b$, existe un entero $b' \in \mathbb{Z}$ tal que $bb' \equiv 1 \pmod{p^n}$, lo cual implica que

$$\left|\frac{a}{b} - ab'\right| \leq p^{-n},$$

y por supuesto que $ab' \in \mathbb{Z}$. Por último, tenemos que encontrar un entero entre 0 y $p^n - 1$, pero este entero lo podemos tomar de la relación entre las congruencias módulo potencias de p^n y el valor absoluto p-ádico. Tomamos α como el único entero tal que

$$0 \leq \alpha \leq p^n - 1 \ \text{ y } \ \alpha \equiv ab' \pmod{p^n}$$

y esto nos da que $|x - \alpha| \leq p^{-n}$, lo cual era lo que buscábamos.

(III) Se sigue directamente de (II) usando para ello la sucesión de enteros α_n con $n = 1, 2, \ldots$

□

De esta proposición podemos deducir un par de cosas importantes como que $\mathbb{Z}_p$ es la completación de $\mathbb{Z}$ respecto al valor absoluto p-ádico. También es importante la sucesión que construimos para demostrar el último apartado, puesto que dicha sucesión es una de las "sucesiones coherentes" que vimos en el primer capítulo.

Corolario 3.32. *$\mathbb{Q}_p = \mathbb{Z}_p[1/p]$, es decir, para todo $x \in \mathbb{Q}_p$ existe un $n \geq 0$ tal que $p^n x \in \mathbb{Z}_p$. La aplicación $\mathbb{Q}_p \longrightarrow \mathbb{Q}_p$ dada por $x \mapsto p\,x$ es un homeomorfismo, es decir, una aplicación continua con inversa también continua.*

Demostración. Si $x \in \mathbb{Q}_p$, podemos calcular su valoración $v_p(x)$. Si $v_p(x) \geq 0$, entonces x es también un elemento de $\mathbb{Z}_p$. Si no, $v_p(x)$ es negativo, y tenemos lo siguiente

$$v_p(p^{-v_p(x)}x) = v_p(x) + v_p(x) = 0,$$

lo cual significa que $p^{-v_p(x)}x \in \mathbb{Z}_p$, como queríamos probar. Esa multiplicación por p es un homeomorfismo, lo cual es inmediato por el hecho de que las operaciones del cuerpo son funciones continuas. □

La valoración p-ádica v_p puede ser extendida a $\mathbb{Q}_p$, porque para cualquier $x \in \mathbb{Q}_p$ existe un entero $v_p(x)$ tal que $|x|_p = p^{-v_p(x)}$.

Uno de los aspectos más importantes de estos resultados es que la topología de $\mathbb{Q}_p$ está muy relacionada con la estructura algebraica de este cuerpo (multiplicación por p, subanillos). Por ejemplo, tenemos que para $x, y \in \mathbb{Q}_p$, se cumple que

$$|x - y| \leq p^{-n} \ \text{ si y solo si } \ x - y \in p\,\mathbb{Z}_p.$$

Corolario 3.33. *Para cualquier $n \geq 1$, la sucesión*

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

es exacta, siendo

$$\begin{aligned} \mathbb{Z}_p &\longrightarrow \mathbb{Z}_p \\ x &\longmapsto p^n\, x, \end{aligned}$$

y las aplicaciones son continuas (tomando en $\mathbb{Z}/p^n\mathbb{Z}$ la topología discreta). En particular,

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

Una sucesión

$$A \xrightarrow{f} B \xrightarrow{g} C$$

es exacta si la imagen de la aplicación f es igual al núcleo de la aplicación g, es decir, si $\mathrm{Im}(f) = \mathrm{Ker}(g)$. Una sucesión de cinco términos como la de arriba es exacta si cumple las siguientes propiedades:

- *La aplicación $\mathbb{Z}_p \longrightarrow \mathbb{Z}_p$ dada por la multiplicación por p^n es inyectiva (su núcleo es la imagen del cero, el cual es cero).*
- *Hay una aplicación $\mathbb{Z}_p \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$ que es sobreyectiva.*
- *El núcleo de esta aplicación es la imagen de $\mathbb{Z}_p$ por la primera aplicación, lo cual es $p^n\mathbb{Z}_p$.*

Vamos a trabajar ahora con los elementos de $\mathbb{Q}_p$ de una manera diferente. Nos basamos en la idea de que en un conjunto compacto cualquiera (como por ejemplo $\mathbb{Q}_p$), podemos encontrar una sucesión de Cauchy convergente a un elemento en particular. Trabajaremos con estos elementos como sucesiones coherentes y expansiones p-ádicas.

Dado $x \in \mathbb{Z}_p$, podemos encontrar una sucesión de Cauchy convergente a x. Esta sucesión es coherente, es decir, verifica que

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

y converge a x porque $|x - \alpha_n|_p \leq p^{-n}$. Tenemos que esta sucesión es única.
Supongamos ahora que existe esta sucesión (α_n). La propiedad de coherencia hace que sea una sucesión de Cauchy, porque $|\alpha_{n+1} - \alpha_n|_p \leq p^{-n}$. Por lo tanto, tiene que converger a algún elemento, el cual estará en $\mathbb{Z}_p$ porque los diferentes α están en $\mathbb{Z}$.

