Sección de Matemáticas
Universidad de La Laguna

Claire Marie Hubbard

Introducción a los números p-ádicos

An Introduction To *p*-adic Numbers

Trabajo Fin de Grado
Grado en Matemáticas
La Laguna, Julio de 2023

Dirigido por
Evelia Rosa García Barroso

Evelia Rosa García Barroso
Departamento de Matemáticas,
Estadística e I.O.
Universidad de La Laguna
38200 La Laguna, Tenerife

Agradecimientos

En primer lugar, me gustaría agradecer a mi familia por su apoyo incondicional durante todo el grado y a lo largo de mi vida. Especialmente, quiero agradecer a mi padre por estar siempre ahí para ayudarme a encontrar soluciones a mis problemas. Han sido un pilar fundamental en mi camino.

A mi tutora Evelia, quiero agradecerle por su orientación, conocimientos y el tiempo dedicado a ayudarme en el desarrollo de este trabajo.

A mi pareja, agradezco su calma, paciencia, cariño y apoyo que me ayudó a dar el último empujón en la recta final.

A mis amigos, con quienes compartí innumerables momentos y risas que alegraban mi día a día. Siempre estuvieron ahí para levantar mi ánimo cuando más lo necesitaba.

Claire Marie Hubbard
La Laguna, 10 de julio de 2023

Resumen · Abstract

Resumen

Esta memoria trata de una introducción a los números p-ádicos y consta de cuatro bloques. El primero consiste en fijar las bases para construir nuestra teoría de los números p-ádicos. Esto incluye valoraciones, valores absolutos, distancias y anillos de valoración. En la segunda parte, resolveremos congruencias de módulo p^n y estudiaremos el Lema de Hensel para la existencia y unicidad de soluciones de polinomios módulo potencias de p. En la tercera, analizaremos los valores absolutos sobre $\mathbb{Q}$, donde confirmamos esencialmente que solo existen tres tipos y construiremos el cuerpo de los números p-ádicos $\mathbb{Q}_p$. Por último, exploraremos el cuerpo $\mathbb{Q}_p$, abordando los enteros p-ádicos $\mathbb{Z}_p$ y dando dos posibles descripciones de los elementos de $\mathbb{Q}_p$ en términos de secuencias coherentes y de expansiones p-ádicas.

Palabras clave: *Valoración – Valor absoluto – Anillo de valoración – Lema de Hensel – Sucesión coherente– Número p-ádico – Completaciones – Cuerpo de los números p-ádicos – Enteros p-ádicos.*

Abstract

This introductory essay about p-adic numbers is divided into four sections. The first aims to establish the foundations for building our theory of p-adic numbers. This includes valuations, absolute values, distances, and valuation rings. In the second part, we will solve congruences modulo p^n and study Hensel's Lemma for the existence and uniqueness of solutions to polynomials modulo powers of p. The third section is an analysis of the absolute values on $\mathbb{Q}$, where we confirm that essentially there are only three types and where we will construct the field of p-adic numbers, denoted by $\mathbb{Q}_p$. Lastly, we will explore the field $\mathbb{Q}_p$, discussing p-adic integers, denoted by $\mathbb{Z}_p$, and providing two possible descriptions of the elements in $\mathbb{Q}_p$ in terms of coherent sequences and of p-adic expansions.

Keywords: *Valuation – Absolute value – Valuation ring – Hensel's Lemma – Coherent sequence – p-adic number – Completions – Field of p-adic numbers – p-adic integers.*

Contenido

Introducción

Durante el último siglo, los números p-ádicos han despertado un creciente interés en la comunidad matemática, apareciendo en amplias ramas, incluso en la Física y la Criptografía. Estos fueron introducidos por el matemático alemán Kurt Hensel en 1897, quien exploraba una analogía entre el anillo de los enteros $\mathbb{Z}$ con su cuerpo de fracciones $\mathbb{Q}$ y el anillo de polinomios con coeficientes complejos $\mathbb{C}[x]$ junto con su cuerpo de fracciones $\mathbb{C}(x)$.

La definición formal de un número p-ádico es la expansión de Laurent en potencias de p de cola finita, donde p es un número primo. Además, con *cola finita* nos referimos a que hay una cantidad finita de potencias de p con exponente negativo, en cambio con exponente positivo pueden haber infinitas.

Los números p-ádicos representan una extensión de los números racionales y con ellos viene asociado el valor absoluto p-ádico. Mientras que en los números reales el valor absoluto mide la distancia de un número al cero en la recta numérica, en los números p-ádicos el valor absoluto se basa en la divisibilidad por potencias de p. Cuanto más divisible sea un número p-ádico por potencias de p, más pequeño será su valor absoluto p-ádico, lo cual resulta contraintuitivo a primera vista. Si comenzamos con el valor absoluto usual y buscamos una completación de $\mathbb{Q}$, obtenemos $\mathbb{R}$, pero si hacemos lo mismo con el valor absoluto p-ádico, obtenemos otra distinta. Además, al existir infinitos números primos, existirán infinitas completaciones de $\mathbb{Q}$ en función del número primo p elegido.

Un matemático destacado por sus contribuciones en el campo de los números p-ádicos y la Geometría Aritmética en la actualidad es el ganador de la medalla Fields de 2018, Peter Scholze. Sus contribuciones han tenido un impacto significativo en la comprensión de los números p-ádicos y su relación con la Geometría. La labor de Peter Scholze ha inspirado a muchos matemáticos y ha impulsado investigaciones adicionales en los números p-ádicos y temas relacionados.

Impulsados por la singularidad inherente de los números p-ádicos y los notables avances que han generado en el ámbito académico actual, elaboramos

esta memoria con el objetivo primordial de profundizar en su comprensión y estudio. Dicha memoria se divide en cuatro secciones.

El primer bloque se centra en establecer los fundamentos necesarios para construir nuestra teoría de los números p-ádicos. Aquí, trabajaremos conceptos como valoraciones, valores absolutos, distancias y anillos de valoración, sentando así las bases para nuestro estudio.

En la segunda parte, nos adentraremos en la resolución de congruencias módulo p^n y dedicaremos especial atención al Lema de Hensel. Este lema será una herramienta clave para demostrar la existencia y unicidad de soluciones de polinomios módulo potencias de p.

La tercera sección estará dedicada al análisis de los valores absolutos en el cuerpo de los números racionales $\mathbb{Q}$. Durante este análisis, confirmaremos esencialmente que existen únicamente tres tipos de valores absolutos. Asimismo, llevaremos a cabo la construcción del cuerpo de los números p-ádicos, conocido como $\mathbb{Q}_p$.

Por último, en el cuarto bloque, exploraremos el cuerpo $\mathbb{Q}_p$, centrándonos en los enteros p-ádicos $\mathbb{Z}_p$. En esta sección, proporcionaremos dos posibles descripciones de los elementos de $\mathbb{Q}_p$: una basada en secuencias coherentes y otra basada en expansiones p-ádicas.

1

Fundamentos

En este capítulo, vamos a introducir una nueva función valor absoluto en el cuerpo de los racionales $\mathbb{Q}$. Esto nos aportará una manera distinta de medir distancias. Una vez realizado eso, podremos definir los números p-ádicos.

Para ello, debemos empezar con los racionales, $\mathbb{Q}$, aunque antes de eso vamos a trabajar en un cuerpo arbitrario $\mathbb{K}$. Aún así, el ejemplo principal que vamos a tener en mente siempre será $\mathbb{Q}$.

Nos interesa construir una teoría abstracta de los valores absolutos que ya conocemos y buscar otras funciones que tengan propiedades similares.

Algo para tener en cuenta desde el principio será que deberíamos pensar en los nuevos valores absolutos como maneras de medir el tamaño.

La referencia principal que hemos seguido para este capítulo es [2].

1.1. Valor absoluto sobre un cuerpo

Definición 1.1. *Sean A un dominio de integridad y $\mathbb{K}$ su cuerpo de fracciones. Se denomina valoración sobre A a una aplicación $v : \mathbb{K}\backslash\{0\} \longrightarrow \mathbb{Z}$ que satisface:*

(i) $v(xy) = v(x) + v(y)$;
(ii) $v(x + y) \geq \min\{v(x), v(y)\}$.

Por convenio tomamos $v(0) = \infty$.

Nos vamos a centrar en la valoración p-ádica, que se define como sigue:

Proposición 1.2. *Sea $p \in \mathbb{Z}$ un número primo. La aplicación*

$$v_p : \mathbb{Q}\backslash\{0\} \longrightarrow \mathbb{Z},$$

donde para cualquier $n \in \mathbb{Z}\backslash\{0\}$, $v_p(n)$ es el único entero no negativo que satisface que

$$n = p^{v_p(n)} n',$$

con n' no divisible por p y para todo $z = \frac{a}{b} \in \mathbb{Q}\backslash\mathbb{Z}$,

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

es una valoración.

Demostración. Sean p un número primo, $x = \frac{a}{b}, y = \frac{c}{d} \in \mathbb{Q}$. Como $a, b, c, d \in \mathbb{Z}$, existen $a', b', c', d' \in \mathbb{Z}$ tales que $a = p^{v_p(a)}a'$, $b = p^{v_p(b)}b'$, $c = c^{v_p(c)}c'$ y $d = p^{v_p(d)}d'$ donde p no divide ni a a' ni a b' ni a c' ni a d'. Por tanto, podemos tomar $x' = \frac{a'}{b'}, y' = \frac{c'}{d'} \in \mathbb{Q}$ que cumplen que $x = p^{v_p(a)-v_p(b)}x', y = p^{v_p(c)-v_p(d)}y'$ y p no divide ni al numerador ni al denominador de x' e y'.

Está claro que $v_p(x) = v_p(a) - v_p(b) \in \mathbb{Z}$. Supongamos que $\frac{a}{b} = \frac{c}{d}$, entonces existe $z \in \mathbb{Z}\backslash\{0\}$ que cumple que $c = za$ y $d = zb$. Se sigue que $v_p(\frac{c}{d}) = v_p(\frac{za}{zb}) = v_p(za) - v_p(zb)$. Además, $z \in \mathbb{Z}$, luego también existe $z' \in \mathbb{Z}$ no divisible por p cumpliendo que $z = p^{v_p(z)}z'$. Por tanto, $za = p^{v_p(z)+v_p(a)}z'a'$, $zb = p^{v_p(z)+v_p(b)}z'b'$ y p no dividirá ni a $z'a'$ ni a $z'b'$, deduciendo así que $c' = z'a'$ y $d' = z'b'$. Finalmente, tenemos que $v_p(\frac{c}{d}) = v_p(z) + v_p(a) - v_p(z) - v_p(b) = v_p(a) - v_p(b) = v_p(\frac{a}{b})$. Concluimos que la aplicación v_p está bien definida.

Veamos que se cumple la primera condición de la Definición 1.1. Como $xy = p^{v_p(x)}x' \cdot p^{v_p(y)}y' = p^{v_p(x)+v_p(y)}x'y'$, se tiene que $v_p(xy) = v_p(x) + v_p(y)$, ya que si p no divide ni a a' ni a b' ni a c' ni a d', tampoco puede dividir a $a'b'$ ni a $c'd'$.

Para la segunda condición de la Definición 1.1, suponemos que $v_p(x) = \alpha, v_p(y) = \beta \in \mathbb{Z}$ y que sin pérdida de generalidad $\alpha \leq \beta$. Tenemos que $x + y = p^{v_p(x)}x' + p^{v_p y}y' = p^{\alpha}(x' + p^{\beta-\alpha}y')$. Entonces, sabemos que como poco, p^{α} divide a $x + y$, ya que podría ocurrir que el numerador de $(x' + p^{\beta-\alpha}y') = \frac{a'd' + p^{\beta-\alpha}c'b'}{b'd'}$ sea un múltiplo de p. Por tanto, hemos probado la segunda condición de la definición de valoración. □

La valoración de la Proposición 1.2 se conoce como la valoración p-ádica. Además, esta aplicación restringida a $\mathbb{Z}$, aunque no cumple ser valoración porque $\mathbb{Z}$ no es un cuerpo, cumple las propiedades (i) y (ii) de la Definición 1.1.

Ejemplo 1.3.

En este ejemplo se puede apreciar que la teoría que estamos desarrollando es bastante general y puede ser aplicado, casi sin cambios, en todo tipo de contextos. El ejemplo que vamos a ver sirve para confirmar la intuición de Hensel sobre la similitud entre $\mathbb{Q}$ y cuerpos de fracciones de funciones.

Sean F un cuerpo cualquiera, $F[t]$ el anillo de polinomios con coeficientes en F y $F(t)$ el cuerpo de funciones racionales sobre F, que es el cuerpo de fracciones cuyos elementos son de la forma $\frac{f(t)}{g(t)}$ donde $f(t), g(t) \in F[t]$ y $g(t)$ es no nulo.

Primero, para cualquier polinomio $f(t) \in F[t]$, definimos $v_\infty(f(t)) = -deg(f(t))$ y lo extendemos a las funciones racionales fijando $v_\infty(0) = \infty$. Su expresión general sería:

$$v_\infty\left(\frac{f(t)}{g(t)}\right) = v_\infty\left(f(t)\right) - v_\infty(g(t)) = deg(g(t)) - deg(f(t)).$$

Vamos a suponer sin pérdida de generalidad que $f(t)$, $\bar{f}(t)$, $g(t)$ y $\bar{g}(t)$ son polinomios no nulos. Tenemos que

$$\begin{aligned} v_\infty\left(\frac{f(t)}{g(t)}\cdot\frac{\bar{f}(t)}{\bar{g}(t)}\right) &= v_\infty\left(\frac{f(t)\cdot\bar{f}(t)}{g(t)\cdot\bar{g}(t)}\right) = deg(g(t)\cdot\bar{g}(t)) - deg(f(t)\cdot\bar{f}(t)) \\ &= [deg(g(t)) + deg(\bar{g}(t))] - [deg(f(t)) + deg(\bar{f}(t))] \\ &= [deg(g(t)) - deg(f(t))] + [deg(\bar{g}(t)) - deg(\bar{f}(t))] \\ &= v_\infty\left(\frac{f(t)}{g(t)}\right) + v_\infty\left(\frac{\bar{f}(t)}{\bar{g}(t)}\right). \end{aligned}$$

Por otra parte, si suponemos que $v_\infty\left(\frac{\bar{f}(t)}{\bar{g}(t)}\right) \geq v_\infty\left(\frac{f(t)}{g(t)}\right)$, ello implica que $deg(f(t)\cdot\bar{g}(t)) \geq deg(\bar{f}(t)\cdot g(t))$. Se sigue que

$$\begin{aligned} v_\infty\left(\frac{f(t)}{g(t)} + \frac{\bar{f}(t)}{\bar{g}(t)}\right) &= v_\infty\left(\frac{f(t)\cdot\bar{g}(t) + \bar{f}(t)\cdot g(t)}{g(t)\cdot\bar{g}(t)}\right) = deg(g(t)\cdot\bar{g}(t)) \\ &- deg(f(t)\cdot\bar{g}(t) + \bar{f}(t)\cdot g(t)) = deg(g(t)) + deg(\bar{g}(t)) \\ &- deg(f(t)\cdot\bar{g}(t) + \bar{f}(t)\cdot g(t)) \geq deg(g(t)) + deg(\bar{g}(t)) \\ &- deg(f(t)\cdot\bar{g}(t)) = deg(g(t)) + deg(\bar{g}(t)) - deg(f(t)) \\ &- deg(\bar{g}(t)) = deg(g(t)) - deg(f(t)) = v_\infty\left(\frac{f(t)}{g(t)}\right) \\ &= \text{mín}\left\{v_\infty\left(\frac{f(t)}{g(t)}\right), v_\infty\left(\frac{\bar{f}(t)}{\bar{g}(t)}\right)\right\}. \end{aligned}$$

Ejemplo 1.4. Veamos algunos ejemplos de cálculo de valoraciones p-ádicas:

(i) La descomposición en factores primos de 400 es $400 = 2^4\cdot 5^2$, que para $p = 5$ se tiene $v_5(400) = 2$ y para $p = 2$, $v_2(400) = 4$.
(ii) Como 2 no divide a 621, entonces $v_2(621) = 0$.
(iii) Consideremos el racional $\frac{123}{48}$ y $p = 3$. Las descomposiciones en números primeros son $123 = 3\cdot 41$ y $48 = 2^4\cdot 3$ y llegamos a que $v_3(\frac{123}{48}) = v_3(123) - v_3(48) = 1 - 1 = 0$.

Proposición 1.5. *Las valoraciones son homomorfismos de grupos.*

Demostración. Sea la valoración $v : \mathbb{K}\backslash\{0\} \longrightarrow \mathbb{Z}$. Sabemos que $\mathbb{K}\backslash\{0\}$ es un grupo multiplicativo y $\mathbb{Z}$ es un grupo aditivo. Por la Definición 1.1, tenemos que $v(xy) = v(x) + v(y)$. Por tanto, v es un homomorfismo de grupos. □

Observación 1.6. De la Proposición 1.5 toda valoración v es homomorfismo de grupos, por tanto $Im\, v$ es un subgrupo de $\mathbb{Z}$ con la operación suma.

Proposición 1.7. *Sean $v : \mathbb{K}\backslash\{0\} \longrightarrow \mathbb{Z}$ una valoración y $\alpha \in \mathbb{K}\{0\}$. Entonces*

(i) $v(1) = 0$,
(ii) $v(\alpha^{-1}) = -v(\alpha)$,
(iii) $v(\alpha) = v(-\alpha)$.

Demostración. Las propiedades (i) y (ii) se cumplen por la Proposición 1.5. Demostremos (iii). Tenemos que $0 = v(1) = v((-1)^2) = v(-1) + v(-1) = 2v(-1)$. Entonces, como $\mathbb{Z}$ es un dominio de integridad y 2 es no nulo, necesariamente $v(-1) = 0$. Se sigue además que $v(-\alpha) = v((-1)\alpha) = v(-1) + v(\alpha) = v(\alpha)$. □

Definición 1.8. *Sean A un dominio de integridad y $\mathbb{K} = c.f.(A)$ su cuerpo de fracciones. Diremos que A es un anillo de valoración si para cualquier $\alpha \in \mathbb{K}\backslash\{0\}$, entonces $\alpha \in A$ o $\alpha^{-1} \in A$.*

Sean $\mathbb{K}$ un cuerpo y $\mathbb{R}^+ = \{x \in \mathbb{R} : x > 0\}$.

Definición 1.9. *Un valor absoluto sobre $\mathbb{K}$ es una aplicación $|\cdot| : \mathbb{K} \longrightarrow \mathbb{R}^+ \cup \{0\}$ que cumple, para todo $x, y, z \in \mathbb{K}$, las siguientes condiciones:*

(i) $|x| = 0$ *si, y solo si,* $x = 0$;
(ii) $|x \cdot y| = |x| \cdot |y|$;
(iii) $|x + y| \leq |x| + |y|$.

Además, diremos que un valor absoluto sobre $\mathbb{K}$ es no arquimediano si se cumple la siguiente condición:

(iv) $|x + y| \leq \text{máx}\{|x|, |y|\}$.

En otro caso diremos que el valor absoluto es arquimediano.

Observación 1.10. La condición (iv) implica la condición (iii) ya que $\text{máx}\{|x|, |y|\} \leq |x| + |y|$. Si comparamos las condiciones (ii) y (iv) con las dos condiciones de la Definición 1.1, observamos que son similares, salvo que el producto del primero se ha convertido en una suma, semejante a los logaritmos, y que la desigualdad de la segunda ha sido invertido. Podemos volver a invertirla si cambiamos de signo y también podremos convertir la suma en un producto si lo transformamos en un exponente.

Ejemplo 1.11.

