1. Los números p-ádicos

Los números p-ádicos fueron introducidos por Kurt Hensel en 1897 cuando mostró la relación de las estructuras de los anillos de factorización única $\mathbb{Z}$ y $\mathbb{C}[X]$ (el anillo de polinomios con coeficientes complejos), con su cuerpo de fracciones respectivo, $\mathbb{Q}$ y $\mathbb{C}(X)$. Esta relación estaba dada así:

Si $m \in \mathbb{Z}$ y p- primo, con $n_j \in \mathbb{N}$ entonces existe $B_j \in \mathbb{C}, 1 \leqslant j \leqslant k$ tal que $m = \pm(p_1^{n_1} \cdots p_k^{n_k})$ y $P(X) = \alpha(X - B_1)^{n1} \cdots (X - B_k)^{n_k}$, luego se puede ver claramente que los números primos son a $\mathbb{Z}$ como los polinomios lineales a $\mathbb{C}[X]$. ($\mathbb{Z}$ y $\mathbb{C}[X]$ son dominios de ideales principales, en los cuales todos los ideales primos no nulos son maximales).

Además, dado que para un polinomio $P(X)$, $B \in \mathbb{C}$, $m \in \mathbb{Z}^+$ y p -primo, es posible expresar

$$P(X) = \sum_{j=0}^{n} \alpha_j (X - B)^j, \alpha_j \in \mathbb{C}, n \in \mathbb{N}$$

y

$$m = \sum_{j=0}^{n} a_j p^j,\ 0 \leqslant a_j \leqslant p - 1,$$

es evidente que en ambos casos se obtiene información sobre el comportamiento de series de potencias. En la primera si B anula $P(X)$ y en la segunda, si p divide a m. En el caso de $P(X)$ observe que se pueden considerar potencias negativas y en ese caso, se tiene una serie de Laurent, así $f(X) = \sum\limits_{j \geqslant n_0} a_j (X - \alpha)^j,\ f(X) \in \mathbb{C}(X)$ y para $X \in \mathbb{Q},\ X = \sum\limits_{j \geqslant n_0} a_j p^j$, de esta forma Hensel vio que el conjunto de las series formales de Laurent en p forman el cuerpo de números p-ádicos, $\mathbb{Q}_p \supseteq \mathbb{Q}$.

Operaciones en base p.

Para el caso decimal se tiene la descomposición en base 10, por ejemplo

$$12453 = (1)10^4 + (2)10^3 + (4)10^2 + (5)10^1 + (3)10^0.$$

Además, de 10, se puede hacer para cualquier $p \in \mathbb{Z} \setminus \{0\}$, en particular se trabajará con p primo.

Ejemplo 1.1. *: Calcular 1244 y 725 en base 7.*

$$\begin{aligned}
1244 &= (177)7 + 5 = ((25)7 + 2)7 + 5 = (25)7^2 + (2)7 + 5 \\
&= ((3)7 + 4)7^2 + (2)7 + 5 = (3)7^3 + (4)7^2 + (2)7 + 5 \\
725 &= (103)7 + 4 = ((14)7 + 5)7 + 4 = (14)7^2 + (5)7 + 4 \\
&= ((2)7)7^2 + (5)7 + 4 = (2)7^3 + (5)7 + 4
\end{aligned}$$

Se denotará $1244 = (\ldots 003425)_7$ y $725 = (\ldots 002054)_7$.
Sean $n, m \in \mathbb{N}$ y p primo, existen $k, j \in \mathbb{N}$ tal que

$$\begin{aligned}
n &= (\ldots a_k a_{k-1} \ldots a_1 a_0)_p \\
m &= (\ldots b_j b_{j-1} \ldots b_1 b_0)_p
\end{aligned}$$

se define $\{c_i\}$ como

$$\begin{aligned}
&c_0 \equiv a_0 + b_0 \mod p \Leftrightarrow a_0 + b_0 = s_0 p + c_0, \\
&c_1 \equiv a_1 + b_1 + s_0 \mod p \Leftrightarrow a_1 + b_1 + s_0 = s_1 p + c_1, \\
&\quad \vdots \\
&c_i \equiv a_i + b_i + s_{i-1} \mod p \Leftrightarrow a_i + b_i + s_{i-1} = s_i p + c_i,
\end{aligned}$$

entonces

$$n+m=(\ldots c_{M+1}c_M\ldots c_1c_0)_p,$$

donde $M=\text{máx}\{k,j\}$ y $0\leq c_{M+1}\leq p-1$.

Ejemplo 1.2. : *Sean* $10320=(\ldots 042042)_7$ *y* $1244=(\ldots 003425)_7$, *entonces*

$$\begin{array}{ccccccc} & 0 & 4 & 2 & 0^{+1} & 4^{+1} & 2\\ + & 0 & 0 & 3 & 4 & 2 & 5\\ \hline & 0 & 4 & 5 & 5 & 0 & 0\end{array}$$

así

$$(\ldots 042042)_7+(\ldots 003425)_7=(\ldots 045500)_7,$$
$$(4)7^4+(5)7^3+(5)7^2=11564=10320+1244.$$

Ejemplo 1.3. : *Calcular* -12 *en base* 7.

$$\begin{aligned}-12\equiv 2\mod 7\Leftrightarrow -12=(-2)7+2\Leftrightarrow -12=-7-7+2,\\ -12=(-7)+(-7)+(2)\\ =(\ldots 66660)_7+(\ldots 66660)_7+(\ldots 00002)_7=(\ldots 66652)_7.\end{aligned}$$

Ejemplo 1.4. : *Tomando* $1140=(3216)_7$ *y* $216=(426)_7$, *es claro que* $1140-426=924$ *y* $924=(2460)_7$. *Pues bien,*

$$\begin{array}{ccccccccccc} & (3216)_7 & = & 3\cdot 7^3 & + & 2\cdot 7^2 & + & 1\cdot 7 & + & 6\\ - & (426)_7 & = & & & 4\cdot 7^2 & + & 2\cdot 7 & + & 6\\ \hline & & & 3\cdot 7^3 & - & 2\cdot 7^2 & - & 1\cdot 7 & + & 0\end{array}$$

Al igual que para la suma, el resultado obtenido no es un desarrollo 3-ádico. Para lograrlo, se debe operar de la siguiente manera:

$$\begin{aligned}3\cdot 7^3-2\cdot 7^2-1\cdot 7+0=&2\cdot 7^3+1\cdot 7^3-2\cdot 7^2-1\cdot 7+0\\ =&2\cdot 7^3+7\cdot 7^2-2\cdot 7^2-1\cdot 7+0\\ =&2\cdot 7^3+5\cdot 7^2-1\cdot 7+0\\ =&2\cdot 7^3+4\cdot 7^2+1\cdot 7^2-1\cdot 7+0\\ =&2\cdot 7^3+4\cdot 7^2+7\cdot 7-1\cdot 7+0\\ =&2\cdot 7^3+4\cdot 7^2+6\cdot 7+0.\end{aligned}$$

Luego, la resta se realiza de forma análoga a la usual restando las cifras correspondientes y cada vez que debamos restar una cifra mayor a una que es menor, se debe tomar prestado de la cifra anterior p unidades, en este caso 7, y se resta 1 a la cifra siguiente, es decir, utilizando congruencias y "sustrayendo unidades":

$$\begin{array}{ccccc} & 3^{-1} & {}^{+7}2^{-1} & {}^{+7}1 & 6\\ - & & 4 & 2 & 6\\ \hline & 2 & 4 & 6 & 0\end{array}$$

Lema 1.1. *Sea* $a=(\ldots a_ka_{k-1}\ldots a_1a_0)_p$ *la expansión en base* p *de* $a\in\mathbb{N}$, *entonces el desarrollo de* $-a$ *es el siguiente*

$$-a=(\ldots(p-1)(p-1)[(p-1)-a_k]\ldots[(p-1)-a_1](p-a_0))_p.$$

Sean $n,m\in\mathbb{N}$ y p primo, existen $k,j\in\mathbb{N}$ tal que

$$n=(\ldots a_ka_{k-1}\ldots a_1a_0)_p$$
$$m=(\ldots b_jb_{j-1}\ldots b_1b_0)_p,$$

por otra parte

$$\begin{aligned}m&=(\ldots b_jb_{j-1}\ldots b_1b_0)_p\\ &=(\ldots b_j\ldots 00)_p+\cdots+(\ldots 0\ldots b_10)_p+(\ldots 00\ldots 0b_0)_p,\end{aligned}$$

entonces

$$\begin{aligned} nm &= (\dots a_k a_{k-1} \dots a_1 a_0)_p (\dots b_j \dots 00)_p + \dots + \\ &+ (\dots a_k a_{k-1} \dots a_1 a_0)_p (\dots 00 \dots 0 b_0)_p. \end{aligned}$$

Sean $n, m \in \mathbb{N}$ y p primo, existen $k, j \in \mathbb{N}$ tal que

$$\begin{aligned} n &= (\dots a_k a_{k-1} \dots a_1 a_0)_p \\ m &= (\dots b_j b_{j-1} \dots b_1 b_0)_p, \end{aligned}$$

por otra parte

$$\begin{aligned} m &= (\dots b_j b_{j-1} \dots b_1 b_0)_p \\ &= (\dots b_j \dots 00)_p + \dots + (\dots 0 \dots b_1 0)_p + (\dots 00 \dots 0 b_0)_p, \end{aligned}$$

entonces

$$\begin{aligned} nm &= (\dots a_k a_{k-1} \dots a_1 a_0)_p (\dots b_j \dots 00)_p + \dots + \\ &+ (\dots a_k a_{k-1} \dots a_1 a_0)_p (\dots 00 \dots 0 b_0)_p. \end{aligned}$$

Ejemplo 1.5. $1244 = (\dots 03425)_7$ *y* $256 = (\dots 00514)_7$

$$\begin{array}{cccccccc} & 0 & 0 & 0 & 3 & 4 & 2 & 5 \\ \times & 0 & 0 & 0 & 0 & 5 & 1 & 4 \\ \hline & 0 & 0 & 2 & 0 & 3 & 3 & 6 \\ + & 0 & 0 & 3 & 4 & 2 & 5 & \\ & 2 & 4 & 0 & 6 & 4 & & \\ \hline 0 & 2 & 4 & 6 & 4 & 3 & 1 & 6 \end{array}$$

así

$$(\dots 03425)_7 (\dots 00514)_7 = (\dots 02464316)_7.$$

Ejemplo 1.6. *El desarrollo en base p de p^n con $n \in \mathbb{N}$ es*

$$p^n = (\dots 001\underbrace{0\dots 00}_{n-ceros})_p.$$

Para el caso cuando la potencia es negativa se hará

$$p^{-n} = (\dots 0, \underbrace{000\dots 00}_{(n-1)-ceros}1)_p.$$

Se mostrará un algoritmo basado en el algoritmo de división de polinomios, que permite escribir a los números racionales en $\mathbb{Q}_p$.
Note que hay racionales que ya se pueden escribir en base p. Por ejemplo

$$\frac{7}{81} = \frac{2 \cdot 3 + 1}{3^4} = \frac{2}{3^3} + \frac{1}{3^4} = 2 \cdot 3^{-3} + 1 \cdot 3{-}4 = (0, 0021).$$

Ahora, escribiendo $\frac{36}{25}$ en base 5, se obtiene

$$\frac{36}{25} = \frac{(1)5^2 + (2)5 + 1}{5^2} = (1)5^0 + (2)5^{-1} + (1)5^{-2},$$

entonces

$$\frac{36}{25} = (\dots 01, 21)_5.$$

Pero hay racionales en $\mathbb{Q}_p$ cuyo desarrollo no es tan evidente. Dado que se admiten infinitas cifras a la izquierda, para realizar la división, se pondrá el divisor a la izquierda y el dividendo a la derecha, es decir, con el orden inverso. Así dados $a = (\dots a_2 a_1 a_0)_p$ y $b = (\dots b_2 b_1 b_0)_p$, se desea hacer el cociente $\frac{a}{b}$, se expresa:

$$\dots b_2 b_1 b_0 \;\; \left|\overline{\; a_0 a_1 a_2 \dots}\right.$$

Ejemplo 1.7. *1. Escribir* $\frac{7}{23}$ *en base* 3.

Dado que $7 = (\ldots 0021)_3$ *y* $23 = (\ldots 000212)_3$ *luego*

$$\begin{array}{r|r}
 & \overline{20110} \\
\ldots 0021 & 21200000\ldots \\
 & \underline{-21100000\ldots} \\
 & 00100000\ldots \\
 & \underline{-0000000\ldots} \\
 & 010000\ldots \\
 & \underline{-12000\ldots} \\
 & 012222\ldots \\
 & \underline{-12000\ldots} \\
 & 00222\ldots
\end{array}$$

Por lo anterior, $\frac{7}{23} = (\ldots 0110201102)_3$.

2. Calcular $\dfrac{23}{11}$ *en base* 5*: Claramente* $23 = (\cdots 0043)_5$ *y* $11 = (\cdots 0021)_5$.

$$\begin{array}{r|r}
 & \overline{33324} \\
\ldots 0021 & 340000\ldots \\
 & \underline{-311000\ldots} \\
 & 0344444444\ldots \\
 & \underline{-311000000\ldots} \\
 & 033444444\ldots \\
 & \underline{-3110000\ldots} \\
 & 0234444\ldots \\
 & \underline{-240000\ldots} \\
 & 043444\ldots \\
 & \underline{-043100\ldots} \\
 & 00340\ldots
\end{array}$$

Por lo anterior, $\dfrac{23}{11} = (\cdots 04233042333)_5$.

Definición 1.1. *Sea* p *un número primo. Se define el orden p-ádico,* $ord_p(x)$*, de un* $x \in \mathbb{Q}$ *de la siguente manera:*

i) Si $x \in \mathbb{Z}$ *entonces* $ord_p(x)$ *es igual a la potencia más grande de* p *que divide a* x.

ii) Si $x = \frac{a}{b}$*, con* $a, b \in \mathbb{Z}$ *y* $b \neq 0$*, entonces* $ord_p(x) = ord_p(a) - ord_p(b)$.

iii) $ord_p(0) = +\infty$.

Sea $p = 7$, se calculará $ord_7(28)$ y $ord_7\left(\frac{13}{98}\right)$

- Puesto que $28 = 2^2 7^1$, entonces $ord_7(28) = 1$.
- Dado que 13 es primo y $98 = 2^1 7^2$, entonces $ord_7\left(\frac{13}{98}\right) = 0 - 2 = -2$.

El orden p-ádico también se denomina valuación p-ádica y se denota por $v_p(x)$.