Todo esto sugiere que podemos identificar los elementos de $\mathbb{Z}_p$ con este tipo de sucesiones. Denotaremos por π_n a las proyecciones definidas de la siguiente manera

$$\begin{aligned} \pi_n : \mathbb{Z}_p &\longrightarrow \mathbb{Z}/p^n\mathbb{Z} \\ x &\longmapsto \pi_n(x) = \alpha_n \ (\text{mód } p^n) \\ x = a_0 + a_1 p + a_2 p^2 + \cdots + &\longmapsto \pi_n(x) = (a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1}p^{n-1}) \text{ mód } p^n. \end{aligned}$$

Identificaremos a cada uno de estos conjuntos $\mathbb{Z}/p^n\mathbb{Z}$ como un anillo topológico con la topología discreta. Consideramos ahora la aplicación

$$\begin{aligned} \psi_n : \quad \mathbb{Z}/p^{n+1}\mathbb{Z} &\longrightarrow \mathbb{Z}/p^n\mathbb{Z} \\ a \ (\text{mód } p^{n+1}) &\longmapsto a \ (\text{mód } p^n) \end{aligned}$$

la cual reduce el módulo del primo p en una potencia. Nuestro objetivo es considerar el producto de todos estos anillos, es decir, el anillo formando por las sucesiones (α_n) tales que $\alpha_n \in \mathbb{Z}/p^n\mathbb{Z}$.

Antes de nada, introducimos un poco de notación. Un elemento $\alpha \in \mathbb{Q}_p$ se puede escribir de diferentes formas. En el Capítulo 1, lo escribíamos como $\alpha = \sum_{i=-k}^{\infty} a_i p^i$. Sin embargo, para realizar operaciones en estos cuerpos, será más fácil escribirlos de la siguiente forma:

$$\alpha = \ldots a_i a_{i-1} \ldots a_2 a_1 a_0 . a_{-1} a_{-2} \ldots a_{-k}$$

Para los enteros p-ádicos en $\mathbb{Z}_p$, escribiremos

$$\alpha = \ldots a_i a_{i-1} \ldots a_2 a_1 a_0$$

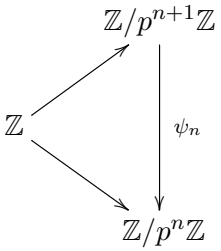
Proposición 3.34. *Si consideramos todas las aplicaciones proyectivas π_n juntas, estas definen una inclusión de la siguiente forma*

$$\varphi : \mathbb{Z}_p \hookrightarrow \prod_{n \geq 1} \mathbb{Z}/p^n\mathbb{Z}$$

que considera $\mathbb{Z}_p$ como un anillo topológico, y lo identifica con el subanillo cerrado $\prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z}$ de sucesiones coherentes, es decir, las sucesiones (α_n) tales que $\psi_n(\alpha_n) = \alpha_{n-1}$ para todo $n > 1$.

Recordaremos ahora lo que es un diagrama de homomorfismos conmutativo. Esto ocurre cuando los homomorfismos obtenidos siguiendo una ruta son los mismos que siguiendo otra.

Por ejemplo, el siguiente diagrama



es conmutativo, porque reducir módulo p^n es lo mismo que reducir módulo p^{n+1} y después reducir módulo p^n, por lo tanto, es lo mismo ir de $\mathbb{Z}$ a $\mathbb{Z}/p^n\mathbb{Z}$ que ir de $\mathbb{Z}$ a $\mathbb{Z}/p^{n+1}\mathbb{Z}$ y después a $\mathbb{Z}/p^n\mathbb{Z}$.
En resumen, para cada n, tenemos el siguiente conjunto de aplicaciones, tal y como vemos en [7].

$$\cdots \longrightarrow \mathbb{Z}/p^{n+1}\mathbb{Z} \xrightarrow{\psi_n} \mathbb{Z}/p^n\mathbb{Z} \xrightarrow{\psi_{n-1}} \cdots \xrightarrow{\psi_2} \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{\psi_1} \mathbb{Z}/p\mathbb{Z}.$$

Definición 3.35 ([7])**.** El límite inverso (o límite proyectivo) de $\mathbb{Z}/p^n\mathbb{Z}$ (respecto de ψ_n) cuando $n \longrightarrow \infty$ es

$$\varprojlim \mathbb{Z}/p^n\mathbb{Z} = \Big\{(x_n) \in \prod_n \mathbb{Z}/p^n\mathbb{Z} : \ \psi_n(x_{n+1}) = x_n \text{ para todo } \ n \geq 1\Big\}.$$

Es decir, un elemento (x_n) de $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ es una sucesión de elementos $x_n \in \mathbb{Z}/p^n\mathbb{Z}$ y que cumple que $x_{n+1} \equiv x_n$ (mód $\mathbb{Z}/p^n\mathbb{Z}$). Se llama límite inverso o proyectivo debido a que tenemos sucesivos cocientes (o proyecciones) de cada uno de ellos.

Nos basamos ahora en [2]. La aplicación

$$\varphi : \mathbb{Z}_p \longrightarrow \varprojlim \mathbb{Z}/p^n\mathbb{Z}$$

es un isomorfismo. Juntando todas las proyecciones π_n y una vez definido el límite inverso, podemos considerar el siguiente homomorfismo

$$\begin{aligned} \pi : \mathbb{Z}_p &\longrightarrow \varprojlim \mathbb{Z}/p^n\mathbb{Z} \\ x &\longmapsto (\pi_1(x), \pi_2(x), \dots) \end{aligned}$$

donde $(\pi_1(x), \pi_2(x), \dots)$ representan cada una de las sucesiones definidas por cada una de las proyecciones π_i con $i = 1, 2, \dots$ construidas anteriormente.
Recíprocamente, consideramos ahora una sucesión $(x_1, x_2, \dots) \in \varprojlim \mathbb{Z}/p^n\mathbb{Z}$. Abusando un poco de notación, escribimos x_n como el único entero tal que $0 \leq x_n \leq p^{n-1}$ que es congruente con x_n módulo p^n y lo escribimos en base p:

$$x_n = a_{n,0} + a_{n,1}p + \cdots + a_{n,n-1}p^{n-1}$$

acabando la sucesión en los términos de orden $n-1$ ya que $x_n < p^n$ por construcción. La condición $x_{n+1} \equiv x_n \pmod{p^n}$ implica que $a_{n+1,i} = a_{n,i}$ para todo $i \in [0, n-1]$. Dicho de otra forma, cuando fijamos i, la sucesión $(a_{n,i})$ es constante y por lo tanto, converge a algún a_i. Tomamos:

$$\varphi(x_1, x_2, \dots) = \dots a_i \dots a_2 a_1 a_0 \in \mathbb{Z}_p.$$

Definimos de esta forma la aplicación $\varphi : \varprojlim \mathbb{Z}/p^n\mathbb{Z} \longrightarrow \mathbb{Z}_p$, la cual es por construcción la aplicación inversa por la derecha y por la izquierda de π. Es decir, π y φ son isomorfismos inversos uno de otro.
Por lo tanto, también podemos definir los enteros p-ádicos de la siguiente forma:

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

Aún así, trabajar con esta definición de $\mathbb{Z}_p$ resulta más complicado. Por eso, definiremos más adelante los enteros p-ádicos de una forma más sencilla.