(i) Sea $\mathbb{K} = \mathbb{Q}$. Se define el valor absoluto usual, también llamado valor absoluto en el infinito,

$$|x| = \begin{cases} x \quad si\ x \geq 0 \\ \\ -x\ si\ x < 0. \end{cases} \tag{1.1}$$

Este valor absoluto es arquimediano ya que si tomamos $x = y = 1$ obtenemos $2 = |1 + 1| \not\leq \max\{|1|, |1|\} = 1$.

(ii) Sea $\mathbb{K}$ un cuerpo. Para todo $x \in \mathbb{K}$ definimos

$$|x| = \begin{cases} 1 \; si \; x \neq 0 \\ \\ 0 \; si \; x = 0. \end{cases} \tag{1.2}$$

La función definida en (1.2) es un valor absoluto para cualquier cuerpo. En efecto, sean $x, y \in \mathbb{K}$. La condición (i) de la Definición 1.9 se cumple por definición de $|\cdot|$. Para la segunda condición de la Definición 1.9 vamos a distinguir dos casos. Si suponemos que x e y son no nulos, entonces $x \cdot y$ es no nulo ya que $\mathbb{K}$ es un cuerpo. Luego, $1 = |x \cdot y| = |x||y|$. En cambio, si x o y es 0, entonces $x \cdot y = 0$. Sin pérdida de generalidad, podemos suponer que $x = 0$. Luego, $0 = |x \cdot y| = |x||y|$. Por tanto, con estos dos casos quedaría probado (ii).
Demostremos (iii) de la Definición 1.9. Si $x = y = 0$, se tendría que $|x+y| = 0 \leq 0 + 0 = |x| + |y|$. En cambio, si suponemos que o bien $x = 0$, o bien $y = 0$, tendríamos que $|x + y| = 1 \leq 0 + 1 = |x| + |y|$. Por otra parte, si x e y son ambos distinto de 0, se seguiría

$$|x + y| = \begin{cases} 0 \leq 1 + 1 = |x| + |y| \; si \; x = -y \\ \\ 1 \leq 1 + 1 \qquad\qquad\quad si \; x \neq -y. \end{cases} \tag{1.3}$$

Concluimos que, efectivamente, (1.2) define un valor absoluto que denominaremos valor absoluto trivial.

(iii) Sean $\mathbb{K} = \mathbb{Q}$, p un número primo y $c > 1$ un número real. Por convenio tomaremos $c^{-\infty} = 0$ y por tanto $|c^{-\infty}| = 0$ para todo valor absoluto $|\cdot|$. La aplicación $|x| = c^{-v_p(x)}$ determina un valor absoluto no arquimediano sobre $\mathbb{Q}$. En efecto, si suponemos que existe $x \neq 0$ tal que $|x| = 0$, se tendría que $\frac{1}{c^{v_p(x)}} = 0$ pero esto es absurdo. Ahora, sean x e y dos racionales. Se sigue que $|xy| = c^{-v_p(xy)} = c^{-v_p(x)-v_p(y)} = c^{-v_p(x)} \cdot c^{-v_p(y)} = |x| \cdot |y|$. Por otra parte, $|x + y| = c^{-v_p(x+y)} \leq c^{-\min\{v_p(x), v_p(y)\}} \leq c^{\max\{-v_p(x), -v_p(y)\}} = \max\{|x|, |y|\}$, luego se cumple la propiedad no arquimediana y por tanto, la propiedad (iii) de la Definición 1.9. Si tomamos $c = p$ en este ejemplo obtenemos el valor absoluto p-ádico.

(iv) Del Ejemplo 1.3 sabemos que v_∞ es una valoración. Esto nos proporciona otro valor absoluto no arquimediano

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

para todo $f(t) \in F(t)$, ya que cumple las hipótesis del Ejemplo 1.11 (iii).

Proposición 1.12. *Todo valor absoluto $|\cdot|$ sobre un cuerpo $\mathbb{K}$ cumple para todo $x \in \mathbb{K}$ las siguientes propiedades:*

(i) $|1| = 1$;
(ii) Si $x^n = 1$, *entonces* $|x| = 1$;
(iii) $|-1| = 1$;
(iv) $|-x| = |x|$;

Demostración. Recordamos que $|x|$ es un número real positivo para todo $x \neq 0$. Se tiene que $|1| = |1^2| = |1|^2$ y además, el único número real positivo α que cumple que $\alpha^2 = \alpha$ es $\alpha = 1$.

Ahora, tomamos $x \in \mathbb{K}$ con $x^n = 1$ y tenemos que $1 = |1| = |x^n| = |x|^n$, entonces $|x| = 1$.

Para probar (iii), como $(-1)^2 = 1$, de la propiedad que acabamos de demostrar, obtenemos que $|-1| = 1$.

De la Definición 1.9 y la propiedad (iii) tenemos $|-x| = |-1 \cdot x| = |-1| \cdot |x| = 1 \cdot |x| = |x|$ y concluimos (iv). □

Observación 1.13. En la Proposición 1.12 basta con tomar, como hipótesis, una aplicación $|\cdot| : \mathbb{K} \longrightarrow \mathbb{R}^+ \cup \{0\}$ que cumpla:

1. $x = 0$ si, y solo si, $|x| = 0$;
2. $|xy| = |x| \cdot |y|$.

Proposición 1.14. *Sean $\mathbb{K}$ un cuerpo finito y $|\cdot|$ un valor absoluto sobre $\mathbb{K}$. Entonces, $|\cdot|$ es el valor absoluto trivial.*

Demostración. Sea $x \in \mathbb{K}$. Si $x = 0$ entonces $|x| = 0$. En cambio, si $x \in \mathbb{K}\backslash\{0\}$ entonces, al ser $\mathbb{K}\backslash\{0\}$ un grupo multiplicativo finito, se tiene que el orden de x, $o(x)$, divide el orden de $\mathbb{K}\backslash\{0\}$. En particular, si $o(x) := M$, se tiene $x^M = 1$ y concluimos la prueba de la Proposición 1.12 *(ii)*.

Proposición 1.15. *Sean $\mathbb{K}$ un cuerpo y $|\cdot| : \mathbb{K} \longrightarrow \mathbb{R}^+ \cup \{0\}$ una aplicación que cumple*

1. $x = 0$ si, y solo si, $|x| = 0$;
2. $|xy| = |x| \cdot |y|$.

Entonces, para todo $x, y, z \in \mathbb{K}$, las siguientes afirmaciones son equivalentes:

(i) $|x + y| \leq \text{máx}\{|x|, |y|\}$;
(ii) $|z + 1| \leq \text{máx}\{|z|, 1\}$.

Demostración. Tomando $x = z$ e $y = 1$, obtenemos que *(i)* implica *(ii)*. Para el recíproco, vamos a estudiar dos casos. Si $y = 0$ entonces ya terminamos. Si $y \neq 0$ tomamos $z := \frac{x}{y} = xy^{-1}$, donde y^{-1} denota el inverso de y en $\mathbb{K}$. Se tiene que $|\frac{x}{y} + 1| \leq \text{máx}\{|\frac{x}{y}|, |1|\}$. Multiplicando a ambos lados por $|y|$, $|y| \cdot |\frac{x}{y} + 1| \leq |y| \cdot \text{máx}\{\frac{|x|}{|y|}, |1|\}$ y concluimos que, $|x + y| \leq \text{máx}\{|x|, |y|\}$. □

Proposición 1.16. *Sean* $\mathbb{K}$ *cuerpo y* $|\cdot| : \mathbb{K} \longrightarrow \mathbb{R}^+ \cup \{0\}$ *una aplicación tal que para todo* $x, y \in \mathbb{K}$, *se cumple:*

(i) $|x| = 0$ *si, y solo si,* $x = 0$*;*
(ii) $|xy| = |x| \cdot |y|$*;*
(iii) $|x| \leq 1$ *si, y solo si,* $|x - 1| \leq 1$.

Entonces, $|\cdot|$ *es un valor absoluto no arquimediano sobre* $\mathbb{K}$.

Demostración. Por hipótesis, tenemos las dos primeras condiciones *(i)* y *(ii)* de la Definición 1.9. Teniendo en cuenta la Proposición 1.15 y la hipótesis, para probar la condición de no arquimediano tenemos que ver que para cualquier $x \in \mathbb{K}$,

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

Habíamos visto previamente en la Observación 1.10 que esta condición implica la tercera de la Definición 1.9.

Sea $x \in \mathbb{K}$ tal que $|x| \leq 1$. Por la Observación 1.13 y la hipótesis *(iii)*, $|x| = |-x| \leq 1$ si, y solo si, $|-x-1| = |-(x+1)| = |x+1| \leq 1$.

A continuación, vamos a distinguir dos casos. Si $|x| \leq 1$ se tiene $|x + 1| \leq 1 = \text{máx}\{|x|, 1\}$. En cambio, si $|x| > 1$, aplicando nuevamente la Observación 1.13, obtenemos $|\frac{1}{x}| = |-\frac{1}{x}| < 1$ y usando la hipótesis (iii), $|-\frac{1}{x} - 1| = |-(\frac{1}{x} + 1)| = |\frac{1}{x} + 1| \leq 1$. Luego, $|1 + \frac{1}{x}| = |\frac{x+1}{x}| \leq 1$, lo que implica que $|x + 1| \leq |x| = \text{máx}\{|x|, 1\}$. □

Observación 1.17. Para cualquier cuerpo $\mathbb{K}$, tenemos un homomorfismo de anillos definido por $f : \mathbb{Z} \longrightarrow \mathbb{K}$

$$n \longrightarrow f(n) = \begin{cases} 1_{\mathbb{K}} + \overset{(n)}{\cdots} + 1_{\mathbb{K}} & si\ n > 0 \\ 0 & si\ n = 0 \\ -(1_{\mathbb{K}} + \overset{(-n)}{\cdots} + 1_{\mathbb{K}}) & si\ n < 0 \end{cases} \tag{1.4}$$

Primeramente, si $\mathbb{Q} = \mathbb{K}$, f es la inclusión de $\mathbb{Z}$ en $\mathbb{Q}$. En cambio, si $\mathbb{K}$ es un cuerpo finito, afirmamos que la imagen de f es un subcuerpo de $\mathbb{K}$ con un número primo de elementos. En efecto, $Im\, f$ es un subanillo de $\mathbb{K}$, luego es un dominio de integridad finito y por tanto, un cuerpo. Además, $Ker\, f$ es un ideal de $\mathbb{Z}$, luego será de la forma $n\mathbb{Z}$ con n un número entero. Por el Primer Teorema de isomorfía, $\mathbb{Z}/n\mathbb{Z} \cong Im\, f$. Como $Im\, f$ es cuerpo y es isomorfo a $\mathbb{Z}/n\mathbb{Z}$, también este último será cuerpo y necesariamente n tendrá que ser un número primo, implicando que $Im\, f$ tendrá, como cardinalidad, un número primo.

Teorema 1.18. *Sea* $A \subseteq \mathbb{K}$ *la imagen de* $\mathbb{Z}$ *en* $\mathbb{K}$ *por el homomorfismo* f *definido en* (1.4). *Un valor absoluto* $|\cdot|$ *sobre* $\mathbb{K}$ *es no arquimediano si, y solo*

si, $|a| \leq 1$*, para todo* $a \in A$*. En particular, un valor absoluto sobre* $\mathbb{Q}$ *es no arquimediano si, y solo si,* $|n| \leq 1$*, para cualquier* $n \in \mathbb{Z}$*.*

Demostración. Supongamos que $|\cdot|$ es un valor absoluto no arquimediano sobre $\mathbb{K}$. Veamos que $|a| \leq 1$, donde $a = 1 + \overset{(n)}{\cdots} + 1$, con $n \in \mathbb{N}$ por inducción sobre n.

Si $n = 1$, $|a| = |1| = 1 \leq 1$ por la Proposición 1.12. Ahora, suponemos cierto para $n = k-1$, es decir, $|a| = |1 + \overset{(k-1)}{\cdots} + 1| \leq 1$. Luego, vamos a probarlo para $n = k$. Se tiene que $|a| = |1 + \overset{(k)}{\cdots} + 1| = |(1 + \overset{(k-1)}{\cdots} + 1) + 1|$. Denotando $\bar{a} = 1 + \overset{(k-1)}{\cdots} + 1$ y usando la Proposición 1.12, $|\bar{a} + 1| \leq \max\{|\bar{a}|, 1\} = 1$ por hipótesis de inducción. Si ahora $n \in \mathbb{Z}\backslash\mathbb{N}$, de la Proposición 1.12 *(iv)* y dado que f es homomorfismo tenemos que $|f(n)| = |-f(n)| = |f(-n)| \leq 1$ pues $-n \in \mathbb{N}$.

Supongamos ahora que $|a| \leq 1$ para todo $a \in A$. Para demostrar que el valor absoluto $|\cdot|$ es no arquimediano, bastará probar, por la Proposición 1.15, que $|x + 1| \leq \max\{|x|, 1\}$, para todo $x \in \mathbb{K}$. Sea $m \in \mathbb{Z}^+$. Entonces,

$$|x+1|^m = \left|\sum_{k=0}^{m} \binom{m}{k} x^k\right| \leq \sum_{k=0}^{m} \left|\binom{m}{k}\right| \left|x^k\right|.$$

Como $\binom{m}{k}$ es un número entero no negativo, por hipótesis obtenemos que coincide su imagen por f, $|\binom{m}{k} 1_{\mathbb{K}}| \leq 1$. Luego,

$$|x+1|^m \leq \sum_{k=0}^{m} \left|\binom{m}{k} 1_{\mathbb{K}}\right| \left|x^k\right| \leq \sum_{k=0}^{m} \left|x^k\right| = \sum_{k=0}^{m} |x|^k. \tag{1.5}$$

Notamos que si $|x| > 1$, entonces el valor más grande de $|x|^k$, donde $k \in \{0, 1, 2, \cdots, m\}$ es cuando $k = m$. Además, si $|x| \leq 1$ entonces $|x|^0 = 1$. Luego, de (1.5) tenemos:

$$|x+1|^m \leq \sum_{k=0}^{m} \max\{1, |x|^m\} = (m+1)\max\{1, |x|^m\}. \tag{1.6}$$

Si tomamos la m-ésima raíz en ambos lados de la inecuación (1.6), se tiene

$$|x+1| \leq \sqrt[m]{m+1} \cdot \sqrt[m]{\max\{1, |x|^m\}} = \sqrt[m]{m+1} \cdot \max\{1, |x|\}. \tag{1.7}$$

La desigualdad (1.7) se cumple para todo entero positivo m, sin importar lo grande que sea. Usando l'Hôpital se obtiene

$$\begin{aligned}\lim_{m\to\infty} \sqrt[m]{m+1} &= \lim_{m\to\infty} (m+1)^{\frac{1}{m}} = \lim_{m\to\infty} e^{\frac{1}{m}\ln(1+m)} = e^{\lim_{m\to\infty} \frac{\ln(m+1)}{m}} \\ &= e^{\lim_{m\to\infty} \frac{1}{m+1}} = e^0 = 1.\end{aligned}$$

Por tanto, $|x+1| \leq \max\{|x|, 1\}$ y por la Proposición 1.15, concluimos que $|\cdot|$ es un valor absoluto no arquimediano. □

Proposición 1.19. *Sean $|\cdot|$ un valor absoluto en $\mathbb{K}$ y f el homomorfismo definido en la Observación 1.17. Si $\sup\{|f(n)| : n \in \mathbb{Z}\} = C < \infty$, entonces $|\cdot|$ es no arquimediano y $C = 1$.*

Demostración. Por reducción al absurdo, supongamos que $C > 1$. Entonces, existirá $m \in \mathbb{Z}$ tal que $|f(m)| > 1$. Pero, por la condición *(ii)* de la Definición 1.9, $|f(m)^k| = |f(m)|^k$ es arbitrariamente grande conforme aumenta k, luego C no puede ser finito y llegamos a una contradicción. Se sigue que $C \leq 1$ y por la propiedad *(i)* de la Proposición 1.12, podemos concluir que $C = 1$. Por tanto, por el Teorema 1.18, $|\cdot|$ es no arquimediano. □

1.2. Distancias

Definición 1.20. *Sean $\mathbb{K}$ un cuerpo y $|\cdot|$ un valor absoluto sobre $\mathbb{K}$. Se define la distancia $d(x, y)$ asociada a $|\cdot|$ entre dos elementos $x, y \in \mathbb{K}$ como*

$$d(x, y) = |x - y|.$$

La aplicación $d(x, y)$ se denomina métrica inducida por el valor absoluto.

Definición 1.21. *Sean $\mathbb{K}$ un cuerpo y $|\cdot|$ un valor absoluto sobre $\mathbb{K}$. Diremos que $\mathbb{K}$ es un espacio métrico si la métrica $d(x, y)$ inducida por $|\cdot|$ cumple para todo $x, y, z \in \mathbb{K}$ las siguientes propiedades:*

(i) $d(x, y) \geq 0$;
(ii) $d(x, y) = 0$, *entonces* $x = y$;
(iii) $d(x, y) = d(y, x)$;
(iv) $d(x, z) \leq d(x, y) + d(y, z)$, *también conocida como la propiedad de la desigualdad triangular.*

Definición 1.22. *Sean $\mathbb{K}$ y $\mathbb{F}$ cuerpos con valores absolutos y $f : \mathbb{K} \longrightarrow \mathbb{F}$ una aplicación. Diremos que f es continua en un punto $x_0 \in \mathbb{K}$ si dado cualquier $\varepsilon > 0$, existe $\delta > 0$ tal que para cualquier $x \in \mathbb{K}$ con $d(x, x_0) < \delta$ se tiene $d(f(x), f(x_0)) < \varepsilon$.*

Proposición 1.23. *Sean $\mathbb{K}$ un cuerpo, d una métrica inducida por el valor absoluto $|\cdot|$ y $x_0, y_0 \in \mathbb{K}$. Se tiene que:*

(i) para todo $\varepsilon > 0$, existe $\delta > 0$ tal que si $d(x, x_0) < \delta$ y $d(y, y_0) < \delta$, entonces $d(x + y, x_0 + y_0) < \varepsilon$.
(ii) para todo $\varepsilon > 0$, existe $\delta > 0$ tal que si $d(x, x_0) < \delta$ y $d(y, y_0) < \delta$, entonces $d(xy, x_0y_0) < \varepsilon$.

Demostración. Fijemos $\varepsilon > 0$ y $x_0, y_0 \in \mathbb{K}$. Sean $x, y \in \mathbb{K}$ tales que $d(x, x_0) = |x - x_0| < \delta$ y $d(y, y_0) = |y - y_0| < \delta$ donde tomamos $\delta = \varepsilon/2$. Entonces, $d(x + y, x_0 + y_0) = |(x + y) - (x_0 + y_0)| \leq |x + y| + |x_0 + y_0| < 2\delta = \varepsilon$, luego *(i)* queda demostrado.

Ahora en el caso del producto, cabe destacar que al ser x_0 e y_0 fijos los podemos acotar por valores positivos A y B respectivamente. Sean $x, y \in \mathbb{K}$ tales que $d(x, x_0) = |x - x_0| < \delta$ y $d(y, y_0) = |y - y_0| < \delta$ tomando $\delta = \frac{\sqrt{(A+B)^2+4\varepsilon}-(A+B)}{2}$. Entonces, $d(xy, x_0y_0) = |xy - x_0y_0| = |xy - xy_0 + xy_0 - x_0y_0| \leq |x| \cdot |y - y_0| + |y_0| \cdot |x - x_0| < |x - x_0 + x_0|\delta + B\delta < \delta^2 + (A + B)\delta = \varepsilon$. Por tanto, se concluye *(ii)*. □

Definición 1.24. *Sea $\mathbb{K}$ un espacio métrico y $d : \mathbb{K} \times \mathbb{K} \longrightarrow \mathbb{R}$ una aplicación que verifica las condiciones de la Definición 1.21. Llamaremos distancia ultramétrica a toda métrica que cumple, para cualesquiera $x, y, z \in \mathbb{K}$, la siguiente condición:*

$$d(x, y) \leq \text{máx}\{d(x, z), d(z, y)\}.$$

Además, un espacio métrico con una distancia ultramétrica se denomina espacio ultramétrico.

