Universidad de Valladolid

FACULTAD DE CIENCIAS

Trabajo Fin De Grado

Grado en Matemáticas

Introducción A Los Números P-ádicos

Autor: Fernando Rabanillo Novoa

Tutor: Manuel Mariano Carnicer Arribas

A mi tutor Manolo Carnicer, por guiarme a lo largo de este trabajo y arrojar luz donde yo no era capaz de ver.

A mis padres y a mi hermano, por apoyarme durante estos años y confiar en mí, porque sin su cariño jamás lo habría conseguido.

A mi abuelo Julián, a mi abuela Aurora y, en especial, a mi abuela Araceli, que te fuiste antes de tiempo. Que allá donde estés te sientas orgullosa de mí.

A mi pareja Raquel, por creer en mí desde el primer momento y darme la paz que necesitaba para lograrlo.

A todos mis familiares, amigos y seres queridos que durante todos estos años me han acompañado en el trayecto, en especial a Fernandito y a Álvaro, juntos empezamos este viaje y espero teneros siempre.

II

Introducción

Nacidos de la necesidad de resolver ecuaciones en teoría de números y desarrollada profundamente en el siglo XX, los números p-ádicos son una extensión fascinante de los números racionales que permiten una nueva forma de entender las congruencias y la distancia entre estos números. Esta nueva teoría tuvo un impacto significativo en diversas áreas de las matemáticas, incluyendo la teoría de números, el análisis, el álgebra y la criptografía.

La historia de los números p-ádicos comienza con la idea de congruencia modular introducida por Carl Friedrich Gauss en su obra *Disquisitiones Arithmeticae* (1801). Gauss estudió las propiedades de los números enteros bajo aritmética modular, que sentaron las bases para el desarrollo posterior de los números p-ádicos.

Sin embargo, el concepto formal de los números p-ádicos fue introducido por el matemático alemán Kurt Hensel en 1897. Hensel observó que, al extender el concepto de valor absoluto a los números racionales de una manera diferente, se podía definir una nueva topología que daba lugar a los números p-ádicos. Su obra fue pionera y abrió una nueva rama en la teoría de números, proporcionando una herramienta poderosa para entender problemas clásicos desde una perspectiva novedosa.

A lo largo del siglo XX, varios matemáticos hicieron contribuciones significativas al desarrollo y la comprensión de los números p-ádicos. Entre ellos destaca Helmut Hasse, quien aplicó los números p-ádicos a la teoría de campos y ecuaciones diofánticas, y Ernst Witt, creador de los vectores de Witt, que aclaran y generalizan la estructura de los números p-ádicos, y la formulación de las extensiones de Witt, que tienen aplicaciones en la teoría de números y la geometría algebraica.

Además, la teoría p-ádica ha sido fundamental en el desarrollo de la teoría de formas modulares y la conjetura de Taniyama-Shimura, que fue crucial en la demostración del último teorema de Fermat por Andrew Wiles en 1995. Los números p-ádicos también han sido aplicados en criptografía y en ciencias de la computación, donde un grupo de matemáticos indios presentaron un algoritmo para multiplicación de enteros basado en los números p-ádicos y que ofrece la mejor complejidad en bits.

A lo largo de este trabajo construiremos estos números con detenimiento, siguiendo para ello el libro de Fernando Q.Gouvêa [1]. Comenzaremos por el primer capítulo, en el que generalizaremos la definición de valor absoluto a cualquier cuerpo, haciendo especial énfasis en los valores absolutos no arquimedianos, cuya propiedad especial dará pie a una topología métrica muy distinta a la que acostumbramos en $\mathbb{Q}$. También presentaremos el Teorema de Ostrowski, que demostraremos siguiendo el texto de Brain Conrad [4], y que nos ayudará a entender mejor cómo son todos los valores absolutos que podemos definir sobre $\mathbb{Q}$, además de dar una pequeña introducción a las valoraciones sobre un cuerpo, para lo cual seguiremos el libro de Ribenboim [2].

Tras este primer capítulo más general donde sentaremos las bases para la definición de los números p-ádicos, abordaremos ya la compleción de $\mathbb{Q}$, presentando el problema de incompletitud de este cuerpo, siguiendo para ello la prueba de José Carlos Santos [5], y construiremos un nuevo cuerpo que lo complete, finalizando este segundo capítulo con la definición de $\mathbb{Q}_p$.

En el tercer y último capítulo, describiremos la estructura algebraica y topológica del nuevo cuerpo $\mathbb{Q}_p$, daremos una idea de cómo representar sus elementos y finalizaremos el trabajo enunciando y demostrando, en dos versiones distintas, el que es posiblemente el resultado más importante de la teoría p-ádica, el Lema de Hensel, cuya primera versión demostraremos siguiendo la prueba el texto de Yiduan Zheng [6], y que nos proporcionará un método para obtener todas las raíces de una ecuación en congruencias y que es aplicable también en la creación de algoritmos para la factorización de polinomios.

Aunque no hablaremos de ello en esta memoria debido a que nos extenderíamos demasiado, en el cuerpo $\mathbb{Q}_p$ podemos definir todos aquellos conceptos típicos del análisis como la continuidad, derivación, integración, series... Estos tendrán propiedades distintas a las del análisis clásico, siendo una de las más notables, como veremos más adelante, la convergencia de las series, menos sutil de lo que estamos acostumbrados.

Por último, enunciaremos el Teorema de Hasse-Minkowski, de gran importancia y que, aunque no demostraremos debido a que necesitaríamos un estudio profundo de las formas cuadráticas para ello, no podía faltar en este trabajo pues dará una utilidad práctica a toda la teoría que habremos desarrollado hasta entonces.

En resumen, los números p-ádicos nos proporcionarán una perspectiva diferente y complementaria a la de los números reales, ampliando las herramientas disponibles para el análisis matemático y la resolución de problemas en diversas áreas de las matemáticas.

Índice general

Capítulo 1

Fundamentos

Los valores absolutos en el contexto de un cuerpo $\mathbb{K}$ son una herramienta fundamental en el estudio del Análisis. Estas funciones nos proporcionan una noción de distancia o tamaño en el cuerpo, permitiendo definir conceptos como límites, continuidad y derivabilidad. En esencia, los valores absolutos capturan la noción de magnitud, independientemente de la dirección, y son una pieza clave en el estudio de las propiedades algebraicas y topológicas de un cuerpo.

1.1. Valores Absolutos sobre un Cuerpo

Cuando hablamos de valores absolutos, rápidamente se nos viene a la mente el valor absoluto usual sobre $\mathbb{R}$ que asigna a cada número real ese mismo número si es positivo o su opuesto si es negativo. A continuación daremos una definición más general sobre un cuerpo arbitrario y una serie de propiedades, además de presentar un caso particular sobre $\mathbb{Q}$ que nos resultará de gran interés a medida que vayamos avanzando en el texto.

Definición 1.1.1. *Sea $\mathbb{K}$ un cuerpo. Un* valor absoluto *definido en $\mathbb{K}$ es una función*

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

que cumple lo siguiente:

1) $|x| = 0$ si, y solo si, $x = 0$;

2) $|xy| = |x||y|$ para cada $x, y \in \mathbb{K}$;

3) $|x + y| \leq |x| + |y|$ para cada $x, y \in \mathbb{K}$.

Definición 1.1.2. *Un valor absoluto sobre $\mathbb{K}$ se dice que es* no arquimediano *si satisface las condiciones 1),2),3) y, además,*

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

para cada $x, y \in \mathbb{K}$.
De no cumplir esta última propiedad, se dice que el valor absoluto es arquimediano.

Observación 1.1.3. *Esta última es más fuerte que la desigualdad triangular. Habitualmente lo que haremos para probar que una aplicación es un valor absoluto no arquimediano será probar las propiedades 1) y 2) junto con esta propiedad.*

A lo largo de este texto veremos las curiosas propiedades que derivan de estos valores absolutos no arquimedianos y como resulta más sencillo trabajar con ellos.

Ejemplo 1.1.4.

a) Si tomamos el cuerpo $\mathbb{K} = \mathbb{Q}$ podemos definir la función

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

Que es el valor absoluto usual, otras veces llamado valor absoluto infinito y denotado como $|\cdot|_\infty$ por motivos que veremos más adelante. Nótese además que es arquimediano ya que para cualesquiera $x, y \in \mathbb{Q}_+$ se tiene que

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

b) Tomando, de nuevo, el cuerpo $\mathbb{Q}$, podemos definir la función

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

Que es el denominado valor absoluto trivial, el cual es no arquimediano.

c) Sea $\mathbb{K}$ un cuerpo, $\mathbb{K}[X]$ su anillo de polinomios y $\mathbb{K}(X)$ su cuerpo de fracciones. Entonces podemos definir una aplicación, v_∞, que da lugar a un valor absoluto no arquimediano en $\mathbb{K}(X)$ de la siguiente forma:
Para cualquier $f(X) \in \mathbb{K}[X]$, $v_\infty(f(X)) = -\deg(f(X))$. Ahora extendemos esto a $\mathbb{K}(X)$ haciendo:

$$v_\infty\left(\frac{f(X)}{g(X)}\right) = v_\infty(f(X)) - v_\infty(g(X))$$

con el ajuste de $v_\infty(0) = \infty$.
Es sencillo comprobar que la aplicación

$$|\cdot|_\infty : \mathbb{K}(X) \longrightarrow \mathbb{R}_+, \quad |f(X)|_\infty = \mathrm{e}^{-v_\infty(f(X))}$$

es un valor absoluto no arquimediano.

A partir de la desigualdad triangular podemos obtener otra que nos será de gran utilidad a la hora de probar ciertos resultados, la llamada *segunda desigualdad triangular*:

Lema 1.1.5 (**Segunda desigualdad triangular**). *Sea $\mathbb{K}$ un cuerpo y $|\cdot|$ un valor absoluto definido en él. Para cada $x, y \in \mathbb{K}$ se cumple*

$$||x| - |y||_\infty \leq |x - y|.$$

Demostración. En virtud de la desigualdad triangular,

$$|x| = |x + y - y| \leq |x - y| + |y| \Longrightarrow |x| - |y| \leq |x - y|.$$

De la misma forma,

$$|y| = |y + x - x| \leq |x - y| + |x| \Longrightarrow |y| - |x| \leq |x - y| \Longrightarrow |x| - |y| \geq -|x - y|.$$

Y, por tanto, se tiene que

$$-|x - y| \leq |x| - |y| \leq |x - y| \Longrightarrow ||x| - |y||_\infty \leq |x - y|.$$

□

Proposición 1.1.6. *Sea $\mathbb{K}$ un cuerpo finito. Entonces el único valor absoluto sobre $\mathbb{K}$ es el trivial.*

Demostración. Sea $\mathbb{K}^*$ el grupo multiplicativo de las unidades de $\mathbb{K}$, entonces todos sus elementos tienen orden finito y supongamos que existe $x \in \mathbb{K}^*$ con $|x| = M \notin \{0, 1\}$. Entonces existe $n \in \mathbb{N}$ tal que $x = x^n$ lo que implica que $M = |x| = |x^n| = |x|^n = M^n$ y, como $M \in \mathbb{R}_+$, entonces $M = M^n \Rightarrow M(M^{n-1} - 1) = 0$, lo cual implica necesariamente que $M \in \{0, 1\}$ y llegamos a un absurdo. □

A continuación vamos a definir un caso particular de valor absoluto sobre $\mathbb{Q}$ que nos será de gran interés a lo largo del texto y que dará pie a definir los números que dan nombre a este trabajo. Para ello requerimos de algunas definiciones y resultados previos.

Lema 1.1.7. *Sea $p \in \mathbb{Z}$ un primo cualquiera. Entonces cualquier entero $n \in \mathbb{Z}$ puede ser escrito de forma única como $n = p^v n'$ con $p \nmid n'$.*

Demostración. Basta con recordar que el anillo de los números enteros $(\mathbb{Z}, +, \cdot)$ es *DFU*. □

Definición 1.1.8. *Sea $p \in \mathbb{Z}$ un número primo. Se define la* valoración p-ádica *en $\mathbb{Z}$ como la función*

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

que a cada entero $n \in \mathbb{Z} \setminus \{0\}$ le asigna el valor $v_p(n)$, siendo este el único entero positivo tal que

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

Esta función está bien definida según el lema previo. Ahora cabe preguntarse, ¿podemos "extender" esta función a los racionales? La respuesta es sí, y lo haremos de la siguiente manera:
Sea $x = a/b \in \mathbb{Q} \setminus \{0\}$ entonces definimos $v_p(x)$ como

$$v_p(x) = v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b).$$

Antes de continuar debemos comprobar que esta función está bien definida en $\mathbb{Q} \setminus \{0\}$. Notemos primero que, para cada par de enteros $h, t \in \mathbb{Z}$, si escribimos

$$h = p^{r_h} n, \;\; t = p^{r_t} m \quad \text{con} \;\; p \nmid nm$$

entonces $ht = p^{r_h + r_t} nm$ y de aquí se extrae que $v_p(ht) = v_p(h) + v_p(t)$.

Lema 1.1.9. *Para cualquier $x \in \mathbb{Q} \setminus \{0\}$ el valor $v_p(x)$ no depende de la representación de x como cociente de dos enteros.*

Demostración. Fijado un $x \in \mathbb{Q} \setminus \{0\}$, supongamos que tenemos dos representaciones distintas de x como cociente de dos enteros

$$x = \frac{a}{b} = \frac{c}{d}.$$

Entonces,

$$ad = bc \Rightarrow v_p(ad) = v_p(bc) \Rightarrow v_p(a) + v_p(d) = v_p(b) + v_p(c) \Rightarrow v_p(a) - v_p(b) = v_p(c) - v_p(d),$$

que es lo que se quería demostrar. □

Propiedades 1.1.10. *Para cada $x, y \in \mathbb{Q} \setminus \{0\}$ se cumple:*

1) $x = p^{v_p(x)}\frac{a}{b}$ *con* $p \nmid ab$ *y, si* $x = p^k\frac{a}{b}$ *con* $p \nmid ab$, *necesariamente* $k = v_p(x)$.

2) $v_p(xy) = v_p(x) + v_p(y)$.

3) $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$.

Demostración.

1) Sea $x = \dfrac{n}{m} = \dfrac{p^{v_p(n)}a}{p^{v_p(m)}b} = p^{v_p(n)-v_p(m)}\dfrac{a}{b} = p^{v_p(x)}\dfrac{a}{b}$ con $p \nmid a$ y $p \nmid b$, luego $p \nmid ab$. Ahora supongamos que podemos escribir x como

$$x = p^k\frac{a}{b} \quad \text{con} \quad p \nmid ab$$

y supongamos que $k > v_p(x)$ (el caso contrario es análogo). Entonces

$$p^k\frac{a}{b} = p^{v_p(x)}\frac{c}{d} \quad \text{con} \quad p \nmid abcd$$

igualando las dos expresiones de x que conocemos

$$x = p^k\frac{a}{b} = p^{v_p(x)}\frac{c}{d} \Longrightarrow \frac{c}{d} = \frac{p^{k-v_p(x)}a}{b} \Longrightarrow p \mid cb$$

y llegamos a una contradicción.

2) Empleando el apartado anterior, si $x = p^{v_p(x)}\dfrac{a}{b}$, $y = p^{v_p(y)}\dfrac{c}{d}$, entonces

$$xy = p^{v_p(x)+v_p(y)}\frac{ac}{bd}$$

y claramente $p \nmid abcd$ pues $p \nmid ab$ y $p \nmid cd$.

3) Supongamos que $v_p(x) = min\{v_p(x), v_p(y)\}$ (en caso contrario se razonaría igual). Entonces $v_p(y) - v_p(x) \geq 0$ y

$$x + y = p^{v_p(x)}\frac{a}{b} + p^{v_p(y)}\frac{c}{d} = p^{v_p(x)}\frac{ad + p^{v_p(y)-v_p(x)}bc}{bd}$$

con $p \nmid abcd$.
Si $v_p(y) - v_p(x) > 0$ entonces $p \nmid (ad + p^{v_p(y)-v_p(x)}bc)$ y $p \nmid bd$. En virtud del primer apartado, $v_p(x + y) = \text{mín}\{v_p(x), v_p(y)\}$.
En el caso de que $v_p(y) - v_p(x) = 0$, entonces podría darse que $p \mid (ad + p^{v_p(y)-v_p(x)}bc)$ y entonces

$$p^{v_p(x)}\frac{ad + p^{v_p(y)-v_p(x)}bc}{bd} = p^{v_p(x)+n}\frac{t}{bd} \quad \text{con} \quad n \geq 1\ , \quad p \nmid tbd$$

y, por el primer apartado, $v_p(x + y) = v_p(x) + n > \text{mín}\{v_p(x), v_p(y)\}$.
Si $v_p(y) - v_p(x) = 0$ pero $p \nmid (ad + p^{v_p(y)-v_p(x)}bc)$ entonces se volvería a dar la igualdad.
Se concluye, por tanto, que $v_p(x + y) \geq \text{mín}\{v_p(x), v_p(y)\}$.

□

La función v_p, que acabamos de definir sobre el cuerpo $\mathbb{Q}$ para cada número primo p, no es un valor absoluto ya que puede tomar valores negativos ($v_2(1/2) = -1$). Sin embargo, podemos definir un valor absoluto a partir de ella, transformando las buenas propiedades vistas en el lema anterior en aquellas dadas en la Definición 1.1.1.

Definición 1.1.11. *Se define el* valor absoluto p-ádico *sobre* $\mathbb{Q}$ *como la función* $|\cdot|_p : \mathbb{Q} \longrightarrow \mathbb{R}_+$ *dada por*

$$|x|_p = \begin{cases} p^{-v_p(x)} & \text{si } x \in \mathbb{Q} \setminus \{0\}, \\ 0 & \text{si } x = 0. \end{cases}$$

Proposición 1.1.12. *Para cada $p \in \mathbb{Z}$ primo, la función $|\cdot|_p$ definida anteriormente es un valor absoluto no arquimediano sobre $\mathbb{Q}$.*

Demostración. Son resultado inmediato de las Propiedades 1.1.10:

1) $|0|_p = 0$ por definición y, si $|x|_p = p^{-v_p(x)} = 0$, como $p^\alpha \neq 0$ para todo $\alpha \in \mathbb{R}$ necesariamente debe ser $x = 0$.

2) Sean $x, y \in \mathbb{Q} \setminus \{0\} \Rightarrow |xy|_p = p^{-v_p(xy)} = p^{-v_p(x)-v_p(y)} = p^{-v_p(x)}p^{-v_p(y)} = |x|_p|y|_p$.
Sean ahora $x, y \in \mathbb{Q}$ y supongamos que $x = 0$ (el caso $y = 0$ es similar) $\Rightarrow |xy|_p = |0 \cdot y|_p = |0|_p = 0 = |0|_p|y|_p$.

3) Supongamos que $v_p(y) \geq v_p(x)$ (en caso contrario se razonaría de la misma manera). Por la Propiedad 1.1.10.3 se tiene que

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

Además hemos probado que $|\cdot|_p$ es un *valor absoluto no arquimediano* sobre $\mathbb{Q}$.

□

Ejemplo 1.1.13.

a) $\mathbb{K} = \mathbb{Q}$, $p = 7$,

$$\left|\frac{2058}{15330}\right|_7 = 7^{-v_7\left(\frac{2058}{15330}\right)} = 7^{v_7(15330)-v_7(2058)} = 7^{1-3} = \frac{1}{49},$$

ya que $2058 = 7^3 \cdot 3 \cdot 2$ *y* $15330 = 73 \cdot 7 \cdot 5 \cdot 3 \cdot 2$.

b) Sea A un dominio de integridad y $\mathbb{K}$ su cuerpo de fracciones. Sea $v : A - \{0\} \longrightarrow \mathbb{R}$ una función que satisface las Propiedades 1.1.10.2 y 1.1.10.3 Si extendemos v a $\mathbb{K}$ de la forma $v(a/b) = v(a) - v(b)$, entonces se puede probar que la función

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

definida por $|x|_v = \mathrm{e}^{-v(x)}$ si $x \neq 0$ y $|0|_v = 0$, es un valor absoluto no arquimediano sobre $\mathbb{K}$. En efecto, veamos que se cumplen las cuatro propiedades:

i) $|0|_v = 0$ *por definición.*

ii) $|xy|_v = \mathrm{e}^{-v(xy)} = \mathrm{e}^{-v(x)-v(y)} = \mathrm{e}^{-v(x)}\mathrm{e}^{-v(y)} = |x|_v|y|_v$.

iii) Supongamos que $v(y) \geq v(x)$, por la Propiedad 1.1.10.3 *se tiene que*

$$|x+y|_v = \mathrm{e}^{-v(x+y)} \leq \mathrm{e}^{v(x)} = \max\{|x|_v, |y|_v\} \leq |x|_v + |y|_v.$$

iv) Implícita en el apartado anterior.

Observación 1.1.14. *Realmente, cualquier número $c > 1$ puede servir como base para un valor absoluto no arquimediano. En el caso de que el cuerpo $\mathbb{K}$ sea finito, una buena elección para esta base sería la característica del cuerpo.*

1.2. Propiedades básicas del valor absoluto sobre un cuerpo

En esta sección vamos a presentar algunas propiedades fundamentales de un valor absoluto no trivial sobre un cuerpo arbitrario $\mathbb{K}$. También daremos una caracterización de los valores absolutos no arquimedianos.

Propiedades 1.2.1. *Sea $\mathbb{K}$ un cuerpo y $|\cdot|$ un valor absoluto no trivial definido en él. Entonces:*

1) $|1| = 1$;

2) $|x^{-1}| = \dfrac{1}{|x|}$ *para cada* $x \in \mathbb{K} \setminus \{0\}$;

3) Si $x \in \mathbb{K}$ *y* $|x^n| = 1$ *entonces* $|x| = 1$;

4) $|-1|=1$*;*

5) para cada $x \in \mathbb{K}$, $|-x|=|x|$.

Demostración.

1) $|1| = |1 \cdot 1| = |1| \cdot |1| = |1|^2$. Luego tenemos un número real positivo $a = |1|$ que satisface la ecuación $a = a^2 \Rightarrow a = 1$.

2) Sea $x \in \mathbb{K} \setminus \{0\}$, $|x^{-1}x| = |1| = 1 \Rightarrow |x^{-1}| \cdot |x| = 1 \Rightarrow |x^{-1}| = \dfrac{1}{|x|}$.

3) Sea $x \in \mathbb{K}$ cualquiera, si $|x^n| = |x|^n = 1$ entonces, como $|x|$ es un número positivo, debe ser $|x| = \sqrt[n]{|x|^n} = \left|\sqrt[n]{1}\right|_\infty = 1$ donde $|\cdot|_\infty$ denota el valor absoluto usual de $\mathbb{R}$.

4) $|(-1)^2| = |1| = 1 \Rightarrow |-1| = 1$ por el apartado anterior.

5) Sea $x \in \mathbb{K}$ cualquiera, entonces $|-x| = |-1| \cdot |x| = 1 \cdot |x| = |x|$.

□

Definición 1.2.2. *Si tenemos un cuerpo* $\mathbb{K}$*, definimos la* imagen de $\mathbb{Z}$ en $\mathbb{K}$ *como la imagen de* $\mathbb{Z}$ *por el homomorfismo* $\phi : \mathbb{Z} \longrightarrow \mathbb{K}$ *definido por*

$$n \longmapsto \begin{cases} \overbrace{1+1+...+1}^{n \text{ veces}} & \text{si } n > 0, \\ 0 & \text{si } n = 0, \\ -\overbrace{(1+1+...+1)}^{-n \text{ veces}} & \text{si } n < 0. \end{cases}$$

Teorema 1.2.3. *Sea* $A = \phi(\mathbb{Z}) \subseteq \mathbb{K}$ *la imagen de* $\mathbb{Z}$ *en* $\mathbb{K}$*. Un valor absoluto,* $|\cdot|$*, en* $\mathbb{K}$ *es no arquimediano si, y solo si,* $|a| \leq 1$ *para todo* $a \in A$*.*

Demostración.

$\boxed{\Rightarrow}$ Supongamos que $|\cdot|$ es no arquimediano. Sea $a = \overbrace{(1+1+...+1)}^{n \text{ veces}} \in A$, realizando una inducción sobre $n \in \mathbb{N}$ tenemos que:

1) Para $n = 1$, entonces $a = 1$ y, por tanto, $|a| = |1| = 1$.

2) Supongamos que se cumple para n, es decir, que para $a = \overbrace{1+1+...+1}^{n \text{ veces}}$, se tiene que $|a| \leq 1$. Para $a = \overbrace{(1+1+...+1)}^{n+1 \text{ veces}}$ se tiene que, por ser $|\cdot|$ *no arquimediano*

$$|a| = |\overbrace{(1+1+...+1)}^{n \text{ veces}} + 1| \leq \text{máx}\{|\overbrace{(1+1+...+1)}^{n \text{ veces}}|, |1|\} = 1.$$

Para el caso de $a = -\overbrace{(1+1+...+1)}^{n \text{ veces}}$ se procedería igual manera por inducción sobre n y teniendo en cuenta que $|-1| = 1$ y que $|a-1| \leq \text{máx}\{|a|, |-1|\} = \text{máx}\{|a|, 1\} = 1$. Se concluye, por tanto, que $|a| \leq 1$ para todo $a \in A$.

$\boxed{\Leftarrow}$ Supongamos ahora que $|a| \leq 1$ para todo $a \in A$. Sean $x, y \in \mathbb{K}$ y $m \in \mathbb{N}$. Por el Binomio de Newton,

$$(x+y)^m = \sum_{j=0}^{m} \binom{m}{j} x^j y^{m-j}$$

donde $x^0 = y^0 = 1$.
Como $\binom{m}{j} \in A$, usando la hipótesis tenemos que

$$\left| \binom{m}{j} \right| \leq 1.$$

Por tanto,

$$|x+y|^m = |(x+y)^m| = \left| \sum_{j=0}^{m} \binom{m}{j} x^j y^{m-j} \right| \leq \sum_{j=0}^{m} |x|^j |y|^{m-j} \leq (m+1) \left(\text{máx} \{|x|, |y|\} \right)^m .$$

Tomando la raíz k-ésima,

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

Finalmente, tomando límites cuando $m \longrightarrow \infty$ concluimos que:

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

Esto último implica que $|\cdot|$ es *no arquimediano.* □

Corolario 1.2.4. *Un valor absoluto,* $|\cdot|$*, sobre* $\mathbb{Q}$ *es no arquimediano si, y solo si,*

$$\sup\{|n| : n \in \mathbb{Z}\} = 1.$$

Demostración.
$\boxed{\Rightarrow}$ Supongamos que es no arquimediano. Entonces por el teorema anterior,

$$|n| \leq 1 \quad \text{para todo} \ \ n \in \mathbb{Z}.$$

Luego, $\sup\{|n| : n \in \mathbb{Z}\} \leq 1$ y, como $1 \in \mathbb{Z}$, se tiene que $\sup\{|n| : n \in \mathbb{Z}\} = 1$.
$\boxed{\Leftarrow}$ Supongamos ahora que $\sup\{|n| : n \in \mathbb{Z}\} = 1$. Entonces $|n| \leq 1$ para todo $n \in \mathbb{Z}$ y, por el teorema anterior, el valor absoluto es no arquimediano. □

1.3. Topología

En $\mathbb{R}$ se definía la topología usual como aquella que tenía como base de abiertos a la clase formada por todos los intervalos abiertos. Por otro lado, haciendo uso del valor absoluto usual en $\mathbb{R}$, se definía la topología métrica como aquella cuya base de abiertos viene dada por las bolas abiertas de radio positivo y centradas en cualquier punto y es ya conocido que ambas topologías coinciden. Hemos visto que en un cuerpo se puede definir un valor absoluto. A continuación veremos que a partir de un valor absoluto podemos siempre medir distancias y esto nos permitirá definir una topología métrica sobre $\mathbb{K}$.

Tanto en esta sección como más adelante aparecerán conceptos topológicos como espacio conexo, compacto, localmente compacto... Por lo general no daremos su definición y utilizaremos, sin demostrarlos, los resultados más básicos de Topología General, que supondremos conocidos, aunque sí recordaremos algunos otros conceptos cuando se requiera.

Definición 1.3.1. *Una* distancia *en un conjunto X es una función*

$$d : X \times X \longrightarrow \mathbb{R}$$

que satisface las siguientes propiedades:

1) $d(x, y) \geq 0$ *para todos* $x, y \in X$*; la igualdad se da si, y solo si,* $x = y$*;*

2) $d(x, y) = d(y, x)$ *para todos* $x, y \in X$*;*

3) $d(x, z) \leq d(x, y) + d(y, z)$ *para todos* $x, y, z \in X$ *(Desigualdad triangular).*

Al par (X, d) *se le conoce como* espacio métrico*.*

Definición 1.3.2. *Sea* $\mathbb{K}$ *un cuerpo y* $|\cdot|$ *un valor absoluto definido en él. Dados dos elementos* $x, y \in \mathbb{K}$*, se define la* distancia entre x e y*, como*

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

Lema 1.3.3. *La función* $d : \mathbb{K} \times \mathbb{K} \longrightarrow \mathbb{R}$ *de la Definición 1.3.2 es una distancia en* $\mathbb{K}$*.*

Demostración. Debemos ver que $d(x, y) = |x - y|$ satisface las tres propiedades de la definición de distancia sobre un conjunto.

1) Sean $x, y \in \mathbb{K}$, entonces $|x - y| \geq 0$ por definición. Además,

$$|x - y| = 0 \Longleftrightarrow x - y = 0 \Longleftrightarrow x = y.$$

2) Sean $x, y \in \mathbb{K}$, entonces $d(x, y) = |x - y| = |-1||x - y| = |y - x| = d(y, x)$.

3) Sean $x, y, z \in \mathbb{K}$, entonces $|x - z| = |x - z - y + y| \leq |x - y| + |y - z|$.

