UNIVERSIDAD AUTÓNOMA DE QUERÉTARO

Facultad de Ingeniería

Licenciatura en Matemáticas Aplicadas

SERIE DE POINCARÉ PARA POLINOMIOS FUERTEMENTE NO DEGENERADOS

TESIS

Que como parte de los requisitos para obtener el grado de

Licenciado en Matemáticas Aplicadas

Presenta:

Juan Mario Hernández Hernández

Dirigido por:

M.C. Víctor Antonio Aguilar Arteaga

Santiago de Querétaro, Querétaro. 2016.

UNIVERSIDAD AUTÓNOMA DE QUERÉTARO

Facultad de Ingeniería

Licenciatura en Matemáticas Aplicadas

SERIE DE POINCARÉ PARA POLINOMIOS FUERTEMENTE NO DEGENERADOS

TESIS

Que como parte de los requisitos para obtener el grado de

Licenciado en Matemáticas Aplicadas

Presenta:

Juan Mario Hernández Hernández

Dirigido por:

M.C. Víctor Antonio Aguilar Arteaga

Sinodales:

M.C. Víctor Antonio Aguilar Arteaga
Presidente

Dr. Samuel Estala Arias
Secretario

M.C. Roberto Torres Hernández
Sinodal

L.M.A. Iván González García
Sinodal

A MI MADRE ISABEL

Quien es un ejemplo de vida, pues a pesar de sus propias adversidades, desde niño supo entenderme y guiarme, celebrar mis triunfos y consolarme en mis fracasos, quien supo otorgarme y alimentar ese poder interno, para sentir que yo era capaz de alcanzar cualquier meta que me propusiera en esta vida.

Agradecimientos

A través de los años he pasado distintas pruebas en mi vida y he aprendido algunas lecciones de cada una de ellas, considero que en esta vida encontramos cosas, personas, lugares, que forman parte de nuestro presente, algunos de ellos continuarán con nosotros y algunos otros inevitablemente quedarán en nuestro pasado, así, al final lo único que realmente nos pertenece y que nadie nos podrá arrebatar son los recuerdos, cada uno, bueno o malo, es una huella que el tiempo ha dejado en cada uno de nosotros, como una marca de sabiduría terrena.

Este trabajo representa el final de un ciclo y en cierta forma un trofeo a cada una de las adversidades que he tenido que sortear a lo largo de mis años, siempre bajo la protección, apoyo y consuelo de Dios. Es por ello que considero necesario mencionar y agradecer a ciertas personas que han tenido un impacto fuerte en mi camino y han sido pieza fundamental en la realización de este trabajo.

Agradezco principalmente a cada uno de los miembros de mi familia, que es lo más valioso que tengo en la vida. A mis padres: Juan e Isabel; mis hermanas: Ivette y Annette; mi cuñado Moisés; a mis sobrinas: Itzel, Yarette y Xiromy. Con quienes he compartido el paso de mis años, quienes me han apoyado a lo largo de mi vida en incontables situaciones y con quienes he aprendido el verdadero valor de la lealtad.

Agradezco:

Al M.C. Víctor Antonio Aguilar Arteaga, quien me platicó sobre este tema y me ofreció su guía y apoyo con dedicación y paciencia en la realización de este trabajo.

Al Dr. Samuel Estala Arias, M.C. Roberto Torres Hernández y L.M.A. Iván González García, por sus observaciones que ayudaron de manera significativa a mejorar este trabajo.

A mis amigos del COBAQ: Julio, Herme, Rosa, Lucy, Gerardo, Mauricio, Cecilia y Cruz; con quienes viví una de las etapas más intensas de mi vida y formé una amistad que ha perdurado a lo largo de estos años.

A mis amigos de la carrera: David, Martín, Lili, Mariana y José, por haberme acompañado a lo largo de este proceso universitario que estuvo lleno de experiencias inolvidables y con quienes compartí los momentos de angustia, satisfacción, estrés, frustración y plenitud que ofrece la Licenciatura en Matemáticas Aplicadas.

Introducción

El campo de los números p-ádicos ($\mathbb{Q}_p$), donde p es un número primo fijo, es una completación de los números racionales distinta a los números reales. Esta diferencia surge de una interpretación diferente del concepto de valor absoluto. Podemos decir, de manera intuitiva, que dos números enteros están p-ádicamente cerca si su diferencia es divisible por una potencia alta de p, cuanto más grande es la potencia, mas cercanos se encuentran los números.

Estos números han sido introducidos en diferentes áreas de la matemática como: teoría de números, geometría algebraica, topología algebraica y análisis matemático. Al ser los números p-ádicos una completación de los números racionales, los conceptos del análisis clásico se extendieron sobre este campo (siendo Hasse uno de los impulsores más importantes), dando origen a lo que hoy se conoce como análisis p-ádico.

Básicamente la idea de la construcción de los números p-ádicos descansa sobre la definición de un valor absoluto no arquimediano llamado valor absoluto p-ádico, definido a su vez, en términos de la valuación p-ádica, la cual se define de la siguiente manera:

Dado p un número primo fijo, la valuación p-ádica en $\mathbb{Z}$ es la función $v_p : \mathbb{Z} - \{0\} \to \mathbb{R}$ tal que, para cada entero $n \in \mathbb{Z}$ con $n \neq 0$, $v_p(n)$ es el único entero no negativo que satisface

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

El dominio de la función $v_p(n)$ se extiende al campo de los números racionales de la siguiente manera:

$$\text{Si } x = \frac{a}{b} \in \mathbb{Q} - \{0\}, \text{ entonces } v_p(x) = v_p(a) - v_p(b)$$

con la convención en ambos dominios de que $v_p(0) = \infty$.

Una vez definida la valuación p-ádica, podemos definir el valor absoluto p-ádico para cualquier $x \in \mathbb{Q}$, como

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

En el libro "Teoría de Números" [2], Borevich y Shafarevich conjeturaron lo siguiente:

Sea $F(x) \in \mathbb{Z}_p[x_1, ..., x_k]$, *y sea* $c_n = \# \left\{ x \in \left(\frac{\mathbb{Z}_p}{p^n \mathbb{Z}_p} \right)^k \ \middle| \ F(x) \equiv 0 \pmod{p^n} \right\}$ *para* $n \geq 1$, *es decir, el número de soluciones de la congruencia* $F(x) \equiv 0 \pmod{p^n}$, *donde* $c_0 = 1$. *Entonces la serie de Poincaré asociada a* F *definida como*

$$P_F(t) = \sum_{n=0}^{\infty} c_n (p^{-k} t)^n$$

es una función racional de t, *con* $t \in \mathbb{C}$ *y* $|t| < 1$.

Esta conjetura llamó la atención de la comunidad matemática de aquella época y la solución se dio en 1974, propuesta por el japonés Jun-Ichi Igusa. Sin embargo, la demostración dada no fue constructiva, por lo que el problema de expresar la serie de Poincaré asociada a un polinomio como función racional explícita quedó abierto.

En esta tesis se aborda el estudio de la serie de Poincaré asociada a polinomios fuertemente no degenerados culminando con una aproximación algebraica de ésta, exhibiendo que efectivamente, para un polinomio fuertemente no degenerado F la serie de Poincaré asociada es una función racional de la forma:

$$P_F(t) = \frac{R(t)}{(1 - p^{-1}t)(1 - p^{k(d-1)}(p^k t)^d)}$$

donde $R(t)$ es un polinomio de grado d efectivamente calculable.

La organización de la tesis es la siguiente:

En el capítulo 1 se enuncian los conceptos fundamentales de las diferentes áreas de las matemáticas que son necesarios para el posterior desarrollo de la teoría central de este documento.

En el capítulo 2 se introduce el campo de los números p-ádicos y se estudian algunas de sus propiedades, haciendo énfasis en las partes fundamentales necesarias para el estudio y correcta comprensión del tema central de esta tesis que se aborda en el capítulo 3.

En el capítulo 3 se introduce la serie de Poincaré y se muestra el camino para llegar a la construcción de una fórmula de la serie asociada a polinomios fuertemente no degenerados.

Índice general

Capítulo 1

Fundamentos

El objetivo de este capítulo es presentar un breve resumen de algunos de los conceptos básicos de la Teoría de números, Álgebra moderna, Topología, Análisis y Árboles; éstos son los fundamentos matemáticos que servirán de base para el estudio de los temas centrales de los capítulos 2 y 3, que son básicamente, el estudio del campo de los números p-ádicos, comenzando por su construcción y terminando con el estudio de algunas de sus propiedades y el estudio de la serie de Poincaré asociada a polinomios fuertemente no degenerados.

Al no ser el tema de estudio de este trabajo los conceptos de las teorías matemáticas anteriormente citadas, omitiremos la demostración de los teoremas que enunciaremos, dando como referencia la cita bibliográfica en la que se puede encontrar la demostración formal de ellos.

Antes de comenzar con la teoría matemática es importante mencionar que a lo largo de esta tesis utilizaremos el símbolo $\subseteq$ para denotar *subconjunto* y el símbolo $\subset$ para denotar *subconjunto propio*.

1.1. Teoría de números

Teorema 1.1 (Algoritmo de la división)
Si $a, b \in \mathbb{Z}$, con $b \neq 0$, entonces existen $q, r \in \mathbb{Z}$, llamados cociente y residuo respectivamente, tales que $a = bq + r$, con $0 \leq r < |b|$.

Para consultar la demostración de este teorema ver [19, p. 17].

Si a, b son dos números enteros, con $b \neq 0$, decimos que a **divide** a b, o que b es **múltiplo** de a, si existe un entero q, tal que $b = aq$ (es decir, en la división tenemos $r = 0$). La notación que se utiliza para describir este

hecho es $a|b$, que se lee "a divide a b", o también podemos decir que a es un **divisor** de b. Si a no divide a b lo denotaremos mediante $a \nmid b$.

Decimos que el **máximo común divisor** de dos enteros a, b, siendo alguno de ellos distinto de cero, es el entero g que cumple:
i) $g|a$ y $g|b$.
ii) Si d es cualquier entero tal que $d|a$ y $d|b$, entonces $d|g$.
El máximo común divisor de a, b se denota por $mcd(a, b)$, o en ocasiones, cuando el contexto no crea ambigüedad, se denota simplemente por (a, b). Si $mcd(a, b) = 1$, decimos que a y b son **coprimos** o **primos relativos**.

Teorema 1.2 (Euclides)
Dados $a, b, c \in \mathbb{Z}$ tal que $a|bc$ y $mcd(a, b) = 1$, entonces $a|c$.

Para consultar la demostración de este teorema ver [19, p. 20].

Un entero p se dice que es un **número primo** si $p \neq 0, \pm 1$ y si sus únicos divisores son ± 1 y $\pm p$; aunque se acostumbra considerar sólo a los números primos positivos (si p es primo, $-p$ también lo es). Cuando los primos difieren a lo más por un signo, decimos que son **asociados**. Un número entero que no es primo se llama **compuesto**.

Teorema 1.3 (Teorema fundamental de la aritmética)
Todo entero a distinto de $0, \pm 1$ se puede factorizar de la forma $a = p_1 p_2 \cdots p_r$, con los p_i primos, y esta factorización de a es esencialmente única, es decir, si $a = q_1 q_2 \cdots q_s$ es otra factorización de a con los q_i primos, entonces $r = s$ y existe una biyección $\sigma : \mathbb{I}_r \to \mathbb{I}_r$ tal que $p_i = q_{\sigma(i)}$, donde $\mathbb{I}_r = \{1, 2, ..., r\}$.

Demostración
Dado $a \neq 0, \pm 1$, tenemos $|a| > 1$, por lo que $a > 1$ o $a < -1$. Supongamos $a > 1$. Haremos inducción sobre el entero positivo a para probar la existencia de la factorización.

i) Para $a = 2$, resulta que a es primo y obtenemos directamente la factorización deseada.

ii) Ahora supongamos que el entero a se puede factorizar como producto de primos para $a \leq n$.
Probaremos que existe la factorización deseada para $a = n + 1$. Si a es primo tenemos $a = p$, que es de hecho la factorización deseada. Si a no es primo, entonces a es compuesto y se puede escribir como $a = bc$ con $1 < b < a$ y $1 < c < a$, y por hipótesis de inducción, b y c se pueden factorizar como producto de primos (pues son menores que a), digamos:

$$b = p_1 \cdots p_m \quad \text{y} \quad c = q_1 \cdots q_n$$

con los p_i y q_i primos. Y juntando estas factorizaciones podemos escribir a de la siguiente forma $a = bc = p_1 \cdots p_m q_1 \cdots q_n$, que es una factorización de a en primos.

Si $a < -1$, entonces $-a > 1$ y si factorizamos $-a$ como producto de primos, digamos $-a = p_1 \cdots p_m$ entonces $a = (-p_1)p_2 \cdots p_m$.
Ahora probaremos la unicidad de la factorización.
Supongamos que a tiene dos factorizaciones, es decir, $a = p_1 \cdots p_r = q_1 \cdots q_s$ con p_i, q_i primos. Sin pérdida de generalidad supongamos $r \leq s$. Entonces la igualdad $p_1 \cdots p_r = q_1 \cdots q_s$ implica que $p_1 | q_1 \cdots q_s$, y como p_1 es primo, tenemos que p_1 divide a algún q_j. Ahora, si reordenaramos los primos q_i, en caso de hacer falta, tendríamos que $q_j = q_1$ y así $p_1 | q_1$, pero como ambos son primos, esto implica que $p_1 = q_1$. Ahora, cancelando p_1 de la igualdad sobre la que estamos trabajando, obtenemos $p_2 \cdots p_r = q_2 \cdots q_s$. Utilizando un razonamiento análogo al que acabamos de explicar, podemos cancelar todos los primos p_i, para obtener al final $1 = q_{r+1} \cdots q_s$, lo que sólo es posible cuando se han cancelado todos los primos q_i, es decir, en el caso $r = s$.
Observemos que en el reordenamiento que se hace en cada paso del proceso anterior obtenemos la biyección deseada.

■

Una **relación binaria** R definida en un conjunto A es un subconjunto de A^2. Decimos que $a, b \in A$ están relacionados si $(a, b) \in R$, y se suele denotar este hecho mediante aRb.

Decimos que una relación R es un conjunto A es una **relación de equivalencia** si cumple la siguientes propiedades:

i) **Reflexividad:** xRx para todo $x \in A$.

ii) **Simetría:** xRy implica yRx para cualesquiera $x, y \in A$.

iii) **Transitividad:** xRy y yRz implican que xRz para todo $x, y, z \in A$.

Si R es una relación de equivalencia, dado $x \in A$, la **clase de equivalencia** de x respecto a R es $[x]_R = \{y \in A \mid xRy\}$.

Dado un entero fijo n diremos que dos enteros a, b son **congruentes módulo** n si $n \mid a - b$ y denotamos este hecho por $a \equiv b \pmod{n}$. Es fácil probar que la congruencia módulo n es una relación de equivalencia en $\mathbb{Z}$, entonces para $a \in \mathbb{Z}$ su clase de equivalencia módulo n es el conjunto $[a] := \{x \in \mathbb{Z} \mid x \equiv a \pmod{n}\}$. Se puede probar también que el residuo de dividir cualquier entero $x \in [a]$ entre n es el mismo residuo que queda al dividir a entre n, sabemos que sólo hay un número finito de posibilidades

para el residuo r que queda al dividir cualquier número entero m entre n, a saber: $r = 0, 1, ..., n-1$; por lo tanto sólo hay n clases de equivalencia: $[0], [1], ..., [n-1]$. Al conjunto de estas clases de equivalencia se les llama **clases residuales módulo** n y un elemento $x \in [a]$ se llama **representante de la clase** $[a]$.

Si definimos la suma y el producto para dos clases residuales $[a], [b]$ como $[a] + [b] = [a+b]$ y $[a][b] = [ab]$ (se puede probar de manera sencilla que las operaciones de suma y producto de dos clases residuales están bien definidas), entonces el conjunto de clases residuales módulo n con las operaciones definidas forman un anillo conmutativo con uno[1] y se denota por $\mathbb{Z}/m\mathbb{Z}$.

Teorema 1.4
La congruencia lineal $ax \equiv b \pmod{m}$ *tiene soluciones módulo* m *si y sólo si* $d = mcd(a, m)|b$. *Cuando hay soluciones, éstas tienen la forma* $x \equiv x_0 + m't \pmod{m}$ *donde* $m = m'd$ *y* x_0 *es cualquier solución particular de la congruencia.*

Para consultar la demostración de este teorema ver [19, p. 43].

1.2. Álgebra

Un **grupo** es un conjunto no vacío G con una operación binaria "$\cdot$"(llamada producto) tal que, para cualesquiera $x, y, z \in G$ se cumple:

i) $x \cdot y \in G$ (**Cerradura**).

ii) $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ (**Conmutatividad**).

iii) Existe un elemento $e \in G$ llamado **identidad** tal que $x \cdot e = e \cdot x = x$.

iv) x tiene **inverso**, es decir, existe $x' \in G$ tal que $x \cdot x' = x' \cdot x = e$.

Si además se cumple que $x \cdot y = y \cdot x \ \forall x, y \in G$ decimos que G es un **grupo abeliano**.

Un subconjunto H de un grupo G es **subgrupo** de G si respecto al producto definido en G, el subconjunto H forma un grupo. Si H es subgrupo de G, y $a \in G$, entonces $Ha := \{ha \in G \mid h \in H\}$; al conjunto Ha se le llama **clase lateral derecha** de H en G (análogamente se define una clase lateral izquierda de H en G). Un subgrupo N de G se dice que es un **subgrupo normal** de G, si para toda $g \in G$ y toda $n \in N$, $gng^{-1} \in N$.

[1] Ver definición de anillo conmutativo con uno en la sección de álgebra.

Proposición 1.5
N es un subgrupo normal de G si y sólo si $gNg^{-1} = N$ para todo $g \in G$.

Para consultar la demostración de esta proposición ver [7, p. 57] .

Por la proposición anterior sabemos que $gNg^{-1} = N$, de donde obtenemos que $(gNg^{-1})g = Ng$, así, $gN = Ng$, es decir, la clase lateral izquierda gN es la clase lateral derecha Ng. Si para dos conjuntos A, B definimos $AB = \{ab \mid a \in A, b \in B\}$, entonces, suponiendo que N es un subgrupo normal de G, y que $a, b \in G$, consideraremos el "producto"$(Na)(Nb)$, y dado que N es normal en G obtenemos

$$NaNb = N(aN)b = N(Na)b = NNab = Nab.$$

Lo que nos proporciona la fórmula $NaNb = Nab \ \ (*)$. Ahora denotaremos por G/N la colección de todas las clases laterales derechas de N en G. Entonces es fácil comprobar que G/N con el producto definido por $(*)$ es un grupo (ver [7, p. 58]), a este grupo se le llama **grupo cociente** o **grupo factor** de G por N.

Dado un conjunto R, decimos que éste es un **anillo**, si en R se encuentran definidas dos operaciones "+" y " $\cdot$ " llamadas suma y producto respectivamente, tales que para cualesquiera $x, y, z \in R$ se cumple:

i) R es un grupo abeliano bajo la suma.

ii) $x \cdot y \in R$.

iii) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

iv) $x \cdot (y + z) = x \cdot y + x \cdot z$,
$(y + z) \cdot x = y \cdot x + z \cdot x$ (**Leyes distributivas**).

En este caso denotamos con 0 y $-x$ a los elementos identidad e inverso respectivamente, ambos bajo la suma.

Si además existe un elemento $1 \in R$ tal que $x \cdot 1 = 1 \cdot x = x \ \forall x \in R$, decimos que R es un **anillo con elemento unitario** o **anillo con unidad**. Por otro lado, si se cumple que $xy = yx \ \forall x, y \in R$ llamamos a R **anillo conmutativo**.

Si R es un anillo conmutativo, decimos que $x \neq 0 \in R$ es un **divisor de cero** si $\exists y \neq 0 \in R$ tal que $xy = 0$.

A un anillo se le llama **anillo con división** si sus elementos distintos del elemento cero forman un grupo bajo la multiplicación. Un **campo** es un anillo conmutativo con división.

Si x y y son elementos de un anillo conmutativo R, entonces x **divide a** y **en** R (x es **divisor** de y o y es **múltiplo** de x), denotado por $x|y$ si existe un elemento $z \in R$ tal que $y = zx$.

Un elemento u en un anillo conmutativo R es llamado una **unidad** si $u|1$ en R, es decir, $\exists v \in R$ tal que $uv = 1$, el elemento v es llamado **inverso** de u y generalmente u es denotado por u^{-1}.

Un subconjunto S de un anillo conmutativo R es un **subanillo** de R si, para cualesquiera $x, y \in S$ se cumple:

i) $1 \in S$.

ii) $x - y \in S$.

iii) $xy \in S$.

Si A y R son anillos conmutativos, un **homomorfismo** de anillos es una función $f : A \to R$ tal que, para cualesquiera $x, y \in A$:

i) $f(1) = 1$.

ii) $f(x + y) = f(x) + f(y)$.

iii) $f(xy) = f(x)f(y)$.

Un homomorfismo que también es una biyección se llama **isomorfismo**. En tal caso, los anillos A y R son llamados **isomorfos** y este hecho se denota por $A \cong R$.

Un **ideal** de un anillo conmutativo R es un subconjunto I de R que cumple lo siguiente:

i) $0 \in I$.

ii) Si $x, y \in I$ entonces $x + y \in I$.

iii) Si $x \in I$ y $r \in R$ entonces $rx \in I$.

Si $I \neq \{0\}, R$ decimos que es un ideal propio. Si I es un ideal propio y dado otro ideal J de R, se cumple que si $I \subseteq J \subseteq R$ entonces $J = I$ o $J = R$, entonces decimos que I es un **ideal maximal** de R. Un anillo conmutativo R es llamado **anillo local** si tiene un único ideal maximal.