Proposición 1.25. *Sea $|\cdot|$ un valor absoluto sobre $\mathbb{K}$ y consideramos la métrica inducida por $|\cdot|$. Entonces, $|\cdot|$ es no arquimediano si, y solo si, $d(x, y)$ es una ultramétrica.*

Demostración. Sean $x, y, z \in \mathbb{K}$. Tenemos la igualdad

$$(x - y) = (x - z) + (z - y).$$

Aplicando la propiedad no arquimediana, obtenemos

$$\begin{aligned} d(x, y) = |x - y| &= |(x - z) + (z - y)| \leq \text{máx}\{|x - z|, |z - y|\} \\ &= \text{máx}\{d(x, z), d(z, y)\}. \end{aligned}$$

Ahora, si tomamos $y = -y_1$ y $z = 0$, entonces $d(x, -y_1) \leq \text{máx}\{d(x, 0), d(0, -y_1)\}$ y $|x + y_1| \leq \text{máx}\{|x|, |y_1|\}$. □

Observación 1.26. Observamos que si d es la distancia ultramétrica inducida por el valor absoluto $|\cdot|$, entonces $d(x, y) \leq \text{máx}\{d(x, z), d(z, y)\} \leq d(x, z) + d(z, y)$. Luego, la condición de ultramétrica implica la desigualdad triangular. Además, la condición *(iv)* de la Definición 1.9 también se conoce como la desigualdad ultramétrica.

Proposición 1.27. *Sean $\mathbb{K}$ un cuerpo y $|\cdot|$ un valor absoluto no arquimediano sobre $\mathbb{K}$. Si $x, y \in \mathbb{K}$ y $|x| \neq |y|$, entonces $|x + y| = \text{máx}\{|x|, |y|\}$.*

Demostración. Supongamos sin pérdida de generalidad que

$$|y| < |x|. \tag{1.8}$$

Como $|\cdot|$ es no arquimediano sabemos, por la Definición 1.9 y la condición (1.8), que

$$|x+y| \leq \text{máx}\{|x|, |y|\} = |x|. \tag{1.9}$$

Además, $x = (x+y) - y$, entonces por la condición *(iv)* de la Definición 1.9 tenemos

$$|x| = |(x+y) - y| \leq \text{máx}\{|x+y|, |y|\}, \tag{1.10}$$

donde $\text{máx}\{|x+y|, |y|\} = |x+y|$ ya que en caso contrario, tendríamos de (1.10) que $|x| \leq \text{máx}\{|x+y|, |y|\} = |y|$ que contradice (1.8). Obtenemos así,

$$|x| \leq \text{máx}\{|x+y|, |y|\} = |x+y|. \tag{1.11}$$

Finalmente, de (1.9) y (1.11) concluimos que $|x| = |x+y|$. □

Definición 1.28. *Sea $(\mathbb{K}, d)$ un espacio métrico. Llamamos triángulo de $\mathbb{K}$ a todo subconjunto de $\mathbb{K}$ formado por tres elementos distintos. Los tres elementos de un triángulo se denominan vértices. Si $x, y, z \in \mathbb{K}$ son los vértices de un triángulo, las longitudes de sus lados son $d(x,y), d(x,z)$ y $d(y,z)$.*

Definición 1.29. *Sea T un triángulo de un espacio métrico. Diremos que T es isósceles si de entre las tres longitudes de sus lados dos son iguales y la tercera no es mayor.*

Corolario 1.30. *En un espacio ultramétrico, todos los triángulos son isósceles.*

Demostración. Sean d una distancia ultramétrica en $\mathbb{K}$ y $x, y, z \in \mathbb{K}$.

Las longitudes de los lados del triángulo son

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

Suponiendo que $|x-y| \neq |y-z|$ y por la Proposición 1.27, obtenemos que $|x-z| = |(x-y)+(y-z)| = \text{máx}\{|x-y|, |y-z|\}$ y resultan dos longitudes iguales de sus lados y el tercero no es mayor. Además, en caso de que $|x-y| = |y-z|$, también hay dos lados iguales. Por otra parte, si tenemos tres lados iguales, necesariamente hay dos lados iguales. Concluimos que todos los triángulos son isósceles. □

Ejemplo 1.31. Vamos a aplicar la Proposición 1.27 al caso del valor absoluto p-ádico restringido a $\mathbb{Z}$. Sean $x, x', y, y', z, z' \in \mathbb{Z}$ y supongamos que $v_p(x) = n$ y $v_p(y) = m$ tales que $x = p^n x'$ y $y = p^m y'$ respectivamente, donde p no divide a x' ni a y'. Además, se dará que $|x|_p > |y|_p$ si $n < m$. Supongamos que existe $\epsilon > 0$ que cumple $m = n + \epsilon$. Entonces,

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

Como p no divide a x', entonces tampoco dividirá a $(x' + p^\epsilon y')$ y por tanto, $v_p(x + y) = n$, lo cual significa que $|x + y|_p = p^{-n} = |x|_p$ como enuncia la Proposición 1.27. En cambio, si suponemos que $|x|_p = |y|_p$, entonces $x + y = p^n(x' + y')$, donde p no divide a x', y'. Aún así, es posible que p divida a $x' + y'$. En tal caso, $v_p(x + y) \geq n = \text{mín}\{v_p(x), v_p(y)\}$. Luego,

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

Concluimos que en ambos casos hay al menos dos lados iguales.

Ejemplo 1.32. Dados $\mathbb{Q}$, la topología 5-ádica y un triángulo cuyos vértices son $x = 2/15, y = 1/5, z = 7/15$. ¿Cuáles son las distancias de los tres lados? Usando la Definición 1.28 y operando tenemos que

$$\begin{aligned}
d(x, y) = |x - y|_5 &= \left|\frac{2}{15} - \frac{1}{5}\right|_5 = \left|-\frac{1}{15}\right|_5 = 5^1 = 5; \\
d(x, z) = |x - z|_5 &= \left|\frac{2}{15} - \frac{7}{15}\right|_5 = \left|-\frac{1}{3}\right|_5 = 5^0 = 1; \\
d(y, z) = |y - z|_5 &= \left|\frac{1}{5} - \frac{7}{15}\right|_5 = \left|-\frac{4}{15}\right|_5 = 5^1 = 5.
\end{aligned}$$

Obsérvese por la Definición 1.30 que el triángulo es isósceles.

Definición 1.33. *Sean $\mathbb{K}$ un cuerpo, $|\cdot|$ un valor absoluto sobre $\mathbb{K}$, $a \in \mathbb{K}$ y $r \in \mathbb{R}^+$.*

La bola abierta de radio r y centro a es el conjunto de puntos de $\mathbb{K}$ cuya distancia al centro es menor estricto que r, es decir,

$$B(a, r) = \{x \in \mathbb{K} : d(x, a) < r\} = \{x \in \mathbb{K} : |x - a| < r\}.$$

La bola cerrada de radio r y centro a es el conjunto de puntos de $\mathbb{K}$ cuya distancia al centro es menor o igual que r, es decir,

$$\bar{B}(a, r) = \{x \in \mathbb{K} : d(x, a) \leq r\} = \{x \in \mathbb{K} : |x - a| \leq r\}.$$

Proposición 1.34. *En los espacios ultramétricos con la topología inducida por la distancia ultramétrica:*

(i) las bolas abiertas son siempre conjuntos abiertos;
(ii) las bolas cerradas son siempre conjuntos cerrados.

Demostración. Consecuencia de estar en un espacio métrico.

Para los valores absolutos no arquimedianos se obtienen propiedades interesantes.

Proposición 1.35. *Sea $\mathbb{K}$ un cuerpo con un valor absoluto no arquimediano. Se cumplen las siguientes propiedades:*

1. *Si $b \in B(a,r)$, entonces $B(a,r) = B(b,r)$. En otras palabras, todo punto dentro de una bola abierta es un centro de la bola.*
2. *Si $b \in \bar{B}(a,r)$, entonces $\bar{B}(a,r) = \bar{B}(b,r)$. En otras palabras, todo punto dentro de una bola cerrada es un centro de la bola.*
3. *$B(a,r)$ es abierto y cerrado y tiene frontera vacía.*
4. *S $r \neq 0$, $\bar{B}(a,r)$ es abierto y cerrado y tiene frontera vacía.*
5. *Sean $a,b \in \mathbb{K}$ y $r,s \in \mathbb{R}^+$. Entonces, $B(a,r) \cap B(b,s)$ es no vacío si, y solo si, $B(a,r) \not\subset B(b,s)$ o $B(b,s) \not\subset B(a,r)$. En otras palabras, dos bolas abiertas son disjuntas o una contiene a la otra.*
6. *Sean $a,b \in \mathbb{K}$ y $r,s \in \mathbb{R}^+$. Entonces, $B(a,r) \cap B(b,s)$ es no vacío si, y solo si, $\bar{B}(a,r) \not\subset \bar{B}(b,s)$ o $\bar{B}(b,s) \not\subset \bar{B}(a,r)$. En otras palabras, dos bolas cerradas son disjuntas o una contiene a la otra.*

Demostración. Demostremos el primer apartado. Sea $b \in B(a,r)$, lo cual es equivalente a que $|b-a| < r$. Ahora, tomando x tal que $|x-a| < r$ y usando la propiedad no arquimediana se tiene que

$$|x-b| \leq \text{máx}\{|x-a|, |b-a|\} < r.$$

Entonces, $x \in B(a,r)$. En cambio si $x \in B(b,r)$, usando el mismo razonamiento de antes, llegamos a que

$$|x-a| \leq \text{máx}\{|x-b|, |b-a|\} < r.$$

El segundo apartado se prueba de forma similar que el primero, cambiando $<$ y bolas abiertas por $\leq$ y bolas cerradas respectivamente.

Para concluir el tercer apartado, sabemos por la Proposición 1.34 que las bolas abiertas son abiertos, luego tenemos que ver que $B(a,r)$ es cerrada, lo cual es equivalente a ver que su complementario es abierto. El complementario de la bola abierta $B(a,r)$ es $C = \{x \in \mathbb{K} : d(x,a) \geq r\}$. Sea $y \in C$. Entonces, $|y-a| \geq r$ y escogemos $s < r$. Vamos a ver que la bola abierta $B(y,s)$ está contenida en C. Se tiene que $|z-y| < s < r \leq |y-a|$, para todo $z \in B(y,r)$. Como todos los triángulos son isósceles, $|z-a| = \text{máx}\{|z-y|, |y-a|\} = |y-a| \geq r$. Entonces, $z \in C$. Luego, todo $y \in C$ se puede contener en una bola abierta que, a su vez, está contenido en C. Por tanto, C es abierto y $B(a,r)$ es cerrada. Nos falta ver que su frontera es vacía. Esto es directo considerando la equivalencia entre tener la frontera vacía y que el conjunto sea abierto y cerrado a la vez.

Demostremos el cuarto apartado. Sabemos por la Proposición 1.34 que las bolas cerradas son cerrados. Falta demostrar que son abiertas. Supongamos por reducción al absurdo que la frontera de $\bar{B}(a,r)$ es no vacía. Entonces, por definición de frontera, existe $x \in Fr(B(a,r))$ tal que cualquiera de sus entornos

interseca con $\bar{B}(a,r)$ y su complementario. Además, x debe estar en el borde de la bola, ya que en caso contrario, estaría en $B(a,r)$ y sabemos por el tercer apartado que $Fr(B(a,r)) = \emptyset$, lo cual es absurdo. Si x está en el borde, entonces $|x-a| = r$. Sea $y \in B(x,\epsilon)$ tal que $\epsilon < r$. Si $y \in Ext(B(a,r))$, entonces $|y-x| < s < r < |y-a|$ y como todos los triángulos son isósceles, $r = |x-a| = \text{máx}\{|y-a|, |y-x|\} > r$, lo cual es una contradicción. Obtenemos que la frontera es vacía. Nuevamente, conjunto sea abierto y cerrado a la vez luego la frontera es vacía.

Probemos el quito apartado. Si $B(a,r) \subseteq B(b,s)$, entonces trivialmente $B(a,r) \cap B(b,s)$ es no vacío. Por otro lado, supongamos sin pérdida de generalidad que $r \leq s$. Si $B(a,r) \cap B(b,s)$ es no vacío, entonces existirá un elemento, c, en la intersección y por el primer apartado se obtiene que $B(a,r) = B(c,r)$ y $B(b,s) = B(c,s)$. Esto implica que $B(a,r) = B(c,r) \subseteq B(c,s) = B(b,s)$ y, por tanto, $B(a,r) \subseteq B(b,s)$.

La prueba del sexto apartado es similar al quinto, cambiando bolas abiertas y el primer apartado por bolas cerradas y el segundo apartado, respectivamente. □

Ejemplo 1.36. Vamos a describir una serie de bolas en $\mathbb{Q}$ con el valor absoluto p-ádico, concretando qué números enteros están contenidos en ellas:

$$\begin{aligned}\bar{B}(0,1) &= \{z \in \mathbb{Q} : |z-0|_p \leq 1\} = \{z \in \mathbb{Q}/|z|_p \leq 1\} \\ &= \left\{\frac{a}{b} \in \mathbb{Q} : p^{v_p(b)-v_p(a)} \leq 1\right\} = \left\{\frac{a}{b} \in \mathbb{Q} : \frac{p^{v_p(b)}}{p^{v_p(a)}} \leq 1\right\} \\ &= \left\{\frac{a}{b} \in \mathbb{Q} : p^{v_p(b)} \leq p^{v_p(a)}\right\} = \left\{\frac{a}{b} \in \mathbb{Q} : v_p(b) \leq v_p(a)\right\}.\end{aligned}$$

Si suponemos $\frac{a}{b}$ irreducible, entonces $\bar{B}(0,1)$ consiste en los racionales tales que p no divide al denominador, lo cual incluye a todos los enteros.

Sea $i \in \mathbb{Z}$. Se tiene que

$$\begin{aligned}B(i,1) &= \{z \in \mathbb{Q} : |z-i|_p < 1\} = \left\{\frac{a}{b} \in \mathbb{Q} : \left|\frac{a-ib}{b}\right|_p < 1\right\} \\ &= \left\{\frac{a}{b} \in \mathbb{Q} : v_p(b) < v_p(a-ib)\right\}.\end{aligned}$$

En este caso, consiste en los racionales tales que p no divide el denominador pero sí divide a $a-ib$. Respecto a los enteros, serán los $a \in \mathbb{Z}$ tal que p divide a $(a-i)$, lo que es equivalente a que $a \equiv i \pmod{p}$.

Teniendo en cuenta este ejemplo, vamos a demostrar la siguiente propiedad.

Proposición 1.37. *Sean $\mathbb{K} = \mathbb{Q}$ y $|\cdot| = |\cdot|_p$. Entonces, podemos expresar $\bar{B}(0,1)$ como unión disjunta de bolas abiertas como sigue*

$$\bar{B}(0,1) = B(0,1) \cup B(1,1) \cup B(2,1) \cup \cdots \cup B(p-1,1).$$

Demostración. Sabemos que $\bar{B}(0,1)$ está compuesto por los puntos $\frac{a}{b}$ tales que p no divide a b. Vamos a ver que solamente uno de lo siguientes números es divisible por p:

$$a,\ a-b,\ a-2b,\ ...,\ a-(p-1)b. \tag{1.12}$$

Por reducción al absurdo supongamos que dos de los valores de (1.12) es divisible por p. Es decir, existen $\lambda, \mu \in \mathbb{Z}$ e $i \neq j \in \{0, 1, \cdots, p-1\}$ tales que $a-ib = \lambda p$ y $a-jb = \mu p$. Si restamos las igualdades anteriores obtenemos $(j-i)b = (\mu-\lambda)p$. Por el Lema de Euclides p tendrá que dividir a $(j-i)$ o a b, pero $j-i < p$ y $j-i \neq 0$ ya que $i \neq j$, por tanto p no puede dividir a $j-i$ y no queda más remedio que p divida a b, lo cual es un absurdo por hipótesis.

Recordando $B(i,1)$ del Ejemplo 1.36, llegamos a que, si $a-ib$ es divisible por p, entonces $\left|\frac{a}{b}-i\right| = \left|\frac{a-ib}{b}\right| < 1$, implicando que $\frac{a}{b} \in B(i,1)$.

Añadir que las bolas son disjuntas, ya que solamente uno de los valores de (1.12) es divisible por p.

Por último, si $\frac{a}{b} \in B(i,1)$, entonces b no es divisible por p y se cumple que $\frac{a}{b} \in \bar{B}(0,1)$. □

Ejemplo 1.38. Tomando el valor absoluto 5-ádico sobre $\mathbb{Q}$, veamos que $B(1,1) = B(1,\frac{1}{2}) = \bar{B}(1,\frac{1}{5})$.

Por el Ejemplo 1.36, sabemos que $B(1,1) = \{\frac{a}{b} \in \mathbb{Q} : v_5(b) < v_5(a-b)\}$. Procedemos a calcular las otras dos bolas:

$$\begin{aligned} B\left(1,\frac{1}{2}\right) &= \left\{\frac{a}{b} \in \mathbb{Q} : \left|\frac{a}{b}-1\right|_5 < \frac{1}{2}\right\} = \left\{\frac{a}{b} \in \mathbb{Q} : \left|\frac{a-b}{b}\right|_5 < \frac{1}{2}\right\} \\ &= \left\{\frac{a}{b} \in \mathbb{Q} : 5^{-v_5(\frac{a-b}{b})} < \frac{1}{2}\right\} \\ &= \left\{\frac{a}{b} \in \mathbb{Q} : 5^{-v_5(a-b)+v_5(b)} < \frac{1}{2}\right\} = \left\{\frac{a}{b} \in \mathbb{Q} : \frac{5^{v_5(b)}}{5^{v_5(a-b)}} < \frac{1}{2}\right\} \\ &= \left\{\frac{a}{b} \in \mathbb{Q} : 2 \cdot 5^{v_5(b)} < 5^{v_5(a-b)}\right\}. \end{aligned}$$

De manera similar cambiando $<$ por $\leq$ y 2 por 5 obtenemos que:

$$\bar{B}(1,1) = \left\{\frac{a}{b} \in \mathbb{Q} : 5 \cdot 5^{v_5(b)} \leq 5^{v_5(a-b)}\right\} = \left\{\frac{a}{b} \in \mathbb{Q} : 5^{v_5(b)+1} \leq 5^{v_5(a-b)}\right\}.$$

Ahora, $\frac{a}{b} \in B(1,1)$ si, y solo si, $5^{v_5(b)} < 5^{v_5(a-b)}$ que es equivalente a que $2 \cdot 5^{v_5(b)} < 5^{v_5(a-b)}$ y a su vez coincide con que $5^{v_5(b)} \leq 5 \cdot 5^{v_5(a-b)}$. Por tanto, $B(1,1) = B\left(1,\frac{1}{2}\right) = \bar{B}\left(1,\frac{1}{5}\right)$.

1.3. Anillos de valoración

Definición 1.39. *Sean $\mathbb{K}$ un cuerpo y $|\cdot|$ un valor absoluto no arquimediano sobre $\mathbb{K}$. El subanillo*

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

se denomina anillo de valoración de $|\cdot|$. El ideal

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

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

$$\kappa = \Theta/\beta$$

se conoce como cuerpo residual de $|\cdot|$.