□

Lema 1.3.4. *Sea* $|\cdot|$ *un valor absoluto sobre un cuerpo* $\mathbb{K}$ *y* d *la distancia asociada a este valor absoluto. Entonces* $|\cdot|$ *es no arquimediano si, y sólo si, para cualesquiera* $x, y, z \in \mathbb{K}$ *se cumple:*

$$d(x, y) \leq \text{máx}\{d(x, z), d(y, z)\} \quad \textit{(Desigualdad ultramétrica).}$$

Demostración.
$\boxed{\Rightarrow}$ Supongamos que $|\cdot|$ es *no arquimediano* y sean $x, y, z \in \mathbb{K}$ cualesquiera. Entonces, por ser no arquimediano,

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

$\boxed{\Leftarrow}$ Supongamos ahora que se da la desigualdad del enunciado para cualquier $x, y, z \in \mathbb{K}$. Sean ahora $x, y \in \mathbb{K}$, si tomamos $z = 0$ entonces

$$\begin{aligned} |x + y| = |x - (-y)| = d(x, -y) \leq \text{máx}\{d(x, 0), d(-y, 0)\} = \\ = \text{máx}\{|x|, |-y|\} = \text{máx}\{|x|, |y|\}. \end{aligned}$$

□

Un conjunto con una distancia definida que satisface la *desigualdad ultramétrica* se dice que es un *espacio ultramétrico*. Por el lema anterior podemos ver que todo cuerpo con un valor absoluto no arquimediano definido en él es, considerando la distancia asociada a este valor absoluto, un espacio ultramétrico.

Proposición 1.3.5. *Sea $\mathbb{K}$ un cuerpo y $|\cdot|$ un valor absoluto no arquimediano definido en él. Si $x, y \in \mathbb{K}$ son tales que $|x| \neq |y|$, entonces*

$$|x + y| = \text{máx}\{|x|, |y|\}.$$

Demostración. Tomamos $x, y \in \mathbb{K}$ tales que $|x| \neq |y|$. Podemos suponer que $|y| < |x|$ (en el caso contrario se razonaría de igual manera). Como el *valor absoluto* es *no arquimediano*, tenemos que

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

Para obtener la desigualad contraria, notemos que, como $|y| < |x|$,

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

ya que de ser $\text{máx}\{|x + y|, |y|\} = |y|$ entonces $|x| \leq |y|$ lo cual no puede ser. □

Corolario 1.3.6. *Sea $\mathbb{K}$ un cuerpo y $|\cdot|$ un valor absoluto no arquimediano definido en él. Entonces dados $x, y, z \in \mathbb{K}$ cualesquiera,*

$$\#\{|x - y|, |x - z|, |y - z|\} \leq 2.$$

Demostración. Tomemos $x, y, z \in \mathbb{K}$ cualesquiera. Si $|x - y| = |y - z|$ entonces ya estaría. De lo contrario, si $|x - y| \neq |y - z|$, por el resultado anterior,

$$|x - z| = |(x - y) + (y - z)| = \text{máx}\{|x - y|, |y - z|\}.$$

□

A través de este pequeño corolario podemos deducir que, dados tres puntos cualesquiera, el triángulo que forman es isósceles. Esto tendrá gran importancia a la hora de trabajar con la topología de un cuerpo cuando el valor absoluto sea no arquimediano.

Al igual que se hace para la topología métrica de $\mathbb{R}$, cuyos abiertos son los formados por uniones de bolas abiertas, para la topología de nuestro cuerpo definiremos dichas bolas, empleando para ello la distancia que, ya sabemos, podemos establecer una vez contamos con un valor absoluto definido.

Definición 1.3.7. *Sea $\mathbb{K}$ un cuerpo y $|\cdot|$ un valor absoluto definido en él. Dados $a \in \mathbb{K}$ y $r \geq 0$, se define la* bola abierta *de centro a y radio r como*

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

y la bola cerrada *de centro a y radio r como*

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

Se define la topología sobre $\mathbb{K}$ asociada a $|\cdot|$ *como la topología métrica para la distancia asociada a $|\cdot|$, es decir, aquella cuyos abiertos son las uniones, numerables o no, de bolas abiertas.*

Recordemos que una aplicación entre dos espacios topológicos se dice que es continua si la imagen inversa de cualquier abierto del espacio de llegada es siempre un abierto del dominio. Esto se puede expresar más fácilmente para el caso de espacios métricos en términos de $\epsilon - \delta$.

Proposición 1.3.8. *Sea $\mathbb{K}$ un cuerpo y $|\cdot|$ un valor absoluto definido en él, entonces este último define una aplicación continua para la topología sobre $\mathbb{K}$ asociada a $|\cdot|$ y la topología usual en $\mathbb{R}_+$.*

Demostración. Sabemos que la aplicación $d : \mathbb{K} \times \mathbb{K} \longrightarrow \mathbb{R}_+$ es continua para la topología métrica inducida por ella misma, por tanto, $|\cdot| = d_{|\mathbb{K}\times\{0\}}$ también lo es. □

Proposición 1.3.9. *Sea $\mathbb{K}$ un cuerpo y $|\cdot|$ un valor absoluto no arquimediano definido en él. Las aplicaciones*

1) $F : \mathbb{K} \times \mathbb{K} \longrightarrow \mathbb{K}$ dada por $F(x, y) = x + y$ para cada $x, y \in \mathbb{K}$,

2) $G : \mathbb{K} \times \mathbb{K} \longrightarrow \mathbb{K}$ dada por $G(x, y) = xy$ para cada $x, y \in \mathbb{K}$,

son continuas para la topología métrica en $\mathbb{K}$.

Demostración. Fijamos un $\epsilon > 0$:

1) Sea $(x_0, y_0) \in \mathbb{K} \times \mathbb{K}$ cualquiera. Tomando $\delta = \epsilon/2$, si $(x, y) \in \mathbb{K} \times \mathbb{K}$ son tales que $|x_0 - x| < \delta$, $|y_0 - y| < \delta$, entonces

$$|F(x_0, y_0) - F(x, y)| = |x_0 + y_0 - x - y| \leq |x_0 - x| + |y_0 - y| < 2\delta = \epsilon,$$

por lo que la aplicación F es continua.

2) De nuevo, sea $(x_0, y_0) \in \mathbb{K} \times \mathbb{K}$ cualquiera. Entonces tomamos $M_1, M_2 \in \mathbb{R}_+$ tales que $|x_0| < M_1$ e $|y_0| < M_2$. Tomando ahora

$$\delta = \frac{\sqrt{(M_1 + M_2)^2 + 4\epsilon} - (M_1 + M_2)}{2}$$

tendríamos que, para cada $(x, y) \in \mathbb{K} \times \mathbb{K}$ con $|x_0 - x| < \delta$ e $|y_0 - y| < \delta$ se tendría que

$$\begin{aligned} |G(x_0, y_0) - G(x, y)| = |x_0 y_0 - xy| = |x_0 y_0 - xy_0 + xy_0 - xy| \leq \\ \leq |x| \cdot |y_0 - y| + |y_0| \cdot |x_0 - x| < \delta^2 + (M_1 + M_2)\delta = \epsilon, \end{aligned}$$

y concluimos que la aplicación G también es continua.

□

A continuación veremos como resultado una serie de curiosas propiedades relativas a estas bolas cuando el valor absoluto definido en $\mathbb{K}$ es no arquimediano.

Proposición 1.3.10. *Sea $\mathbb{K}$ un cuerpo y $|\cdot|$ un valor absoluto no arquimediano definido en él. Entonces:*

1) Todo punto que pertenece a una bola abierta es centro de la misma.

2) Todo punto que pertenece a una bola cerrada es centro de la misma.

3) Para cualquier $a \in \mathbb{K}$ y para todo $r > 0$, $B(a,r)$ es cerrado y abierto.

4) Para cualquier $a \in \mathbb{K}$ y para todo $r > 0$, $\bar{B}(a,r)$ es cerrado y abierto.

5) Dos bolas abiertas o bien son disjuntas o bien una está contenida en la otra.

6) Dos bolas cerradas de radio positivo o bien son disjuntas o bien una está contenida en la otra.

Demostración.

1) Sea $b \in B(a,r)$ y $x \in B(b,r)$. Entonces

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

Por tanto $B(b,r) \subseteq B(a,r)$. La contención $B(a,r) \subseteq B(b,r)$ se prueba análogamente y se concluye que $B(a,r) = B(b,r)$.

2) Se prueba de la misma manera que el apartado anterior, sustituyendo las desigualdades estrictas por no estrictas.

3) Si consideramos $B(a,r)$, entonces es abierta por definición. Por otro lado, si tomamos $y \in \mathbb{K} \setminus B(a,r)$ entonces para cualquier $x \in B(y,r)$, si fuese $x \in B(a,r)$ entonces

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

y se llega al absurdo. Por tanto $B(y,r) \subseteq \mathbb{K} \setminus B(a,r)$, lo que implica que este último es abierto y su complementario cerrado.

4) Sea $\bar{B}(a,r)$, entonces es claro que para cualquier $b \in \bar{B}(a,r)$ se cumple, por lo visto en el segundo apartado, que $B(b,r) \subseteq \bar{B}(b,r) = \bar{B}(a,r)$. Luego, es abierto. Por otro lado, si tomamos $y \in \mathbb{K} \setminus \bar{B}(a,r)$ entonces para cualquier $x \in B(y,r)$, si fuese $x \in \bar{B}(a,r)$ entonces

$$|y-a| = |y-a+x-x| \leq \text{máx}\{|x-y|, |x-a|\} \leq r$$

y se llega al absurdo. Por tanto $B(y,r) \subseteq \mathbb{K} \setminus \bar{B}(a,r)$, por lo que este último es abierto y su complementario cerrado.

5) Supongamos que $B(a,r) \cap B(b,s) \neq \emptyset$. Sea $x \in B(a,r) \cap B(b,s)$, entonces $B(a,r) = B(x,r)$ y $B(b,s) = B(x,s)$. Luego $B(a,r) \subseteq B(b,s)$ o $B(b,s) \subseteq B(a,r)$ según sea $r \leq s$ o $s \leq r$.

6) Es análoga a la demostración del apartado previo.

□

Ejemplo 1.3.11. *Veamos que, si consideramos el cuerpo $\mathbb{Q}$ con el valor absoluto p-ádico, $|\cdot|_p$, entonces*

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

Primero, si tomamos $n, m \in \mathbb{N}$ con $0 \leq n < m \leq p-1$, si fuese $B(n,1) \cap B(m,1) \neq \emptyset$, entonces $B(n,1) = B(m,1)$, luego $n \in B(m,1)$ y $|m-n|_p < 1$. Pero $0 < m-n < p$ lo que implica que $v_p(m-n) = 0$ y $|m-n|_p = 1$ y llegamos a una contradicción. Por tanto podemos afirmar que las p bolas serán disjuntas.
Para probar la igualdad lo haremos probando ambas contenciones:
Sea $x \in \bar{B}(0,1)$, es decir, $x = \frac{a}{b}$ con $p \nmid b$. Si probamos que

$$\{a+(p), (a-b)+(p), (a-2b)+(p), ..., (a-(p-1)b)+(p)\} \subseteq \mathbb{Z}_p$$

son p elementos distintos en $\mathbb{Z}_p$, entonces alguno de ellos debe ser divisible por p. Supongamos que

$$(a-tb)+(p) = (a-nb)+(p) \ \ con \ \ 0 \leq n < t \leq p-1 \iff$$
$$\iff (a-nb)-(a-tb) \in (p) \iff p \mid (t-n)b \iff p \mid (t-n).$$

Pero $0 < t-n \leq p-1$ y llegamos a una contradicción. Podemos afirmar entonces que todos los elementos son distintos y, por tanto, uno de ellos, pongamos $a-mb$, debe ser divisible por p. Esto implica lo siguiente:

$$|x-m|_p = \left|\frac{a-mb}{b}\right|_p = p^{-v_p(a-mb)} < 1 \quad pues \ \ v_p(a-mb) > 0.$$

Recíprocamente, si tomamos $x = a/b \in B(0,1) \sqcup B(1,1) \sqcup ... \sqcup B(p-1,1)$:

- *Si $x \in B(0,1) \subseteq \bar{B}(0,1)$ y ya estaría.*
- *Si $x \in B(j,1)$ para algún $j = 1, ..., p-1$, veamos que $|x|_p = 1$ o lo que es lo mismo, $v_p(x) = 0$. Primeramente tendríamos que*

$$|x-j|_p = \left|\frac{a}{b} - j\right|_p = \left|\frac{a-jb}{b}\right|_p = p^{v_p(b)-v_p(a-jb)} < 1.$$

Esto implica que $a-jb$ es divisible por una potencia de p estrictamente mayor que aquella por la que podemos dividir a b. Escribamos
$a-jb = p^m t$ y $b = p^r h$, entonces

$$\frac{a-jb}{b} = \frac{p^m t}{p^r h} \quad con \ \ m > r, \ p \nmid th.$$

Despejando $x = a/b$ tendríamos que

$$x = \frac{a}{b} = \frac{p^m t + jb}{p^r h} = \frac{p^r(p^{m-r}t + jh)}{p^r h} = \frac{(p^{m-r}t + jh)}{h}.$$

Si p dividiese a $(p^{m-r}t + jh)$ entonces necesariamente $p \mid jh$ pero esto no puede ser ya que $p \nmid j$ y $p \nmid h$, luego $p \nmid (p^{m-r}t + jh)h$ lo que implica, por la Propiedad 1.1.10.1, que $v_p(x) = 0$, luego $x \in \bar{B}(0,1)$.

Recordamos que, dado un punto $x \in \mathbb{K}$, se definía su componente conexa como la unión de todos los subconjuntos conexos que contienen a x, que, por ser la unión de conjuntos conexos y no disjuntos, es conexa.

El siguiente resultado nos proporciona una particularidad más de la topología generada por un valor absoluto no arquimediano.

Proposición 1.3.12. *Sea $\mathbb{K}$ un cuerpo y $|\cdot|_p$ un valor absoluto no arquimediano definido en él. Entonces el espacio $\mathbb{K}$ es totalmente disconexo.*

Demostración. Vamos a probar primero que todo subconjunto con dos elementos distintos no puede ser conexo.
Sea $S \in \mathbb{K}$ un subconjunto con $x, y \in S$ y $x \neq y$. Tomamos $r \in \mathbb{R}$ con $0 < r < |x - y|$. Entonces $y \notin B(x, r)$. Como esta bola es también cerrada, $\mathbb{K} \setminus B(x, r)$ es abierto.

$$x \in A = S \cap B(x, r) \subseteq B(x, r), \quad y \in B = S \cap (\mathbb{K} \setminus B(x, r)) \subseteq \mathbb{K} \setminus B(x, r).$$

Como $S = A \sqcup B$ y ambos son abiertos para la topología del subespacio en S, se concluye que S no es conexo. Esto, junto con el hecho de que todo conjunto unipuntual es conexo, nos asegura que el espacio $\mathbb{K}$ es totalmente disconexo. □

1.4. Álgebra

En esta sección ahondaremos en las estructuras algebraicas que podemos definir a partir de un cuerpo con un valor absoluto no arquimediano.

También haremos una breve introducción a los anillos de valoración que nos será de gran utilidad más adelante, cuando estemos explorando las propiedades del cuerpo de los números p-ádicos.

Proposición 1.4.1. *Sea $\mathbb{K}$ un cuerpo y $|\cdot|$ un valor absoluto no arquimediano definido en él. Entonces la bola cerrada*

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

es un subanillo del cuerpo $\mathbb{K}$.

Demostración. Sean $x, y \in \bar{B}(0, 1)$, entonces $y \in \bar{B}(x, 1)$ lo que implica que $x - y \in \bar{B}(0, 1)$ pues $\bar{B}(0, 1) = \bar{B}(x, 1)$. Por otro lado, como

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

podemos concluir que $\mathcal{O}$ es un subanillo de $\mathcal{K}$.

□

Proposición 1.4.2. *Sea $\mathbb{K}$ un cuerpo y $|\cdot|$ un valor absoluto no arquimediano definido en él. Entonces la bola abierta*

$$\mathcal{B} = B(0, 1)$$

es un ideal del anillo $\mathcal{O}$ y todo elemento del conjunto $\mathcal{O} \setminus \mathcal{B}$ es invertible en $\mathcal{O}$.

Demostración. Veamos primero que es, efectivamente, un ideal.
Sean $x, y \in B(0,1)$ entonces:

i) $x \in B(0,1) = B(y,1) \Longrightarrow |x-y| < 1 \Longrightarrow x - y \in B(0,1)$.

ii) Sea $r \in \mathcal{O} = \bar{B}(0,1) \Longrightarrow |rx| = |r| \cdot |x| \leq |x| < 1 \Longrightarrow rx \in B(0,1)$.

Veamos ahora que $\mathcal{O}^* = \{x \in \mathbb{K} : |x| = 1\}$.
Si $x \in \mathcal{O}^*$, entonces $x, x^{-1} \in \mathcal{O}$, es decir, $|x| \leq 1$ y $|x^{-1}| \leq 1$ y, como se cumple que

$$|x \cdot x^{-1}| = |x| \cdot |x^{-1}| = 1,$$

necesariamente $|x| = 1$.
Para la contención contraria, tomamos un $x \in \mathbb{K}$ tal que $|x| = 1$. Si fuese $x^{-1} \in \mathcal{O}$, se tendría que $|x^{-1}| > 1$ y entonces

$$1 = |x \cdot x^{-1}| = |x| \cdot |x^{-1}| = |x^{-1}| > 1,$$

lo cual es imposible. □

Observación 1.4.3. *El último aserto del enunciado previo implica que, en los anteriores términos, el ideal $\mathcal{B}$ es maximal para el anillo $\mathcal{O}$. En consecuencia, el anillo cociente $\mathcal{O}/\mathcal{B}$ es un cuerpo al que daremos nombre. De hecho, como veremos más adelante cuando hablemos de valoraciones sobre un cuerpo, $\mathcal{B}$ es el único ideal maximal del anillo $\mathcal{O}$.*

Definición 1.4.4. *Sea $\mathbb{K}$ un cuerpo y $|\cdot|$ un valor absoluto no arquimediano sobre él. El subanillo*

$$\mathcal{O} = \bar{B}(0,1) \subset \mathbb{K}$$

recibe el nombre de anillo de valoración de $|\cdot|$. *El ideal*

$$\mathcal{B} = B(0,1) \subset \mathcal{O}$$

recibe el nombre ideal de valoración de $|\cdot|$. *Por último, el cuerpo*

$$\mathcal{K} = \mathcal{O}/\mathcal{B}$$

recibe el nombre de cuerpo de residuos de $|\cdot|$.

A continuación vamos a ver qué forma toman estos objetos algebraicos cuando consideramos el caso particular del valor absoluto p-ádico. Recordemos que, dado un número primo p y un entero n, el número, también entero y no negativo, $v_p(n)$, no es más que la potencia a la que aparece elevado p en la descomposición en primos de n. Con esto en mente, pasamos al siguiente resultado:

Proposición 1.4.5. *Sea $\mathbb{K} = \mathbb{Q}$ con el valor absoluto p-ádico $|\cdot|_p$. Entonces:*

1) El anillo de valoración de $|\cdot|_p$ es $\mathcal{O} = \mathbb{Z}_{(p)} = \left\{\frac{a}{b} \in \mathbb{Q} : v_p(a) - v_p(b) \geq 0\right\}$.

2) El ideal de valoración de $|\cdot|_p$ es $\mathcal{B} = p\mathbb{Z}_{(p)} = \left\{\frac{a}{b} \in \mathbb{Q} : v_p(a) - v_p(b) > 0\right\}$.

3) cuerpo de residuos de $|\cdot|_p$ *es* $\mathcal{K} = \mathbb{Z}/p\mathbb{Z}$.

Demostración.

1) Por definición,

$$\mathcal{O} = \bar{B}(0,1) = \left\{\frac{a}{b} \in \mathbb{Q} : \left|\frac{a}{b}\right|_p \leq 1\right\} = \left\{\frac{a}{b} \in \mathbb{Q} : p^{v_p(b)-v_p(a)} \leq 1\right\} = \\ = \left\{\frac{a}{b} \in \mathbb{Q} : v_p(b) \leq v_p(a)\right\}.$$

A partir de esta redefinición del *anillo de valoración de* $|\cdot|_p$ es sencillo probar que $\mathcal{O} = \mathbb{Z}_{(p)}$.

2) Aplicando los mismos argumentos que antes,

$$\mathcal{B} = B(0,1) = \left\{\frac{a}{b} \in \mathbb{Q} : \left|\frac{a}{b}\right|_p < 1\right\} = \left\{\frac{a}{b} \in \mathbb{Q} : p^{v_p(b)-v_p(a)} < 1\right\} = \\ = \left\{\frac{a}{b} \in \mathbb{Q} : v_p(b) < v_p(a)\right\}.$$

De aquí se obtiene inmediatamente que $\mathcal{B} = p\mathbb{Z}_{(p)}$.

3) Según lo probado en los dos apartados anteriores, queremos demostrar que

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

Para ello nos vamos a valer del homomorfismo inclusión $i : \mathbb{Z} \hookrightarrow \mathbb{Z}_{(p)}$ y de aquel de paso al cociente

$$\pi : \mathbb{Z}_{(p)} \longrightarrow \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)},$$

que sabemos que son inyectivo y sobreyectivo respectivamente.
Definimos ahora el homomorfismo dado por la composición de los dos anteriores, $f = \pi \circ i$. Si vemos que es sobreyectivo y que $\ker(f) = p\mathbb{Z}$, en virtud del Primer Teorema de Isomorfía, concluiríamos que

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

Primero, es claro que $p\mathbb{Z} \subseteq \ker(f)$ ya que $p\mathbb{Z} \subseteq p\mathbb{Z}_{(p)}$. Por otro lado, los únicos enteros que se encuentran en $p\mathbb{Z}_{(p)}$ son los múltiplos de p, por tanto $\ker(f) = p\mathbb{Z}$.
Continuando con la sobreyectividad, sea $a/b + p\mathbb{Z}_{(p)} \in \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}$ cualquiera. Queremos ver que existe $n \in \mathbb{Z}$ tal que

$$\frac{a}{b} - n = \frac{a - nb}{b} \in p\mathbb{Z}_{(p)},$$

es decir, $p \nmid b$ y $p \mid (a - nb)$.
La primera condición se cumple pues $a/b \in \mathbb{Z}_{(p)}$. Para la segunda condición usamos un resultado probado en el Ejemplo 1.3.11 que nos asegura que existe un $n \in \{0, 1, ..., p-1\}$ tal que $p \mid (a - nb)$. Hemos probado entonces que $f = \pi \circ i$ es sobreyectiva y, por tanto,

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

□

Ejemplo 1.4.6. *Vamos a calcular el anillo de valoración, el ideal de valoración y el cuerpo de residuos para $\mathbb{K}(X)$ con el valor absoluto $|\cdot|_\infty$ definido en el Ejemplo 1.1.4.c:*

$$\mathcal{O} = \left\{ \frac{f(X)}{g(X)} \in \mathbb{K}(X) : \left| \frac{f(X)}{g(X)} \right|_\infty \leq 1 \right\} = \left\{ \frac{f(X)}{g(X)} \in \mathbb{K}(X) : \mathrm{e}^{\deg(f(X))-\deg(g(X))} \leq 1 \right\} = \\ = \left\{ \frac{f(X)}{g(X)} \in \mathbb{K}(X) : \deg(f(X)) \leq \deg(g(X)) \right\}.$$

$$\mathcal{B} = \left\{ \frac{f(X)}{g(X)} \in \mathbb{K}(X) : \left| \frac{f(X)}{g(X)} \right|_\infty < 1 \right\} = \left\{ \frac{f(X)}{g(X)} \in \mathbb{K}(X) : \mathrm{e}^{\deg(f(X))-\deg(g(X))} < 1 \right\} = \\ = \left\{ \frac{f(X)}{g(X)} \in \mathbb{K}(X) : \deg(f(X)) < \deg(g(X)) \right\}.$$

Calcular el cuerpo de residuos requiere algo más de trabajo. Vamos a empezar definiendo una aplicación $\varphi : \mathcal{O} \longrightarrow \mathbb{K}$ dada por

$$\varphi\left(\frac{f(X)}{g(X)}\right) = \begin{cases} 0 & si \quad \frac{f(X)}{g(X)} \in \mathcal{B}, \\ \\ \frac{LT(f(X))}{LT(g(X))} & si \quad \frac{f(X)}{g(X)} \notin \mathcal{B}. \end{cases}$$

donde $LT(f(X))$ representa el término líder del polinomio. Veamos que está bien definida, que es sobreyectiva y que se trata, efectivamente, de un homomorfismo:

- *Supongamos que tenemos dos representaciones distintas de la misma fracción:*

$$\frac{f(X)}{g(X)} = \frac{h(X)}{l(X)} \Longleftrightarrow f(X)l(X) = h(X)g(X).$$

Entonces los términos líderes de izquierda y derecha deben coincidir:

$$LT(f(X)l(X)) = LT(h(X)g(X)) \Longleftrightarrow LT(f(X))LT(l(X)) = LT(h(X))LT(g(X)) \\ \Longleftrightarrow \frac{LT(f(X))}{LT(g(X))} = \frac{LT(h(X))}{LT(l(X))}.$$

Por lo que la imagen por φ no depende del representante.

- *Para probar la sobreyectividad, tomamos un elemento cualquiera $a \in \mathbb{K}$. Este elemento puede verse como un cociente de polinomios constantes $a = a/1 \in \mathcal{O}$ que claramente no pertenece a $\mathcal{B}$. Entonces*

$$\varphi\left(\frac{a}{1}\right) = \frac{LT(a)}{LT(1)} = a.$$

Y queda probada la sobreyectividad. Veamos que es homomorfismo de anillos:

- *$\varphi(0) = 0$ ya que $0 \in \mathcal{B}$ por ser este último un ideal.*

- *Sean* $\frac{f(X)}{g(X)}, \frac{h(X)}{l(X)} \in \mathcal{O}$. *Entonces si* $\frac{f(X)}{g(X)} \in \mathcal{B}$ *(respect.* $\frac{h(X)}{l(X)} \in \mathcal{B}$*), se tiene que* $\frac{f(X)}{g(X)}\frac{h(X)}{l(X)} \in \mathcal{B}$ *por ser un ideal. Por tanto,*

$$\varphi\left(\frac{f(X)}{g(X)}\frac{h(X)}{l(X)}\right) = 0 = \varphi\left(\frac{f(X)}{g(X)}\right)\varphi\left(\frac{h(X)}{l(X)}\right).$$

En el caso de que $\frac{f(X)}{g(X)}, \frac{h(X)}{l(X)} \notin \mathcal{B}$*, es decir,* $\deg(f(X)) = \deg(g(X))$ *y* $\deg(h(X)) = \deg(l(X))$*, entonces* $\frac{f(X)}{g(X)}\frac{h(X)}{l(X)} \notin \mathcal{B}$ *ya que* $\deg(f(X)h(X)) = \deg(g(X)l(X))$ *y, además,*

$$\varphi\left(\frac{f(X)}{g(X)}\frac{h(X)}{l(X)}\right) = \frac{LT(f(X)h(X))}{LT(g(X)l(X)))} = \frac{LT(f(X))LT(h(X))}{LT(g(X)LT(l(X)))} = \\ = \varphi\left(\frac{f(X)}{g(X)}\right)\varphi\left(\frac{h(X)}{l(X)}\right).$$

Por tanto, la aplicación se comporta como un homomorfismo para el producto.

- *De nuevo, sean* $\frac{f(X)}{g(X)}, \frac{h(X)}{l(X)} \in \mathcal{O}$*, si* $\frac{f(X)}{g(X)}, \frac{h(X)}{l(X)} \in \mathcal{B}$*, entonces* $\frac{f(X)}{g(X)} + \frac{h(X)}{l(X)} \in \mathcal{B}$ *y se tiene:*

$$\varphi\left(\frac{f(X)}{g(X)} + \frac{h(X)}{l(X)}\right) = 0 = \varphi\left(\frac{f(X)}{g(X)}\right) + \varphi\left(\frac{h(X)}{l(X)}\right).$$

En el caso de que $\frac{f(X)}{g(X)} \in \mathcal{B}$ *pero* $\frac{h(X)}{l(X)} \notin \mathcal{B}$ *(respect.* $\frac{f(X)}{g(X)} \notin \mathcal{B}$ *pero* $\frac{h(X)}{l(X)} \in \mathcal{B}$*), es decir,* $\deg(f(X)) < \deg(g(X))$ *y* $\deg(h(X)) = \deg(l(X))$ *entonces*

$$\deg(f(X)l(X) + g(X)h(X)) = \deg(g(X)h(X)) = \deg(g(X)) + \deg(h(X)) = \\ = \deg(g(X)) + \deg(l(X)) = \deg(g(X)l(X)).$$

Podemos afirmar entonces que $\frac{f(X)}{g(X)} + \frac{h(X)}{l(X)} = \frac{f(X)l(X)+g(X)h(X)}{g(X)l(X)} \in \mathcal{B}$ *y*

$$\varphi\left(\frac{f(X)}{g(X)} + \frac{h(X)}{l(X)}\right) = \varphi\left(\frac{f(X)l(X) + g(X)h(X)}{g(X)l(X)}\right) = \\ = \frac{LT(f(X)l(X) + g(X)h(X))}{LT(g(X)l(X))} = \frac{LT(g(X)h(X))}{LT(g(X)l(X))} = \frac{LT(g(X))LT(h(X))}{LT(g(X))LT(l(X))} = \\ = \frac{LT(h(X))}{LT(l(X))} = 0 + \varphi\left(\frac{h(X)}{l(X)}\right) = \varphi\left(\frac{f(X)}{g(X)}\right) + \varphi\left(\frac{h(X)}{l(X)}\right).$$

Por último, si $\frac{f(X)}{g(X)}$, $\frac{h(X)}{l(X)} \notin \mathcal{B}$*, es decir,* $\deg(f(X)) = \deg(g(X))$ *y* $\deg(h(X)) = \deg(l(X))$*, pueden ocurrir dos cosas:* $\frac{f(X)}{g(X)} + \frac{h(X)}{l(X)} \in \mathcal{B}$ *o* $\frac{f(X)}{g(X)} + \frac{h(X)}{l(X)} \notin \mathcal{B}$*. En el primer caso,*

$$\frac{f(X)}{g(X)} + \frac{h(X)}{l(X)} \in \mathcal{B} \iff LT(f(X)l(X)) + LT(g(X)h(X)) = 0 \iff \\ \iff \frac{LT(f(X))}{LT(g(X))} + \frac{LT(h(x))}{LT(l(X))} = \varphi\left(\frac{f(X)}{g(X)}\right) + \varphi\left(\frac{h(X)}{l(X)}\right) = 0.$$

Por tanto, $\varphi\left(\frac{f(X)}{g(X)}+\frac{h(X)}{l(X)}\right)=0=\varphi\left(\frac{f(X)}{g(X)}\right)+\varphi\left(\frac{h(X)}{l(X)}\right)$. *Si por el contrario* $\frac{f(X)}{g(X)}+\frac{h(X)}{l(X)}\notin\mathcal{B}$, *quiere decir que los términos líderes de los polinomios* $f(X)l(X)$ *y* $g(X)h(X)$ *no se anulan al sumarlos y, por tanto*

$$\varphi\left(\frac{f(X)}{g(X)}+\frac{h(X)}{l(X)}\right)=\varphi\left(\frac{f(X)l(X)+g(X)h(X)}{g(X)l(X)}\right)=$$
$$=\frac{LT(f(X)l(X)+g(X)h(X))}{LT(g(X)l(X)}=\frac{LT(f(X))LT(l(X))+LT(g(X))LT(h(X))}{LT(g(X))LT(l(X))}=$$
$$=\frac{LT(f(X))}{LT(g(X))}+\frac{LT(h(X))}{LT(l(X))}=\varphi\left(\frac{f(X)}{g(X)}\right)+\varphi\left(\frac{h(X)}{l(X)}\right).$$

Por lo que se trata de un homomorfismo. Además es inmediato que $\ker(\varphi)=\mathcal{B}$ *ya que el término líder de un polinomio no nulo es siempre distinto de cero. En virtud del Primer Teorema de Isomorfía concluimos que*

$$\mathcal{K}={}^{\mathcal{O}}\!/_{\mathcal{B}}\cong\mathbb{K}\,.$$

1.5. Valores Absolutos en $\mathbb{Q}$

Al comienzo del capítulo habíamos presentado tres tipos valores absolutos diferentes sobre $\mathbb{Q}$: el valor absoluto trivial, el valor absoluto usual $|\cdot|_\infty$ y, para cada primo p, el valor absoluto p-ádico $|\cdot|_p$.
A lo largo de esta sección veremos que cualquier otro valor absoluto que definamos sobre $\mathbb{Q}$ será, en esencia, igual a alguno de los ya conocidos. Pero, ¿qué significa que dos valores absolutos sean iguales? Sabemos que dos anillos son esencialmente el mismo si existe un isomorfismo que los relaciona. También sabemos que dos funciones definidas en un conjunto son iguales si coinciden las imágenes de cada punto del dominio. A continuación, veremos cuándo podemos decir que dos valores absolutos "el mismo" y daremos herramientas para comprobarlo.