Lema 1.2. *Para todo* $x, y \in \mathbb{Q}$ *se cumple:*

i) $ord_p(xy) = ord_p(x) + ord_p(y)$

ii) $ord_p(x + y) \geq \min\{ord_p(x), ord_p(y)\}$

Sea $p = 7$,

- $ord_7(28 \cdot 98) = ord_7(2^3 7^3) = 3 = ord_7(2^2 7^1) + ord_7(2^1 7^2)$
- $ord_7(28 + 98) = ord_7(2^1 3^2 7^1) = 1 \geq \min\{1, 2\}$.

2. Valores absolutos sobre campos

Sea $\Bbbk$ un campo y $\mathbb{R}^+ = \{x \in \mathbb{R} : x \geq 0\}$ el conjunto de los números reales no negativos. Un **valor absoluto** sobre $\Bbbk$ es una función

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

que satisface las siguientes condiciones:

i) $|x| = 0$ si y sólo si $x = 0$.

ii) $|xy| = |x||y|$ para todo $x, y \in \Bbbk$.

iii) $|x + y| \leq |x| + |y|$ para todo $x, y \in \Bbbk$.

Un valor abosluto sobre un campo $\Bbbk$ es llamado **no arquimediano** si satisface además

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

para todo $x, y \in \Bbbk$. En otro caso se dice que el valor absoluto es **arquimediano**.

Observación 1

La condición $|x + y| \leq \text{máx}\ \{|x|, |y|\}$ implica la condición $iii)$ de la definición de valor absoluto porque $\text{máx}\ \{|x|, |y|\} \leq |x| + |y|$.

Ejemplo 2.1. *Sea $\Bbbk = \mathbb{Q}$, se define un valor absoluto sobre $\Bbbk$ como:*

1.
$$|x| = \begin{cases} x & si\ x \geq 0. \\ -x & si\ x < 0. \end{cases}$$

*Este valor absoluto se conoce como **valor absoluto usual**, y se denotará por $|\cdot|_\infty$ y es arquimediano, pues si $x = y = 1$ se tiene*

$$|x + y| = 2 > máx\{|x|, |y|\} = 1.$$

2. *Sea $\Bbbk$ un campo, se define un valor absoluto sobre $\Bbbk$ como:*

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

*Este valor absoluto se conoce como **valor absoluto trivial**.*

Proposición 2.1. *Si $\Bbbk$ es un campo de orden finito entonces el único valor absoluto que se puede definir sobre $\Bbbk$ es el trivial.*

Demostración. Sea $|\cdot| : \Bbbk \longrightarrow \mathbb{R}^+$ un valor absoluto sobre $\Bbbk$. Para 0 se tiene que $|0| = 0$ por la definición de valor absoluto.
Si $x \in \Bbbk$ es tal que $x \neq 0$ entonces $x^n = x$, donde $n \in \mathbb{N}$ es el orden de $\Bbbk$. Luego,

$$|x^n| = |x| \Longrightarrow |x|^n = |x| \Longrightarrow |x|^{n-1} = 1 \Longrightarrow |x| = 1.$$

Así, $|\cdot|$ es el valor absoluto trivial. $\square$

Definición 2.1. *Sea $p \in \mathbb{Z}$ un número primo fijo. La **valuación** $p-$**ádica** sobre $\mathbb{Z}$ es la función*

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

definida como sigue: Para cada entero $n \in \mathbb{Z}$,$n \neq 0$, sea $v_p(n)$ el único entero no negativo que satisface

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

El dominio de la función $v_p(n)$ se extiende al campo de los números racionales de la siguiente manera: si $x = \frac{a}{b} \in \mathbb{Q} - \{0\}$ entonces

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

con la convención de que $v_p(0) = +\infty$.

Observación 2

El teorema fundamental de la aritmética garantiza la existencia y unicidad de la función $v_p(n), \forall n \in \mathbb{Z}$, en la definición anterior.
La valuación $p-$ádica de cualquier $x \in \mathbb{Q} - \{0\}$ está determinada por la fórmula

$$x = p^{v_p(x)} \frac{a}{b} \text{ donde } a, b \in \mathbb{Z} \text{ y } p \nmid ab.$$

Lema 2.1. *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

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

y

$$m = p^{v_p(m)} m' \text{ donde } p \nmid m'.$$

Luego,

$$mn = p^{v_p(m)} m' p^{v_p(n)} n' \text{ donde } p \nmid m'n'.$$

Así,

$$mn = p^{v_p(m)+v_p(n)} m'n' \text{ donde } p \nmid m'n'.$$

Por tanto, $v_p(mn) = v_p(m) + v_p(n)$. □

Proposición 2.2. *La valuación $p-$ádica cumple las siguientes propiedades:*

1. *Para cualquier $x \in \mathbb{Q}$, el valor de $v_p(x)$ no depende de su representación como cociente de dos enteros.*
2. *$v_p(xy) = v_p(x) + v_p(y)$, para todo $x, y \in \mathbb{Q}$.*
3. *$v_p(x + y) \geq$ mín$\{v_p(x), v_p(y)\}$, para todo $x, y \in \mathbb{Q}$.*

Con la convención de que $x < +\infty$ para todo $x \in \mathbb{R}$ y $x + \infty = +\infty$.

Demostración. 1. Sea $x \in \mathbb{Q}$ tal que $x = \frac{a}{b} = \frac{c}{d}$ con $a, b, c, d \in \mathbb{Z}$. Se tiene que

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

Así, el valor de $v_p(x)$ no depende de su representación como cociente de dos enteros.

2. Para el caso en el que $x = 0$ o $y = 0$ la condición se cumple claramente. Sean $x, y \neq 0$ y además $x = \frac{a}{b}$ y $y = \frac{c}{d}$, se tiene

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

3. Para el caso en el que $x = 0$ o $y = 0$, las condición se cumple claramente. Sean $x, y \neq 0$ y además $x = \frac{a}{b}$ y $y = \frac{c}{d}$, por la observación anterior,

$$\begin{aligned} x + y &= p^{v_p(x)} \frac{a'}{b'} + p^{v_p(y)} \frac{c'}{d'}, \\ &= p^t \left(p^{v_p(x)-t} \frac{a'}{b'} + p^{v_p(y)-t} \frac{c'}{d'} \right), \end{aligned}$$

donde $t =$mín $\{v_p(x), v_p(y)\}$. La última igualdad implica que

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

□

Definición 2.2. *Para cualquier $x \in \mathbb{Q}$, se define el* ***valor absoluto p-ádico*** *de x como*

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

Proposición 2.3. *La función $|\cdot|_p$ definida anteriormente es un valor absoluto no arquimediano sobre $\mathbb{Q}$.*

Demostración. 1. Por definición $|x|_p = 0$ si y sólo si $x = 0$.

2. Sean $x, y \in \mathbb{Q}$, si alguno de ellos es cero entonces $|xy|_p = 0 = |x|_p |y|_p$.

   Para $x, y \neq 0$ se tiene

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

3. Sean $x, y \in \mathbb{Q}$, si alguno de ellos es cero entonces $|x+y|_p =$máx$\{|x|_p, |y|_p\}$.

   Para $x, y \neq 0$, sea $k :=$máx$\{-v_p(x), -v_p(y)\}$, luego $k = -$mín$\{v_p(x), v_p(y)\}$.

   Por la proposición anterior,

$$\begin{aligned} & v_p(x+y) &\geq& -k \\ \Longrightarrow & k &\geq& -v_p(x+y) \\ \Longrightarrow & p^k &\geq& p^{-v_p(x+y)}. \end{aligned}$$

   Así, máx$\{|x|_p, |y|_p\} \geq |x+y|_p$.

□

Propiedades

Algunas propiedades de los valores absolutos se enuncian en la siguiente proposición.

Proposición 2.4 (Proposition 1.6, [1])**.** *Sea $\Bbbk$ un campo y $|\cdot|$ un valor absoluto sobre $\Bbbk$, para todo $x, y \in \Bbbk$ se cumple:*

1. $|1| = |-1| = 1$,
2. $|x| = |-x|$,
3. $||x| - |y||_{\mathbb{R}} \leq |x \pm y|$,
4. $|x - y| \leq |x| + |y|$,
5. $|\frac{x}{y}| = \frac{|x|}{|y|}$ *donde* $y \neq 0$.

$|\cdot|_{\mathbb{R}}$ *denota el valor absoluto usual definido en* $\mathbb{R}$.

Demostración. 1.

$$|1| = |(1)(1)| = |1||1| \Longrightarrow |1| = 1.$$

   Por otro lado,

$$1 = |1| = |(-1)(-1)| = |-1||-1| = |-1|^2 \Longrightarrow |-1| = 1.$$

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

3. Se tiene

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

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

Por otro lado,

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

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

De (1) y (2) se obtiene

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

De la desigualdad anterior se sigue que

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

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

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

$\square$

La siguiente es un caracterización de los campos no arquimedianos.

Teorema 2.1. *Sea $A \subset \mathbb{k}$ la imagen de $\mathbb{Z}$ bajo la función $f : \mathbb{Z} \to \mathbb{k}$ definida de la siguiente manera*

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

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

Demostración. Sea $|\cdot|$ un valor absoluto no arquimediano sobre $\mathbb{k}$.

Se probará por inducción que $|f(n)| \leq 1$ para todo $n \in \mathbb{N}$.

Para $n = 1$ se tiene que $|f(1)| = |1| = 1$, así la proposición es válida para $n = 1$.
Supóngase que la proposición es válida para n, es decir, si $|f(n)| \leq 1$, entonces para $n + 1$ se tiene

$$|f(n + 1)| = |\underbrace{1 + 1 + \cdots + 1}_{n} + 1| \leq \max\{|f(n)|, 1\} = 1.$$

Así, $|f(n)| \leq 1$ para todo $n \in \mathbb{N}$.

Por propiedad, $|x| = |-x|$, si $n \in \mathbb{Z}$ y $n < 0$ entonces

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

Para $n = 0$, se cumple que $|f(0)| = 0 \leq 1$. Por tanto, $|a| \leq 1$ para todo $a \in A$.

Inversamente, sea $|\cdot|$ un valor absoluto sobre $\mathbb{k}$, tal que $|a| \leq 1$ para todo $a \in A$.
Se probará que $|x + y| \leq \max\{|x|, |y|\}$ para todo $x, y \in \mathbb{k}$.
Si $y = 0$ entonces se cumple que $|x + y| \leq \max\{|x|, |y|\}$ para cualquier $x \in \mathbb{k}$.
Si $y \neq 0$ entonces se cumple la siguiente equivalencia

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

Así, basta con probar que $|x+1| \leq \text{máx}\{|x|, 1\}$ para todo $x \in \Bbbk$.
Sea $x \in \Bbbk$, para m cualquier entero positivo se tiene

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

Luego,

$$\binom{m}{k} \in A \Longrightarrow \left|\binom{m}{k}\right| \leq 1,$$

implica

$$|x+1|^m \leq \sum_{k=0}^{m} |x|^k$$

Si $|x| \geq 1$ entonces $|x|^k \leq |x|^m$ para todo $k = 0, 1, \cdots, m$ y si $|x| < 1$ entonces $|x|^k < 1$ para todo $k = 0, 1, \cdots, m$. Así,

$$\sum_{k=0}^{m} |x|^k \leq (m+1)\text{máx}\{1, |x|^m\}$$

$$\Longrightarrow |x+1| \leq \sqrt[m]{m+1}\left(\text{máx}\{1, |x|\}\right).$$

Lo anterior se hizo sin importar el número m, es decir, la última desigualdad es válida $\forall m \in \mathbb{N}$.
Haciendo $m \longrightarrow \infty$ y usando $\text{lím}_{m\to\infty} \sqrt[m]{m+1} = 1$, se obtiene

$$|x+1| \leq \text{máx}\{|x|, 1\},$$

tal como se quería demostrar.

□

Ahora se puede justificar de alguna manera la diferencia entre un valor absoluto arquimediano y un valor absoluto no arquimediano.

Definición 2.3. *Un valor absoluto es* ***arquimediano*** *si tiene la siguiente propiedad:*

Dados $x, y \in \Bbbk$, $x \neq 0$, existe un entero positivo n tal que $|nx| > |y|$.

La propiedad anterior es conocida como la propiedad arquimediana. Esta propiedad se cumple para $\mathbb{Q}$ y $\mathbb{R}$ con el valor absoluto usual. Se puede ver que la propiedad arquimediana es equivalente a

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

Es decir, hay enteros arbitrariamente "grandes". Con esta caracterización, se observa que un valor absoluto no arquimediano no tiene la propiedad arquimediana.

Métrica inducida por un valor absoluto

Sea $\Bbbk$ un campo y $|\cdot|$ un valor absoluto sobre $\Bbbk$, se define la **distancia** $d(x, y)$ entre dos elementos $x, y \in \Bbbk$ como

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

La función $d(x, y)$ es llamada la **métrica inducida por el valor absoluto.**
El nombre de métrica está justificado por la siguiente proposición.

Proposición 2.5. *Sea $\Bbbk$ un campo y $|\cdot|$ un valor absoluto sobre $\Bbbk$, entonces la métrica inducida por el valor absoluto es efectivamente una métrica.*

Demostración. Para cualquier valor absoluto sobre $\Bbbk$ se cumple:

1. $d : \Bbbk \longrightarrow \mathbb{R}^+$.

2. $$d(x, y) = |x - y| \geq 0 \qquad \forall x, y \in \Bbbk.$$

   Además,

   $$d(x, y) = |x - y| = 0 \Leftrightarrow x - y = 0 \Leftrightarrow x = y.$$

3.
$$d(x,y)=|x-y|=|-(y-x)|=|y-x|=d(y,x) \qquad \forall x,y\in \Bbbk.$$

4.
$$\begin{aligned} d(x,y) &= |x-y| \\ &= |x-y+(z-z)| \\ &= |(x-z)+(z-y)| \\ &\leq |x-z|+|z-y| \\ &= d(x,z)+d(z,y) \qquad \forall x,y,z\in \Bbbk. \end{aligned}$$

De $1,2,3$ y 4 se concluye que la métrica inducida por el valor absoluto es una métrica.

□

Proposición 2.6. *La función valor absoluto, $|\cdot|:\Bbbk\to\mathbb{R}^+$, es continua.*

Demostración. Sea $x\in\Bbbk$ y $\epsilon>0$, si $|x-y|<\epsilon$ entonces

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

Así, $|\cdot|$ es continua en x.
Como $x\in\Bbbk$ se tomó de manera arbitraria se obtiene que $|\cdot|$ es continua. □

La siguiente proposición da una primera consecuencia de dotar a un campo con una topología inducida por un valor absoluto.