Proposición 1.40. *Sean $\mathbb{K}$ un cuerpo y $|\cdot|$ un valor absoluto no arquimediano sobre $\mathbb{K}$. Entonces,*

(a) $\Theta = \{x \in \mathbb{K} : |x| \leq 1\}$ es un subanillo de $\mathbb{K}$,
(b) $\beta = \{x \in \mathbb{K} : |x| < 1\}$ es un ideal de Θ,
(c) Θ es un anillo local y β es su único ideal maximal.

Demostración. En *(a)* tenemos que $\Theta \subseteq \mathbb{K}$ por definición de Θ y $\Theta \neq \emptyset$ ya que $0 \in \Theta$. Sean $x, y \in \Theta$, entonces $|xy| = |x||y| \leq 1$, luego $xy \in \Theta$. Por otro lado, $|x+y| \leq \text{máx}\{|x|, |y|\} \leq 1$ por ser $|\cdot|$ no arquimediano y en consecuencia $x+y \in \Theta$. Añadir que, por la Proposición 1.12, $1_{\mathbb{K}} \in \Theta$, entonces Θ es unitario.

Para demostrar *(b)*, tenemos que $0 \in \beta$ ya que $|0| < 1$. Si tomamos $x, y \in \beta$ y $z \in \Theta$ se tiene que $|xz| = |x||z| < 1$ y por consiguiente, $xz \in \beta$. Además, $|x+y| \leq \text{máx}\{|x|, |y|\} < 1$ por la condición *(iv)* de la Definición 1.9 y por tanto, $x + y \in \beta$.

Nos faltaría por probar (c). Vamos a demostrar que $\Theta \backslash \beta = \Theta^*$, siendo Θ^* el conjunto de las unidades de Θ. Se tiene que $x \in \Theta \backslash \beta$ si, y solo si $|x| = 1$, luego $x \neq 0$ y $x \in \mathbb{K}^*$ por ser $\mathbb{K}$ cuerpo. Entonces, existe $x^{-1} \in \mathbb{K}$ tal que $x \cdot x^{-1} = 1$. En consecuencia, se tiene que $|x \cdot x^{-1}| = |x| \cdot |x^{-1}| = 1$, de lo que deducimos $|x^{-1}| = 1$ y concluimos que $x \in \Theta^*$.

Si ahora tomamos $x \in \Theta^*$, entonces existe $x^{-1} \in \Theta^*$ tal que $x \cdot x^{-1} = 1$ y por consiguiente $|x \cdot x^{-1}| = 1$. Como $|x| \leq 1$, se tiene que $|x| = |x^{-1}| = 1$ y por tanto, $x \in \Theta \backslash \beta$.

Finalmente, tenemos un anillo Θ y $\Theta^* = \Theta \backslash \beta$. Esto implicaría que $\Theta \backslash \Theta^* = \Theta \backslash (\Theta \backslash \beta) = \beta$ es un ideal. Usando la caracterización de anillos locales, concluimos que Θ es un anillo local y $\Theta \backslash \Theta^* = \beta$ es su único ideal maximal. □

Observación 1.41. Recordamos que el cociente de un anillo conmutativo unitario por un ideal maximal es un cuerpo, luego esto corrobora que el cuerpo residual Θ/β es realmente un cuerpo.

Proposición 1.42. *Sean $\mathbb{K} = \mathbb{Q}$ y $|\cdot|$ el valor absoluto p-ádico. Entonces,*

(i) el anillo de valoración asociado a $|\cdot|_p$ es $\Theta = \mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} : p \text{ no divide a } b\}$;
(ii) el ideal de valoración es $\beta = p\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} : p \text{ no divide a } b \text{ y } p \text{ divide a } a\}$;
(iii) el cuerpo residual Θ/β es un cuerpo con p elementos.

Demostración. Para (i), supongamos $\frac{a}{b} \in \Theta$ ya reducido. Por definición, si $\frac{a}{b} \in \Theta$ entonces $|\frac{a}{b}| = p^{-v} \leq 1$, lo cual es equivalente a que $v \geq 0$ y esto ocurre si, y solo si, p no divide a b, implicando que $\frac{a}{b} \in \mathbb{Z}_{(p)}$.

En (ii), obtenemos que p no divide a b siguiendo el mismo razonamiento de (i). Además, como $|\frac{a}{b}| < 1$ si, y solo si, $v > 0$, entonces necesariamente p divide a a.

Demostremos (iii). Vamos a definir la siguiente correspondencia:

$$f : \mathbb{Z} \longrightarrow \kappa = \Theta/\beta = \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}$$
$$n \longrightarrow f(n) = \left[\frac{n}{1}\right] = \frac{[n]_p}{[1]_p}$$

donde $[\,\cdot\,]_p$ denota la clase de módulo p en $\mathbb{Z}$. Observamos que la correspondencia está bien definida ya que p no divide a 1. Además si tomamos $m, m' \in \mathbb{Z}$ tales que $m = m'$, entonces $f(m) = [\frac{m}{1}] = [\frac{m'}{1}] = f(m')$, por tanto es aplicación. Ahora, si tomamos $a, b \in \mathbb{Z}$ se tiene que $f(a+b) = [\frac{a+b}{1}] = [\frac{a}{1} + \frac{b}{1}] = [\frac{a}{1}] + [\frac{b}{1}] = f(a) + f(b)$ y también $f(a \cdot b) = [\frac{ab}{1}] = [\frac{a}{1}] \cdot [\frac{b}{1}] = f(a) \cdot f(b)$, luego f es homomorfismo. El núcleo sería $kerf = \{n \in \mathbb{Z} : f(n) = 0\} = \{n \in \mathbb{Z} : [\frac{n}{1}] = [0]\} = \{n \in \mathbb{Z} : p \textit{ divide a } n\} = p\mathbb{Z}$.

Veamos que $Imf = \kappa$. $Imf \subseteq \kappa$ por definición de Imf. Sea $[\frac{a}{b}] \in \kappa$, entonces p no divide a b. Si p divide a a, entonces $[\frac{a}{b}] = [0]$ y basta con tomar $n = 0$ ya que $f(0) = [0]$. En cambio, si p no divide a a, entonces $[\frac{a}{b}] \neq [0]$. Como p no divide a b, entonces existe un entero b_1 tal que $bb_1 \equiv 1 \pmod{p}$ y $\frac{[a]}{[b]} = \frac{[ab_1]}{[1]} = f(ab_1)$ con ab_1 entero. Por el Primer Teorema de Isomorfía, se obtiene

$$\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}.$$

□

Ejemplo 1.43. Vamos a calcular el anillo de valoración, el ideal de valoración y el cuerpo residual para la valoración no arquimediana sobre $F(t)$ desarrollada en el Ejemplo 1.11 (iv).

Por un lado, para todo $\frac{f(t)}{g(t)}$ en $F[t]$, se tiene que $\left|\frac{f(t)}{g(t)}\right| = e^{deg(f(t))-deg(g(t))} = \frac{e^{deg(f(t))}}{e^{deg(g(t))}} \leq 1$ si, y solo si, $deg(f(t)) \leq deg(g(t))$. Luego, el anillo de valoración sería $\Theta = \left\{\frac{f(t)}{g(t)} \in F(t) : deg(f(t)) \leq deg(g(t))\right\}$. Por otro lado, siguiendo el mismo procedimiento llegamos a que el ideal de valoración se definiría como $\beta = \left\{\frac{f(t)}{g(t)} \in F(t) : deg(f(t)) < deg(g(t))\right\}$. En el caso del cuerpo residual, desarrollando nuevamente llegaríamos a

$$\kappa = \left\{ \frac{f(t)}{g(t)} + \beta \ : \ \frac{f(t)}{g(t)} \in F(t) \text{ y } deg(f(t)) = deg(g(t)) \right\} \cup \{0 + \beta\},$$

donde $z(t) + \beta$ denota la clase de $z(t) \in F(t)$ en Θ/β.

2

Resolución de congruencias módulo p^n

Los números p-ádicos están estrechamente relacionados con el problema de resolución de congruencias módulo potencias de un número primo p. Las referencias principales que hemos seguido para este capítulo son [3] y [4].

Comenzaremos este capítulo recordando el Teorema de Lagrange. A pesar de no existir un resultado análogo a él para módulos de potencias de primos, hay un algoritmo para determinar cuándo una solución módulo p genera soluciones de módulos de potencias de p más grandes. La motivación proviene del método de Newton para la aproximación de raíces sobre los números reales. La idea consiste en *elevar* soluciones módulo p a módulo p^2, estas a módulo p^3 y así sucesivamente, siempre y cuando sea posible.

Definimos el epimorfismo

$$\begin{aligned} \varphi_n : \mathbb{Z}[x] &\longrightarrow \mathbb{Z}_n[x] \\ f(x) = \sum_{i=0}^{n} a_i x^i &\longrightarrow \varphi_n(f(x)) := f(x) = \sum_{i=0}^{n} [a_i]_n x^i, \end{aligned}$$

donde $[a_i]_n$ representa la clase de a_i (mód n). El epimorfismo φ_n no es inyectivo, pues puede ocurrir que $\varphi_n(f(x)) = 0$ en $\mathbb{Z}_n[x]$ si todos los coeficientes a_i de $f(x)$ son múltiplos de n. Además, si $\varphi_n(f(x)) \neq 0$, ocurre que $\deg \varphi_n(f(x)) \leq \deg f(x)$. Añadir que si n es un número primo, entonces $\mathbb{Z}_n$ es un cuerpo y $\varphi_n(f(x))$ tiene a lo sumo tantas raíces en $\mathbb{Z}_n$ como su grado, concluyendo así que $\varphi_n(f(x))$ tiene a lo máximo $\deg f(x)$ raíces en $\mathbb{Z}_n$. En caso de que n no sea un número primo, $\varphi_n(f(x))$ puede tener en $\mathbb{Z}_n$ más raíces que su grado, como muestra el polinomio $f(x) = x^2 + x + 7$ para $n = 9$, cuyas raíces son $x = 1$, 4 y 7 (mód 9). Por otra parte, $a \in \mathbb{Z}$ verifica $f(a) = 0$ (mód n) si, y solo si, $[a]_n \in \mathbb{Z}_n$ es raíz de $\varphi_n(f(x))$.

Mediante el razonamiento previo obtenemos el siguiente teorema:

Teorema 2.1 (Teorema de Lagrange). *Sean p un número primo y $f(x) \in \mathbb{Z}[x]$. Entonces, o todos los coeficientes de $f(x)$ son divisibles por p, o $f(x) \equiv 0$*

(mód p) tiene como mucho $\deg f(x)$ *soluciones, donde* $\deg f(x)$ *denota el grado de* $f(x)$.

Si $n = p$ es un número primo, queremos determinar raíces de $\varphi_{p^j}(f(x))$ de la forma $z + tp^{j-1}$. Para ello, necesitaremos en primer lugar algunos resultados previos.

Proposición 2.2. *Sean* $f(x) \in \mathbb{Z}[x]$ *y* $a \in \mathbb{Z}$. *Entonces,* $\frac{f^{(k)}(a)}{k!} \in \mathbb{Z}$ *para todo* $0 \leq k \leq \deg f(x)$.

Demostración. Sea $f(x) = \sum_{i=0}^{n} a_i x^i$, donde $n = \deg f(x)$. Entonces, $f^{(k)}(x) = \sum_{i=k}^{n} i(i-1)\cdots(i-(k-1))a_i x^{i-k}$ y si sustituimos a y dividimos por $k!$ tenemos

$$\begin{aligned}\frac{f^{(k)}(a)}{k!} &= \sum_{i=k}^{n} \frac{i(i-1)\cdots(i-(k-1))}{k!} a_i a^{i-k} \\ &= \sum_{i=k}^{n} \frac{i(i-1)\cdots(i-(k-1))(i-k)(i-k-1)\cdots 2\cdot 1}{k!(i-k)(i-k-1)\cdots 2\cdot 1} a_i a^{i-k} \\ &= \sum_{i=k}^{n} \frac{i!}{k!(i-k)!} a_i a^{i-k} = \sum_{i=0}^{n} \binom{i}{k} a_i a^{i-k} \in \mathbb{Z}.\end{aligned}$$

□

Lema 2.3. *Sean* $f(x) \in \mathbb{Z}[x]$, $n \in \mathbb{N}$, $n > 1$ *y* p *un número primo. Entonces, para cualesquiera* $a, t \in \mathbb{Z}$ *se tiene:*

$$f(a + p^n t) \equiv f(a) + f'(a)p^n t \ (\textit{mód}\ p^{n+1}).$$

Demostración. Sean $f(x) \in \mathbb{Z}[x]$ y $k = \deg f(x)$. Aplicando el desarrollo de Taylor en el punto $x = -p^n t$ llegamos a

$$f(x + p^n t) = f(x) + f'(x)p^n t + \frac{f''(x)}{2!}p^{2n}t^2 + \frac{f'''(x)}{3!}p^{3n}t^3 + \cdots + \frac{f^{(k)}(x)}{k!}p^{kn}t^k.$$

Entonces,

$$f(a + p^n t) = f(a) + f'(a)p^n t + \frac{f''(a)}{2!}p^{2n}t^2 + \frac{f'''(a)}{3!}p^{3n}t^3 + \cdots + \frac{f^{(k)}(a)}{k!}p^{kn}t^k.$$

Ahora, por la Proposición 2.2, $f(a + p^n t) \in \mathbb{Z}$. Si procedemos a aplicar módulo p^{n+1}, obtenemos $f(a + p^n t) \equiv f(a) + f'(a)p^n t$, pues $p^{sn} \equiv 0$ (mód p^{n+1}) para todo $2 \leq s \leq n$. □

Teorema 2.4 (Lema de Hensel). *Sean* $f \in \mathbb{Z}[x]$, $n \geq 1$, p *un número primo y* $c \in \mathbb{Z}/p^n\mathbb{Z}$ *una solución de* $f(x) \equiv 0$ *(mód* p^n*). Si* p *no divide a* $f'(c)$, *entonces* $f(x) \equiv 0$ *(mód* p^{n+1}*) tiene una única solución congruente con* c *(mód* p^n*), que viene dada por* $c + p^n t$, *donde*

$$t = -f'(c)^{-1}\frac{f(c)}{p^n} \ (\textit{mód}\ p). \tag{2.1}$$

Demostración. Como $f(c) = 0 \pmod{p^n}$, sabemos que p^n divide a $f(c)$ y $\frac{f(c)}{p^n}$ es un número entero. Por hipótesis, p no divide a $f'(c)$, luego $f'(c)$ es invertible módulo p. Sea $t = -f'(c)^{-1}\frac{f(c)}{p^n} \pmod{p}$. Por el Lema 2.3, se tiene que

$$\begin{aligned} f(c+p^n t) &= f(c) + f'(c)p^n t = f(c) + f'(c)p^n \cdot \left(-f'(c)^{-1}\frac{f(c)}{p^n}\right) \\ &= f(c) - f(c) = 0 \pmod{p^{n+1}}. \end{aligned}$$

Esto prueba que $c+p^n t$ es una solución de $f(x) \equiv 0 \pmod{p^{n+1}}$, donde $c+p^n t \equiv c \pmod{p^n}$.

Para probar la unicidad de $t \pmod{p}$, supongamos que existe $w \pmod{p}$ tal que $f(c+p^n w) \equiv 0 \pmod{p^{n+1}}$. Por el Lema 2.3 obtenemos

$$f(c+p^n t) \equiv f(c) + f'(c)p^n t \equiv 0 \equiv f(c) + f'(c)p^n w \equiv f(c+p^n w) \pmod{p^{n+1}}.$$

Simplificando, resulta $f'(c)p^n t \equiv f'(c)p^n w \pmod{p^{n+1}}$, pero por hipótesis p no divide a $f'(c)$, por tanto p^{n+1} tampoco lo dividirá, entonces $f'(c)$ es una unidad $\pmod{p^{n+1}}$ y llegamos a que $p^n t \equiv p^n w \pmod{p^{n+1}}$. Así pues, p^{n+1} divide a $p^n(t-w)$ en $\mathbb{Z}$ y en consecuencia, p divide a $t-w$. Concluimos que $t \equiv w \pmod{p}$ y por ende, $t \pmod{p}$ es único. □

Ejemplo 2.5. Queremos resolver la congruencia $x^2 + 1 \equiv 0 \pmod{5^2}$. Comenzamos buscando raíces de la correspondiente congruencia módulo 5, $x^2 + 1 \equiv 0 \pmod{5}$. Probando con todos los valores de $\mathbb{Z}/5\mathbb{Z}$, obtenemos que las soluciones son $x = 2 \pmod{5}$ y $x = 3 \pmod{5}$. Observamos que existen a lo sumo dos soluciones por el Teorema 2.1. Consideramos el caso $x_1 = 2$. Se tiene que $f(2) = 5 \equiv 0$ y $f'(2) = 4 \not\equiv 0 \pmod{5}$, cumpliéndose así las hipótesis del Lema 2.4. Sustituyendo en la expresión (2.1):

$$t_1 \equiv -4^{-1} \cdot \frac{5}{5} = -4 \equiv 1 \pmod{5},$$

llegamos a que $t_1 = 1$ y por tanto, $x_2 = 2 + 5t_1 = 7 \pmod{5^2}$. Ahora, veamos el caso cuando $x_1 = 3$. Se tiene que $f(3) = 10 \equiv 0$ y $f'(3) = 6 \not\equiv 0 \pmod{5}$, cumpliéndo también las hipótesis del Teorema 2.4. Sustituyeno nuevamente en (2.1):

$$t_1 \equiv -6^{-1} \cdot \frac{10}{5} = -1^{-1} \cdot 2 \equiv 3 \pmod{5}.$$

Luego, $x_2 = 3 + t_1 5 = 3 + 3 \cdot 5 = 18 \pmod{5^2}$.

Teorema 2.6 (Lema de Hensel - Versión Generalizada). *Sean $f \in \mathbb{Z}[x]$, $n \geq 1$, p un número primo y $c \in \mathbb{Z}/p^n\mathbb{Z}$ una solución de $f(x) \equiv 0$ (mód p^n). Supongamos que p divide a $f'(c)$.*

(i) Si p^{n+1} divide a $f(c)$, entonces $f(x) \equiv 0$ (mód p^{n+1}) tiene p soluciones congruentes con c (mód p^n). Estas vienen dadas por $c + p^n t$, donde $t = 0, 1, ..., p-1$.

(ii) Si p^{n+1} no divide a $f(c)$, entonces $f(x) \equiv 0$ (mód p^{n+1}) no tiene soluciones congruentes con c (mód p^n).

Demostración. Por hipótesis, p divide a $f'(c)$, por tanto p^{n+1} divide a $f'(c)p^n$ y aplicando el Lema 2.3 tenemos que

$$f(c + p^n t) \equiv f(c) \text{ (mód } p^{n+1}). \tag{2.2}$$

Si p^{n+1} divide a $f(c)$, entonces de (2.2) obtenemos que $f(c+p^n t) \equiv 0$ (mód p^{n+1}) con t arbitrario. Luego, para los p valores de t (mód p) se tiene que $c + p^n t$ son soluciones de $f(x) \equiv 0$ (mód p^{n+1}). Si ahora p^{n+1} no divide a $f(c)$, entonces de (2.2) tenemos que $f(x) \not\equiv 0$ (mód p^{n+1}), por tanto no hay soluciones de $f(x) \equiv 0$ (mód p^{n+1}) que sean congruentes con c (mód p^n). □

Ejemplo 2.7. Sea $f(x) = x^2 + x + 7 \in \mathbb{Z}[x]$, del cual queremos encontrar todas las soluciones de $f(x) \equiv 0$ (mód 3^2). Probando con todos los valores de $\mathbb{Z}/3\mathbb{Z}$, resulta que $x \equiv 1$ (mód 3) es la única solución de $f(x) \equiv 0$ (mód 3). Además, tenemos $f'(x) = 2x + 1$, luego 3 divide a $f'(1) = 3$ y 3^2 divide a $f(1) = 9$. Por tanto, por el Teorema 2.6, $f(x) \equiv 0$ (mód 3^2) posee 3 soluciones congruentes con 1 (mód 3), las cuales son $x_1 \equiv 1 + 0 \cdot 3 \equiv 1$, $x \equiv 1 + 1 \cdot 3 \equiv 4$ y $x \equiv 1 + 2 \cdot 3 \equiv 7$ (mód 3^2).