Definición 1.5.1. *Dos valores absolutos* $|\cdot|_1$ *y* $|\cdot|_2$ *definidos en un cuerpo* $\mathbb{K}$ *son* equivalentes *si todo conjunto abierto respecto de uno lo es respecto del otro.*

Lema 1.5.2. *Sea* $|\cdot|$ *un valor absoluto no arquimediano definido en un cuerpo* $\mathbb{K}$. *Entonces para cada número real* $\alpha>0$, $|\cdot|^\alpha$ *es un valor absoluto no arquimediano sobre* $\mathbb{K}$.

Demostración. Las propiedades *1)* y *2)* de la Definición 1.1.1. son inmediatas. Para probar la desigualdad triangular y la propiedad no arquimediana lo que haremos será probar la segunda que es más fuerte. Para ello basta tener en cuenta que $|\cdot|$ es no arquimediano, entonces

$$|x+y|^\alpha\leq(\text{máx}\{|x|,|y|\})^\alpha=\text{máx}\{|x|^\alpha,|y|^\alpha\}.$$

□

Observación 1.5.3. *Nótese que sin la condición de no arquimediano, el lema anterior no sería cierto en el sentido de que* $|\cdot|^\alpha$ *podría no ser ni siquiera un valor absoluto. Para*

mostrar esto basta considerar en $\mathbb{R}$ *el valor absoluto usual con* $\alpha = 2$, $x = 1$, $y = 2$ *entonces*

$$|1+2|^2 = 9 > |1|^2 + |2|^2 = 5.$$

El siguiente resultado nos proporciona una herramienta eficaz para comparar dos valores absolutos:

Proposición 1.5.4. *Sean* $|\cdot|_1$ *y* $|\cdot|_2$ *dos valores absolutos definidos en un cuerpo* $\mathbb{K}$. *Son equivalentes:*

1) $|\cdot|_1$ *y* $|\cdot|_2$ *son equivalentes.*

2) Para cualquier $x \in \mathbb{K}$ *se tiene que* $|x|_1 < 1$ *si, y solo si* $|x|_2 < 1$.

3) Existe $\alpha \in \mathbb{R}_+$ *tal que para cada* $x \in \mathbb{K}$ *se cumple que*

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

Demostración.
$\boxed{1 \Rightarrow 2}$ Supongamos que $|\cdot|_1$ y $|\cdot|_2$ son equivalentes y sean

$$B_j(0,1) = \{x \in \mathbb{K} : |x|_j < 1\} \quad \text{para} \ \ j = 1, 2.$$

Entonces si $x \in B_1(0,1)$ se tiene que $\lim_{n\to\infty} x^n = 0$ para la topología inducida por $|\cdot|_1$ ya que $|x^n|_1 = |x|_1^n$. Como, por hipótesis, $B_2(0,1)$ es un entorno abierto del 0 para esa misma topología, existe un $n_0 \in \mathbb{N}$ tal que $|x|_2^n < 1$ para cada $n \geq n_0$ lo que implica que $|x|_2 < 1$.
Con un razonamiento simétrico tendríamos que si $|x|_2 < 1$ entonces $|x|_1 < 1$.
$\boxed{2 \Rightarrow 3}$ Supongamos ahora que para cualquier $x \in \mathbb{K}$ se tiene que $|x|_1 < 1$ si, y solo si $|x|_2 < 1$.
Sea $y \in \mathbb{K}$ satisfaciendo que $|y|_1 \neq 0$ y $|y|_2 \neq 1$. Reemplazando y por y^-1 si fuese necesario, podemos asumir que $0 < |y|_1 < 1$. Así, haciendo uso de la hipótesis,

$$\alpha = \frac{\ln(|y|_1)}{\ln(|y|_2)}$$

es un número real positivo que, además, es el que cumple que $|y|_1^\alpha = |y|_2$.
Si existiese $x \in \mathbb{K}$ tal que $|x|_1 \neq |x|_2^\alpha$ entonces, de nuevo, reemplazando x por x^{-1} si fuese necesario, existe un punto x en $\mathbb{K}$ con

$$|x|_1^\alpha < |x|_2.$$

Ahora elegimos un número racional r/s satisfaciendo que

$$|x|_1^\alpha < |y|_1^{\alpha r/s} = |y|_2^{r/s} < |x|_2.$$

Esta elección es posible porque la imagen de la aplicación $r/s \to |y|_2^{r/s}$ es densa en $(0, \infty)$.
Se tiene entonces que

$$|x^s|_1^\alpha < |y^r|_1^\alpha = |y^r|_2 < |x^s|_2,$$

y se concluye que

$$|x^s y^{-r}|_1 < 1, \quad |x^s y^{-r}|_2 > 1,$$

lo que contradice la hipótesis inicial. Luego $|x|_1^\alpha = |x|_2$ para todo $x \in \mathbb{K}$.
$\boxed{3 \Rightarrow 1}$ Supongamos que existe $\alpha \in \mathbb{R}_+$ tal que para cada $x \in \mathbb{K}$ se cumple que

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

Entonces, para cualquier par $(a, r) \in \mathbb{K} \times \mathbb{R}_+$,

$$B_1(a, r) = B_2(a, r^{1/\alpha}).$$

Efectivamente,

$$|x - a|_1 < r \iff |x - a|_2^\alpha < r \iff |x - a|_2 < r^{1/\alpha}.$$

Esto es suficiente para probar que ambas topologías son equivalentes ya que, si $U \subseteq$ es un abierto para la topología inducida por $|\cdot|_1$, para cualquier elemento $x \in U$ existe una bola $B_1(x, r) \subseteq U$ y, por lo que acabamos de ver, $B_2(x, r^{1/\alpha}) \subseteq U$.

□

Proposición 1.5.5 (**Fórmula del producto**). *Para todo $x \in \mathbb{Q} \setminus \{0\}$ se cumple que*

$$\prod_{p \in \mathcal{P} \cup \{\infty\}} |x|_p = 1,$$

donde $\mathcal{P}$ denota el conjunto de todos los números primos.

Demostración. Vamos a suponer primero que $x \in \mathbb{Z}^+$. Sea

$$x = p_1^{\epsilon_1} p_2^{\epsilon_2} ... p_r^{\epsilon_r}$$

su descomposición en primos. Por comodidad llamemos $\mathcal{P}_x = \{p \in \mathcal{P} : p \nmid x\}$. Podemos clasificar el valor de $|x|_p$ en función de p de la siguiente forma:

$$|x|_p = \begin{cases} 1 & \text{si } p \in \mathcal{P}_x, \\ p^{-\epsilon_i} & \text{si } p \notin \mathcal{P}_x, \\ x & \text{si } p = \infty. \end{cases}$$

Descomponemos entonces el producto de la siguiente forma:

$$\prod_{p \in \mathcal{P} \cup \{\infty\}} |x|_p = \prod_{p \in \mathcal{P}_x} |x|_p \cdot \prod_{p \notin \mathcal{P}_x} |x|_p \cdot |x|_\infty = \prod_{p \in \mathcal{P}_x} 1 \cdot \prod_{i=1}^{r} p^{-\epsilon_i} \cdot x =$$

$$= p_1^{-\epsilon_1} \cdot p_2^{-\epsilon_2} \cdot ... \cdot p_r^{-\epsilon_r} \cdot x = \frac{1}{x} \cdot x = 1.$$

Finalmente, como $|-x|_p = |x|_p$, podemos extender el resultado a todo $\mathbb{Z}$ y, por el segundo apartado de Propiedades 1.2.1, se concluye el resultado para todo $\mathbb{Q}$. □

Ejemplo 1.5.6.

a) Sea $|\cdot|$ el valor absoluto usual en $\mathbb{R}$. Es sencillo comprobar que $|\cdot|' = \sqrt{|\cdot|}$ es otro valor absoluto en $\mathbb{R}$ (la desigualdad triangular proviene de que $\sqrt{a+b} \leq \sqrt{a} + \sqrt{b}$ para $a, b \geq 0$). Por la última caracterización del lema anterior, como $|x| = (|x|')^2$, ambos valores absolutos son equivalentes.

b) Otro ejemplo de equivalencia sería el del valor absoluto p-ádico para cualquier primo p y el del Ejemplo 1.1.13.b. *En este caso, bastaría tomar $\alpha = \ln(p)$.*

c) En general un valor absoluto no arquimediano, $|\cdot|_1$, y otro arquimediano, $|\cdot|_2$, definidos sobre el mismo cuerpo $\mathbb{K}$, no pueden ser equivalentes. Para ver esto, basta emplear la tercera caracterización del lema anterior. Sabemos que existen $x, y \in \mathbb{K}$ tales que

$$|x+y|_2 > \text{máx}\{|x|_2, |y|_2\}.$$

Si ambos valores absolutos fuesen equivalentes, existiría $\alpha \in \mathbb{R}_+$ con $|a|_1^\alpha = |a|_2$ para cada $a \in \mathbb{K}$. Luego,

$$|x+y|_2 = |x+y|_1^\alpha \leq \text{máx}\{|x|_1, |y|_1\}^\alpha = \text{máx}\{|x|_1^\alpha, |y|_1^\alpha\} = \text{máx}\{|x|_2, |y|_2\}$$

y se llega a una contradicción.

Lema 1.5.7. *Sea $|\cdot|$ un valor absoluto sobre $\mathbb{Q}$. Si existen $C > 0$ y $\alpha > 0$ tales que $|n| \leq Cn^\alpha$ ($|n| \geq Cn^\alpha$ respect.) para cada entero $n \geq 1$, entonces $|k| \leq |k|_\infty$ ($|k| \geq |k|_\infty$ respect.) para todo $k \in \mathbb{Z}$.*

Demostración. Fijamos dos enteros $n \geq 1$ y $r \geq 1$ cualesquiera. Entonces,

$$|n^r| \leq Cn^{r\alpha} \Rightarrow \sqrt[r]{|n^r|} \leq \sqrt[r]{Cn^{r\alpha}} \Rightarrow \sqrt[r]{|n|^r} \leq \sqrt[r]{Cn^{r\alpha}} \Rightarrow |n| \leq C^{1/r} n^\alpha.$$

Haciendo tender ahora $r \to \infty$ obtenemos que $|n| \leq n^\alpha = |n|_\infty^\alpha$ para todo $n \geq 1$ y, como $|n| = |-n|$, podemos afirmar que $|k| \leq |k|_\infty^\alpha$ para todo $k \in \mathbb{Z}$ (el caso $k = 0$ es trivial). □

Lema 1.5.8. *Sean $|\cdot|_1$ y $|\cdot|_2$ dos valores absolutos sobre $\mathbb{Q}$ tales que existe $\alpha > 0$ con $|p|_1 = |p|_2^\alpha$ para cada $p \in \mathbb{Z}^+$ primo, entonces $|\cdot|_1$ y $|\cdot|_2$ son equivalentes.*

Demostración. Sea $q = \dfrac{a}{b} \in \mathbb{Q}$ cualquiera. Tomando la descomposición en primos de a y b se tiene que

$$q = \frac{a}{b} = \frac{u_a p_{j_1}^{\epsilon_{j_1}} p_{j_2}^{\epsilon_{j_2}} \ldots p_{j_r}^{\epsilon_{j_r}}}{u_b p_{l_1}^{\epsilon_{l_1}} p_{l_2}^{\epsilon_{l_2}} \ldots p_{l_t}^{\epsilon_{l_t}}}.$$

$$|q|_1 = \left|\frac{a}{b}\right|_1 = \frac{|a|_1}{|b|_1} = \frac{\left|p_{j_1}^{\epsilon_{j_1}} p_{j_2}^{\epsilon_{j_2}} \ldots p_{j_r}^{\epsilon_{j_r}}\right|_1}{\left|p_{l_1}^{\epsilon_{l_1}} p_{l_2}^{\epsilon_{l_2}} \ldots p_{l_t}^{\epsilon_{l_t}}\right|_1} = \frac{|p_{j_1}|_1^{\epsilon_{j_1}} |p_{j_2}|_1^{\epsilon_{j_2}} \ldots |p_{j_r}|_1^{\epsilon_{j_r}}}{|p_{l_1}|_1^{\epsilon_{l_1}} |p_{l_2}|_1^{\epsilon_{l_2}} \ldots |p_{l_t}|_1^{\epsilon_{l_t}}} =$$

$$= \frac{|p_{j_1}|_2^{\alpha\epsilon_{j_1}} |p_{j_2}|_2^{\alpha\epsilon_{j_2}} \ldots |p_{j_r}|_2^{\alpha\epsilon_{j_r}}}{|p_{l_1}|_2^{\alpha\epsilon_{l_1}} |p_{l_2}|_2^{\alpha\epsilon_{l_2}} \ldots |p_{l_t}|_2^{\alpha\epsilon_{l_t}}} = \frac{\left|p_{j_1}^{\epsilon_{j_1}}\right|_2^\alpha \left|p_{j_2}^{\epsilon_{j_2}}\right|_2^\alpha \ldots \left|p_{j_r}^{\epsilon_{j_r}}\right|_2^\alpha}{\left|p_{l_1}^{\epsilon_{l_1}}\right|_2^\alpha \left|p_{l_2}^{\epsilon_{l_2}}\right|_2^\alpha \ldots \left|p_{l_t}^{\epsilon_{l_t}}\right|_2^\alpha} = \frac{\left|p_{j_1}^{\epsilon_{j_1}} p_{j_2}^{\epsilon_{j_2}} \ldots p_{j_r}^{\epsilon_{j_r}}\right|_2^\alpha}{\left|p_{l_1}^{\epsilon_{l_1}} p_{l_2}^{\epsilon_{l_2}} \ldots p_{l_t}^{\epsilon_{l_t}}\right|_2^\alpha} = \frac{|a|_2^\alpha}{|b|_2^\alpha} = \left|\frac{a}{b}\right|_2^\alpha =$$

$$= |q|_2^\alpha.$$

Y, en virtud de la Proposición 1.5.4, los dos valores absolutos $|\cdot|_1$ y $|\cdot|_2$ son equivalentes. □

Ya tenemos las herramientas necesarias para comparar dos valores absolutos y ver si son, esencialmente, "el mismo" o no. A continuación haremos uso de ellas para demostrar el resultado más importante de esta sección: el Teorema de Ostrowski. Este viene a corroborar lo que ya habíamos anticipado: en $\mathbb{Q}$ cualquier valor absoluto es equivalente a uno de los tres ya conocidos.

Teorema 1.5.9 (**Ostrowski**). *Todo valor absoluto arquimediano en $\mathbb{Q}$ es equivalente a $|\cdot|_\infty$ y todo valor absoluto no trivial no arquimediano en $\mathbb{Q}$ es equivalente a $|\cdot|_p$ para algún primo p.*

Demostración. Veamos primero que cualquier valor absoluto arquimediano, $|\cdot|$, en $\mathbb{Q}$ es equivalente a $|\cdot|_\infty$. Para ello vamos a encontrar un $\alpha \in \mathbb{R}_+$ que cumpla

$$|q| = |q|_\infty^\alpha$$

para todo $q \in \mathbb{Q}$.
Sea n_0 el menor entero positivo tal que $|n_0| > 1$ que existe por el Corolario 1.2.4 y tomamos $\alpha > 0$ de tal manera que $n_0^\alpha = |n_0|$, es decir, $\alpha = \log_{n_0}(|n_0|) > 0$. Entonces,

$$|n_0| = n_0^\alpha = |n_0|_\infty^\alpha.$$

Consideramos ahora la expansión en base n_0 de un entero cualquiera $n \geq 1$:

$$n = \sum_{i=0}^{t} a_i n_0^i, \quad \text{con } \ 0 \leq a_i < n_0, \ t \geq 0 \ \text{ y } \ a_t \geq 1.$$

Como n_0 era el menor entero positivo satisfaciendo $|n_0| > 1$, se tiene que $|a_i| \leq 1 \ \forall i = 0, 1, ..., t$. Así,

$$|n| \leq \sum_{i=0}^{t} |a_i||n_0^i| \leq \sum_{i=0}^{t} |n_0^i| = \frac{|n_0|^t}{1 - \frac{1}{|n_0|}}.$$

Sea

$$C = \frac{1}{1 - 1/|n_0|} > 0,$$

se tiene que

$$|n| \leq \frac{|n_0|^t}{1 - 1/|n_0|} = C n_0^{t\alpha} \leq C n^\alpha,$$

pues $a_t \geq 1$ y, por tanto, $n_0^t \leq n$. Se concluye que para todo $n \geq 1$ se tiene que $|n| \leq C n^\alpha$. Aplicando ahora el Lema 1.5.7. podemos afirmar que $|k| \leq |k|_\infty^\alpha$ para todo $k \in \mathbb{Z}$.
Buscamos ahora obtener la desigualdad contraria. Como hicimos anteriormente, basta probar que existe un $H > 0$ tal que $|n| \geq H n^\alpha$ para todo entero $n \geq 1$ y aplicar el Lema 1.5.7.
Fijamos un entero $n > 0$ y, como antes, consideramos su desarrollo en *base* n_0 dado por $n = \sum_{i=0}^{t} a_i n_0^i$. Se tiene que $n_0^t \leq n < n_0^{t+1}$ (pues $0 \leq a_i < n_0$), así

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

donde, para el último paso, se ha usado la desigualdad $|k| \leq k^\alpha$ probada antes. Luego,

$$|n| \geq n_0^{\alpha(t+1)} - (n_0^{t+1} - n)^\alpha = n_0^{\alpha(t+1)} \left(1 - \left(1 - \frac{n}{n_0^{t+1}}\right)^\alpha\right) \geq$$
$$\geq n^\alpha \left(1 - \left(1 - \frac{1}{n_0}\right)^\alpha\right),$$

tomando

$$H = 1 - \left(1 - \frac{1}{n_0}\right)^\alpha > 0,$$

obtenemos la desigualdad $|n| \geq Hn^\alpha$ para todo $n \geq 1$. En virtud del Lema 1.5.7 se concluye que

$$|k| = |k|_\infty^\alpha \quad \text{para todo} \quad k \in \mathbb{Z}.$$

Hasta aquí hemos probado la igualdad de arriba solo en $\mathbb{Z}$, pero esto es suficiente para extenderlo a $\mathbb{Q}$ ya que, para cada $q = \frac{m}{n} \in \mathbb{Q}$,

$$|q| = \left|\frac{m}{n}\right| = |m| \left|\frac{1}{n}\right| = \frac{|m|}{|n|} = \frac{|m|_\infty^\alpha}{|n|_\infty^\alpha} = \left|\frac{m}{n}\right|_\infty^\alpha = |q|_\infty^\alpha.$$

En virtud del Lema 1.5.4, los dos valores absolutos sobre $\mathbb{Q}$, $|\cdot|$ y $|\cdot|_\infty$, son equivalentes. Ahora nos centraremos en el caso de un valor absoluto no trivial no arquimediano, $|\cdot|$, sobre $\mathbb{Q}$ y vamos a ver que es equivalente a $|\cdot|_p$ para algún primo p.
Por el Corolario 1.2.4, se tiene que $|n| \leq 1$ para todo $n \in \mathbb{Z}$.
Si todos los primos positivos tuviesen $|p| = 1$, entonces dado un $m \in \mathbb{Z} \setminus \{0\}$ cualquiera,

$$|m| = |p_1^{\epsilon_1} p_2^{\epsilon_2} ... p_{j_m}^{\epsilon_{j_m}}| = |p_1|^{\epsilon_1} |p_2|^{\epsilon_2} ... |p_{j_m}|^{\epsilon_{j_m}} = 1,$$

y $|\cdot|$ sería trivial. Por tanto, debe existir al menos un primo positivo $p \in \mathbb{Z}$ satisfaciendo $|p| < 1$. Además, este primo p es el único que lo cumple ya que, de existir otro, $p' \in \mathbb{Z}^+ \setminus \{p\}$, con $|p'| < 1$, por la identidad de Bézout, existirían $a, b \in \mathbb{Z} \setminus \{0\}$ con $ap + bp' = 1$ y, como consecuencia,

$$1 = |1| = |ap + bp'| \leq \text{máx}\{|a||p|, |b||p'|\} < \text{máx}\{|a|, |b|\} \leq 1,$$

lo que es absurdo.
Tomando $\alpha = \log_{|p|}(1/p)$ se tiene que

$$|p|^\alpha = 1/p = |p|_p \quad \text{y} \quad |p'|^\alpha = 1 = |p'|_p$$

para todo primo distinto de p. Por tanto, $|\cdot|^\alpha$ y $|\cdot|_p$ coinciden en todos los enteros primos positivos y, por el Lema 1.5.8 se concluye que $|\cdot|$ y $|\cdot|_p$ son equivalentes. □

Este resultado es fundamental y lo usaremos de ahora en adelante para extender todo el trabajo que hagamos para valores absolutos p-ádicos a cualquier valor absoluto no trivial no arquimediano.

1.6. Valoraciones sobre un cuerpo $\mathbb{K}$

En Álgebra, una valoración sobre un cuerpo es una función que asocia a cada elemento otro perteneciente a un grupo ordenado. En especial, cuando ese grupo ordenado de llegada es $\mathbb{R} \cup \{\infty\}$, nos permiten medir, de cierta manera, el "orden" o "la multiplicidad" de los elementos del cuerpo.

Las valoraciones juegan un papel importante en diversas ramas de las matemáticas, incluyendo teoría de números, geometría algebraica y análisis p-ádico.

A lo largo de este texto ya hemos hablado de un caso particular, la valoración p-ádica, que es la que genera el valor absoluto p-ádico. En esta sección veremos la definición general, algunas propiedades, algunos resultados y ejemplos de valoraciones distintas a la que ya conocemos, siguiendo para ello el texto de Paulo Ribenboim [2].

Definición 1.6.1. *Se dice que $(G, +, \leq)$ es un grupo Abeliano* totalmente ordenado *si $(G, +)$ es un grupo Abeliano y $\leq$ es un orden total en G tal que para todo $a, b, c \in G$,*

$$a \leq b \implies a + c \leq b + c.$$

Definición 1.6.2. *Sea $\mathbb{K}$ un cuerpo y $(G, +, \leq)$ un grupo Abeliano totalmente ordenado. Una* valoración sobre $\mathbb{K}$ *es una aplicación*

$$v : \mathbb{K} \longrightarrow G \cup \{\infty\}$$

que satisface las siguientes condiciones:

1) $v(x) = \infty$ si, y solo si, $x = 0$;

2) $v(xy) = v(x) + v(y)$ para cada $x, y \in \mathbb{K}$;

3) $v(x + y) \geq \min\{v(x), v(y)\}$ para cada $x, y \in \mathbb{K}$.

Al par $(\mathbb{K}, v)$ se le conoce como cuerpo de valoración.

Definición 1.6.3. *Sea $\mathbb{K}$ un cuerpo. Una valoración* de rango uno *sobre $\mathbb{K}$ es una valoración, v, con llegada en un subgrupo de $(\mathbb{R}, +, \leq)$.*

Es este caso especial de valoraciones, las de rango uno, las que vamos a estudiar con más detenimiento.

Ejemplo 1.6.4. *Algunos ejemplos de valoraciones sobre un cuerpo son:*

a) La llamada valoración trivial *que está definida sobre un cuerpo cualquiera $\mathbb{K}$ como*

$$v(x) = \begin{cases} 0 & si\ x \neq 0, \\ \infty & si\ x = 0. \end{cases}$$

b) La valoración p-ádica, v_p, que se estudió en la sección 1.1. Además, en este caso en particular donde la llegada es en $\mathbb{Z}$ se dice que es una valoración discreta.

c) Sea $\mathbb{K} = \mathbb{C}(X)$ el cuerpo de las funciones racionales en la recta afín $\mathbb{A}^1_{\mathbb{C}}$ y fijamos un punto $a \in \mathbb{A}^1_{\mathbb{C}}$. Para un polinomio $f(X)$ no nulo, definimos $v_a(f)$ como la multiplicidad de la raíz $X = a$ en f y extendemos a $\mathbb{K}$ haciendo lo siguiente: $v_a(f/g) = v_a(f) - v_a(g)$ con el convenio de $v_a(h) = \infty$ si $h(X) = 0$.
Entonces v_a define una valoración sobre $\mathbb{K}$ y su anillo de valoración son las funciones racionales que no tienen un polo $X = a$, es decir, cuyo denominador no se anula en $X = a$.

Propiedades 1.6.5. *Sea $\mathbb{K}$ un cuerpo con una valoración v. Entonces, para cada $x, y \in \mathbb{K} \setminus \{0\}$:*

1) $v(1) = 0$,

2) $v(x^{-1}) = -v(x)$,

3) $v(-x) = v(x)$,

4) si $v(x) < v(y)$ entonces $v(x + y) = v(x)$.

Demostración.

1) Por definición, $v(1) = v(1 \cdot 1) = v(1) + v(1)$, por lo que necesariamente $v(1) = 0$.

2) Por la propiedad anterior, $0 = v(1) = v(xx^{-1}) = v(x) + v(x^{-1})$.

3) $v(-x) = v(-1) + v(x) = v(x)$ ya que $v(1) = v((-1)^2) = v(-1) + v(-1) = 0$, por lo que $v(-1) = 0$.

4) Supongamos que $v(x) < v(y)$. Por reducción al absurdo, si suponemos que

$$v(x + y) > \text{mín}\{v(x), v(y)\} = v(x),$$

entonces

$$v(x) = v(x + y - y) \geq \text{mín}\{v(x + y), v(-y)\} = \text{mín}\{v(x + y), v(y)\}.$$

Ahora, si fuese $\text{mín}\{v(x + y), v(y)\} = v(y)$, entonces la cadena de desigualdades anterior nos llevaría a que $v(x) \geq v(y)$, lo que contradiría nuestra hipótesis inicial. Necesariamente, $\text{mín}\{v(x + y), v(y)\} = v(x + y)$ y llegamos entonces a que

$$v(x) \geq v(x + y),$$

lo que nos lleva a un absurdo.

□

Definición 1.6.6. *Sea $\mathbb{K}$ un cuerpo y v_1, v_2 dos valoraciones de rango uno sobre $\mathbb{K}$. Decimos que estas dos valoraciones son* equivalentes *si existe un número real $\alpha > 0$ tal que $v_2(x) = \alpha v_1(x)$ para cada $x \in \mathbb{K}$.*

De forma análoga al Ejemplo 1.1.13.b), a partir de una valoración, v, de rango uno sobre $\mathbb{K}$, podemos definir siempre un valor absoluto no arquimediano utilizando como base cualquier número real $\alpha > 1$, haciendo $|x| = \alpha^{-v(x)}$. De esta forma y como veremos en los siguientes resultados, las valoraciones de rango uno equivalentes guardan una estrecha relación con los valores absolutos no arquimedianos equivalentes vistos en el capítulo anterior.