Proposición 2.7. *Sea $\Bbbk$ un campo con un valor absoluto $|\cdot|$. Las operaciones de suma, producto y tomar inversos son funciones continuas.*

Demostración.

1. Sean $x_0,y_0\in\Bbbk$ fijos. Para cualquier $\epsilon>0$, tomando $\delta=\frac{\epsilon}{2}$, se tiene que si

$$|x_0-x|<\delta \quad y \quad |y_0-y|<\delta$$

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

Por lo tanto, la suma es una función continua.

2. Sean $x_0,y_0\in\Bbbk$ fijos.
Para cualquier $\epsilon>0$, tomando $\delta=$mín$\{\frac{\epsilon}{2(|x_0|+1)},\frac{\epsilon}{2(|y_0|+1)},1\}$, se tiene que si

$$|x_0-x|<\delta \quad y \quad |y_0-y|<\delta,$$

entonces

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

Así,

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

Por tanto, el producto es una función continua.

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

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

En consecuencia, la operación de tomar inversos aditivos es continua.

4. Sea $x_0 \in \Bbbk \setminus \{0\}$ fijo. Para cualquier $\epsilon > 0$, tomando $\delta = \text{mín}\{\frac{|x_0|}{2}, \frac{\epsilon |x_0|^2}{2}\}$, se tiene que si

$$|x_0 - x| < \delta,$$

entonces

$$\begin{array}{rrcccc} & ||x| - |x_0||_{\mathbb{R}} & \leq & |x - x_0| & < & \frac{|x_0|}{2}, \\ \Longrightarrow & -\frac{|x_0|}{2} & < & |x| - |x_0| & < & \frac{|x_0|}{2}, \\ \Longrightarrow & \frac{|x_0|}{2} & < & |x| & < & \frac{3|x_0|}{2}, \\ \Longrightarrow & & & \frac{1}{|x|} & < & \frac{2}{|x_0|} \end{array}$$

Así,

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

Por tanto, la operación de tomar inversos multiplicativos es continua.

□

Proposición 2.8. *Sea $\Bbbk$ un campo y sea $|\cdot|$ un valor absoluto no arquimediano sobre $\Bbbk$. Si $x, y \in \Bbbk$ y $|x| \neq |y|$ entonces*

$$|x + y| = máx\{|x|, |y|\}.$$

Demostración. Sin pérdida de generalidad sea $|x| > |y|$. Se tiene que

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

Por otro lado,

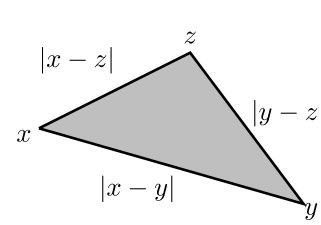
$$x = (x + y) - y \Longrightarrow |x| \leq \text{máx}\{|x + y|, |y|\},$$

como $|x| > |y|$, implica

$$\text{máx}\{|x + y|, |y|\} = |x + y| \Longrightarrow |x| \leq |x + y|. \qquad (**)$$

De $(*)$ y $(**)$ se obtiene $|x + y| = |x|$. □

Corolario 2.1. *En un campo con un valor absoluto no arquimediano $|\cdot|$, todos los "triángulos"son isósceles.*



Demostración. Sean x, y y z tres puntos del espacio (los vértices del triángulo). Las longitudes de los lados del triángulo son las tres distancias

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

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

Si $|x - y| = |y - z|$ el triángulo ya es isósceles.

Si $|x - y| \neq |y - z|$ entonces por la proposición anterior se obtiene

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

Así, todos los triángulos son isósceles. □

3. Valores Absolutos sobre $\mathbb{Q}$

El objetivo es caracterizar los valores absolutos sobre $\mathbb{Q}$, de acuerdo a la topología que generan. Dos valores absolutos $|\cdot|_1$ y $|\cdot|_2$ sobre un campo $\Bbbk$ se dicen **equivalentes** si definen la misma topología sobre $\Bbbk$.

Lema 3.1. *Sea $\Bbbk$ un campo y $|\cdot|$ un valor absoluto definido sobre él. Se tiene que*

$$\lim_{n\to\infty} x^n = 0 \Longleftrightarrow |x| < 1.$$

Demostración. Supóngase que $\lim_{n\to\infty} x^n = 0$ entonces para $\epsilon = 1$ existe $N \in \mathbb{N}$ tal que $|x^n - 0| = |x^n| = |x|^n < 1$.
para $n \geq N$.
Luego, $|x|^N < 1$. Esto implica que $|x| < 1$.

Recíprocamente, si $x = 0$ no hay nada que probar. Para $x \neq 0$, sea $\epsilon > 0$.
Como $|x| < 1$ entonces $\frac{1}{|x|} > 1$.
Luego, existe $h \in \mathbb{R}$ con $h > 0$ tal que $\frac{1}{|x|} = 1 + h$.
Por la desigualdad de Bernoulli se tiene

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

Por la propiedad Arquimediana existe $N \in \mathbb{N}$ tal que $Nh > \frac{1}{\epsilon} - 1$, es decir, $1 + Nh > \frac{1}{\epsilon}$.
Luego,

$$\frac{1}{|x|^N} > \frac{1}{\epsilon} \Longrightarrow \epsilon > |x|^N.$$

Así, para $n \geq N$ se tiene que $|x|^n < \epsilon$.
Por tanto, $\lim_{n\to\infty} x^n = 0$. □

Lema 3.2. *Sean $|\cdot|_1$ y $|\cdot|_2$ valores absolutos sobre un campo $\Bbbk$. Los siguientes enunciados son equivalentes:*

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

ii) *Para cualquier $x \in \Bbbk$ se tiene que $|x|_1 < 1$ si y sólo si $|x|_2 < 1$;*

iii) *Existe un número real positivo α tal que para cada $x \in \Bbbk$ se tiene*

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

Demostración. Para demostrar que *i)* implica *ii)*, sea $x \in \Bbbk$ tal que $|x|_1 < 1$, por el Lema 3.1 se tiene que $\lim_{n\to\infty} x^n = 0$ con $|\cdot|_1$.
Como los valores absolutos son equivalentes entonces todo abierto de $(\Bbbk, d_{|\cdot|_1})$ es un abierto en $(\Bbbk, d_{|\cdot|_2})$.
Así, $\lim_{n\to\infty} x^n = 0$ con $|\cdot|_2$ y por el lema anterior se obtiene $|x|_2 < 1$.
De manera análoga se prueba que si $|x|_2 < 1$ entonces $|x|_1 < 1$.

Para demostrar que *ii)* implica *iii)*, se distinguen dos casos. Si $|\cdot|_1$ es el valor absoluto trivial para $x \neq 0, 1$ se tiene que si $|x|_1 = 1$ entonces $|x|_2 = 1$, pues de lo contrario se obtiene que $|x|_1 \neq 1$ siendo una contradicción a que $|\cdot|_1$ es el valor absoluto trivial.

Si $|\cdot|_1$ no es el valor absoluto trivial entonces existe $x_0 \neq 0, 1$ tal que $|x_0|_1 < 1$.
Luego, $|x_0|_2 < 1$. Sea

$$\alpha = log_{|x_0|_2} |x_0|_1.$$

Con esto $|x_0|_1 = |x_0|_2^\alpha$.
Se tiene que $\alpha > 0$ pues de lo contrario se obtiene $|x_0|_1 \geq 1$, lo cual no es posible por que $|x_0|_1 < 1$.
Dado $x \in \Bbbk$, se tienen los siguientes casos:
Si $|x|_1 = 1$ entonces $|x|_2 = 1$ pues de lo contrario se obtiene que $|x|_1 \neq 1$ siendo una contradicción.
Así, $|x|_1 = |x|_2^\alpha$.

Si $|x|_1 = |x_0|_1$ entonces $|x|_2 = |x_0|_2$, por que si $|x|_2 < |x_0|_2$ entonces $|\frac{x}{x_0}|_2 < 1$ esto implica que $|\frac{x}{x_0}|_1 < 1$ y así $|x|_1 < |x_0|_1$, que es una contradicción a la suposición inicial. Análogamente se obtiene una contradicción al suponer $|x|_2 > |x_0|_2$.
Así, $|x|_1 = |x_0|_1 = |x_0|_2^\alpha = |x|_2^\alpha$.
Si $|x|_1 \neq 1$ y $|x|_1 \neq |x_0|_1$ entonces sea

$$S = \left\{ r = \frac{m}{n} : m, n \in \mathbb{N} \quad y \quad |x|_1^{\frac{m}{n}} < |x_0|_1 \right\}.$$

Se tiene

$$\frac{m}{n} \in S \Longleftrightarrow |x|_1^{\frac{m}{n}} < |x_0|_1 \Longleftrightarrow |x|_1^m < |x_0|_1^n \Longleftrightarrow \left| \frac{x^m}{x_0^n} \right|_1 < 1,$$

de ahí que $\left| \frac{x^m}{x_0^n} \right|_2 < 1$ implica que $|x|_2^m < |x_0|_2^n$, por lo anterior, $|x|_2^{\frac{m}{n}} < |x_0|_2$.
Así,

$$S = \left\{ r = \frac{m}{n} : m, n \in \mathbb{N} \quad y \quad |x|_2^{\frac{m}{n}} < |x_0|_2 \} = \{ r = \frac{m}{n} : m, n \in \mathbb{N} \quad y \quad |x|_1^{\frac{m}{n}} < |x_0|_1 \right\}.$$

Es decir,

$$S = \left\{ r = \frac{m}{n} : m, n \in \mathbb{N} \quad y \quad |x|_2 < |x_0|_2^{\frac{n}{m}} \} = \{ r = \frac{m}{n} : m, n \in \mathbb{N} \quad y \quad |x|_1 < |x_0|_1^{\frac{n}{m}} \right\}.$$

Sean

$$s = log_{|x_0|_1} |x|_1 \quad y \quad t = log_{|x_0|_2} |x|_2.$$

Se obtiene,

$$S = \left\{ r = \frac{m}{n} : m, n \in \mathbb{N} \quad y \quad s < \frac{1}{r} \right\} = \left\{ r = \frac{m}{n} : m, n \in \mathbb{N} \quad y \quad t < \frac{1}{r} \right\}.$$

Si $s \neq t$ se tiene que $s < t$ ó $t < s$.
Si $s < t$ entonces existe $p \in \mathbb{Q}$ tal que $s < p < t$, luego se tiene que $\frac{1}{p} \in S$ pues $s < \frac{1}{\frac{1}{p}} = p$. Por otro lado, $\frac{1}{p} \notin S$ pues $\frac{1}{\frac{1}{p}} = p < t$, luego $\frac{1}{p} \in S$ y $\frac{1}{p} \notin S$ con contradicción. Análogamente si $t < s$ se obtiene una contradicción, entonces $s = t$ y por lo tanto,

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

Para demostrar que *iii)* implica *i)*, sea $B_{|\cdot|_1}(x, r)$ una bola abierta en $(\mathbb{k}, d_{|\cdot|_1})$.
Como para cualquier $z \in \mathbb{k}$ se tiene que

$$|z|_1 = |z|_2^\alpha$$

con α un número real positivo.
Luego,

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

en consecuencia, $y \in B_{|\cdot|_2}(x, \sqrt[\alpha]{r})$.
Así, toda bola abierta en $(\mathbb{k}, d_{|\cdot|_1})$ es una bola abierta en $(\mathbb{k}, d_{|\cdot|_2})$. Por tanto, $|\cdot|_1$ y $|\cdot|_2$ son equivalentes. □

Los siguientes corolarios se obtienen como consecuencia inmediata del Lema 3.2.

Corolario 3.1. *En el campo de los números racionales, el valor absoluto usual no es equivalente a ningún valor absoluto $p-$ádico.*

Corolario 3.2. *En el campo de los números racionales, si p, q son primos distintos entonces $|\cdot|_p$ y $|\cdot|_q$ no son equivalentes.*

Lema 3.3. *Sea $|\cdot|$ un valor absoluto definido sobre $\mathbb{Q}$. Si se conoce $|n|$ para todo $n \in \mathbb{N}$ entonces se puede determinar $|x|$ para todo $x \in \mathbb{Q}$.*

Demostración. Por definición se tiene $|0| = 0$. Para n entero negativo se tiene que $-n \in \mathbb{N}$, entonces $|n| = |-n|$. Para cualquier $n \in \mathbb{Z} - \{0\}$ se tiene que $|\frac{1}{n}| = \frac{1}{|n|}$. Así, si $\frac{a}{b} \in \mathbb{Q}$ se tiene $|\frac{a}{b}| = |a||\frac{1}{b}| = \frac{|a|}{|b|}$. □

Lema 3.4. ***(Ostrowski)*** *Cada valor absoluto no trivial sobre $\mathbb{Q}$ es equivalente a uno de los valores absolutos $|\cdot|_p$, donde p es un número primo o $p=\infty$, recordando que $|\cdot|_\infty$ es el valor absoluto usual.*

Demostración. Sea $|\cdot|$ un valor absoluto no trivial sobre $\mathbb{Q}$, se distinguen dos casos:

1. Si $|\cdot|$ es arquimediano, sea n_0 el menor entero positivo para el cual $n_0>1$, existe tal entero por que de lo contrario $|\cdot|$ sería no arquimediano. Sea $\alpha = log_{n_0}|n_0|$, entonces $|n_0| = n_0^\alpha$. Se probará que $|x| = |x|_\infty^\alpha$ para todo $x\in\mathbb{Q}$, por el lema anterior basta con verificar esto para $n\in\mathbb{N}$. Sea $n\in\mathbb{N}$ escribiendo n en base n_0 se obtiene

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

con $0\le a_i\le n_0-1$ para $i=1,\cdots,k$ y $a_k\neq 0$.

Tomando valores absolutos se obtiene

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

como n_0 es el entero más pequeño cuyo valor absoluto es mayor que 1 se tiene que $|a_i|\le 1$ para $i=1,\cdots,k$. Luego,

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

Sea $C=\frac{n_0^\alpha}{n_0^\alpha-1}$. Se tiene que $C>0$. Entonces $|n|\le Cn_0^{k\alpha}\le Cn^\alpha$. Esta última desigualdad es válida para cada $n\in\mathbb{N}$, pues n se tomó de manera arbitraria.