3

Los números p-ádicos

Habiendo costruido el cimiento, podemos comenzar a aplicar la teoría general de valores absolutos al caso específico del cuerpo de los números racionales $\mathbb{Q}$. En la segunda parte del capítulo, se tratará el problema de *completar* $\mathbb{Q}$. La referencia principal que hemos seguido para este capítulo es [2].

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

Hasta ahora hemos visto algunos ejemplos de valores absolutos sobre $\mathbb{Q}$. El siguiente paso será demostrar que dichos ejemplos conforman una lista completa de todos los posibles valores absolutos sobre $\mathbb{Q}$. Para ello será necesaria la noción de valores absolutos equivalentes. Finalmente, probaremos la fórmula producto como una ilustración de cómo funcionan todos los valores absolutos juntos en la aritmética de $\mathbb{Q}$.

Recordamos los valores absolutos sobre $\mathbb{Q}$ que hemos estudiado hasta ahora:

- el valor absoluto trivial;
- el valor absoluto usual $|\cdot|_\infty$, que también denominamos valor absoluto en el infinito;
- el valor absoluto p-ádico $|\cdot|_p$, para cada p número primo.

Se puede apreciar que, exceptuando el valor absoluto trivial, que tenderemos a ignorar, hemos denotado todos los valores absolutos de la forma $|\cdot|_p$ donde p es un número primo o ∞. Resulta ser conveniente pensar en ∞ como un *número* primo de $\mathbb{Z}$, referenciándolo como el primo infinito y a su correspondiente valor absoluto como el ∞-ádico valor absoluto. Esto nos permitirá utilizar expresiones como "$|\cdot|_p$ para todo primo $p \leq \infty$", aunque esta notación solo lo utilizaremos por conveniencia.

Usamos valores absolutos sobre un cuerpo $\mathbb{K}$ para definir una topología en $\mathbb{K}$. Ello nos permite dar la siguiente definición:

Definición 3.1. *Diremos que dos valores absolutos $|\cdot|_1$ y $|\cdot|_2$ sobre un cuerpo $\mathbb{K}$ son equivalentes si definen la misma topología sobre $\mathbb{K}$, es decir, si todo abierto respecto a un valor absoluto, también lo es respecto al otro.*

Lema 3.2. *Sean $\mathbb{K}$ un cuerpo con un valor absoluto $|\cdot|$ y (x_n) una sucesión en $\mathbb{K}$. Son equivalentes:*

(i) $\lim_{x\to\infty} x_n = y$;
(ii) cualquier conjunto abierto que contiene a y también contiene todos, salvo una cantidad finita, de los x_n.

Demostración. Comenzaremos asumiendo (ii). Como la bola abierta de centro y y radio ϵ, $B(y,\epsilon)$, es un abierto, todos los x_n, salvo una cantidad finita, estarán contenidos en ella, luego existe $N \in \mathbb{N}$ tal que x_n pertenece a $B(y,\epsilon)$ para todo $n \geq N$. Por tanto, para todo ϵ existe N natural tal que $|x_n - y| < \epsilon$, es decir, x_n converge a y. Ahora, supongamos que x_n converge a y y tomemos un abierto U que contiene a y. Entonces, existen r cumpliendo que $B(y,r)$ está contenido en U y $N \in \mathbb{N}$ tal que $|x_n - y| < r$, para todo $n \geq N$. Así pues, salvo una cantidad finita de $n \in \mathbb{N}$, $x_n \in B(y,r) \subseteq U$. □

Observación 3.3.

1. El Lema 3.2 ofrece una definición de sucesiones convergentes en términos de conjuntos abiertos. Entonces, si dos valores absolutos determinan los mismos conjuntos abiertos, también determinarán las mismas sucesiones convergentes. Esta constituye la primera de muchas caracterizaciones de valores absolutos equivalentes.
2. Sean (X,d) un espacio métrico y $d(x,y) = |x-y|$ la métrica inducida por el valor absoluto $|\cdot|$. Recordamos que la topología inducida por la métrica d, T_d, viene determinada por la base

$$\beta := \{B_d(a,\epsilon) : a \in X,\, \epsilon > 0\}.$$

Proposición 3.4. *Sean $|\cdot|_1$ y $|\cdot|_2$ dos valores absolutos sobre un cuerpo $\mathbb{K}$. Los siguientes enunciados son equivalentes:*

(i) Los valores absolutos $|\cdot|_1$ y $|\cdot|_2$ son equivalentes ;
(ii) cualquier sucesión (x_n) en $\mathbb{K}$ converge a y con respecto a $|\cdot|_1$ si, y solo si, (x_n) converge a y con respecto a $|\cdot|_2$;
(iii) para cualquier $x \in \mathbb{K}$, $|x|_1 < 1$ si, y solo si, $|x|_2 < 1$;
(iv) existe un número real positivo α tal que para todo $x \in \mathbb{K}$ se tiene que

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

Demostración. Primero supondremos cierto (i). Por el Lema 3.2, cualquier sucesión que converge respecto de $|\cdot|_1$ también lo hará respecto de $|\cdot|_2$.

Ahora, supongamos cierto (ii). Sean $x \in \mathbb{K}$ y (x^n) la sucesión de potencias de x. Si $\lim_{x\to\infty} x^n = 0$, entonces para cualquier $\varepsilon > 0$, existe $N \in \mathbb{N}$ tal que $|x^n - 0|_1 < \varepsilon$, para todo $n \geq N$. Tomando $\varepsilon = 1$, tenemos que $|x|_1 < 1$. En cambio, si elegimos x tal que $|x|_1 < 1$, entonces $\lim_{n\to\infty} |x^n|_1 = 0$ y por tanto, $\lim_{x\to\infty} x^n = 0$. Además, la sucesión (x^n) también tiende a 0 respecto a $|\cdot|_2$, luego por el mismo razonamiento llegamos a que $|x|_2 < 1$.

Tomemos (iii) por hipótesis. Sea $x_0 \in \mathbb{K}$ no nulo tal que $|x_0|_1 < 1$. Entonces, $|x_0|_2 < 1$, luego existirá $\alpha := \frac{\log|x_0|_1}{\log|x_0|_2} \in \mathbb{R}$ cumpliendo que

$$|x_0|_1 = |x_0|_2^{\alpha}. \tag{3.1}$$

Ahora, seleccionamos cualquier otro $x \in \mathbb{K}$ no nulo. Si $|x|_1 = |x_0|_1$, se sigue que $|x|_2 = |x_0|_2$, ya que en caso contrario $|\frac{x}{x_0}|_2 < 1$ o $|\frac{x_0}{x}|_2 < 1$, pero $|\frac{x}{x_0}|_1 = |\frac{x_0}{x}|_1 = 1$ lo cual es absurdo por hipótesis. Por tanto, llegamos a que $|x|_1 = |x|_2^{\alpha}$. En el caso de que $|x|_1 = 1$, necesariamente se tiene que dar que $|x|_2 = 1$, luego también se cumple $|x|_1 = |x|_2^{\alpha}$. Observamos que la igualdad que cumplen ciertos x implica también la igualdad con las potencias de x. En particular, $|x_0^n|_1 = |x_0^n|_2^{\alpha}$ para cualquier $n \in \mathbb{Z}$. Por último queda considerar el caso cuando $|x|_i \neq 1$ y $|x|_i \neq |x_0|_i$ para $i = 1, 2$. Como antes, tomemos β real tal que

$$|x|_1 = |x|_2^{\beta}, \tag{3.2}$$

también cumpliéndose para cualquier entero n, $|x^n|_1 = |x^n|_2^{\beta}$. Podemos asumir que $|x|_1 < 1$, ya que en caso contrario podemos escoger $|\frac{1}{x}|_1 < 1$, y por tanto $|x|_2 < 1$. Procederemos a probar que $\alpha = \beta$. Sean n y m dos enteros positivos. Entonces, $|x|_1^n < |x_0|_1^m$ si, y solo si, $|\frac{x^n}{x_0^m}|_1 < 1$, únicamente si $|\frac{x^n}{x_0^m}|_2 < 1$ y solo en caso de que $|x|_2^n < |x_0|_2^m$. Luego, $n \cdot \log|x|_1 < m \cdot \log|x_0|_1$ a condición de que $n \cdot \log|x|_2 < m \cdot \log|x_0|_2$, que podemos escribir como $\frac{n}{m} < \frac{\log|x_0|_1}{\log|x|_1}$ lo cual es equivalente a $\frac{n}{m} < \frac{\log|x_0|_2}{|x|_2}$. Se sigue que el conjunto de fracciones que son más pequeñas que el primer cociente de logaritmos es igual al conjunto de fracciones que son más pequeñas que el segundo. Como existen fracciones tan cercanas a un número real como queramos, necesariamente ambos cocientes de logaritmos deben ser iguales, es decir

$$\frac{\log|x_0|_1}{\log|x|_1} = \frac{\log|x_0|_2}{\log|x|_2},$$

deduciéndose que

$$\frac{\log|x_0|_1}{\log|x_0|_2} = \frac{\log|x|_1}{\log|x|_2}. \tag{3.3}$$

Pero, usando las Ecuaciones (3.1), (3.3) y (3.2) llegamos a que

$$\alpha = \frac{\log |x_0|_2^\alpha}{\log |x_0|_2} = \frac{\log |x_0|_1}{\log |x_0|_2} = \frac{\log |x|_1}{\log |x|_2} = \frac{\log |x|_2^\beta}{\log |x|_2} = \beta.$$

Por último, tomamos (iv) por hipótesis. Para demostrar (i) tenemos que probar que las topologías que definen los dos valores absolutos son idénticas, para lo cual basta probar que cualquier bola abierta con respecto a $|\cdot|_1$ es también una bola abierta con respecto a $|\cdot|_2$. Consideramos la bola abierta $|x-a|_1 < r$. De *(iv)* existe $\alpha \in \mathbb{R}^+$ tal que $|x-a|_2^\alpha < r$, lo que es equivalente a $|x-a|_2 < r^{\frac{1}{\alpha}}$. Por tanto, podemos concluir que las topologías que definen ambos valores absolutos son idénticas. □

Proposición 3.5. *Sean $|\cdot|_1$ y $|\cdot|_2$ dos valores absolutos equivalentes sobre un cuerpo $\mathbb{K}$. Si toda bola abierta con respecto a uno de los valores absolutos es también una bola abierta con respecto al otro, entonces las topologías que determinan $|\cdot|_1$ y $|\cdot|_2$ son idénticas*

Demostración. Recordamos que la topología inducida por $|\cdot|_1$ son las bolas abiertas $|x-a|_1 < \epsilon$, donde ϵ es real positivo y a es un elemento de $\mathbb{K}$ e igual ocurre con $|\cdot|_2$. Ahora, por hipótesis, toda bola abierta respecto a $|\cdot|_1$ es también una bola abierta respecto de $|\cdot|_2$, pero estos son abiertos en sus respectivas topologías inducidas. Por tanto, las topologás son idénticas. □

Proposición 3.6. *Si $|\cdot|_*$ es un valor absoluto equivalente al trivial, entonces $|\cdot|_*$ es el trivial.*

Demostración. Por la Proposición 3.4 sabemos que existe α real tal que $|x|_* = |x|^\alpha$, donde denotamos $|\cdot|$ al valor absoluto trivial. Procedemos a estudiar dos casos. En el primero, $x = 0$, entonces $|x|_* = |x|^\alpha = 0$. En el segundo, suponiendo x no nulo, tenemos que $|x|_* = |x|^\alpha = 1$. Pero entonces tenemos que

$$|x|_* = \left\{ \begin{array}{l} 1 \; si \; x \neq 0 \\ \\ 0 \; si \; x = 0. \end{array} \right\} = |x|.$$

Por tanto, $|\cdot|$ y $|\cdot|_*$ son iguales. □

Proposición 3.7. *Sean p, q dos números enteros primos distintos. Entonces los valores absolutos p-ádico y q-ádico no son equivalentes. Además, si p es un número primo y $q = \infty$, los valores absolutos $|\cdot|_p$ y $|\cdot|_\infty$ tampoco son equivalentes.*

Demostración. Por reducción al absurdo, supongamos que $|\cdot|_p$ y $|\cdot|_q$ sí son equivalentes. Como p y q son distintos, podemos suponer sin pérdida de generalidad que $p < q$. Luego, tomando $x = p$, tenemos que $|x|_p < 1$ y $|x|_q = 1$, pero

llegamos a un absurdo por la Proposición 3.4 *(iii)*, concluyendo que $|\cdot|_p$ y $|\cdot|_q$ no son equivalentes.

A continuación, en el caso de $q = \infty$ y tomando nuevamente $x = p$, se sigue que $|x|_p < 1$ y $|x|_\infty = p > 1$ ya que 1 no es primo y llegamos de nuevo a un absurdo. □

Proposición 3.8. *Los valores absolutos arquimedianos y no arquimedianos no son equivalentes.*

Demostración. Denotamos $|\cdot|_*$ un valor absoluto arquimediano y $|\cdot|_\#$ un valor absoluto no arquimediano. Por reducción al absurdo supongamos que ambos valores absolutos son equivalentes. Retomemos el homomorfismo $f : \mathbb{Z} \longrightarrow \mathbb{K}$ de la Observación 1.17. Como $|\cdot|_*$ es arquimediano, por el Teorema 1.18 sabemos que existirá n entero tal que $|f(n)|_* > 1$. Pero $|\cdot|_\#$ es no arquimediano y de nuevo por el Teorema 1.18 $|f(m)| \leq 1$ para cualquier entero m y en particular el caso $m = n$, luego $|\frac{1}{f(n)}| \geq 1$ y $|\frac{1}{f(n)}|_* < 1$, llegando así a un absurdo por la Proposición 3.4 *(iii)*. Concluimos que $|\cdot|_*$ y $|\cdot|_\#$ no pueden ser equivalentes. □

Ejemplo 3.9. El valor absoluto $|\cdot|$ del Ejemplo 1.11 (iii) es equivalente al valor absoluto p-ádico: en efecto, tomemos $\alpha = \frac{\log(p)}{\log(c)}$, entonces $c^\alpha = p$ y obtenemos

$$|x|_p = p^{-v_p(x)} = (c^\alpha)^{-v_p(x)} = (c^{-v_p(x)})^\alpha = |x|^\alpha.$$

Entonces, de la Proposición 3.4 *(iv)* concluimos que $|\cdot|_p$ y $|\cdot|$ son equivalentes.

Teorema 3.10 (Ostrowski). *Todo valor absoluto no trivial sobre $\mathbb{Q}$ es equivalente a uno de los valores absolutos $|\cdot|_p$ con p un número primo o $p = \infty$.*

Demostración. Sea $|\cdot|$ un valor absoluto no trivial sobre $\mathbb{Q}$. Procederemos a distinguir dos casos.

1. Supongamos que $|\cdot|$ es arquimediano. Vamos a probar que $|\cdot|$ es equivalente al valor absoluto usual o ∞-ádico. Como $|\cdot|$ es arquimediano existe al menos un entero positivo n tal que $|n| > 1$. Sea n_0 el menor entero positivo tal que $|n_0| > 1$. Existe $\alpha = \frac{\log|n_0|}{\log(n_0)} \in \mathbb{R}^+$ cumpliendo que

$$|n_0| = n_0^\alpha. \tag{3.4}$$

Demostraremos que los valores absolutos son equivalentes haciendo uso de la Proposición 3.4 *(iv)* para dicho α, es decir, demostraremos que

$$|x| = |x|_\infty^\alpha \text{ para todo } x \in \mathbb{Q}. \tag{3.5}$$

Teniendo en cuenta que $|\frac{n}{m}| = \frac{|n|}{|m|}$, bastará probar (3.5) para los enteros positivos.

La igualdad (3.5) se cumple cuando $n = n_0$ por (3.4). En cambio, si n es distinto de n_0 vamos a expresarlo en base n_0

$$n = a_0 + a_1 n_0 + \cdots + a_k n_0^k \tag{3.6}$$

donde $0 \leq a_i \leq n_0 - 1$, $a_k \neq 0$ y k entero. Además, observamos que k viene determinado por la desigualdad

$$n_0^k \leq n < n_0^{k+1}, \tag{3.7}$$

de lo que deducimos que $k = \lfloor \frac{\log n}{\log n_0} \rfloor$, donde $\lfloor \cdot \rfloor$ denota la función parte entera. Tomando valor absoluto,

$$|n| = |a_0 + a_1 n_0 + \cdots + a_k n_0^k| \leq |a_0| + |a_1| n_0^\alpha + \cdots + |a_k| n_0^{\alpha k}$$

y como n_0 es el menor entero cuyo valor absoluto es mayor que 1, deducimos que $|a_i| \leq 1$. Entonces,

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

Si elegimos $C = \frac{n_0^\alpha}{n_0^\alpha - 1}$ y teniendo en cuenta la desigualdad (3.7) se sigue que $|n| \leq C n_0^{k\alpha} \leq C n^\alpha$. Además, C no depende del n tomado, entonces también se cumple para enteros de la forma n^N, cumpliéndose $|n^N| \leq C n^{N\alpha}$. Aplicando la raíz N-ésima, logramos $|n| \leq \sqrt[N]{C} n^\alpha$. Como N puede ser cualquier valor entero positivo, tendemos $N \to \infty$, lo que obliga a $\sqrt[N]{C} \to 1$, proporcionando la desigualdad $|n| \leq n^\alpha$.
A continuación, demostraremos la desigualdad en el otro sentido. Regresando a la expresión (3.6) y teniendo en cuenta (3.7) y (3.4), llegamos a que

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

y despejando,

$$|n| \geq n_0^{(k+1)\alpha} - |n_0^{k+1} - n| \geq n_0^{(k+1)\alpha} - (n_0^{k+1} - n)^\alpha. \tag{3.8}$$

Además, por (3.7) se cumple que

$$-(n_0^{k+1} - n)^\alpha \geq -(n_0^{k+1} - n_0^k)^\alpha. \tag{3.9}$$

Ahora, por (3.9) y (3.8), tenemos que

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

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

donde nuevamente $C' = 1-(1-1/n_0)^{\alpha}$ es positivo y tampoco depende del n tomado. Siguiendo el mismo procedimiento de antes, $|n^N| \geq C' n^{N\alpha}$ y aplicando la raíz N-ésima y tendiendo N a infinito, llegamos finalmente a que $|n| \geq n^{\alpha}$.