Lema 1.6.7. *Sea v una valoración de rango uno sobre $\mathbb{K}$ y $1 < \alpha < \beta$ dos números reales. Entonces los valores absolutos no arquimedianos definidos por $|x|_1 = \alpha^{-v(x)}$ y $|x|_2 = \beta^{-v(x)}$, para cada $x \in \mathbb{K}$, son equivalentes.*

Demostración. Tomando $r = \log_\alpha(\beta) > 0$, entonces

$$|x|_1^r = (\alpha^r)^{-v(x)} = \beta^{-v(x)} = |x|_2,$$

para cada $x \in \mathbb{K}$. En virtud del Lema 1.5.4, $|\cdot|_1$ y $|\cdot|_2$ son equivalentes. □

Lema 1.6.8. *Sea $\alpha > 1$ y v_1, v_2 dos valoraciones de rango uno equivalentes sobre $\mathbb{K}$. Entonces los valores absolutos no arquimedianos $|x|_1 = \alpha^{-v_1(x)}$ y $|x|_2 = \alpha^{-v_2(x)}$ son equivalentes.*

Demostración. Es inmediato a partir del Lema 1.5.4 y de la definición de valoraciones de rango uno equivalentes. □

Definimos ahora los conjuntos formados por las clases de equivalencias de valoraciones de rango uno y valores absolutos sobre un cuerpo $\mathbb{K}$:

$$\mathcal{V} := \{\text{clases de equivalencia de valoraciones de rango uno sobre } \mathbb{K}\},$$

$$\mathcal{A} := \{\text{clases de equivalencia de valores absolutos no arquimedianos sobre } \mathbb{K}\}.$$

Se tiene el siguiente resultado:

Proposición 1.6.9. *Sea $\mathbb{K}$ un cuerpo. Existe una aplicación $f : \mathcal{A} \longrightarrow \mathcal{V}$ biyectiva.*

Demostración. Fijamos un número real $\alpha > 1$. Definimos la aplicación

$$f : \mathcal{A} \longrightarrow \mathcal{V}$$

como aquella que asocia a cada clase de un valor absoluto no arquimediano $|\cdot|$ la valoración de rango uno $v(x) = -\log_\alpha(|x|)$. El Lema 1.6.7 y el Lema 1.6.8 nos asegura que esta aplicación está bien definida. Veamos que se trata de una biyección.
Sean $|\cdot|_1$ y $|\cdot|_2$ dos valores absolutos no arquimedianos no equivalentes y supongamos que su imagen por f es la misma, es decir, existe $r > 0$ tal que

$$\log_\alpha(|x|_1) = r \log_\alpha(|x|_2)$$

para cada $x \in \mathbb{K}$. Por tanto,

$$|x|_1 = \alpha^{\log_\alpha(|x|_1)} = \alpha^{r \log_\alpha(|x|_2)} = (|x|_2)^r,$$

por lo que $|\cdot|_1$ y $|\cdot|_2$ son equivalentes y hemos llegado a una contradicción. Podemos asegurar que f es inyectiva.
Para la sobreyectividad, tomemos una valoración, v', de rango uno sobre $\mathbb{K}$. Consideramos el valor absoluto no arquimediano dado por $|x| = \alpha^{-v'(x)}$. Entonces la imagen de este último por f es la valoración dada por

$$v(x) = -\log_\alpha(|x|) = -\log_\alpha(\alpha^{-v'(x)}) = -(-v'(x)) = v'(x),$$

y concluimos que f es una biyección. □

Gracias a este resultado, podemos trabajar indistintamente con valores absolutos no arquimedianos sobre $\mathbb{K}$ o con valoraciones sobre $\mathbb{K}$, según nos convenga.

Definición 1.6.10. *Sea $\mathbb{K}$ un cuerpo y v una valoración sobre $\mathbb{K}$. El subanillo*

$$A_v = \{x \in \mathbb{K} : v(x) \geq 0\}$$

se denomina anillo de valoración de v. *Un dominio de integridad D se dice que es un* anillo de valoración *cuando existe una valoración v sobre $K(D)$ tal que $D = A_v$. En el caso particular de que exista una valoración, v, de rango uno tal que $D = A_v$, se dice que D es un anillo de valoración de* rango uno.

Observación 1.6.11. *Notemos que $A_v = K(D)$ exactamente cuando v es la valoración trivial.*

Esta definición encaja perfectamente con la dada en la Definición 1.4.4 para el caso particular de la valoración p-ádica.

Proposición 1.6.12. *Sean v_1 y v_2 dos valoraciones de rango uno sobre $\mathbb{K}$. Entonces $A_{v_1} = A_{v_2}$ si, y solo si, v_1 y v_2 son equivalentes.*

Demostración. Si consideramos los valores absolutos asociados $|\cdot|_1$ y $|\cdot|_2$, en virtud de la Proposición 1.6.9, queremos demostrar que:

$|\cdot|_1$ y $|\cdot|_2$ equivalentes si, y solo si, $B_1 := \{x \in \mathbb{K} : |x|_1 \leq 1\} = B_2 := \{x \in \mathbb{K} : |x|_2 \leq 1\}$.

$\boxed{\Leftarrow}$ Supongamos que $|\cdot|_1$ y $|\cdot|_2$ son equivalentes. Entonces existe un $r > 0$ tal que $|x|_2 = |x|_1^r$ para cada $x \in \mathbb{K}$. Claramente tenemos una contención ya que

$$|x|_2 \leq 1 \Longrightarrow |x|_1^r \leq 1 \Longrightarrow |x|_1 \leq 1^{1/r} = 1.$$

La contraria es también inmediata por el mismo argumento ya que $|x|_1 = (|x|_2)^{1/r}$ para cada $x \in \mathbb{K}$.
$\boxed{\Rightarrow}$ Supongamos que $B_1 = B_2$. Entonces, en virtud del Lema 1.5.4, usando la segunda equivalencia de este resultado, podemos asegurar que $|\cdot|_1$ y $|\cdot|_2$ son equivalentes. □

Definición 1.6.13. *Un grupo Abeliano totalmente ordenado, $(G, +, \leq)$, se dice que satisface la* Propiedad Arquimediana *si para todo $a, b \in G$ con $0 < a \leq b$, existe $n \in \mathbb{N}$ tal que*

$$b \leq na = \overbrace{a + a + ... + a}^{n \text{ veces}}.$$

A continuación vamos a presentar un lema que más tarde nos ayudará a caracterizar los anillos de valoración de rango uno de dos formas distintas. Su demostración, que aparece en el texto de Laszlo Fuchs [3] y que originalmente se la debemos a Otto Ludwing Hölder, no la daremos con todo el detalle necesario ya que para ello sería preciso dar las definiciones y las principales propiedades de las Cortaduras de Dedekind y creemos que esto no justificaría la extensión que esto nos llevaría para un resultado que es técnico y que se aleja del objeto central del trabajo.

Lema 1.6.14. *Si $(G, +, \leq)$ es un grupo Abeliano totalmente ordenado que satisface la Propiedad Arquimediana, entonces existe un isomorfismo que conserva el orden entre G y un subgrupo de $(\mathbb{R}, +, \leq)$.*

Demostración. Podemos suponer que $G \neq \{0\}$ y entonces existe un $a \in G$ con $a > 0$. Vamos a definir una aplicación $\mu : G \longrightarrow \mathbb{R}$ de la siguiente forma:

- $\mu(a) = 1$.
- Si $b > 0$, consideramos el conjunto

$$S_b := \left\{ \frac{m}{n} \in \mathbb{Q} : n > 0, ma < nb \right\}.$$

  Si $a < b$, entonces $1 \in S_b$. Si por el contrario $b < a$, por la Propiedad Arquimediana, existe $n \in \mathbb{N}$ tal que $1/n \in S_b$. Por tanto, $S_b \neq +\emptyset$. Además, si $b < a$ entonces $1 \notin S_b$ y si $a < b$, por lo mismo que antes, existe $m \in \mathbb{N}$ tal que $b < ma$ y, por tanto, $m \notin S_b$. En cualquiera de los casos, $S_b \neq \mathbb{Q}$.
  Por otro lado, si tenemos $m/n \in S_b$ y $m'/n' \in \mathbb{Q}$ con $m'/n' \leq m/n$, entonces $ma \leq nb$ y $m'n \leq mn'$. Juntando ambas desigualdades,

$$m'mna \leq mn'nb \Longrightarrow m'a \leq n'b \Longrightarrow m'/n' \in S_b.$$

  Por tanto S_b debe estar acotado superiormente ya que sabemos que existe, al menos, un racional que no pertenece a S_b y también sabemos que un número pertenece, todos los menos también por lo que si no existiese cota superior, debería ser $\mathbb{Q} = S_b$. Definimos entonces $\mu(b) = \sup S_b$ (un conjunto S_b de racionales satisfaciendo estas condiciones se dice que es una *cortadura de Dedekind*).

- Si $b \in G$ con $b < 0$, entonces $\mu(b) = -\mu(-b)$ que sí está definido pues $-b > 0$ y usamos el apartado anterior.
- Por último, $\mu(0) = 0$.

Ahora habría que verificar que μ es, en efecto, un isomorfismo que conserva el orden. Es en este momento cuando necesitaríamos utilizar las propiedades de las Cortaduras de Dedekind que, como ya anticipamos, se alejan del objeto central del trabajo y supondrían extenderlo en exceso, por lo que omitiremos este paso.
Utilizando entonces las propiedades de las Cortaduras de Dedekind se llega a que ve que $\mu(b - c) = \mu(b) - \mu(c)$ y $\mu(b) > 0$ si, y solo si, $b > 0$ para cada $b, c \in G$. Por tanto, μ es un isomorfismo que preserva el orden y hemos probado lo que queríamos. □

Notación 1.6.15. *Sea $A \subseteq R$ un subanillo de un anillo R y $x \in R \setminus A$. Denotamos por $A[x]$ al mínimo anillo que contiene al subanillo A y al elemento x.*

Tenemos ya todas las herramientas necesarias para demostrar el siguiente resultado que caracteriza los anillos de valoración:

Teorema 1.6.16. *Sea D un dominio de integridad y K su cuerpo de fracciones. Son equivalentes:*

1) D es un anillo de valoración de rango uno no trivial.

2) D es un subanillo maximal propio de K.

3) Se cumplen las siguientes dos propiedades:

i) para cada $x \in K \setminus \{0\}$, si $x \notin D$, entonces $x^{-1} \in D$;

ii) sea $x \in D$ con $x^{-1} \notin D$. Si $y \in K^*$, entonces existe $n \in \mathbb{N}$ tal que $x^n \in Dy$.

Demostración.
$\boxed{1 \Rightarrow 2}$ Supongamos que D es un anillo de valoración no trivial. Entonces, por la Proposición 1.6.12, $D \neq K$ ya que, de lo contrario, v sería trivial. Sea $B \subseteq K$ un subanillo tal que $D \subsetneq B \subseteq K$. Sea $x \in B$ y $x \notin D$, entonces $v(x) < 0$, lo que implica que $v(x^{-1}) > 0$.
Sea $y \in K \setminus \{0\}$, si consideramos los números reales $v(x^{-1})$ y $v(y^{-1})$, sabemos que existe un $n \in \mathbb{N}$ tal que $nv(x^{-1}) \geq v(y^{-1})$, luego $v(y) \geq v(x^n)$ por lo que $y \in Dx^n \subseteq DB \subseteq B$. Por tanto, $B = K$ y como consecuencia, D es un subanillo maximal propio de K.
$\boxed{2 \Rightarrow 3}$ Para probar *i)*, supongamos que D es un subanillo maximal propio de K. Sea $x \in K$ con $x \notin D$. Por reducción al absurdo, supongamos que $x^{-1} \notin D$. Entonces, $D[x^{-1}]$ es un subanillo que contiene estrictamente a D que, por hipótesis, es maximal, luego $D[x^{-}1] = K$. Podemos escribir entonces

$$x = a_0 + a_1 x^{-1} + ... + a_n x^{-n}$$

con $a_i \in D$ para cada $i = 0, 1, ..., n$. De esta manera,

$$x^{n+1} = a_0 x^n + a_1 x^{n-1} + ... + a_n.$$

De la misma forma, para cada $k \geq 1$, se puede expresar x^{n+k} como una combinación lineal con coeficientes en D, de los elementos 1, x, x^2,..., x^n. Por tanto, $K = D[x]$ es un D-módulo finitamente generado. Como K es el cuerpo de fracciones de D y $K \neq D$, hemos llegado a una contradicción ya que K no es un ideal fraccionario. Por tanto, $x^{-1} \in D$.
Para probar *ii)*, sea $x \in D$ con $x^{-1} \notin D$, entonces $D[x^{-1}] = K$ por la maximalidad de D. Sea ahora $y \in K^*$ cualquiera, entonces $y^{-1} \in D[x^{-1}]$ y pude ser escrito como

$$y^{-1} = a_0 + a_1 x^{-1} + ... + a_n x^{-n}$$

con $a_0, a_1, ..., a_n \in D$. Si denotamos

$$a = a_0 x^n + a_1 x^{n-1} + ... + a_n \in D,$$

esto implica que $y^{-1} = ax^{-n}$ y entonces $x^n = ay \in Dy$.
$\boxed{3 \Rightarrow 1}$ Supongamos que se cumplen las dos propiedades de *3)* y denotemos por $U = D^*$. Comenzamos definiendo el grupo $G = {}^{K^*}\!/_U$ y vamos a ver que podemos establecer en él un orden total.
Sean $x, y \in K^*$ (denotamos por xU e yU sus respectivas clases en G) con $xU \not\leq yU$, entonces $x \nmid y$, por lo que $yx^{-1} \notin D$. Teniendo en cuenta nuestra hipótesis, necesariamente $(yx^{-1})^{-1} = xy^{-1} \in D$, por lo que $yU \leq xU$. Con esto hemos probado que G es un grupo multiplicativo totalmente ordenado.
Ahora, si $U \leq xU$ con $U \neq xU$, significa que existe $x \in D$ y $x \notin U$, por lo que $x^{-1} \notin D$. Si $yU \in G$, aplicando *ii)*, existe $n \in \mathbb{N}$ tal que $x^n \in Dy$, por lo que y divide a x^n y así $yU \leq x^nU = (xU)^n$. Esto prueba que G satisface la Propiedad Arquimediana.
Sabemos, además, que existe un isomorfismo, ϕ, entre un grupo Abeliano aditivo y ordenado, H, y el grupo multiplicativo ordenado G anteriormente descrito y que dicho isomorfismo conserva el orden. Esto hace que H satisfaga la Propiedad Arquimediana y, en virtud del Lema 1.6.14, podemos considerar H como un subgrupo de $(\mathbb{R}, +, \leq)$. Definimos una aplicación

$$v : K \longrightarrow H \cup \{\infty\},$$

dada por

- $v(0) = \infty$;
- Si $x \in K^*$, sea $z_x = \phi(xU) \in H$, entonces $v(x) = z_x$. Veamos que v es una valoración en $\mathbb{K}$. Si $z_x = \phi(xU)$ y $z_y = \phi(yU)$ con $x, y \in K^*$, entonces

  $$z_x + z_y = \phi(xU) + \phi(yU) = \phi(xU \cdot yU) = \phi(xyU)$$

  por tanto, $v(xy) = v(x) + v(y)$. De la misma forma, si $v(x) \leq v(y)$, entonces $xU \leq yU$ y así $x \mid y$. Como consecuencia, $x \mid (x + y)$, luego

  $$v(x + y) \geq v(x) = \text{mín}\{v(x), v(y)\}.$$

  Para finalizar, notemos que $x \in D$ si, y solo si, $U \leq xU$, es decir, $x \in D$ si, y solo si, $v(x) \geq 0$, lo que implica que D es el anillo de valoración de v lo que concluye la prueba.

□

Finalizamos esta pequeña introducción a las valoraciones sobre un cuerpo con un resultado que utilizaremos más adelante en la descripción de los números p-ádicos:

Proposición 1.6.17. *Sea D un anillo de valoración de rango uno no trivial, entonces D es un anillo local.*

Demostración. Por el Teorema 1.6.16, sabemos que para cada $x \in K \setminus \{0\}$ con $x \notin D$ entonces $x^{-1} \in D$. Como $D \subsetneq K$ (por ser anillo de valoración no trivial) entonces D no puede ser un cuerpo al ser K el mínimo cuerpo que contiene a D. Sabemos entonces que

existe un ideal maximal de D no nulo que llamamos $\mathcal{M}$. Queremos ver que es el único. Por reducción al absurdo, si existiese otro ideal maximal $\mathcal{M}' \neq \mathcal{M}$ de D, entonces escojo $x, y \in D$ con $x \in \mathcal{M} \setminus \mathcal{M}'$ e $y \in \mathcal{M}' \setminus \mathcal{M}$. Considero el elemento $xy^{-1} \in K$. Si $xy^{-1} \in D$, entonces $x = xy^{-1}y \in \mathcal{M}'$ lo cual es una contradicción, por lo que $xy^{-1} \notin D$. Del mismo modo, $x^{-1}y \notin D$. Por tanto hemos contradicho nuestra hipótesis al suponer que existen dos ideales maximales distintos en D. Afirmamos que D es un anillo local. □

Observación 1.6.18. *Este resultado también es cierto para anillos de valoración que no sean necesariamente de rango uno. La demostración es muy similar aunque para el propósito para el que nosotros para el queremos este resultado, es suficiente con demostrarlo para el caso de rango uno.*

Capítulo 2

Compleción de $\mathbb{Q}$

A pesar de su riqueza y versatilidad, $\mathbb{Q}$ tiene una propiedad notable: no es completo para ningún valor absoluto no trivial. Esta característica significa que hay sucesiones de números racionales que convergen a un límite que no está en $\mathbb{Q}$, lo que sugiere que el cuerpo de los racionales es "demasiado pequeño"para abarcar todos los números de interés. La falta de completitud hace que su utilidad en diversas áreas matemáticas y en aplicaciones prácticas donde se requiere el tratamiento de la totalidad de los números reales sea limitada. Es por ello que resulta de gran interés la compleción de $\mathbb{Q}$ y, en especial para nosotros, la que se realiza a través de un valor absoluto p-ádico.

2.1. Introducción

Comenzamos este nuevo capítulo recordando algunos conceptos básicos de Análisis y justificando la necesidad de añadir límites a algunas sucesiones de interés.

A lo largo de esta sección trataremos con límites respecto de diferentes valores absolutos sin hacer distinción entre la notación. Salvo que se indique otra cosa, los límites de sucesiones de valores absolutos serán respecto del valor absoluto usual en $\mathbb{R}$ y, cuando las sucesiones sean de números racionales que no vengan indicados como valores absolutos, los límites se tomarán respecto del valor absoluto p-ádico.

Definición 2.1.1. *Sea $\mathbb{K}$ un cuerpo y $|\cdot|$ un valor absoluto definido en él.*

1) Una sucesión $(x_n)_{n\in\mathbb{N}}$ de elementos de $\mathbb{K}$ se dice que es de Cauchy *si para cada $\epsilon > 0$, existe un $n_0 \in \mathbb{N}$, que depende de ϵ, tal que*

$$|x_n - x_m| < \epsilon \quad si \;\; n, m \geq n_0.$$

2) Se dice que $\mathbb{K}$ es completo *para $|\cdot|$ si toda sucesión de Cauchy de elementos de $\mathbb{K}$ tiene límite en $\mathbb{K}$.*

Ejemplo 2.1.2. *Veamos que $\mathbb{Q}$ no es completo para $|\cdot|_\infty$. Definimos la ya conocida sucesión*

$$x_n = \left(1 + \frac{1}{n}\right)^n, \;\; n \in \mathbb{N},$$

que es claramente de números racionales. Esta sucesión converge hacia e *cuando* $n \to \infty$*, por lo que es de Cauchy para* $|\cdot|_\infty$*. Sin embargo,* $e \notin \mathbb{Q}$*, por lo que no puede ser completo.*

Es ya conocido que $\mathbb{R}$ es completo para el valor absoluto $|\cdot|_\infty$. De hecho, como $\mathbb{Q}$ es denso en $\mathbb{R}$, es el cuerpo más pequeño que contiene a $\mathbb{Q}$ y que es completo para este valor absoluto. En estas circunstancias se dice que $\mathbb{R}$ es el completado de $\mathbb{Q}$ para el valor absoluto $|\cdot|_\infty$. Este término se puede generalizar a cualquier cuerpo $\mathbb{K}$ a través de la siguiente definición:

Definición 2.1.3. *Sea* $\mathbb{K}$ *un cuerpo y* $|\cdot|$ *un valor absoluto definido en él. Se dice que otro cuerpo* $\mathbb{L}$ *con un valor absoluto* $|\cdot|_\mathbb{L}$ *definido en él, y para el cual es completo, es el* completado de $\mathbb{K}$ *para el valor absoluto* $|\cdot|$ *si existe una inclusión* $i : \mathbb{K} \hookrightarrow \mathbb{L}$ *tal que* $i(\mathbb{K})$ *es denso en* $\mathbb{L}$ *y* $|x| = |i(x)|_\mathbb{L}$ *para todo* $x \in \mathbb{K}$*.*

Lema 2.1.4. *Sea* $|\cdot|$ *un valor absoluto no arquimediano definido en* $\mathbb{Q}$*. Entonces una sucesión de números racionales,* $(x_n)_{n\in\mathbb{N}}$*, es de Cauchy para* $|\cdot|$ *si, y solo si,* $\lim_{n\to\infty} |x_{n+1} - x_n| = 0$.

Demostración.
$\boxed{\Rightarrow}$ Es inmediata.
$\boxed{\Leftarrow}$ Supongamos que $\lim_{n\to\infty} |x_{n+1} - x_n| = 0$. Fijado un $\epsilon > 0$, entonces existe $n_0 \in \mathbb{N}$ tal que $|x_{n+1} - x_n| < \epsilon$ para todo $n \geq n_0$.
Sean ahora $m, l \geq n_0$ y supongamos que $m = l + s$. Entonces

$$\begin{aligned} |x_m - x_l| &= |x_m - x_{m-1} + x_{m-1} - x_{m-2} + x_{m-2} - ... - x_{m-s+1} + x_{m-s+1} - x_l| \leq \\ &\leq \text{máx}\{|x_m - x_{m-1}|, |x_{m-1} - x_{m-2}|, \ ..., |x_{m-s+1} - x_l|\} \leq \epsilon. \end{aligned}$$

Por tanto, $(x_n)_{n\in\mathbb{N}}$ es una sucesión de Cauchy. □

Este último resultado no es necesariamente cierto cuando se tiene un valor absoluto arquimediano. Basta considerar en $\mathbb{R}$, con el valor absoluto $|\cdot|_\infty$, la sucesión se sumas parciales de la serie armónica:

$$S_n = \sum_{k=1}^{n} \frac{1}{n}, \quad n \in \mathbb{N},$$

que no es de Cauchy por no ser convergente y ser $\mathbb{R}$ completo y, sin embargo,

$$\lim_{n\to\infty} |S_{n+1} - S_n|_\infty = \lim_{n\to\infty} \frac{1}{n+1} = 0.$$

Lema 2.1.5. *Consideramos en* $\mathbb{Q}$ *un valor absoluto no trivial* $|\cdot|$*. Sea* $(x_n)_{n\in\mathbb{N}}$ *una sucesión de Cauchy de números racionales para ese valor absoluto, entonces existe* $M > 0$ *tal que* $|x_n| \leq M$ *para cada* $n \in \mathbb{N}$*.*

Demostración. Fijado un $\epsilon > 0$, existe $n_0 \in \mathbb{N}$ tal que

$$|x_n - x_m| < \epsilon$$

para todo $n, m \geq n_0$. Empleando la segunda desigualdad triangular,

$$|x_n| - |x_m| \leq |x_n - x_m| < \epsilon \implies |x_n| < \epsilon + |x_m|$$

para cada $n, m \geq n_0$. Tomando $m = n_0$,

$$|x_n| < \epsilon + |x_{n_0}|$$

para cada $n \geq n_0$. Sea $M = \text{máx}\{|x_1|, |x_2|, ..., |x_{n_0-1}|, |x_{n_0}|, \epsilon + |x_{n_0}|\}$, entonces

$$|x_n| \leq M \text{ para todo } n \in \mathbb{N},$$

como queríamos demostrar. □

A continuación vamos a presentar dos propiedades relativas a la suma y producto de límites que, si bien son ya conocidos en Análisis, conviene generalizarlas para cualquier cuerpo con un valor absoluto no trivial.

Lema 2.1.6. *Sea $\mathbb{K}$ un cuerpo con un valor absoluto no trivial, $|\cdot|$, definido en él y sean $(x_n)_{n\in\mathbb{N}}$, $(y_n)_{n\in\mathbb{N}}$ dos sucesiones en $\mathbb{K}$ tales que, para ese valor absoluto,*

$$\lim_{n\to\infty} x_n = x, \quad \lim_{n\to\infty} y_n = y.$$

Entonces:

1) $\lim_{n\to} x_n + y_n = x + y$.

2) $\lim_{n\to} x_n y_n = xy$.

Demostración. 1) Fijado un $\epsilon > 0$, existen $n_0, m_0 \in \mathbb{N}$ satisfaciendo que

$$|x_n - x| < \frac{\epsilon}{2}, \quad |y_n - y| < \frac{\epsilon}{2}$$

para todo $n \geq n_0, \ m \geq m_0$. Entonces, para cada $n \geq N_0 = \text{máx}\{n_0, m_0\}$ se tiene que

$$|x_n + y_n - x - y| \leq |x_n - x| + |y_n - y| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon$$

2) Por el lema previo podemos encontrar un $M > 0$ tal que $|y_n| \leq M$ y $|x| \leq M$. Sea $\epsilon > 0$, sabemos que existen $n_0, m_0 \in \mathbb{N}$ satisfaciendo que

$$|x_n - x| < \frac{\epsilon}{2M}, \quad |y_n - y| < \frac{\epsilon}{2M}$$

para todo $n \geq n_0, \ m \geq m_0$. Entonces, para cada $n \geq N_0 = \text{máx}\{n_0, m_0\}$ se tiene que

$$|x_n y_n - xy| = |x_n y_n - xy_n| + |xy_n - xy| = |x_n - x||y_n| + |y_n - y||x| <$$
$$< M\frac{\epsilon}{2M} + M\frac{\epsilon}{2M} = \epsilon.$$

□

Seguidamente vamos a demostrar un importante resultado que ya habíamos adelantado en la introducción de esta sección.

Proposición 2.1.7. *El cuerpo $\mathbb{Q}$ de los racionales no es completo para ningún valor absoluto no trivial.*

Demostración. Gracias al Teorema de Ostrowski podemos trabajar únicamente con los valores absolutos del tipo $|\cdot|_p$ cuando $p \leq \infty$. Lo que vamos a hacer será fijar un valor absoluto $|\cdot|_p$ para algún primo $p < \infty$ (ya está probado que $\mathbb{Q}$ no es completo para $|\cdot|_\infty$) y encontrar una sucesión de Cauchy que no sea convergente para $|\cdot|_p$.
Consideramos la sucesión en $\mathbb{Q}$ dada por

$$(x_n)_{n\in\mathbb{N}} = \left(\sum_{k=1}^{n} p^{k!}\right)_{n\in\mathbb{N}}.$$

En virtud del Lema 2.1.4, dado que

$$|x_{n+1} - x_n|_p = |p^{(n+1)!}|_p = p^{-(n+1)!} \xrightarrow[n\to\infty]{} 0,$$

tenemos que la sucesión $(x_n)_{n\in\mathbb{N}}$ es efectivamente de Cauchy para $|\cdot|_p$. Por reducción al absurdo, vamos a suponer ahora que $\lim_{n\to\infty} x_n = a/b$ respecto de $|\cdot|_p$, con $a \in \mathbb{Z}$ y $b \in \mathbb{N}$ coprimos.
Para cada $n \in \mathbb{N}$, es claro p solo divide una vez a $\sum_{k=1}^{n} p^{k!}$ como consecuencia se tiene que $\sum_{k=1}^{n} p^{k!} \in \mathbb{S}\,(0, p^{-1}) := \{x \in \mathbb{Q} : |x| = p^{-1}\}$ para cada $n \in \mathbb{N}$ y, por ser este conjunto cerrado (es el complementario de $B(0,1) \cup (\mathbb{Q} \setminus \bar{B}(0,1))$), el límite también estará en la esfera, luego podemos afirmar que $|a/b|_p = p^{-1}$, lo que implica, por el hecho de que a y b sean coprimos, que $p \nmid b$. Esto último lo utilizaremos más adelante.
Fijado un $n \in \mathbb{N}$ cualquiera, tenemos que

$$\frac{a}{b} = \lim_{m\to\infty} \sum_{k=1}^{n+m} p^{k!} = \lim_{m\to\infty} \sum_{k=1}^{m} p^{(n+k)!} + \sum_{k=1}^{n} p^{k!} \Longrightarrow \lim_{m\to\infty} \sum_{k=1}^{m} p^{(n+k)!} = \frac{a}{b} - \sum_{k=1}^{n} p^{k!}.$$

De nuevo, como cada uno de los términos $\sum_{k=1}^{m} p^{(n+k)!}$ está en la esfera $\mathbb{S}\left(0, p^{-(n+1)!}\right)$, el límite cuando m tiene a infinito también debe pertenecer a dicha esfera, es decir,

$$\left| a/b - \sum_{k=1}^{n} p^{k!} \right|_p = p^{-(n+1)!}.$$

De esto último, junto con el hecho de que $p \nmid b$, se deduce que

$$v_p\left(a - b\sum_{k=1}^{n} p^{k!}\right) = v_p\left(b\left(\frac{a}{b} - \sum_{k=1}^{n} p^{k!}\right)\right) = v_p(b) + v_p\left(\frac{a}{b} - \sum_{k=1}^{n} p^{k!}\right) =$$
$$= 0 + (n+1)! = (n+1)!,$$

es decir, $p^{(n+1)!} \mid \left(a - b\sum_{k=1}^{n} p^{k!}\right)$.