Aplicando la desigualdad a un entero de la forma n^N se obtiene

$$|n^N|\le Cn^{N\alpha} \Longrightarrow |n|\le \sqrt[N]{C}n^\alpha,$$

haciendo que $N\longrightarrow\infty$ se obtiene $|n|\le n^\alpha$ pues $\lim_{N\to\infty}\sqrt[N]{C}=1$. Esta desigualdad, es válida para cualquier número natural n por ser n arbitrario.

Por otro lado, como $n_0^{k+1}>n\ge n_0^k$ se tiene

$$\begin{aligned}
n_0^{(k+1)\alpha} &= |n_0^{k+1}|, \\
&= |n + n_0^{k+1} - n|, \\
&\le |n| + |n_0^{k+1} - n|,
\end{aligned}$$

Luego $n_0^{(k+1)\alpha} - |n_0^{k+1}-n|\le |n|$, implica $n_0^{(k+1)\alpha} - (n_0^{k+1}-n)^\alpha\le|n|$. Ahora como $n\ge n_0^k$ se obtiene

$$\begin{aligned}
|n| &\ge n_0^{(k+1)\alpha} - (n_0^{k+1} - n_0^k)^\alpha, \\
&= n_0^{(k+1)\alpha}\left(1 - \left(1 - \frac{1}{n_0}\right)^\alpha\right), \\
&= C' n_0^{(k+1)\alpha}, \\
&> C' n^\alpha,
\end{aligned}$$

donde $C' = 1-(1-\frac{1}{n_0})^\alpha > 0$ y no depende de n.

Aplicando la desigualdad a n^N se obtiene

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

haciendo que $N \longrightarrow \infty$ se obtiene $|n| \geq n^{\alpha}$ pues $\lim_{N\to\infty} \sqrt[N]{C'} = 1$. Así, $|n| = n^{\alpha}$. Por tanto, $|n| = |n|_{\infty}^{\alpha}$ para todo $n \in \mathbb{N}$, tal como se quería probar.

2. Si $|\cdot|$ es no arquimediano se tiene que $|n| \leq 1$ para todo $n \in \mathbb{Z}$. Luego, por ser $|\cdot|$ distinto del trivial, al menos para un $m \in \mathbb{Z}$ se tiene que $|m| < 1$.

   Sea n_0 el menor número natural para el que $|n_0| < 1$, n_0 es primo, por que de lo contrario existen enteros a, b tales que $1 < a, b < n_0$ y $n_0 = ab$, por la elección de n_0 se tiene que $|a| = |b| = 1$ y así $|n_0| = 1$, contradiciendo el hecho de que $|n_0| < 1$.

   Sea entonces $n_0 = p$. Se probará que $|x| = |x|_p^{\alpha}$ para todo $x \in \mathbb{Q}$, por el lema anterior basta con mostrar esto para $n \in \mathbb{N}$.

   Sean $n \in \mathbb{N}$ y $\alpha = log_{\frac{1}{p}}|p|$. Si $p \nmid n$ entonces $n = pq + r$ donde $0 < r < p$, por la elección de p se tiene que $|r| = 1$.

   Además, $|pq| < 1$ pues $|p| < 1$ y $|q| \leq 1$. Esto implica que $|n| =$máx$\{|pq|, |r|\} = 1$, esto último es consecuencia de la Proposición 2.8.

   Por otro lado, para n tal que $p|n$ se tiene que $n = p^v n'$ con $p \nmid n'$. Entonces

$$|n| = |p|^v |n'| = |p|^v = \left(\frac{1}{p}\right)^{v\alpha} = |n|_p^{\alpha}.$$

   Por tanto, $|\cdot|$ es equivalente a $|\cdot|_p$.

□

Este teorema dice que si se quiere estudiar $\mathbb{Q}$ con algún valor absoluto no trivial, esencialmente sólo se tienen dos opciones: el valor absoluto trivial y algún valor absoluto p-ádico.

Completaciones

El objetivo es obtener el campo de los números $p-$ádicos, $\mathbb{Q}_p$, mediante un proceso de completación al campo de los números racionales $\mathbb{Q}$.

4. Sucesión de Cauchy

Sea $\mathbb{k}$ un campo y sea $|\cdot|$ un valor absoluto sobre $\mathbb{k}$.

1. Una sucesión de elementos de $\mathbb{k}$, $\{x_n\}$, es llamada una **sucesión de Cauchy** si para cada $\epsilon > 0$ existe $M \in \mathbb{N}$ tal que $|x_n - x_m| < \epsilon$ siempre que $n, m \geq M$.

2. El campo $\mathbb{k}$ es llamado **completo con respecto a** $|\cdot|$ si cada sucesión de Cauchy de elementos de $\mathbb{k}$ tiene un límite en $\mathbb{k}$.

Lema 4.1. *Una sucesión $\{x_n\}$ de números racionales es una sucesión de Cauchy con respecto a un valor absoluto no arquimediano $|\cdot|$ si y sólo si se tiene*

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

Demostración. Sea $\epsilon > 0$, por ser $\{x_n\}$ sucesión de Cauchy existe $N \in \mathbb{N}$ tal que si $m, n \geq N$, entonces $|x_n - x_m| < \epsilon$. En particular, si $n \geq N$ entonces $|x_{n+1} - x_n| < \epsilon$. Así,

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

Recíprocamente, sea $\epsilon > 0$, como $\lim_{n\to\infty} |x_{n+1} - x_n| = 0$ existe $N \in \mathbb{N}$ tal que si $n \geq N$ entonces $|x_{n+1} - x_n| < \epsilon$.
Sean $n, m \geq N$, sin pérdida de generalidad se considera $m > n$, entonces $m = n + r$. Luego,

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

Así, $\{x_n\}$ es una sucesión de Cauchy. □

Teorema 4.1. *El campo $\mathbb{Q}$ de números racionales no es completo con respecto a cualquiera de los valores absolutos no triviales.*

Demostración. Por el Lema de Ostrowski (Lema 4) es suficiente probar esto para los valores absolutos $|\cdot|_p$, donde p es un número primo ó $p = \infty$.
Es bien sabido que $\mathbb{Q}$ no es completo con $|\cdot|_\infty$, entonces solamente se analiza el caso cuando p es un número primo.

Sea $\mathbb{Q}$ con el valor absoluto $|\cdot|_p$, donde p es un número primo fijo. Considérese la sucesión

$$a_n = 1 + p + p^2 + p^3 + \cdots + p^n.$$

Se tiene que la sucesión (a_n) es de Cauchy, pues

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

Además, a_n converge al número $1 + p + p^2 + p^3 + \cdots + p^n + \cdots$.
Si $1 + p + p^2 + p^3 + \cdots + p^n + \cdots$ es un número racional s, se tiene que

$$s = 1 + p + p^2 + p^3 + \cdots + p^n + \cdots = 1 + p(1 + p + p^2 + p^3 + \cdots + p^n + \cdots) = 1 + ps.$$

Es decir, s es igual a un número mayor que el, lo que es una contradicción. Así, $1 + p + p^2 + p^3 + \cdots + p^n + \cdots$ no es un número racional.
Por tanto, $\mathbb{Q}$ con el valor absoluto $|\cdot|_p$ no es completo. □

Definición 4.1. *Sea $|\cdot| = |\cdot|_p$ un valor absoluto no arquimediano sobre $\mathbb{Q}$. Se denota por $\mathcal{C}$ o $\mathcal{C}_p(\mathbb{Q})$, el conjunto de todas las sucesiones de Cauchy de elementos de $\mathbb{Q}$ con respecto a $|\cdot|_p$, es decir,*

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

Proposición 4.1. *Definiendo*

$$
\begin{aligned}
(x_n) + (y_n) &= (x_n + y_n), \\
(x_n) \cdot (y_n) &= (x_n y_n), \\
0 &= (0) \quad y \\
1 &= (1).
\end{aligned}
$$

Se tiene que $\mathcal{C}$ es una anillo conmutativo con unidad.

Demostración. Para ver que la suma es cerrada en $\mathcal{C}$ sean $(x_n), (y_n) \in \mathcal{C}$ y $\epsilon > 0$, existen $N_1, N_2 \in \mathbb{N}$ tal que si $n, m \geq N_1$ entonces $|x_n - x_m| < \epsilon$ y si $m, n \geq N_2$ entonces $|y_n - y_m| < \epsilon$. Sea $N =$máx$\{N_1, N_2\}$. Si $n, m \geq N$ entonces

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

Así, $(x_n + y_n) \in \mathcal{C}$.
Para probar que el producto es cerrado en $\mathcal{C}$ primero se verá que toda sucesión de Cauchy es acotada. Sea (x_n) una sucesión de Cauchy, para $\epsilon = 1$ existe $N \in \mathbb{N}$ tal que si $n, m \geq N$ entonces $|x_n - x_m| < 1$. En particular $|x_n - x_N| < 1$ si $n > N$, entonces

$$||x_n| - |x|_N|_{\mathbb{R}} \leq |x_n - x_N| < 1$$

Luego, $-1 < |x_n| - |x_N| < 1$ si $n > N$. Esto implica que $|x_n| < |x_N| + 1$ si $n > N$.
Sea $k =$máx$\{|x_1|, |x_2|, \cdots, |x_N|, |x_N| + 1\}$. Se tiene que $|x_n| \leq k$ para todo $n \in \mathbb{N}$. Así, la sucesión (x_n) está acotada. Se probará ahora que el producto es cerrado.
Sean $(x_n), (y_n) \in \mathcal{C}$ y $\epsilon > 0$, por lo anterior existen $k_1, k_2 \in \mathbb{R}$ mayores que cero, tal que $|x_n| < k_1$ y $|y_n| < k_2$ para todo $n \in \mathbb{N}$.
Sea $k =$máx$\{k_1, k_2\}$. Para $\frac{\epsilon}{k}$ existen $N_1, N_2 \in \mathbb{N}$ tal que si $n, m \geq N_1$ entonces $|x_n - x_m| < \frac{\epsilon}{k}$ y si $m, n \geq N_2$ entonces $|y_n - y_m| < \frac{\epsilon}{k}$. Sea $N =$máx$\{N_1, N_2\}$. Si $n, m \geq N$ entonces

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

Así, $(x_n y_n) \in \mathcal{C}$.
Las propiedades de Anillo se heredan por ser $\mathbb{Q}$ un campo y de la definición de las operaciones, también comprobar que el elemento neutro es $0 = (0)$ y el elemento unidad es $1 = (1)$ se sigue de la definición de las operaciones. □

Lema 4.2. *La función $f : \mathbb{Q} \longrightarrow \mathcal{C}$ definida por $f(x) = (x)$ es una inclusión de $\mathbb{Q}$ en $\mathcal{C}$.*

Demostración. La función está bien definida y es inyectiva pues

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

Además es un morfismo de anillos, pues $f(x + y) = (x + y) = (x) + (y) = f(x) + f(y)$, $f(1) = (1)$ y $f(xy) = (xy) = (x) \cdot (y) = f(x) \cdot f(y)$. □

Definición 4.2. *Se define $\mathcal{N} \subset \mathcal{C}$ como el conjunto*

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

es decir, el conjunto de sucesiones que convergen a cero con respecto al valor absoluto $|\cdot|_p$.

Proposición 4.2. *$\mathcal{N}$ es un ideal en $\mathcal{C}$.*

Demostración. Se tiene,

1. $(0) \in \mathcal{N}$ pues $\lim_{n\to 0} |0|_p = 0$.
2. Si $(x_n), (y_n) \in \mathcal{N}$ para $\epsilon > 0$ existen N_1, N_2 tal que si $n \geq N_1$ y $m \geq N_2$ entonces

   $$|x_n|_p < \epsilon \quad y \quad |x_m|_p < \epsilon.$$

   Sea $N =$máx$\{N_1, N_2\}$. Para $n \geq N$ se tiene $|x_n + y_n|_p \leq$máx$\{|x_n|_p, |y_n|_p\} < \epsilon$

   $$\Longrightarrow \lim_{n\to\infty} x_n + y_n = 0.$$

   Así, $(x_n) + (y_n) \in \mathcal{N}$.
3. Sea $(y_n) \in \mathcal{C}$ y $(x_n) \in \mathcal{N}$, se tiene $(x_n)(y_n) = (x_n y_n)$, luego $|x_n y_n|_p = |x_n|_p |y_n|_p$, como $(y_n) \in \mathcal{C}$ entonces existe $k \in \mathbb{R}$ tal que $|y_n|_p \leq k$ para todo $n \in \mathbb{N}$.

   Luego,

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

   Así, $(x_n)(y_n) \in \mathcal{N}$.

$\square$

Lema 4.3. *La función $f : \mathbb{Q} \longrightarrow \mathcal{C}$ definida por $f(x) = (x)$ es una inclusión de $\mathbb{Q}$ en $\mathcal{C}$. Si (x_n) es una sucesión de Cauchy tal que $x_n \nrightarrow 0$ entonces existen $c > 0$ y $N \in \mathbb{N}$ tal que $|x_n|_p > c$, para $n \geq N$.*

Demostración. Puesto que $x_n \nrightarrow 0$ existe $\epsilon > 0$ tal que para todo $M \in \mathbb{N}$ se cumple $|x_k|_p > \epsilon$ para algún $k \geq M$.
Para este $\epsilon > 0$ existe $N' \in \mathbb{N}$ tal que si $m, n \geq N'$ entonces $|x_n - x_m|_p < \epsilon$. Sea $N \in \mathbb{N}$ tal que $|x_N|_p > \epsilon$ y $N \geq N'$. Para cualquier $n \geq N$ se tiene

$$\begin{aligned} & |x_n - x_N|_p < \epsilon, \\ \Longrightarrow\ & ||x_n| - |x_N||_{\mathbb{R}} \leq |x_n - x_N|_p < \epsilon, \\ \Longrightarrow\ & -\epsilon < |x_n|_p - |x_N|_p < \epsilon, \\ \Longrightarrow\ & |x_N|_p - \epsilon < |x_n|_p. \end{aligned}$$

Poniendo $c = |x_N|_p - \epsilon$ se cumple que $|x_n|_p > c > 0$, para todo $n \geq N$. $\square$

Proposición 4.3. *$\mathcal{N}$ es un ideal maximal en $\mathcal{C}$.*

Demostración. Sea I un ideal de $\mathcal{C}$ tal que $\mathcal{N} \subset I$ y $\mathcal{N} \neq I$, se probará que $I = \mathcal{C}$.
Como $I \neq \mathcal{N}$ existe $(x_n) \in I$ tal que $x_n \nrightarrow 0$, usando además, que (x_n) es una sucesión de Cauchy, por el Lema 4.3 existen $c > 0$ y $N \in \mathbb{N}$ tal que si $n \geq N$ entonces $|x_n|_p > c$. Se define (y_n) como

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

Se tiene

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

La sucesión (x_n) es de Cauchy y por Lema 5, se tiene $\lim_{n\to\infty} |x_{n+1} - x_n|_p = 0$,

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

Entonces por Lema 5, se obtiene que (y_n) es sucesión de Cauchy.
Luego, $(x_n)(y_n) \in I$ por ser I un ideal de $\mathcal{C}$.
Por otro lado,

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

Entonces $1 - (x_n y_n) \in \mathcal{N}$, sea $(z_n) = 1 - (x_n y_n)$. Luego, $1 = (x_n y_n) + (z_n) \in I$ pues $(z_n), (x_n y_n) \in I$.
Así, $I = \mathcal{C}$ y por tanto $\mathcal{N}$ es maximal en $\mathcal{C}$. $\square$

Definición 4.3. *Se define el* ***campo de los números** $p-$**ádicos*** *como el campo*

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

Observación 1 La inclusión natural de los números racionales $\mathbb{Q}$ en $\mathbb{Q}_p$, $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$, es la función que a

cada $x \in \mathbb{Q}$ le asigna la clase de equivalencia de la sucesión constante (x), esto porque dos sucesiones constantes nunca difieren por un elemento de $\mathcal{N}$.
Para extender el valor absoluto al campo $\mathbb{Q}_p$, se mostrará primero un hecho de las sucesiones de Cauchy.