2. Supongamos que $|\cdot|$ es no arquimediano. Por el Teorema 1.18, $|n| \leq 1$ para todo $n \in \mathbb{Z}$. Sea n_0 el menor entero positivo tal que $|n_0| < 1$ (que existe porque $|\cdot|$ es no trivial). Comenzaremos demostrando que n_0 es un número primo. Por reducción al absurdo asumamos que existen números naturales a y b más pequeños que n_0 tales que $n_0 = a \cdot b$. Teniendo en cuenta que $|n_0| < 1$, entonces $|a| < 1$ o $|b| < 1$, con $a < n_0$ o $b < n_0$ lo cual es absurdo por la elección de n_0, luego $|a| = |b| = 1$, pero a su vez $1 = |ab| = |n_0| < 1$ que también es absurdo. Llegamos así a que n_0 es primo y lo denotaremos por $p = n_0$. Queremos demostrar que $|\cdot|$ es efectivamente equivalente al valor absoluto $|\cdot|_p$ cumpliendo las hipótesis del Ejemplo 3.9. Para ello, verificaremos que siendo n un entero no divisible por p, entonces $|n| = 1$. Si dividimos n por p, obtenemos $n = rp + s$ con $0 < s < p$. Por el mismo razonamiento de antes, como $s < p$, entonces $|s| = 1$. Añadir que $|rp| < 1$, ya que $|r| \leq 1$ por ser $|\cdot|$ no arquimediano y $|p| < 1$ por construción. Por el Corolario 1.30 se sigue que $|n| = 1$. Finalmente, dado cualquier n entero, podemos escribirlo como $n = p^v n'$ donde p no divide a n'. Por tanto, $|n| = |p|^v |n'| = |p|^v = c^{-v}$ donde $c = |p|^{-1} > 1$, concluyendo que $|\cdot|$ es equivalente a valor absoluto p-ádico.

□

Proposición 3.11 (Fórmula Producto). *Para cualquier $x \in \mathbb{Q}\backslash\{0\}$, se cumple que*

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

donde $p \leq \infty$.

Demostración. De nuevo, bastará con probarlo para enteros positivos. Tomemos x un entero positivo, el cual podemos factorizar como $x = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, siendo p_i primo para todo $i = 1, 2, ..., k$. Se sigue que

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

Por tanto,

$$\prod_{p\leq\infty}|x|_p = \left(\prod_{q\neq p}|x|_q\right)|x|_q|x|_{p_1}|x|_{p_2}\cdots|x|_{p_k}|x|_\infty$$
$$= 1\cdot p_1^{-a_1}p_2^{-a_2}\cdots p_k^{-a_k}p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k} = 1.$$

□

3.2. Completaciones

Ahora estamos listos para construir, para cada primo p, el cuerpo p-ádico $\mathbb{Q}_p$. Procederemos a construir completaciones para cada uno de los valores absolutos sobre $\mathbb{Q}$.

Definición 3.12. *Sea $|\cdot|$ un valor absoluto sobre un cuerpo $\mathbb{K}$.*

(i) Una sucesión de elementos $x_n \in \mathbb{K}$ será una sucesión de Cauchy si para cada $\varepsilon > 0$ existe $M \in \mathbb{N}$ tal que $|x_n - x_m| < \varepsilon$ cuando $n, m \geq M$.
(ii) Diremos que $\mathbb{K}$ es completo si toda sucesión de Cauchy con respecto a $|\cdot|$ tiene límite en $\mathbb{K}$.
(iii) Un subconjunto S de $\mathbb{K}$ será denso en $\mathbb{K}$ si toda bola abierta que contiene un elemento de $\mathbb{K}$ también contiene un elemento de S.

Definición 3.13. *Sea $\mathbb{K}$ un cuerpo de valoración. Llamaremos completación al cuerpo de valoración más pequeño que es completo y tal que $\mathbb{K}$ es denso en él.*

Observación 3.14. Sabemos por teoría de Análisis que $\mathbb{Q}$ no es completo con respecto al valor absoluto usual $|\cdot|_\infty$ y su completación es $\mathbb{R}$.

Proposición 3.15. *$\mathbb{Q}$ es completo respecto al valor absoluto trivial $|\cdot|$.*

Demostración. Está claro que $\mathbb{Q}$ es un cuerpo y anillo de valoración y por ende un cuerpo de valoración. Además, trivialmente $\mathbb{Q}$ es denso en $\mathbb{Q}$. Los únicos valores posibles del valor absoluto trival son 0 y 1, luego una sucesión (x_n) en $\mathbb{Q}$ será de Cauchy con respecto al valor absoluto trivial cuando $|x_m - x_n| = 0$ para todo m y n suficientemente grande, pero esto solamente ocurre cuando $x_n = x_m$ para m y n suficientemente grandes, es decir, converge a un racional, por tanto, $\mathbb{Q}$ es completo. □

La meta de esta sección es construir para todo número primo p un cuerpo al que podemos extender el valor absoluto p-ádico, que sea completo al extenderlo y tal que $\mathbb{Q}$ sea denso en él.

Lema 3.16. *Una sucesión (x_n) en un cuerpo $\mathbb{K}$ con un valor absoluto no arquimediano $|\cdot|$ es de Cauchy si, y solo si,* $\lim_{x\to\infty}|x_{n+1} - x_n| = 0$.

Demostración. Si comenzamos suponiendo que la sucesión es de Cauchy entonces es directo por Definición 3.12 (i). Por otro lado, tomemos $m = n + r > n$. Entonces,

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

ya que es un valor absoluto no arquimediano y como $\lim_{x\to\infty} |x_{n+1} - x_n| = 0$ existirá $n \in \mathbb{N}$ tal que $|x_m - x_n| < \varepsilon$ para todo $n, m \geq N$ y todo $\varepsilon > 0$ arbitrario. □

Observación 3.17. La hipótesis de no arquimediano en el Lema 3.16 es imprescindible. En efecto, sea $\mathbb{R}$ con el valor absoluto usual $|\cdot|$. Si definimos la sucesión real creciente $(x_n) = (\sqrt{n})$, tenemos que $\lim_{n\to\infty} |x_{n+1} - x_n| = \lim_{n\to\infty} |\frac{1}{\sqrt{n}+\sqrt{n+1}}| \leq \lim_{n\to\infty} |\frac{1}{2\sqrt{n}}| = 0$, luego términos consecutivos se van acercando cada vez más, pero aumentando el valor de n los términos de la sucesión crecen arbitrariamente, por tanto no está acotada y no puede converger. Concluimos que (x_n) no es una sucesión de Cauchy.

Introducimos el siguiente concepto que nos ayudará en la demostración del lema que sigue.

Definición 3.18. *Sea p un primo. Diremos que una secuencia de enteros α_n tal que $0 \leq \alpha_n \leq p^n - 1$ es coherente si para cada $n \geq 1$, se cumple que $\alpha_n \equiv \alpha_{n+1}$ (mód p^n).*

Lema 3.19. *El cuerpo de los racionales $\mathbb{Q}$ no es completo respecto de ninguno de los valores absolutos no triviales.*

Demostración. Dado el Teorema de Ostrowski 3.10, lo probaremos para $|\cdot|_p$, donde $p \leq \infty$. Sabemos que $\mathbb{Q}$ no es completo respecto a $|\cdot|_\infty$ por la Observación 3.14, luego falta demostrarlo para los valores absolutos p-ádicos. Necesitamos construir una sucesión de Cauchy en $\mathbb{Q}$ cuyo límite no sea racional. Para construirla, encontraremos una sucesión coherente de soluciones módulo p^n de una ecuación que no tiene solución en $\mathbb{Q}$. Primero veamos el caso cuando $p \neq 2$. Sea a un entero tal que no es un cuadrado en $\mathbb{Q}$, p no divide a a y la congruencia $X^2 \equiv a \pmod{p}$ tiene solución. Para cumplir estas condiciones, tomaremos $a = n^2 + kp$, donde p no divide a n.

A continuación, construiremos la sucesión de Cauchy (x_n) con respecto a $|\cdot|_p$. Sea x_0 una solución arbitraria de $x_0^2 \equiv a$ (mód p), y elegimos x_1 tal que $x_1 \equiv x_0$ (mód p) y $x_1^2 \equiv a$ (mód p^2). Esto se cumple porque $f'(x_0) = 2x_0 \not\equiv 0$ ya que en caso contrario, tendríamos $x_0 \equiv 0$ (mód p), pero entonces $f(x_0) \equiv -a \not\equiv 0$ puesto que p no divide a a, luego llegamos a un absurdo. Por el mismo razonamiento y dado que si p no divide a a, entonces p^n tampoco lo divide, llegamos a la expresión general: $x_n \equiv x_{n-1} \pmod{p^n}$ y $x_n^2 \equiv p^{n+1}$.

Por construcción, $|x_{n+1} - x_n| = |\lambda p^{n+1}| \leq p^{-(n+1)} \to 0$ cuando $n \to \infty$. Tras esto y el Lema 3.16, llegamos a que efectivamente (x_n) es una sucesión de Cauchy. Por otro lado, tenemos que $|x_n^2 - a| = |\mu p^{n+1}| \leq p^{-(n+1)}$ también tiende a cero cuando n se va a infinito, entonces el límite de (x_n), en caso de que existiera, tendrá que ser $\sqrt{a}$, pero a no es cuadrado de ningún racional, por tanto el límite no puede existir en $\mathbb{Q}$, demostrándose que $\mathbb{Q}$ no es completo con respecto a $|\cdot|_p$.

Ahora, veamos el caso cuando $p = 2$. Sea b un entero tal que no es un cubo en $\mathbb{Q}$, p no divide a b y la congruencia $X^3 \equiv b \pmod{p}$ tiene solución. Para cumplir estas condiciones, tomaremos $b = n^3 + kp$, donde p no divide a n. Siguiendo el mismo procedimiento que en el caso $p \neq 2$ llegamos a que la solución tendría que ser la raíz cúbica de b, pero habíamos supuesto que b no era un cubo en $\mathbb{Q}$, luego llegamos a la misma conclusión, por lo tanto, $\mathbb{Q}$ tampoco es completo con respecto a $|\cdot|_p$, para $p < \infty$. □

Como $\mathbb{Q}$ no es completo, podemos construir una completación con respecto a un valor absoluto no trivial. La idea consiste en añadir a $\mathbb{Q}$ los límites de todas las sucesiones de Cauchy. Como a primeras el límite no existe, realmente lo que hacemos es sustituir el límite que no tenemos con la sucesión que sí tenemos. Para ello, comenzamos con el conjunto de toda las sucesiones de Cauchy y usamos operaciones algebraicas sobre $\mathbb{Q}$ para trabajar con este objeto.

Definición 3.20. *Sea $|\cdot|_p$ un valor absoluto no arquimediano sobre $\mathbb{Q}$. Denotamos por $\mathcal{C}$ o $\mathcal{C}_p(\mathbb{Q})$ el conjunto de todas las sucesiones de Cauchy en $\mathbb{Q}$ con respecto a $|\cdot|_p$.*

Proposición 3.21. *Sean (x_n) y (y_n) sucesiones de Cauchy en $\mathbb{Q}$ con respecto al valor absoluto no arquimediano $|\cdot|_p$. Entonces, $\mathcal{C}$ es un anillo conmutativo unitario con las operaciones:*

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

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

Demostración. Como $\mathbb{Q}$ es un anillo conmutativo y unitario, sabemos que $\mathcal{C}$ es cerrado para las operaciones. Por la misma razón, $\mathcal{C}$ también es conmutativo. Veamos que la sucesión resultante de usar estas operaciones es nuevamente una sucesión de Cauchy. Tomando $\varepsilon/2 > 0$ sabemos que existen N_1 y N_2 tales que $|x_{n_1} - x_{m_1}| < \varepsilon/2$ y $|y_{n_2} - y_{m_2}| < \varepsilon/2$ para todo n_1, $m_1 \geq N_1$ y n_2, $m_2 \geq N_2$. Si elegimos $N_0 = \text{máx}\{N_1, N_2\}$, entonces

$$|(x_n + y_n) - (x_m + y_m)| \leq |x_n - x_m| + |y_n - y_m| < \varepsilon$$

para todo n, $m \geq N_0$.

Recordamos que las sucesiones de Cauchy están acotadas. Supongamos que $|x_n| < A$ y $|y_n| < B$ para todo n. Si seleccionamos $\varepsilon', \varepsilon'' > 0$, existen N_1' y N_2' tales que $|x_{n_1'} - x_{m_1'}| < \varepsilon'/B$ y $|y_{n_2'} - y_{m_2'}| < \varepsilon''/A$ para todo $n_1', m_1' \geq N_1'$ y $n_2', m_2' \geq N_2'$. Luego, si elegimos $N_0' = \text{máx}\{N_1', N_2'\}$, entonces

$$\begin{aligned} |x_n y_n - x_m y_m| &= |x_n y_n - x_n y_m + x_n y_m - x_m y_m| < |x_n y_n - x_n y_m| \\ &\quad + |x_n y_m - x_m y_m| \leq x_n||y_n - y_m| + |y_m||x_n - x_m| \\ &\leq A|y_n - y_m| + B|x_n - x_m| < \varepsilon, \end{aligned}$$

donde $\varepsilon = \varepsilon' + \varepsilon''$.

Concluimos que la suma y el producto de sucesiones de Cauchy son nuevamente sucesiones de Cauchy.

Además, se deduce que los elementos neutros para la suma y el producto serán las sucesiones constantes 0 y 1, respectivamente. En efecto, si tomamos una sucesión cualquiera (a_k), entonces

$$(a_k) + (0) = (a_k + 0) = (a_k);\ (a_k) \cdot (1) = (a_k \cdot 1) = (a_k).$$

□

Observación 3.22.

1. Teniendo en cuenta cómo esta definido el producto en $\mathcal{C}$, el inverso de una sucesión (x_n) se definirá como $(y_n) = (\frac{1}{x_n})$. Para que exista el inverso de una sucesión será necesario que ninguno de sus términos sea nulo o tiendan en valor absoluto a cero. Si un término x_{n_0} vale cero, entonces tendríamos un término divido por cero, lo cual no tiene sentido. En caso de que los términos tiendan a cero en valor absoluto, el problema que surge es que el inverso de esa suceción puede no ser de Cauchy. Por ejemplo, si tenemos la sucesión de Cauchy (p^n) con respecto al valor absoluto p-ádico, entonces $|p^n|_p = p^{-n}$ que tiende a cero cuando n tienda a infinito. La sucesión inversa sería $(\frac{1}{p^n})$, pero $|\frac{1}{p^n}|_p = p^n$, lo cual tiende a infinito cuando n tiende a infinito, obteniéndose que no es de Cauchy.
2. El anillo $\mathcal{C}$ no es un cuerpo ya que existen elementos no nulos que no tienen inverso. Además, existen divisores de cero, como por ejemplo la sucesión de Cauchy $0, p, 0, p^2, 0, ...$ respecto de $|\cdot|_p$ que al ser multiplicada por la sucesión de Cauchy $p, 0, p^2, 0, p^3, ...$, obtenemos la sucesión constante cero $0, 0, 0, ...$.

Proposición 3.23. *Sean (x_n) una sucesión de Cauchy y (y_n) una sucesión tal que $\lim_{n\to\infty} |x_n - y_n| = 0$. Entonces, (y_n) es también una sucesión de Cauchy y tiene el mismo límite que (x_n).*

Demostración. Se deduce la desigualdad $|y_n - y_m| = |y_n - x_n + x_n - x_m + x_m - y_m| \leq |y_n - x_n| + |x_n - x_m| + |x_m - y_m|$. Por hipótesis, $\lim_{n\to\infty} |x_n - y_n| = 0$ y (x_m) es una sucesión de Cauchy, luego $0 \leq \lim_{n\to\infty} |y_n - y_m| \leq 0$ por tanto, $\lim_{n\to\infty} |y_n - y_m| = 0$ y consecuentemente $\lim_{n\to\infty} |x_n| = \lim_{n\to\infty} |y_n|$. □

Observación 3.24. Sea x un racional cualquiera. Denotaremos la sucesión constante $x, x, x, ...$ por $\widetilde{x}$ que siempre es de Cauchy.

Proposición 3.25. *La correspondencia*

$$\begin{aligned} \varphi : \mathbb{Q} &\longrightarrow \mathcal{C} \\ x &\longmapsto \widetilde{x} \end{aligned}$$

es un homomorfismo inyectivo de anillos.

Demostración. Sean x, y racionales cualesquiera. Primero, vemos que φ es una aplicación. La imagen de cualquier racional cae en $\mathcal{C}$ y si $x = y$ entonces las sucesiones que determinan serán iguales. Además, $\varphi(x+y) = \widetilde{x+y} = \widetilde{x} + \widetilde{y} = \varphi(x) + \varphi(y)$ y $\varphi(x \cdot y) = \widetilde{x \cdot y} = \widetilde{x} \cdot \widetilde{y} = \varphi(x) \cdot \varphi(y)$, luego es homomorfismo de anillos ya que $\varphi(1) = \widetilde{1}$. Está claro que si $x = 0$, entonces $x \in \ker \varphi$. Supongamos ahora que $x \in \ker \varphi$. Así, $\varphi(x) = \widetilde{x} = \widetilde{0}$ que es lo mismo que $x, x, x, ... = 0, 0, 0, ...$, llegando a que necesariamente $x = 0$ y concluyendo que φ es inyectivo. □

Proposición 3.26. *El conjunto*

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

es un ideal maximal de $\mathcal{C}$.

Demostración. El elemento neutro de $\mathcal{C}$ para la suma es $\widetilde{0}$ que pertenece a $\mathcal{N}$ ya que es una sucesión de Cauchy que tiende a 0. Sean $(x_n), (y_n)$ elementos de $\mathcal{N}$ y (z_n) un elemento cualquiera de $\mathcal{C}$. Ya sabemos que la suma y el producto de sucesiones de Cauchy es también una sucesión de Cauchy. Entonces, solamente falta probar que tienden a 0. Tenemos que $(x_n) + (y_n) = (x_n + y_n)$ y $0 \leq \lim_{n\to\infty} |x_n + y_n|_p \leq \lim_{n\to\infty}(|x_n|_p + |y_n|_p) = 0$, luego se cumple que tiende a 0. En el caso del producto, tenemos que $\lim_{n\to\infty} |x_n|_p = 0$ y se sigue que $\lim_{n\to\infty} |x_n z_n|_p = 0$, por tanto también se cumple.

Falta demostrar que $\mathcal{N}$ es maximal. Sean (x_n) una sucesión de Cauchy de $\mathcal{C}$ que no tiende a cero, es decir, que no pertenece a $\mathcal{N}$ e I el ideal generado por (x_n) en $\mathcal{C}$. Veamos que necesariamente $I = \mathcal{C}$. Como (x_n) es de Cauchy y no tiende a cero, entonces existe N natural tal que $|x_n|_p \geq c > 0$ para todo $n \geq N$. En particular, esto significa que x_n es no nulo para todo $n \geq N$, luego podemos definir una nueva sucesión (y_n) tal que $y_n = 0$ para todo $n < N$ e $y_n = \frac{1}{x_n}$ para $n \geq N$. Además, (y_n) es de Cauchy ya que para $n \geq N$ se verifica que $|y_{n+1} - y_n|_p = |\frac{1}{x_{n+1}} - \frac{1}{x_n}|_p = \frac{|x_{n+1}-x_n|_p}{|x_n x_{n+1}|_p} \leq \frac{|x_{n+1}-x_n|_p}{c^2}$ tiende a cero, por tanto (y_n) pertenece a $\mathcal{C}$ ya que $|\cdot|_p$ es no arquimediano. Observamos que

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

Esto implica que la sucesión producto $(x_n)(y_n)$ consiste en un número finito de ceros seguido de una cantidad infinita de unos. Si restamos la sucesión $(x_n y_n)$ a $\widetilde{1}$, obtenemos una sucesión de Cauchy que tiende a 0, es decir, $\widetilde{1} - (x_n)(y_n) \in \mathcal{N}$. Pero entonces $\widetilde{1}$ puede ser expresado como un múltiplo de (x_n) sumado con un elemento de $\mathcal{N}$, penteneciendo así a I. Concluimos que $I = \mathcal{C}$ y que $\mathcal{N}$ es maximal. □

Definición 3.27. *Definimos el cuerpo de los números p-ádicos como el cociente del anillo $\mathcal{C}$ con el ideal maximal $\mathcal{N}$, es decir, $\mathbb{Q}_p = \mathcal{C}/\mathcal{N}$.*

Observación 3.28. La diferencia de dos sucesiones constantes distintas nunca será un elemento de $\mathcal{N}$, sino otra sucesión constante no nula. Luego, tenemos una inclusión de $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ que envía cada $x \in \mathbb{Q}$ a la clase de equivalencia de la sucesión constante $\widetilde{x}$.