Si R es un anillo conmutativo y $b_1, ..., b_n \in R$, entonces el conjunto de todas las combinaciones lineales $I = \{r_1b_1 + \cdots + r_nb_n \mid r_i \in R\}$ es un ideal en R y es llamado el **ideal generado** por $b_1, ..., b_n$. En particular si $n = 1$ entonces $I = \{rb \mid r \in R\}$ es un ideal en R y es llamado el **ideal principal** generado por b.

Dado un ideal I de un anillo R, definimos R/U (**anillo cociente**) como el conjunto de todas las clases laterales de I en R obtenidas al considerar

a I como subgrupo de R bajo la suma. En este caso no hay distinción de clase lateral izquierda y derecha puesto que R es un grupo abeliano bajo la suma, así las clases laterales son de la forma $r + I$, con $r \in R$. De acuerdo con lo expuesto al principio de la sección, R/U es un grupo bajo la adición dada por $(a + I) + (b + I) = (a + b) + I$.

Ahora, para que R/U tenga una estructura de anillo lo dotamos con el producto $(a + I)(b + I) = ab + I$. Se puede probar que efectivamente R/U satisface los axiomas de anillo con las dos operaciones definidas en él, para más detalles ver [15, p. 182] y [7, p. 116].

Teorema 1.6
Si R es un anillo conmutativo con unidad y M es un ideal de R entonces M es ideal maximal de R si y sólo si R/M es un campo.

Para consultar la demostración de este teorema ver [7, p. 122].

1.3. Espacios métricos

Un **espacio métrico** es un par $\langle X, d\rangle$ (cuando no se presta a ambigüedades se escribe simplemente X) donde X es un conjunto y d es una **métrica (distancia)** en X, es decir, $d : X \times X \to \mathbb{R} \cup \{0\}$ es una función que, para cualesquiera $x, y, z \in X$, satisface:

i) $d(x, y) = 0$ si y sólo si $x = y$.
ii) $d(x, y) = d(y, x)$.
iii) $d(x, y) \leq d(x, z) + d(z, y)$ (**Desigualdad del triángulo**).

Los elementos de X son llamados puntos.

Por **sucesión** entendemos una función f definida en todos los números naturales. Si $f(n) = x_n$ se acostumbra representar la sucesión f por el símbolo $\{x_n\}$. Si A es un conjunto y $x_n \in A$ para todo n, decimos que $\{x_n\}$ es una sucesión en A, o una sucesión de elementos de A.

Se dice que una sucesión $\{a_n\}$ en un espacio métrico $\langle X, d\rangle$ **converge** si existe un punto $a \in X$ con la propiedad de que para cada $\epsilon > 0$ existe un número natural N tal que $n \geq N$ implica que $d(a_n, a) < \epsilon$. En este caso decimos que $\{a_n\}$ converge hacia a o que a es el límite de $\{a_n\}$, y escribimos $a_n \to a$ o $\lim_{n\to\infty} a_n = a$. Si $\{a_n\}$ no converge se dice que **diverge**.

Dada una sucesión $\{a_n\}$ consideremos la sucesión $\{n_k\}$constituida por enteros positivos de modo que $n_1 < n_2 < n_3 < \cdots$. La sucesión $\{a_{n_i}\}$ se llama **subsucesión** de $\{a_n\}$.

Dada una sucesión $\{a_n\}$ definimos una sucesión asociada $\{s_n\}$, donde $s_n = \sum_{k=1}^{n} a_k$. Utilizamos para $\{s_n\}$ la expresión $a_1 + a_2 + a_3 + \cdots$ abreviado frecuentemente con $\sum_{n=1}^{\infty} a_n$. A esta última se le llama **serie infinita** o simplemente serie. A los números s_n se les llama **sumas parciales** de la serie. Si la sucesión $\{s_n\}$ converge hacia s decimos que la serie **converge** y en este caso escribimos

$$\sum_{n=1}^{\infty} = s.$$

Al número s se le llama **suma de la serie**. Por otro lado si $\{s_n\}$ diverge, decimos que la serie **diverge**. Frecuentemente escribimos $\sum a_n$ para escribir de forma más compacta el símbolo de serie cuando esto no se presta a ambigüedades.

En el siguiente teorema y comentario el símbolo $|\cdot|$ denota el módulo complejo.

Teorema 1.7 (Criterio de comparación)
Si $|a_n| \leq c_n$ para $n \geq N_0$, donde N_0 es un número natural dado y $\sum c_n$ converge también converge $\sum a_n$.

Para consultar la demostración de este teorema ver [16, p. 64].

Decimos que $\sum a_n$ es **absolutamente convergente** si $\sum |a_n|$ converge.

Teorema 1.8
Si $\sum a_n$ converge absolutamente entonces $\sum a_n$ converge.

Para consultar la demostración de este teorema ver [16, p. 76].

1.4. Topología

Una **topología** sobre un conjunto X es una colección $\mathcal{T}$ de subconjuntos de X con las siguientes propiedades:

i) $\emptyset, X \in \mathcal{T}$.

ii) La unión arbitraria de elementos de $\mathcal{T}$ pertenece a $\mathcal{T}$.

iii) La intersección finita de elementos de $\mathcal{T}$ pertenece a $\mathcal{T}$.

Un conjunto X para el que se ha definido una topología $\mathcal{T}$ se llama **espacio topológico**, denotado $\langle X, \mathcal{T} \rangle$, o si no se presta a ambigüedades, simplemente X.

Si $\langle X, \mathcal{T} \rangle$ es un espacio topológico decimos que un subconjunto A de X es **abierto** si $A \in \mathcal{T}$ y decimos que es **cerrado** si $X - A \in \mathcal{T}$.

Dado un subconjunto A de X, la **clausura** de A se define como la intersección de todos los conjuntos cerrados que contienen a A y se denota por $\overline{A}$. Un punto $p \in A$ es llamado **punto interior** de A si existe un conjunto abierto G tal que $p \in G \subseteq A$; el conjunto de puntos interiores de A es llamado el **interior** de A y se denota por $Int(A)$. El **exterior** de A, escrito como $Ext(A)$, se define como el interior de $X - A$, y la **frotera** de A denotada por $Fr(A)$ se define como el conjunto de puntos de X que no pertenecen a $Int(A)$ ni a $Ext(A)$ es decir $Fr(A) = X - (Int(A) \cup Ext(A))$.

Si A es subconjunto de un espacio topológico X, y si $x \in X$, decimos que x es **punto límite** (punto de acumulación) de A si para cada conjunto abierto G que contiene a x se cumple que $(G - \{x\}) \cap A \neq \emptyset$. El conjunto de todos los puntos límite de A se denota por A'.

Teorema 1.9
Sea A un subconjunto de un espacio topológico X, entonces $\overline{A} = A \cup A'$.
Para consultar la demostración de este teorema ver [13, p. 111]

Teorema 1.10
Sea A subconjunto de un espacio topológico X, entonces $Int(A)$ y $Fr(A)$ son disjuntos y $\overline{A} = Int(A) \cup Fr(A)$.
Para consultar la demostración de este teorema ver [3, p. 72].

Un subconjunto A de un espacio X se dice que es **denso** en X si $\overline{A} = X$.

1.5. Árboles

Dado un conjunto A, una **cadena** en A es un elemento u de A^n, para $n \in \mathbb{N}$. El número natural n se denomina **longitud** de u y se denota por

$|u|$. La única cadena de longitud 0 se denomina **cadena vacía** y es denotada por ϵ. El conjunto $\cup_{i\geq 0} A^i$ de todas las cadenas en A se denota por A^*.

Dadas dos cadenas $u = (u_1, ..., u_n)$, $v = (v_1, ..., v_m)$, la **concatenación** de ambas, denotada por uv es la cadena $(u_1, ..., u_n, v_1, ..., v_m)$.

Dadas $u, v \in A^*$, v es **prefijo** de u si existe $w \in A^*$ tal que $u = vw$. Si v es prefijo de u se denota por $v \leq u$. Análogamente v es **sufijo** de u si existe $w \in A^*$ tal que $u = wv$. Decimos que v es **subcadena** de u si existen $w_1, w_2 \in A^*$ tales que $u = w_1 v w_2$. Si v es prefijo (sufijo o subcadena) de u se dice **propio** si $u \neq v$. Si u no es prefijo de v, ni v es prefijo de u, decimos que u, v son **disjuntas** y se denota por $u|v$.

Un **dominio de árbol** D es un subconjunto no vacío de $\mathbb{N}^*$ (cadenas de enteros positivos) que cumple:
i) Para todo $u \in D$, todo prefijo de u está en D.
ii) Para todo $u \in D$, $i \in \mathbb{N}$, si $ui \in D$ entonces $uj \in D$ para $1 \leq j \leq i$.

Dado un conjunto Σ (al que llamamos conjunto de etiquetas), un **árbol Σ-etiquetado** (en adelante simplemente **árbol**) es una aplicación $t : D \to \Sigma$, siendo D un dominio de árbol. El dominio de un árbol t lo denotamos por $dom(t)$.

Sea t un árbol. Un **nodo** de t es un elemento de $dom(t)$. El **grado** de un nodo u es $g(u) = \#\{i \mid ui \in dom(t)\}$. El árbol t está **finitamente ramificado** si para todo $u \in dom(t)$, $g(u)$ es finito. Una hoja de t es un nodo tal que $g(u) = 0$. El nodo representado por ϵ se denomina **raíz** del árbol. El árbol t es **finito** si $dom(t)$ lo es, análogamente si $dom(t)$ es infinito, entonces decimos que t es un **árbol infinito**. Dado $u \in dom(t)$, los nodos $ui \in dom(t)$ se denominan **hijos** de u. Dados dos nodos $u, v \in dom(t)$, decimos que u es **antecesor** de v, (o que v es **sucesor** de u) si $u \leq v$.

Dado un árbol t, un **camino finito** con **origen** u y **destino** v, es una sucesión de nodos de t de la forma u_0 , ... , u_n con $u_0 = u$ y $u_n = v$, tal que, para todo j, $1 \leq j \leq n$, $u_j = u_{j-1} i_j$; la **longitud** de tal camino es n. Una **rama** es un camino con origen en la raíz y destino en una hoja. Un **camino infinito** con origen u es una secuencia infinita de nodos de t de la forma u_0, u_1, u_2 , ... tal que $u_0 = u$ y para todo $j \geq 1$, $u_j = u_{j-1} i_j$. Si t es un árbol finito, la **altura** de un nodo $u \in dom(t)$ es la mayor longitud de los caminos con origen u. La **profundidad** de t es la altura de su raíz.

Lema 1.11 (Lema de König)
Sea t un árbol infinito finitamente ramificado, entonces existe un camino infinito con origen en la raíz.

Para consultar la demostración de este lema ver [9, p. 5].

Capítulo 2

Números p-ádicos

El objetivo de este capítulo es construir el campo de los números p-ádicos, denotado por $\mathbb{Q}_p$ y estudiar algunas de sus propiedades más interesantes, lo cual será una base para el estudio de la serie de Poincaré, tema que abordaremos en el siguiente capítulo.

2.1. Principios básicos

El objetivo principal de esta sección será introducir un nuevo valor absoluto definido sobre los números racionales, esto nos dará una nueva forma de medir distancias y realizar cálculos. En secciones posteriores nos encargaremos de construir el campo de los números p-ádicos como una completación de los números racionales respecto a este nuevo valor absoluto. Sin embargo, estudiaremos a lo largo de esta sección las propiedades de los valores absolutos sobre campos en general, teoría que por supuesto será claramente aplicable al campo $\mathbb{Q}$.

A lo largo de este capítulo $\mathbb{K}$ denotará un campo arbitrario, y denotaremos mediante $\mathbb{R}_+ = \{x \in \mathbb{R} \mid x \geq 0\}$ al conjunto de números reales no negativos. Comenzaremos con la definición de valor absoluto sobre un campo, y analizaremos algunos hechos fundamentales derivados de la definición.

2.1.1. Valores absolutos sobre campos

Definición 2.1
*Un **valor absoluto** sobre $\mathbb{K}$ es una función $|\cdot|: \mathbb{K} \to \mathbb{R}_+$ que satisface las siguientes condiciones:*

i) $|x| = 0$ *si y sólo si* $x = 0$.

ii) $|xy| = |x||y| \quad \forall x, y \in \mathbb{K}$.

iii) $| x + y | \leq | x | + | y | \ \ \forall x, y \in \mathbb{K}$.

Si además el valor absoluto satisface $| x + y | \leq \text{máx}\{| x |, | y |\}\ \forall x, y \in \mathbb{K}$ *decimos que es un* ***valor absoluto no arquimediano****; en caso contrario se dice que el valor absoluto es* ***arquimediano****.*

Notemos que la condición $| x + y | \leq \text{máx}\{| x |, | y |\}$ implica la parte 3 de la definición de valor absoluto, ya que $\text{máx}\{| x |, | y |\} \leq | x | + | y |$.

Ejemplo 2.2

El ***valor absoluto trivial*** *sobre un campo* $\mathbb{K}$ *se define como sigue:*

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

Claramente este valor absoluto es no arquimediano.

Ejemplo 2.3

El valor absoluto sobre $\mathbb{Q}$ *definido de la siguiente manera*

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

es llamado el ***valor absoluto usual*** *sobre* $\mathbb{Q}$ *y lo denotaremos mediante* $| \cdot |_\infty$*, el por qué de esta notación será más claro cuando abordemos el estudio de los valores absolutos sobre* $\mathbb{Q}$*.*

Además este valor absoluto es arquimediano, pues, si tomamos $x = y = 1$ *tenemos* $|x + y| = |1 + 1| = |2| > 1 = \text{máx}\{|1|, |1|\}$.

Definición 2.4

Dado un número primo fijo p*, la* ***valuación p-ádica*** *en* $\mathbb{Z}$ *es la función* $v_p : \mathbb{Z} - \{0\} \to \mathbb{R}$ *definida como sigue:*

Para cada número entero $n \neq 0$*,* $v_p(n)$ *es el único entero positivo que satisface*

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

El dominio de la función $v_p(n)$ *se extiende al campo de los números racionales como sigue:*

$$Si \ x = \frac{a}{b} \in \mathbb{Q} - \{0\}, \ entonces \ v_p(x) = v_p(a) - v_p(b)$$

con la convención en ambos dominios de que $v_p(0) = \infty$*.*

Notemos que el teorema fundamental de la aritmética garantiza la existencia y unicidad de la valuación p-ádica definida sobre los números enteros.

Una pregunta básica que surge inmediatamente después de leer la definición de valuación p-ádica sobre los números racionales es preguntarnos si efectivamente esta bien definida, que es precisamente lo que probaremos a continuación con ayuda del siguiente lema.

Lema 2.5
Si $m, n \in \mathbb{Z}$, *entonces* $v_p(mn) = v_p(m) + v_p(n)$

Demostración
Sean $m, n \in \mathbb{Z}$, se tiene

$$\begin{aligned} m &= p^{v_p(m)}m' && con\ p \nmid m' \\ n &= p^{v_p(n)}n' && con\ p \nmid n'. \end{aligned}$$

De las ecuaciones anteriores tenemos

$$\begin{aligned} mn &= p^{v_p(m)}m'p^{v_p(n)}n' && con\ p \nmid m'n' \\ mn &= p^{v_p(m)+v_p(n)}m'n' && con\ p \nmid m'n'. \end{aligned}$$

Y por definición se tiene

$$v_p(mn) = v_p(m) + v_p(n).$$

■

Proposición 2.6
Para cualquier $x \in \mathbb{Q}$, $v_p(x)$ *no depende de la representación de* x *como cociente de dos enteros.*
Demostración
Sea $x \in \mathbb{Q}$ tal que $x = \frac{a}{b} = \frac{c}{d}$ con $a, b, c, d \in \mathbb{Z}$. Tenemos que

$$\begin{aligned} ad &= bc \\ v_p(ad) &= v_p(bc) \\ v_p(a) + v_p(d) &= v_p(b) + v_p(c) \\ v_p(a) - v_p(b) &= v_p(c) - v_p(d) \\ v_p\left(\frac{a}{b}\right) &= v_p\left(\frac{c}{d}\right). \end{aligned}$$

■

A partir de las proposiciones anteriores podemos deducir que para cualquier $x \in \mathbb{Q} - \{0\}$ se tiene

$$x = \frac{a}{b} = \frac{p^{v_p(a)}a'}{p^{v_p(b)}b'} = p^{v_p(a)-v_p(b)}\frac{a'}{b'} = p^{v_p(x)}\frac{a'}{b'}.$$

Así la valución p-ádica de un número racional queda determinada por la fórmula

$$x = \frac{a}{b} = p^{v_p(x)}\frac{a'}{b'}.$$

El siguiente lema muestra que la valuación p-ádica definida anteriormente efectivamente es una valuación sobre un campo.

Lema 2.7
Para todo x,y $\in \mathbb{Q}$*, se tiene:*

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

ii) $v_p(x+y) \geq \text{mín}\{v_p(x), v_p(y)\}$.

Demostración

i) Sean $x = \frac{a}{b}$, $y = \frac{c}{d}$. Se tiene que

$$\begin{aligned} v_p(x) + v_p(y) &= v_p(a) - v_p(b) + v_p(c) - v_p(d) \\ &= v_p(a) + v_p(c) - [v_p(b) + v_p(d)] \\ &= v_p(ac) - v_p(bd) \\ &= v_p\left(\frac{ac}{bd}\right) \\ &= v_p(xy). \end{aligned}$$

ii) Sean x, y como en el inciso anterior, entonces

$$x = p^{v_p(x)}\frac{a'}{b'}, \qquad y = p^{v_p(y)}\frac{c'}{d'}$$
$$x + y = p^{v_p(x)}\frac{a'}{b'} + p^{v_p(y)}\frac{c'}{d'}.$$

Sea $t = \text{mín}\{v_p(x), v_p(y)\}$, así factorizando

$$x + y = p^t\left[p^{v_p(x)-t}\frac{a'}{b'} + p^{v_p(y)-t}\frac{c'}{d'}\right].$$

Por lo tanto $v_p(x+y) \geq \text{mín}\{v_p(x), v_p(y)\}$.

■

Ahora definiremos el valor absoluto p-ádico que será de vital importancia nuestro trabajo futuro.

Definición 2.8
Para cualquier $x \in \mathbb{Q}$, se define el ***valor absoluto p-ádico*** *de x como sigue*

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

Proposición 2.9
La función $| \cdot |_p$ es un valor absoluto no arquimediano sobre $\mathbb{Q}$.

Demostración

i) Se cumple por definición.

ii) Sean $x, y \in \mathbb{Q}$.
Si alguno de los dos, o ambos son igual a cero, claramente

$$| xy |_p = | x |_p | y |_p.$$

Si ambos son distintos de cero, entonces

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

iv) Sean $x, y \in \mathbb{Q}$.
Supongamos s.p.g. que $\text{mín}\{v_p(x), v_p(y)\} = v_p(x)$, entonces por el lema 2.7 tenemos

$$\begin{aligned} & v_p(x+y) \geq v_p(x) \\ \implies & p^{v_p(x+y)} \geq p^{v_p(x)} \\ \implies & \frac{1}{p^{v_p(x+y)}} \leq \frac{1}{p^{v_p(x)}} \\ \implies & | x+y |_p \leq | x |_p \end{aligned}$$

Por otro lado

$$\begin{aligned} & v_p(x) \leq v_p(y) \\ \implies & p^{v_p(x)} \leq p^{v_p(y)} \\ \implies & \frac{1}{p^{v_p(x)}} \geq \frac{1}{p^{v_p(y)}} \\ \implies & \text{máx}\{| x |_p, | y |_p\} = | x |_p \end{aligned}$$

Por lo tanto $|x+y|_p \leq \text{máx}\{|x|_p, |y|_p\}$.

Además, como sabemos que la parte **iv)** implica la parte **iii)** de la definición de valor absoluto, la proposición queda demostrada.

■

2.1.2. Propiedades básicas de valores absolutos

En esta sección estudiaremos algunas de las propiedades básicas de los valores absolutos en general que se utilizarán en las siguientes secciones.

Proposición 2.10
Sea $|\cdot|$ un valor absoluto sobre $\mathbb{K}$, entonces para todo $x, y \in \mathbb{K}$ se cumple lo siguiente:

i) $|1| = |-1| = 1$.

ii) $|x| = |-x|$.

iii) $||x| - |y||_{\mathbb{R}} \leq |x \pm y|$.

iv) $|x - y| \leq |x| + |y|$.

v) $\left|\dfrac{x}{y}\right| = \dfrac{|x|}{|y|}$ *con* $y \neq 0$.

Donde $|\cdot|_{\mathbb{R}}$ es el valor absoluto usual en $\mathbb{R}$ (la definición es análoga a la definición del valor absoluto usual sobre $\mathbb{Q}$).