Lema 4.4. *Sea $(x_n) \in \mathcal{C}$, $(x_n) \notin \mathcal{N}$. La sucesión de números reales es eventualmente estacionaria, es decir, existe un entero N tal que $|x_n|_p = |x_m|_p$ si $m, n \geq N$.*

Demostración. Como (x_n) es una sucesión de Cauchy que no tiende a cero, por el Lema 5 existen $c > 0$ y $N_1 \in \mathbb{N}$ tal que

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

Por otro lado, existe $N_2 \in \mathbb{N}$ tal que

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

Sea $N =$máx$\{N_1, N_2\}$ si $n, m \geq N$ entonces

$$|x_n - x_m|_p < c \leq |x_n|_p \quad y \quad |x_n - x_m|_p < c \leq |x_m|_p.$$

Luego, si $n, m \geq N$ entonces $|x_n - x_m|_p \leqslant$máx$\{|x_n|_p, |x_m|_p\}$.
Como todos los triángulos son isósceles, se obtiene $|x_n|_p = |x_m|_p$ si $n, m \geq N$. □

Definición 4.4. *Si $\lambda \in \mathbb{Q}_p$ y (x_n) es cualquier sucesión de Cauchy representante de λ, se define*

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

Observación 2

Abusando de notación, se suele usar el mismo símbolo $(|\cdot|_p)$ para representar al valor absoluto $p-$ádico sobre $\mathbb{Q}$ y $\mathbb{Q}_p$, porque después solamente se trabajará con $\mathbb{Q}_p$.

Proposición 4.4. *El límite de la definición anterior está bien definido.*

Demostración. Se tiene,

1. El límite existe pues por el lema anterior existe $N \in \mathbb{N}$ tal que
   $|x_n|_p = |x_m|_p$ si $m, n \geq N$. Así, $\lim_{n\to\infty} |x_n|_p = |x_N|_p$.

2. El límite no depende de la elección de la sucesión representante de λ, pues si (x_n) y (y_n) son representantes de λ entonces $(x_n) - (y_n) = (x_n - y_n) \in \mathcal{N}$.
   Sea $\epsilon > 0$, existe $N \in \mathbb{N}$ tal que si $n \geq N$ entonces $|x_n - y_n|_p < \epsilon$. De donde

$$||x_n|_p - |y_n|_p|_{\mathbb{R}} \leq |x_n - y_n|_p < \epsilon \Longrightarrow ||x_n|_p - |y_n|_p|_{\mathbb{R}} < \epsilon$$

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

□

Proposición 4.5. *La función $|\cdot|_p : \mathbb{Q}_p \longrightarrow \mathbb{R}^+$, definida anteriormente es un valor absoluto no arquimediano.*

Demostración. Se tiene,

1. Si $|\lambda|_p = 0$ entonces $\lim_{n\to\infty} |x_n|_p = 0$ para toda sucesión representante de la clase λ. Entonces $(x_n) \in \mathcal{N}$, es decir, $\lambda = 0$.
   Por otro lado, si $\lambda = 0$ entonces para algún representante (x_n) de λ se tiene que $\lim_{n\to\infty} |x_n|_p = 0$, así $|\lambda|_p = 0$.

2. Se tiene,

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

3. Por el Lema 4.4 existen naturales N_1, N_2 y N_3 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 $N =$máx$\{N_1, N_2, N_3\}$, entonces $|\lambda + \beta|_p = \text{lím}_{n\to\infty}|x_n + y_n|_p = |x_N + y_N|_p$,
   $|\lambda|_p = \text{lím}_{n\to\infty}|x_n|_p = |x_N|_p$ y $|\beta|_p = \text{lím}_{n\to\infty}|y_n|_p = |y_N|_p$.
   Usando la desigualdad $|x_N + y_N|_p \leq$máx$\{|x_N|_p, |y_N|_p\}$ se obtiene
   $|\lambda + \beta|_p \leq$máx $\{|\lambda|_p, |\beta|_p\}$.

De $1, 2$ y 3 se concluye que $|\cdot|_p$ es un valor absoluto no arquimediano. □

Observación 3 De la definición se puede observar que la imagen de $\mathbb{Q}$ bajo $|\cdot|_p$ es igual a la imagen de $\mathbb{Q}_p$ bajo $|\cdot|_p$.
Además, si $x \in \mathbb{Q}$ y λ_x es su imagen bajo la inclusión, por la definición se obtiene que $|x|_p = |\lambda_x|_p$.

Proposición 4.6. *La imagen de $\mathbb{Q}$ bajo la inclusión $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ es un subconjunto denso en $\mathbb{Q}_p$.*

Demostración. Sean $\epsilon > 0$ y $\lambda \in \mathbb{Q}_p$. Se construirá una sucesión constante que esta contenida en $B(\lambda, \epsilon)$.
Sea (x_n) una sucesión de Cauchy representante de λ y sea $\epsilon' > 0$ tal que $\epsilon' < \epsilon$.
Como (x_n) es de Cauchy existe $N \in \mathbb{N}$ tal que si $m, n \geq N$ entonces $|x_n - x_m| < \epsilon'$. Sea $y = x_N$, se construye la sucesión constante (y).
Si $\beta \in \mathbb{Q}_p$ es representada por (y), se tiene que β es la imagen de $y \in \mathbb{Q}$ bajo la inclusión. Luego, $\lambda - \beta$ es representada por la sucesión $(x_n - y)$ y entonces

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

Para $n \geq N$ se tiene $|x_n - y| = |x_n - x_N| < \epsilon'$.
Así,

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

Por tanto, $\beta \in B(\lambda, \epsilon)$. □

Proposición 4.7. *$\mathbb{Q}_p$ es completo con respecto a $|\cdot|_p$.*

Demostración. Sea (λ_n) una sucesión de Cauchy de elementos de $\mathbb{Q}_p$.
Por la proposición anterior, para cada $i \in \mathbb{N}$ existe β_i que es clase de equivalencia de una sucesión constante de números racionales (y_i) y satisface

$$|\lambda_i - \beta_i|_p < \frac{1}{i}.$$

Sea $z_i = y_i$ para todo $i \in \mathbb{N}$.
Se tiene que (z_i) es una sucesión de números racionales, se probará que es sucesión de Cauchy.
Sea $\epsilon > 0$, existe $k \in \mathbb{N}$ tal que $\frac{1}{k} < \epsilon$, luego por ser (λ_n) sucesión de Cauchy existe $N \in \mathbb{N}$ tal que si $n, m \geq N$ entonces $|\lambda_n - \lambda_m|_p < \frac{1}{k}$.
Sea $N' =$máx$\{k, N\}$, usando que $\beta_n - \beta_m$ es la clase de equivalencia de la sucesión constante $(z_n - z_m) = (x_t)$, si $n, m \geq N'$ se obtiene

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

Así, (z_n) es sucesión de Cauchy en $\mathbb{Q}$. Sea λ la clase de equivalencia de (z_n) en $\mathbb{Q}_p$, se probará que $\text{lím}_{n\to\infty} \lambda_n = \lambda$.
Sea $\epsilon > 0$, existe $k \in \mathbb{N}$ tal que $\frac{1}{k} < \epsilon$. Como $(z_n) = (y_n)$ es sucesión de Cauchy en $\mathbb{Q}$, existe $N \in \mathbb{N}$ tal que si $m, n \geq N$ entonces $|y_m - y_n|_p < \frac{1}{k}$.
Sea $N' =$máx$\{k, N\}$, si $n \geq N'$ se tiene

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

como $n > k$ se cumple $|\lambda_n - \beta_n|_p < \frac{1}{n} < \frac{1}{k}$, además $|\beta_n - \lambda|_p = \text{lím}_{m\to\infty} |z_n - z_m|_p \leq \frac{1}{k}$ pues si $m, n \geq N$ entonces $|y_m - y_n|_p < \frac{1}{k}$. Entonces,

$$|\lambda_n - \lambda|_p < \frac{1}{k} < \epsilon.$$

Así, $\text{lím}_{n\to\infty} \lambda_n = \lambda$. Por tanto, $\mathbb{Q}_p$ es completo. $\square$

El siguiente teorema es muy importante, dado que resume todo el trabajo realizado.

Teorema 4.2. *Para cada primo $p \in \mathbb{Z}$ existe un campo $\mathbb{Q}_p$ con un valor absoluto no arquimediano $|\cdot|_p$, tal que:*

1. *Existe una inclusión $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$, y el valor absoluto inducido por $|\cdot|_p$ sobre $\mathbb{Q}$ vía esta inclusión es un valor absoluto $p-$ádico.*

2. *La imagen de $\mathbb{Q}$ bajo esta inclusión es densa en $\mathbb{Q}_p$ (con respecto al valor absoluto $|\cdot|_p$); y*

3. *$\mathbb{Q}_p$ es completo con respecto al valor absoluto $|\cdot|_p$.*

El campo $\mathbb{Q}_p$ que satisface $1, 2$ y 3 es único salvo isomorfismos que preservan valores absolutos.

Demostración. Los incisos $1, 2$ y 3 fueron probados en las proposiciones previas al teorema.
Resta ver la unicidad. Sea K un campo que satisface las condiciones $1, 2$ y 3 del teorema, entonces existe una inclusión h de $\mathbb{Q}$ en K tal que la imagen de $\mathbb{Q}$ es densa en K con respecto al valor absoluto $|\cdot|_p$.
Sea g la inclusión de $\mathbb{Q}$ en $\mathbb{Q}_p$, entonces se forma la función $f : \mathbb{Q}_p \to K$ de la siguiente manera: si $\lambda \in \mathbb{Q}_p$ entonces por la densidad de $g(\mathbb{Q})$ existe una sucesión (z_n) tal que $z_n \to \lambda$ y $z_n = g(z'_n)$ donde $z'_n \in \mathbb{Q}$ para todo $n \in \mathbb{N}$.
El valor absoluto se mantiene igual en $\mathbb{Q}$ y en $g(\mathbb{Q})$ entonces (z'_n) es sucesión de Cauchy en $\mathbb{Q}$ y luego $(h(z'_n))$ es sucesión de Cauchy en K, pues el valor absoluto se mantiene igual en K y en $h(K)$.
Como K es completo existe $k \in K$ tal que $k = \text{lím}_{n\to\infty} h(z'_n)$. Definiendo $f(\lambda) = k$, se tiene

1. f está bien definida y es inyectiva: sean $(z_n), (y_n) \subset g(\mathbb{Q})$ tal que $\text{lím}_{n\to\infty} z_n = \lambda = \text{lím}_{n\to\infty} y_n$. Entonces $z_n = g(z'_n)$ y $y_n = g(y'_n)$ con $z'_n, y'_n \in \mathbb{Q}$ implica

$$\lim_{n\to\infty} z_n = \lambda = \lim_{n\to\infty} y_n \Longleftrightarrow \lim_{n\to\infty} z_n - y_n = 0,$$

si y sólo si

$$\lim_{n\to\infty} |g(z'_n) - g(y'_n)|_p = 0 \Longleftrightarrow \lim_{n\to\infty} |g(z'_n) - g(y'_n)|_K = 0,$$

equivalente a

$$\lim_{n\to\infty} h(z'_n) - h(y'_n) = 0 \Longleftrightarrow \lim_{n\to\infty} h(z'_n) = \lim_{n\to\infty} h(y'_n).$$

2. f es sobreyectiva. En efecto, sea $w \in K$, existe $(w_n) \subset h(\mathbb{Q})$ tal que $\lim_{n\to\infty} w_n = w$ y $w_n = h(w'_n)$ donde $w'_n \in \mathbb{Q}$ para todo $n \in \mathbb{N}$.

   Se tiene (w'_n) es sucesión de Cauchy en $\mathbb{Q}$ entonces $(g(w'_n))$ es sucesión de Cauchy en $\mathbb{Q}_p$. Sea $\lambda \in \mathbb{Q}_p$ tal que $\lim_{n\to\infty} g(w'_n) = \lambda$ entonces $f(\lambda) = w$.

3. Ahora se probará que f es morfismo. Por definición se tiene $f(1) = 1^*$ donde 1^* es la unidad en K.

   Luego, sean $x, y \in \mathbb{Q}_p$, existen $(g(x'_n)), g((y'_n))$ tal que

$$\lim_{n\to\infty} g(x'_n) = x \qquad \lim_{n\to\infty} g(y'_n) = y.$$

   Además,

$$\lim_{n\to\infty} h(x'_n) = f(x) \qquad \lim_{n\to\infty} h(y'_n) = f(y).$$

   Se tiene,

$$f(x) + f(y) = \lim_{n\to\infty} h(x'_n) + \lim_{n\to\infty} h(y'_n) = \lim_{n\to\infty} h(x'_n) + h(y'_n).$$

   Por otro lado,

$$\lim_{n\to\infty} g(x'_n) + g(y'_n) = x + y \Longrightarrow \lim_{n\to\infty} h(x'_n) + h(y'_n) = f(x) + f(y).$$

   Así, $f(x+y) = f(x) + f(y)$. Por tanto, f es morfismo.

   De manera análoga se obtiene $f(xy) = f(x)f(y)$.