Seguimos ahora con la línea del libro [4]. Vamos a representar ahora los elementos de $\mathbb{Q}_p$ como "series de potencias de p". Empezamos con el entero p-ádico $x \in \mathbb{Z}_p$. Existe una sucesión coherente de enteros α_n convergente a x y tal que:

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

Para entender mejor cómo son los elementos αn, los escribimos en base p. Una vez escritos en esta base, es muy fácil reducirlos módulo p^n. Eliminamos todos sus elementos salvo los últimos n dígitos. Esto hace que la condición de coherencia

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

nos indique que los últimos n dígitos de ambos números son los mismos. Fijándonos en la sucesión, lo que tenemos es lo siguiente

$$\begin{aligned}
&\alpha_0 = b_0, && 0 \leq b_0 \leq p-1,\\
&\alpha_1 = b_0 + b_1 p, && 0 \leq b_1 \leq p-1,\\
&\alpha_2 = b_0 + b_1 p + b_2 p^2, && 0 \leq b_2 \leq p-1,\\
&\alpha_3 = b_0 + b_1 p + b_2 p^2 + b_3 p^3, && 0 \leq b_3 \leq p-1,
\end{aligned}$$

y así sucesivamente. Juntando todo esto, obtenemos una expansión infinita

$$x = b_0 + b_1 p + b_2 p^2 + b_3 p^3 + \dots + b_n p^n + \dots$$

Para ver que la igualdad anterior se cumple, nos tenemos que asegurar de que estas series convergen a x. Por eso, enunciamos el siguiente lema.

Lema 3.36. *Dado cualquier $x \in \mathbb{Z}_p$, las series*

$$b_0 + b_1 p + b_2 p^2 + b_3 p^3 + \cdots + b_n p^n + \cdots$$

obtenidas de la misma forma que arriba, convergen a x.

Demostración. Sabemos que las series convergen a x si su sucesión de sumas parciales converge a x. Pero las sumas parciales de nuestras series son exactamente las de α_n, las cuales convergen a x, ya que las hemos cogido de esa forma. Así, hemos probado que estas series convergen a x. □

Corolario 3.37. *Todo $x \in \mathbb{Z}_p$ puede ser escrito de la forma*

$$x = b_0 + b_1 p + b_2 p^2 + b_3 p^3 + \cdots + b_n p^n + \cdots ,$$

con $0 \leq b_i \leq p-1$, y estos coeficientes b_i son únicos.

Demostración. Ya hemos demostrado todo salvo la unicidad. Sabemos que los α_n son únicos, y esto implica que los b_n también son únicos, puesto que son los elementos en base p. □

Queremos hacer esto mismo con todos los elementos de $\mathbb{Q}_p$. Sabemos que son de la forma y/p^m con $y \in \mathbb{Z}_p$. Si desarrollamos y en serie de potencias de p y luego lo dividimos por p^m, obtenemos una serie en potencias de p donde algunas de estas potencias serán negativas. Todo esto lo podemos enunciar de la siguiente forma.

Corolario 3.38. *Todo $x \in \mathbb{Q}_p$ puede ser expresado como*

$$\begin{aligned} x &= b_{-n_0} p^{-n_0} + \cdots + b_0 + b_1 p + b_2 p^2 + \cdots + b_n p^n + \cdots \\ &= \sum_{n \geq -n_0} b_n p^n, \end{aligned}$$

con $0 \leq b_n \leq p-1$ y $-n_0 = v_p(x)$. Esta representación es única.

Demostración. Es obvio, ya que en su momento vimos la unicidad de los $v_p(x)$, y dijimos que la función de estos se aproximaba al orden. □

Todo esto está relacionado con los conceptos que vimos en el Capítulo 1. Vemos que podemos relacionar un elemento de $\mathbb{Q}_p$, es decir, un número p-ádico, con su expansión p-ádica. Los coeficientes b_n pueden ser tomados como representantes de las diferentes clases módulo p. Los números entre 0 y $p-1$ son los diferentes representantes que tomamos.

Proposición 3.39 ([8]). *Sea $\mathbb{Z}_p$ el cuerpo de los números p-ádicos.*

1. *Las unidades p-ádicas son*

$$\begin{aligned}\mathbb{Z}_p^* &= \{x \in \mathbb{Z}_p : 0 \neq b_0 \in (\mathbb{Z}/p\mathbb{Z})^*\} \\ &= \{x \in \mathbb{Z}_p : |x|_p = 1\},\end{aligned}$$

   siendo $x = b_0 + b_1 p + b_2 p^2 + \cdots + b_n p^n + \cdots$.

2. *Los únicos ideales de $\mathbb{Z}_p$ distintos de cero son los ideales principales*

$$p^k\mathbb{Z}_p = \{x \in \mathbb{Z}_p : v_p(x) \geq k\},$$

   siendo $x = b_k\, p^k + b_{k+1}\, p^{k+1} + b_{k+2}\, p^{k+2} + \cdots \in \mathbb{Z}_p$, con $b_k \neq 0$, y k puede ser negativo. En este caso, denotamos $v_p(x) = k$ y $|x|_p = p^{-k}$. Este orden será nuestro n_0 del corolario anterior.