Demostración

i) $|1| = |(1)(1)| = |1||1| \implies |1| = 1$.
$1 = |1| = |(-1)(-1)| = |-1||-1| = |-1|^2 \implies |-1| = 1$.

ii) $|-x| = |(-1)x| = |-1||x| = |x|$.

iii) Tenemos que

$$|y| = |y + (x - x)| = |(y + x) + (-x)| \leq |y + x| + |-x| = |y + x| + |x|.$$

Así

$$-|y + x| \leq |x| - |y|. \quad (1)$$

Además

$$|x| = |x + (y - y)| = |(x + y) + (-y)| \leq |x + y| + |-y| = |x + y| + |y|.$$

Entonces

$$|x| - |y| \leq |x + y|. \quad (2)$$

Y de (1) y (2) tenemos

$$-|y + x| \leq |x| - |y| \leq |x + y|$$
$$\implies ||x| - |y||_{\mathbb{R}} \leq |x + y|.$$

Por otro lado

$$||x| - |y||_{\mathbb{R}} \leq |x + (-y)| = |x - y|.$$

iv) $|x-y| = |x+(-y)| \leq |x| + |-y| = |x| + |y|$.

v) Como $y \neq 0$ tenemos

$$|x| = \left|(x)\frac{y}{y}\right| = \left|y\left(\frac{x}{y}\right)\right| = |y|\left|\frac{x}{y}\right|$$
$$\Longrightarrow \frac{|x|}{|y|} = \left|\frac{x}{y}\right|.$$

■

El siguiente teorema muestra una propiedad necesaria y suficiente para que un valor absoluto sea no arquimediano; y para ello recordaremos que para cualquier campo $\mathbb{K}$, existe la función $f : \mathbb{Z} \to \mathbb{K}$ definida como sigue

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

que es la inclusión usual de $\mathbb{Z}$ en $\mathbb{Q}$ cuando $\mathbb{Q} \subseteq \mathbb{K}$.

Teorema 2.11
Sea $A \subseteq \mathbb{K}$ la imagen de $\mathbb{Z}$ bajo la función f antes definida. Un valor absoluto $|\cdot|$ sobre $\mathbb{K}$ es no arquimediano si y sólo si $|a| \leq 1$ para todo $a \in A$. En particular, un valor absoluto sobre $\mathbb{Q}$ es no arquimediano si y sólo si $|n| \leq 1$ $\forall n \in \mathbb{Z}$.

Demostración

$\Rightarrow$) Sea $|\cdot|$ un valor absoluto no arquimediano sobre $\mathbb{K}$. Como $|\cdot|$ es no arquimediano tenemos que $|x+y| \leq \text{máx}\{|x|, |y|\}$ $\forall x, y \in \mathbb{K}$, y en particular sabemos que $|a+1| \leq \text{máx}\{|a|, |1|\} = \text{máx}\{|a|, 1\}$ $\forall a \in A$. Así probaremos por inducción que $|f(n)| \leq 1$ $\forall n \in \mathbb{N}$.
Para $n = 1$, tenemos que $|f(1)| = |1| = 1$.
Supongamos cierto para n, es decir $|f(n)| \leq 1$, así para $n+1$ tenemos

$$|f(n+1)| = |\underbrace{1+...+1}_{n \text{ veces}} + 1| \leq \text{máx}\{|f(n)|, 1\} = 1.$$

Así, $|f(n)| \leq 1$ $\forall n \in \mathbb{N}$.
Por otro lado sabemos que $|x| = |-x|$. Así, si $n \in \mathbb{Z}$, y $n < 0$, entonces

$$|f(n)| = |-\underbrace{(1+...+1)}_{-n \text{ veces}}| = |\underbrace{1+...+1}_{-n \text{ veces}}| \leq 1.$$

Y para $n = 0$, $|f(0)| = 0 \leq 1$. Por lo tanto $|f(n)| \leq 1$ $\forall n \in \mathbb{Z}$

⇐) Sea $|\cdot|$ un valor absoluto sobre $\mathbb{K}$, tal que $|a| \leq 1 \ \ \forall a \in A$.
Si $y = 0$, se cumple que $|x+y| \leq \max\{|x|,|y|\} \ \ \forall x \in \mathbb{K}$.
Si $y \neq 0$, se cumple entonces la equivalencia

$$|x+y| \leq \max\{|x|,|y|\} \iff \left|\frac{x}{y}+1\right| \leq \max\left\{\left|\frac{x}{y}\right|, 1\right\}.$$

Así basta probar que $|x+1| \leq \max\{|x|,1\} \ \ \forall x \in \mathbb{K}$.
Sean $x \in \mathbb{K}$, $m \in \mathbb{Z}^+$, entonces tenemos que

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

Como $\binom{m}{k} \in A$, entonces $\left|\binom{m}{k}\right| \leq 1$.
Así se sigue que

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

Y así llegamos a que $|x+1| \leq \max\{1,|x|\}\ \sqrt[m]{m+1} \ \ \forall m \in \mathbb{N}$.
Ahora, haciendo $m \to \infty$ y dado que $\lim_{m\to\infty} \sqrt[m]{m+1} = 1$, obtenemos

$$|x+1| \leq \max\{|x|,1\}.$$

■

Propiedad arquimediana

Un valor absoluto es arquimediano si tiene la siguiente propiedad: Dados $x, y \in \mathbb{K}$, $x \neq 0$, existe un entero positivo n tal que $|nx| > |y|$.

Es claro que la propiedad arquimediana es equivalente a decir que existen enteros cuyo valor absoluto es arbitrariamente "grande", en otras palabras, esta propiedad es equivalente a decir que $\sup\{|n| \,|\, n \in \mathbb{Z}\} = \infty$. Básicamente de la propiedad arquimediana se derivan las siguientes proposiciones.

Corolario 2.12
Un valor absoluto $|\cdot|$ *es no arquimediano si y sólo si* $\sup\{|n| \mid n \in \mathbb{Z}\} = 1$.

Demostración
⇒) Del teorema anterior sabemos que $|a| \leq 1 \ \ \forall a \in A$, y como $f(1) = 1$, se sigue que $\sup\{|n| \mid n \in \mathbb{Z}\} = 1$.

$\Leftarrow$) Si $\sup\{|n| \mid n \in \mathbb{Z}\} = 1$, entonces $|n| \leq 1 \ \ \forall n \in \mathbb{Z}$, y por el teorema anterior, el valor absoluto no es arquimediano.

■

Proposición 2.13
Si $\sup\{|n| \mid n \in \mathbb{Z}\} = C < \infty$, *entonces* $|\cdot|$ *no es arquimediano y* $C = 1$.

Demostración
Como $|1| = 1$, $\sup\{|n| \mid n \in \mathbb{Z}\} \geq 1$. Si $\sup\{|n| \mid n \in \mathbb{Z}\} = C > 1$, entonces $\exists m \in \mathbb{Z}$ tal que $|m| > 1$, además $|m^k| = |m|^k \ \ \forall k \in \mathbb{N}$, así

$$\lim_{k \to \infty} |m|^k = \infty.$$

Entonces existe $r \in \mathbb{N}$ tal que $|m|^r > C$, lo que es una contradicción, por lo tanto $C = 1$. Y por el corolario anterior se obtiene que $|\cdot|$ es no arquimediano.

■

2.1.3. Topología de valores absolutos

El principal propósito de un valor absoluto es el de proporcionarnos una noción de "tamaño", para en base a ello ser capaces de desarrollar el concepto de distancia entre dos números, es decir, obtener una métrica en el campo que estemos estudiando. Una vez obtenida una distancia podemos desarrollar otros conceptos como el de conjuntos abiertos, cerrados y en general investigar la topología del campo. Éste será nuestro objetivo en esta subsección.

Definición 2.14
Sea $\mathbb{K}$ *un campo y sea* $|\cdot|$ *un valor absoluto sobre* $\mathbb{K}$, *se define la distancia* $d(x, y)$ *entre dos elementos* $x, y \in \mathbb{K}$ *como*

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

La función d es llamada la ***métrica inducida por el valor absoluto*** $|\cdot|$.

Proposición 2.15
La métrica inducida por un valor absoluto es efectivamente una métrica.

Demostración
Sea $|\cdot|$ un valor absoluto sobre $\mathbb{K}$, y sea $d(x, y)$ la métrica inducida por $|\cdot|$.

i) $d : \mathbb{K} \times \mathbb{K} \to \mathbb{R}_+$, así $d(x,y) \geq 0 \ \ \forall x, y \in \mathbb{K}$.
Ahora, si $d(x,y) = 0$, entonces

$$\begin{aligned} & |x-y| = 0 \\ \iff & x - y = 0 \\ \iff & x = y. \end{aligned}$$

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

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

■

Lema 2.16
La función valor absoluto, $|\cdot| : \mathbb{K} \to \mathbb{R}_+$ es continua.

Demostración
Sea $x_0 \in \mathbb{K}$ y sea $\epsilon > 0$. Tomando $\delta = \epsilon$, tenemos que $|x - x_0| < \epsilon$. Así

$$||x| - |x_0||_{\mathbb{R}} \leq |x - x_0| < \epsilon$$

De lo que se sigue que $|\cdot|$ es continua en x_0, y como x_0 se eligió de manera arbitraria, entonces $|\cdot|$ es continua.

■

Proposición 2.17
Sea $\mathbb{K}$ un campo y $|\cdot|$ un valor absoluto definido sobre él. Las operaciones de suma, producto y tomar inversos aditivo y multiplicativo son continuas.

Demostración

1) Sean $x_0, y_0 \in \mathbb{K}$ fijos. Para cualquier $\epsilon > 0$, tomando $\delta = \dfrac{\epsilon}{2}$ se tiene que si $|x - x_0| < \delta$ y $|y - y_0| < \delta$, entonces

$$|(x_0 + y_0) - (x + y)| \leq |x_0 - x| + |y_0 - y| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon$$

Así la suma es una función continua.

2) Sean $x_0, y_0 \in \mathbb{K}$ fijos. Para cualquier $\epsilon > 0$ dado, si elegimos δ como $\delta = \text{mín}\left\{ \dfrac{\epsilon}{2(|x_0|+1)}, \dfrac{\epsilon}{2(|y_0|+1)}, 1 \right\}$ se tiene que si $|x - x_0| < \delta$ y $|y - y_0| < \delta$, entonces

$$|y| = |y - y_0 + y_0| \leq |y - y_0| + |y_0| < 1 + |y_0|.$$

Además

$$\begin{aligned}
|x_0y_0 - xy| &= |x_0y_0 - x_0y + x_0y - xy| \\
&\leq |x_0||y_0 - y| + |y||x_0 - x| \\
&< |x_0| \left(\frac{\epsilon}{2(|x_0|+1)} \right) + (1 + |y_0|) \left(\frac{\epsilon}{2(|y_0|+1)} \right) \\
&= \frac{\epsilon}{2} \left(\frac{|x_0|}{|x_0|+1} \right) + \frac{\epsilon}{2} \\
&< \frac{\epsilon}{2} + \frac{\epsilon}{2} \\
&= \epsilon.
\end{aligned}$$

Por lo tanto el producto es una función continua.

3) Sea $x_0 \in \mathbb{K}$. Para cualquier $\epsilon > 0$, tomando $\delta = \epsilon$ se tiene que

$$|x - x_0| < \delta \implies |-x - (x_0)| = |x_0 - x| < \delta = \epsilon.$$

Así la operación de tomar inverso aditivo es continua.

4) Sea $x_0 \in \mathbb{K} - 0$. Para cualquier $\epsilon > 0$, tomando $\delta = \text{mín} \left\{ \frac{|x_0|}{2}, \frac{\epsilon|x_0|}{2} \right\}$ tenemos que si $|x - x_0| < \delta$, entonces

$$\begin{aligned}
&||x| - |x_0||_{\mathbb{R}} \leq |x - x_0| < \frac{|x_0|}{2} \\
\implies &-\frac{|x_0|}{2} < |x| - |x_0| < \frac{|x_0|}{2} \\
\implies &\frac{|x_0|}{2} < |x| < \frac{3|x_0|}{2} \\
\implies &\frac{1}{|x|} < \frac{2}{|x_0|}.
\end{aligned}$$

Por otro lado

$$\left| \frac{1}{x_0} - \frac{1}{x} \right| = \frac{|x - x_0|}{|x||x_0|} < \left(\frac{2}{|x_0|} \right) \left(\frac{1}{|x_0|} \right) \left(\frac{\epsilon|x_0|^2}{2} \right) = \epsilon.$$

Por lo tanto la operación de tomar inverso multiplicativo es continua.

■

Definición 2.18
Un espacio métrico que satisface $d(x,y) \leq \text{máx}\{d(x,z), d(z,y)\}$ *para todo* x, y, z *se llama* ***espacio ultramétrico****.*

Proposición 2.19
Sean $|\cdot|$ un valor absoluto sobre un campo $\mathbb{K}$ y $d(x,y) = |x-y|$ la métrica inducida por $|\cdot|$. El valor absoluto $|\cdot|$ es no arquimediano si y sólo si el espacio es ultramétrico.

Demostración
$\Rightarrow$) Para $x, y, z \in \mathbb{K}$ se tiene

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

Y como $|\cdot|$ es no arquimediano, entonces

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

$\Leftarrow$) Sean $x, y \in \mathbb{K}$. Sabemos que $d(x,-y) \leq \text{máx}\{d(x,0), d(0,-y)\}$, por lo tanto $|x+y| \leq \text{máx}\{|x|, |y|\}$.

■

Proposición 2.20
Sea $\mathbb{K}$ un campo y $|\cdot|$ un valor absoluto no arquimediano sobre $\mathbb{K}$. Si $x, y \in \mathbb{K}$ y $|x| \neq |y|$ entonces $|x+y| = \text{máx}\{|x|, |y|\}$.

Demostración
Sin pérdida de generalidad sea $|x| > |y|$. Como $|\cdot|$ es no arquimediano, tenemos

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

Por otro lado, podemos expresar a x de la forma $x = (x+y)+(-y)$, entonces se cumple $|x| \leq \text{máx}\{|x+y|, |y|\}$; como sabemos que $|x| > |y|$, tenemos que $\text{máx}\{|x+y|, |y|\} = |x+y|$, y así

$$|x| \leq |x+y| \quad (ii).$$

De (i) y (ii) tenemos que $|x+y| = \text{máx}\{|x|, |y|\}$.

■

Corolario 2.21
En un espacio ultramétrico todos los triángulos son isósceles.

Demostración
Sean $x, y, z \in X$ espacio ultramétrico. Las longitudes de los lados de un triángulo son $d(x,y)$, $d(y,z)$, $d(z,x)$.
Ahora $d(x,y) = |x-y|$, además $x-y = (x-z)+(z-y)$, de aquí tenemos dos casos:

- Si $d(x,z) = |x-z| = |z-y| = d(z,y) = d(y,z)$ entonces el triángulo es isósceles.

- Si $d(x,z) = |x-z| \neq |z-y| = d(z,y) = d(y,z)$ entonces tenemos que $d(x,y) = \text{máx}\{d(x,z), d(z,y)\}$.

Y así todos los triángulos son isósceles.

■

Definición 2.22
*Sea $\mathbb{K}$ un campo con valor absoluto $|\cdot|$. Y sean $a \in \mathbb{K}$ y $r \in \mathbb{R}_+$. La **bola abierta** con radio r y centro en a es el conjunto*

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

*La **bola cerrada** con centro en a y radio r es el conjunto*

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

Proposición 2.23
Sea $\mathbb{K}$ un campo con valor absoluto $|\cdot|$ no arquimediano, entonces:

i) Si $b \in B(a,r)$, entonces $B(a,r) = B(b,r)$.

ii) Si $b \in \overline{B}(a,r)$, entonces $\overline{B}(a,r) = \overline{B}(b,r)$.

iii) $B(a,r)$ es abierto y cerrado.

iv) $\overline{B}(a,r)$ es abierto y cerrado si $r \neq 0$.

v) Si $a,b \in \mathbb{K}$ y $r,s \in \mathbb{R}^+$, entonces $B(a,r) \cap B(b,s) \neq \emptyset$ si y sólo si $B(a,r) \subseteq B(b,s)$ ó $B(b,s) \subseteq B(a,r)$.

vi) Si $a,b \in \mathbb{K}$ y $r,s \in \mathbb{R}^+$, entonces $\overline{B}(a,r) \cap \overline{B}(b,s) \neq \emptyset$ si y sólo si $\overline{B}(a,r) \subseteq \overline{B}(b,s)$ ó $\overline{B}(b,s) \subseteq \overline{B}(a,r)$.

Demostración

i) Sea $b \in B(a,r)$, es decir, $|b-a| < r$. Ahora, sea $x \in B(a,r)$, entonces $|x-a| < r$. Por otro lado

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

Así $x \in B(b,r)$ y $B(a,r) \subseteq B(b,r)$. Análogamente $B(b,r) \subseteq B(a,r)$. Entonces $B(a,r) = B(b,r)$.

ii) Sean $b \in \overline{B}(a,r)$ y $x \in \overline{B}(a,r)$. Entonces tenemos que $|b-a| \leq r$ y $|x-a| \leq r$. Por otro lado

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

Así $x \in \overline{B}(b,r)$ y $\overline{B}(a,r) \subseteq \overline{B}(b,r)$. Análogamente $\overline{B}(b,r) \subseteq \overline{B}(a,r)$. Entonces $\overline{B}(a,r) = \overline{B}(b,r)$.

iii) $B(a,r)$ es abierto por definición. Para probar que $B(a,r)$ es cerrado, sean $x \in fr(B(a,r))$ y $s \leq r$. Se tiene

$$B(x,s) \cap B(a,r) \neq \emptyset$$

Así $\exists y \in B(x,s) \cap B(a,r)$, con lo que se tiene $|y-a| < r$ y $|y-x| < s$. Entonces $|x-a| \leq \text{máx}\{|x-y|, |y-a|\} < \text{máx}\{s,r\} \leq r$. De esta manera $x \in B(a,r)$, entonces $fr(B(a,r)) \subseteq B(a,r)$. Por lo tanto $B(a,r)$ es cerrado.

iv) Sabemos que $\overline{B}(a,r)$ es cerrado. Ahora tenemos

$$\overline{B}(a,r) = fr(B(a,r)) \cup B(a,r) = B(a,r)$$

Así $\overline{B}(a,r)$ es abierto.

v) $\Rightarrow$ **)** Como $B(a,r) \cap B(b,s) \neq \emptyset$, entonces $\exists c \in B(a,r) \cap B(b,s)$.
Por 1) tenemos que $B(a,r) = B(c,r)$ y $B(b,s) = B(c,s)$.
Si $r \leq s$ entonces $B(c,r) \subseteq B(c,s)$ y $B(a,r) \subseteq B(b,s)$
Si $s \leq r$ entonces $B(c,s) \subseteq B(c,r)$ y $B(b,s) \subseteq B(a,r)$.
$\Leftarrow$ **)** Como forzosamente un conjunto es subconjunto del otro, entonces es claro que la intersección es no vacía.

vi) La prueba es análoga a la demostración del inciso anterior.

■

2.1.4. Álgebra

En esta parte estudiaremos la relación entre un valor absoluto (no arquimediano) y la estructura algebraica de un campo.

Teorema 2.24
Sea $\mathbb{K}$ un campo y $|\cdot|$ un valor absoluto no arquimediano definido sobre $\mathbb{K}$. El conjunto $\mathcal{O} = \overline{B}(0,1) = \{x \in \mathbb{K} \mid |x| \leq 1\}$ es subanillo de $\mathbb{K}$, su subconjunto $\mathcal{B} = B(0,1) = \{x \in \mathbb{K} \mid |x| < 1\}$ es un ideal maximal de $\mathcal{O}$; además los únicos elementos invertibles en $\mathcal{O}$ son los elementos del conjunto $\mathcal{O} - \mathcal{B}$.

Demostración

·) En primer lugar mostraremos que $\mathcal{O}$ es subanillo de $\mathbb{K}$.
i) $1 \in \mathcal{O}$, pues $|1| = 1 \leq 1$.
ii) Sean $x, y \in \mathcal{O}$, es decir, $|x| \leq 1$ e $|y| \leq 1$. Entonces podemos decir que $|x - y| \leq \text{máx}\{|x|, |-y|\} = \text{máx}\{|x|, |y|\} \leq 1$.
iii) $|xy| = |x||y| \leq 1 \cdot 1 = 1 \leq 1$.

·) Ahora probaremos que $\mathcal{B}$ es ideal de $\mathcal{O}$.
i) $0 \in \mathcal{O}$ pues $|0| = 0 < 1$.
ii) Sean $x, y \in \mathcal{B}$. Entonces $|x + y| \leq \text{máx}\{|x|, |y|\} < 1$, pues $|x| < 1$ e $|y| < 1$.
iii) Sean $r \in \mathcal{O}$ y $x \in \mathcal{B}$. Entonces $|r| \leq 1$ y $|x| < 1$ lo que implica que $|rx| = |r||x| \leq |x| < 1$.

·) El siguiente objetivo es probar que $\mathcal{B}$ es ideal maximal de $\mathcal{O}$.
Supongamos que $\mathcal{I}$ es un ideal de $\mathcal{O}$ tal que $\mathcal{B} \subset \mathcal{I}$. Como $\mathcal{I}$ es ideal de $\mathcal{O}$ se tiene que $\mathcal{I} \subseteq \mathcal{O}$ además como $\mathcal{B} \neq \mathcal{I}$, entonces $\exists z \in \mathcal{I}$ tal que $z \notin \mathcal{B}$, por lo que $|z| = 1$. Así $zz^{-1} = 1 \in \mathcal{I}$, pues $\mathcal{I}$ es ideal de $\mathcal{O}$, y $z^{-1} \in \mathcal{O}$. Entonces, para cualquier $x \in \mathcal{O}$, $1x \in \mathcal{I}$, es decir, $x \in \mathcal{I}$. Así $\mathcal{O} \subseteq \mathcal{I}$ e $\mathcal{I} = \mathcal{O}$. Por lo tanto $\mathcal{B}$ es ideal maximal de $\mathcal{O}$.