De $1, 2$ y 3 se concluye que f es un isomorfismo. Para ver que f preserva valores absolutos, sea $\lambda \in \mathbb{Q}_p$ entonces existe (z_n) tal que $z_n \to \lambda$ y $z_n = g(z'_n)$ donde $z'_n \in \mathbb{Q}$ para todo $n \in \mathbb{N}$.
Se tiene

$$|\lambda|_p = \lim_{n\to\infty} |z_n|_p = \lim_{n\to\infty} |h(z'_n)|_K,$$

como $|\cdot|_K$ es continua entonces $\lim_{n\to\infty} |h(z'_n)|_K = |f(\lambda)|_K$.
Así, $|\lambda|_p = |f(\lambda)|_K$. □

El teorema anterior permite fijar la atención solamente en los elementos de $\mathbb{Q}_p$ y considerar a $\mathbb{Q}$ como un subconjunto de $\mathbb{Q}_p$, exactamente igual a como se trabaja en $\mathbb{R}$.

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

Hasta el momento se construyó para cada número primo p, el campo de los números $p-$ádicos $(\mathbb{Q}_p)$, a manera de resumen se presentan los siguientes hechos:

1. Hay un valor absoluto no arquimediano, $|\cdot|_p$, sobre $\mathbb{Q}_p$ y $\mathbb{Q}_p$ es completo respecto a este valor absoluto.

2. Existe una inclusión $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ cuya imagen es densa en $\mathbb{Q}_p$ y la restricción del valor absoluto $|\cdot|_p$ a la imagen de $\mathbb{Q}$ coincide con el valor absoluto $p-$ádico definido en $\mathbb{Q}$.

3. El conjunto de valores de $\mathbb{Q}$ y $\mathbb{Q}_p$ bajo $|\cdot|_p$ es el mismo, específicamente,

$$\begin{aligned} \{x \in \mathbb{R}^+ : x = |\lambda|_p, \lambda \in \mathbb{Q}\} &= \{x \in \mathbb{R}^+ : x = |\lambda|_p, \lambda \in \mathbb{Q}_p\} \\ &= \{p^n : n \in \mathbb{Z}\} \cup \{0\}. \end{aligned}$$

4. Como consecuencia del inciso anterior se tiene que para cada $x \in \mathbb{Q}_p$, $x \neq 0$, existe un entero $v_p(x)$ tal que $|x|_p = p^{-v_p(x)}$. En otras palabras, la valuación $p-$ádica se extiende a $\mathbb{Q}_p$.

Definición 5.1. *El* ***anillo de enteros*** $p-$***ádicos*** *es el conjunto*

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

Observación 4

Las unidades de $\mathbb{Z}_p$ son aquéllos elementos $x \in \mathbb{Z}_p$ tales que $|x|_p = 1$.

Definición 5.2. *El anillo $\mathbb{Z}_p$ de enteros p−ádicos es un anillo local cuyo ideal maximal es el ideal principal $p\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq \frac{1}{p}\}$. Además, cada elemento del complemento $\mathbb{Z}_p - p\mathbb{Z}_p$ es invertible en $\mathbb{Z}_p$, siendo los únicos elementos invertibles en $\mathbb{Z}_p$.*

Demostración.

1. Para probar que $\mathbb{Z}_p$ es subanillo de $\mathbb{Q}_p$, hay que observar lo siguiente:

    a) Sean $x, y \in \mathbb{Z}_p$ entonces $|x|_p \leq 1$ y $|y|_p \leq 1$.
    Luego, $|x-y|_p \leq$máx$\{|x|_p, |-y|_p\}$ =máx$\{|x|_p, |y|_p\} \leq 1$. Así, $x - y \in \mathbb{Z}_p$.

    b) Sean $x, y \in \mathbb{Z}_p$ entonces $|xy|_p = |x|_p|y|_p \leq 1$. Así, $xy \in \mathbb{Z}_p$.

    c) $1 \in \mathbb{Z}_p$ pues $|1|_p = 1 \leq 1$.

    De $a), b)$ y $c)$ se obtiene que $\mathbb{Z}_p$ es subanillo de $\mathbb{Q}_p$.

2. Para probar que $p\mathbb{Z}_p$ es ideal de $\mathbb{Z}_p$, hay que observar lo siguiente:

    a) $0 \in p\mathbb{Z}_p$ pues $|0|_p = 0 \leq \frac{1}{p}$.

    b) Sean $x, y \in p\mathbb{Z}_p$ entonces $|x|_p \leq \frac{1}{p}$ y $|y|_p \leq \frac{1}{p}$.
    Se tiene que $|x-y|_p \leq$máx $\{|x|_p, |y|_p\} \leq \frac{1}{p}$.
    Por tanto, $(p\mathbb{Z}_p\ , +)$ es subrgrupo de $(\mathbb{Z}_p\ , +)$.

    c) Sean $r \in \mathbb{Z}_p$ y $x \in p\mathbb{Z}_p$. Se tiene

    $$|r|_p \leq 1 \Longrightarrow |rx|_p = |r|_p|x|_p \leq |x|_p \leq \frac{1}{p}.$$

    Así, $rx \in p\mathbb{Z}_p$.

    De $a)$, $b)$ y $c)$ se obtiene que $p\mathbb{Z}_p$ es un ideal de $\mathbb{Z}_p$.

3. Sea I ideal de $\mathbb{Z}_p$, se tiene que $I \subset \mathbb{Z}_p$. Si existe $z \in I$ tal que $z \notin p\mathbb{Z}_p$, entonces $|z|_p = 1$.
    Luego, la igualdad $|1|_p = |z|_p|z^{-1}|_p$ implica que $|z^{-1}|_p = 1$ por tenerse que $|z|_p = 1$. Entonces $z^{-1} \in \mathbb{Z}_p$ y por ser I ideal de $\mathbb{Z}_p$ se obtiene $1 = zz^{-1} \in I$.

    Para cualquier $x \in \mathbb{Z}_p$ se tiene que $1x \in I$, es decir, $x \in I$. Luego, $\mathbb{Z}_p \subset I$, es decir, $I = \mathbb{Z}_p$.

    Entonces cualquier ideal de $\mathbb{Z}_p$ distinto de $\mathbb{Z}_p$ consta de elementos que no son unidades de $\mathbb{Z}_p$, así está contenido en $p\mathbb{Z}_p$.

    Por tanto, $p\mathbb{Z}_p$ es el único ideal maximal de $\mathbb{Z}_p$, es decir, $\mathbb{Z}_p$ es un anillo local.

4. Si $x \in \mathbb{Z}_p - p\mathbb{Z}_p$ entonces $|x|_p = 1$. Luego $x \neq 0$ y $x^{-1} \in \mathbb{Q}_p$. Se tiene $|x^{-1}|_p = \frac{1}{|x|_p} = 1$.
    Entonces $x^{-1} \in \mathbb{Z}_p - p\mathbb{Z}_p$. Así, cada elemento de $\mathbb{Z}_p - p\mathbb{Z}_p$ es invertible en $\mathbb{Z}_p$.

    Si $x \in p\mathbb{Z}_p$ fuera invertible se tendría que existe $y \in \mathbb{Z}_p$ tal que $xy = 1$, es decir, $|x|_p|y|_p = 1$, pero esta es una contradicción pues $|x|_p|y|_p \leq |x|_p \leq \frac{1}{p}$. Así, los únicos elementos invertibles de $\mathbb{Z}_p$ son los elementos de $\mathbb{Z}_p - p\mathbb{Z}_p$.

□

La proposición anterior permite establecer la siguiente definición.

Definición 5.3. *El grupo de unidades de $\mathbb{Z}_p$ es*

$$\mathbb{Z}_p^{\times} = \{x \in \mathbb{Z}_p : |x|_p = 1\}.$$

6. Límites proyectivos

Un sistema proyectivo de grupos contiene:

- Un conjunto dirigido $(I, \leqslant)$.
- Una familia $(G_i)_{i\in I}$ de grupos.
- Una familia de homomorfismos de grupos $\pi_i^j : G_j \to G_i$, si $i \leqslant j$, tal que los siguientes axiomas se satisfacen:

$$\pi_i^i = Id_{G_i} \ \text{ y } \ \pi_i^j \circ \pi_j^k = \pi_i^k, \ \text{ si } \ i \leqslant j \leqslant k$$

  Note que, comparando con el sistema directo, los homomorfismo se recorren en dirección opuesta.

Ejemplo 2

Sean p primo, $I = \mathbb{N}$ con el orden usual. Para $n \in \mathbb{N}$, considere $G_n = \mathbb{Z}/p^n\mathbb{Z}$ y para $m \geqslant n$, la proyección canónica $\pi_n^m : \mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$, entonces (G_n, π_n^m) forma un sistema proyectivo de grupos.

Definición 4

Sea (G_i, π_i^j) un sistema proyectivo de grupos. El límite proyectivo del sistema es el conjunto $G = \varprojlim G_i$ de todos los $a \in \prod\limits_{i\in I} G_i$ tal que $a_i = \pi_i^j(a_j)$ se tiene para cada par $i \leqslant j$ en I.

Proposición 2

El límite proyectivo G del sistema (G_i) es un subgrupo del producto $\prod\limits_{i\in I} G_i$. Sea $\pi_i : G \to G_i$ sea una aplicación dada por la proyección a la i -ésima coordenada. Entonces π_i es un homomorfismo de grupos. El límite proyectivo tiene la propiedad universal: Si Z es un grupo con un homomorfismo de grupos $\alpha_i : Z \to G_i$ tales que $\alpha_i = \pi_i^j \circ \alpha_j$ se cumple para todos $i \leqslant j$, entonces existe exactamente un homomorfismo de grupos $\alpha : Z \to G$, tales que los diagramas conmutan.

$$\begin{tikzcd}
Z \arrow[r, "\alpha"] \arrow[dr, "\alpha_i := \pi_i^j \circ \alpha_j"'] & G \arrow[d, "\pi_i"] \\
 & G_i
\end{tikzcd}$$

Definición 5

Suponga que los grupos G_i es un sistema proyectivo dado son grupos topológicos y que los homomorfismos π_i^j son continuados, entonces se equipa $G = \varprojlim G_i$ con la topología inducida por las proyecciones $p_i : G \to G_i$ y recibe el nombre de límite topológico proyectivo.
Dado que la topología del producto $\prod\limits_i G_i$ es inducida por las proyecciones, también el límite proyectivo G envía al subespacio con la topología del producto.

Proposición 3

Sea (G_i, π_i^j) un sistema proyectivo de grupos topológicos con límite G. Entonces G es un subgrupo cerrado del producto $\prod_i G_i$, de ahí que éste es un grupo topológico. Si todos los G_i son Hausdorff, entonces G es Hausdorff. Si todos los G_i son localmente compactos y si un número finito son compactos, entonces G es localmente compacto.

Definición 6

Un grupo profinito es un grupo localmente compacto isomorfo al límite proyectivo de grupos finitos.

Ejemplo 3 Sea p primo. El grupo profinito $\mathbb{Z}_p = \varprojlim\limits_{n} \mathbb{Z}/p^n\mathbb{Z}$, es llamado el grupo de enteros p-ádicos.

7. Topología en $\mathbb{Q}_p$

Definición 7.1. *Se define la* ***bola con centro en*** a ***y radio*** p^r *al conjunto*

$$B(a, p^r) = \{x \in \mathbb{Q}_p : |x - a|_p \leq p^r\}, \quad r \in \mathbb{Z}.$$

Observación 5

Es irrelevante hacer distinción entre la bola abierta y la bola cerrada, pues

$$B(a,p^r)=\{x\in\mathbb{Q}_p : |x-a|_p<p^r\}=\{x\in\mathbb{Q}_p : |x-a|_p\le p^{r-1}\}=\overline{B}(a,p^{r-1}).$$

Definición 7.2. *La **esfera con centro en** a **y radio** p^r es el conjunto*

$$S(a,p^r)=\{x\in\mathbb{Q}_p : |x-a|_p=p^r\},\quad r\in\mathbb{Z}.$$

Proposición 7.1. *Se cumple lo siguiente:*

1. *$B(a,p^r)$ es un conjunto abierto y cerrado.*
2. *Si $b\in B(a,p^r)$ entonces $B(a,p^r)=B(b,p^r)$.*
3. *Si $a,b\in\mathbb{Q}_p$ entonces $B(a,p^r)\cap B(b,p^s)\neq\emptyset$ si y sólo si $B(a,p^r)\subset B(b,p^s)$ ó $B(b,p^s)\subset B(a,p^r)$.*

Demostración.

1. El conjunto $B(a,p^r)$ es abierto por definición de abierto en un espacio métrico. Para probar que $B(a,p^r)$ es un conjunto cerrado, sea $c\notin B(a,p^r)$, entonces $|c-a|_p>p^r$. Sea $B(c,|c-a|_p-p^r)$, para cualquier $z\in B(c,|c-a|_p-p^r)$ se tiene

   $$|a-z|_p\le \text{máx}\{|a-c|_p,|z-c|_p\}.$$

   Como todos los triángulos son isósceles, entonces

   $$|a-z|_p= \text{máx}\{|a-c|_p,|z-c|_p\}.$$

   Luego, $|a-z|_p=|a-c|_p>p^r$. Así, $B(c,|c-a|_p-p^r)\subset B(a,p^r)^c$. Por tanto, $B(a,p^r)$ es un conjunto cerrado.

2. Sea $x\in B(a,p^r)$ entonces $|x-a|_p\le p^r.\Longrightarrow |x-b|_p=|(x-a)+(a-b)|_p\le\text{máx}\{|x-a|_p,|b-a|_p\}\le p^r\Longrightarrow x\in B(b,p^r)\Longrightarrow B(a,p^r)\subset B(b,p^r)$. Análogamente se obtiene $B(b,p^r)\subset B(a,p^r)$.

   Así, $B(a,p^r)=B(b,p^r)$.

3. Si $B(a,p^r)\cap B(b,p^s)\neq\emptyset$ entonces existe $c\in B(a,p^r)\cap B(b,p^s)$. Por 1, se tiene que $B(c,p^r)=B(a,p^r)$ y $B(c,p^s)=B(b,p^s)$.

   Sin pérdida de generalidad sea $p^r\le p^s$

   $$\Longrightarrow B(c,p^r)\subset B(c,p^s)\Longrightarrow B(a,p^r)\subset B(b,p^s).$$

   Así, $B(a,p^r)\subset B(b,p^s)$.

   Recíprocamente, las contenciones implican que la intersección es distinta del vacío.