3. *$\mathbb{Z}$ es denso en $\mathbb{Z}_p$.*

Demostración. 1. Sea x una unidad. Luego

$$x \in \mathbb{Z}_p^* \iff x \in \mathbb{Z}_p \text{ y } \frac{1}{x} \in \mathbb{Z}_p \iff |x|_p \leq 1 \text{ y } \left|\frac{1}{x}\right|_p \leq 1 \iff |x|_p = 1.$$

2. Sea $\mathcal{I}$ un ideal distinto de cero de $\mathbb{Z}_p$, y sea x un elemento de $\mathbb{Z}_p$ con valoración mínima $v_p(x) = k \geq 0$. Por lo tanto, tenemos que

$$x = p^k(b_k + b_{k+1}\, p + b_{k+2}\, p^2 + \cdots)$$

   donde el segundo factor es una unidad. Esto implica que

$$x\mathbb{Z}_p = p^k\mathbb{Z}_p \subset \mathcal{I}.$$

   Demostramos ahora que $\mathcal{I} \subset p^k\mathbb{Z}_p$, los cuales resultaran ser iguales, es decir, veremos que $\mathcal{I} = p^k\mathbb{Z}_p$. Si $\mathcal{I}$ no está contenido en $p^k\mathbb{Z}_p$, luego existe un elemento en $\mathcal{I}$ que no está en $p^k\mathbb{Z}_p$, pero ese elemento tiene que tener una valoración (orden) más pequeña que k, lo cual no puede ser porque k es la mínima valoración. Por lo tanto, $\mathcal{I} = p^k\mathbb{Z}_p$.

3. Para ver que $\mathbb{Z}$ es denso en $\mathbb{Z}_p$, tenemos que ver que para todo elemento $x \in \mathbb{Z}_p$ y todo $\varepsilon > 0$, $B(x, \varepsilon) \cap \mathbb{Z}$ es no vacío.
   Tomamos $x \in \mathbb{Z}_p$ y $\varepsilon > 0$. Existe un k suficientemente grande para el cual $p^{-k} < \varepsilon$. Tomamos como $\tilde{x} \in \mathbb{Z}$ al entero obtenido cortando la serie de x después de $x_{k-1}p^{k-1}$. Luego

$$x - \tilde{x} = x_k p^k + x_{k+1} p^{k+1} + \cdots$$

implica que

$$|x - \tilde{x}|_p \leq p^{-k} < \varepsilon.$$

Por lo tanto, $\mathbb{Z}$ es denso en $\mathbb{Z}_p$.

□

Proposición 3.40 ([3]). *Sea $x = (\alpha_n) = \sum b_i\, p^i \in \mathbb{Z}_p$. Las condiciones siguientes son equivalentes:*

(I) $x \in \mathcal{U}(\mathbb{Z}_p)$ siendo $\mathcal{U}(\mathbb{Z}_p)$ el conjunto de unidades de $\mathbb{Z}_p$;

(II) $p \nmid \alpha_1$;

(III) $p \nmid \alpha_k$ para todo $k \geq 1$;

(IV) $b_0 \neq 0$.

Demostración. Las condiciones (II),(III) y (IV) son equivalentes ya que $b_0 = \alpha_0 \equiv \alpha_1 \equiv \alpha_i$ (mód p) usando la sucesión coherente de enteros α_n que hemos construido anteriormente.
Si x es una unidad con inverso $y = (\beta_n)$, se cumple que $xy = 1$. Esto implica que $\alpha_1\beta_1 \equiv 1$ (mód p), con lo cual $p \nmid \alpha_1$.
Suponemos ahora que $p \nmid \alpha_1$ y por lo tanto $p \nmid \alpha_k$ para todo $k \geq 1$. Luego, para cada k, existe un entero β_k tal que $\alpha_k\beta_k \equiv 1$ (mód p^k). La sucesión (β_k) es coherente porque $\alpha_{k+1}\beta_{k+1} \equiv 1$ (mód p^{k+1}) y esto implica que $\alpha_k\beta_k \equiv 1 \equiv \alpha_{k+1}\beta_{k+1} \equiv \alpha_k\beta_{k+1}$ (mód p^k), utilizando que $\alpha_{k+1} \equiv \alpha_k$ (mód p^k); por lo tanto $\beta_{k+1} \equiv \beta_k$ (mód p^k). Luego, (β_k) representa a un entero p-ádico y tal que $xy = 1$, y x es una unidad de $\mathbb{Z}_p$. □

Proposición 3.41 ([3]). *Para $x = (\alpha_n) \in \mathbb{Z}_p$:*

(I) $p \mid x \iff x \notin \mathcal{U}(\mathbb{Z}_p) \iff \alpha_1 \equiv 0$ (mód p) $\iff \alpha_k \equiv 0$ (mód p) $\forall k \geq 1$;

(II) para $n \geq 1$, $p^n \mid x \iff \alpha_n \equiv 0$ (mód p^n) $\iff \alpha_k \equiv 0$ (mód p^n) $\forall k \geq n$.

Proposición 3.42 ([3]). *$\mathbb{Z}_p$ es un DFU (dominio de factorización única). El único elemento irreducible (primo) es p (y sus asociados).*
Dicho de otra forma, todo elemento $x \in \mathbb{Z}_p$ distinto de cero se puede escribir de manera única como $x = p^m\varepsilon$ donde $m \in \mathbb{Z}$ y $\varepsilon \in \mathcal{U}(\mathbb{Z}_p)$.