·) Por último probaremos que cada elemento de $\mathcal{O} - \mathcal{B}$ es invertible en $\mathcal{O}$.
Sea $x \in \mathcal{O} - \mathcal{B}$, entonces $|x| = 1$, así $x \neq 0$ y $x^{-1} \in \mathbb{K}$. Además $|x^{-1}| = \dfrac{1}{|x|} = 1$, y así $x^{-1} \in \mathcal{O} - \mathcal{B}$. Ahora, supongamos que existe un elemento x invertible en $\mathcal{O}$ tal que $x \notin \mathcal{O} - \mathcal{B}$, entonces $|x| < 1$, y como x es invertible $\exists x^{-1} \in \mathcal{O}$ tal que $|x||x^{-1}| = 1$, pero $|x||x^{-1}| < 1$, lo que es una contradicción. Por lo tanto los únicos elementos invertibles en $\mathcal{O}$ son $\mathcal{O} - \mathcal{B}$.

■

Definición 2.25
Sea $|\cdot|$ un valor absoluto no arquimediano sobre $\mathbb{K}$. El subanillo $\mathcal{O} = \overline{B}(0,1)$ es llamado ***anillo de valuación*** *de $|\cdot|$. El ideal $\mathcal{B} = B(0,1)$ es llamado* ***ideal de valuación*** *de $|\cdot|$. El cociente $\kappa = \mathcal{O}/\mathcal{B}$ es llamado* ***campo de residuos*** *de $|\cdot|$.*

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

En esta sección estudiaremos todos los "tipos"de valores absolutos que se pueden definir sobre el campo de los números racionales. Comenzaremos haciendo mención de los valores absolutos sobre $\mathbb{Q}$ que hemos definido hasta el momento: El valor absoluto trivial, el valor absoluto usual, y por último, el valor absoluto p-ádico. Probaremos entonces que en determinada forma, los anteriores son todos los tipos de valores absolutos que se pueden definir sobre $\mathbb{Q}$.

Comenzaremos por dar una definición que nos ayudará a entender en qué sentido dos valores absolutos serán considerados "iguales".

Definición 2.26
Dos valores absolutos $|\cdot|_1$ y $|\cdot|_2$ sobre un campo $\mathbb{K}$ se dicen equivalentes si definen la misma topología sobre $\mathbb{K}$.

Lema 2.27
Sea $|\cdot|$ un valor absoluto definido sobre un campo $\mathbb{K}$, entonces $\lim_{n\to\infty} x^n = 0$ si y sólo si $|x| < 1$.

Demostración
$\Rightarrow$) Como $\lim_{n\to\infty} x^n = 0$, entonces para $\epsilon = 1$ $\exists N \in \mathbb{N}$ tal que

$$|x^n - 0| = |x^n| = |x|^n < 1 \text{ para } n \geq N.$$

Luego $|x|^N < 1$, lo que implica que $|x| < 1$.

$\Leftarrow$) Si $x = 0$ es claro que la implicación se cumple.
En otro caso, si $x \neq 0$, entonces $\frac{1}{|x|} > 1$ pues $|x| < 1$, así $\exists h > 0$ tal que $\frac{1}{|x|} = 1 + h$. Ahora, por la desigualdad de Bernoulli, tenemos que

$$\left(\frac{1}{|x|}\right)^k = (1+h)^k \geq 1 + kh \ \ \forall k \in \mathbb{N}.$$

Sea $\epsilon > 0$, por la propiedad arquimediana sabemos que $\exists N_\epsilon \in \mathbb{N}$ tal que $N_\epsilon h > \frac{1}{\epsilon} - 1$, luego $1 + N_\epsilon h > \frac{1}{\epsilon}$, de lo que se sigue que $\frac{1}{|x|^{N_\epsilon}} > \frac{1}{\epsilon}$ y entonces $|x|^{N_\epsilon} < \epsilon$. Para $n \geq N_\epsilon$ se cumple que $|x|^n < \epsilon$ y así $\lim_{n\to\infty} x^n = 0$.

■

Lema 2.28
Sean $|\cdot|_1$ y $|\cdot|_2$ dos valores absolutos definidos sobre un campo $\mathbb{K}$, entonces los siguientes enunciados son equivalentes:

i) $|\cdot|_1$ *y* $|\cdot|_2$ *son valores absolutos equivalentes.*

ii) Para todo $x \in \mathbb{K}$ *se tiene que* $|x|_1 < 1$ *si y sólo si* $|x|_2 < 1$.

iii) Existe un número real positivo α *tal que* $|x|_1 = |x|_2^{\alpha}$ *para todo* $x \in \mathbb{K}$.

Demostración

·) i) $\Longrightarrow$ ii)
Sea $x \in \mathbb{K}$ tal que $|x|_1 < 1$, entonces, por el lema anterior, tenemos $\lim_{n\to\infty} x^n = 0$ con $|\cdot|_1$. Como $|\cdot|_1$ y $|\cdot|_2$ son equivalentes, todo abierto de $\langle \mathbb{K}, d_{|\cdot|_1} \rangle$ es abierto en $\langle \mathbb{K}, d_{|\cdot|_2} \rangle$, donde $d_{|\cdot|_1}, d_{|\cdot|_2}$ son las métricas inducidas por los valores absolutos $|\cdot|_1, |\cdot|_2$ respectivamente. Así $\lim_{n\to\infty} x^n = 0$ con $|\cdot|_2$, y por el lema anterior $|x|_2 < 1$. Análogamente, si $|x|_2 < 1$ entonces $|x|_1 < 1$.

·) ii) $\Longrightarrow$ iii)
Sea $x \in \mathbb{K}$, distinguiremos dos casos:
Si $|\cdot|_1$ es el valor absoluto trivial, para $x \neq 0, 1$ tenemos que si $|x|_1 = 1$ entonces $|x|_2 = 1$ pues, de lo contrario, tendríamos que $|x|_1 \neq 1$, lo que es una contradicción.
Si $|\cdot|_1$ no es el valor absoluto trivial, entonces existe $x_0 \neq 0, 1$ tal que $|x_0|_1 < 1$, lo que a su vez implica que $|x_0|_2 < 1$. Sea $\alpha = \log_{|x_0|_2} |x_0|_1$, de esta manera $|x_0|_2^{\alpha} = |x_0|_1$. Además $\alpha > 0$, pues de lo contrario sucedería que $|x_0|_1 \geq 1$, lo que es una contradicción.
Ahora, si $|x|_1 = 1$ entonces $|x|_2 = 1$, pues de lo contrario tendríamos que $|x|_1 \neq 1$, lo que es una contradicción. Así $|x|_1 = |x|_2^{\alpha}$.
Por otro lado, si $|x|_1 = |x_0|_1$, entonces $|x|_2 = |x_0|_2$, porque si $|x|_2 < |x_0|_2$ entonces $|\frac{x}{x_0}|_2 < 1$, lo que implica que $|\frac{x}{x_0}|_1 < 1$ y así $|x|_1 < |x_0|_1$, lo que es una contradicción. Análogamente se obtiene una contradicción al suponer que $|x|_2 > |x_0|_2$. Así $|x|_1 = |x_0|_1 = |x_0|_2^{\alpha} = |x|_2^{\alpha}$.
Por último, si $|x|_1 \neq 1$ y $|x|_1 \neq |x_0|_1$, sea entonces

$$S = \left\{ \frac{m}{n} \;\middle|\; m, n \in \mathbb{N},\ |x|_1^{\frac{m}{n}} < |x_0|_1 \right\}.$$

Se tiene

$$\frac{m}{n} \in S \iff |x|_1^{\frac{m}{n}} < |x_0|_1, \iff |x|_1^m = |x_0|_1^n \iff \left| \frac{x^m}{x_0^n} \right|_1 < 1$$
$$\iff \left| \frac{x^m}{x_0^n} \right|_2 < 1 \iff |x|_2^m = |x_0|_2^n \iff |x|_2^{\frac{m}{n}} < |x_0|_2.$$

Así, se sigue que

$$S = \left\{ \frac{m}{n} \;\middle|\; m,n \in \mathbb{N},\ |x|_2^{\frac{m}{n}} < |x_0|_2 \right\} = \left\{ \frac{m}{n} \;\middle|\; m,n \in \mathbb{N},\ |x|_1^{\frac{m}{n}} < |x_0|_1 \right\}.$$

Esto implica

$$S = \left\{ \frac{m}{n} \;\middle|\; m,n \in \mathbb{N},\ |x|_2 < |x_0|_2^{\frac{n}{m}} \right\} = \left\{ \frac{m}{n} \;\middle|\; m,n \in \mathbb{N},\ |x|_1 < |x_0|_1^{\frac{n}{m}} \right\}.$$

Ahora, sean $s = \log_{|x_0|_1} |x|_1$ y $t = \log_{|x_0|_2} |x|_2$. Obtenemos así que

$$S = \left\{ r = \frac{m}{n} \;\middle|\; m,n \in \mathbb{N},\ s < \frac{1}{r} \right\} = \left\{ r = \frac{m}{n} \;\middle|\; m,n \in \mathbb{N},\ t < \frac{1}{r} \right\}.$$

Si $s \neq t$ se tiene que $s < t$ o $t < s$. Supongamos $s < t$, entonces $\exists p \in \mathbb{Q}$ tal que $s < p < t$, luego se sigue que $\frac{1}{p} \in S$, pues $s < \frac{1}{\frac{1}{p}} = p$. Por otro lado, $\frac{1}{p} \notin S$ pues $\frac{1}{\frac{1}{p}} = p < t$. Y así llegamos a una contradicción, pues $\frac{1}{p} \in S$ y $\frac{1}{p} \notin S$. Análogamente se obtiene una contradicción al suponer $t < s$. Por lo tanto $s = t$ y podemos concluir que

$$|x|_1 = |x_0|_1^s = (|x_0|_2^\alpha)^s = (|x_0|_2^s)^\alpha = |x|_2^\alpha$$

·) iii) $\Longrightarrow$ i)
Sea $B_{|\cdot|_1}(x,r)$ una bola abierta en $\langle \mathbb{K}, d_{|\cdot|_1} \rangle$. Sabemos que $\forall z \in \mathbb{K}$, $|z|_1 = |z|_2^\alpha$ para algún $\alpha \in \mathbb{R}^+$. Luego

$$y \in B_{|\cdot|_1}(x,r) \iff |x-y|_1 < r \iff |x-y|_2^\alpha < r \iff |x-y| < \sqrt[\alpha]{r}$$
$$\iff y \in B_{|\cdot|_2}(x, \sqrt[\alpha]{r}).$$

Así toda bola abierta en $\langle \mathbb{K}, d_{|\cdot|_1} \rangle$ es bola abierta en $\langle \mathbb{K}, d_{|\cdot|_2} \rangle$. Análogamente toda bola abierta en $\langle \mathbb{K}, d_{|\cdot|_2} \rangle$ es bola abierta en $\langle \mathbb{K}, d_{|\cdot|_1} \rangle$. Por lo tanto $|\cdot|_1$ y $|\cdot|_2$ son equivalentes.

■

Corolario 2.29
Sean p, q dos números primos distintos, entonces $|\cdot|_p$ y $|\cdot|_q$ no son equivalentes.
Demostración
Tenemos que $|p|_p = \frac{1}{p}$, mientras que $|p|_q = 1$; entonces, por el lema anterior $|\cdot|_p$ y $|\cdot|_q$ no son equivalentes.

■

Lema 2.30
Sea $|\cdot|$ un valor absoluto sobre $\mathbb{Q}$. Si se conoce $|n|$ para toda $n \in \mathbb{N}$, entonces se puede determinar $|x|$ para toda $x \in \mathbb{Q}$.

Demostración
En primer lugar $|0| = 0$ por definición. Ahora, para $n \in \mathbb{Z}^-$ se tiene que $-n \in \mathbb{N}$, entonces $|n| = |-n|$. Para cualquier $n \in \mathbb{Z} - \{0\}$ tenemos que $|\frac{1}{n}| = \frac{1}{|n|}$. Así podemos decir que para cualquier $\frac{a}{b} \in \mathbb{Q}$ se tiene que $|\frac{a}{b}| = |a||\frac{1}{b}| = \frac{|a|}{|b|}$.

■

Teorema 2.31 (Ostrowsky)
Cada valor absoluto no trivial sobre $\mathbb{Q}$ *es equivalente a uno de los valores absolutos* $|\cdot|_p$ *para* p *un número primo fijo o* $p = \infty$.

Demostración
Dado un valor absoluto $|\cdot|$ no trivial sobre $\mathbb{Q}$, distinguiremos dos casos:

•) $|\cdot|$ es un valor absoluto arquimediano:
Probaremos que $|\cdot|$ es equivalente al valor absoluto usual $|\cdot|_\infty$. Sea n_0 el menor entero positivo tal que $|n_0| > 1$ (podemos asegurar la existencia de tal entero por la propiedad arquimediana) y $\alpha = \log_{n_0} |n_0|$, así tenemos, por la definición de α, que $|n_0| = n_0^\alpha$.
Probaremos que $|x| = |x|_\infty^\alpha \ \forall x \in \mathbb{N}$. Sea $n \in \mathbb{Z}^+$, y escribiendo n en base n_0 tenemos

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

con $0 \leq a_i < n_0$ para $i = 0, 1, ..., k$ y $a_k \neq 0$. Además sabemos que k queda determinada por $n_0^k \leq n < n_0^{k+1}$. Ahora, tomando valores absolutos obtenemos lo siguiente

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

Como n es el entero más pequeño para el que su valor absoluto es mayor que 1, decimos que $|a_i| \leq 1$, para $i = 1, ..., k$. Así,

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

Tomando $C = \frac{n_0^\alpha}{n_0^\alpha - 1}$ tenemos que $C > 0$ y $|n| \leq C n_0^{k\alpha} \leq C n^\alpha \ \forall n \in \mathbb{N}$, pues $n_0^k \leq n$. Si aplicamos la desigualdad anterior a n^N obtenemos $|n^N| \leq C n^{N\alpha}$. Si sacamos la raíz n-ésima tenemos que $|n| \leq \sqrt[N]{C} n^\alpha$. Haciendo $N \to \infty$ tenemos que $\sqrt[N]{C} \to 1$, y así $|n| \leq n^\alpha$.
Por otro lado $n = a_0 + a_1 n_0 + \cdots + a_k n_0^k$, y como $n_0^k \leq n < n_0^{k+1}$, tenemos

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

Por lo que

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

De lo anterior obtenemos que

$$\begin{aligned} |n| &\geq n_0^{(k+1)\alpha} - (n_0^{k+1} - n_0^k)^{\alpha} \\ &= n_0^{(k+1)\alpha}\left[1 - \left(1 - \frac{1}{n_0}\right)^{\alpha}\right] \\ &= C' n_0^{(k+1)\alpha} \\ &\geq C' n^{\alpha}. \end{aligned}$$

Haciendo $C' = 1 - (1 - \frac{1}{n_0})^{\alpha}$; de esta forma $C' > 0$ y no depende de n. Ahora, aplicando la desigualdad obtenida al entero n^N tenemos $|n^N| \geq C' n^{N\alpha}$, lo que implica que $|n| \geq \sqrt[N]{C'} n^{\alpha}$. Haciendo $N \to \infty$ tenemos $|n| \geq n^{\alpha}$ pues $\lim_{N\to\infty} \sqrt[N]{C'} = 1$. Así $|n| = n^{\alpha}$, por lo tanto $|n| = |n|_{\infty}^{\alpha}$ $\forall n \in \mathbb{N}$. Y por el lema anterior, $|\cdot|$ y $|\cdot|_{\infty}$ son equivalentes.

·) $|\cdot|$ es un valor absoluto no arquimediano:
Dado que $|\cdot|$ es no arquimediano, se cumple que $|n| \leq 1$ $\forall n \in \mathbb{Z}$; además, como $|\cdot|$ es no trivial, existe al menos un $n \in \mathbb{Z}$ tal que $|n| < 1$. Sea n_0 el menor número natural para el que $|n_0| < 1$, entonces n_0 debe ser primo, pues de lo contrario tendríamos, por el teorema fundamental de la aritmética, que $n_0 = ab$ con $a, b < n_0$, y por nuestra elección de n_0, $|a| = |b| = 1$, pero $|a||b| = 1 = |n_0| < 1$, lo que es una contradicción. Así $n_0 = p$ para algún p primo.
Ahora, sean $n \in \mathbb{N}$ y $\alpha = \log_{\frac{1}{p}} |p|$. Si $p \nmid n$, entonces $|n|_p = 1$ y $n = pq + r$ con $0 < r < p$; por la elección que hicimos de p, se cumple que $|r| = 1$, además como $|p| < 1$ y $|q| \leq 1$, también tenemos que $|pq| < 1$, así $|n| = |pq + r| = \max\{|pq|, |r|\} = 1$, y esto implica que $|n| = |n|_p^{\alpha} = 1$.
Por otro lado, si $p \mid n$, podemos escribir a n de la forma $n = p^v n'$ con $p \nmid n'$. Así $|n| = |p|^v |n'| = |p|^v = (\frac{1}{p})^{\alpha v} = (\frac{1}{p^v})^{\alpha} = |n|_p^{\alpha}$.
Entonces por los lemas 2.28 y 2.30, $|\cdot|$ es equivalente a $|\cdot|_p$.

■

2.3. Completaciones

En esta sección se construirá el campo de los números p-ádicos como una completación del campo de los números racionales respecto al valor absoluto $|\cdot|_p$. Comenzaremos por las definiciones básicas necesarias para comprender la teoría de esta sección, después continuaremos con una serie de teoremas que demostrarán los hechos matemáticos fundamentales que nos permitirán conseguir la construcción deseada, y finalmente culminaremos la sección con la prueba de que el campo de los números p-ádicos es efectivamente completo.

Definición 2.32
Sea $\mathbb{K}$ un campo y sea $|\cdot|$ un valor absoluto sobre $\mathbb{K}$. Una sucesión de elementos de $\mathbb{K}$, $\{x_n\}$ es llamada un ***sucesión de Cauchy*** *si para cada $\epsilon > 0$ existe $M \in \mathbb{N}$ tal que $|x_n - x_m| < \epsilon$ siempre que $m, n \geq M$.*

Definición 2.33
Un campo $\mathbb{K}$ es ***completo*** *respecto a $|\cdot|$ si cada sucesión de Cauchy de elementos de $\mathbb{K}$ tiene un límite en $\mathbb{K}$.*

Lema 2.34
Una sucesión $\{x\}_n$ de números racionales es de Cauchy con respecto a un valor absoluto no arquimediano $|\cdot|$ si y sólo si $\lim_{n\to\infty} |x_{n+1} - x_n| = 0$.

Demostración

$\Rightarrow$) Sea $\epsilon > 0$, como $\{x_n\}$ es de Cauchy, $\exists N \in \mathbb{N}$ tal que $|x_n - x_m| < \epsilon$, $\forall m, n \geq N$. En particular, si $n \geq N$, tenemos que $|x_n - x_{n+1}| < \epsilon$, así $\lim_{n\to\infty} |x_n - x_{n+1}| = 0$.

$\Leftarrow$) Sea $\epsilon > 0$, como $\lim_{n\to\infty} |x_n - x_{n+1}| = 0$, $\exists N \in \mathbb{N}$ tal que, si $n \geq \mathbb{N}$, entonces $|x_{n+1} - x_n| < \epsilon$. Sean $m, n \geq \mathbb{N}$, sin pérdida de generalidad sea $m > n$ y $m = n + r$, tenemos que

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

Así $\{n_n\}$ es de Cauchy.

■

Teorema 2.35
$\mathbb{Q}$ no es completo respecto a cualquiera de los valores absolutos no triviales.

Demostración
Por el teorema de Ostrowsky sólo es necesario verificar esto para los valores absolutos $|\cdot|_p$ y $|\cdot|_\infty$. Además es bien sabido que $\mathbb{Q}$ no es completo respecto a $|\cdot|_\infty$, por lo que sólo probaremos para $|\cdot|_p$ con p un número primo fijo.
Consideremos la sucesión de números racionales $\{a_n\}$ tal que $a_n = 1 + p + p^2 + \cdots + p^n$. $\{a_n\}$ es de Cauchy puesto que:

$$\lim_{n\to\infty} |a_{n+1} - a_n|_p = \lim_{n\to\infty} |p^{n+1}|_p = \lim_{n\to\infty} p^{-n-1} = 0.$$

Además es claro que $\{a_n\}$ converge a $1 + p + p^2 + \cdots + p^n + \cdots$. Si $1 + p + p^2 + \cdots + p^n + \cdots$ fuese un número racional r, tendríamos entonces que $r = 1 + p + p^2 + \cdots + p^n + \cdots = 1 + p(1 + p + \cdots + p^n + \cdots) = 1 + pr$, lo que es una contradicción. Así r no es un número racional, y por lo tanto $\mathbb{Q}$ no es completo, como queríamos probar.

■

Definición 2.36
Se denota por $\mathcal{C}$ o $\mathcal{C}_p(\mathbb{Q})$ al conjunto de todas las sucesiones de Cauchy de elementos de $\mathbb{Q}$ con respecto a $|\cdot|_p$.

Lema 2.37
Toda sucesión de Cauchy es acotada.

Demostración
Sea $\{x_n\}$ una sucesión de Cauchy de elementos de un campo $\mathbb{K}$, sea $|\cdot|$ un valor absoluto definido sobre $\mathbb{K}$.
Entonces para $\epsilon = 1$, $\exists N \in \mathbb{N}$ tal que, si $n, m \geq N$ entonces $|x_n - x_m| < 1$, en particular $|x_n - x_N| < 1$, así $||x_n| - |x_N||_{\mathbb{R}} \leq |x_n - x_N| < 1$, luego $-1 < |x_n| - |x_N| < 1$ de lo que se sigue que $|x_n| < |x_N| + 1$ para $n \geq N$. Sea $k = \text{máx}\{|x_1|, ..., |x_{N-1}|, |x_N| + 1\}$, entonces $|x_n| \leq k \ \forall n \in \mathbb{N}$. Así $\{x_n\}$ es acotada.