□

Proposición 7.2. *Sean $a\in\mathbb{Q}_p$ y $n\in\mathbb{Z}$, los conjuntos $a+p^n\mathbb{Z}_p$ son bolas en $\mathbb{Q}_p$, es decir, $a+p^n\mathbb{Z}_p=B(a,p^{-n})$.*

Demostración. Se tiene $x\in a+p^n\mathbb{Z}_p\Longleftrightarrow x=a+p^ny$ con $y\in\mathbb{Z}_p\Longleftrightarrow x-a=p^ny\Longleftrightarrow |x-a|_p\le p^{-n}\Longleftrightarrow x\in B(a,p^{-n})$. □

Proposición 7.3. *Sea $a \in \mathbb{Q}_p$ y $n \in \mathbb{Z}$, los conjuntos $a + p^n\mathbb{Z}_p^\times$ son esferas en $\mathbb{Q}_p$, es decir, $a + p^n\mathbb{Z}_p^\times = S(a, p^{-n})$.*

Demostración. Se tiene $x \in a + p^n\mathbb{Z}_p^\times \iff x = a + p^n y$ con $y \in \mathbb{Z}_p^\times \iff x - a = p^n y \iff |x-a|_p = p^{-n} \iff x \in S(a, p^{-n})$. □

Proposición 7.4. *$\mathbb{Q}_p$ es un espacio de Hausdorff totalmente disconexo.*

Demostración. Todo espacio métrico es de Hausdorff, así $\mathbb{Q}_p$ es un espacio de Hausdorff.
Sea $S \neq \emptyset$ un subconjunto de $\mathbb{Q}_p$. Si $x, y \in S$ con $x \neq y$, sea $p^r = |x - y|_p$, entonces $B(x, \frac{p^r}{2})$ es un conjunto abierto y cerrado que contiene a x y no contiene a y.
Luego, $\mathbb{Q}_p - B(x, \frac{p^r}{2})$ es un conjunto abierto que contiene a y y no contiene a x. Entonces, existen dos conjuntos abiertos $B(x, \frac{p^r}{2})$ y $\mathbb{Q}_p - B(x, \frac{p^r}{2})$ distintos del vacío y cuya intersección es vacía, además

$$S = \left(S \cap B\left(x, \frac{p^r}{2}\right)\right) \cup \left(S \cap \left(\mathbb{Q}_p - B\left(x, \frac{p^r}{2}\right)\right)\right).$$

Así, S es disconexo, Luego, ningún conjunto con dos o más puntos puede ser conexo, es decir, los únicos subconjuntos conexos son de la forma $\{x\}$.
Por tanto, $\mathbb{Q}_p$ es totalmente disconexo. □

Proposición 7.5. *La inclusión $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ tiene una imagen densa. En particular, dado $x \in \mathbb{Z}_p$ y $n \geq 1$ existe $\alpha \in \mathbb{Z}$ con $0 \leq \alpha \leq p^n - 1$, tal que $|x - \alpha|_p \leq p^{-n}$. El entero α con estas propiedades es único.*
Para cualquier $x \in \mathbb{Z}_p$ existe una sucesión de Cauchy α_n que converge a x con las siguientes características:

(i) $\alpha_n \in \mathbb{Z}$ *para todo* n *y* $0 \leq \alpha_n \leq p^n - 1$.

(ii) *Para cada* n *se tiene* $\alpha_n \equiv \alpha_{n-1} \pmod{p^{n-1}}$.

La sucesión (α_n) con estas propiedades es única.

Demostración. 1) Por las propiedades de $|\cdot|_p$ basta verificar que cada bola centrada en un entero $p-$ádico y de 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 $\frac{a}{b} \in \mathbb{Q}$, con m.c.d$(a, b) = 1$, tal que $|x - \frac{a}{b}|_p \leq p^{-n} < 1$. Además,

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

esto implica que $p \nmid b$.

Como $p \nmid b$ entonces $p^n \nmid b$ y en consecuencia $(p^n, b) = 1$. Luego, existen $b', c \in \mathbb{Z}$ tal que $bb' + cp^n = 1$. Esto implica que $bb' \equiv 1 \pmod{p^n}$. Entonces

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

usando el hecho de que $p \nmid b$ y $p^n | 1 - bb'$ se obtiene
$\frac{a(1-bb')}{b} = p^t \frac{a'}{b}$, $\quad t \geq n$ implica $\left|\frac{a(1-bb')}{b}\right|_p \leq \frac{1}{p^n}$, por lo tanto $|x - ab'|_p = \left|x - \frac{a}{b} + \frac{a}{b} - ab'\right|_p \leq$ $\text{máx}\{\left|x - \frac{a}{b}\right|_p, \left|\frac{a}{b} - ab'\right|_p\} \leq p^{-n}$.

Así, ab' es un entero contenido en $B(x, p^{-n})$. Por 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 $\alpha \equiv ab' \pmod{p^n}$, se tiene

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

Así, α es el único entero que satisface $0 \leq \alpha \leq p^n - 1$ y $|x - \alpha|_p \leq p^{-n}$.

2) Sea $x \in \mathbb{Z}_p$, usando lo probado en 1), se tiene que para todo $n \in \mathbb{N}$ existe un único α_n que satisface

$$0 \leq \alpha_n \leq p^n - 1 \quad y \quad |x - \alpha_n|_p \leq p^{-n}.$$

Sea (α_n) la sucesión descrita. Se tiene

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

entonces $\text{lím}_{n\to\infty} |\alpha_{n+1} - \alpha_n|_p \leq \text{lím}_{n\to\infty} p^{-n} = 0$, implica $\text{lím}_{n\to\infty} |\alpha_{n+1} - \alpha_n|_p = 0$.
Luego, por el Lema de Cauchy se tiene que (α_n) es de Cauchy. Por otro lado

$$|x - \alpha_n|_p \leq p^{-n} \quad \forall n \in \mathbb{N} \Longrightarrow \lim_{n\to\infty} |x - \alpha_n| = 0 \Longrightarrow \lim_{n\to\infty} \alpha_n = x.$$

La sucesión (α_n) satisface (i) por como fue escogida. Además, por como se escogió la sucesión se tiene que

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

esto último implica $\alpha_n \equiv \alpha_{n-1} \pmod{p^{n-1}}$.Así, se satisface (ii).
Por último, la unicidad en 1) garantiza la unicidad de (α_n).

□

Corolario 7.1. *Sea $n \in \mathbb{N}$ se tiene*

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

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

$$f : \mathbb{Z}_p / p^n\mathbb{Z}_p \longrightarrow \mathbb{Z}/p^n\mathbb{Z}.$$

dado que

$$f(x + p^n\mathbb{Z}_p) = \alpha_x + p^n\mathbb{Z}.$$

f esta 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, $|x - y|_p \leq p^{-n}$, luego se tiene que

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

por lo que

$$\alpha_x \equiv \alpha_y \pmod{p^n} \Longrightarrow \alpha_x + p^n\mathbb{Z} = \alpha_y + p^n\mathbb{Z} \Longrightarrow f(x + p^n\mathbb{Z}_p) = f(y + p^n\mathbb{Z}).$$

f es biyección:
f es inyectiva pues

$$f(x + p^n\mathbb{Z}_p) = f(y + p^n\mathbb{Z}) \Longrightarrow \alpha_x + p^n\mathbb{Z} = \alpha_y + p^n\mathbb{Z} \Longrightarrow \alpha_x \equiv \alpha_y \pmod{p^n}.$$

Luego,

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

Por lo tanto,

$$x - y \in p^n\mathbb{Z}_p \Longrightarrow x + p^n\mathbb{Z}_p = y + p^n\mathbb{Z}_p.$$

f es sobreyectiva pues para cualquier $k + p^n\mathbb{Z}$ se tiene $f(k + p^n\mathbb{Z}_p) = k + p^n\mathbb{Z}$.

f es homomorfismo:

1. Se tiene que $f(1 + p^n\mathbb{Z}_p) = 1 + p^n\mathbb{Z}$.

2. Se tiene que $f(x+p^n\mathbb{Z}_p+y+p^n\mathbb{Z}_p) = f(x+y+p^n\mathbb{Z}_p) = \alpha_{x+y}+p^n\mathbb{Z} = \alpha_x+\alpha_y+p^n\mathbb{Z} = f(x+p^n\mathbb{Z}_p)+f(y+p^n\mathbb{Z}_p)$.

   La cadena de igualdades se justifica por,

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

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

3. Se tiene $f((x+p^n\mathbb{Z}_p)(y+p^n\mathbb{Z}_p)) = f(xy+p^n\mathbb{Z}_p) = \alpha_{xy}+p^n\mathbb{Z} = \alpha_x\alpha_y+p^n\mathbb{Z} = f(x+p^n\mathbb{Z}_p)f(y+p^n\mathbb{Z}_p)$.

   La cadena de igualdades se justifica usando

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

   Luego,
$$\alpha_x\alpha_y \equiv \alpha_{xy} \pmod{p^n} \Longrightarrow \alpha_{xy}+p^n\mathbb{Z} = \alpha_x\alpha_y+p^n\mathbb{Z}.$$

□

Proposición 7.6. *Las esferas son conjuntos abiertos y cerrados.*

Demostración. Puesto que $\mathbb{Z}_p^\times = \mathbb{Z}_p - p\mathbb{Z}_p$, el Corolario 1 afirma que si $n \in \mathbb{N}$ entonces $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$.
Esto implica que los números $0, 1, 2, \cdots, p^n-1$ son representantes de las clases de $\mathbb{Z}_p/p^n\mathbb{Z}_p$, es decir,

$$\mathbb{Z}_p = \bigsqcup_{i=0}^{p^n-1} i+p^n\mathbb{Z}_p \Longrightarrow \mathbb{Z}_p^\times = \bigsqcup_{i=1}^{p-1} i+p\mathbb{Z}_p.$$

En consecuencia,

$$S(a,p^n) = a+p^{-n}\mathbb{Z}_p^\times = \bigsqcup_{i=1}^{p-1} a+ip^{-n}+p^{-(n-1)}\mathbb{Z}_p = \bigsqcup_{i=1}^{p-1} B(a+ip^{-n}, p^{-(n-1)}).$$

Así, $S(a,p^n)$ es un conjunto abierto y cerrado, para cada $a \in \mathbb{Q}_p$ y $n \in \mathbb{Z}$, pues las bolas son conjuntos abiertos y cerrados. □

Los siguientes resultados son necesarios para introducir un proceso de integración en $\mathbb{Q}_p$.

Corolario 7.2. $\mathbb{Z}_p$ *es compacto.*

Demostración. Puesto que $\mathbb{Z}_p = B(0,1)$ es un conjunto cerrado y además $\mathbb{Z}_p \subset \mathbb{Q}_p$ que es un conjunto completo entonces $\mathbb{Z}_p$ es completo.
Por otro lado, por el Corolario 1, si $n \in \mathbb{N}$ entonces $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$.
Entonces, los números $0, 1, 2, \cdots, p^n-1$ son representantes de las clases de $\mathbb{Z}_p/p^n\mathbb{Z}_p$, es decir,

$$\mathbb{Z}_p = \bigsqcup_{i=0}^{p^n-1} i+p^n\mathbb{Z}_p \Longrightarrow \mathbb{Z}_p = \bigsqcup_{i=0}^{p^n-1} B(i,p^n),$$

por la Proposición 5. Luego, para cualquier $\epsilon > 0$ existe $n \in \mathbb{N}$ tal que $p^{-n} < \epsilon$ y se obtiene

$$\mathbb{Z}_p = \bigsqcup_{i=0}^{p^n-1} B(i,p^n) \subset \bigcup_{i=0}^{p^n-1} B(i,\epsilon).$$

Así, $\mathbb{Z}_p$ es totalmente acotado.
Como $\mathbb{Z}_p$ es completo y totalmente acotado, por el teorema de Heine Borel se concluye que $\mathbb{Z}_p$ es compacto. □

Proposición 7.7. *Las esferas y las bolas son conjuntos compactos.*

Demostración. Para cualquier $n \in \mathbb{Z}$ y $a \in \mathbb{Q}_p$ se tiene que $B(a, p^n) = a + p^{-n}\mathbb{Z}_p$.
Sea $h : \{p^{-n}\} \times \mathbb{Z}_p \longrightarrow \mathbb{Q}_p$ definida por $h((x, y)) = xy$.
Se tiene que h es la operación producto restringida al conjunto $\{p^{-n}\} \times \mathbb{Z}_p$ y como la operación producto es continua se obtiene que h es continua.
Luego, $B(0, p^n) = h(\{p^{-n}\} \times \mathbb{Z}_p)$, entonces $B(0, p^n)$ es un compacto pues es la imagen continua de un compacto.
Sea $g : \{a\} \times p^{-n}\mathbb{Z}_p \longrightarrow \mathbb{Q}_p$ definida por $h((x, y)) = x + y$.
Se tiene que g es la operación suma restringida al conjunto $\{a\} \times p^{-n}\mathbb{Z}_p$ y como la operación suma es continua se obtiene que g es continua.
Luego, $B(a, p^n) = g(\{a\} \times p^{-n}\mathbb{Z}_p)$, entonces $B(a, p^n)$ es un compacto pues es la imagen continua de un compacto.
Así, las bolas son conjuntos compactos.
De manera análoga se prueba que las esferas son conjuntos compactos. □

Corolario 7.3. $\mathbb{Q}_p$ *es localmente compacto.*

Demostración. Para $a \in \mathbb{Q}_p$, basta con tomar $B(a, 1)$ que es un conjunto compacto por la proposición anterior. □

Proposición 7.8. $\mathbb{Z}_p^{\times}$ *es compacto.*

Proposición 7.9. $\mathbb{Q}_p^{\times}$ *es localmente compacto.*

Ejercicios 1:

1. Determine las valuaciones indicadas: $v_3(18),\ v_2(1728)$ y $v_5\left(\dfrac{49}{50}\right)$.
2. Encuentre los valores absolutos: $|9|_3,\ |24|_2$ y $\left|\dfrac{15}{28}\right|_7$
3. Demuestre que un campo no contiene divisores de cero.
4. Encuentre la expansión p -ádica de $\frac{1}{p}$, luego halle la expansión p-ádica de $\frac{1}{2}$ si p es un primo impar.
5. Si $a \in \mathbb{Q}_p$ tiene una expansión p -ádica canónica $\cdots a_n \cdots a_2 a_1 a_0 a_{-1} \cdots a_{-m},$, ¿Cuál es la expansión canónica p -ádica de $-a$?
6. Encuentre la norma p- ádica de $(p^n)!$
7. Encuentre la norma p -ádica de $n!$.
8. Pruebe que $\mathbb{Z}_p \cap \mathbb{Q} = \{\frac{a}{b} \in \mathbb{Q} : p \not| b\}$, luego muestre que $\mathbb{Z}_p^{\times} \cap \mathbb{Q} = \{\frac{a}{b} \in \mathbb{Q} : p \not| ab\}$.