Lema 3.29. *Sea $(x_n) \in \mathcal{C}\backslash\mathcal{N}$. La sucesión de números reales $|x_n|_p$ es eventualmente estacionaria, es decir, existe N entero tal que $|x_n|_p = |x_m|_p$ para $n, m \geq N$.*

Demostración. Como (x_n) es de Cauchy y no tiende a 0, podemos encontrar c y N_1 tales que si $n \geq N_1$, entonces $|x_n|_p \geq c > 0$. Por otro lado, también existe N_2 para el cual si $n, m \geq N_2$, se cumple que $|x_n - x_m|_p < c$. Tomando $N = \text{máx}\{N_1, N_2\}$ se obtiene que si $n, m \geq N$, $|x_n - x_m|_p < c \leq \text{mín}\{|x_n|_p, |x_m|_p\}$ y como todos los triángulos en $\mathbb{Q}$ respecto al valor absoluto p-ádico son isósceles (por el Corolario 1.30), tomando el triángulo de vértices x_n, x_m y $x_n + x_m$ se concluye que $|x_n|_p = |x_m|_p$. □

Corolario 3.30. *Sean $(x_n) \in \mathcal{C}$ y $\lambda \in \mathbb{Q}_p = \mathcal{C}/\mathcal{N}$ tal que $\lambda = \lim_{x\to\infty} x_n$. Entonces, existe $\lim_{x\to\infty} |x_n|_p$.*

Demostración. Vamos a distinguir dos casos. En el primero tomamos $\lambda = 0$, entonces x_n tiende a cero y por tanto $|x_n|_p$ también, implicándose que $|\lambda|_p = 0$. En el segundo caso tenemos λ no nulo, luego por el Lema 3.29 la sucesión para n suficientemente grande se volverá estacionaria, existiendo así el límite. □

Proposición 3.31. *Sean $(x_n), (y_n) \in \mathcal{C}$ y $\lambda \in \mathbb{Q}_p$ la clase de ambas sucesiones. Entonces, $\lim_{n\to\infty} |x_n|_p = \lim_{n\to\infty} |y_n|_p$.*

Demostración. Si (y_n) es equivalente a (x_n), entonces $(x_n - y_n) \to 0$ cuando $n \to \infty$ y lo mismo ocurre en valor absoluto, llegando a que $|x_n| - |y_n|$ también tiende a cero. Por tanto, $\lim_{n\to\infty} |x_n| = \lim_{n\to\infty} |y_n|$. □

Proposición 3.32. *Sean p un número primo y $\lambda \in \mathbb{Q}_p$ la clase de la sucesión (x_n). La aplicación*

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

$$\lambda \longrightarrow |\lambda|_p := \lim_{x\to\infty} |x_n|_p \tag{3.10}$$

es un valor absoluto no arquimediano.

Demostración. La condición (i) de la Definición 1.9 se cumple porque $\lambda = 0$ si, y solo si, $(x_n) \in \mathcal{N}$, es decir, $(x_n) \to 0$, que es equivalente a que $\lim_{n\to\infty} |x_n|_p = 0$. Sean $\lambda, \mu \in \mathbb{Q}_p$ clases de (x_n) y (y_n), respectivamente. Se sigue que $\lambda\mu$ es la clase de $(x_n y_n)$. Entonces $|x_n y_n|_p = |x_n|_p |y_n|_p$ y tomando límites,

$$|\lambda\mu|_p = \lim_{n\to\infty} |x_n y_n|_p = \lim_{n\to\infty} |x_n|_p |y_n|_p = (\lim_{n\to\infty} |x_n|_p)(\lim_{n\to\infty} |y_n|_p) = |\lambda|_p |\mu|_p.$$

Ahora, $\lambda + \mu$ es la clase de $(x_n + y_n)$ y $|x_n + y_n|_p \leq |x_n|_p + |y_n|_p$, luego tomando límites como antes

$$|\lambda+\mu|_p = \lim_{n\to\infty} |x_n+y_n|_p \leq \lim_{n\to\infty} (|x_n|_p+|y_n|_p) = \lim_{n\to\infty} |x_n|_p + \lim_{n\to\infty} |y_n|_p = |\lambda|_p+|\mu|_p.$$

Concluimos que efectivamente $|\cdot|_p$ es un valor absoluto no arquimediano en $\mathbb{Q}_p$. □

Proposición 3.33. *La Definición 1.9 y el valor absoluto 3.10 de $|\cdot|_p$ son consistentes, es decir, para cualquier x racional, se cumple que $|x|_p = |\lambda|_p$, donde λ es la clase de la sucesión constante $\widetilde{x}$.*

Demostración. Se tiene que $|x|_p = \lim_{n\to\infty} |x|_p = |\lambda|_p$. □

Observación 3.34. Las Proposiciones 3.31, 3.32 y 3.33 muestran que efectivamente hemos definido un valor absoluto sobre $\mathbb{Q}_p$ que extiende el valor absoluto p-ádico sobre $\mathbb{Q}$.

Proposición 3.35. *La imagen de $\mathbb{Q}$ por $|\cdot|_p$ es igual a la imagen de $\mathbb{Q}_p$ por $|\cdot|_p$. En otras palabras, para cualquier $\lambda \in \mathbb{Q}_p \backslash \{0\}$ existe $n \in \mathbb{Z}$ tal que $|\lambda|_p = p^{-n}$.*

Demostración. Sea λ la clase de (x_n). Como $\lambda \neq 0$ y $|x_n|_p \in \mathbb{R}^+$, por el Lema 3.29 obtenemos que $\lim_{n\to\infty} |x_n|_p = p^k$, para un cierto $k \in \mathbb{Z}$. □

Teorema 3.36. *Para cada primo p, existe un cuerpo $\mathbb{Q}_p$ con un valor absoluto no arquimediano $|\cdot|_p$ tal que:*

(i) existe una inclusión $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ y el valor absoluto inducido por $|\cdot|_p$ sobre $\mathbb{Q}$ por la inclusión coincide con el valor absoluto p-ádico;
(ii) la imagen de $\mathbb{Q}$ bajo la inclusión es denso en $\mathbb{Q}_p$ con respecto al valor absoluto $|\cdot|_p$;
(iii) $\mathbb{Q}_p$ es completo con respecto al valor absoluto $|\cdot|_p$.

El cuerpo $\mathbb{Q}_p$ satisfaciendo (i), (ii) y (iii) es único salvo isomorfismo que preserva los valores absolutos.

Demostración. Comenzaremos probando la existencia. La propiedad (i) se cumple por la Observación 3.34 y la Proposición 3.35. Para probar (ii), tenemos que ver que toda bola abierta que encierra a un cierto elemento de $\mathbb{Q}_p$, λ, contiene un elemento de $\mathbb{Q}$, es decir, una sucesión constante. Sean λ la clase de la sucesión de Cauchy (x_n) y $\varepsilon > \varepsilon' > 0$. Por la Definición 3.12 *(i)*, existe $N \in \mathbb{N}$ tal que $|x_n - x_m| < \varepsilon'$ cuando $n, m \geq N$. Tomemos $y = x_N$ y consideramos la sucesión constante $\widetilde{y}$. Veamos que $\widetilde{y} \in B(\lambda, \varepsilon)$, es decir, $|\lambda - \widetilde{y}|_p < \varepsilon$. Recordamos que $\lambda - \widetilde{y}$ es la clase de la sucesión $(x_n - y)$ y $|\lambda - \widetilde{y}|_p = \lim_{n\to\infty} |x_n - y|_p$, pero para $n \geq N$ se cumple que $|x_n - y|_p = |x_n - x_N|_p < \varepsilon'$, luego tomando límites

$$\lim_{n\to\infty} |x_n - y|_p \leq \varepsilon' < \varepsilon, \tag{3.11}$$

por tanto $(\widetilde{y})$ efectivamente pertenece a $B(\lambda, \varepsilon)$. Demostremos (iii). Sea $\lambda_1, \lambda_2, ..., \lambda_n, ...$ una sucesión de Cauchy de elementos de $\mathbb{Q}_p$ tal que λ_i es la clase de la sucesión de Cauchy $(x_k^{(i)})$ de elementos de $\mathbb{Q}$. Como la imagen de $\mathbb{Q}$ es denso en $\mathbb{Q}_p$, para cada i podemos encontrar $\widetilde{y_i}$ de $\mathbb{Q}_p$ que se aproxima a λ_i tanto como queramos. Tomemos la expresión $|\lambda_i - \widetilde{y_i}|_p < \frac{1}{i}$ y aplicando límite $\lim_{i\to\infty} |\lambda_i - \widetilde{y_i}|_p = 0$. Por la Propiedad 3.23 se concluye que la sucesión $(\widetilde{y_i})$ es de Cauchy. Además, el valor absoluto de una sucesión constante es igual al valor absoluto de la constante, luego la sucesión de números racionales (y_n) es de Cauchy y define un elemento de $\mathbb{Q}_p$. Sea λ el elemento de $\mathbb{Q}_p$ correspondiente a (y_n). Probaremos que la sucesión λ (identificamos la clase con la sucesión) es justamente el límite que buscamos. Sea $\varepsilon > 0$. Como $\lambda = (y_n)$ es Cauchy, existe N tal que para cualesquiera $n, m \geq N$ se cumple que $|y_n - y_m|_p < \varepsilon/2$. Considerando la sucesión de sucesiones constantes $(\widetilde{y_n})$, tenemos la diferencia $\lambda - \widetilde{y_n}$ que representa $(y_m - y_n)$, donde n es fijo y m varía. Entonces, $|\lambda - \widetilde{y_n}|_p = \lim_{m\to\infty} |y_m - y_n|_p \leq \varepsilon/2 < \varepsilon$, luego la sucesión $\lambda - (\widetilde{y_n})$ converge a cero en $\mathbb{Q}_p$. En otras palabras, la sucesión de sucesiones constantes $(\widetilde{y_n})$ converge a la sucesión de Cauchy $\lambda = (y_n)$. Recapitulando, sabemos que $|\lambda - \widetilde{y_n}|_p$ converge a cero y $(\widetilde{y_n})$ converge a λ. Por lo cual, volviendo a usar la Propiedad 3.23, (λ_n) converge a λ y como (λ_n) es una sucesión arbitraria de Cauchy en $\mathbb{Q}_p$, hemos demostrado que cualquier sucesión de Cauchy en $\mathbb{Q}_p$ tiene límite.

Finalmente, falta demostrar la unicidad. Supongamos que existe K otro cuerpo que cumple (i), (ii) y (iii). Entonces tenemos dos cuerpos y dos inclusiones, $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ y $\mathbb{Q} \hookrightarrow \mathbb{K}$, preservando ambos valores absolutos. Si tenemos una sucesión de Cauchy (x_n) donde x_n racional, podemos tomar su imagen en $\mathbb{Q}_p$ y en K. Ambas serán sucesiones de Cauchy y también convergerán. Ahora si tomamos λ en $\mathbb{Q}_p$, como $\mathbb{Q}$ es denso en $\mathbb{Q}_p$, existe una sucesión (x_n) de términos en $\mathbb{Q}$ cuyo límite es λ. Además, como x_n es racional, luego podemos tomar sus imágenes en K que también formarán una sucesión de Cauchy. Añadir que al ser K completo, la sucesión convergerá y llamemos $f(\lambda)$ al límite. Esto genera una

correspondencia f de $\mathbb{Q}_p$ en K que coincide con la identidad cuando es restringida a $\mathbb{Q}$. Está claro que la imagen de cualquier elemento de $\mathbb{Q}_p$ está en K y si hay dos elementos iguales, necesariamente sus imágenes también lo serán. Además, por cómo están definidas las operaciones llegamos a que f es un homomorfismo de anillos y al tratarse de cuerpos, f será inyectivo. □

Observación 3.37. En la Expresión (3.11) tenemos un $\leq$ ya que la sucesión puede tender a un cierto valor a pesar de ser consistentemente menor que él.

4

Exploración de $\mathbb{Q}_p$

La meta de este capítulo es explorar el cuerpo $\mathbb{Q}_p$ que hemos construido en el capítulo 3. La referencia principal que hemos seguido para este capítulo es [2].

Vamos a identificar $\mathbb{Q}$ con su imagen en $\mathbb{Q}_p$ y pensaremos en $\mathbb{Q}$ como un subcuerpo de $\mathbb{Q}_p$. El objetivo es entender cómo son sus elementos y en particular, comprobar que tienen una representación única usando potencias de p.

Sabemos por la Proposición 3.35 que tanto $\mathbb{Q}$ como $\mathbb{Q}_p$ tienen la misma imagen bajo $|\cdot|_p$. En particular, dicho conjunto imagen es igual a $\{p^n : n \in \mathbb{Z}\} \cup \{0\}$. Esto nos será de gran utilidad y lo enunciaremos como un lema:

Lema 4.1. *Para cada $x \in \mathbb{Q}_p \backslash \{0\}$ existe un entero $n \in \mathbb{Z}$ tal que $|x|_p = p^{-n}$. Recíprocamente, para cada $n \in \mathbb{Z}$ podemos encontrar $x \in \mathbb{Q}_p$ que cumple $|x|_p = p^{-n}$.*

Otra manera de expresarlo en términos de la valoración p-ádica, v_p, sería:

Lema 4.2. *Para cada $x \in \mathbb{Q}_p \backslash \{0\}$ existe un entero $v_p(x) = n$ tal que $|x|_p = p^{-n}$. En otras palabras, la valoración p-ádica v_p se extiende a $\mathbb{Q}_p$.*

4.1. Los enteros p-ádicos

Ahora comenzaremos a explorar la estructura de $\mathbb{Q}_p$. De la Proposición 3.32 sabemos que $|\cdot|_p$ es un valor absoluto no arquimediano. Podemos entonces dar la siguiente definición:

Definición 4.3. *El anillo de los enteros p-ádicos es el anillo de valoración respecto de $|\cdot|_p$ $\mathbb{Z}_p := \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$.*

Observación 4.4. Sabemos de la Definición 1.39 que $\mathbb{Z}_p$ es la bola unidad cerrada de centro 0. Por teoría de Análisis sabemos que un conjunto es cerrado si, y solo si, toda sucesión convergente contenida en él también tiene límite en él, luego toda sucesión convergente de elementos de $\mathbb{Z}_p$ tiene límite en $\mathbb{Z}_p$. Además, como

$\mathbb{Q}_p$ es completo, todas sus sucesiones de Cauchy convergen a un elemento de $\mathbb{Q}_p$. Por tanto, toda sucesión de Cauchy en $\mathbb{Z}_p$ converge a un elemento de $\mathbb{Z}_p$, entonces $\mathbb{Z}_p$ también es completo.

Proposición 4.5. *El anillo de los enteros p-ádicos $\mathbb{Z}_p$ es un anillo local cuyo ideal maximal es $p\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p < 1\}$. Además:*

(i) $\mathbb{Q} \cap \mathbb{Z}_p = \mathbb{Z}_{(p)} := \{\frac{a}{b} \in \mathbb{Q} : p \text{ no divide a } b\}$.
(ii) La imagen de la inclusión $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ es densa. En particular, dado $x \in \mathbb{Z}_p$ y $n \geq 1$, existe un único $\alpha \in \mathbb{Z}$ tal que $0 \leq \alpha \leq p^n - 1$ que cumple $|x - \alpha|_p \leq p^{-n}$.
(iii) Para cualquier $x \in \mathbb{Z}_p$ existe una sucesión de Cauchy (α_n) que converge a x y que verifica las siguientes propiedades:
a) *$\alpha_n \in \mathbb{Z}$ safistace $0 \leq \alpha_n \leq p^n - 1$;*
b) *para todo $n \geq 2$ tenemos $\alpha_n \equiv \alpha_{n-1}$ (mód p^{n-1}).*

Demostración. Sabemos que $\mathbb{Z}_p$ es un anillo de valoración y por la Proposición 1.40, tenemos que es un anillo local. Veamos ahora que su único ideal maximal está generado por p. Por el Lema 4.1, si $x \in \mathbb{Z}_p \subseteq \mathbb{Q}_p$ es no nulo, entonces existe un entero positivo n tal que $|x|_p = p^{-n}$. Ahora, si $|x|_p < 1 = p^0$, se tiene que $|x|_p \leq p^{-1}$ y como $|p|_p = p^{-1}$, resulta que $\left|\frac{x}{p}\right| \leq 1$ y por tanto, $x \in p\mathbb{Z}_p$. Teniendo en cuenta la Proposición 1.40 *(c)* y que $\mathbb{Z}_p \neq p\mathbb{Z}_p$, se concluye que el ideal de valoración coincide con $p\mathbb{Z}_p$.

Demostremos (i). Sabemos $\mathbb{Q} \cap \mathbb{Z}_p = \{x \in \mathbb{Q} : |x|_p \leq 1\}$. Si suponemos $x = \frac{a}{b} \in \mathbb{Q} \cap \mathbb{Z}_p$ fracción irreducible, entonces $|x| \leq 1$ y necesariamente p no divide a b. En cambio, si $x = \frac{a}{b} \in \mathbb{Q}$ tal que p no divide a b, luego $|x| \leq 1$. Por tanto, concluimos que $\mathbb{Q} \cap \mathbb{Z}_p = \mathbb{Z}_{(p)}$.

Para probar (ii), tomamos $x \in \mathbb{Z}_p$ y $n \geq 1$. Como $\mathbb{Q}$ es denso en $\mathbb{Q}_p$, podemos seleccionar $\frac{a}{b} \in \mathbb{Q}$ tal que

$$\left|x - \frac{a}{b}\right|_p \leq p^{-n} < 1. \tag{4.1}$$

De hecho, queremos probar que podemos escoger un entero. Observamos que $|\frac{a}{b}|_p = |\frac{a}{b} - x + x|_p \leq \max\{|x - \frac{a}{b}|_p, |x|_p\} \leq 1$ por la condición *(iv)* de la Definición 1.9, la desigualdad (4.1) y porque $x \in \mathbb{Z}_p$. Entonces $\frac{a}{b} \in \mathbb{Z}_{(p)}$, es decir, p no divide a b. Recordamos que si p no divide a b, existe $b' \in \mathbb{Z}/p\mathbb{Z}$ único tal que $bb' \equiv 1$ (mód p^n), es decir, existe $k \in \mathbb{Z}$ tal que $1 - bb' = kp^n$. Esto implica que

$$\left|\frac{a}{b} - ab'\right|_p = \left|\frac{a(1 - bb')}{b}\right|_p = \left|\frac{akp^n}{b}\right|_p \leq p^{-n},$$

y donde $ab' \in \mathbb{Z}$. Por último, escogemos α como el único entero tal que

$$0 \leq \alpha \leq p^n - 1 \quad \text{y} \quad \alpha \equiv ab' \text{ (mód } p^n), \tag{4.2}$$

entonces $|x-\alpha|_p = |x-\frac{a}{b}+\frac{a}{b}-\alpha|_p \leq \max\{|x-\frac{a}{b}|_p, |\frac{a}{b}-\alpha|_p\} \leq 1$ por la condición *(iv)* de la Definición 1.9, la inecuación (4.1) y por (4.2).