■

Proposición 2.38
$\mathcal{C}$ es un anillo conmutativo con unidad definiendo las operaciones de suma y producto de la siguiente manera $\{x_n\} + \{y_n\} = \{x_n + y_n\}$ y $\{x_n\}\{y_n\} = \{x_n y_n\}$.

Demostración

·) Probaremos la cerradura de la suma:
Sean $\{x_n\}, \{y_n\} \in \mathcal{C}$ y $\epsilon > 0$, entonces existen $N_1, N_2 \in \mathbb{N}$ tales que si $n, m \geq N_1$ entonces $|x_n - x_m|_p < \epsilon$, y si $n, m \geq N_2$ entonces $|x_n - x_m|_p < \epsilon$. Sea $N = \text{máx}\{N_1, N_2\}$, entonces si $n, m \geq N$ tenemos que $|x_n + y_n - (x_m + y_m)|_p = |(x_n - x_m) + (y_n - y_m)|_p \leq \text{máx}\{|x_n - x_m|_p, |y_n - y_m|_p\} < \epsilon$. Así $\{x_n + y_n\}$ es de Cauchy.

·) Probaremos ahora la cerradura del producto:
Sean $\{x_n\}, \{y_n\} \in \mathcal{C}$ y sea $\epsilon > 0$, por el lema anterior sabemos que $\exists k_1, k_2 \in \mathbb{R}_+$ tal que $|x_n|_p < k_1$ y $|y_n|_p < k_2$ $\forall n \in \mathbb{N}$; si elegimos $k = \text{máx}\{k_1, k_2\}$ entonces, para $\frac{\epsilon}{k}$ $\exists N_1, N_2 \in \mathbb{N}$ tales que, si $n, m \geq N_1$ entonces $|x_n - x_m|_p < \frac{\epsilon}{k}$ y si $n, m \geq N_2$ entonces $|y_n - y_m|_p < \frac{\epsilon}{k}$. Sea $N = \text{máx}\{N_1, N_2\}$, ahora, si $n, m \geq N$ se tiene que

$$\begin{aligned} |x_n y_n - x_m y_m|_p &= |x_n y_n - x_m y_n + x_m y_n - x_m y_m|_p \\ &= |y_n(x_n - x_m) + x_m(y_n - y_m)|_p \\ &\leq \text{máx}\{|y_n|_p |x_n - x_m|_p, |x_m|_p |y_n - y_m|_p\} \\ &< \text{máx}\left\{k\left(\frac{\epsilon}{k}\right), k\left(\frac{\epsilon}{k}\right)\right\} = \epsilon. \end{aligned}$$

Así $\{x_n, y_n\} \in \mathcal{C}$.

Por último, es fácil notar que el elemento neutro es $\{0\}$ y el elemento unidad es $\{1\}$, también es claro que el resto de las propiedades de anillo conmutativo se cumplen. Así $\mathcal{C}$ es un anillo conmutativo con unidad.

■

Lema 2.39
La función $f : \mathbb{Q} \to \mathcal{C}$ definida por $f(x) = \{x\}$ es una inclusión de $\mathbb{Q}$ en $\mathcal{C}$.

Demostración
La función está bien definida y es inyectiva, puesto que

$$f(x) = f(y) \iff \{x\} = \{y\} \iff x = y.$$

Además f es homomorfismo de anillos, pues

i) $f(1) = \{1\}$.

ii) $f(x + y) = \{x + y\} = \{x\} + \{y\} = f(x) + f(y)$.

iii) $f(xy) = \{xy\} = \{x\}\{y\} = f(x)f(y)$.

■

Definición 2.40
Se define $\mathcal{N} \subseteq \mathcal{C}$ como el conjunto $\mathcal{N} = \{\{x_n\} \mid x_n \to 0\}$, es decir, el conjunto de sucesiones de Cauchy que convergen a cero respecto a $|\cdot|_p$.

Proposición 2.41
$\mathcal{N}$ es un ideal maximal en $\mathcal{C}$.

Demostración

i) $\{0\} \in \mathcal{N}$, puesto que $\lim_{n\to\infty} |0|_p = 0$.

ii) Para probar la cerradura de la suma, consideremos $\{x_n\}, \{y_n\} \in \mathcal{N}$. Para $\epsilon > 0$ existen N_1, N_2 tales que, si $n \geq N_1$ y $m \geq N_2$ entonces $|x_n|_p < \epsilon$ y $|y_m|_p < \epsilon$. Sea $N = \text{máx}\{N_1, N_2\}$, para $n \geq N$ se tiene $|x_n + y_n|_p \leq \text{máx}\{|x_n|_p, |y_n|_p\} < \epsilon$, así $\lim_{n\to\infty} x_n + y_n = 0$, por lo tanto $\{x_n\} + \{y_n\} \in \mathcal{N}$.

iii) Sean $\{x_n\} \in \mathcal{C}$ y $\{y_n\} \in \mathcal{N}$. Tenemos que $\{x_n\}\{y_n\} = \{x_n y_n\}$, luego $|x_n y_n|_p = |x_n|_p |y_n|_p$, y como $\{x_n\} \in \mathcal{C}$, $\exists k \in \mathbb{R}$ tal que $|x_n|_p \leq k \, \forall n \in \mathbb{N}$. Luego

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

Entonces $\lim_{n\to\infty} |x_n y_n|_p = 0$, y así $\{x_n\}\{y_n\} \in \mathcal{N}$.

iv) Por último probaremos que $\mathcal{N}$ es ideal maximal. Sea $\mathcal{I}$ ideal de $\mathcal{C}$ tal que $\mathcal{N} \subseteq \mathcal{I}$ y $\mathcal{N} \neq \mathcal{I}$.
Como $\mathcal{I} \neq \mathcal{N}$, $\exists \{x_n\} \in \mathcal{I}$ tal que $x_n \nrightarrow 0$. Así existe $c > 0$ y $N \in \mathbb{N}$ tal que si $n \geq N$, entonces $|x_n|_p > c$. Definimos $\{y_n\}$ como

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

Así, para $n \geq N$ se tiene que

$$|y_{n+1} - y_n|_p = \left| \frac{1}{x_{n+1}} - \frac{1}{x_n} \right|_p = \frac{|x_n - x_{n+1}|_p}{|x_{n+1}|_p |x_n|_p} < \frac{|x_n - x_{n+1}|_p}{c^2}.$$

Como la sucesión $\{x_n\}$ es de Cauchy, tenemos $\lim_{n\to\infty} |x_{n+1} - x_n|_p = 0$. Entonces

$$\lim_{n\to\infty} |y_{n+1} - y_n|_p \leq \lim_{n\to\infty} \frac{|x_n - x_{n+1}|_p}{c^2} = 0.$$

Por lo que $\lim_{n\to\infty} |y_{n+1} - y_n|_p = 0$. Entonces $\{y_n\}$ es de Cauchy; además $\{x_n\}\{y_n\} \in \mathcal{I}$ por ser $\mathcal{I}$ ideal.
Por otro lado

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

Entonces $\{1\} - \{x_n y_n\} \in \mathcal{N}$. Sea $\{z_n\} = \{1\} - \{x_n y_n\}$, luego $\{1\} = \{x_n y_n\} + \{z_n\} \in \mathcal{I}$ pues, $\{x_n y_n\}, \{z_n\} \in \mathcal{I}$. Así $\mathcal{I} = \mathcal{C}$ y por lo tanto $\mathcal{N}$ es maximal en $\mathcal{C}$.

■

Definición 2.42
Se define el ***campo de los números p-ádicos*** *como el campo* $\mathbb{Q}_p = \mathcal{C}/\mathcal{N}$.

Lema 2.43
Sea $\{x_n\} \in \mathcal{C}$, $\{x_n\} \notin \mathcal{N}$. *La sucesión de números reales* $\{|x_n|_p\}$ *es eventualmente estacionaria, es decir,* $\exists N \in \mathbb{N}$ *tal que* $|x_n|_p = |x_m|_p$ *cuando* $m, n \geq N$.
Demostración
Como $x_n \nrightarrow 0$, existen $c > 0$ y $N_1 \in \mathbb{N}$ tales que, si $n \geq N_1$ entonces $|x_n|_p \geq c > 0$. Por otro lado, al ser $\{x_n\}$ de Cauchy, $\exists N_2 \in \mathbb{N}$ tal que si $n, m \geq N_2$ entonces $|x_n - x_m|_p < c$.
Sea $N = \text{máx}\{N_1, N_2\}$, y si $n, m \geq N$, entonces $|x_n - x_m|_p < c \leq |x_n|_p, |x_m|_p$. Se sigue que si $n, m \geq N$, entonces $|x_n - x_m|_p < \text{máx}\{|x_n|_p, |x_m|_p\}$. Como sabemos que todos los triángulos son isósceles (por el corolario 2.21) entonces $|x_n|_p = |x_m|_p$ si $m, n \geq N$.

■

Ahora nos encontramos en condiciones de extender el valor absoluto p-ádico (hasta el momento definido sólo sobre $\mathbb{Q}$) a todo el campo $\mathbb{Q}_p$.

Definición 2.44
Si $\lambda \in \mathbb{Q}_p$ *y* $\{x_n\}$ *es cualquier sucesión de Cauchy representante de* λ, *se define* $|\lambda|_p = \lim_{n\to\infty} |x_n|_p$.

La siguiente proposición garantiza que hemos definido correctamente el valor absoluto p-ádico sobre $\mathbb{Q}_p$.

Proposición 2.45
El límite de la definición anterior está bien definido.

Demostración
En primer lugar el límite existe, pues, por el lema 2.43, $\exists N \in \mathbb{N}$ tal que $|x_n|_p = |x_m|_p$ si $n, m \geq N$. Así $\lim_{n\to\infty} |x_n|_p = |x_N|_p$.
Por otro lado, el límite no depende de la elección de la sucesión representante de λ, pues si $\{x_n\}$ y $\{y_n\}$ son ambas representantes de λ, entonces $\{x_n\} - \{y_n\} \in \mathcal{N}$. Sea $\epsilon > 0$, entonces $\exists N \in \mathbb{N}$ tal que, si $n \geq N$ entonces $|x_n - y_n|_p < \epsilon$. Así tenemos que

$$
\begin{aligned}
&||x_n|_p - |y_n|_p|_{\mathbb{R}} \leq |x_n - y_n|_p < \epsilon \\
\implies &||x_n|_p - |y_n|_p|_{\mathbb{R}} < \epsilon \\
\implies &\lim_{n\to\infty}(|x_n|_p - |y_n|_p) = 0 \\
\implies &\lim_{n\to\infty}|x_n|_p = \lim_{n\to\infty}|y_n|_p.
\end{aligned}
$$

■

Proposición 2.46
La función $|\cdot|_p : \mathbb{Q}_p \to \mathbb{R}_+$ *definida anteriormente es un valor absoluto no arquimediano.*

Demostración

·) Probaremos el primer axioma de valor absoluto:
Sea $\{x_n\}$ representante de λ. Si $|\lambda|_p = 0$, tenemos que $\lim_{n\to\infty}|x_n|_p = 0$, entonces $\{x_n\} \in \mathcal{N}$, *i.e.* $\lambda = 0$. Ahora, si $\lambda = 0$, sea $\{x_n\}$ un representante de λ, entonces $\lim_{n\to\infty}|x_n|_p = 0$, así $|\lambda|_p = 0$.

·) Probaremos $|\lambda\beta|_p = |\lambda|_p|\beta|_p$:
Sean $\{x_n\}, \{y_n\}$ representantes de λ, β respectivamente, entonces

$$
\begin{aligned}
|\lambda|_p|\beta|_p &= \lim_{n\to\infty}|x_n|_p \lim_{n\to\infty}|y_n|_p \\
&= \lim_{n\to\infty}|x_n|_p|y_n|_p \\
&= \lim_{n\to\infty}|x_n y_n|_p = |\lambda\beta|_p.
\end{aligned}
$$

·) Por último probaremos que $|\lambda + \beta|_p \leq \text{máx}\{|\lambda|_p, |\beta|_p\}$:
Sean $\{x_n\}, \{y_n\}$ representantes de λ, β respectivamente. Entonces existen $N_1, N_2, N_3 \in \mathbb{N}$ tales que $|x_n|_p = |x_{N_1}|_p$ si $n \geq N_1$, $|y_n|_p = |y_{N_2}|_p$ si $n \geq N_2$ y $|x_n + y_n|_p = |x_{N_3} + y_{N_3}|_p$ si $n \geq N_3$. Sea $N = \text{máx}\{N_1, N_2, N_3\}$, así

$$
\begin{aligned}
|\lambda|_p &= \lim_{n\to\infty}|x_n|_p = |x_N|_p, \\
|\beta|_p &= \lim_{n\to\infty}|y_n|_p = |y_N|_p, \\
y \quad |\lambda + \beta|_p &= \lim_{n\to\infty}|x_n + y_n|_p = |x_N + y_N|_p.
\end{aligned}
$$

Como $|x_N + y_N|_p \leq \text{máx}\{|x_N|_p, |y_N|_p\}$, pues $|\cdot|_p$ es un valor absoluto no arquimediano sobre $\mathbb{Q}$, entonces $|\lambda + \beta| \leq \text{máx}\{|\lambda|_p, |\beta|_p\}$.

■

Lema 2.47
La imagen de $\mathbb{Q}$ bajo la inclusión $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ es un subconjunto denso en $\mathbb{Q}_p$.

Demostración
Probaremos que $\overline{\mathbb{Q}} = \mathbb{Q}_p$, lo que es lo mismo que probar $\mathbb{Q}_p = \mathbb{Q} \cup \mathbb{Q}'$, esto por el teorema 1.9. Sean $\epsilon > 0$, $\lambda \in \mathbb{Q}_p$ y sea $\{x_n\}$ una sucesión de Cauchy representante de λ. Sea ϵ' con $\epsilon' < \epsilon$, como $\{x_n\}$ es de Cauchy, $\exists N \in \mathbb{N}$ tal que $|x_n - x_m|_p < \epsilon'$ si $n, m \geq N$. Sea $y = x_N$, construimos entonces la sucesión constante $\{y\}$. Si $\beta \in \mathbb{Q}_p$ es representada por $\{y\}$, entonces β es la imagen de $y \in \mathbb{Q}$ bajo la inclusión. Así, $\lambda - \beta$ es representada por $\{x_n - y\}$ y

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

Como para $n \geq N$ tenemos que $|x_n - y|_p = |x_n - x_N| < \epsilon'$, entonces

$$\lim_{n \to \infty} |x_n - y|_p \leq \epsilon' < \epsilon.$$

Esto implica $\beta \in B(\lambda, \epsilon)$ y así $\lambda \in \mathbb{Q}'$. Luego $\mathbb{Q}_p \subseteq \mathbb{Q} \cup \mathbb{Q}'$, además, claramente $\mathbb{Q} \cup \mathbb{Q}' \subseteq \mathbb{Q}_p$. Por lo tanto $\mathbb{Q}$ es denso en $\mathbb{Q}_p$.

■

Proposición 2.48
$\mathbb{Q}_p$ es completo respecto a $|\cdot|_p$.

Demostración
Sea $\{\lambda_n\}$ una sucesión de Cauchy de elementos de $\mathbb{Q}_p$. Por el lema anterior, para cada $i \in \mathbb{N}$ $\exists \beta_i \in B(\lambda_i, \frac{1}{i})$ tal que β_i es la clase de equivalencia de una sucesión constante de números racionales $\{y_i\}$ y satisface $|\lambda_i - \beta_i|_p < \frac{1}{i}$.
Definamos $z_i = y_i$, así $\{z_i\}$ es una sucesión de números racionales y a continuación se probará que es de Cauchy.
Sea $\epsilon > 0$, entonces $\exists k \in \mathbb{N}$ tal que $\frac{1}{k} < \epsilon$. Por otro lado, como $\{\lambda_n\}$ es de Cauchy $\exists N' \in \mathbb{N}$ tal que, si $n, m \geq N'$ entonces $|\lambda_n - \lambda_m|_p < \frac{1}{k}$.
Sea $N = \text{máx}\{k, N'\}$, tenemos que $\beta_n - \beta_m$ es la clase de equivalencia de la sucesión constante $\{x_t\} = \{z_n - z_m\}$, entonces, si $n, m \geq N$ se sigue que

$$\begin{aligned}
|z_n - z_m|_p &= \lim_{t \to \infty} |x_t|_p \\
&= |\beta_n - \beta_m|_p \\
&= |\beta_n - \lambda_n + \lambda_n - \lambda_m + \lambda_m - \beta_m|_p \\
&\leq \text{máx}\{|\beta_n - \lambda_n|_p, |\lambda_n - \lambda_m|_p, |\lambda_m - \beta_m|_p\} \\
&< \text{máx}\left\{\frac{1}{n}, \frac{1}{k}, \frac{1}{m}\right\} = \frac{1}{k} < \epsilon.
\end{aligned}$$

Así $\{z_n\}$ es de Cauchy en $\mathbb{Q}$. Por último, sea λ la clase de equivalencia de $\{z_n\}$, se probará entonces que $\lim_{n\to\infty} \lambda_n = \lambda$. Sea $\epsilon > 0$, entonces $\exists k \in \mathbb{N}$ tal que $\frac{1}{k} < \epsilon$. Como $\{z_n\} = \{y_n\}$ es de Cauchy en $\mathbb{Q}$, entonces $\exists N^{'} \in \mathbb{N}$ tal que $|y_n - y_m|_p < \frac{1}{k}$ para $n, m \geq N^{'}$. Sea $N = \text{máx}\{k, N^{'}\}$, si $n \geq N$ tenemos que

$$|\lambda_n - \lambda|_p = |\lambda_n - \beta_n + \beta_n - \lambda|_p \leq \text{máx}\{|\lambda_n - \beta_n|_p, |\beta_n - \lambda|_p\}.$$

Ahora, como $n \geq k$, se cumple $|\lambda_n - \beta_n|_p < \frac{1}{n} \leq \frac{1}{k}$, además $|\beta_n - \lambda|_p = \lim_{m\to\infty} |z_n - z_m|_p \leq \frac{1}{k}$, pues si $m, n \geq N^{'}$, entonces $|y_m - y_n|_p < \frac{1}{k}$. Entonces $|\lambda_n - \lambda|_p \leq \frac{1}{k} < \epsilon$, así

$$\lim_{n\to\infty} \lambda_n = \lambda.$$

Por lo tanto $\mathbb{Q}_p$ es completo respecto a $|\cdot|_p$.

■

2.4. El campo $\mathbb{Q}_p$

Al igual que después de construir el campo de los números reales, podemos ser capaces de "olvidar" la construcción algebraica para trabajar de manera más natural con estos números entendiéndolos como un campo que contiene a los números racionales, el objetivo de esta sección es exponer las propiedades de $\mathbb{Q}_p$ entendiendo este conjunto de números como un campo que contiene a los números racionales, tratando en cierto sentido, de alejarnos de la parte algebraica realizada en la sección anterior.

Definición 2.49
En el campo de los números p-ádicos se define la bola con centro en a y radio p^r como el conjunto $B(a, p^r) = \{x \in \mathbb{Q}_p \mid |x - a|_p \leq p^r\}$, con $r \in \mathbb{Z}$.

Notemos que es irrelevante distinguir entre la bola abierta y la bola cerrada puesto que el conjunto $B(a, p^r) = \{x \in \mathbb{Q}_p \mid |x - a|_p < p^r\}$ es igual al conjunto $B(a, p^{r-1}) = \{x \in \mathbb{Q}_p \mid |x - a|_p \leq p^{r-1}\}$.

Definición 2.50
*El **anillo de enteros p-ádicos** es $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$.*

Notemos que las unidades de $\mathbb{Z}_p$ son los elementos $x \in \mathbb{Z}_p$ tales que $|x|_p = 1$.

Proposición 2.51
El anillo $\mathbb{Z}_p$ de enteros p-ádicos es un anillo local cuyo ideal maximal es el ideal principal $p\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq \frac{1}{p}\}$. Además los elementos del conjunto $\mathbb{Z}_p - p\mathbb{Z}_p$ son los únicos invertibles en $\mathbb{Z}_p$.

Demostración
Por la definición de $\mathbb{Z}_p$ y por la construcción de $p\mathbb{Z}_p$ sabemos por el teorema 2.24 que $\mathbb{Z}_p$ es anillo y $p\mathbb{Z}_p$ es un ideal maximal de $\mathbb{Z}_p$. Ahora probaremos que $p\mathbb{Z}_p$ es el único ideal maximal de $\mathbb{Z}_p$.
Sea I ideal de $\mathbb{Z}_p$, entonces $I \subseteq \mathbb{Z}_p$. Ahora, si existe algún $z \in I$ tal que $p \notin p\mathbb{Z}_p$, entonces $|z|_p = 1$. Así la igualdad $|1| = |z|_p|z^{-1}|_p$ implica que $|z^{-1}|_p = 1$, entonces $z^{-1} \in \mathbb{Z}_p$ y por ser I ideal de $\mathbb{Z}_p$ tenemos que $1 = zz^{-1} \in I$. Así para cualquier $x \in \mathbb{Z}_p$ se tiene $1x \in I$ es decir $x \in I$. Luego $\mathbb{Z}_p \subseteq I$ y así $I = \mathbb{Z}_p$. Entonces cualquier ideal propio de $\mathbb{Z}_p$ consta de elementos que no son unidades de $\mathbb{Z}_p$ y por lo tanto está contenido en $p\mathbb{Z}_p$.
Además por el teorema 2.24 tenemos que los únicos elementos invertibles en $\mathbb{Z}_p$ son $\mathbb{Z}_p - p\mathbb{Z}_p$.