Demostración. Sea $x = (\alpha_n) \in \mathbb{Z}_p$ distinto de cero. Luego existe $k \geq 1$ tal que $\alpha_k \not\equiv 0$ (mód p^k). Sea n el índice mayor tal que $\alpha_n \equiv 0$ (mód p^n), con $n = 0$ si $\alpha_k \not\equiv 0$ (mód p^k) para todo k (este es el caso en el que x es una unidad, por la Proposición 3.40). Por la

Proposición 3.41, n es el entero más grande tal que $p^n \mid x$. Por lo tanto, $x = p^n\varepsilon$ donde $p \nmid \varepsilon$, con lo cual ε es una unidad.
Para probar la unicidad, suponemos que $x = p^m\eta$ donde $m \geq 0$ y $\eta \in \mathcal{U}(\mathbb{Z}_p)$. Sin pérdida de generalidad, $m \geq n$. Ahora $p^m\eta = p^n\varepsilon$, de donde tenemos que $p^{m-n}\eta = \varepsilon$. Como ε es una unidad, no es divisible por p, con lo que $m - n = 0$ y en consecuencia $m = n$ y $\eta = \varepsilon$. Por último, vemos que p es irreducible en $\mathbb{Z}_p$. Factorizamos $p = xy$, con $x = p^m\varepsilon$ e $y = p^n\eta$; luego $p = p^{m+n}\varepsilon\eta$ con $\varepsilon\eta$ el producto de dos unidades y por tanto, una unidad. Por unicidad, tenemos que $m + n = 1$, con lo que uno de los dos $m, n = 0$ y también x o y unidades. □

Ahora se puede entender por qué $\mathbb{Z}_p$ y $\mathbb{Q}_p$ son llamados objetos *locales*, específicamente, anillos locales y cuerpos locales. Una expansión en serie de potencias o de Laurent de alguna función $f(x)$ alrededor de un punto p_0 sólo puede converger cerca de p_0, aunque la función pueda definirse (como una función meromorfa) en todos los puntos de $\mathbb{C}$. Dado que una serie de potencias no tiene sentido fuera de su radio de convergencia, las series de potencias en general sólo dan información local sobre las funciones $f(x)$ (en concreto, cerca de p_0). Del mismo modo, los elementos de $\mathbb{Z}_p$ y $\mathbb{Q}_p$ darán información "local" acerca del primo $p \in \mathcal{P}$.

$\mathbb{Z}_p$ es un dominio de factorización única y su cuerpo de fracciones es $\mathbb{Q}_p$. El único elemento irreducible (primo) en $\mathbb{Z}_p$ es p.

Tenemos el siguiente diagrama

$$\begin{array}{ccc} \mathbb{Z} & \subset & \mathbb{Q} \\ \cap & & \cap \\ \mathbb{Z}_p & \subset & \mathbb{Q}_p \end{array}$$

Sea $\mathbb{Z}_{(p)} = \mathbb{Q} \cap \mathbb{Z}_p = \{\frac{a}{b} \in \mathbb{Q} : p \nmid b\} = \{x \in \mathbb{Q} \mid ordp(x) \geq 0\}$.

$$\begin{array}{ccccc} \mathbb{Z} & \subset & \mathbb{Z}_{(p)} & \subset & \mathbb{Q} \\ & & \cap & & \\ & & \mathbb{Z}_p & & \end{array}$$

Los elementos de $\mathbb{Z}_{(p)} = \mathbb{Z}_p \cap \mathbb{Q}$ son los enteros p-ádicos cuya sucesión de dígitos es en última estancia periódica (así como los racionales son los números reales cuya expansión decimal es en última estancia periódica).

$\mathbb{Z}$ es denso en $\mathbb{Z}_p$ y $\mathbb{Q}$ es denso en $\mathbb{Q}_p$.

Los números naturales son exactamente los enteros p-ádicos con un número finito de dígitos diferentes de 0. Los números enteros (estrictamente) negativos corresponden exactamente a aquellos p-ádicos cuyos dígitos, excepto un número finito, son iguales a $p - 1$.

3.4. Aritmética p-ádica

Una vez vista la construcción de los números p-ádicos, es interesante ver cómo funcionan las diferentes operaciones aritméticas entre estos números. Para ello, veremos un par de ejemplos de estas operaciones en distintos cuerpos.
Antes de nada, introducimos un poco de notación. Un elemento $\alpha \in \mathbb{Q}_p$ se puede escribir de diferentes formas. En el Capítulo 1, lo escribíamos como $\alpha = \sum_{i=-k}^{\infty} a_i p^i$. Sin embargo, para realizar operaciones en estos cuerpos, será más fácil escribirlos de la siguiente forma:

$$\alpha = \ldots a_i a_{i-1} \ldots a_2 a_1 a_0 . a_{-1} a_{-2} \ldots a_{-k}$$

Recordemos que para los enteros p-ádicos en $\mathbb{Z}_p$, escribimos

$$\alpha = \ldots a_i a_{i-1} \ldots a_2 a_1 a_0$$

Una vez visto esto, podemos ver un par de ejemplos:

(i) Adición, sustracción, multiplicación y división en $\mathbb{Q}_7$. Algunos de estos ejemplos se tomaron de los libros [5, 6].

$$\begin{array}{rr} & \ldots\ 2\ 3\ 0\ 6\ 2\ 4\ 4 \\ + & \ldots\ 1\ 6\ 5\ 2\ 3\ 3\ 2 \\ \hline & \ldots\ \mathbf{4\ 2\ 6\ 1\ 6\ 0\ 6} \end{array} \qquad \begin{array}{rr} & \ldots\ 4\ 6\ 5\ 3\ 0.\ 2\ 5 \\ + & \ldots\ 2\ 0\ 6\ 5\ 6.\ 4\ 1 \\ \hline & \ldots\ \mathbf{0\ 0\ 5\ 1\ 6.\ 6\ 6} \end{array}$$

$$\begin{array}{rr} & \ldots\ 4\ 6\ 5\ 3\ 0.\ 2\ 5 \\ - & \ldots\ 2\ 0\ 6\ 5\ 6.\ 4\ 1 \\ \hline & \ldots\ \mathbf{2\ 5\ 5\ 4\ 0.\ 5\ 4} \end{array}$$