Finalmente, obsérvese que la sucesión (α_n) de la Proposición 4.5 *(ii)* es coherente (ver Defnición 3.18). □

Corolario 4.6. *$\mathbb{Z}$ es denso en $\mathbb{Z}_p$.*

Demostración. Se cumple por la Propiedad 4.5 *(ii)*.

Corolario 4.7.

(i) Para cada $x \in \mathbb{Q}_p$ existe $n \geq 0$ tal que $p^n x \in \mathbb{Z}_p$, es decir, $\mathbb{Q}_p = \mathbb{Z}_p[1/p]$.
(ii) La aplicación

$$\begin{aligned} \varphi : \mathbb{Q}_p &\longrightarrow \mathbb{Q}_p \\ x &\longrightarrow px \end{aligned}$$

es un homeomorfismo.
(iii) Los conjuntos $p^n\mathbb{Z}_p$ con $n \geq 1$ forman un sistema fundamental de entornos de $0 \in \mathbb{Q}_p$ que recubre $\mathbb{Q}_p$.

Demostración. Demostremos *(i)*. Si $x \in \mathbb{Q}_p$, por el Lema 4.2 calculamos $v_p(x)$ que es un entero. En caso de que $v_p(x) \geq 0$, entonces $x \in \mathbb{Z}_p$ por la Definición 4.3. En cambio si $v_p(x) < 0$, se tiene que $v_p(p^{-v_p(x)}x) = -v_p(x) + v_p(x) = 0$, luego $p^{-v_p(x)}x \in \mathbb{Z}_p$ y por tanto $x \in \mathbb{Z}_p[1/p]$.

Ahora, *(ii)* sigue de la Proposición 1.23.

Falta demostrar *(iii)*. Recordamos que $\mathbb{Z}_p$ es la bola unidad cerrada centrada en 0, luego es un abierto que contiene a 0 y, por tanto, un entorno de 0. Como la multiplicación por p, es decir φ, es un homeomorfismo, envía abiertos en abiertos, esto implica que para cada $n \geq 1$ el conjunto $p^n\mathbb{Z}_p$ es un entorno abierto de 0. Además, por el Corolario 4.7 (i) obtenemos

$$\bigcup_{n\in\mathbb{Z}} p^n\mathbb{Z}_p = \mathbb{Q}_p.$$

Para probar que los conjuntos $p^n\mathbb{Z}_n$ forman un sistema fundamental de entornos de $0 \in \mathbb{Q}_p$, tenemos que demostrar que cualquier abierto al que pertenece 0 contiene a $p^n\mathbb{Z}_p$ para algún n, lo cual se cumple ya que toda bola abierta contiene un bola cerrada de radio menor. □

Corolario 4.8. *Sean $x \in \mathbb{Q}_p$ y n_0 el mayor entero n tal que $x \in p^n\mathbb{Z}_p$. Entonces, $v_p(x) = n_0$.*

Demostración. Si $v_p(x) = n \in \mathbb{Z}$, entonces $|x|_p = p^{-n} \not\leq p^{-(n+1)}$ y $x \in p^n\mathbb{Z}_p$. Pero $x \notin p^{n+1}\mathbb{Z}_p$, luego $n_0 = n$. □

Uno de los puntos principales de estos resultados es que la topología de $\mathbb{Q}_p$ está cercanamente conectada con su estructura algebraica. Por tanto, un concepto que tendremos presente es que $|x-y|_p \leq p^{-n}$ si, y solo si, $x-y \in p^n\mathbb{Z}_p$. En particular, $\bar{B}(0,p^{-n}) = p^n\mathbb{Z}_p$.

Las unidades p-ádicas son los elementos invertibles de $\mathbb{Z}_p$ y denotaremos su conjunto por $\mathbb{Z}_p^\times$. Además, si $x \in \mathbb{Z}_p^\times$, entonces $|x| \leq 1$ y $|x^{-1}| \leq 1$ (es decir $|x^{-1}|_p = |x|_p^{-1}$) y $\mathbb{Z}_p^\times = \{x \in \mathbb{Q}_p : |x|_p = 1\}$. Se sigue que $\mathbb{Z}_p^\times \cap \mathbb{Q} = \left\{\frac{a}{b} : p \text{ no divide a } ab\right\}$.

4.2. Los elementos de $\mathbb{Q}_p$

Para poder comprender mejor los elementos de $\mathbb{Q}_p$, veremos dos descripciones diferentes de estos.

4.2.1. Descripción de $\mathbb{Q}_p$ en términos de sucesiones coherentes

Dado $x \in \mathbb{Z}_p$, podemos encontrar una sucesión de Cauchy (α_n) que converge a x con las características que se detallan en la Proposición 4.5 (iii). Como la sucesión (α_n) es coherente, será de Cauchy, porque $|\alpha_{n+1}-\alpha_n|_p \leq p^{-n}$ para todo $n \geq 1$. Además, por la Observación 4.4, (α_n) converge a un elemento de $\mathbb{Z}_p$.

Proposición 4.9. *Sea (x_n) una sucesión de Cauchy de números enteros. Entonces, (x_n) converge a un elemento de $\mathbb{Z}_p$.*

Demostración. Sigue de la Observación 4.4, pues identificamos $\mathbb{Z}$ con su imagen en $\mathbb{Z}_p$. □

Por la Proposición 4.9, podemos identificar los elementos de $\mathbb{Z}_p$ con las sucesiones de Cauchy de términos enteros.

Para demostrar la siguiente propiedad es necesario establecer algunos conceptos. Denotaremos φ_n a la proyección en el cociente

$$\varphi_n : \mathbb{Z}_p \longrightarrow \mathbb{Z}/p^n\mathbb{Z},$$

donde $\varphi_n(x) \equiv \alpha_n \pmod{p^n}$. También fijamos $A_n = \mathbb{Z}/p^n\mathbb{Z}$, donde definimos $\phi_n : A_n \longrightarrow A_{n-1}$ tal que la imagen de $a \pmod{p^n}$ es $a \pmod{p^{n-1}}$. Queremos considerar el producto de todos los anillos A_i con $i = 1, 2, \ldots, n, \ldots$ donde las operaciones se definen término a término.

Proposición 4.10. *Las proyecciones φ_n proporcionan una inclusión*

$$\varphi : \mathbb{Z}_p \hookrightarrow \prod_{n\geq 1} A_n$$

que identifica $\mathbb{Z}_p$ con el anillo de sucesiones coherentes $\prod_{n\geq 1} A_n$, es decir, las sucesiones (α_n) tal que $\phi_n(\alpha_n) = \alpha_{n-1}$ para cada $n \geq 1$.

Demostración. Sea $\lambda \in \mathbb{Z}_p$. Por la Proposición 4.5 *(iii)* existe una sucesión (α_n) coherente que converge a λ. Entonces, $\varphi(\lambda) := (\varphi_1(\lambda), \varphi_2(\lambda), \ldots, \varphi_n(\lambda), \ldots) = (\alpha_1, \alpha_2, \ldots, \alpha_n, \ldots)$. Sabemos que necesariamente $0 \in \ker \varphi$. Si $\lambda \in \ker \varphi$, se tiene que $\varphi(\lambda) = (\alpha_1, \alpha_2, \ldots, \alpha_n, \ldots) = (0, 0, \ldots)$, luego $\lambda = 0$ y φ es inyectivo. Además, φ es sobreyectiva porque φ_n lo es para todo n, por tanto concluimos que φ identifica $\mathbb{Z}_p$ con $\prod_{n\geq 1} A_n$. □

4.2.2. Descripción de $\mathbb{Q}_p$ en términos de expansiones p-ádicas

Sea $x \in \mathbb{Z}_p$ un entero p-ádico. Por la Proposición 4.5 *(iii)* sabemos que existe una sucesión de enteros coherente (α_n) que converge a x tal que $\alpha_n \equiv x \pmod{p^n}$, $\alpha_{n+1} \equiv \alpha_n \pmod{p^n}$ y $0 \leq \alpha_n \leq p^n - 1$. A continuación, expresaremos α_n en base p:

$$\begin{aligned} \alpha_1 &= b_0 & 0 \leq b_0 \leq p-1 \\ \alpha_2 &= b_0 + b_1 p & 0 \leq b_1 \leq p-1 \\ \alpha_3 &= b_0 + b_1 p + b_2 p^2 & 0 \leq b_2 \leq p-1 \\ \alpha_4 &= b_0 + b_1 p + b_2 p^2 + b_3 p^3 & 0 \leq b_3 \leq p-1 \\ &\cdots & \cdots, \end{aligned} \tag{4.3}$$

obteniendo la expansión en serie

$$b_0 + b_1 p + b_2 p^2 + \cdots + b_n p^n + \cdots. \tag{4.4}$$

Obsérvese que el término b_i en cada uno de los α_j es el mismo para todo $j > i \geq 0$ porque hemos definido la sucesión (α_n) tal que $\alpha_{n+1} \equiv \alpha_n \pmod{p^n}$ y $0 \leq \alpha_n \leq p^n - 1$.

Lema 4.11. *Dado cualquier $x \in \mathbb{Z}_p$, la serie (4.4) converge a x.*

Demostración. Recordamos que una serie converge a x si, y solo si, la sucesión de sus sumas parciales converge a x. Como las sumas parciales son α_n, converge a x por la Propiedad 4.5 *(iii)*. □

Corolario 4.12. *Todo $x \in \mathbb{Z}_p$ puede expresarse como*

$$x = b_0 + b_1 p + b_2 p^2 + \cdots + b_n p^n + \cdots, \tag{4.5}$$

donde $0 \leq b_i \leq p-1$ y esta representación es única.

Demostración. La igualdad (4.5) se cumple por el Lema 4.11. Además, la representación es única porque los términos α_n de (4.3) son únicos, luego los términos b_n también lo son pues son los dígitos de x en base p. □

Corolario 4.13. *Todo $x \in \mathbb{Q}_p$ puede expresarse de la forma*

$$x = b_{-m}p^{-m} + \cdots + b_0 + b_1 p + b_2 p^2 + \cdots + b_n p^n + \cdots = \sum_{n \geq -m} b_n p^n, \tag{4.6}$$

donde $0 \leq b_i \leq p-1$ y $-m = v_p(x)$. Además, esta representación es única.

Demostración. Si $x \in \mathbb{Z}_p \subseteq \mathbb{Q}_p$ se cumple por el Corolario 4.12, luego supongamos que $x \in \mathbb{Q}_p \backslash \mathbb{Z}_p$.

Sea n el mayor entero tal que $x \in p^n \mathbb{Z}_p$. Si $n \geq 0$ entonces $x \in \mathbb{Z}_p$. Supongamos $n < 0$ y $n = -m$ para cierto $m > 0$. Por el Corolario 4.8, $v_p(x) = -m$. Además, podemos expresar $x = p^{-m}y$, donde $y = p^m x \in \mathbb{Z}_p$. Entonces, por el Corolario 4.12, tenemos

$$y = a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n + \cdots . \tag{4.7}$$

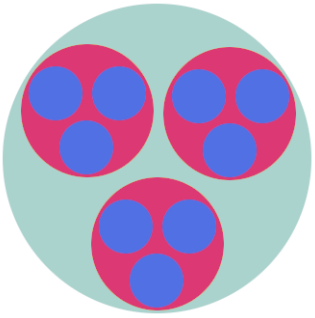
Si multiplicamos (4.7) por p^{-m}, se tiene

$$x = p^{-m}y = a_0 p^{-m} + a_1 p^{-m+1} + a_2 p^{-m+2} + \cdots + a_n p^{-m+n} + \cdots , \tag{4.8}$$

donde algunas potencias tienen exponente negativo. Si en (4.8) reescribimos $b_{i-m} := a_i$, para todo $i \geq 0$ llegamos a la expresión (4.6).

Además, esta expresión es única ya que al tomar $-m$ el mayor entero negativo tal que $x \in p^{-m}\mathbb{Z}_p$, será único e $y \in \mathbb{Z}_p$, entonces por el Corolario 4.12 también es único. □

El siguiente diagrama es una posible representación de los números 3-ádicos



donde en cada círculo hay otros tres indefinidamente. En esta representación el círculo de mayor tamaño representa la base donde vamos a comenzar. Consideramos cada color como una potencia de 3 que va aumentando conforme más niveles de color haya y donde cada trío de círculos del mismo color y contenidos en los mismos círculos son los posibles coeficientes que puedan acompañar a la potencia de 3, siendo estos 0, 1 y 2.

5

Conclusiones

A lo largo de esta memoria, hemos estudiado los números p-ádicos y algunas de sus propiedades. Comenzamos definiendo los valores absolutos y las distancias en función de estos números, los cuales nos han proporcionado resultados que a primera vista no concuerdan con nuestra intuición, como en el caso de los espacios ultramétricos donde todo punto dentro de una bola es un centro y todos los triángulos son isósceles.

Hemos abordado el problema de determinar soluciones de polinomios módulo potencias de un primo, demostrando el Lema de Hensel y una generalización del mismo. Estos resultados tienen como objetivo *elevar* las soluciones que tenemos en módulo potencia de un primo al módulo de la potencia inmediatamente superior, determinando si existen y, en tal caso, cuáles son.

También hemos construido la completación del cuerpo de los números racionales $\mathbb{Q}$ con respecto al valor absoluto p-ádico, obteniendo así el cuerpo de los números p-ádicos $\mathbb{Q}_p$. Demostramos el Teorema de Ostrowski, concluyendo que todo valor absoluto no trivial sobre $\mathbb{Q}$ es equivalente a un valor absoluto p-ádico, considerando p un número primo o $p = \infty$. Además probamos la Fórmula Producto, donde el producto de todos los valores absolutos de un racional no nulo es igual a 1.

Por último, hemos estudiado los elementos de $\mathbb{Q}_p$, en particular los enteros p-ádicos $\mathbb{Z}_p$. A continuación presentamos dos posibles descripciones de sus elementos, utilizando secuencias coherentes y expansiones p-ádicas, donde analizamos las propiedades en cada una de estas descripciones.

Como indica el título, esta memoria constituye una introducción a los números p-ádicos. Este estudio podría ampliarse profundizando en el Lema de Hensel y en el principio local-global. También se podría continuar explorando enfoques analíticos mediante el análisis de $\mathbb{Q}_p$ y $\mathbb{C}_p$, o desde un punto de vista algebraico, estudiando los espacios vectoriales y las extensiones de cuerpos. Para ello puede consultarse [2].

Bibliografía

[1] Díaz, Francisco J. y García Calcines, José M. *Curso de Topología General.* Vision Net. 2005.

[2] Gouvêa, Fernando Q. *p-adic Numbers. An Introduction.* Third edition. Universitext. 2020.

[3] *Lecture 7: Polynomial Congruences To Prime Power Moduli* [en línea]. [Fecha de consulta: 24-06-2023]. Disponible en: https://www.math.uzh.ch/gorodnik/nt/lecture7.pdf.

[4] *Prime Power Congruences* [en línea]. [Fecha de consulta: 28-06-2023]. Disponible en: https://sites.millersville.edu/bikenaga/number-theory/prime-power-congruences/prime-power-congruences.html.

An Introduction To p-adic Numbers

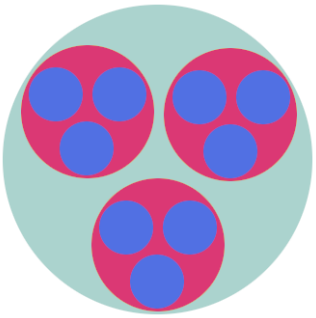
Claire Marie Hubbard
Facultad de Ciencias • Sección de Matemáticas
Universidad de La Laguna
alu0101328324@ull.edu.es

Abstract

In this work we shall introduce and study the p-adic numbers. Firstly, we aim to establish the foundations for building our theory of p-adic numbers. In the second part, we will solve congruences modulo p^n and prove Hensel's Lemma. The third section will confirm that essentially there are only three types of absolute values on $\mathbb{Q}$ and we will construct the field of p-adic numbers, denoted by $\mathbb{Q}_p$. Section four will explore the field $\mathbb{Q}_p$, discussing the p-adic integers, denoted by $\mathbb{Z}_p$, and providing two possible descriptions of elements in $\mathbb{Q}_p$.

1. Introduction

The importance of p-adic numbers goes beyond mathematics, finding applications in theoretical physics, cryptography, computer science, and other scientific and engineering disciplines. These numbers were introduced by the German mathematician Kurt Hensel in 1897, who was exploring an analogy between the ring of integers $\mathbb{Z}$ with its field of fractions $\mathbb{Q}$ and the ring of polynomials with complex coefficients $\mathbb{C}[x]$ along with its field of fractions $\mathbb{C}(x)$.
The p-adic numbers are finite-tailed Laurent series in p, where p is a prime number.



A visualisation of the 3-adic numbers.

While in real numbers, the absolute value measures the distance of a number from zero on the number line, in p-adic numbers, the absolute value is based on divisibility by powers of p. Although counter-intuitive at first glance, the more divisible a p-adic number is by powers of p, the smaller its p-adic absolute value will be.
As there are infinite prime numbers, the p-adic numbers also form infinite completions of the rational numbers $\mathbb{Q}$ with respect to the p-adic absolute value.

2. Ultrametric Distances

The p-adic absolute value on a field where p is a prime number is non-arquimedian and therefore the distance induced by this absolute value is an ultrametric and the field associated is an ultrametric space. When working with a space of this quality one will obtain surprising results such as:

1. Let $\mathbb{K}$ be a field and $|\cdot|$ be a non-archimedean absolute value on $\mathbb{K}$. If $x, y \in \mathbb{K}$ and $|x| \neq |y|$, then $|x+y| = \max\{|x|, |y|\}$.
2. In an ultrametric space, all triangles are isosceles.
3. Every point inside a ball is a center of that ball.
4. Two balls are either disjoint or one contains the other.

3. Helsel's Lemma

Hensel's Lemma provides a method for lifting solutions of polynomials modulo prime powers to solutions of the module of immediate higher power and states the following:
Let $f \in \mathbb{Z}[x]$, $n \geq 1$, p be a prime number, and $c \in \mathbb{Z}_{p^n}$ a solution of $f(x) \equiv 0 \pmod{p^n}$. If p does not divide $f'(c)$, then $f(x) \equiv 0 \pmod{p^{n+1}}$ has a unique solution congruent to $c \pmod{p^n}$, given by $c + p^n t$, where

$$t = -f'(c)^{-1}\frac{f(c)}{p^n} \pmod{p}.$$

This result provides the possibility to create coherent sequences, which are sequences of integers α_n that satisfy $0 \leq \alpha_n \leq p^n - 1$ and $\alpha_n \equiv \alpha_{n+1} (\text{mod } p^n)$.

4. The Absolute Values on $\mathbb{Q}$

Ostrowski's Theorem establishes that there exists a complete list of all possible absolute values on $\mathbb{Q}$, and any other absolute value is equivalent to one of them. The list includes:

1. Trivial absolute value.
2. p-adic absolute value, where p is a prime number.
3. Usual or ∞-adic absolute value.

The Product Formula, consequence of Ostrowski's Theorem, states:
For any $x \in \mathbb{Q}\backslash\{0\}$, it holds that

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

5. Exploring $\mathbb{Q}_p$

Here we explore the field of p-adic numbers $\mathbb{Q}_p$, discussing in particular the properties of the p-adic integers $\mathbb{Z}_p$. Later we shall give two possible descriptions of $x \in \mathbb{Q}_p$. The first in terms of p-adic expansions

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

and the second where we identify x with the coherent sequence (α_n) that converges to it.

References

[1] Gouvêa, Fernando Q. *p-adic Numbers. An Introduction.* Third edition. Universitext. 2020.