■

Proposición 2.52

i) La inclusión $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ tiene una imagen densa en $\mathbb{Z}_p$. En particular, 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 $|x - \alpha|_p \leq \frac{1}{p^n}$.

ii) Para cualquier $x \in \mathbb{Z}_p$ existe una única sucesión de Cauchy $\{\alpha_n\}$ que converge a x y satisface lo siguiente:
a) $\alpha_n \in \mathbb{Z}$ para cada n y $0 \leq \alpha_n \leq p^n - 1$.
b) Para cada n se tiene $\alpha_n \equiv \alpha_{n-1} \pmod{p^{n-1}}$.

Demostración
i) Por las propiedades de $|\cdot|_p$ basta verificar que cada bola con centro en un entero p-ádico y radio p^{-n} con $n \in \mathbb{N}$ contiene un entero. Sea $x \in \mathbb{Z}_p$ y $n \in \mathbb{N}$. Como $\mathbb{Q}$ es denso en $\mathbb{Q}_p$ existe $\frac{a}{b} \in \mathbb{Q}$ tal que $|x - \frac{a}{b}|_p \leq \frac{1}{p^n} < 1$. Además $|\frac{a}{b}|_p = |\frac{a}{b} - x + x|_p \leq \max\{|x|_p, |x - \frac{a}{b}|_p\} \leq 1$, entonces $p \nmid b$, y así $p^n \nmid b$, es decir, $(p^n, b) = 1$, por lo que $\exists b', c \in \mathbb{Z}$ tales que $bb' + cp^n = 1$ y entonces $bb' \equiv 1 \pmod{p^n}$.
Por otro lado

$$\left|\frac{a}{b} - ab'\right|_p = \left|\frac{a - abb'}{b}\right|_p = \left|\frac{a(1 - bb')}{b}\right|_p.$$

Y como $p \nmid b$ y $p^n \mid 1 - bb'$, tenemos que $\frac{a(1-bb')}{b} = p^t\frac{a'}{b}$, para algún $t \geq n$, así

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

Entonces

$$|x - ab'|_p = |x - \tfrac{a}{b} + \tfrac{a}{b} - ab'| \leq \text{máx}\{|x - \tfrac{a}{b}|_p, |\tfrac{a}{b} - ab'|_p\} \leq p^{-n}.$$

Así ab' es un entero contenido en $B(x, \frac{1}{p^n})$, por lo tanto la imagen de $\mathbb{Z}$ es densa en $\mathbb{Z}_p$. Para la segunda parte, sea α el único entero que satisface $0 \leq \alpha \leq p^n - 1$ y $\alpha \equiv ab' \pmod{p^n}$, así tenemos que

$$|x - \alpha|_p = |x - ab' + ab' - \alpha|_p \leq \text{máx}\{|x - ab'|_p, |ab' - \alpha|_p\} \leq \tfrac{1}{p^n}.$$

Entonces α cumple las condiciones establecidas.

ii) Sea $x \in \mathbb{Z}_p$. Por $i)$ sabemos que para cada $n \in \mathbb{N}$ $\exists! \alpha_n$ tal que $0 \leq \alpha_n \leq p^n - 1$ y $|x - \alpha_n|_p \leq p^{-n}$. Sea $\{\alpha_n\}$ la sucesión descrita, entonces se tiene

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

Así

$$\begin{aligned} &\lim_{n\to\infty} |\alpha_{n+1} - \alpha_n|_p \leq \lim_{n\to\infty} p^{-n} = 0 \\ \implies &\lim_{n\to\infty} |\alpha_{n+1} - \alpha_n|_p = 0 \ . \end{aligned}$$

Entonces por el lema 2.34, $\{\alpha_n\}$ es de Cauchy. Por otro lado $|x - \alpha_n|_p \leq p^{-n}$ para todo $n \in \mathbb{N}$, así $\lim_{n\to\infty} |x - \alpha_n|_p = 0$, por lo tanto $\lim_{n\to\infty} \alpha_n = x$.
Así $\{\alpha\}$ satisface $a)$ por construcción, además

$$\begin{aligned} |\alpha_n - \alpha_{n-1}|_p &= |\alpha_n - x + x - \alpha_{n-1}|_p \\ &\leq \text{máx}\{|\alpha_n - x|_p, |x - \alpha_{n-1}|_p\} \\ &= p^{-(n-1)} \end{aligned}$$

entonces $\alpha_n \equiv \alpha_{n-1} \pmod{p^{n-1}}$.
Por último, la unicidad en $1)$ garantiza la unicidad de la sucesión.

■

Corolario 2.53
Para cualquier $n \in \mathbb{N}$, $\dfrac{\mathbb{Z}_p}{p^n\mathbb{Z}_p} \cong \dfrac{\mathbb{Z}}{p^n\mathbb{Z}}$.

Demostración
Para $x \in \mathbb{Z}_p$, sea α_x el único número entero que cumple $|x - \alpha_x|_p \leq p^{-n}$ y $0 \leq \alpha_x \leq p^n - 1$. Se define

$$f : \frac{\mathbb{Z}_p}{p^n\mathbb{Z}_p} \to \frac{\mathbb{Z}}{p^n\mathbb{Z}}$$

como $f(x + p^n\mathbb{Z}_p) = \alpha_x + p^n\mathbb{Z}$. Probaremos que f es un isomorfismo.

i) f está bien definida:
Si $x + p^n\mathbb{Z}_p = y + p^n\mathbb{Z}_p$ entonces $x - y \in p^n\mathbb{Z}_p$, es decir, $|x - y|_p \leq p^{-n}$. Por otro lado

$$\begin{aligned} |\alpha_x - \alpha_y|_p &= |\alpha_x - x + y - \alpha_y + x - y|_p \\ &\leq \text{máx}\{|\alpha_x - x|_p, |y - \alpha_y|_p, |x - y|_p\} \\ &= p^{-n}. \end{aligned}$$

Así $\alpha_x \equiv \alpha_y \pmod{p^n}$ entonces $\alpha_x + p^n\mathbb{Z}_p \equiv \alpha_y + p^n\mathbb{Z}_p$ y por lo tanto $f(\alpha_x + p^n\mathbb{Z}_p) = f(\alpha_y + p^n\mathbb{Z}_p)$.

ii) f es inyectiva:
En primer lugar tenemos que

$$\begin{aligned} & f(x + p^n\mathbb{Z}_p) = f(y + p^n\mathbb{Z}_p) \\ \implies \quad & \alpha_x + p^n\mathbb{Z}_p = \alpha_y + p^n\mathbb{Z}_p \\ \implies \quad & \alpha_x \equiv \alpha_y \pmod{p^n}. \end{aligned}$$

Por otro lado

$$\begin{aligned} |x - y|_p &= |x - \alpha_x + \alpha_x - \alpha_y + \alpha_y - y|_p \\ &\leq \text{máx}\{|x - \alpha_x|_p, |\alpha_x - \alpha_y|_p, |\alpha_y - y|_p\} \\ &\leq p^{-n}. \end{aligned}$$

Así, $x - y \in p^n\mathbb{Z}_p$ por lo que $x + p^n\mathbb{Z}_p = y + p^n\mathbb{Z}_p$.

iii) f es sobreyectiva:
Para $h + p^n\mathbb{Z} \in \frac{\mathbb{Z}}{p^n\mathbb{Z}}$ se tiene que $f(h + p^n\mathbb{Z}_p) = h + p^n\mathbb{Z}$.

iv) f es homomorfismo:
- $f(1 + p^n\mathbb{Z}_p) = 1 + p^n\mathbb{Z}$.
- $f(x + p^n\mathbb{Z}_p + y + p^n\mathbb{Z}_p) = f(x + y + p^n\mathbb{Z}_p) = \alpha_{x+y} + p^n\mathbb{Z} = \alpha_x + \alpha_y + p^n\mathbb{Z} = f(x + p^n\mathbb{Z}_p) + f(y + p^n\mathbb{Z}_p)$. Esto porque

$$\begin{aligned} |\alpha_x + \alpha_y - \alpha_{x+y}|_p &= |\alpha_x - x + \alpha_y - y + x + y - \alpha_{x+y}|_p \\ &\leq \text{máx}\{|\alpha_x - x|_p, |\alpha_y - y|_p, |x + y - \alpha_{x+y}|_p\} \\ &\leq p^{-n}. \end{aligned}$$

Entonces $\alpha_x + \alpha_y \equiv \alpha_{x+y} \pmod{p^n}$ y $\alpha_x + \alpha_y + p^n\mathbb{Z} = \alpha_{x+y} + p^n\mathbb{Z}$.

·) $f([x+p^n\mathbb{Z}_p][y+p^n\mathbb{Z}_p]) = f(xy+p^n\mathbb{Z}_p) = \alpha_{xy}+p^n\mathbb{Z} = \alpha_x\alpha_y + p^n\mathbb{Z} = f(x+p^n\mathbb{Z}_p)f(y+p^n\mathbb{Z}_p)$. Lo anterior porque

$$\begin{aligned}|\alpha_{xy}-\alpha_x\alpha_y|_p &= |\alpha_{xy}-xy+xy-y\alpha_x+y\alpha_x-\alpha_x\alpha_y|_p \\ &\leq \text{máx}\{|\alpha_{xy}-xy|_p, |xy-y\alpha_x|_p, |y\alpha_x-\alpha_x\alpha_y|_p\} \\ &\leq \text{máx}\{|\alpha_{xy}-xy|_p, |y|_p|x-\alpha_x|_p, |\alpha_x|_p|y-\alpha_y|_p\} \\ &\leq p^{-n}.\end{aligned}$$

Entonces $\alpha_{xy} \equiv \alpha_x\alpha_y$ y así $\alpha_{xy}+p^n\mathbb{Z} = \alpha_x\alpha_y+p^n\mathbb{Z}$.

■

Proposición 2.54
Si $\{x_n\}$ es una sucesión de Cauchy en $\mathbb{Q}_p$ formada por números enteros entonces su límite está en $\mathbb{Z}_p$.
Demostración
Sea $x = \lim_{n\to\infty} x_n$, entonces existe $N \in \mathbb{N}$ tal que $|x_n - x|_p < 1$ si $n \geq N$. Tenemos entonces que $|x|_p = |x - x_N + x_N|_p \leq \text{máx}\{|x-x_N|_p, |x_N|_p\} \leq 1$. Así $x \in \mathbb{Z}_p$.

■

Proposición 2.55
Cada $x \in \mathbb{Z}_p$ puede escribirse en la forma $x = b_0 + b_1p + \cdots + b_np^n + \cdots$ con $0 \leq b_i \leq p-1$, además esta representación es única.

Demostración
Sea $x \in \mathbb{Z}_p$, por la proposición 2.52 existe una única sucesión de Cauchy $\{\alpha_n\}$ que converge a x y satisface:
i) $\alpha_n \in \mathbb{Z}\ \forall n$ con $0 \leq \alpha_n \leq p^n - 1$.
ii) $\alpha_n \equiv \alpha_{n-1} \pmod{p^{n-1}}$.

Escribiendo cada α_n en base p se obtiene una serie de la siguiente forma:
1) $\alpha_1 = b_0$ con $0 \leq b_0 \leq p-1$.

2) $\alpha_2 = b_0' + b_1p$ con $0 \leq b_0', b_1 \leq p-1$ y $0 \leq \alpha_2 \leq p^2-1$. Ahora, como $\alpha_2 \equiv \alpha_1 \pmod{p}$ tenemos que $b_0' + b_1p \equiv b_0 \pmod{p}$, luego $b_0' \equiv b_0 \pmod{p}$ y $b_0' = b_0$, así $\alpha_2 = b_0 + b_1p$.

3) En general, si
$\alpha_{n+1} = b_0' + b_1'p + \cdots + b_n'p^n$ con $0 \leq b_i' \leq p-1$ y $0 \leq \alpha_{n+1} \leq p^{n+1}-1$,
y $\alpha_n = b_0 + b_1 + \cdots + b_{n-1}p^{n-1}$ con $0 \leq b_i \leq p-1$ y $0 \leq \alpha_n \leq p^n - 1$.
Dado que $\alpha_{n+1} \equiv \alpha_n \pmod{p^n}$, tenemos

$$b_0' + b_1' p + \cdots + b_n' p^n \equiv b_0 + b_1 + \cdots + b_{n-1} p^{n-1} \pmod{p^n}$$

entonces

$$b_0' + b_1' p + \cdots + b_{n-1}' p^{n-1} = b_0 + b_1 + \cdots + b_{n-1} p^{n-1}$$

Así $b_i' = b_i$ para cada i. Entonces

$$\begin{aligned}
\alpha_1 &= b_0 \\
\alpha_2 &= b_0 + b_1 p \\
\alpha_3 &= b_0 + b_1 p + b_2 p^2 \\
&\vdots \\
\alpha_{n+1} &= b_0 + b_1 p + \cdots + b_n p^n \\
&\vdots
\end{aligned}$$

con $0 \leq b_i \leq p-1$.
Como las sumas parciales son las α_n que convergen a x, esto implica que la serie construida converge a x.
Por lo tanto $x = b_0 + b_1 p + \cdots + b_n p^n + \cdots$ con $0 \leq b_i \leq p-1$, y la unicidad se garantiza por la unicidad de la sucesión $\{\alpha_n\}$.

■

Corolario 2.56
Cada $x \in \mathbb{Q}_p$ puede ser escrito de manera única en la forma

$$x = b_{-n_0} p^{-n_0} + b_{-n_0+1} p^{-n_0+1} + \cdots + b_0 + \cdots + b_n p^n + \cdots = \sum_{n \geq -n_0} b_n p^n$$

con $0 \leq b_i \leq p-1$ y $b_{-n_0} \neq 0$. Además $v_p(x) = -n_0$.

Demostración
Sea $x \in \mathbb{Q}_p$, distinguimos dos casos:
1) $x \in \mathbb{Z}_p$:
Sabemos que x se puede representar de manera única como $x = b_0 + b_1 p + \cdots + b_n p^n + \cdots$ con $0 \leq b_i \leq p-1$.
Ahora, sea n_k el menor entero positivo tal que $b_{n_k} \neq 0$, así

$$x = \sum_{n \geq n_k} b_n p^n = b_{n_k} p^{n_k} + \sum_{n \geq n_k + 1} b_n p^n$$

$$\implies |x|_p = \left| \sum_{n \geq n_k} b_n p^n \right|_p \leq \text{máx} \left\{ \left| b_{n_k} p^{n_k} \right|_p, \left| \sum_{n \geq n_k + 1} b_n p^n \right|_p \right\}.$$

Por la proposición 2.20 (todos los triángulos son isósceles) tenemos

$$|x|_p = \text{máx}\left\{ p^{-n_k}, \left| \sum_{n \geq n_k+1} b_n p^n \right|_p \right\}.$$

Como $|\sum_{n\geq n_k+1} b_n p^n|_p \leq p^{-n}$ entonces $|x|_p = p^{-n_k}$ y $v_p(x) = n_k$.

2) $x \notin \mathbb{Z}_p$:
Sea $n_0 = -v_p(x)$, se tiene que $n_0 \in \mathbb{Z}$, $n_0 > 0$, además $xp^{n_0} \in \mathbb{Z}_p$, luego

$$xp^{n_0} = \sum_{n\geq 0} b_n p^n, \quad b_0 \neq 0.$$

Entonces

$$x = p^{-n_0} \sum_{n\geq 0} b_n p^n = \sum_{n\geq -n_0} b_n p^n.$$

La unicidad se da por la unicidad de xp^{n_0} y es claro que $v_p(x) = -n_0$.

■

Ejemplo 2.57
$-1 = (p-1) + (p-1)p + \cdots + (p-1)p^n + \cdots$.

Esto es cierto debido a que, tomando sumas parciales obtenemos

$$s_n = (p-1) + (p-1)p + \cdots + (p-1)p^n = (p-1)\frac{p^{n+1}-1}{p-1} = p^{n+1} - 1.$$

Entonces

$$\lim_{n\to\infty} s_n = \lim_{n\to\infty} p^{n+1} - \lim_{n\to\infty} 1 = -1.$$

Esto porque

$$\lim_{n\to\infty} |p^{n+1} - 0|_p = \lim_{n\to\infty} |p^{n+1}|_p = \lim_{n\to\infty} \frac{1}{p^{n+1}} = 0.$$

Además, como hemos concluido que

$$-1 = (p-1)\sum_{i=1}^{\infty} p^i,$$

entonces también podemos decir que

$$\frac{1}{1-p} = \sum_{i=1}^{\infty} p^i.$$

■

2.5. El caso n-dimensional

Definición 2.58
*Una **norma** es una función $||\cdot||$ de un espacio vectorial*[1] $\langle X, F\rangle$ *a los números reales no negativos que satisface las siguientes propiedades para cualesquiera $x, y \in X$, $\alpha \in F$:*

i) $||x|| = 0$ *si y sólo si* $x = 0$.

ii) $||\alpha x|| = |\alpha|||x||$.

iii) $||x + y|| \leq ||x|| + ||y||$.

Si además la norma satisface $||x + y|| \leq$ máx$\{||x||, ||y||\}$, decimos que la norma es no arquimediana.

El espacio $\mathbb{Q}_p^n$ consiste de los puntos $x = (x_1, ..., x_n)$ con $x_j \in \mathbb{Q}_p$. La norma sobre $\mathbb{Q}_p^n$ se define como $||x||_p = \max\limits_{1\leq j\leq n} |x_j|_p$, $x \in \mathbb{Q}_p^n$.

Proposición 2.59
$||\cdot||_p$ es una norma no arquimediana.

Demostración
En primer lugar $||x||_p \geq 0$ para todo $x \in \mathbb{Q}_p^n$, pues $||x||_p = \max\limits_{1\leq j\leq n} |x_j|_p \geq 0$ por definición de valor absoluto.
Probaremos ahora que la norma definida anteriormente es efectivamente una norma.

i) $||x||_p = 0$ si y sólo si $x = 0$:
Si $||x||_p = 0$ entonces $\max\limits_{1\leq j\leq n} |x_j|_p = 0$, entonces $|x_j|_p \leq 0$ para todo j, y como el valor absoluto es una función no negativa entonces $|x_j|_p = 0$, por lo tanto $x_j = 0$.
Por otro lado, si $x = 0$, es claro que $||x||_p = 0$.

ii) $||\alpha x||_p = |\alpha|_p||x||_p$:
$||\alpha x||_p = \max\limits_{1\leq j\leq n} |\alpha x_j|_p = \max\limits_{1\leq j\leq n} |\alpha|_p|x|_p = |\alpha|_p \max\limits_{1\leq j\leq n} |x_j|_p = |\alpha|_p||x||_p$.

iv) $||x + y||_p \leq$ máx$\{||x||_p, ||y||_p\}$:

$$\begin{aligned} ||x + y||_p &= \max_{1\leq j\leq n} \{|x_j + y_j|_p\} \\ &\leq \max_{1\leq j\leq n} \text{máx}\{|x_j|_p, |y_j|_p\} \\ &= \text{máx}\{\max_{1\leq j\leq n} |x_j|_p, \max_{1\leq j\leq n} |y_j|_p\} \\ &= \text{máx}\{||x||_p, ||y||_p\}. \end{aligned}$$

[1] *Para consultar la definición de espacio vectorial ver [4].*

Como demostramos que $||x+y||_p \leq \text{máx}\{||x||_p, ||y||_p\}$, esto implica que $||x+y|| \leq ||x|| + ||y||$, y así la proposición queda demostrada.

■

Capítulo 3

Serie de Poincaré

En este capítulo estudiaremos la serie de Poincaré asociada a polinomios fuertemente no degenerados, los cuales se definirán más adelante. Antes de revisar los aspectos teóricos daremos una breve introducción histórica al surgimiento y estudio del problema, para esto será necesario definir las congruencias de enteros p-ádicos, concepto que es indispensable para entender la definición de la serie de Poincaré.

Definición 3.1
Decimos que dos números enteros p-ádicos a, b son ***congruentes*** *módulo p^n si $|a-b|_p \leq \frac{1}{p^n}$ y denotamos este hecho mediante $a \equiv b \pmod{p^n}$.*

3.1. Introducción

En 1964 los rusos Z.I. Borevich e I.R. Shafarevich publicaron el libro Teoría de números ([2]) en el cual apareció la siguiente conjetura:

Sean $F(x) \in \mathbb{Z}_p[x_1, ..., x_k]$ *y* $c_n = \#\left\{ x \in \left(\frac{\mathbb{Z}_p}{p^n\mathbb{Z}_p}\right)^k \;\middle|\; F(x) \equiv 0 \pmod{p^n} \right\}$ *para* $n \geq 1$*, es decir, el número de soluciones de la congruencia* $F(x) \equiv 0 \pmod{p^n}$*, donde* $c_0 = 1$*. Entonces la serie de Poincaré asociada a* F *y definida como*

$$P_F(t) = \sum_{n=0}^{\infty} c_n (p^{-k}t)^n$$

es una función racional de t*, para* $t \in \mathbb{C}$ *y* $|t| < 1$.

Ellos basaron la validez de esto observando el comportamiento de algunos casos particulares de funciones. Esta conjetura llamó la atención de la comunidad matemática de aquella época, y la conjetura se demostró en 1974, cuando el japonés Jun-Ichi Igusa probó la validez de este resultado como consecuencia de resultados más generales, utilizando un argumento no constructivo, apoyándose para su demostración en el teorema de resolución de singularidades del nipón Heisuke Hironaka, el cual es un resultado muy profundo en geometría algebraica. Años después, Jean Denef aportó otra prueba de la conjetura usando eliminación de cuantificadores en el campo de los números p-ádicos. La prueba de la conjetura está fuera de los alcances de esta tesis, pero para más detalles puede consultarse [8].