Nótese que $-\ldots 20654.41 = \ldots 46010.26$ y restar ese número es lo mismo que sumarle su opuesto. Luego, tenemos que

$$\begin{array}{rr} & \ldots\ 4\ 6\ 5\ 3\ 0.\ 2\ 5 \\ + & \ldots\ 4\ 6\ 0\ 1\ 0.\ 2\ 6 \\ \hline & \ldots\ \mathbf{2\ 5\ 5\ 4\ 0.\ 5\ 4} \end{array}$$

Nótese que en general si $\alpha = \displaystyle\sum_{i=k}^{\infty} a_i p^i$, entonces $-\alpha = \displaystyle\sum_{i=k}^{\infty} b_i p^i$, donde

$$b_k = p - a_k, \quad b_i = (p-1) - a_i \ \text{ si } \ i > k$$

$$
\begin{array}{r}
\ldots\ 2\ 6\ 3 \\
\times\quad \ldots\ 1\ 5\ 4 \\
\hline
\ldots\ 4\ 4\ 5 \\
\ldots\ 0\ 4\ 1 \\
\ldots\ 2\ 6\ 3 \\
\hline
\ldots\ \mathbf{4\ 5\ 5}
\end{array}
\qquad
\begin{array}{r}
\ldots\ 2\ 3\ 0\ 6\ 2\ 4\ 4 \\
\times\quad \ldots\ 1\ 6\ 5\ 2\ 3\ 3\ 2 \\
\hline
\ldots\ 4\ 6\ 1\ 5\ 5\ 2\ 1 \\
\ldots\ 2\ 2\ 5\ 0\ 6\ 5 \\
\ldots\ 2\ 5\ 0\ 6\ 5 \\
\ldots\ 5\ 5\ 2\ 1 \\
\ldots\ 6\ 1\ 6 \\
\ldots\ 6\ 3 \\
\ldots\ 4 \\
\hline
\ldots\ \mathbf{4\ 3\ 2\ 0\ 3\ 0\ 1}
\end{array}
$$

$$
\begin{array}{rl|l}
\ldots 421 & & \ldots 153 \\
\cline{3-3}
-\ldots 1161 & & \ldots 615 \\
\cline{1-1}
\ldots 230 & & \\
-\ldots 153 & & \\
\cline{1-1}
\ldots 400 & &
\end{array}
$$

(II) Adición, sustracción, multiplicación y división en $\mathbb{Q}_5$.

$$
\begin{array}{r}
\ldots\ 0\ 0\ 0\ 0\ 3\ 4\ 1 \\
+\quad \ldots\ 1\ 1\ 1\ 1\ 1\ 1\ 1 \\
\hline
\ldots\ \mathbf{1\ 1\ 1\ 2\ 0\ 0\ 2}
\end{array}
\qquad
\begin{array}{r}
\ldots\ 0\ 0\ 0\ 0\ 3\ 4\ 1 \\
+\quad \ldots\ 4\ 4\ 4\ 4\ 1\ 0\ 4 \\
\hline
\ldots\ \mathbf{0\ 0\ 0\ 0\ 0\ 0\ 0}
\end{array}
$$

$$
\begin{array}{r}
\ldots\ 1\ 1\ 1\ 1\ 1\ 1\ 1 \\
+\quad \ldots\ 4\ 4\ 4\ 4\ 1\ 0\ 4 \\
\hline
\ldots\ \mathbf{1\ 1\ 1\ 0\ 2\ 2\ 0}
\end{array}
$$

Hagamos ahora una serie de operaciones distintas. Cogemos los números racionales $\frac{2}{3}$ y $\frac{5}{6}$, los calculamos en $\mathbb{Q}_5$ y los sumamos:

$$\frac{2}{3} = \cdots 313131314. = \overline{31}4.$$
$$\frac{5}{6} = \cdots 404040410. = \overline{04}10.$$

$$\begin{array}{rr} & \ldots\ 3\ 1\ 3\ 1\ 3\ 1\ 4. = \overline{31}4. \\ + & \ldots\ 4\ 0\ 4\ 0\ 4\ 1\ 0. = \overline{04}10. \\ \hline & \ldots\ \mathbf{2\ 2\ 2\ 2\ 2\ 2\ 4}. = \mathbf{\overline{2}4}. \end{array}$$

Pero

$$\begin{aligned} \overline{2}4. &= 4 + 2 \cdot (5 + 5^2 + 5^3 + \cdots) \\ &= 4 + 10 \cdot (1 + 5 + 5^2 + 5^3 + \cdots) \\ &= 4 + 10 \cdot \frac{1}{1-5} \\ &= \frac{3}{2}. \end{aligned}$$

Multipliquemos ahora $\frac{1}{6}$ por $\frac{2}{3}$.

$$\begin{aligned} \frac{2}{3} &= \cdots 313131314. = \overline{31}4. \\ \frac{1}{6} &= \cdots 40404041. = \overline{04}1. \end{aligned}$$

$$\begin{array}{rr} & \ldots\ 3\ 1\ 3\ 1\ 3\ 1\ 4. \\ \times & \ldots\ 0\ 4\ 0\ 4\ 0\ 4\ 1. \\ \hline & \ldots\ 3\ 1\ 3\ 1\ 3\ 1\ 4 \\ & \ldots\ 1\ 3\ 1\ 3\ 2\ 1 \\ & \ldots\ 0\ 0\ 0\ 0\ 0 \\ & \ldots\ 1\ 3\ 2\ 1 \\ & \ldots\ 0\ 0\ 0 \\ & \ldots\ 2\ 1 \\ & \ldots\ 0 \\ \hline & \ldots\ \mathbf{3\ 4\ 2\ 1\ 0\ 2\ 4}. \end{array}$$

El resultado es igual a $\overline{3421024}.0 = \frac{1}{9}$.