Por otro lado,

$$\left|a - b\sum_{k=1}^{n} p^{k!}\right|_\infty \leq |a|_\infty + b\sum_{k=1}^{n} p^{k!} < |a|_\infty + b\sum_{k=0}^{n!} p^k = |a|_\infty + b\frac{p^{n!+1}-1}{p-1} < |a|_\infty + bp^{n!+1}.$$

Tomando límites respecto del valor absoluto $|\cdot|_\infty$,

$$\lim_{n\to\infty} \frac{|a|_\infty + bp^{n!+1}}{p^{(n+1)!}} = \lim_{n\to\infty}\left(\frac{|a|}{p^{(n+1)!}} + \frac{b}{p^{n\cdot n!-1}}\right) = 0 < 1,$$

luego, para un $n_0 \in \mathbb{N}$ suficientemente grande, se tendría que

$$\left|a - b\sum_{k=1}^{n_0} p^{k!}\right|_\infty < |a|_\infty + bp^{n_0!+1} < p^{(n_0+1)!}.$$

Por tanto hemos llegado a que $\left|a - b\sum_{k=1}^{n} p^{k!}\right|_\infty$ es un entero no negativo que es múltiplo de $p^{(n+1)!}$ y, a la vez, es estrictamente menor que $p^{(n+1)!}$. La única posibilidad es que $\left|a - b\sum_{k=1}^{n} p^{k!}\right|_\infty = 0$ pero esto no es posible pues habíamos visto que $\left|a - b\sum_{k=1}^{n} p^{k!}\right|_p = p^{-(n+1)!} \neq 0$ y, como consecuencia, $a - b\sum_{k=1}^{n} p^{k!} \neq 0$.
Hemos llegado a una contradicción y, por ende, la sucesión de Cauchy $(x_n)_{n\in\mathbb{N}}$ no puede converger en $\mathbb{Q}$ lo que implica que este último no es completo para ningún valor absoluto no trivial. □

2.2. Construcción de $\mathbb{Q}_p$

Como ya hemos visto en la sección anterior, $\mathbb{Q}$ no es completo respecto de ningún valor absoluto no trivial, por lo que nuestro siguiente objetivo será lograr que lo sea. De este modo, cuando completamos respecto $|\cdot|_p$ lo que obtendremos serán los llamados números p-ádicos, que representaremos por $\mathbb{Q}_p$. En particular, podríamos decir que los números reales son los números ∞-ádicos. La manera en la que vamos a completar $\mathbb{Q}$ es bastante intuitiva. Fijado un número primo p vamos a añadir todos los límites, respecto de $|\cdot|_p$, de cualquier sucesión de Cauchy de números racionales, identificando aquellas que de converger, lo harían hacia el mismo límite.

Definición 2.2.1. *Denotamos por $\mathcal{C} = \mathcal{C}_p(\mathbb{Q})$ al conjunto de todas las sucesiones de Cauchy para $|\cdot|_p$ de elementos de $\mathbb{Q}$, es decir,*

$$\mathcal{C} = \mathcal{C}_p(\mathbb{Q}) = \{(x_n)_{n\in\mathbb{N}} : (x_n)_{n\in\mathbb{N}} \text{ es una sucesión de Cauchy de } \mathbb{Q} \text{ para } |\cdot|_p\}.$$

De ahora en adelante, cuando no haya confusión, omitiremos nombrar el valor absoluto p-ádico para el que una sucesión es de Cauchy. A continuación vamos a probar dos resultados que si bien ya son conocidos en Análisis, es necesario verificar que se cumplen para un valor absoluto p-ádico.

Proposición 2.2.2. *Sean $(x_n)_{n\in\mathbb{N}}, (y_n)_{n\in\mathbb{N}} \in \mathcal{C}$, entonces las operaciones*

$$(x_n)_{n\in\mathbb{N}} + (y_n)_{n\in\mathbb{N}} = (x_n + y_n)_{n\in\mathbb{N}},$$

$$(x_n)_{n\in\mathbb{N}} \cdot (y_n)_{n\in\mathbb{N}} = (x_n y_n)_{n\in\mathbb{N}},$$

hacen que $(\mathcal{C}, +, \cdot)$ sea un anillo conmutativo con unidad.

Demostración. Únicamente vamos a probar que $\mathcal{C}$ es cerrado para las operaciones de suma y producto, siendo el resto de propiedades sencillas de demostrar.
Sean $(x_n)_{n\in\mathbb{N}}, (y_n)_{n\in\mathbb{N}} \in \mathcal{C}$, entonces fijado un $\epsilon > 0$ sabemos que existen $n_0, m_0 \in \mathcal{C}$ tales que

$$|x_n - x_m|_p < \frac{\epsilon}{2}, \quad |y_r - y_s|_p < \frac{\epsilon}{2}$$

para cada $n, m \geq n_0$ y $r, s \geq m_0$. Tomando $N_0 = \text{máx}\{n_0, m_0\}$ y aplicando la desigualdad triangular, se tiene que, para cada $n, m \geq N_0$,

$$|x_n + y_n - x_m - y_m|_p \leq |x_n - x_m|_p + |y_n - y_m|_p \leq \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon,$$

por lo que $(x_n + y_n)_{n\in\mathbb{N}} \in \mathcal{C}$.
Continuando con el producto, en virtud del Lema 2.1.5 sabemos que existe $M > 0$ tal que $|x_n|_p, |y_n|_p \leq M$ para todo $n \in \mathbb{N}$. Fijado un $\epsilon > 0$, existen $n_1, m_1 \in \mathbb{N}$ tales que

$$|x_n - x_m|_p < \frac{\epsilon}{2M}, \quad |y_r - y_s|_p < \frac{\epsilon}{2M}$$

para cada $n, m \geq n_1$ y $r, s \geq m_1$. Tomando $N_1 = \text{máx}\{n_1, m_1\}$ se tendría que, para todo $n, m \geq N_1$,

$$|x_n y_n - x_m y_m|_p = |x_n y_n - x_n y_m + x_n y_m - x_m y_m|_p \leq |x_n(y_n - y_m)|_p + |y_m(x_n - x_m)|_p =$$
$$= |x_n|_p |y_n - y_m|_p + |y_m|_p |x_n - x_m|_p < M\frac{\epsilon}{2M} + M\frac{\epsilon}{2M} = \epsilon,$$

por lo que $(x_n y_n)_{n\in\mathbb{N}} \in \mathcal{C}$. □

Observación 2.2.3. *Aunque no lo hayamos probado en la demostración anterior, es claro que el elemento neutro para la suma es la sucesión constante $(x_n)_{n\in\mathbb{N}} = (0)_{n\in\mathbb{N}}$ y el elemento neutro para el producto es la sucesión constante $(x_n)_{n\in\mathbb{N}} = (1)_{n\in\mathbb{N}}$.*

Nos preguntamos ahora si nuestro nuevo anillo es un dominio o, mejor aún, un cuerpo. Con el siguiente ejemplo veremos que existen divisores del cero distintos del cero y, por tanto, no es dominio y, consecuentemente, tampoco cuerpo.

Ejemplo 2.2.4. *Definimos las sucesiones de números racionales $(x_n)_{n\in\mathbb{N}}$, $(y_n)_{n\in\mathbb{N}}$ dadas por*

$$x_{2n-1} = 0, \quad x_{2n} = p^n,$$

$$y_{2n-1} = p^n, \quad y_{2n} = 0,$$

para cada $n \in \mathbb{N}$. Es claro que $(x_n)_{n\in\mathbb{N}} \cdot (y_n)_{n\in\mathbb{N}} = (0)_{n\in\mathbb{N}}$ y que ninguna de ellas es la sucesión idénticamente nula. Veamos que son de Cauchy:

$$|x_{2n-1}|_p = 0, \quad |x_{2n}|_p = p^{-n} \ \text{ para cada } \ n \in \mathbb{N}.$$

Sea $\epsilon > 0$ cualquiera, sabemos que existe $n_0 \in \mathbb{N}$ tal que

$$\frac{1}{p^n} < \epsilon$$

para todo $n \geq n_0$. Entonces para cada $r, s \geq 2n_0$ se tendría que:

- *Si r, s impares, entonces claramente $|x_r - x_s|_p = |0|_p < \epsilon$.*
- *Si r par y s impar (respect. r impar y s par), $r/2 \geq n_0$ por lo que*

$$|x_r - x_s|_p = |x_r|_p = \left|p^{r/2}\right|_p = \frac{1}{p^{r/2}} < \epsilon.$$

- *Por último, si r y s son pares, supongamos sin pérdida de generalidad que $r < s$. Entonces se tendría que*

$$|x_r - x_s|_p = \left|p^{r/2} - p^{s/2}\right|_p = \left|p^{r/2}(1 - p^{s/2-r/2})\right|_p =$$
$$= \left|p^{r/2}\right|_p \left|1 - p^{s/2-r/2}\right|_p = \left|p^{r/2}\right|_p = \frac{1}{p^{r/2}} < \epsilon,$$

  donde para la penúltima igualdad hemos utilizado que $p \nmid (1 - p^{s/2-r/2})$ y, por tanto, su valor absoluto p-ádico es igual a uno.

Queda claro que la sucesión $(x_n)_{n\in\mathbb{N}}$ es de Cauchy.
Mediante un razonamiento similar se concluye que $(y_n)_{n\in\mathbb{N}}$ también lo es y, como consecuencia, el anillo $\mathcal{C}$ no es un dominio al contener divisores del cero distintos del cero.

Definición 2.2.5. *Se define el subconjunto $\mathcal{N} \subset \mathcal{C}$ como*

$$\mathcal{N} = \{(x_n)_{n\in\mathbb{N}} \in \mathcal{C} : \lim_{n\to\infty} x_n = 0\}.$$

Es sencillo ver, en base a que el producto de una sucesión que converge hacia cero por otra sucesión acotada converge también hacia cero y por el Lema 2.1.6, que el conjunto anteriormente definido es un ideal del anillo $\mathcal{C}$.

Lema 2.2.6. *Sea $(x_n)_{n\in\mathbb{N}} \in \mathcal{C}$ que no tiende hacia cero. Entonces existen $\delta > 0$ y $n_0 \in \mathbb{N}$ tal que $|x_n|_p \geq \delta$ para todo $n \geq n_0$.*

Demostración. Por reducción al absurdo, supongamos que para todo $\delta > 0$ y para cada $n_0 \in \mathbb{N}$, podemos encontrar un $n \geq n_0$ tal que $|x_n|_p < \delta$.
Fijamos un $\epsilon > 0$ cualquiera. Por ser una sucesión de Cauchy, existe $n_0 \in \mathbb{N}$ tal que $|x_n - x_m|_p < \epsilon/2$ para cada $n, m \geq n_0$.
Por otra parte, para ese $\epsilon/2$ y ese $n_0 \in \mathbb{N}$, por lo dicho anteriormente, deberá existir un $N \geq n_0$ tal que $|x_N|_p < \epsilon/2$. Entonces, si $n \geq n_0$:

$$|x_n|_p \leq |x_n - x_N|_p + |x_N|_p < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon,$$

pero esto implicaría que $x_n \xrightarrow[n\to\infty]{} 0$, que es una contradicción. □

Proposición 2.2.7. *El ideal $\mathcal{N} \subset \mathcal{C}$ es maximal.*

Demostración. Supongamos que existe un ideal $\mathcal{M}$ del anillo $\mathcal{C}$ con $\mathcal{N} \subsetneq \mathcal{M}$ y veamos que debe ser entonces $\mathcal{M} = \mathcal{C}$ (o lo que es lo mismo, $1 \in \mathcal{M}$).
Como $\mathcal{N} \subsetneq \mathcal{M}$, debe existir $(x_n)_{n\in\mathbb{N}} \in \mathcal{M}$ que no converge hacia cero. Entonces $\langle (x_n)_{n\in\mathbb{N}}, \mathcal{N}\rangle \subseteq \mathcal{M}$.
En virtud del Lema 2.2.6, deben existir un $\delta > 0$ y un $n_0 \in \mathbb{N}$ tales que

$$|x_n|_p \geq \delta > 0$$

para cada $n \geq n_0$. Esto implica que $x_n \neq 0$ para cada $n \geq n_0$. A partir de esto vamos a definir una sucesión dada por

$$y_n = \begin{cases} 0 & \text{si } n < n_0, \\ 1/x_n & \text{si } n \geq n_0. \end{cases}$$

Lo primero que vamos a ver es que se trata de una sucesión de Cauchy. Para ello vamos a emplear la caracterización de sucesiones de Cauchy que nos proporciona el Lema 2.1.4:

$$\lim_{n\to\infty} |y_{n+1} - y_n|_p = \lim_{\substack{n\to\infty \\ n\geq n_0}} |y_{n+1} - y_n|_p = \lim_{n\to\infty} \left| \frac{1}{x_{n+1}} - \frac{1}{x_n} \right|_p =$$
$$= \lim_{n\to\infty} \frac{|x_n - x_{n+1}|_p}{|x_{n+1}|_p |x_n|_p} \leq \lim_{n\to\infty} \frac{|x_{n+1} - x_n|_p}{\delta^2} = \frac{1}{\delta^2} \lim_{n\to\infty} |x_{n+1} - x_n|_p = 0,$$

por lo que podemos asegurar que $(y_n)_{n\in\mathbb{N}} \in \mathcal{C}$. La sucesión producto $(x_n)_{n\in\mathbb{N}}(y_n)_{n\in\mathbb{N}} \in \langle (x_n)_{n\in\mathbb{N}} \rangle$ es de la forma:

$$x_n y_n = \begin{cases} 0 & \text{si } n < n_0, \\ 1 & \text{si } n \geq n_0. \end{cases}$$

que claramente converge hacia 1. Por tanto, la sucesión $(1 - x_n y_n)_{n\in\mathbb{N}} = (1)_{n\in\mathbb{N}} - (x_n y_n)_{n\in\mathbb{N}} \in \mathcal{N}$ y podemos escribir

$$(1)_{n\in\mathbb{N}} = \overbrace{(x_n y_n)_{n\in\mathbb{N}}}^{\in\langle (x_n)_{n\in\mathbb{N}}\rangle} + \overbrace{((1)_{n\in\mathbb{N}} - (x_n y_n)_{n\in\mathbb{N}})}^{\in\mathcal{N}} \Longrightarrow (1)_{n\in\mathbb{N}} \in \langle ((x_n)_{n\in\mathbb{N}}, \mathcal{N}\rangle \subseteq \mathcal{M},$$

que es exactamente lo que queríamos probar. □

La idea que hay detrás de los resultados anteriores es usar el ideal $\mathcal{N}$ para identificar entre sí las diferentes sucesiones de $\mathcal{C}$ que deberían converger hacia un mismo límite, es decir, aquellas cuya diferencia se va haciendo cada vez más y más pequeña hasta converger a cero.

Ya tenemos entonces todos los ingredientes que nos van a permitir definir un nuevo cuerpo que completará a $\mathbb{Q}$ respecto del valor absoluto p-ádico.

Definición 2.2.8. *Se define el* cuerpo de los números p-ádicos*, denotado por $\mathbb{Q}_p$, como*

$$\mathbb{Q}_p = {}^{\mathcal{C}}\!/_{\mathcal{N}}\,.$$

No debe llevarnos a confusión el nombre de *números p-ádicos* ya que, en realidad, los elementos de $\mathbb{Q}_p$ no son números como tal, si no clases de equivalencia de sucesiones de Cauchy en $\mathbb{Q}$.

A continuación, vamos a probar que este cuerpo, junto con un valor absoluto adecuado que definiremos en las siguientes líneas, completa a $\mathbb{Q}$.

Lema 2.2.9. *Sea $(x_n)_{n\in\mathbb{N}}$ una sucesión de Cauchy que no converge hacia cero. Entonces existe un $n_0 \in \mathbb{N}$ tal que $|x_n|_p = |x_m|_p$ para todo $n, m \geq n_0$.*

Demostración. Por el Lema 2.2.6, sabemos que existe un $\delta > 0$ y un $n_1 \in \mathbb{N}$ tal que

$$|x_n|_p \geq \delta > 0$$

para cada $n \geq n_1$. Por otro lado, como $(x_n)_{n\in\mathbb{N}}$ es de Cauchy, existe un $n_2 \in \mathbb{N}$ tal que

$$|x_n - x_m|_p < \delta$$

para cada $n, m \geq n_2$. Tomando $n_0 = \text{máx}\{n_1, n_2\}$, se tiene que

$$|x_n - x_m|_p < \delta \leq \text{máx}\{|x_n|_p, |x_m|_p\}$$

para cada $n, m \geq n_0$. Atendiendo a esto último, si existiesen $n, m \geq n_0$ tales que $|x_n|_p \neq |x_m|_p$, entonces, en virtud de la Proposición 1.3.5,

$$\delta > |x_n - x_m|_p = |x_n + (-x_m)|_p = \text{máx}\{|x_n|_p, |-x_m|_p\} = \text{máx}\{|x_n|_p, |x_m|_p\} \geq \delta,$$

llegando a una contradicción. Se concluye que $|x_n|_p = |x_m|_p$ para cada $n, m \geq n_0$. □

Lema 2.2.10. *Sea $(x_n)_{n\in\mathbb{N}}$ una sucesión de Cauchy que converge hacia cero. Entonces $\lim_{n\to\infty} |x_n|_p$ existe y vale cero.*

Demostración. Fijado un $\epsilon > 0$, existe un $n_0 \in \mathbb{N}$ tal que

$$|x_n|_p < \epsilon$$

para cada $n \geq n_0$. Como $||x_n|_p|_\infty = |x_n|_p$, entonces claramente $\lim_{n\to\infty} |x_n|_p = 0$. □

Lema 2.2.11. *Sean $\lambda \in \mathbb{Q}_p$ y $(x_n)_{n\in\mathbb{N}}, (y_n)_{n\in\mathbb{N}} \in \mathcal{C}$ dos representantes distintos de λ. Entonces*

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

Demostración. Sea $\lambda \in \mathbb{Q}_p$ y $(x_n)_{n\in\mathbb{N}}, (y_n)_{n\in\mathbb{N}} \in \mathcal{C}$ dos representantes distintos de λ, es decir, $\lim_{n\to\infty} x_n - y_n = 0$. Entonces,

$$\lim_{n\to\infty} |x_n - y_n|_p = 0.$$

Aplicando el Lema 1.1.5, se tiene que

$$0 \leq ||x_n|_p - |y_n|_p|_\infty \leq |x_n - y_n|_p \Longrightarrow \lim_{n\to\infty} (|x_n|_p - |y_n|_p) = 0,$$

que es lo mismo que decir que $\lim_{n\to\infty} |x_n|_p = \lim_{n\to\infty} |y_n|_p$. □

Gracias a estos tres lemas, vamos a poder definir un valor absoluto en $\mathbb{Q}_p$ que, adelantamos ya, hará que $\mathbb{Q}_p$ sea completo. Recordemos que $\mathbb{Q}_p$ es un cociente, por ello, cada vez que nos refiramos a un elemento $\lambda \in \mathbb{Q}_p$, realmente estamos hablando de una clase de equivalencia formada por sucesiones de Cauchy con la condición de que la diferencia de dos cualesquiera de ellas converja hacia cero.

Definición 2.2.12. *Sea $\lambda \in \mathbb{Q}_p$ y $(x_n)_{n\in\mathbb{N}}$ es un representante de dicha clase, entonces definimos $|\lambda|_p$ como*

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

Aunque la notación sea la misma, no debemos confundir el valor absoluto p-ádico definido para los números racionales con este nuevo valor absoluto, definido para números p-ádicos. Tenemos mucho que probar aquí. Nuestro objetivo final será ver que $(\mathbb{Q}_p, |\cdot|_p)$ es el completado de $\mathbb{Q}$. Pero antes debemos ver que la definición anterior nos proporciona un valor absoluto no arquimediano sobre $\mathbb{Q}_p$.

Proposición 2.2.13. *La aplicación $|\cdot|_p : \mathbb{Q}_p \longrightarrow \mathbb{R}_+$ es un valor absoluto no arquimediano.*

Demostración. Recordemos que un elemento $\lambda \in \mathbb{Q}_p$ es el cero si, y solo si, algún representante suyo está en $\mathcal{N}$ (aunque de estar uno, lo están todos).
Sea $\lambda \in \mathbb{Q}_p$ y $(x_n)_{n\in\mathbb{N}}$ un representante de dicha clase. Supongamos que $|\lambda|_p = \lim_{n\to\infty} |x_n|_p = 0$ y recordemos que dicho límite es respecto del valor absoluto usual en $\mathbb{R}$. Entonces, fijado un $\epsilon > 0$ cualquiera, existe $n_0 \in \mathbb{N}$ tal que

$$||x_n|_p|_\infty = |x_n|_p < \epsilon \quad \text{para todo } n \geq n_0.$$

y, en consecuencia, $(x_n)_{n\in\mathbb{N}} \in \mathcal{N}$ y $\lambda = 0$.
Recíprocamente, si $\lambda = 0$, significa que $\lim_{n\to\infty} x_n = 0$ y, por el Lema 2.2.10,

$$|\lambda|_p = \lim_{n\to\infty} |x_n|_p = 0.$$

Continuando con el producto, sean $\lambda, \mu \in \mathbb{Q}_p$ y $(x_n)_{n\in\mathbb{N}}, (y_n)_{n\in\mathbb{N}} \in \mathcal{C}$ sendos representantes de sus clases. Entonces,

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

Por último vamos a probar la propiedad no arquimediana que, como ya hemos visto a lo largo de este texto, es más fuerte que la desigualdad triangular. De nuevo, sean $\lambda, \mu \in \mathbb{Q}_p$ y $(x_n)_{n\in\mathbb{N}}, (y_n)_{n\in\mathbb{N}} \in \mathcal{C}$ representantes de las respectivas clases. Entonces,

$$|\lambda + \mu|_p = \lim_{n\to\infty} |x_n + y_n|_p \leq \lim_{n\to\infty} \text{máx}\{|x_n|_p, |y_n|_p\} =$$
$$\text{máx}\{\lim_{n\to\infty} |x_n|_p, \lim_{n\to\infty} |y_n|_p\} = \text{máx}\{|\lambda|_p, |\mu|_p\}.$$

□

Ya tenemos el primer paso. Ahora vamos a definir una inclusión de $\mathbb{Q}$ en $\mathbb{Q}_p$ de manera que satisfaga las condiciones de la Definición 2.1.3.

Proposición 2.2.14. *La aplicación $i : \mathbb{Q} \longrightarrow \mathbb{Q}_p$ dada por $i(x) = \lambda_x$, siendo λ_x la clase de la sucesión constante $(x)_{n\in\mathbb{N}}$, es inyectiva y cumple que*

$$|x|_p = |i(x)|_p \quad \textit{para cada } \ x \in \mathbb{Q}.$$

Demostración. Comenzando por la inyectividad, sean $x, y \in \mathbb{Q}$ distintos y supongamos que $i(x) = i(y)$. Esto quiere decir que las sucesiones constantes $(x)_{n\in\mathbb{N}}$ y $(y)_{n\in\mathbb{N}}$ pertenecen a la misma clase de $\mathbb{Q}_p$. Por tanto, la sucesión resta de ambas debe estar en $\mathcal{N}$. Como $(x-y)_{n\in\mathbb{N}}$ es una sucesión constante, converge hacia $x - y \in \mathbb{Q}$, por lo que debe ser $x = y$ y hemos llegado a una contradicción.
La segunda parte es inmediata. Dado un $x \in \mathbb{Q}$ cualquiera, entonces $i(x)$ tiene a $(x)_{n\in\mathbb{N}}$ como representante, por tanto,

$$|i(x)|_p = \lim_{n\to\infty} |x|_p = |x|_p.$$

□

Proposición 2.2.15. *Para todo $\lambda \in \mathbb{Q}_p$ no nulo, existe $m \in \mathbb{Z}$ tal que $|\lambda|_p = p^{-m}$.*

Demostración. Sea $\lambda \in \mathbb{Q}_p \setminus \{0\}$ y $(x_n)_{n\in\mathbb{N}}$ un representante suyo. Entonces sabemos por el Lema 2.2.9 que existe un $n_0 \in \mathbb{N}$ tal que $|x_n|_p$ converge hacia $|x_{n_0}|_p = p^{-v_p(x_{n_0})} = p^{-m}$ con $m \in \mathbb{Z}$. Teniendo en cuenta como se define $|\lambda|_p$, concluimos que $|\lambda|_p = \lim_{n\to\infty} |x_n|_p = |x_{n_0}|_p = p^{-m}$ para cierto $m \in \mathbb{Z}$. □

Siguiendo la Definición 2.1.3, el siguiente paso será probar que $i(\mathbb{Q})$ es denso en $\mathbb{Q}$ para la topología métrica generada por $|\cdot|_p$.

Proposición 2.2.16. *El conjunto $i(\mathbb{Q})$ es denso en $\mathbb{Q}_p$ para la topología generada por $|\cdot|_p$.*

Demostración. Recordemos que $\mu \in i(\mathbb{Q}) \iff \mu = (x)_{n\in\mathbb{N}}$ para algún $x \in \mathbb{Q}$.
Fijamos $\lambda \in \mathbb{Q}_p$ y $r > 0$. Vamos a ver que, entonces, existe un elemento de $i(\mathbb{Q})$ en la bola $B(\lambda, r)$. Sea $(x_n)_{n\in\mathbb{N}}$ un representante de la clase λ y $\epsilon < r$ positivo. Como $(x_n)_{n\in\mathbb{N}}$ es de Cauchy, sabemos que existe $n_0 \in \mathbb{N}$ tal que

$$|x_n - x_m|_p < \epsilon$$

para cada $n, m \geq n_0$.
Sea $\mu \in \mathbb{Q}_p$ la clase a la que pertenece la sucesión constante $((x_{n_0})_{n\in\mathbb{N}})$, es decir, $\mu = i(x_{n_0})$. Entonces, $(x_n - x_{n_0})_{n\in\mathbb{N}}$ es un representante de la clase $\lambda - \mu$ y se tiene que

$$|\lambda - \mu|_p = \lim_{n\to\infty} |x_n - x_{n_0}|_p = \lim_{\substack{n\to\infty \\ n\geq n_0}} |x_n - x_{n_0}|_p \leq \epsilon < r.$$

Por tanto, $\mu = (x_{n_0})_{n\in\mathbb{N}} \in i(\mathbb{Q}) \cap B(\lambda, r)$.
Como toda bola abierta y no vacía del espacio $(\mathbb{Q}_p, |\cdot|_p)$ tiene intersección no vacía con $i(\mathbb{Q})$, se concluye que $i(\mathbb{Q})$ es denso en $(\mathbb{Q}_p, |\cdot|_p)$. □

Observación 2.2.17. *Nótese que hemos necesitado tomar $\epsilon < r$ ya que las desigualdades estrictas no necesariamente se conservan bajo el límite. Basta pensar en la sucesión, en $(\mathbb{R}, |\cdot|_\infty)$, dada por $(1-1/n)_{n\in\mathbb{N}}$, que es estrictamente menor que 1 en todos sus términos pero su límite es 1.*

Por último, nos queda probar que el cuerpo $\mathbb{Q}_p$ es completo respecto del valor absoluto $|\cdot|_p$.

Proposición 2.2.18. *$\mathbb{Q}_p$ es completo respecto del valor absoluto $|\cdot|_p$.*

Demostración. Sea $(\lambda_m)_{m\in\mathbb{N}}$ una sucesión de Cauchy de elementos de $\mathbb{Q}_p$ para el valor absoluto $|\cdot|_p$. Veamos que tiene límite en dicho cuerpo.
Por la densidad de $i(\mathbb{Q})$ sabemos que, para cada $m \in \mathbb{N}$, existe una sucesión $i(x_n^{(m)}) \subseteq i(\mathbb{Q})$ tal que

$$\lambda_m = \lim_{n\to\infty} i(x_n^{(m)}).$$

Entonces, por lo anterior, para cada $m \in \mathbb{N}$, existe un $N_m \in \mathbb{N}$ tal que

$$\left|\lambda_m - i(x_n^{(m)})\right|_p < \frac{1}{m} \tag{2.1}$$

para cada $n \geq N_m$. Construimos una sucesión de subíndices tomando, para cada $m \in \mathbb{N}$, un $j_m > N_m$ y lo podemos hacer de forma que

$$j_1 < j_2 < \ldots < j_m < \ldots .$$

Definimos la sucesión de números racionales $l_n = x_n^{(j_n)}$. Veamos primero que es de Cauchy en $\mathbb{Q}$.
Fijamos un $\epsilon > 0$, como $(\lambda_m)_{m\in\mathbb{N}}$ es de Cauchy en $\mathbb{Q}_p$, existe $N_1 \in \mathbb{N}$ tal que

$$|\lambda_r - \lambda_s|_p < \frac{\epsilon}{3}$$

para cada $r, s > N_1$. Por otro lado, por la forma en la que hemos escogido los j_n se tiene

$$\left|\lambda_r - i(x_{j_r}^{(r)})\right|_p < \frac{1}{r}, \quad \left|\lambda_s - i(x_{j_s}^{(s)})\right|_p < \frac{1}{s}.$$

Así pues, para todo $r, s > 3/\epsilon$ tendríamos que .

$$\left|\lambda_r - i(x_{j_r}^{(r)})\right|_p < \frac{1}{r} < \frac{\epsilon}{3}, \quad \left|\lambda_s - i(x_{j_s}^{(s)})\right|_p < \frac{1}{s} < \frac{\epsilon}{3}.$$

Por tanto, para cada $r, s > N_0 = \text{máx}\{N_1, 3/\epsilon\}$ se cumple, en virtud de la desigualdad triangular,

$$\begin{aligned} |l_r - l_s|_p = \left|x_{j_r}^{(r)} - x_{j_s}^{(s)}\right|_p = \left|i(x_{j_r}^{(r)}) - i(x_{j_s}^{(s)})\right|_p = \\ = \left|\left(i(x_{j_r}^{(r)}) - \lambda_r\right) + (\lambda_r - \lambda_s) + \left(\lambda_s - i(x_{j_s}^{(s)})\right)\right|_p \leq \\ \leq \left|i(x_{j_r}^{(r)}) - \lambda_r\right|_p + |\lambda_r - \lambda_s|_p + \left|\lambda_s - i(x_{j_s}^{(s)})\right|_p \leq 3 \cdot \frac{\epsilon}{3} = \epsilon. \end{aligned}$$

Ya hemos probado que $(l_n)_{n\in\mathbb{N}}$ es una sucesión de Cauchy en $\mathbb{Q}$, por tanto, podemos considerar su clase $\mu \in \mathbb{Q}_p$.
Primeramente, para cada $m \in \mathbb{N}$, se tiene que

$$\left|\mu - i(x_{j_m}^{(m)})\right|_p = \lim_{n\to\infty} |l_n - l_m|_p$$

y, como la sucesión es de Cauchy, existe $N_2 \in \mathbb{N}$ tal que

$$|l_n - l_m|_p < \frac{\epsilon}{2}$$

para cada $n, m > N_2$. De aquí obtenemos que, tomando $m > N_2$,

$$\left|\mu - i(x_{j_m}^{(m)})\right|_p = \lim_{n\to\infty} |l_n - l_m|_p = \lim_{\substack{n\to\infty \\ n>N_2}} |l_n - l_m|_p \leq \frac{\epsilon}{2}.$$

Por otro lado, usando (2.1),

$$\left|\lambda_m - i(x_{j_m}^{(m)})\right|_p < \frac{1}{m} < \frac{\epsilon}{2}$$

para cada $m > 2/\epsilon$.
Entonces, para cada $m > \text{máx}\{N_2, 2/\epsilon\}$,

$$|\mu - \lambda_m|_p = \left|\left(\mu - i(x_{j_m}^{(m)})\right) + \left(i(x_{j_m}^{(m)}) - \lambda_m\right)\right|_p \leq$$
$$\left|\mu - i(x_{j_m}^{(m)})\right|_p + \left|i(x_{j_m}^{(m)}) - \lambda_m\right|_p \leq 2 \cdot \frac{\epsilon}{2} = \epsilon.$$

Por tanto, la clase $\mu \in \mathbb{Q}_p$ es el límite de la sucesión de Cauchy $(\lambda_m)_{m\in\mathbb{N}}$. □

Lema 2.2.19. *Sea $(x_n)_{n\in\mathbb{N}}$ una sucesión de Cauchy en $\mathbb{Q}$. Se tiene que*

$$\left|\lim_{n\to\infty} i(x_n)\right|_p = \lim_{n\to\infty} |x_n|_p,$$

donde el valor absoluto de la izquierda es aquel de la Definición 2.2.12 y el de la derecha el valor absoluto p-ádico en $\mathbb{Q}$.