Como primer resultado del estudio de la serie de Poincaré probaremos que ésta es convergente. En efecto, si observamos que para cada $n \in \mathbb{N}$ el término c_n está acotado de la forma $c_n \leq p^{nk}$, tenemos que

$$\sum_{n=0}^{m} |c_n(p^{-k}t)^n| \leq \sum_{n=0}^{m} p^{nk}p^{-nk}|t|^n = \sum_{n=0}^{m} |t|^n < \infty.$$

Como $\sum_{n=0}^{\infty} |t|^n$ converge y $P_F(t)$ es absolutamente convergente, por el criterio de comparación, entonces la serie de Poincaré converge.

Por la definición de la serie de Poincaré podemos darnos cuenta que el problema principal consiste en hallar el número de soluciones de las congruencias involucradas en la serie, entonces, es oportuno analizar la definición de congruencia de enteros p-ádicos y ver la relación que guardan los anillos $\mathbb{Z}_p/p^n\mathbb{Z}_p$ y $\mathbb{Z}/p^n\mathbb{Z}$.

Centremos nuestra atención en el anillo $\mathbb{Z}_p/p^n\mathbb{Z}_p$, sus elementos son de la forma $a + p^n\mathbb{Z}_p = [a]$ donde a es un entero p-ádico que es representante de la clase de equivalencia $[a]$, ahora, por la proposición 2.52, sabemos que existe un único $\alpha \in \mathbb{Z}$ tal que $|x - \alpha|_p \leq \frac{1}{p^n}$, es decir $a \equiv \alpha \pmod{p^n}$, así siempre es posible encontrar un número entero representante de cualquier clase de equivalencia. Además, por el corolario 2.53 sabemos que $\mathbb{Z}_p/p^n\mathbb{Z}_p$ y $\mathbb{Z}/p^n\mathbb{Z}$ son isomorfos, por lo que es posible calcular los coeficientes c_n de la serie de Poincaré (en el caso $k = 1$) como el número de soluciones de $F(x) = 0$ en $\mathbb{Z}/p^n\mathbb{Z}$.

En vista de lo que se acaba de comentar, usaremos el hecho de que para calcular los coeficientes c_n de la serie de Poincaré basta con considerar soluciones en el anillo $(\mathbb{Z}/p^n\mathbb{Z})^k$; con esto presente estamos en condiciones de introducir un primer ejemplo y exponer los resultados de este capítulo.

Ejemplo 3.2
Calcularemos la serie de Poincaré para el polinomio $F(x) = x$, en el campo de los números 2-ádicos.

Podemos calcular fácilmente cada coeficiente c_n analizando la congruencia $F \equiv 0 \pmod{2^n}$ para cada valor de n:

- Para $n = 0$, $c_0 = 1$ por definición.
- Para $n = 1$, c_1 es igual al número de soluciones de $F(x) = x \equiv 0 \pmod 2$, pero las clases de equivalencia módulo 2 son $[0], [1]$, por lo que es claro que existe una única solución para este caso (la cual es $[0]$). Así $c_1 = 1$.
- Para $n = 2$. c_2 es igual al número de soluciones de $x \equiv 0 \pmod{2^2}$, es decir soluciones de $x \equiv 0 \pmod 4$, pero las clases de equivalencia módulo 4 son $[0], [1], [2], [3]$, y nuevamente existe una única solución, entonces $c_2 = 1$.
- En general para cualquier n, c_n es igual al número de soluciones de la congruencia $x \equiv 0 \pmod{2^n}$, pero es fácil notar que ésta tiene una única solución para cualquier valor de n como se mostró en los casos anteriores, por lo tanto $c_n = 1$ para cada $n \in \mathbb{N}$.

Ahora, la serie de Poincaré asociada al polinomio $f(x) = x$ está dada por:

$$P_f(t) = \sum_{n=0}^{\infty} c_n (2^{-1}t)^n = \sum_{n=0}^{\infty} \left(\frac{t}{2}\right)^n.$$

Analizando las sumas parciales tenemos

$$s_m = \sum_{n=0}^{m} \left(\frac{t}{2}\right)^n = \frac{(\frac{t}{2})^{m+1} - 1}{(\frac{t}{2}) - 1} \underset{m\to\infty}{\longrightarrow} \frac{1}{1 - \frac{t}{2}}.$$

Entonces la serie de Poincaré asociada al polinomio $f(x) = x$ es:

$$P_f(t) = \frac{1}{1 - (\frac{t}{2})} = \frac{2}{2 - t}.$$

En general, para el polinomio $f(x) = x$ en el campo de los números p-ádicos, es fácil ver que, como en el ejemplo anterior, $c_n = 1$ para todo n. Así la serie de Poincaré queda dada por

$$P_f(t) = \sum_{n=0}^{\infty} \left(\frac{t}{p}\right)^n = \frac{1}{1 - \frac{t}{p}} = \frac{p}{p - t}.$$

■

En el ejemplo anterior fue sencillo calcular los coeficientes c_n, sin embargo, necesitaremos otro tipo de artificios para resolver el mismo problema para polinomios más complicados, o más aún, para poder obtener algunos resultados en el caso general. Esto es lo que trataremos en la siguiente sección.

3.2. Número de soluciones de congruencias

Sea $f(x)$ un polinomio con coeficientes en $\mathbb{Z}_p$, una solución de $f(x) = 0$ sobre $(\mathbb{Z}/p^n\mathbb{Z})^k$ puede ser representada como una k-tupla $x = (x_1, \ldots, x_k)$ con $0 \leq x_i \leq p^n - 1$, y además podemos escribir cada x_i en su expansión en base p como sigue:

$$x_i = \sum_{j=0}^{n-1} a_j^{(i)} p^j \text{ donde } 0 \leq a_j^{(i)} \leq p-1.$$

Claramente $f(x) \equiv 0 \pmod{p^n}$ implica que $f(x) \equiv 0 \pmod{p^l}$ para todo $l \leq n$, puesto que

$$f(x) \equiv 0 \pmod{p^n} \implies |f(x)|_p \leq \frac{1}{p^n}$$
$$\implies |f(x)|_p \leq \frac{1}{p^l} \implies f(x) \equiv 0 \pmod{p^l}.$$

También observamos que x es congruente con un único $x' \in \left(\mathbb{Z}/p^l\mathbb{Z}\right)^k$ módulo p^l. En efecto, si $x \in (\mathbb{Z}/p^n\mathbb{Z})^k$ y $x' \in \left(\mathbb{Z}/p^l\mathbb{Z}\right)^k$ con $x = (x_1, \ldots, x_k)$ y $x' = (x_1', \ldots, x_k')$, entonces podemos expresar cada entrada x_i y x_i' de la forma

$$x_i = \sum_{j=0}^{n-1} a_j^{(i)} p^j \text{ con } 0 \leq a_j^{(i)} \leq p-1,$$
$$x_i' = \sum_{j=0}^{l-1} b_j^{(i)} p^j \text{ con } 0 \leq b_j^{(i)} \leq p-1.$$

Entonces $x \equiv x' \pmod{p^l}$ implica que para cada $i \in \{1, \ldots, k\}$ se cumple:

$$x_i = a_0^{(i)} + a_1^{(i)} p + \cdots + a_n^{(i)} p^{n-1} \overset{p}{\equiv} b_0^{(i)} + b_1^{(i)} p + \cdots + b_{l-1}^{(i)} p^{l-1} = x_i'.$$

Así por las propiedades de congruencias tenemos que $a_0^{(i)} \equiv b_0^{(i)} \pmod{p}$, ya que los demás términos se anulan al ser todos congruentes con cero módulo p, y como $0 \leq a_j^{(i)}, b_j^{(i)} \leq p-1$ tenemos que $a_0 = b_0$. Mediante un proceso análogo al anterior, es claro que $a_j^{(i)} = b_j^{(i)} \ \forall\, j \in \{0, \ldots, l-1\}$. Así, si $x' \equiv x \pmod{p^l}$, entonces $x' = \sum_{j=0}^{l-1} a_j^{(i)} p^j$, y por lo tanto x' es único.

Definición 3.3
*Sean x, x' como se han definido anteriormente, decimos que x es **descendiente** de x' si cada entrada de x' consiste de los primeros $l-1$ términos de la entrada correspondiente de x.*

Definición 3.4
*Una solución $a = (a_1\,,\,\ldots\,,\,a_k)$ en $(\mathbb{Z}/p\mathbb{Z})^k$ de $f \equiv 0 \pmod{p}$ es **no singular** si alguna de las derivadas parciales $f_{x_i}(a)$ no es congruente con cero módulo p. En otro caso decimos que la solución es singular.*

Lema 3.5
Sea $f(x_1,...,x_k)$ un polinomio sobre $\mathbb{Z}_p$ y sea $a = (a_1\,,\,\ldots\,,\,a_k) \in (\mathbb{Z}/p\mathbb{Z})^k$ una solución no singular de $f \equiv 0 \pmod{p}$, entonces existen $p^{(n-1)(k-1)}$ soluciones de $f \equiv 0 \pmod{p^n}$ descendientes de a.

Demostración
Sea $a^{(m)} = (a_1^{(m)},...,a_k^{(m)})$ una solución de la congruencia $f \equiv 0 \pmod{p^m}$ descendiente de $a = a^{(1)}$. Probaremos que existen p^{k-1} soluciones $a^{(m+1)}$ de $f \equiv 0 \pmod{p^{m+1}}$ descendientes de $a^{(m)}$. La prueba se va a hacer usando un argumento del tipo inductivo sobre el "índice de incidencia"de las soluciones $a^{(m)}$.
Pensando en números expresados en su expansión en base p, la idea es decidir para cuáles valores de b_i con $0 \leq b_i \leq p-1$ el vector $a^{(m+1)} = (a_1^{(m)} + b_1 p^m\,,\,\ldots\,,\,a_k^{(m)} + b_k p^m)$ es una solución de $f \equiv 0 \pmod{p^{m+1}}$. Considerando $b = (b_1,...,b_k)$, por el teorema de Taylor tenemos que:

$$f(a^{(m)} + bp^m) =$$
$$f(a^{(m)}) + \sum_{i=1}^{k} \frac{\partial f}{\partial x_i}(a^{(m)}) b_i p^m + \frac{1}{2} \sum_{i_1,i_2=1}^{k} \frac{\partial^2 f}{\partial x_{i_1} \partial x_{i_2}}(a^{(m)})(b_{i_1} p^m)(b_{i_2} p^m) + \cdots +$$
$$\frac{1}{r!} \sum_{i_1,\ldots,i_r=1}^{k} \frac{\partial^r f}{\partial x_{i_1} \cdots \partial x_{i_r}}(a^{(m)})(b_{i_1} p^m) \cdots (b_{i_r} p^m) +$$
$$\frac{1}{(r+1)!} \sum_{i_1,\ldots,i_{r+1}=1}^{k} \frac{\partial^{r+1} f}{\partial x_{i_1} \cdots \partial x_{i_{r+1}}}(a^{(m)})(b_{i_1} p^m) \cdots (b_{i_{r+1}} p^m).$$

Ahora, sabemos que $f(a^{(m)}) \equiv 0 \pmod{p^m}$, es decir, $f(a^{(m)}) = cp^m$, y los términos con derivadas de orden superior contienen p elevado a una potencia mayor que m por lo que son congruentes con cero módulo p^{m+1}, entonces para que

$$f(a^{(m)} + bp^m) = p^m \left(c + \sum_{i=1}^{k} f_{x_i}(a^{(m)}) b_i \right) \equiv 0 \pmod{p^{m+1}}$$

debe cumplirse que

$$c + \sum_{i=1}^{k} f_{x_i}(a^{(m)}) b_i \equiv 0 \pmod{p}.$$

Y como $a^{(m)} \equiv a^{(1)} \pmod{p}$, entonces podemos transformar la congruencia anterior en:

$$c + \sum_{i=1}^{k} f_{x_i}(a^{(1)})b_i \equiv 0 \pmod{p}.$$

Ahora, por hipótesis sabemos que $f_{x_i}(a^{(1)}) \not\equiv 0 \pmod{p}$ para algún i; distinguiendo a tal i como l, tenemos que, para cualquier elección de los b_i, $i \neq l$, obtendremos una congruencia lineal en la variable b_l de la forma:

$$f_{x_l}(a^{(1)})b_l \equiv -c - \sum_{\substack{i=1 \\ i\neq l}}^{k} f_{x_i}(a^{(1)})b_i \pmod{p}.$$

Y como $p \nmid f_{x_l}(a^{(1)})$ tenemos que $mcd(f_{x_l}(a^{(1)}), p) = 1$ por lo que la congruencia anterior tiene solución. Así hay p posibles elecciones para cada b_i, $i \neq l$, por lo que hay p^{k-1} soluciones de $f \equiv 0 \pmod{p^{m+1}}$.
Por último, utilizando $n-1$ veces el enunciado que acabamos de probar podemos concluir que existen $p^{(n-1)(k-1)}$ soluciones de $f \equiv 0 \pmod{p^n}$.
■

Dado el hecho de que cada solución de $f \equiv 0 \pmod{p^n}$ está "conectada" con sus descendientes *mod* p^{n+1} podemos interpretar nuestro problema usando la estructura de un árbol. Si a es una solución de $f = 0$ en $(\mathbb{Z}/p\mathbb{Z})^k$, entonces designamos a como la raíz del árbol y consideramos los nodos del árbol como los descendientes de a. Así cada solución *mod* p^n tiene por hijos a sus descendientes *mod* p^{n+1}. Decimos que el árbol descrito es el árbol asociado a a.

Proposición 3.6
Si a es una solución de $f \equiv 0 \pmod{p}$ que tiene un número infinito numerable de descendientes, entonces existe una solución $\bar{a}$ en $\mathbb{Z}_p^k$ de $f = 0$ tal que $\bar{a} \equiv a \pmod{p}$.

Demostración
Sea T el árbol asociado a a. Por hipótesis T es un árbol infinito, sin embargo, cada nodo de T es de grado finito, puesto que sólo existen un número finito de soluciones de $f \equiv 0 \pmod{p^n}$ para cada n.
Así, por el lema 1.11 existe un camino infinito, que comienza en a con vértices $a = a^{(1)}, a^{(2)}, ...$, que satisface $f(a^{(n)}) \equiv 0 \pmod{p^n}$ y $a^{(n+1)} \equiv a^{(n)} \pmod{p^n}$. Entonces existen enteros $c_i^{(j)}$ con $i = 0, 1, ...$ y $j = 1, ..., k$ que satisfacen $0 \leq c_i^{(j)} \leq p-1$, tales que:

$$a^{(n)} = \left(\sum_{i=0}^{n-1} c_i^{(1)} p^i \, , \, ... \, , \, \sum_{i=0}^{n-1} c_i^{(k)} p^i \right).$$

Definimos entonces $\overline{a}$ como sigue:

$$\overline{a} = \left(\sum_{i=0}^{\infty} c_i^{(1)} p^i \, , \ldots , \sum_{i=0}^{\infty} c_i^{(k)} p^i \right).$$

Así $\overline{a}$ es un elemento de $\mathbb{Z}_p^k$, puesto que, cada una de las entradas del vector $\overline{a}$ es de la forma

$$\sum_{i=0}^{\infty} c_i^{(j)} p^i$$

y si definimos la sucesión $\{s_n^{(j)}\}$ como $s_n^{(j)} = \sum_{i=0}^{n-1} c_i^{(j)} p^i$, tenemos que cada uno de los términos de la sucesión es un número entero y por la proposición 2.54 cada entrada de $\overline{a}$ es un entero p-ádico, así $\overline{a} \in \mathbb{Z}_p^k$.
Por otro lado, para que $\overline{a} \equiv a \pmod{p}$ se debe cumplir $||\overline{a} - a||_p \leq \frac{1}{p}$. Tenemos que

$$||\overline{a} - a||_p = \max_{1 \leq j \leq k} \{|\overline{a}_j - a_j|_p\}.$$

Ahora, tomando $|\overline{a}_j - a_j|_p$ para j arbitrario se tiene

$$\begin{aligned} |\overline{a}_j - a_j|_p = \left| \left(c_0^{(j)} + \sum_{i=1}^{\infty} c_i^{(j)} p^i \right) - c_0^{(j)} \right|_p &= \left| \sum_{i=1}^{\infty} c_i^{(j)} p^i \right|_p = \left| p \sum_{i=1}^{\infty} c_i^{(j)} p^{i-1} \right|_p \\ &= |p|_p \left| \sum_{i=1}^{\infty} c_i^{(j)} p^{i-1} \right|_p \leq \frac{1}{p} \cdot 1 = \frac{1}{p}. \end{aligned}$$

Entonces $||\overline{a} - a||_p \leq \frac{1}{p}$ y así $\overline{a} \equiv a \pmod{p}$.
Por último, por la continuidad de f tenemos que $f(\overline{a}) = 0$.

■

Corolario 3.7
Si a es una solución no singular de $f \equiv 0 \pmod{p}$, entonces existe una solución $\overline{a}$ en $\mathbb{Z}_p^k$ tal que $f(\overline{a}) = 0$ y $\overline{a} \equiv a \pmod{p}$.

Demostración
Por el lema 3.5 sabemos que a tiene un número infinito numerable de descendientes y por la proposición anterior dicho $\overline{a}$ existe.

■

Ejemplo 3.8
Calcularemos la serie de Poincaré para el polinomio $F(x, y) = x^2 + y^2$ en el campo de los números 3-ádicos.

En primer lugar notamos que $F(x, y) \equiv 0 \pmod{3}$ tiene una única solución que es $(0, 0)$. Además esta solución es singular, pues

$$\frac{\partial F}{\partial x}(0,0) = 0 \equiv 0 \pmod 3 \quad \text{y} \quad \frac{\partial F}{\partial y}(0,0) = 0 \equiv 0 \pmod 3.$$

Para encontrar el número de soluciones de $F \equiv 0 \pmod{3^n}$ para $n \geq 2$, nos basaremos en el hecho de que toda solución de tal congruencia es descendiente de la única solución de $F \equiv 0 \pmod 3$.

Entonces, para $n = 2$, las soluciones descendientes de $(0,0)$, en expansión base 3, son de la forma $(3a_1^{(1)}, 3a_1^{(2)})$, con $0 \leq a_1^{(j)} \leq 2$ de donde observamos que para cualquier elección de los $a_1^{(j)}$ se cumple que $F(3a_1^{(1)}, 3a_1^{(2)}) \equiv 0 \pmod 9$. Y como los dos términos $a_1^{(j)}$ pueden tomar tres posibles valores, entonces $c_2 = 3^2 = 9$.

Ahora, para $n \geq 3$, sea

$$a = \left(\sum_{i=1}^{n-1} 3^i a_i^{(1)} \, , \, \sum_{i=1}^{n-1} 3^i a_i^{(2)} \right), \quad \text{con } 0 \leq a_i^{(j)} \leq 2$$

una solución de $F \equiv 0 \pmod{3^n}$ descendiente de $(0,0)$. Entonces observamos que $F(a) = 3^2 F(a^*) \equiv 0 \pmod{3^n}$ si y sólo si $F(a^*) \equiv 0 \pmod{3^{n-2}}$, donde $a^* = (\sum_{i=1}^{n-1} 3^{i-1} a_i^{(1)}, \sum_{i=1}^{n-1} 3^{i-1} a_i^{(2)})$. Podemos observar en cada entrada de la solución que el término $3^{n-2} a_{n-1}^{(j)}$ es congruente con cero módulo 3^{n-2}, por lo que se tiene libre elección para el posible valor de a_{n-1}, es decir, tenemos $3^2 = 9$ posibilidades; entonces lo que buscamos es que la parte 'restante' de a^*, es decir $(\sum_{i=1}^{n-2} 3^{i-1} a_i^{(1)}, \sum_{i=1}^{n-2} 3^{i-1} a_i^{(2)})$ sea solución de $F \equiv 0 \pmod{3^{n-2}}$, congruencia de la que hay c_{n-2} soluciones. Así, para $n \geq 3$ tenemos que $c_n = 9c_{n-2}$ soluciones.

Por último haremos un poco de trabajo algebraico para obtener la serie de Poincaré asociada al polinomio.

$$\begin{aligned}
\sum_{n=2}^{\infty} c_n (3^{-2}t)^n &= \sum_{n=2}^{\infty} 9c_{n-2} \left(\frac{t}{9}\right)^n \\
&= 9 \sum_{n=2}^{\infty} c_{n-2} \left(\frac{t}{9}\right)^n \\
&= 9 \left(\frac{t}{9}\right)^2 \sum_{n=2}^{\infty} c_{n-2} \left(\frac{t}{9}\right)^{n-2} \\
&= \frac{t^2}{9} P_F(t).
\end{aligned}$$

Si escribimos el primer término de otra forma obtenemos

$$\begin{aligned} P_F(t) - c_0(3^{-2}t)^0 - c_1(3^{-2}t) &= \frac{t^2}{9}P_F(t) \\ P_F(t) - P_F(t)\frac{t^2}{9} &= c_0 + c_1\left(\frac{t}{9}\right) \\ P_F(t)\left(1 - \frac{t^2}{9}\right) &= 1 + \frac{t}{9} \\ P_F(t) &= \frac{1+\frac{t}{9}}{1-\frac{t^2}{9}} = \frac{9+t}{9-t^2}. \end{aligned}$$

Y podemos ver claramente que la serie de Poincaré asociada al polinomio $F(x,y) = x^2 + y^2$ es una función racional de t.

En la siguiente sección utilizaremos las ideas expuestas en el ejemplo anterior para deducir una fórmula para la serie de Poincaré asociada a cierta clase de polinomios.