Dividamos $\frac{2}{3}$ por $\frac{1}{12}$.

$$\begin{aligned} \frac{2}{3} &= \cdots 313131314. = \overline{31}4. \\ \frac{1}{12} &= \cdots 242424243. = \overline{24}3. \end{aligned}$$

$$\begin{array}{l|l} \ldots 313131314. & \ldots 242424243. \\ \hline -\ldots 333334. & \ldots 13. \\ \hline \ldots 4242430. & \\ -\ldots 424243. & \\ \hline \ldots 000000 & \end{array}$$

Efectivamente $\frac{2}{3}$ entre $\frac{1}{12}$ es 8 y en $\mathbb{Z}_5$, $8 = 13 = 3 + 1 \cdot 5$.

Estas son algunas de las muchas operaciones aritméticas que se pueden realizar. Lo más importante de todos estos cálculos es saber en todo momento el cuerpo en el que estamos trabajando, puesto que un 4 no es lo mismo en $\mathbb{Q}_3$ que en $\mathbb{Q}_5$, y equivocarse en el cálculo de uno de estos elementos puede acarrear fallos en los pasos siguientes.

3.5. El Lema de Hensel

Continuamos basándonos en el libro [4]. El resultado que da nombre a esta sección es la propiedad algebraica más importante de los números p-ádicos. También es fundamental este resultado para otros cuerpos como $\mathbb{Q}_p$, el cual es completo respecto a una valoración no arquimediana. Este lema nos ayuda a saber si un polinomio tiene raíces en $\mathbb{Z}_p$. Se basa en aproximar raíces de un polinomio, y ver que verifican la condición para la derivada del polinomio.

Teorema 3.43 ([4])**.** *(Lema de Hensel) Sea $F(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ un polinomio cuyos coeficientes están en $\mathbb{Z}_p$. Suponemos que existe un único entero p-ádico $\alpha_1 \in \mathbb{Z}_p$ tal que*

$$F(\alpha_1) \equiv 0 \ (\text{mód } p\mathbb{Z}_p)$$

y

$$F'(\alpha_1) \not\equiv 0 \ (\text{mód } p\mathbb{Z}_p),$$

donde $F'(X)$ es la derivada de $F(X)$. Entonces existe un entero p-ádico $\alpha \in \mathbb{Z}_p$ tal que $\alpha \equiv \alpha_1 \ (\text{mód } p\mathbb{Z}_p)$ y $F(\alpha) = 0$.

Una aplicación muy importante del Lema de Hensel es encontrar las raíces de la unidad en $\mathbb{Q}_p$. Recordemos que un elemento ζ de un cuerpo es una raíz m-ésima de la unidad si $\zeta^m = 1$, y es una raíz primitiva m-ésima si $\zeta^n \neq 1$ para $0 < n < m$. En $\mathbb{R}$, solo hay dos raíces de la unidad, 1 y -1.

Para aplicar el Lema de Hensel, necesitamos un polinomio y su derivada. Como estamos buscando raíces de la unidad, consideramos $F(X) = X^m - 1$ y su derivada es $F'(X) = mX^{m-1}$. Para aplicar el Lema de Hensel, calculamos el valor de λ en $F'(X)$, y obtenemos que $F'(\lambda) = m\lambda^{m-1}$. $F'(\lambda)$ es congruente a cero módulo p si p divide a m o si divide a λ (en este caso, λ no será una raíz aproximada de $F(X)$). Por eso en la segunda condición del lema se pide que m no sea divisible por p. Para la primera condición, necesitamos encontrar una raíz aproximada.

Definición 3.44. Sean $g(X)$ y $h(X)$ polinomios en $\mathbb{Z}_p[X]$ y sean $\bar{g}(X)$ y $\bar{h}(X) \in \mathbb{F}_p[X]$ los polinomios obtenidos de reducir los coeficientes módulo p. Diremos que $g(X)$ y $h(X)$ son primos relativos módulo p si $\gcd(\bar{g}, \bar{h}) = 1$ en $\mathbb{F}_p[X]$, o equivalentemente, si existen polinomios $a(X), b(X) \in \mathbb{Z}_p[X]$ tales que

$$a(X)g(X) + b(X)h(X) \equiv 1 \pmod{p};$$

donde entendemos la relación de congruencia de los polinomios elemento a elemento, es decir, dos polinomios son congruentes módulo p si cada coeficiente de uno de ellos es congruente módulo p con el correspondiente coeficiente del otro polinomio.

Teorema 3.45. *(Segunda forma del Lema de Hensel) Sea $f(X) \in \mathbb{Z}_p[X]$ un polinomio con coeficientes en $\mathbb{Z}_p$. Entonces, existen polinomios $g_1(X), h_1(X) \in \mathbb{Z}_p[X]$ tales que*

(I) $g_1(X)$ es mónico;

(II) $g_1(X)$ y $h_1(X)$ son primos relativos módulo p;

(III) $f(X) \equiv g_1(X)h_1(X) \pmod{p}$ (coeficiente a coeficiente).

Entonces existen polinomios $g(X), h(X) \in \mathbb{Z}_p[X]$ tales que

(I) $g(X)$ es mónico;

(II) $g(X) \equiv g_1(X) \pmod{p}$ y $h(X) \equiv h_1(X) \pmod{p}$;

(III) $f(X) = g(X)h(X)$.

3.6. Local y globalmente

Una de las consecuencias del Lema de Hensel es que podemos encontrar raíces de polinomios con coeficientes enteros. No es difícil ver que un polinomio tiene raíces en $\mathbb{Z}_p$, para ello basta ver si el polinomio tiene raíces módulo p. Lo mismo pasa con $\mathbb{R}$, donde podemos

encontrar raíces de manera sencilla, ya que un polinomio puede tener signos opuestos en dos puntos x_1 y x_2, luego deberá existir una raíz entre estos dos valores.