Demostración. Como $(x_n)_{n\in\mathbb{N}}$ es una sucesión de Cauchy en $\mathbb{Q}$, el Lema 2.2.9 y el Lema 2.2.10 nos aseguran que la sucesión $(|x_n|_p)_{n\in\mathbb{N}}$ converge en $(\mathbb{R}, |\cdot|_\infty)$. La sucesión $(i(x_n))_{n\in\mathbb{N}}$ de $\mathbb{Q}_p$ es claramente de Cauchy pues

$$|i(x_n) - i(x_m)|_p = |i(x_n - x_m)|_p = |x_n - x_m|_p.$$

La Proposición 2.2.18 nos asegura que $(i(x_n))_{n\in\mathbb{N}}$ es convergente en $\mathbb{Q}_p$. Además, es claro que $\lim_{n\to\infty} |x_n|_p = \lim_{n\to\infty} |i(x_n)|_p$.
En virtud de la Proposición 1.3.8 se tiene que $\lim_{n\to\infty} |i(x_n)|_p = |\lim_{n\to\infty} i(x_n)|_p$. Concluimos que

$$\left|\lim_{n\to\infty} i(x_n)\right|_p = \lim_{n\to\infty} |x_n|_p.$$

□

Observación 2.2.20. *Notemos que si tenemos un cuerpo cualquiera $\mathbb{K}$ con un valor absoluto no arquimediano $|\cdot|$ definido en él y un homomorfismo de inclusión $j : \mathbb{K} \hookrightarrow \mathbb{Q}_p$ satisfaciendo que $j(\mathbb{K})$ es denso en $\mathbb{Q}_p$, entonces el resultado anterior es igualmente cierto para cualquier sucesión de Cauchy de $\mathbb{K}$.*

Los resultados anteriores nos permiten demostrar el siguiente teorema que será de gran importancia de ahora en adelante, ya que nos permitirá trabajar con $\mathbb{Q}_p$ olvidando la construcción.

Teorema 2.2.21. *Para cada primo $p \in \mathbb{Z}^+$ existe un cuerpo $\mathbb{Q}_p$ con un valor absoluto no arquimediano $|\cdot|_p$ cumpliendo que*

1) existe un homomorfismo de cuerpos inyectivo $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$, y el valor absoluto inducido por $|\cdot|_p$ en $\mathbb{Q}$ a través de esa inclusión es el valor absoluto p-ádico;

2) la imagen de $\mathbb{Q}$ por esa inclusión es densa en $\mathbb{Q}_p$;

3) $\mathbb{Q}_p$ es completo respecto del valor absoluto $|\cdot|_p$.

El cuerpo $\mathbb{Q}_p$ satisfaciendo 1), 2) y 3) es único salvo el isomorfismo que preserva los valores absolutos.

Demostración. Las afirmaciones *1), 2)* y *3)* ya han sido probadas en las Proposiciones 2.2.14, 2.2.15, 2.2.16, 2.2.18 respectivamente. Solo nos queda probar la unicidad.
Sea $\mathbb{K}$ otro cuerpo con un valor absoluto no arquimediano $|\cdot|_K$ definido en él que satisface las condiciones *1), 2)* y *3)* y denotemos por

$$i : \mathbb{Q} \longrightarrow \mathbb{Q}_p,$$
$$j : \mathbb{Q} \longrightarrow \mathbb{K},$$

a los dos homomorfismos inyectivos. Veamos que la aplicación $f : \mathbb{Q}_p \longrightarrow \mathbb{K}$, que cumple $|f(i(x)|_p = |j(x)|_K$ para todo $x \in \mathbb{Q}$, está bien definida y es un isomorfismo.
Tomamos $\lambda \in \mathbb{Q}_p$. Hay dos posibilidades:
Si $\lambda \in i(\mathbb{Q})$, entonces un representante de λ sería la sucesión constante $(x)_{n\in\mathbb{N}}$ para algún $x \in \mathbb{Q}$ y definimos $f(\lambda) := j(x)$.
En otro caso, por la propiedad *2)*, debe existir una sucesión $(x_n)_{n\in\mathbb{N}}$ de $\mathbb{Q}$ tal que

$$\lambda = \lim_{n\to\infty} i(x_n). \tag{2.2}$$

Como toda sucesión convergente es de Cauchy, $(i(x_n))_{n\in\mathbb{N}}$ es de Cauchy y, como $|i(x)|_p = |x|_p = |j(x)|_K$ para todo $x \in \mathbb{Q}$, para cada $n, m \in \mathbb{N}$ se tiene que

$$|i(x_n) - i(x_m)|_p = |i(x_n - x_m)|_p = |x_n - x_m|_p = |j(x_n - x_m)|_K = |j(x_n) - j(x_m)|_K$$

y la sucesión $(j(x_n))_{n\in\mathbb{N}}$ también es de Cauchy en $\mathbb{K}$.
Como $\mathbb{K}$ es completo por la propiedad *3)*, la anterior sucesión tiene límite. Definimos entonces la imagen de λ como

$$f(\lambda) := \lim_{n\to\infty} j(x_n).$$

Antes de continuar, debemos ver que f está bien definida. Tomemos un elemento $\lambda \in \mathbb{Q}_p$ y dos representantes suyos $(a_n)_{n\in\mathbb{N}}$ y $(b_n)_{n\in\mathbb{N}}$.

- Si $\lambda \in i(\mathbb{Q})$, entonces necesariamente existe $a \in \mathbb{Q}$ tal que $a_n = a = b_n$ para todo $n \in \mathbb{N}$ por lo que no hay problemas.
- Si $\lambda \in \mathbb{Q}_p \setminus i(\mathbb{Q})$, sean $(x_n)_{n\in\mathbb{N}}$, $(y_n)_{n\in\mathbb{N}}$ dos sucesiones de $\mathbb{Q}$ tales que

$$\lim_{n\to\infty} i(x_n) = \lim_{n\to\infty} i(y_n) = \lambda.$$

Queremos ver que $\lim_{n\to\infty} j(x_n) = \lim_{n\to\infty} j(y_n)$. Notemos que

$$|j(x_n)-j(y_n)|_K = |j(x_n-y_n)|_K = |x_n-y_n|_p = |i(x_n-y_n)|_p = |i(x_n)-i(y_n)|_p \xrightarrow[n\to\infty]{} 0.$$

Por tanto, $f(\lambda)$ no depende de la sucesión de $\mathbb{Q}$ escogida.

Veamos ahora que $|f(\lambda)|_K = |\lambda|_p$ para todo $\lambda \in \mathbb{Q}_p$. Por un lado, si $\lambda \in i(\mathbb{Q})$,

$$|\lambda|_p = |i(x)|_p = |x|_p = |j(x)|_K = |f(\lambda)|_K.$$

Por el contrario, si $\lambda = \lim_{n\to\infty} i(x_n) \in \mathbb{Q}_p \setminus i(\mathbb{Q})$ cualquiera, entonces por el Lema 2.2.19 y la Observación 2.2.20,

$$|\lambda|_p = \left|\lim_{n\to\infty} i(x_n)\right|_p = \lim_{n\to\infty} |i(x_n)|_p = \lim_{n\to\infty} |j(x_n)|_K = \left|\lim_{n\to\infty} j(x_n)\right|_K = \\ = |f(\lambda)|_K .$$

Por tanto, la aplicación f conserva el valor absoluto. En particular, al conservar el valor absoluto, es claramente continua ya que para cada $\epsilon > 0$, tomando $\delta = \epsilon > 0$, si $|\lambda - \mu|_p < \delta$, entonces $|f(\lambda) - f(\mu)|_K = |f(\lambda - \mu)|_K = |\lambda - \mu|_p < \epsilon$.

Veamos que es un homomorfismo de cuerpos usando, para ello, el Lema 2.1.6.
Sean $\alpha, \beta \in \mathbb{Q}_p$, sabemos que existen sucesiones $(x_n)_{n\in\mathbb{N}}, (y_n)_{n\in\mathbb{N}}$ de $\mathbb{Q}$ tales que $\alpha = \lim_{n\to\infty} i(x_n)$, $\beta = \lim_{n\to\infty} i(y_n)$. Atendiendo a la continuidad de f:

$$f(\alpha+\beta) = f\left(\lim_{n\to\infty} i(x_n) + \lim_{n\to\infty} i(y_n)\right) = f\left(\lim_{n\to\infty} (i(x_n) + i(y_n))\right) = \\ = f\left(\lim_{n\to\infty} i(x_n+y_n)\right) = \lim_{n\to\infty} f(i(x_n+y_n)) = \lim_{n\to\infty} j(x_n+y_n) = \lim_{n\to\infty} (j(x_n)+j(y_n)) = \\ = \lim_{n\to\infty} j(x_n) + \lim_{n\to\infty} j(y_n) = \lim_{n\to\infty} f(i(x_n)) + \lim_{n\to\infty} f(i(y_n)) = f\left(\lim_{n\to\infty} i(x_n)\right) + f\left(\lim_{n\to\infty} i(y_n)\right) = \\ = f(\alpha) + f(\beta).$$

De la misma forma se prueba que $f(\alpha\beta) = f(\alpha)f(\beta)$. Tomando ahora dos elementos inversos el uno del otro, $\lambda, \lambda^{-1} \in \mathbb{Q}_p$, se tiene que

$$f(1_{\mathbb{Q}_p}) = f(\lambda\lambda^{-1}) = f(\lambda)f(\lambda)^{-1} = 1_{\mathbb{K}},$$

por tanto f es un homomorfismo de cuerpos.
La inyectividad está clara por ser f un homomorfismo de cuerpos no nulo pues $\ker(f)$ es un ideal de un cuerpo que no es el total y, por tanto, $\ker(f) = \{0\}$.
Queremos ver ahora que f es sobreyectiva. Para ello usaremos un razonamiento inverso al que habíamos empleado para su definición. Sea $\mu \in \mathbb{K}$. Como $j(\mathbb{Q})$ es denso en $\mathbb{K}$,

debe existir una sucesión $(x_n)_{n\in\mathbb{N}}$ de racionales tal que $\mu = \lim_{n\to\infty} j(x_n)$ y, como $\mathbb{Q}_p$ es completo, $\lim_{n\to\infty} i(x_n)$ existe y lo llamamos $\lambda \in \mathbb{Q}_p$. Entonces, por como habíamos definido f, tenemos que $f(\lambda) = \mu$ y f es sobreyectiva.
Por último, notemos que $j : \mathbb{Q} \longrightarrow \mathbb{K}$ es continua al preservar el valor absoluto de cada elemento de $x \in \mathbb{Q}$. Si vemos a $\mathbb{Q}$ como un subconjunto denso de $\mathbb{Q}_p$, entonces existe una única extensión de la inclusión j al cuerpo $\mathbb{Q}_p$, que es precisamente la aplicación f. Si tuviésemos otro isomorfismo, $g : \mathbb{Q}_p \longrightarrow \mathbb{K}$, preservando los valores absolutos, entonces es una aplicación continua. Además, como g es isomorfismo, $g(1_{\mathbb{Q}_p}) = 1_{\mathbb{K}} = j(1_{\mathbb{Q}_p})$, por tanto $g_{|\mathbb{Z}} = j_{|\mathbb{Z}}$ y, en consecuencia, $g_{|\mathbb{Q}} = j$. Por tanto, la aplicación g es continua y extiende a j, por lo que necesariamente $g = f$, concluyendo así la demostración. □

Capítulo 3

Primeras propiedades de $\mathbb{Q}_p$

En el capítulo anterior definimos el cuerpo de los números p-ádicos como una compleción de $\mathbb{Q}$ respecto del valor absoluto p-ádico.

En este nuevo capítulo nos adentraremos en las propiedades de $\mathbb{Q}_p$, estudiando su estructura algebraica, su topología, la representación de sus elementos y finalizaremos con dos versiones del Lema de Hensel. También enunciaremos el Teorema de Hasse-Minkowski con el fin de plantear una utilidad práctica de los números p-ádicos.

3.1. Estructura algebraica y topológica de $\mathbb{Q}_p$

El objetivo de esta sección será explorar la estructura algebraica de los números p-ádicos. Para ello vamos a particularizar lo visto en la sección 1.4 al cuerpo $\mathbb{Q}_p$ con el valor absoluto no arquimediano $|\cdot|_p$. A su vez, también hablaremos de la topología métrica que induce el valor absoluto $|\cdot|_p$ en $\mathbb{Q}_p$.

Comenzamos introduciendo un nuevo tipo de notación que recalca el hecho de que podemos ver al cuerpo de los racionales $\mathbb{Q}$ como un subcuerpo de $\mathbb{Q}_p$ gracias a los resultados vistos en la sección anterior.

Notación 3.1.1. *De ahora en adelante, para cada $\alpha \in \mathbb{Q}$, entenderemos por α a la sucesión constante $i(\alpha) = (\alpha, \alpha, ..., \alpha, ...)$, es decir, cuando hablemos de $\alpha \in \mathbb{Q}$ y $\alpha \in \mathbb{Q}_p$ en un mismo enunciado, nos estaremos refiriendo a un número racional en el primer caso y a la sucesión constante en $\mathbb{Q}_p$ en el segundo, aunque los trataremos indistintamente gracias a lo visto en las proposiciones 2.2.14 y 2.2.15.*

Definición 3.1.2. *El anillo de valoración de $|\cdot|_p$ sobre el cuerpo $\mathbb{Q}_p$,*

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

recibe el nombre de enteros p-ádicos.

Claramente $\mathbb{Z}_p$ es un caso particular de lo ya visto en la sección 1.4, por lo que ya conocemos algunas de sus propiedades derivadas de la topología métrica generada por un valor absoluto no arquimediano. La siguiente colección de proposiciones son importantes y dan lugar a una serie de consecuencias implícitas que más tarde detallaremos.

Lema 3.1.3. *Sea $p \in \mathbb{Z}$ primo y $n \geq 1$. Si $\mathrm{mcd}(a,p) = 1$, entonces la ecuación $ax \equiv 1 \pmod{p^n}$ tiene solución.*

Demostración. Como $\mathrm{mcd}(a,p) = 1$, entonces para cada $n \in \mathbb{N}$, $\mathrm{mcd}(a,p^n) = 1$. Por la Identidad de Bézout, sabemos que existen $r, s \in \mathbb{Z}$ tales que

$$ra + sp^n = 1 \Longrightarrow ra - 1 = -sp^n \Longrightarrow ra \equiv 1 \pmod{p^n}$$

y ese $r \in \mathbb{Z}$ resuelve la ecuación. □

De ahora en adelante denotaremos por $p\mathbb{Z}_p$ al ideal del anillo $\mathbb{Z}_p$ generado por p. Notemos que si $x \in \mathbb{Z}_p$, entonces

$$x \in p\mathbb{Z}_p \Longleftrightarrow \exists y \in \mathbb{Z}_p \text{ tal que } \frac{x}{p} = y \Longleftrightarrow \left|\frac{x}{p}\right|_p = \frac{|x|_p}{|p|_p} \leq 1 \Longleftrightarrow |x|_p \leq \frac{1}{p}.$$

Proposición 3.1.4. *El anillo $\mathbb{Z}_p$ es un anillo local cuyo ideal maximal es $p\mathbb{Z}_p$.*

Demostración. Primeramente, $\mathbb{Z}_p$ es un anillo de valoración y, por la Proposición 1.6.17, es un anillo local. Además, por la Proposición 1.4.2, $B(0,1) = \{x \in \mathbb{Q}_p : |x|_p < 1\}$ es su ideal maximal. Queremos ver ahora que $B(0,1) = p\mathbb{Z}_p$.
Si $x \in B(0,1)$, por la Proposición 2.2.15, existe $n \in \mathbb{Z}$ tal que $|x|_p = p^{-n} < 1$ por lo que debe ser $n \geq 1$, lo que implica que $|x|_p = p^{-n} \leq 1/p$ y, por tanto, $x \in p\mathbb{Z}_p$.
Hemos probado que $B(0,1) \subseteq p\mathbb{Z}_p$. Como $B(0,1)$ es maximal, las únicas opciones son $p\mathbb{Z}_p = \mathbb{Z}_p$ o $B(0,1) = p\mathbb{Z}_p$. Notemos que la primera de ellas es imposible ya que $|1/p|_p = p > 1$, por lo que $1 \notin p\mathbb{Z}_p$. Concluimos que $B(0,1) = p\mathbb{Z}_p$. □

Proposición 3.1.5. *Se cumple que*

$$\mathbb{Q} \cap \mathbb{Z}_p = \mathbb{Z}_{(p)} := \left\{\frac{a}{b} \in \mathbb{Q} : v_p(a) - v_p(b) \geq 0\right\}.$$

Demostración. Es inmediato. □

Proposición 3.1.6. *Dado $x \in \mathbb{Z}_p$ y $n \geq 1$, existe un único $\alpha \in \mathbb{Z}$ con $0 \leq \alpha \leq p^n - 1$ tal que $|x - \alpha|_p \leq p^{-n}$.*

Demostración. Tomamos $x \in \mathbb{Z}_p$ y fijamos un $n \geq 1$. Como $\mathbb{Q}$ es denso en $\mathbb{Q}_p$, sabemos que existe un elemento de $\mathbb{Q}$ tan cercano a x como queramos. En particular, existe $a/b \in \mathbb{Q}$ tal que

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

Primeramente, por tratarse de un valor absoluto no arquimediano,

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

Por la Proposición 3.1.5, $a/b \in \mathbb{Z}_{(p)}$. Podemos asumir entonces que $p \nmid b$. Aplicando ahora el Lema 3.1.3, existe $c \in \mathbb{Z}$ tal que $bc \equiv 1 \pmod{p^n}$, es decir, $p^n \mid (1-bc)$. Se tiene entonces que

$$\left|\frac{a}{b} - ac\right|_p = \left|\frac{a-abc}{b}\right|_p = p^{v_p(b)-v_p(a-abc)} = p^{-v_p(a-abc)} = p^{-v_p(a(1-bc))} \leq p^{-n}.$$

Por tanto, hemos encontrado un entero, $ac \in \mathbb{Z}$, tal que

$$|x-ac|_p = \left|x - \frac{a}{b} + \frac{a}{b} - ac\right|_p \leq \text{máx}\left\{\left|x-\frac{a}{b}\right|_p, \left|\frac{a}{b}-ac\right|_p\right\} \leq p^{-n}.$$

Nos falta ver que podemos tomarlo en entre cero y $p^n - 1$ pero esto es inmediato ya que existe un único $\alpha \in \mathbb{Z}$ con $0 \leq \alpha \leq p^n - 1$ y $\alpha \equiv ac \pmod{p^n}$, es decir, $p^n \mid (ac - \alpha)$ y en consecuencia $|ac-\alpha|_p \leq p^{-n}$. Se tiene entonces que

$$|x-\alpha|_p = |x - ac + ac - \alpha|_p \leq \text{máx}\{|x-ac|_p, |ac-\alpha|_p\} \leq p^{-n},$$

y ya hemos encontrado el entero α satisfaciendo las dos hipótesis.
Además, si existiese otro entero β con $0 \leq \beta \leq p^n - 1$, $\beta \neq \alpha$ y $|x-\beta|_p \leq p^{-n}$. De las dos primeras condiciones que cumple β junto con el hecho de que $0 \leq \alpha \leq p^n - 1$ obtenemos que $p^n \nmid (\alpha - \beta)$. Utilizando ahora la tercera propiedad de β,

$$|\alpha-\beta|_p = |\alpha - x + x - \beta|_p \leq \text{máx}\{|\alpha - x|_p, |\beta - x|_p\} \leq p^{-n}$$

lo que implica que $p^n \mid (\alpha - \beta)$ y hemos llegado a una contradicción. Concluimos que existe un único entero α con $0 \leq \alpha \leq p^n - 1$ y $|\alpha - x|_p \leq p^{-n}$. □

Proposición 3.1.7. *Para cada $x \in \mathbb{Z}_p$, existe una única sucesión de Cauchy $(\alpha_n)_{n\in\mathbb{N}}$ que converge hacia x satisfaciendo que:*

1) $\alpha_n \in \mathbb{Z}$ cumple que $0 \leq \alpha_n \leq p^n - 1$,

2) para cada $n \in \mathbb{N}$, $\alpha_{n+1} \equiv \alpha_n \pmod{p^n}$.

Demostración. Sea $x \in \mathbb{Z}_p$ cualquiera. Por la proposición anterior, para cada $n \in \mathbb{N}$, existe un único $\alpha_n \in \mathbb{Z}$ tal que $0 \leq \alpha_n \leq p^n - 1$ y $|x - \alpha_n|_p \leq p^{-n}$. Veamos que la sucesión $(\alpha_n)_{n\in\mathbb{N}}$ cumple las condiciones del enunciado:
Primero, fijado un $\epsilon > 0$, existe $n_0 \in \mathbb{N}$ tal que $p^{-n} < \epsilon$ para todo $n \geq n_0$. Entonces, para cada $n \geq n_0$,

$$|x - \alpha_n|_p \leq p^{-n} < \epsilon,$$

lo que nos asegura que $(\alpha_n)_{n\in\mathbb{N}}$ converge hacia x y, como consecuencia, es de Cauchy.
Segundo, para cada $n \in \mathbb{N}$,

$$|\alpha_{n+1} - \alpha_n|_p = |\alpha_{+1} - \alpha_n + x - x|_p \leq \text{máx}\{|x - \alpha_{n+1}|_p, |x - \alpha_n|_p\} \leq p^{-n},$$

por tanto, $p^n \mid (\alpha_{n+1} - \alpha_n)$ o, lo que es lo mismo, $\alpha_{n+1} \equiv \alpha_n \pmod{p^n}$.
Para demostrar la unicidad, supongamos que existe otra sucesión $(\beta_n)_{n\in\mathbb{N}}$ de enteros que converge hacia x tal que:

1) $\beta_n \in \mathbb{Z}$ cumple que $0 \leq \beta_n \leq p^n - 1$,

2) para cada $n \in \mathbb{N}$, $\beta_{n+1} \equiv \beta_n \pmod{p^n}$.

Supongamos que existe $n \in \mathbb{N}$ tal que $\alpha_n \neq \beta_n$. Tenemos, por la primera propiedad que cumplen ambos números, que $p^n \nmid (\alpha_n - \beta_n)$ y, por tanto, $|\alpha_n - \beta_n|_p > p^{-n}$. Por otro lado, existe $m_0 \in \mathbb{N}$ tal que

$$|\alpha_{m_0} - x|_p \leq p^{-n}, \quad |\beta_{m_0} - x|_p \leq p^{-n}.$$

Claramente podemos suponer que $m_0 = n + k$ con $k \geq 1$. Entonces,

$$\begin{gathered}|\alpha_n - \beta_n|_p = |\alpha_n - \alpha_{n+1} + \alpha_{n+1} - \alpha_{n+2} + \alpha_{n+2} + ... - \alpha_{n+k} - \alpha_{n+k} - \\ -\beta_n - \beta_{n+1} + \beta_{n+1} - \beta_{n+2} + \beta_{n+2} + ... - \beta_{n+k} - \beta_{n+k} - x + x|_p \leq \\ \leq \text{máx}\{|\alpha_n - \alpha_{n+1}|_p, |\alpha_{n+1} - \alpha_{n+2}|_p, ..., |\alpha_{n+k-1} - \alpha_{n+k}|_p, |\alpha_{n+k} - x|_p, \\ |\beta_n - \beta_{n+1}|_p, |\beta_{n+1} - \beta_{n+2}|_p, ..., |\beta_{n+k-1} - \beta_{n+k}|_p, |\beta_{n+k} - x|_p\} \leq p^{-n}\end{gathered}$$

y hemos llegado a que $p^{-n} < |\alpha_n - \beta_n|_p \leq p^{-n}$ que es absurdo. Por tanto, la sucesión que converge a x y satisface las condiciones del enunciado es única. □

Observación 3.1.8. *Sea $p \in \mathbb{Z}$ primo. Una sucesión $(\alpha_n)_{n\in\mathbb{N}}$ de números enteros que satisface las dos condiciones de la proposición anterior:*

- $0 \leq \alpha_n \leq p^n - 1$ *para cada* $n \in \mathbb{N}$*;*
- $\alpha_{n+1} \equiv \alpha_n \pmod{p^n}$ *para cada* $n \in \mathbb{N}$*;*

se dice que es una sucesión coherente. *Es inmediato que toda sucesión coherente es de Cauchy ya que la segunda condición nos asegura que $|\alpha_{n+1} - \alpha_n|_p \leq p^{-n}$.*

De esta colección de cuatro resultados, que podemos considerar como un único teorema, se desprenden una serie de consecuencias, algunas más evidentes y otras que presentaremos a modo de resultados. La primera de ellas, y quizás la más importante, es que $\mathbb{Z}_p$ es el completado de $\mathbb{Z}$ respecto del valor absoluto p-ádico, de hecho, algunos textos que construyen los números p-ádicos, lo hacen probando primero esto. A continuación, veremos una serie de corolarios que nos ayudarán a escrudiñar más todavía la estructura algebraica de $\mathbb{Q}_p$.

Corolario 3.1.9. *Se tiene lo siguiente:*

1) Para cada $x \in \mathbb{Q}_p$, existe $n \geq 0$ tal que $p^n x \in \mathbb{Z}_p$.

2) Para cada $n \in \mathbb{Z}$, la aplicación

$$\psi_n : \mathbb{Q}_p \longrightarrow \mathbb{Q}_p$$

dada por $\psi_n(x) = p^n x$ es un homeomorfismo.

3) Los conjuntos $p^n\mathbb{Z}_p$, para cada $n \in \mathbb{Z}$, forman una base de abiertos del $0 \in \mathbb{Q}_p$ que, además, recubren todo $\mathbb{Q}_p$.

Demostración.

1) Sea $x \in \mathbb{Q}_p$. Si $x = 0$ entonces claramente $x \in \mathbb{Z}_p$. Supongamos que $x \neq 0$. Entonces por la Proposición 2.2.15, existe $n \in \mathbb{Z}$ tal que $|x|_p = p^{-n}$.
Si $n \geq 0$ entonces claramente $x = p^0 x \in \mathbb{Z}_p$.
Si $n < 0$ entonces considero el entero positivo $-n$. Entonces $p^{-n}x \in \mathbb{Z}_p$ ya que

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

2) Veamos que la aplicación ψ_n es un homomorfismo de grupos aditivos biyectivo, continuo y con inversa continua.
Sean $x, y \in \mathbb{Q}_p$, entonces

$$\psi_n(x+y) = p^n(x+y) = p^n x + p^n y = \psi_n(x) + \psi_n(y).$$

Por ende, ψ_n es un homomorfismo de grupos aditivos (esto no es necesario para esta demostración pero nos vendrá bien más tarde).
Para probar la inyectividad, si $x, y \in \mathbb{Q}_p$,

$$\psi_n(x) = \psi_n(y) \iff p^n x = p^n y \iff x = y.$$

Por último, para la sobreyectividad, si $y \in \mathbb{Q}_p$, entonces $p^{-n}y \in \mathbb{Q}_p$ y $\psi_n(p^{-n}y) = y$.
La continuidad de ψ_n está clara gracias a la Proposición 1.3.9, ya que es una restricción de la aplicación producto al subespacio $\{p^n\} \times \mathbb{Q}_p$.
Lo mismo para su inversa, que vuelve a ser la aplicación producto restringida esta vez al subespacio $\{p^{-n}\} \times \mathbb{Q}_p$. Por tanto, ψ_n es un isomorfismo de grupos aditivos continuo con inversa continua, es decir, un homeomorfismo.