3.3. Polinomios fuertemente no degenerados

Entendemos por polinomio homogéneo un polinomio tal que cada uno de sus términos tiene el mismo grado d. En este caso decimos que el grado del polinomio es d.

Definición 3.9
*Un **polinomio fuertemente no degenerado** es un polinomio homogéneo $F(x_1, ..., x_k)$ tal que la única solución singular (en caso de existir) de $F \equiv 0 \pmod{p}$, es $(0, ..., 0)$.*

Algunos ejemplos de polinomios fuertemente no degenerados son los siguientes: $F(x) = x$, $F(x,y) = x^2 + y^2$, ambos estudiados en ejemplos anteriores, $F(x) = x^2 + y^2 + xy$ para $p = 5$ por ejemplo, o de forma más general polinomios de la forma $F(x) = \sum_{i=1}^{k} x_i^d$ donde $p \nmid d$.

Teorema 3.10
Sea $F(x_1, ..., x_k)$ un polinomio fuertemente no degenerado de grado d con coeficientes en $\mathbb{Z}_p$. Sea c_n el número de soluciones de $F = 0$ en $(\frac{\mathbb{Z}}{p^n\mathbb{Z}})^k$ con $c_0 = 1$.

Entonces

a) $c_n = \begin{cases} (c_1-1)p^{(n-1)(k-1)} + p^{k(n-1)} & \text{para } 1 \leq n \leq d \\ (c_1-1)p^{(n-1)(k-1)} + p^{k(d-1)}c_{n-d} & \text{para } d < n \end{cases}$

b) La serie de Poincaré asociada a F es

$$P_F(t) = \frac{R(t)}{(1-p^{-1}t)(1-p^{-k}t^d)}$$

donde $R(t)$ es un polinomio de grado d efectivamente calculable.

Demostración

a) Consideremos

$$c_n = N_n + S_n$$

donde N_n es el número de soluciones módulo p^n descendientes de las soluciones no singulares módulo p, y S_n es el número de soluciones módulo p^n descendientes de $(0,...,0)$, que es la única solución singular módulo p.
Como $(0,...,0)$ es la única solución singular módulo p, entonces hay $c_1 - 1$ soluciones no singulares módulo p, así por el lema 3.5 tenemos

$$N_n = (c_1-1)p^{(n-1)(k-1)}.$$

Ahora, para calcular S_n trabajaremos por casos:

i) $n = 1$:
Por definición $S_1 = 1$.

ii) $2 \leq n \leq d$:
Sea

$$a = \left(\sum_{i=1}^{n-1} a_i^{(1)} p^i \, , \, \ldots \, , \, \sum_{i=1}^{n-1} a_i^{(k)} p^i \right)$$

un vector arbitrario, descendiente de $(0,...,0)$, congruente con 0 módulo p con $0 \leq a_i^{(j)} \leq p-1$. Entonces $a = pa^*$ donde

$$a^* = \left(\sum_{i=1}^{n-1} a_i^{(1)} p^{i-1} \, , \, \ldots \, , \, \sum_{i=1}^{n-1} a_i^{(k)} p^{i-1} \right).$$

Como $d \geq n$, tenemos por la homogeneidad de F que

$$F(a) = F(pa^*) = p^d F(a^*) \equiv 0 \pmod{p^n}.$$

Así todos los vectores son soluciones, y como hay $k(n-1)$ coeficientes $a_i^{(j)}$ y p posibles valores para cada uno de ellos, tenemos que $S_n = p^{k(n-1)}$.
Así $c_n = (c_1-1)p^{(n-1)(k-1)} + p^{k(n-1)}$.

iii) $d < n$:
Continuando con la notación del inciso anterior, la congruencia
$$F(a) = p^d F(a^*) \equiv 0 \pmod{p^n}$$
se cumple si y sólo si $F(a^*) \equiv 0 \pmod{p^{n-d}}$.
Pero $p^{n-d}, ..., p^{n-2} \equiv 0 \pmod{p^{n-d}}$, entonces tenemos libre elección para cada uno de sus respectivos $d-1$ coeficientes en cada entrada de a^*, quedando $p^{k(d-1)}$ elecciones posibles.
Ahora queremos que la parte "restante" de a^*, que es
$$\left(\sum_{i=1}^{n-d} a_i^{(1)} p^{i-1}, \dots, \sum_{i=1}^{n-d} a_i^{(k)} p^{i-1} \right),$$
sea una solución de $F \equiv 0 \pmod{p^{n-d}}$, congruencia de la que hay exactamente c_{n-d} soluciones. Así concluimos que $S_n = p^{k(d-1)} c_{n-d}$.
Entonces $c_n = (c_1 - 1)p^{(n-1)(k-1)} + p^{k(d-1)} c_{n-d}$.

b) Ahora deduciremos una función generadora para $P_F(t)$.
Podemos notar que para el caso $n = d$ ambas fórmulas obtenidas para c_n en el inciso a) coinciden, así podemos decir que

$$\begin{aligned}
\sum_{n=d}^{\infty} c_n (p^{-k}t)^n &= \sum_{n=d}^{\infty} \left[(c_1 - 1)p^{(n-1)(k-1)} + p^{k(d-1)} c_{n-d} \right] (p^{-k}t)^n \\
&= (c_1 - 1) \sum_{n=d}^{\infty} p^{(n-1)(k-1)} (p^{-k}t)^n + p^{k(d-1)} \sum_{n=d}^{\infty} c_{n-d} (p^{-k}t)^n \\
&= (c_1 - 1)(p^{-k}t) \sum_{n=d}^{\infty} (p^{k-1})^{n-1} (p^{-k}t)^{n-1} + p^{k(d-1)} \sum_{n=d}^{\infty} c_{n-d} (p^{-k}t)^n \\
&= (c_1 - 1)(p^{-k}t) \sum_{n=d}^{\infty} (p^{-1}t)^{n-1} + p^{k(d-1)} \sum_{n=d}^{\infty} c_{n-d} (p^{-k}t)^n.
\end{aligned}$$

Ahora, notemos que
$$\sum_{n=d}^{\infty} (p^{-1}t)^{n-1} = \sum_{n=1}^{\infty} (p^{-1}t)^{n-1} - \sum_{n=1}^{d-1} (p^{-1}t)^{n-1}.$$
Además
$$\sum_{n=1}^{\infty} (p^{-1}t)^{n-1} = \lim_{m \to \infty} \sum_{n=1}^{m} (p^{-1}t)^{n-1} = \lim_{m \to \infty} \frac{(p^{-1}t)^m - 1}{p^{-1}t - 1} = -\frac{1}{p^{-1}t - 1},$$
puesto que
$$|(p^{-1}t)^m - 0| = |p^{-m}t^m| = \frac{|t|^m}{|p|^m} \leq \frac{1}{p^m} \underset{m \to \infty}{\longrightarrow} 0.$$

Entonces

$$\sum_{n=d}^{\infty}(p^{-1}t)^{n-1} = -\frac{1}{p^{-1}t-1} - \left[\frac{(p^{-1}t)^{d-1}-1}{p^{-1}t-1}\right] = -\frac{(p^{-1}t)^{d-1}}{p^{-1}t-1}.$$

Retomando la primera ecuación obtenemos

$$\begin{aligned}\sum_{n=d}^{\infty} c_n(p^{-k}t)^n &= (c_1-1)(p^{-k}t)\left[-\frac{(p^{-1}t)^{d-1}}{p^{-1}t-1}\right] + p^{k(d-1)}\sum_{n=d}^{\infty} c_{n-d}(p^{-k}t)^n \\ &= \frac{(c_1-1)(p^{-k}t)(p^{-1}t)^{d-1}}{1-p^{-1}t} + p^{k(d-1)}(p^{-k}t)^d\sum_{n=d}^{\infty} c_{n-d}(p^{-k}t)^{n-d} \\ &= \frac{(c_1-1)(p^{-k}t)(p^{-1}t)^{d-1}}{1-p^{-1}t} + p^{k(d-1)}(p^{-k}t)^d P_F(t).\end{aligned}$$

Y reescribiendo el primer miembro de la ecuación tenemos

$$\begin{aligned}P_F(t) - \sum_{n=0}^{d-1} c_n(p^{-k}t)^n &= \frac{(c_1-1)(p^{-k}t)(p^{-1}t)^{d-1}}{1-p^{-1}t} + p^{k(d-1)}(p^{-k}t)^d P_F(t) \\ P_F(t)\left[1-p^{k(d-1)}(p^{-k}t)^d\right] &= \frac{(c_1-1)(p^{-k}t)(p^{-1}t)^{d-1} + (1-p^{-1}t)Q_F(t)}{1-p^{-1}t} \\ P_F(t) &= \frac{(c_1-1)(p^{-k}t)(p^{-1}t)^{d-1} + (1-p^{-1}t)Q_F(t)}{(1-p^{-1}t)(1-p^{k(d-1)}(p^{-k}t)^d)} \\ P_F(t) &= \frac{(c_1-1)(p^{-k}t)(p^{-1}t)^{d-1} + (1-p^{-1}t)Q_F(t)}{(1-p^{-1}t)(1-p^{-k}t^d)},\end{aligned}$$

donde $Q_F(t) = \sum_{n=0}^{d-1} c_n(p^{-k}t)^n$.

■

Es importante resaltar que el polinomio $Q_F(t)$ es un polinomio de grado $d-1$ que es posible calcular de manera directa usando la primera fórmula del inciso a) del teorema y la suma para series geométricas. Además por la forma de $Q_F(t)$ tenemos que el numerador obtenido es un polinomio de grado d.

Ahora analizaremos los ejemplos 3.2 y 3.8, usando la fórmula obtenida.

En primer lugar, en el caso general del ejemplo 3.2, estudiamos el polinomio $F(x) = x$, del cual obtuvimos que $c_1 = 1$, siendo (0) la única solución, ahora notemos que $\frac{dF}{dx} = 1$ y $\frac{dF}{dx}(0) = 1 \not\equiv 0 \pmod{p}$, por lo

que $F(x) = x$ es un polinomio fuertemente no degenerado. Entonces podemos aplicar la fórmula que acabamos de obtener para calcular la serie de Poincaré asociada:

$$\begin{aligned} P_F(t) &= \frac{(1-1)(p^{-1}t)(p^{-1}t)^{d-1} + (1-p^{-1}t)\sum_{n=0}^{1-1} c_n (p^{-1}t)^n}{(1-p^{-1}t)(1-p^{-1}t^1)} \\ &= \frac{(1-\frac{t}{p})(1)}{(1-\frac{t}{p})(1-\frac{t}{p})} \\ &= \frac{1}{1-\frac{t}{p}} \\ &= \frac{p}{p-t}. \end{aligned}$$

En el ejemplo 3.8 estudiamos el polinomio $F(x,y) = x^2 + y^2$, y encontramos que $F \equiv 0 \pmod{p}$ tiene una única solución, a saber $(0,0)$, la cual es singular, entonces $F(x,y) = x^2 + y^2$ es fuertemente no degenerado y podemos aplicar la fórmula anterior para calcular la serie de Poincaré asociada en los números 3-ádicos:

$$\begin{aligned} P_F(t) &= \frac{(1-1)(3^{-2}t)(3^{-1}t)^{2-1} + (1-3^{-1}t)\sum_{n=0}^{2-1} c_n (3^{-2}t)^n}{(1-3^{-1}t)(1-3^{-2}t^2)} \\ &= \frac{(1-\frac{t}{3})(1+\frac{t}{9})}{(1-\frac{t}{3})(1-\frac{t^2}{9})} \\ &= \frac{1+\frac{t}{9}}{1-\frac{t^2}{9}} \\ &= \frac{9+t}{9-t^2}. \end{aligned}$$

Así corroboramos que los resultados obtenidos al aplicar la fórmula corresponden a los resultados obtenidos previamente.

Ejemplo 3.11
Calcularemos la serie de Poincaré asociada a $F(x,y,z) = x^2 + 2y^2 + 3z^2$ en el campo de los números 5-ádicos, utilizando la fórmula obtenida en el teorema 3.10.

Primero probaremos que el polinomio es fuertemente no degenerado, para ello estudiaremos sus soluciones módulo 5.

Dado que módulo 5 tenemos 5 clases de equivalencia (a saber [0], [1], [2], [3] y [4]), por la definición del polinomio que estamos estudiando analizaremos el resultado de elevar al cuadrado cada una en módulo 5.

$[a]$	$[a^2]$
$[0]$	$[0]$
$[1]$	$[1]$
$[2]$	$[4]$
$[3]$	$[4]$
$[4]$	$[1]$

Como sólo hay 3 posibles resultados al elevar cualquier número al cuadrado en módulo 5, entonces podemos analizar todos los posibles valores que toma el polinomio para cada combinación de valores de x^2, y^2, z^2, los cuales se muestran organizados en la siguiente tabla.

x^2	y^2	z^2	$x^2 + 2y^2 + 3z^2$
$[0]$	$[0]$	$[0]$	$[0]$
$[0]$	$[0]$	$[1]$	$[3]$
$[0]$	$[0]$	$[4]$	$[2]$
$[0]$	$[1]$	$[0]$	$[2]$
$[0]$	$[1]$	$[1]$	$[0]$
$[0]$	$[1]$	$[4]$	$[4]$
$[0]$	$[4]$	$[0]$	$[3]$
$[0]$	$[4]$	$[1]$	$[1]$
$[0]$	$[4]$	$[4]$	$[0]$
$[1]$	$[0]$	$[0]$	$[1]$
$[1]$	$[0]$	$[1]$	$[4]$
$[1]$	$[0]$	$[4]$	$[3]$
$[1]$	$[1]$	$[0]$	$[3]$
$[1]$	$[1]$	$[1]$	$[1]$
$[1]$	$[1]$	$[4]$	$[0]$
$[1]$	$[4]$	$[0]$	$[4]$
$[1]$	$[4]$	$[1]$	$[2]$
$[1]$	$[4]$	$[4]$	$[1]$
$[4]$	$[0]$	$[0]$	$[4]$
$[4]$	$[0]$	$[1]$	$[2]$
$[4]$	$[0]$	$[4]$	$[1]$
$[4]$	$[1]$	$[0]$	$[1]$
$[4]$	$[1]$	$[1]$	$[4]$
$[4]$	$[1]$	$[4]$	$[3]$
$[4]$	$[4]$	$[0]$	$[2]$
$[4]$	$[4]$	$[1]$	$[0]$
$[4]$	$[4]$	$[4]$	$[4]$

De acuerdo a la tabla, hay cinco posibles combinaciones de clases de equivalencia de cuadrados de números módulo 5 que satisfacen $F \equiv 0 \pmod 5$. Ahora, desglosaremos las combinaciones de clases de equivalencia de números que originan estas cinco combinaciones encontradas:
·) $[0]$, $[0]$, $[0]$.

La única solución que genera esta combinación de clases de equivalencia de cuadrados de números es la solución $(0,0,0)$.

·) $[0]$, $[1]$, $[1]$.
Las soluciones que generan esta combinación son $(0,1,1)$, $(0,1,4)$, $(0,4,1)$ y $(0,4,4)$.

·) $[0]$, $[4]$, $[4]$.
Las soluciones que generan esta combinación son $(0,2,2)$, $(0,2,3)$, $(0,3,2)$ y $(0,3,3)$.

·) $[1]$, $[1]$, $[4]$.
Las soluciones que generan esta combinación son $(1,1,2)$, $(1,4,2)$, $(4,1,2)$, $(4,4,2)$, $(1,1,3)$, $(1,4,3)$, $(4,1,3)$ y $(4,4,3)$.

·) $[4]$, $[4]$, $[1]$.
Las soluciones que generan esta combinación son $(2,2,1)$, $(2,3,1)$, $(3,2,1)$, $(3,3,1)$, $(2,2,4)$, $(2,3,4)$, $(3,2,4)$, $(3,3,4)$.

Por lo tanto tenemos que $c_1 = 25$. Ahora hay que verificar que la solución $(0,0,0)$ en caso de ser singular, sea la única; para esto hay que observar que

$$\frac{\partial F}{\partial x} = 2x\,, \quad \frac{\partial F}{\partial y} = 4y\,, \quad \frac{\partial F}{\partial z} = 6z.$$

Es fácil notar que evaluando cada derivada parcial en cada una de las 25 soluciones encontradas, la única que hace todas las derivadas parciales congruentes con cero módulo 5 es la solución $(0,0,0)$, por lo tanto ésta es la única solución singular y así F es un polinomio fuertemente no degenerado.

Ahora lo que resta es aplicar la fórmula para hallar la serie de Poincaré asociada.

$$\begin{aligned} P_F(t) &= \frac{(25-1)(5^{-3}t)(5^{-1}t)^{2-1} + (1-5^{-1}t)\sum_{n=0}^{2-1} c_n(5^{-3}t)^n}{(1-5^{-1}t)(1-5^{-3}t^2)} \\ &= \frac{(24)(\frac{t}{5^3})(\frac{t}{5}) + (1-\frac{t}{5})(c_0(\frac{t}{5^3})^0 + c_1(\frac{t}{5^3}))}{(1-\frac{t}{5})(1-\frac{t^2}{5^3})} \\ &= \frac{\frac{24t^2}{5^4} + (1-\frac{t}{5})(1+\frac{25t}{5^3})}{(1-\frac{t}{5})(1-\frac{t^2}{5^3})} \end{aligned}$$

$$
\begin{aligned}
&= \frac{\frac{24t^2}{5^4} + 1 + \frac{25t}{5^3} - \frac{t}{5} - \frac{25t^2}{5^4}}{1 - \frac{t^2}{5^3} - \frac{t}{5} + \frac{t^3}{5^4}} \\
&= \frac{-\frac{t^2}{5^4} + 1}{\frac{t^3}{5^4} - \frac{t^2}{5^3} - \frac{t}{5} + 1} \\
&= \frac{\frac{-t^2+5^4}{5^4}}{\frac{t^3-5t^2-125t+5^4}{5^4}} \\
&= \frac{-t^2 + 625}{t^3 - 5t^2 - 125t + 625}.
\end{aligned}
$$

■

Capítulo 4

Conclusiones

Nuestro objetivo principal en este trabajo fue el de estudiar la serie de Poincaré asociada a polinomios fuertemente no degenerados, sin embargo, para lograrlo fue necesario introducir el campo de los números p-ádicos. El estudio de los resultados e incógnitas acerca de este tipo de números constituye una rama amplia del conocimiento matemático que sería imposible tratar de cubrir en este documento, sin embargo alcanzamos a sentar las bases para el estudio profundo de este tema, el cual además de ser interesante, cobra importancia en la actualidad debido a su incursión en otras áreas de la matemática, e incluso en otras ciencias, ya que recientemente han surgido nuevos modelos de sistemas físicos usando números p-ádicos.

Gracias al teorema 3.10 pudimos comprobar la racionalidad de la serie de Poincaré asociada a polinomios fuertemente no degenerados al obtener una fórmula relativamente sencilla que escribe esta serie como una función racional. Sin embargo, podemos pensar esta conjetura en un caso más general en el que el campo de los números p-ádicos es reemplazado por un cuerpo local no arquimediano arbitrario, originando una nueva conjetura que hasta la fecha es un problema abierto, pues aunque existen artículos sobre algunos casos particulares, el caso general sigue sin demostrarse.

Bibliografía

[1] BACHMAN, GEORGE, *Introduction to p-adic numbers and valuation theory*, Academic press, Nueva York, 1964.

[2] BOREVICH, Z.I. e I.R. SHAFAREVICH, *Number theory*, Academic press, Nueva York, 1966.

[3] DUGUNDJI, JAMES, *Topology*, Allin and Bacon Inc., 1966.

[4] FRIEDBERG, STEPHEN, ET. AL. *Álgebra lineal*, primera edición, Publicaciones cultural, México, 1982.

[5] GOLDMAN, JAY R., *Number of solution of congruences: Poincaré series for strongly nondegenerate forms*, Proceedings of the american mathematical society, Volumen 87, No. 4 (586-590), 1983.

[6] GOUVÊA, FERNANDO, *p-adic numbers: An introduction*, segunda edición, Springer, Berlín, 1997.

[7] HERSTEIN, I.N. *Álgebra moderna*, segunda edición, Trillas, México, 1990.

[8] IGUSA, JUN I., *An introduction to the theory of local zeta functions*, 2000.

[9] KNUTH, D. *The art of computer, programming. Vol. 1: Fundamental algorithms*, segunda edición , Addison-Wesley, Reading, Mass., 1973.

[10] KOBLITZ, NEAL, *p-adic numbers, p-adic analysis and zeta-functions*, segunda edición, Springer-Verlag, Nueva York, 1948.

[11] KREYSZIG, ERWIN, *Introductory functional analysis with aplications*, John Wiley and sons, 1978.

[12] MAHLER, KURT, *p-adic numbers and their functions*, segunda edición, Cambridge university press, Gran Bretaña, 1981.

[13] MUNKRES, JAMES, *Topología*, segunda edición, Pearson educación, Madrid, 2002.

[14] ROBERT, ALAIN M. *A course in p-adic analysis*, graduate text in mathematics, Springer-Verlag, Nueva York, 2000.

[15] ROTMAN, JOSEPH, *Advanced modern algebra*, Prentice Hall, 2002.

[16] RUDIN, WALTER, *Principios de análisis matemático*, tercera edición, McGraw Hill, México, 1980.

[17] RUIZ, JOSÉ LUIS *Una teoría computacional acerca de la lógica ecuacional*, Universidad de Sevilla, 2001.

[18] VLADIMIROV, V.S., I.V. VOLOVICH y E.I. ZELENOV, *p-adic analysis and mathematical physics*, World scientific publishing co., Singapur, 1994.

[19] ZALDÍVAR, FELIPE, *Introducción a la teoría de números*, FCE, México, 2012.

Índice alfabético