Encontrar raíces en $\mathbb{Q}$ resulta más interesante, pues si estas están en $\mathbb{Q}$, también están en $\mathbb{R}$ y en $\mathbb{Q}_p$ para todo $p \leq \infty$. Entonces, como toda raíz en $\mathbb{Q}$ tiene que estar en $\mathbb{Q}_p$, no pueden existir raíces racionales si para algún $p \leq \infty$ no existen raíces p-ádicas.
Para estudiar la existencia o no de estas raíces, nos basamos en la analogía de Hensel, la cual enunciaba que los cuerpos p-ádicos eran equivalentes a los cuerpos de las series de Laurent, y que el estudio de estos elementos nos daba información local.
Por último, cabe destacar el hecho de que las raíces de $\mathbb{Q}$ son también raíces de $\mathbb{Q}_p$ para todo p significa que una raíz "global" es a su vez "local" para cada p. El proceso inverso implicaría que una raíz "local" puede dar lugar a una raíz "global". Por consiguiente, juntando la información local para todo $p \leq \infty$ obtenemos información global.
Un ejemplo muy interesante son las ecuaciones diofánticas, para las cuales tenemos que buscar soluciones en $\mathbb{Q}$, o al menos decidir la existencia de alguna. La ecuación $X^2+Y^2+Z^2 = 0$ solo tiene la solución trivial $X = Y = Z = 0$ en $\mathbb{R}$. Por tanto, puesto que cualquier otra solución en $\mathbb{Q}$ también está en $\mathbb{R}$ podemos concluir que no existen raíces en $\mathbb{Q}$.

Existe una estrecha relación entre las propiedades locales y las globales. Si una solución es global, es decir, está en $\mathbb{Q}$, entonces también existen soluciones locales para todos los primos. Sin embargo, que la falta de soluciones globales implique la falta de soluciones locales es más difícil de demostrar.
Principio Local-Global: *La existencia o no de soluciones en $\mathbb{Q}$ (globales) de una ecuación diofántica puede conocerse estudiando, para cada $p \leq \infty$, las soluciones de la ecuación en $\mathbb{Q}_p$ (locales).*
Cabe destacar que en ningún caso, hemos afirmado que una ecuación tiene soluciones en $\mathbb{Q}$ si y solo si tiene soluciones en todos los $\mathbb{Q}_p$. Este principio resulta fundamental para el siguiente resultado.

Teorema 3.46 ([9])**.** *(Hasse-Minkowski) Sea la forma cuadrática*

$$F(X_1, X_2, \ldots, X_n) \in \mathbb{Q}[X_1, X_2, \ldots, X_n]$$

que resulta ser un polinomio homogéneo de grado 2 en n variables. Entonces, la ecuación

$$F(X_1, X_2, \ldots, X_n) = 0$$

tiene soluciones no triviales en $\mathbb{Q}$ si y solo si tiene soluciones no triviales en $\mathbb{Q}_p$ para cada $p \leq \infty$.

Definición 3.47. Se dice que dos números enteros son primos relativos si no tienen ningún factor primo en común o, equivalentemente, si no existe otro divisor distinto de 1 y -1.

Enunciamos ahora la proposición que recoge todos los posibles casos que se pueden estudiar para saber si una ecuación tiene o no soluciones.

Proposición 3.48. *Sean a, b y c tres enteros primos relativos libres de cuadrados. La ecuación*

$$aX^2 + bY^2 + cZ^2 = 0$$

tiene soluciones no triviales en $\mathbb{Q}$ si y solo si se cumplen las siguientes condiciones:

(I) a, b y c no son todos positivos o todos negativos;

(II) para cada primo distinto de 2 divisor de a, existe un número entero $r \in \mathbb{Z}$ tal que $b + r^2 c \equiv 0$ (mód p) y, análogamente para todos los primos distintos de 2 divisores de b y c;

(III) si a, b y c son distintos de 2, entonces la suma de dos de ellos es divisible por 4;

(IV) si $a = 2$, se tiene que $b + c$ o $a + b + c$ es divisible por 8 y, análogamente para los casos $b = 2$ y $c = 2$.

Bibliografía

[1] Baker, A., An Introduction to p-adic Numbers and p-adic Analysis.

Estas notas fueron escritas para un último curso de grado impartido en la Universidad de Manchester en Septiembre de 1988. Disponible en `http://www.maths.gla.ac.uk/~ajb/dvi-ps/padicnotes.pdf`

[2] Caruso, X., Computations with p-adic numbers.

Este documento contiene las notas de una conferencia que Xavier Caruso dió en el "Journées Nationales du Calcul Formel" (JNCF) en enero de 2017. Disponible en `https://arxiv.org/abs/1701.06794v1`

[3] Cremona, J. E., Introduction to Number Theory. Lecture Notes 2018.

Disponible en `http://homepages.warwick.ac.uk/staff/J.E.Cremona/courses/MA257/ma257.pdf`

[4] Gouvêa, F. Q., p-adic Numbers. An Introduction, Springer-Verlag, 2nd ed., 1997.

[5] Katok, S., p-adic Analysis Compared with Real, Student Mathematical Library, vol. 37, AMS, 2007.

[6] Koblitz, N., p-adic Numbers, p-adic Analysis, and Zeta-Functions, 2nd ed., Springer-Verlag, 1984.

[7] Martin, K., Number Theory II, Spring 2010 Notes.

Disponible en `http://www2.math.ou.edu/~kmartin/ntii/ntii.pdf`

[8] Oggier, F., Introduction to Algebraic Number Theory.

Apuntes de clase para la introducción a la teoría de números algebraicos. Dados en NTU de enero a abril de 2009 y 2010. Disponible en `http://www1.spms.ntu.edu.sg/~frederique/ANT10.pdf`

[9] Serre, J. P., A course in Arithmetic, Springer-Verlag, 1973.