3) Recordemos que los elementos del ideal principal $p^n\mathbb{Z}_p$ con $n \in \mathbb{Z}$ están caracterizados por:

$$x \in p^n\mathbb{Z}_p \iff \left|\frac{x}{p^n}\right|_p \leq 1 \iff |x|_p \leq p^{-n}.$$

Teniendo esto en cuenta, es inmediato que $0 \in p^n\mathbb{Z}_p$ para cada $n \in \mathbb{Z}$. Además, como ψ_n es un homeomorfismo, la imagen de abiertos es abierta. Esto nos asegura que $\psi_n(\mathbb{Z}_p) = p^n\mathbb{Z}_p$ es un abierto ($\mathbb{Z}_p = \bar{B}(0,1)$ es abierto por la Proposición 1.3.10).
Para ver que es una base de abiertos, sea $r > 0$, consideramos la bola $B(0,r)$. Existe $n \in \mathbb{Z}^+$ tal que $p^{-n} < r$. Entonces, para cada $x \in p^n\mathbb{Z}_p$,

$$\left|\frac{x}{p^n}\right|_p \leq 1 \Longrightarrow |x|_p \leq |p^n|_p = p^{-n} < r \Longrightarrow x \in B(0,r),$$

lo que significa que, efectivamente, $\{p^n\mathbb{Z}\}_{n\in\mathbb{Z}_p}$ forma una base de abiertos del $0 \in \mathbb{Q}_p$.
Por último, gracias a lo visto en el apartado 1) de este corolario,

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

□

Observación 3.1.10. *Es claro que, para cada $n \geq 1$, si restringimos el dominio del homeomorfismo ψ_n al anillo $\mathbb{Z}_p$ entonces la imagen de dicha aplicación está contenida en $\mathbb{Z}_p$.*

A continuación, vamos a ver cómo podemos extender la valoración p-ádica, v_p, a $\mathbb{Q}_p$. Recordemos que, dado un $x \in \mathbb{Q}$, $|x|_p = p^{-v_p(x)}$. Por la Proposición 2.2.15, para cada $x \in \mathbb{Q}_p$, $|x|_p = p^{-n}$ para algún $n \in \mathbb{Z}$. Intuitivamente, podemos definir, para cada $x \in \mathbb{Q}_p$, $v_p(x)$ como ese entero n. Podemos dar una definición más natural gracias al corolario anterior:

Lema 3.1.11. *Sea $x \in \mathbb{Q}_p \setminus \{0\}$. Entonces existe $n_0 = \text{máx}\{n \in \mathbb{Z} : x \in p^n\mathbb{Z}_p\}$ y se tiene que $v_p(x) = n_0$.*

Demostración. Sea $n_0 \in \mathbb{Z}$ tal que $|x|_p = p^{-n_0}$, es decir, $n_0 = v_p(x)$. Entonces, $x \in p^{n_0}\mathbb{Z}$. Si tomamos otro entero $n > n_0$, se tiene que $p^{-n_0} > p^{-n}$ y, como consecuencia,

$$|x|_p = p^{-n_0} > p^{-n} \iff x \notin p^n\mathbb{Z}_p.$$

Concluimos que $n_0 = \text{máx}\{n \in \mathbb{Z} : x \in p^n\mathbb{Z}_p\}$. □

Observación 3.1.12. *Nótese que para el caso de $x = 0 \in \mathbb{Q}_p$, tiene sentido asignar el valor $v_p(0) = \infty$ ya que $0 \in p^n\mathbb{Z}_p$ para cada $n \in \mathbb{Z}_+$, por lo que el conjunto* $\text{máx}\{n \in \mathbb{Z} : 0 \in p^n\mathbb{Z}_p\}$ *no estaría acotado.*

Para finalizar esta breve introducción a la estructura algebraica de $\mathbb{Q}_p$, vamos con un importante resultado que más adelante nos ayudará a demostrar que hay una correspondencia biyectiva entre los elementos de $\mathbb{Z}_p$ y las sucesiones de Cauchy de este mismo anillo. Pero antes, definamos que es una sucesión exacta:

Definición 3.1.13. *Una sucesión $A \xrightarrow{f} B \xrightarrow{g} C$ se dice que es* exacta *si* $\text{Im}(f) = \ker(g)$. *Una sucesión de cinco términos se dice que es* exacta *si lo es cada una de sus partes.*

Proposición 3.1.14. *Para cada $n \geq 1$, existe un homomorfismo de anillos, φ_n, tal que la sucesión*

$$0 \longrightarrow \mathbb{Z}_p \xrightarrow{\psi_{n|\mathbb{Z}_p}} \mathbb{Z}_p \xrightarrow{\varphi_n} \mathbb{Z}/p^n\mathbb{Z} \longrightarrow 0,$$

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

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

Demostración. Primeramente, por el 3.1.9, la aplicación ψ_n es inyectiva y continua lo que implica que $\psi_{n|\mathbb{Z}_p}$ es también inyectiva y continua, por tanto, $\text{Im}(0) = 0 = \ker(\psi_{n|\mathbb{Z}_p})$. Además, $\text{Im}(\psi_{n|\mathbb{Z}_p}) = p^n\mathbb{Z}_p$.

Continuando con la sucesión, definimos ahora la aplicación

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

dada por $\varphi_n(x) = \alpha_n \pmod{p^n}$ siendo α_n el único que satisface que $0 \leq \alpha_n \leq p^n - 1$ y $|x - \alpha_n|_p \leq p^{-n}$ (existe en virtud de la Proposición 3.1.6).
Veamos que se trata de un homomorfismo de anillos. Sean $x, y \in \mathbb{Z}_p$, entonces

$$\varphi_n(x) = \alpha, \quad \varphi_n(y) = \beta, \quad \varphi_n(x+y) = \lambda,$$

siendo α, β y λ los únicos enteros entre 0 y $p^n - 1$ tales que

$$|x - \alpha_n|_p \leq p^{-n}, \quad |y - \beta_n|_p \leq p^{-n}, \quad |x + y - \lambda|_p \leq p^{-n}.$$

Queremos ver que $\alpha + \beta \equiv \lambda \pmod{p^n}$.

$$|\alpha + \beta - \lambda|_p = |\alpha - x + \beta - y + x + y - \lambda|_p \leq \text{máx}\{|\alpha - x|_p, |\beta - y|_p, |x + y - \lambda|_p\} \leq p^{-n},$$

por lo que $p^n \mid (\alpha + \beta - \lambda)$ y esto implica que $\varphi_n(x+y) = \varphi_n(x) + \varphi_n(y)$.
Por otro lado, para esos mismos $x, y \in \mathbb{Z}_p$, sea $\delta \in \mathbb{Z}_p$ el único entero entre 0 y $p^n - 1$ tal que

$$|xy - \delta|_p \leq p^{-n}, \text{ i.e., } \delta = \varphi_n(xy),$$

queremos ver que $\alpha\beta \equiv \delta \pmod{p^n}$.

$$|\alpha\beta - \delta|_p = |\alpha\beta - xy + xy - \beta x + \beta x - \delta|_p \leq \text{máx}\{|\beta|_p|\alpha - x|_p, |xy - \delta|_p, |x|_p|\beta - y|_p\}$$

- $|x|_p|\beta - y|_p \leq |\beta - y|_p \leq p^{-n}$, pues $|x|_p \in \bar{B}(0,1)$;
- $|xy - \delta|_p \leq p^{-n}$;
- Si $p \mid \beta$, entonces $|\beta|_p < 1$ y entonces $|\beta|_p|\alpha - x|_p < |\alpha - x|_p \leq p^{-n}$. Si por el contrario $p \nmid \beta$, entonces $|\beta|_p = 1$ y $|\beta|_p|\alpha - x|_p = |\alpha - x|_p \leq p^{-n}$.

Por tanto, $|\alpha\beta - \delta|_p \leq p^{-n}$ y como consecuencia $\alpha\beta \equiv \delta \pmod{p^n}$. Hemos probado que φ_n es un homomorfismo de anillos.
En cuanto al núcleo de φ_n se tiene que

$$x \in \ker(\varphi_n) \iff \varphi_n(x) = \alpha_n \pmod{p^n} = 0 \pmod{p^n} \iff |x|_p \leq p^{-n} \iff$$
$$\iff x \in p^n\mathbb{Z}_p = \text{Im}(\psi_{n|\mathbb{Z}_p}).$$

Si tomamos un elemento $(\alpha \pmod{p^n}) \in \mathbb{Z}/p^n\mathbb{Z}$ cualquiera, podemos suponer sin ningún problema que $0 \leq \alpha \leq p^n - 1$. Entonces $\alpha \in \mathbb{Z}$ y, como $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$, $\varphi_n(\alpha)$ es el único entero comprendido entre el cero y $p^n - 1$ con $|\alpha - \varphi_n(\alpha)|_p \leq p^{-n}$, es decir, $\varphi_n(\alpha) = \alpha$, por lo que φ_n es sobreyectiva.
Para la continuidad de φ_n, si tomamos $(\alpha \pmod{p^n}) \in \mathbb{Z}/p^n\mathbb{Z}$, con $0 \leq \alpha \leq p^n - 1$, queremos ver que $\varphi_n^{-1}(\{\alpha \pmod{p^n}\})$ es un abierto de $\mathbb{Z}_p$, es decir, la intersección de un abierto de $\mathbb{Q}_p$ con $\mathbb{Z}_p$. Pero esto es claro ya que

$$\varphi_n^{-1}(\{\alpha \pmod{p^n}\}) = \{x \in \mathbb{Z}_p : |x - \alpha|_p \leq p^{-n}\} = \bar{B}(\alpha, p^{-n}) \cap \mathbb{Z}_p.$$

Por tanto, para cada $V \subseteq \mathbb{Z}/p^n\mathbb{Z}$ se tiene que ${\varphi_n}^{-1}(V) = \bigcup_{\alpha \in V}\{\alpha\}$ es abierto para el subespacio $\mathbb{Z}_p$ y, por ende, φ_n es continua. Concluimos que la cadena

$$0 \longrightarrow \mathbb{Z}_p \xrightarrow{\psi_{n|\mathbb{Z}_p}} \mathbb{Z}_p \xrightarrow{\varphi_n} \mathbb{Z}/p^n\mathbb{Z} \longrightarrow 0$$

es exacta y todas las aplicaciones que la componen son continuas ($0 \longrightarrow \mathbb{Z}_p$ y $\mathbb{Z}/p^n\mathbb{Z} \longrightarrow 0$ es inmediato que lo son).
Además, en virtud del Primer Teorema de Isomorfía aplicado a φ_n, tenemos que

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

□

Continuando con la exploración de $\mathbb{Q}_p$, vamos a adentrarnos ahora en su topología (la generada por $|\cdot|_p$).

Como ya advertimos en la sección 1.3, daremos por conocidos los conceptos de espacio de Hausdorff, espacio topológico compacto y espacio topológico conexo.

Recordamos que un espacio topológico se dice que es localmente compacto cuando todo punto tiene un entorno compacto.

Lema 3.1.15. *Sea $a \in \mathbb{Q}$ y $n \in \mathbb{Z}$. Entonces*

$$a + p^n\mathbb{Z}_p := \{x \in \mathbb{Q}_p : x - a \in p^n\mathbb{Z}_p\} = \bar{B}(a, p^{-n}).$$

Demostración. Sabemos que, para cada $x, y \in \mathbb{Q}_p$, se tiene que

$$x - y \in p^n\mathbb{Z}_p \Longleftrightarrow |x - y|_p \leq p^{-n}.$$

Tomando $y = a$ se obtiene la igualdad entre ambos conjuntos. □

Proposición 3.1.16. *$\mathbb{Q}_p$ es un espacio topológico de Hausdorff totalmente disconexo.*

Demostración. Que $\mathbb{Q}_p$ sea disconexo es inmediato por la Proposición 1.3.12. Además, por ser un espacio métrico, es un espacio de Hausdorff. □

Lema 3.1.17. *Sea $\mathbb{K}$ un cuerpo con un valor absoluto no arquimediano, $|\cdot|$, definido en él. Entonces $\mathbb{K}$ con la topología generada por $|\cdot|$ es localmente compacto si, y solo si, existe un entorno del cero que sea compacto.*

Demostración.
$\boxed{\Rightarrow}$ Es inmediato por la definición de localmente compacto.
$\boxed{\Leftarrow}$ Supongamos que existe un entorno U del cero compacto. Tomemos un punto $a \in \mathbb{K}$ cualquiera. Entonces, existe $r > 0$ con $B(0, r) \subseteq U$. Por tanto, $\bar{B}(0, r/2) \subseteq B(0, r) \subseteq U$. Sabemos que $\bar{B}(0, r/2)$ es compacta por ser un subespacio cerrado de un compacto. Además, la aplicación

$$T_a : \mathbb{K} \longrightarrow \mathbb{K}$$

dada por $T_a(x) = a + x$ es continua en virtud de la Proposición 1.3.9. Por otro lado,

$$x \in a + \bar{B}(0, r/2) \Longleftrightarrow x - a \in \bar{B}(0, r/2) \Longleftrightarrow |x - a| \leq r/2 \Longleftrightarrow x \in \bar{B}(a, r/2).$$

Como T_a es continua, la imagen de un compacto es compacta y, por tanto, $T_a(\bar{B}(0, r/2)) = a + \bar{B}(0, r/2) = \bar{B}(a, r/2)$ es compacto. □

Proposición 3.1.18. *$\mathbb{Z}_p$ es compacto.*

Demostración. Por un resultado de Topología en Espacios Métricos, sabemos que todo subespacio completo y totalmente acotado es compacto (recordemos que un espacio métrico es totalmente acotado si para cada $\epsilon > 0$ existe un número finito de bolas, con centro en ese espacio y radio ϵ, que lo recubren). Por un lado, $\mathbb{Z}_p$ es completo por ser un subespacio cerrado de un completo.
Fijamos un $n \in \mathbb{N}$ cualquiera, veamos que

$$\mathbb{Z}_p = \bigcup_{i=0}^{p^n-1} B(i, p^{-n}).$$

$\boxed{\subseteq}$ Sea $x \in \mathbb{Z}_p$, en virtud de la Proposición 3.1.6, existe un único $\alpha \in \mathbb{Z}$ con $0 \leq \alpha \leq p^n - 1$ tal que $|x - \alpha|_p \leq p^{-n}$, es decir, $x \in B(\alpha, p^{-n})$. Por tanto,

$$\mathbb{Z}_p \subseteq \bigcup_{i=0}^{p^n-1} B(i, p^{-n}).$$

$\boxed{\supseteq}$ Si $x \in B(i, p^{-n})$ para algún $i \in \{0, 1, ..., p^n - 1\}$,

$$|x|_p = |x - i + i|_p \leq \text{máx}\{|x - i|_p, |i|_p\} \leq \text{máx}\{1/p^n, 1/p^{v_p(i)}\} = \frac{1}{p^{v_p(i)}} \leq 1,$$

ya que $p^n \nmid i$ y entonces $0 \leq v_p(i) < n$. Por tanto, $x \in \mathbb{Z}_p$ y tenemos la igualdad.
Ahora, sea $\epsilon > 0$ cualquiera, sabemos que existe $n_0 \in \mathbb{N}$ tal que $p^{-n_0} < \epsilon$ y tendríamos, a tenor de lo visto arriba, que

$$\mathbb{Z}_p = \bigcup_{i=0}^{p^{n_0}-1} B(i, p^{-n_0}) \subseteq \bigcup_{i=0}^{p^{n_0}-1} B(i, \epsilon),$$

pues claramente $B(i, p^{-n_0}) \subseteq B(i, \epsilon)$ para cada $i \in \{0, 1, ..., p^{n_0} - 1\}$.
De esta forma, $\mathbb{Z}_p$ es completo y totalmente acotado y, por tanto, compacto. □

Corolario 3.1.19. *$\mathbb{Q}_p$ es localmente compacto.*

Demostración. Consecuencia directa de la Proposición 3.1.18 junto con el Lema 3.1.17. □

3.2. Representación mediante sucesiones coherentes

Hasta ahora, los elementos de $\mathbb{Q}_p$ siguen siendo desconocidos para nosotros. Hemos trabajado sobre las propiedades algebraicas y topológicas, pero no sabemos qué aspecto tienen los números p-ádicos más allá de que son clases integradas por sucesiones de Cauchy. En esta sección daremos, a través de sucesiones coherentes, la primera de las dos representaciones distintas de los elementos de $\mathbb{Q}_p$ de las que hablaremos.

Sabemos, gracias a la Proposición 3.1.7, que para cada $x \in \mathbb{Z}_p$ existe una única sucesión coherente (ver Observación 3.1.8), y por tanto de Cauchy, de elementos de $\mathbb{Z}_p$ que converge hacia x. Tenemos entonces una correspondencia inyectiva entre los elementos

de $\mathbb{Z}_p$ y las sucesiones coherentes de enteros p-ádicos. Pero además, como $\mathbb{Z}_p$ es cerrado y cada sucesión coherente es convergente (recordemos que $\mathbb{Z}_p$ es completo), dicho límite deberá estar necesariamente en $\mathbb{Z}_p$.

Atendiendo al párrafo anterior, podemos crear una correspondencia biyectiva entre los enteros p-ádicos y las sucesiones coherentes de $\mathbb{Z}_p$ y, de esta manera, identificar cada entero p-ádico con su correspondiente sucesión coherente. A continuación vamos a formalizar esta idea mediante un resultado, pero antes necesitamos presentar los ingredientes que utilizaremos.

Recordamos la aplicación

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

definida en la Proposición 3.1.14, donde $\varphi_n(x) = \alpha_n \pmod{p^n}$, siendo α_n el único entero tal que $0 \leq \alpha_n \leq p^n - 1$ con $|x - \alpha_n|_p \leq p^{-n}$. Para simplificar la notación, llamaremos

$$A_n := {}^{\mathbb{Z}}\!/_{p^n\mathbb{Z}}$$

y consideramos en A_n la topología discreta (todos los subconjuntos de A_n son abiertos).

El segundo ingrediente que necesitamos es el producto cartesiano de todos estos espacios A_n, denotado por

$$\prod_{n\in\mathbb{N}} A_n = A_1 \times A_2 \times ... \times A_n \times ... ,$$

y donde consideraremos, como es de esperar, la ya conocida topología producto. Los elementos de este espacio serán sucesiones $(a_n)_{n\in\mathbb{N}}$ donde $a_n \in A_n$ para cada $n \in \mathbb{N}$. Además, en virtud de la Proposición 3.1.18 y de un conocido resultado de Topología General, podemos afirmar que $\prod_{n\in\mathbb{N}} A_n$ es compacto para la topología producto. Denotaremos por

$$\mathcal{R}_p := \{(a_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} A_n : (a_n)_{n\in\mathbb{N}} \text{ coherente}\} \subseteq \prod_{n\in\mathbb{N}} A_n$$

al subespacio formado por todas las sucesiones coherentes. Estamos ya en condiciones de presentar el siguiente resultado:

Proposición 3.2.1. *La aplicación*

$$\varphi : \mathbb{Z}_p \longrightarrow \prod_{n\in\mathbb{N}} A_n,$$

dada por $\varphi(x) = (\varphi_n(x))_{n\in\mathbb{N}}$ *para cada* $x \in \mathbb{Z}_p$*, es inyectiva y se tiene que* $\mathrm{Im}(\varphi) = \mathcal{R}_p$.

Demostración. Sea $x \in \mathbb{Z}_p$, entonces $\varphi(x) = (\varphi_n(x))_{n\in\mathbb{N}} = (\alpha_n)_{n\in\mathbb{N}}$ que, en virtud de la Proposición 3.1.7, es una sucesión coherente y, por tanto, $\mathrm{Im}(\varphi) \subseteq \mathcal{R}_p$.
Si ahora tomamos una sucesión coherente $(a_n)_{n\in\mathbb{N}} \in \mathcal{R}_p$, entonces ya hemos visto que converge hacia un elemento $x \in \mathbb{Z}_p$. Además, sabemos, de nuevo por la Proposición 3.1.7, que existe una única sucesión coherente convergiendo hacia x y esa es, precisamente, $(\varphi_n(x))_{n\in\mathbb{N}}$. Se concluye que $(\varphi_n(x))_{n\in\mathbb{N}} = (a_n)_{n\in\mathbb{N}}$ y como consecuencia $\mathrm{Im}(\varphi) = \mathcal{R}_p$.

Para probar la inyectividad, lo haremos por reducción al absurdo. Sean $x, y \in \mathbb{Z}_p$ dos enteros p-ádicos distintos y supongamos que $\varphi(x) = (\varphi_n(x))_{n\in\mathbb{N}}\varphi(y) = (\varphi_n(y))_{n\in\mathbb{N}}$. Como ambas sucesiones coinciden, deben converger hacia el mismo límite, pero la primera converge hacia x y la segunda hacia y, llegando a una contradicción. Podemos afirmar entonces que φ es inyectiva. □

El resultado anterior formaliza lo que ya habíamos anticipado al inicio de la sección. Podemos representar los enteros p-ádicos a través de las sucesiones coherentes de $\mathcal{R}_p$.

3.3. Representación mediante expansiones p-ádicas

Introducimos ahora otro tipo de representación para enteros p-ádicos que es, quizás, la que nos da una visión más concreta de $\mathbb{Q}_p$, las expansiones p-ádicas, las cuales nos permiten descomponer y analizar números p-ádicos en base a potencias de p. Veremos que todo entero p-ádico tiene una expansión que le identifica y luego extenderemos esta propiedad a cualquier número p-ádico. Esta representación es particularmente útil para la resolución de ecuaciones diofánticas, la teoría de congruencias y otros problemas aritméticos.

Notación 3.3.1. *Al contrario de la sección anterior donde tomábamos $n \geq 1$, a lo largo de esta haremos un cambio de subíndices y consideraremos que las sucesiones están indexadas a partir del cero con este inclusive.*

Lema 3.3.2. *Sea $\mathbb{K}$ un cuerpo y $|\cdot|$ un valor absoluto no arquimediano definido en él tal que $\mathbb{K}$ es completo para dicho valor absoluto. Entonces para cualquier sucesión $(a_n)_{n\in\mathbb{N}_0}$,*

$$\sum_{n=0}^{\infty} a_n \ \textit{converge} \iff \lim_{n\to\infty} |a_n| = 0.$$

Demostración. Supongamos que $\lim_{n\to\infty} |a_n| = 0$. Entonces para cualquier $n, m \in \mathbb{N}_0$ con $m > n$ se tiene que, por la propiedad no arquimediana,

$$|S_m - S_n| = \left| \sum_{n+1\leq k\leq m} a_k \right| \leq \text{máx}\{|a_k| : n+1 \leq k \leq m\},$$

y, usando la hipótesis, concluimos que la sucesión de sumas parciales $(S_n)_{n\in\mathbb{N}_0}$ es de Cauchy, y, por tanto, convergente por ser $\mathbb{K}$ completo. □

El siguiente teorema es uno de los más importantes en lo concerniente a representación los números p-ádicos.

Teorema 3.3.3. *Todo elemento $x \in \mathbb{Z}_p$ se puede escribir de forma única como*

$$x = \sum_{n=0}^{\infty} b_n p^n$$

con $b_n \in \{0, 1, ..., p-1\}$ para todo $n \in \mathbb{N}_0$.

Demostración. Consideramos una serie cualquiera como la del enunciado, $\sum_{n=0}^{\infty} b_n p^n$ con $b_n \in \{0, 1, ..., p-1\}$ para todo $n \in \mathbb{N}_0$. Denotemos por

$$S_n = b_0 + b_1 p + ... + b_n p^n,$$

es decir, $(S_n)_{n\in\mathbb{N}_0}$ es la sucesión de sumas parciales. Notemos que, para cada $n \in \mathbb{N}_0$,

$$|S_n|_p \leq \text{máx}\{|b_0|_p, |b_1 p|_p, ..., |b_n p^n|_p\} = |b_j p^j|_p \leq 1,$$

donde b_j con $j \in \{0, 1, ..., n\}$ es el primer coeficiente no nulo de la suma.
Por el Lema 3.3.2, es claro que la serie converge en $\mathbb{Q}_p$ pues

$$|b_n p^n|_p = |b_n|_p |p^n|_p \leq |p^n|_p = p^{-n} \xrightarrow[n\to\infty]{} 0.$$

Sea $x = \sum_{n=0}^{\infty} b_n p^n$. Entonces, en virtud del Lema 2.2.19, se tiene que

$$|x|_p = \left|\lim_{n\to\infty} S_n\right|_p = \lim_{n\to\infty} |S_n|_p \leq 1,$$

por lo que $x \in \mathbb{Z}_p$. Además, es claro que para todo $n \in \mathbb{N}_0$,

$$|S_n - x|_p \leq \frac{1}{p^{n+1}} .$$

Veamos qué aspecto tienen los b_n.
Como $x + p\mathbb{Z}_p \in {}^{\mathbb{Z}_p}\!/_{p\mathbb{Z}_p} \cong {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$, existe un único $a_0 \in \{0, 1, ..., p-1\}$ tal que $x \equiv a_0$ (mód p), es decir, $x = a_0 + y_1 p$ para algún $y_1 \in \mathbb{Z}_p$. Tenemos entonces

$$|x - a_0|_p = |y_1 p|_p = |y_1|_p |p|_p \leq \frac{1}{p}.$$

De la misma forma, podemos tomar $a_1 \in \{0, 1, ..., p-1\}$ como el único entero tal que $y_1 = a_1 + y_2 p$ para algún $y_2 \in \mathbb{Z}_p$. Juntando ambas expresiones se tiene que

$$x = a_0 + a_1 p + y_2 p^2$$

con

$$|x - (a_0 + a_1 p)|_p = |y_2 p^2|_p = |y_2|_p |p|_p^2 \leq \frac{1}{p^2} .$$

Repitiendo este razonamiento se llega a que, para cada $n \in \mathbb{N}$,

$$|x - (a_0 + a_p + ... + a_{n-1} p^{n-1} + a_n p^n)|_p \leq \frac{1}{p^{n+1}},$$

con $a_k \in \{0, 1, ..., p-1\}$ para cada $k = 0, 1, ..., n$. La sucesión $T_n = a_0 + a_1 p + ... + a_n p^n$ cumple que, para un $\epsilon > 0$ cualquiera, existe $n_0 \in \mathbb{N}$ tal que $1/p^{n+1} < \epsilon$ para cada $n \geq n_0$ y, por tanto,

$$|x - T_n| \leq \frac{1}{p^{n+1}} < \epsilon$$

para cada $n \geq n_0$. Podemos afirmar entonces que $\lim_{n\to\infty} T_n = x$.
Supongamos que las dos series (o expansiones) que tenemos para x son distintas:

$$x = \sum_{n=0}^{\infty} b_n = \sum_{n=0}^{\infty} a_n$$

y $b_n \neq a_n$ para algún $n \in \mathbb{N}_0$.
Sea $m = \text{mín}\{m \in \mathbb{N}_0 : b_m \neq a_m\}$. Tenemos que $b_m \not\equiv a_m \pmod{p}$ lo que implica que $|b_m - a_m|_p = 1$.
Por cómo hemos definido m se tiene que

$$|S_m - T_m|_p = |(b_m - a_m)p^m|_p = |b_m - a_m|_p |p^m|_p = \frac{1}{p^m} .$$

Pero, por la propiedad no arquimediana del valor absoluto, se tendría que

$$|S_m - T_m|_p = |S_m - x + x - T_m|_p \leq \text{máx}\{|S_m - x|_p, |T_m - x|_p\} \leq \frac{1}{p^{m+1}} .$$

Hemos llegado a una contradicción lo que significa que $a_n = b_n$ para todo $n \in \mathbb{N}_0$. Así pues, hemos probado que podemos identificar cada elemento de $\mathbb{Z}_p$ con la serie $\sum_{n=0}^{\infty} a_n$ construida anteriormente. □

Observación 3.3.4. *Notemos que si tenemos $x, y \in \mathbb{Z}_p$ tales que $x \equiv y \pmod{p^n}$ para cada $n \in \mathbb{N}$, entonces, por como hemos construido las expansiones p-ádicas, se tendría que ambas coincidirían y como consecuencia $x = y$.*

Ya hemos demostrado que podemos representar de forma única mediante el límite de una serie a todo elemento de $\mathbb{Z}_p$. Ahora lo que nos interesa es extender esta representación a los números p-ádicos. Esto es sencillo a raíz del teorema anterior:

Corolario 3.3.5. *Todo $x \in \mathbb{Q}_p$ se puede escribir de forma única como*

$$x = \sum_{n=-n_0}^{\infty} b_n p^n,$$

con $0 \leq b_n \leq p-1$ para cada $n \in \mathbb{N}_0$ y $-n_0 = v_p(x)$.

Demostración. Sea $x \in \mathbb{Q}_p$. Si $x \in \mathbb{Z}_p$ entonces $v_p(x) \geq 0$. Por el Teorema 3.3.3 podemos escribir

$$x = \sum_{n=0}^{\infty} b_n p^n$$

con $0 \leq b_n \leq p-1$ para cada $n \in \mathbb{N}_0$.
Supongamos que $v_p(x) = n_0 > 0$. En ese caso, haciendo la misma construcción que en la demostración del Teorema 3.3.3,

$$x = b_0 + b_1 p + ... + b_{n_0-1} p^{n_0-1} + y p^{n_0}$$

con $y \in \mathbb{Z}_p$. Tenemos que

$$p^{-n_0} = |x|_p = |b_0 + b_1 p + ... + b_{n_0-1} p^{n_0-1} + y p^{n_0}|_p,$$

por lo que necesariamente $b_0 = b_1 = ... = b_{n_0-1} = 0$. Por tanto $x = \sum_{n=n_0}^{\infty} b_n p^n$ si $x \in \mathbb{Z}_p$. Supongamos ahora que $x \in \mathbb{Q}_p \setminus \mathbb{Z}_p$. Entonces $v_p(x) = -n_0 < 0$ con $n_0 \in \mathbb{N}$. En virtud del Corolario 3.1.9, existe $y \in \mathbb{Z}_p$ con $v_p(y) = 0$ tal que $x = y p^{-n_0}$. Por lo que acabamos de probar arriba, sabemos que

$$y = \sum_{n=v_p(y)}^{\infty} c_n p^n = \sum_{n=0}^{\infty} c_n p^n,$$

con $0 \leq c_n \leq p-1$ para cada $n \in \mathbb{N}_0$. Sustituyendo:

$$x = y p^{-n_0} = \left(\sum_{n=0}^{\infty} c_n p^n \right) p^{-n_0} = \sum_{n=0}^{\infty} c_n p^{n-n_0} = \sum_{j=-n_0}^{\infty} c_j p^j,$$

con $0 \leq c_j \leq p-1$ para cada $j \in \mathbb{N}_0$, que es exactamente lo que queríamos demostrar. □

Ejemplo 3.3.6.

a) La expansión p-ádica de $1/(1-p^m)$ *para cualquier* $m \in \mathbb{N}$*:*

$$\sum_{n=0}^{\infty} (p^m)^n = \frac{1}{1-p^m}.$$

La forma de demostrarlo es análoga a la suma de series geométricas que se estudia en Análisis, pero con para el valor absoluto $|\cdot|_p$*. Notemos además que la condición necesaria y suficiente de convergencia para series geométricas para el valor absoluto usual, en el caso del valor absoluto p-ádico también se cumple ya que* $|p^m|_p = p^{-m} < 1$*.*

b) Ahora vamos a dar una idea de cómo calcular la expansión 7-ádica de $128/9$ *utilizando lo anterior. Para ello, lo primero que tenemos que hacer es buscar la mínima potencia de* 7 *que es congruente con* 1 *módulo 9.*

$$7^3 = 343 = 38 \cdot 9 + 1.$$

Ahora escribimos $128/9$ *como la diferencia entre el primer entero mayor, en este caso,* 15 *pues* $128/9 = 14{,}2222222$ *y un número racional en el que aparezca* $1 - 7^n$ *para algún* $n \in \mathbb{N}$ *en el denominador:*

$$\frac{128}{9} = 15 - \frac{7}{9} = 15 - 7\frac{1}{9} = 15 - 7\frac{38}{342} = 15 - 7\frac{38}{1-7^3} = 15 + 7 \cdot 38(1 + 7^3 + (7^3)^2 + ...),$$

en virtud del apartado anterior.

3.4. Lema de Hensel

Los números p-ádicos, introducidos a finales del siglo XIX, proporcionan una forma alternativa de analizar ecuaciones polinómicas y resolver problemas de congruencias que no pueden ser tratados adecuadamente en el contexto de los números racionales o reales. El Lema de Hensel, a menudo comparado con el Teorema de Newton para aproximaciones en análisis real, permite transformar soluciones aproximadas de ecuaciones polinómicas módulo p a soluciones exactas en el cuerpo de los números p-ádicos. En términos más formales, si una ecuación polinómica tiene una raíz que satisface ciertas condiciones módulo p, entonces esta raíz puede ser elevada a una solución en el contexto p-ádico. A lo largo de esta sección demostraremos este resultado, dando algún ejemplo de uso y alguna conexión con otras áreas de las matemáticas. También enunciaremos y demostraremos una versión más general del Lema de Hensel, el cual nos asegura que si un polinomio se factoriza módulo p en dos polinomios coprimos, entonces esta factorización se puede elevar a cualquier potencia mayor de p. Esto proporciona un algoritmo para lo que se conoce como *levantamiento de Hensel*, que es fundamental en la factorización de polinomios y es uno de los más eficientes conocidos.

Notación 3.4.1. *Sea $F(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}_p[X]$ un polinomio. Denotamos por $F'(X)$ a la derivada de $F(X)$, es decir,*

$$F'(X) = \sum_{k=0}^{n} k a_k X^{k-1}.$$

Únicamente precisamos de un lema previo antes del Lema de Hensel:

Lema 3.4.2. *Sea $\mathbb{K}$ un cuerpo y $F(X) \in \mathbb{K}[X]$. Entonces*

$$F(X+Y) = F(X) + F'(X)Y + G(X,Y)Y^2$$

para algún polinomio $G(X,Y) \in \mathbb{K}[X,Y]$.

Demostración. Escribamos $F(X) = a_0 + a_1 X + ... + a_n X^n$ para algún $n \in \mathbb{N}_0$. Sustituyendo X por $X+Y$ y usando el Binomio de Newton,

$$F(X+Y) = a_0 + a_i(X+Y) + ... + a_n(X+Y)^n =$$
$$= a_+ a_1 X + a_1 Y + \sum_{k=2}^{n} a_k (X^k + kX^{k-1}Y + G_k(X,Y)Y^2)$$

siendo $G_k(X,Y)$ la suma de todos los términos de los binomios $(X+Y)^k$ (excepto de los dos primeros que ya los hemos sacado fuera) y sacando Y^2 como factor común, por lo que $G_k(X,Y)$ es siempre un polinomio. Por tanto,

$$F(X+Y) = \sum_{k=0}^{n} a_k X^k + \sum_{k=0}^{n} k a_k X^{k-1} Y + \sum_{k=2}^{n} G_k(X,Y)Y^2 = F(X) + F'(X)Y + G(X,Y)Y^2$$

con $G(X,Y) \in \mathbb{K}[X,Y]$. □

Teorema 3.4.3 (**Lema de Hensel**). *Sea $F(X) = a_0 + a_1X + ... + a_dX^d$ un polinomio con $a_i \in \mathbb{Z}_p$ para cada $i \in \{0, 1, ..., d\}$. Supongamos que existe un elemento de $\beta \in \mathbb{Z}/p\mathbb{Z}$ tal que*

$$F(\beta) \equiv 0 \pmod{p}$$

y

$$F'(\beta) \not\equiv 0 \pmod{p}.$$

Entonces existe un único $\alpha \in \mathbb{Z}_p$ tal que $\alpha \equiv \beta \pmod{p}$ y $F(\alpha) = 0$.

Demostración. Mediante inducción vamos a construir una sucesión de Cauchy de elementos de $\mathbb{Z}_p$ cuyo límite será la raíz α buscada. Buscamos entonces una sucesión $(\alpha_n)_{n\in\mathbb{N}} \subseteq \mathbb{Z}_p$ tal que:

- $F(\alpha_n) \equiv 0 \pmod{p^n}$,
- $\alpha_n \equiv \beta \pmod{p}$,

para todo $n \in \mathbb{N}$.
Para $n = 1$ es inmediato tomando $\alpha_1 = \beta$. Supongamos que es cierto para n, es decir, existen $\alpha_1, ..., \alpha_n \in \mathbb{Z}_p$ tales que

- $F(\alpha_k) \equiv 0 \pmod{p^k}$,
- $\alpha_k \equiv \beta \pmod{p}$,

para cada $k = 1, 2, ..., n$.
Queremos encontrar un elemento $\alpha_{n+1} \in \mathbb{Z}_p$ tal que

- $F(\alpha_{n+1}) \equiv 0 \pmod{p^{n+1}}$,
- $\alpha_{n+1} \equiv \beta \pmod{p}$.

Usando nuestra hipótesis de inducción, existe una raíz α_n que es divisible por p^n. Para que la sucesión que estamos construyendo sea de Cauchy, el término α_{n+1} debe cumplir que $\alpha_{n+1} \equiv \alpha_n \pmod{p^n}$. Además, de satisfacer esa condición, entonces

$$|\alpha_{n+1} - \beta|_p = |\alpha_{n+1} - \beta + \alpha_n - \alpha_n|_p \leq \text{máx}\{|\alpha_{n+1} - \alpha_n|_p, |\alpha_n - \beta|_p\} \leq \frac{1}{p},$$

lo que implica que $\alpha_{n+1} \equiv \beta \pmod{p}$.
Para cumplir la condición de Cauchy, el α_{n+1} buscado se debe poder escribir como

$$\alpha_{n+1} = \alpha_n + p^n t_n$$

para algún $t_n \in \mathbb{Z}_p$, por lo que la búsqueda del α_{n+1} se reduce a la buscar un $t_n \in \mathbb{Z}_p$ tal que

$$F(\alpha_n + p^n t^n) \equiv 0 \pmod{p^{n+1}}.$$

Por el Lema 3.4.2,

$$F(\alpha_n + p^n t_n) = F(\alpha_n) + F'(\alpha_n)p^n t_n + G(\alpha_n, p^n t_n)p^{2n}t_n^2 \equiv F(\alpha_n) + F'(\alpha_n)p^n t_n \pmod{p^{n+1}},$$

ya que $p^{n+1} \mid p^{2n}$ para todo $n \geq 1$. Queremos encontrar un $t_n \in \mathbb{Z}_p$ tal que

$$F(\alpha_n) + F'(\alpha_n)p^n t_n \equiv 0 \pmod{p^{n+1}}.$$

Para ello notemos que, por hipótesis de inducción, $F(\alpha_n) \equiv 0 \pmod{p^n}$, por lo que podemos escribir $F(\alpha_n) = p^n q$ para algún $q \in \mathbb{Z}$. Tenemos entonces la ecuación en congruencias con incógnita t_n,

$$p^n q + F'(\alpha_n)p^n t_n \equiv 0 \pmod{p^{n+1}}$$

que, al dividir por p^n, se convierte en

$$q + F'(\alpha_n)t_n \equiv 0 \pmod{p}.$$

Como $F'(\alpha_n) \not\equiv 0 \pmod{p}$, $F'(\alpha_n)$ es una unidad de $\mathbb{Z}/p\mathbb{Z}$ y claramente

$$t_n \equiv -q(F'(\alpha_n))^{-1} \pmod{p}.$$

Por tanto, hemos podido construir el elemento α_{n+1} de la sucesión. Afirmamos entonces que existe una sucesión de Cauchy, $(\alpha_n)_{n\mathbb{N}}$, de enteros p-ádicos que es de Cauchy y que cumple que $F(\alpha_n) \equiv 0 \pmod{p^n}$ y $\alpha_n \equiv \beta \pmod{p}$ para cada $n \in \mathbb{N}$.
Esta sucesión converge en $\mathbb{Z}_p$ por ser $\mathbb{Z}_p$ completo y cerrado. Sea $\alpha = \lim_{n\to\infty} \alpha_n \in \mathbb{Z}_p$. Queremos ver que $\alpha \equiv \beta \pmod{p}$ y $F(\alpha) = 0$.
Sea $n \in \mathbb{N}$ cualquiera, entonces, como $\alpha_{n+1} \equiv \alpha_n \pmod{p^n}$, para cualquier $m = n+k > n$ se tendría que

$$\alpha_m - \alpha_n = \alpha_m - \alpha_{m-1} + \alpha_{m-1} + \alpha_{m-2} - \alpha_{m-2} + ... + \alpha_{m-k+1} - \alpha_{m-k+1} - \alpha_n,$$

y teniendo en cuenta que p^n divide a cada resta $(\alpha_{i+1} - \alpha_i)$, concluimos que $\alpha_m \equiv \alpha_n \pmod{p^n}$ para cada $m > n$. Ahora, si $m \longrightarrow \infty$,

$$\alpha \equiv \alpha_n \pmod{p^n}$$

y, como esto es cierto para un número natural cualquiera, tomamos $n = 1$ y tenemos $\alpha \equiv \beta \pmod{p}$. Ya tenemos la primera condición, veamos la segunda.
Notemos que, como $\alpha \equiv \alpha_n \pmod{p^n}$, entonces $F(\alpha) \equiv F(\alpha_n) \equiv 0 \pmod{p^n}$, esto significa que $p^n \mid F(\alpha)$ y, por ende, $|F(\alpha)|_p \leq 1/p^n$. Haciendo tender $n \longrightarrow \infty$, llegamos a que $|F(\alpha)|_p = 0$, lo que solo puede ocurrir si $F(\alpha) = 0$.
Para finalizar con la demostración, veamos la unicidad de α. Supongamos que existe α' tal que $F(\alpha') = 0$ y $\alpha' \equiv \beta \equiv \alpha \pmod{p}$. Si vemos que $\alpha' \equiv \alpha \pmod{p^n}$ para cada $n \in \mathbb{N}$, entonces tendrán la misma expansión p-ádica y, por el Teorema 3.3.3, podremos concluir que $\alpha' = \alpha$. Procedemos, de nuevo, por inducción sobre n:
Para $n = 1$ ya está visto tres líneas más arriba. Supongamos que se cumple para n, es decir, $\alpha' \equiv \alpha \pmod{p^n}$. Podemos escribir $\alpha' = \alpha + p^n r_n$ con $r_n \in \mathbb{Z}_p$. En virtud del Lema 3.4.2,

$$F(\alpha') = F(\alpha + p^n r_n) \equiv F(\alpha) + F'(\alpha)p^n r_n \pmod{p^{n+1}}.$$

Como $F(\alpha') = F(\alpha) = 0$, llegamos a que

$$F'(\alpha)p^n r_n \equiv 0 \pmod{p^{n+1}} \implies F'(\alpha)r_n \equiv 0 \pmod{p},$$

y, como $F'(\alpha) \not\equiv 0 \pmod{p}$, llegamos a que $r_n \equiv 0 \pmod{p}$ y, como consecuencia, $\alpha' = \alpha + p^{n+1}s_n$ para algún $s_n \in \mathbb{Z}_p$, lo que implica que $\alpha' \equiv \alpha \pmod{p^{n+1}}$ y con esto concluye la demostración. □

Ejemplo 3.4.4.

a) Sea $n \geq 1$ que no es múltiplo de p y $u \in \mathbb{Z}_p$ con $u \equiv 1 \pmod{p}$. Si consideramos el polinomio $F(X) = X^n - u$, entonces $F(1) = 1 - u \equiv 0 \pmod{p}$ y $F'(1) = n \not\equiv 0 \pmod{p}$. Aplicando el Lema de Hensel, existe una única raíz α tal que $\alpha \equiv 1 \pmod{p}$ y $\alpha^n = u$.

b) Si suponemos que $p > 2$, una aplicación muy útil del Lema de Hensel es que nos permite saber cuándo un número p-ádico es un cuadrado. Supongamos que tenemos $x \in \mathbb{Q}_p^*$. Atendiendo a las propiedades de la valoración p-ádica, es una condición necesaria para que x sea un cuadrado que $v_p(x) = 2k$ para algún $k \in \mathbb{Z}$. En ese caso, $y = x/p^{2k}$ cumple que $|y|_p = 1$, por lo que realmente tenemos que ver cuándo un elemento de $\mathbb{Z}_p^*$ es un cuadrado.
Si $y \in \mathbb{Z}_p^*$ fuese un cuadrado, entonces $y \equiv z^2 \pmod{p}$ para algún z y $|y|_p = |z|_p^2 = 1$ lo que implica que $z \in \mathbb{Z}_p^*$.
Consideramos el polinomio $F(X) = X^2 - y$. Entonces, por lo que acabamos de ver, $F(z) \equiv 0 \pmod{p}$ y $F'(z) = 2z \not\equiv 0 \pmod{p}$. Aplicando el Lema de Hensel, $F(X)$ tiene una raíz que es congruente con z módulo p. Por lo tanto, $y \in \mathbb{Z}_p$ será un cuadrado si, y solo si, su imagen por la aplicación de paso al cociente de $\mathbb{Z}_p$ a $\mathbb{Z}/p\mathbb{Z}$ es un cuadrado de $\mathbb{Z}/p\mathbb{Z}$ (recordemos que $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$).
Para $p = 2$ lo anterior no es cierto ya que $F'(v) = 2v \equiv 0 \pmod{2}$.

Lema 3.4.5. *Sea $m \geq 1$. Si $\xi \in \mathbb{Q}_p$ es una raíz m-ésima de la unidad, entonces $\xi \in \mathbb{Z}_p^*$.*

Demostración. Supongamos que $\xi \in \mathbb{Q}_p$ es una raíz m-ésima de la unidad. Entonces existe $n \in \mathbb{Z}$ tal que

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

Por tanto,

$$1 = |\xi^m|_p = |\xi|_p^m = \frac{1}{p^{mn}} \Longrightarrow\ n = 0 \Longrightarrow \xi \in \mathbb{Z}_p^*.$$

□

Proposición 3.4.6. *Sea $p \in \mathbb{Z}_+$ un primo cualquiera y m un entero positivo cualquiera que no es múltiplo de p. Entonces existe una raíz primitiva m-ésima de la unidad en $\mathbb{Q}_p$ si, y solo si, m divide a $p - 1$.*

Demostración. Fijamos un primo cualquiera p y un entero positivo m que no es divisible por p. Recordemos que el grupo de unidades de $\mathbb{F}_p$ es un grupo cíclico de orden $p - 1$ y que

$$X^m - 1 = \prod_{k|m} \Phi_k(X)$$

donde $\Phi_k(X)$ es el polinomio ciclotómico de grado k.
$\boxed{\Rightarrow}$ Por reducción al absurdo, supongamos que $m \nmid (p-1)$ y que $\alpha \in \mathbb{Q}_p$ es una raíz primitiva m-ésima de la unidad que claramente debe ser no nula ($\Phi_m(\alpha) = 0$). En virtud del Lema 3.4.5, $\alpha \in \mathbb{Z}_p$ y que, para el polinomio $F(X) = X^m - 1$, $F(\alpha) = 0$ y $F'(\alpha) \neq 0$. Entonces, por el Lema de Hensel, $\alpha \in \mathbb{Z}_p$ es una raíz del polinomio $F(X)$ cuando lo

reducimos a módulo p, es decir, α es una raíz primitiva m-ésima de la unidad en $\mathbb{F}_p$. Esto es lo mismo que decir que α, visto como un elemento de $\mathbb{F}_p$, tiene orden m. Pero sabemos que el orden de cada elemento de $\mathbb{F}_p$ tiene que dividir a $p-1$ y hemos llegado a una contradicción.
$\boxed{\Leftarrow}$ Supongamos que $m \mid (p-1)$ $a\mathbb{F}_p^*$ un generador de $\mathbb{F}_p^*$ (cuyo orden sabemos que es $p-1$). Entonces, $\alpha = a^{\frac{p-1}{m}} \in \mathbb{F}_p^*$ tiene orden m, por lo que es una raíz del polinomio $\Phi_m(X) \in \mathbb{F}_p[X]$.
Por otro lado, podemos escribir

$$X^m - 1 = \Phi_m(X)Q(X)$$

$Q(X) = \prod_{m|n, m\neq n} \Phi_m(X)$. Reduciendo a módulo p, derivando y evaluando en α,

$$m\alpha^{m-1} = \Phi'_m(\alpha)Q(\alpha) + \Phi_m(\alpha)Q'(\alpha) = \Phi'_m(\alpha)Q(\alpha),$$

y, como $Q(\alpha) \neq 0$, podemos afirmar que $\Phi_m(\alpha) = 0$ y $\Phi'_m(\alpha) \neq 0$. Aplicando el Lema de Hensel, α, ahora visto como un entero p-ádico, es una raíz de $\Phi_m(X)$ y, por tanto, una raíz primitiva de la unidad en $\mathbb{Q}_p$. □

Veamos ahora otra versión del Lema de Hensel que es más general que aquella que ya hemos demostrado.

Notación 3.4.7. *Dados dos polinomios $F(X), G(X) \in \mathbb{Z}_p[X]$ y $n \in \mathbb{N}$, decimos que son congruentes módulo p^n, y escribimos*

$$F(X) \equiv G(X) \pmod{p^n},$$

si lo son coeficiente a coeficiente.

Teorema 3.4.8 (Lema de Hensel, Segunda Versión). *Sea $F(X) \in \mathbb{Z}_p[X]$. Supongamos que existen polinomios $G_1(X), H_1(X) \in \mathbb{Z}_p[X]$ tales que*

i) $G_1(X)$ es mónico,

ii) $G_1(X)$ y $H_1(X)$ son coprimos módulo p,

iii) $F(X) \equiv G_1(X)H_1(X) \pmod{p}$.

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

i) $G(X)$ es mónico,

ii) $G(X) \equiv G_1(X) \pmod{p}$ y $H(X) \equiv H_1(X) \pmod{p}$,

iii) $F(X) = G(X)H(X)$.

Demostración. Sean $d = \deg(F(X))$ y $m = \deg(G_1(X))$. Entonces $\deg(H_1(X)) \leq d - m$ ya que podría ser que el término de mayor grado de $F(X)$ fuese divisible por p y, por tanto, cero en $\mathbb{F}_p$. Vamos a construir dos sucesiones de polinomios, $(G_n(X))_{n\in\mathbb{N}}$ y $(H_n(X))_{n\in\mathbb{N}}$ que cumplan que, para cada $n \in \mathbb{N}$,

i) $G_n(X)$ mónico de grado m,

ii) $G(X)_{n+1} \equiv G_n(X) \pmod{p^n}$ y $H_{n+1}(X) \equiv H_n(X) \pmod{p^n}$,

iii) $F(X) \equiv G_n(X)H_n(X) \pmod{p^n}$.

Por la condición ii) que pedimos, $G_2(X)$ y $H_2(X)$ se tendrían que poder escribir como

$$G_2(X) = G_1(X) + pR_1(X), \quad H_2(X) = H_1(X) + pS_1(X)$$

para ciertos polinomios $R_1(X), S_1(X) \in \mathbb{Z}_p[X]$. Por tanto, la condición iii) quedaría como

$$\begin{gathered} F(X) \equiv (G_1(X) + pR_1(X))(H_1(X) + pS_1(X)) \equiv \\ \equiv G_1(X)H_1(X) + pG_1(X)S_1(X) + pH_1(X)R_1(X) + p^2R_1(X)S_1(X) \equiv \\ \equiv G_1(X)H_1(X) + pG_1(X)S_1(X) + pH_1(X)R_1(X) \pmod{p^2}. \end{gathered}$$

Como una de las hipótesis es que $F(X) \equiv G_1(X)H_1(X) \pmod{p}$, existe un polinomio $T_1(X) \in \mathbb{Z}_p[X]$ tal que

$$F(X) = G_1(X)H_1(X) + pT_1(X).$$

Sustituyendo, quedaría la ecuación

$$pT_1(X) \equiv pG_1(X)S_1(X) + pH_1(X)R_1(X) \pmod{p^2},$$

o lo que es lo mismo, al dividir por p,

$$T_1(X) \equiv G_1(X)S_1(X) + H_1(X)R_1(X) \pmod{p}. \tag{3.1}$$

Queremos ver qué forma tienen esos polinomios $R_1(X)$ y $S_1(X)$. Utilizamos ahora la segunda hipótesis que nos dice que $G_1(X)$ y $H_1(X)$ son coprimos. Por la Identidad de Bézout, sabemos que existen polinomios $A(X), B(X) \in \mathbb{Z}_p[X]$ tales que

$$A(X)G_1(X) + B(X)H_1(X) \pmod{p}.$$

Definimos los dos polinomios

$$\bar{R}(X) = B(X)T_1(X), \quad \bar{S}(X) = A(X)T_1(X).$$

Veamos que $\bar{G}_2(X) = G_1(X) + p\bar{R}_1(X)$ y $H_2(X) = H_1(X) + p\bar{S}_1(X)$ cumplen las congruencias.

ii) Claramente $\bar{G}_2(X) \equiv G_1(X) \pmod{p}$ y $\bar{H}_2(X) \equiv H_1(X) \pmod{p}$.

iii) Como $\bar{R}_1(X)$ y $\bar{S}_1(X)$ cumplen que $T_1(X) \equiv G_1(X)\bar{S}_1(X) + H_1(X)\bar{R}_1(X) \pmod{p}$,

$$\begin{gathered} \bar{G}_2(X)\bar{H}_2(X) = (G_1(X) + p\bar{R}_1(X))(H_2(X) + p\bar{S}_1(X)) \equiv \\ \equiv G_1(X)H_1(X) + p\bar{S}_1(X)G_1(X) + p\bar{R}_1(X)H_1(X) \equiv G_1(X)H_1(X) + pT_1(X) \equiv \\ \equiv F(X) \pmod{p^2}. \end{gathered}$$

Al polinomio $G_2(X)$ que buscamos le pedimos dos condiciones más que a $H_2(X)$: que sea mónico y de grado m. El polinomio $\bar{G}_2(X)$ obtenido antes cumple las congruencias, pero

no podemos asegurar que sea mónico de grado m. Vamos a solucionar esto:
Sabemos que

$$T_1(X) \equiv G_1(X)\bar{S}_1(X) + H_1(X)\bar{R}_1(X) \pmod{p}.$$

Ahora dividimos el polinomio $\bar{R}_1(X)$ entre $G_1(X)$ y llamamos $R_1(X)$ al resto (no confundir con el $R_1(X)$ que hemos usado antes para poner nombre a una de las dos incógnitas). Se tiene que

$$\bar{R}_1(X) = G_1(X)Q(X) + R_1(X)$$

para algún polinomio $Q(X) \in \mathbb{Z}_p[X]$. Claramente $\deg(R_1(X)) < \deg(G_1(X))$, por lo tanto $G_1(X) + pR_1(X)$ será mónico de grado m. Si ahora definimos el polinomio $S_1(X)$ como

$$S_1(X) = \bar{S}_1(X) + H_1(X)Q(X)$$

entonces

$$\begin{gathered} R_1(X)H_1(X) + S_1(X)G_1(X) \equiv \\ \equiv (\bar{R}_1(X) - G_1(X)Q(X))H_1(X) + (\bar{S}_1(X) + H_1(X)Q(X))G_1(X) \equiv \\ \equiv \bar{R}_1(X)H_1(X) - G_1(X)Q(X)H_1(X) + \bar{S}_1(X)G_1(X) + H_1(X)Q(X)G_1(X) \equiv \\ \equiv \bar{R}_1(X)H_1(X) + \bar{S}_1(X)G_1(X) \equiv T_1(X) \pmod{p} \end{gathered}$$

Por tanto, $R_1(X)$ y $S_1(X)$ son también soluciones de (3.1). Como vimos antes, esto significa que los polinomios definidos como

$$G_2(X) = G_1(X) + pR_1(X), \quad H_2(X) = H_1(X) + pS_1(X)$$

cumplen las condiciones i), ii) y iii) y, por tanto, los tomamos como los segundos elementos de las sucesiones $(G_n(X))_{n\in\mathbb{N}}$ y $(H_n(X))_{n\in\mathbb{N}}$ respectivamente.
Si ahora lo suponemos cierto para dos polinomios $G_n(X)$ y $H_n(X)$ utilizando un razonamiento idéntico al anterior, podemos encontrar polinomios $G_{n+1}(X)$ y $H_{n+1}(X)$ que cumplan las condiciones i), ii) y iii). Este paso lo omitiremos para no extender en exceso la demostración, pues la forma de proceder es exactamente la misma, cambiando únicamente los subíndices y exponentes en función del $G_n(X)$ (respect. $H_n(X)$) que queramos calcular.
Recordemos que las congruencias entre polinomios son término a término. Entonces, si denotamos por $(g_i^{(n)})_{n\in\mathbb{N}}$ (respect. $(h_j^{(n)})_{n\in\mathbb{N}}$) a la sucesión en la que cada $g_i^{(n)}$ es el coeficiente que acompaña a X^i en el polinomio G_n, por la propiedad ii) se tiene que es una sucesión de Cauchy y, por tanto, convergente (lo mismo para $(h_j^{(n)})_{n\in\mathbb{N}}$).
Sean $G(X)$ y $H(X)$ los límites de $G_{n+1}(X)$ y $H_{n+1}(X)$ respectivamente, es decir, los coeficientes de $G(X)$ y $H(X)$ son los límites de las correspondientes sucesiones de coeficientes de $G_{n+1}(X)$ y $H_{n+1}(X)$. Vamos a razonar para $G(X)$, siendo idéntico para $H(X)$.
Primeramente, sea $n \in \mathbb{N}$ cualquiera, entonces, como $G(X)_{n+1} \equiv G_n(X) \pmod{p^n}$, para cualquier $m = n + k > n$ se tendría que

$$\begin{gathered} G_m(X) - G_n(X) = G_m(X) - G_{m-1}(X) + G_{m-1}(X) + G_{m-2}(X) - G_{m-2}(X) + ...+ \\ +G_{m-k+1}(X) - G_{m-k+1}(X) - G_n(X), \end{gathered}$$

y teniendo en cuenta que p^n divide a cada resta $(G_{i+1}(X) - G_i(X))$ (siempre refiriéndonos a los coeficientes), concluimos que $G_m(X) \equiv G_n(X) \pmod{p^n}$ para cada $m > n$. Ahora, si $m \longrightarrow \infty$,

$$G(X) \equiv G_n(X) \pmod{p^n}$$

y, como esto es cierto para un número natural cualquiera, tomamos $n = 1$ y tenemos $G(X) \equiv G_1(X) \pmod{p}$ (respect. $H(X) \equiv H_1(X) \pmod{p^n}$). Además, en virtud de esto último, es claro que $G(X)$ es mónico.
Por último, si llamamos b_i al coeficiente que acompaña a X^i en el polinomio $G(X)H(X)$, entonces sabemos que $b_i = \lim_{n\to\infty} b_i^{(n)}$ donde $b_i^{(n)}$ es el coeficiente que acompaña a X^i en el polinomio $G_n(X)H_n(X)$. Usando la propiedad iii) que satisfacen los polinomios $G_n(X)H_n(X)$, tenemos que, si denotamos por f_i al coeficiente que acompaña a X^i en el polinomio $F(X)$,

$$|f_i - b_i^{(n)}|_p \leq p^{-n},$$

para cada $n \in \mathbb{N}$ y cada $i \in \{0, 1, ..., d\}$. Fijado un $\epsilon > 0$ cualquiera, sabemos que existe $n_0 \in \mathbb{N}$ tal que $p^{-n} < \epsilon$ para cada $n \geq n_0$. Por tanto, para todo $n \geq n_0$,

$$|f_i - b_i^{(n)}|_p \leq p^{-n} < \epsilon.$$

Concluimos que $f_i = \lim_{n\to\infty} b_i^{(n)} = b_i$ y, en consecuencia, $F(X) = G(X)H(X)$, concluyendo así la demostración. □

Antes finalizar este trabajo, no podemos despedirnos sin antes enunciar un resultado de gran importancia en la teoría p-ádica. Aunque no lo vayamos a probar, ya que su demostración requeriría un estudio pormenorizado de las formas cuadráticas y de sus propiedades, algo que no creemos necesario pues se alejaría de la finalidad de esta memoria, con el fin de justificar que los números p-ádicos tienen utilidad práctica y no solo teórica, presentamos el siguiente teorema, el cual se lo debemos a los matemáticos alemanes Helmut Hasse & Hermann Minkowski y dice así:

Teorema 3.4.9 (**Hasse-Minkowski**). *Sea*

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

una forma cuadrática (polinomio homogéneo de segundo grado en n variables). Entonces la ecuación

$$F(X_1, X_2, ..., X_n) = 0$$

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

Demostración. Ver el texto de Borevich & Shafarevich [7]. □

Referencias

[1] GOUVÊA, Fernando Q. *p-adic Numbers*. Springer Berlin Heidelberg, 1997.

[2] RIBENBOIM, Paulo. *The theory of classical valuations*. Springer Science & Business Media, pp. 55-61, 2012.

[3] FUCHS, Laszlo. *Partially ordered algebraic systems*. Courier Corporation, pp. 44-46, 2014.

[4] CONRAD, B.; LANDESMAN, A. *Math 676: Algebraic Number Theory*. 2019. `http://math.stanford.edu/~conrad/676Page/handouts/ostrowski.pdf` (20/06/2024)

[5] JOSÉ CARLOS SANTOS, (`https://math.stackexchange.com/users/446262/jos\%c3\%a9-carlos-santos`). *Examples of Cauchy sequences in the rational numbers that do not converge in said set with respect to the p-adic topology*. MathExchange (2022-12-20). `https://math.stackexchange.com/q/4599448` (20/06/2024)

[6] ZHENG, YIDUAN. *p-ADIC NUMBERS, Qp, AND HENSEL'S LEMMA*. 2020. `https://math.uchicago.edu/~may/REU2020/REUPapers/Zheng,Yiduan.pdf` (20/06/2024)

[7] BOREVICH, Zenon Ivanovich; SHAFAREVICH, Igor Rostislavovich. *Number theory*. Academic press, pp.60-62, 1986.