8. Series en $\mathbb{Q}_p$

Ahora, se muestra la forma de representar un número $p-$ádico como una serie de potencias, es importante conocer esta forma pues permite operar con estos números.

Proposición 8.1. *Cada $x \in \mathbb{Z}_p$ puede escribirse en la forma*

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

con $0 \leq b_i \leq p-1$. Además, esta representación es única.

Demostración. Sea $x \in \mathbb{Z}_p$, entonces existe una sucesión de Cauchy (α_n) que converge a x, y satisface

1. $\alpha_n \in \mathbb{Z}$ y además $0 \leq \alpha_n \leq p^n - 1$.
2. $\alpha_n \equiv \alpha_{n-1} \pmod{p^{n-1}}$.

La sucesión con estas propiedades es única. Poniendo los α_n en base p se obtiene una serie de la siguiente manera

1. $\alpha_1 = b_0$ donde $0 \leq b_0 \leq p-1$.
2. $\alpha_2 = b_0' + b_1 p$ con $0 \leq b_0', b_1 \leq p-1$ y $0 \leq \alpha_2 \leq p^2 - 1$.
   Como $\alpha_2 \equiv \alpha_1 \pmod{p}$ entonces $b_1 p + b_0' \equiv b_0 \pmod{p}$, luego $b_0' \equiv b_0 \pmod{p}$.
   Esto implica que $b_0' = b_0$ y así $\alpha_2 = b_0 + b_1 p$.
3. En general se tiene que si
   $\alpha_{n+1} = b_0' + b_1' p + b_2' p^2 + \cdots + b_n' p^n$ con $0 \leq b_i' \leq p-1$ y $0 \leq \alpha_{n+1} \leq p^{n+1} - 1$
   $\alpha_{n+1} = b_0 + b_1 p + b_2 p^2 + \cdots + b_{n-1} p^{n-1}$ con $0 \leq b_i \leq p-1$ y $0 \leq \alpha_n \leq p^n - 1$
   Como $\alpha_{n+1} \equiv \alpha_n \pmod{p^n}$ entonces

$$b_0' + b_1' p + b_2' p^2 + \cdots + b_n' p^n \equiv b_0 + b_1 p + b_2 p^2 + \cdots + b_{n-1} p^{n-1} \pmod{p^n}$$

$$\begin{aligned}
\Longrightarrow \quad b_0 + b_1 p + b_2 p^2 + \cdots + b_{n-1} p^{n-1} &= b_0' + b_1' p + b_2' p^2 + \cdots + b_n' p^n \\
\Longrightarrow \quad b_i &= b_i' \qquad \forall i : 1, ..., n-1.
\end{aligned}$$

Así, se obtiene

$$\begin{array}{rl}
\alpha_1 = b_0 & 0 \leq b_0 \leq p-1 \\
\alpha_2 = b_0 + b_1 p & 0 \leq b_1 \leq p-1 \\
\alpha_3 = b_0 + b_1 p + b_2 p^2 & 0 \leq b_2 \leq p-1 \\
\vdots & \vdots \\
\alpha_n = b_0 + b_1 p + b_2 p^2 + \cdots + b_{n-1} p^{n-1} & 0 \leq b_{n-1} \leq p-1 \\
\alpha_{n-1} = b_0 + b_1 p + b_2 p^2 + \cdots + b_{n-1} p^{n-1} + b_n p^n & 0 \leq b_n \leq p-1 \\
\vdots & \vdots
\end{array}$$

Como las sumas parciales de la serie recién construida son los α_n que convergen a x se cumple que la serie construida converge a x. Así, x puede escribirse en la forma

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

con $0 \leq b_i \leq p-1$. La unicidad se obtiene de la unicidad de la sucesión (α_n). $\square$

Corolario 8.1. *Cada $x \in \mathbb{Q}_p$ puede ser escrito en la forma*

$$x = b_{-n_0} p^{-n_0} + b_{-n_0+1} p^{-n_0+1} + \cdots + b_0 + b_1 p + \cdots + b_n p^n + \cdots = \sum_{n \geq -n_0} b_n p^n,$$

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

Demostración. Sea $x \in \mathbb{Q}_p$.
Si $x \in \mathbb{Z}_p$ entonces por la proposición anterior

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

con $0 \leq b_i \leq p-1$ y esta representación es única.
Por otro lado, sea n_k el menor entero positivo tal que $b_{n_k} \neq 0$ se tiene

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

$$\begin{array}{rrcl}
\Longrightarrow & |x|_p & = & \left|\sum_{n \geq n_k} b_n p^n\right|_p, \\
& & \leq & \max\left\{|b_{n_k} p^{n_k}|_p, \left|\sum_{n \geq n_k+1} b_n p^n\right|_p\right\}, \\
\Longrightarrow & |x|_p & = & \max\left\{p^{-n_k}, \left|\sum_{n \geq n_k} b_n p^n\right|_p\right\}, \\
\Longrightarrow & |x|_p & = & p^{-n_k}, \\
\Longrightarrow & v_p(x) & = & n_k.
\end{array}$$

Si $x \notin \mathbb{Z}_p$, sea $n_0 = -v_p(x)$ se tiene que $n_0 \in \mathbb{Z}$, $n_0 \geq 0$ y además $xp^{n_0} \in \mathbb{Z}_p$. Luego,

$$xp^{n_0} = \sum_{n \geq 0} b_n p^n,$$

con $b_0 \neq 0$. Entonces

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

La unicidad de la representación se deduce de la unicidad de xp^{n_0} y además se tiene $v_p(x) = -n_0$. $\square$

Ejemplo 8.1. 1. *Se tiene que*

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

Tomando sumas parciales se obtiene

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

Luego,

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

pues

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

2. *En el ejemplo anterior se obtuvo*

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

Esto implica que

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

Teorema 8.1. *Una sucesión $\{a_n\}$ en $\mathbb{Q}_p$ es una sucesión de Cauchy, y por lo tanto convergente, si y solo si se satisface que $\lim_{n\to\infty} |a_{n+1} - a_n|_p = 0$.*

Demostración. $\rightarrow$. Si $\{a_n\}$ es de Cauchy entonces, si $\epsilon > 0$ existe $N \in \mathbb{N}$ tal que si $m, n > N$ entonces $|a_m - a_n|_p < \epsilon$, tomando $m = n+1$, se obtiene lo deseado.

$\leftarrow$. Si

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

entonces para $\epsilon > 0$ existe $N \in \mathbb{N}$ tal que si $n \geq N$ entonces

$$|a_{n+1} - a_n|_p < \epsilon,$$

ahora bien, sean $m, n > N$ entonces

$$\begin{aligned} |a_m - a_n|_p &= |a_{n+r} - a_{n+r-1} + a_{n+r-1} - \ldots + a_{n+1} - a_n|_p\,, \\ &\leq \max\{|a_{n+r} - a_{n+r-1}|_p\,, \ldots, |a_{n+1} - a_n|_p\}, \\ &< \epsilon, \end{aligned}$$

y esto completa la prueba

□

Definición 8.1. *Se dice que una serie $\sum_{i=1}^{\infty} a_i$, converge en $\mathbb{Q}_p$ si la sucesión de sumas parciales $S_n = \sum_{i=1}^{n} a_i$, converge en $\mathbb{Q}_p$, y se dice que converge absolutamente si $\sum_{i=1}^{\infty} |a_i|_p$ converge en $\mathbb{R}$.*

Proposición 8.2. *Si la serie $\sum_{i=1}^{\infty} |a_i|_p$, converge en $\mathbb{R}$, entonces $\sum_{i=1}^{\infty} a_i$ converge en $\mathbb{Q}_p$.*

Demostración. Como $\sum_{i=1}^{\infty} |a_i|_p$ converge, la sucesión de sumas parciales es de Cauchy, por lo tanto si $\epsilon > 0$ existe $N \in \mathbb{N}$ tal que si $m, n > N$ se tiene que $\sum_{i=n+1}^{m} |a_i|_p < \epsilon$, por la desigualdad triangular $|S_m - S_n|_p = \left|\sum_{i=n+1}^{m} a_i\right|_p \leq \sum_{i=n+1}^{m} |a_i|_p < \epsilon$, lo que implica que $\{S_n\}$ es de Cauchy y por lo tanto la serie converge en $\mathbb{Q}_p$. □

Proposición 8.3. *Una serie $\sum_{n=1}^{\infty} a_n$ con $a_n \in \mathbb{Q}_p$ converge en $\mathbb{Q}_p$ si y solo si $\lim_{n\to\infty} a_n = 0$, con lo que se tiene $|\sum_{n=1}^{\infty} a_n|_p \leq \max_n |a_n|_p$.*

Demostración. La serie converge si y solo si la sucesión de sumas parciales $S_n = \sum_{i=1}^{n} a_i$ converge. Pero $a_n = S_n - S_{n-1}$, se sigue por el teorema previamente visto que $\lim_{n\to\infty} a_n = 0$. Ahora suponga que $\sum_{n=1}^{\infty} a_n$ converge. Si $\sum_{n=1}^{\infty} a_n = 0$, no hay nada que demostrar. En otro caso, para cualquier suma parcial $\left|\sum_{n=1}^{N} a_n\right|_p \leq \max_{1\leq n\leq N} |a_n|_p$, entonces para un N lo suficientemente grande $\max_{1\leq n\leq N} |a_n|_p = \max_n |a_n|_p$. Dado que $\lim_{n\to\infty} a_n = 0$, y

$$\left|\sum_{n=1}^{\infty} a_n\right|_p = \left|\sum_{n=1}^{N} a_n\right|_p .$$

□

Definición 8.2. *Se dice que una serie $\sum_{n=1}^{\infty} a_n$ converge incondicionalmente si para cualquier reordenamiento de los términos $a_n \to a'_n$ la serie $\sum_{n=1}^{\infty} a'_n$ también converge.*

Teorema 8.2. *Si $\sum_{n=1}^{\infty} a_n$ converge, esta converge incondicionalmente, y la suma no depende del reordenamiento.*

Demostración. Sea $\epsilon > 0$ entonces existe un $N \in \mathbb{N}$ tal que si $n > N$ se tiene que $|\sum_{i=1}^{\infty} a_i - \sum_{i=1}^{n} a_i|_p < \epsilon$. Defina $S = \sum_{i=1}^{n} a_i$ y $S' = \sum_{i=1}^{n} a'_i$, y denote por S_1 y S'_1, la suma de todos los términos de S para los cuales $|a_n|_p > \epsilon$, y de todos los términos de S' para los cuales $|a'_n|_p > \epsilon$, respectivamente. Es claro que S_1 y S'_1 tienen los mismos términos; por lo tanto $S_1 = S'_1$. Con esto se tiene que $|S - S_1|_p < \epsilon$ y $|S' - S'_1|_p < \epsilon$, por lo cual $|S - S'|_p < \epsilon$. Con lo cual se logra obtener $|\sum_{i=1}^{\infty} a_i - \sum_{i=1}^{n} a'_i|_p < \epsilon$. y como $\epsilon \to \epsilon$ y $n \to \infty$ se ve que la serie $\sum_{i=1}^{n} a'_i$ converge y $\sum_{i=1}^{\infty} a_i = \sum_{i=1}^{\infty} a'_i$. □

Teorema 8.3. *Existe una serie $\sum_{i=1}^{\infty} a_i$ en $\mathbb{Q}_p$ que converge, pero no converge absolutamente.*

Teorema 8.4. *Sean $b_{ij} \in \mathbb{Q}_p$, i,j=1,2,..., tal que para cualquier $\epsilon > 0$ existe un entero $N = N(\epsilon)$ para el cual $\max(i,j) \geq N \to |b_{ij}|_p < \epsilon$. Entonces las series $\sum_i \left(\sum_j b_{ij}\right)$ and $\sum_j \left(\sum_i b_{ij}\right)$, convergen, y sus sumas son iguales.*

Demostración. Se tiene que las series $\sum_j b_{ij}$ y $\sum_i b_{ij}$ convergen, además, para todo $i \geq N$ se tiene $\left|\sum_j b_{ij}\right|_p \leq \max |b_{ij}|_p < \epsilon$, y similarmente, para todo $j \geq N$ $|\sum_i b_{ij}|_p < \epsilon$. Por lo tanto las series dobles convergen.
Por último,

$$\left|\sum_{i=1}^{\infty}\left(\sum_{j=1}^{\infty} b_{ij}\right) - \sum_{i=1}^{n}\left(\sum_{j=1}^{n} b_{ij}\right)\right|_p = \left|\sum_{i=1}^{n}\left(\sum_{j=n+1}^{\infty} b_{ij}\right) + \sum_{i=n+1}^{\infty}\left(\sum_{j=1}^{\infty} b_{ij}\right)\right|_p < \epsilon$$

que solo puede ser cierto para cualquier ϵ solamente si las series son iguales. □

Para cerrar esta sección se presenta un resultado importante sobre extensiones algebraicas de $\mathbb{Q}_p$ y una función que conecta con los números complejos.

Lema 8.1. *(Lema de Hensel) Sea $f(x) = c_0 + c_1x + \cdots + c_nx^n$ con $c_i \in \mathbb{Z}_p, i = 0, \ldots, n$ y sea $f'(x) = c_1 + 2c_2x + \ldots + nc_nx^{n-1}$ su derivada formal. Si $a_0 \in \mathbb{Z}_p$ tal que $f(a_0) \equiv 0 \mod p$ y $f'(a_0) \not\equiv 0 \mod p$, entonces existe un único entero $p-$ádico x_0 sujeto a $x_0 \equiv a_0 \mod p$ que satisface $f(x_0) = 0$.*

Demostración. La demostración de este resultado puede ser consultada en [1]. □

El Lema de Hensel permite ver, por ejemplo, que el polinomio $x^2 + 1$ es reducible en $\mathbb{Q}_5$, pero no lo es en $\mathbb{Q}_7$, en efecto, note que en $\mathbb{Q}_5$ se tiene que

$$\begin{aligned} 2^2 + 1 = 5 \equiv 0 \mod 5, \\ 3^2 + 1 = 10 \equiv 0 \mod 5, \end{aligned}$$

además, se tiene que

$$\begin{aligned} 2(2) = 4 \not\equiv 0 \mod 5, \\ 2(3) = 6 \not\equiv 0 \mod 5. \end{aligned}$$

Por lo tanto, existen $x_2, x_3 \in \mathbb{Z}_5$ tal que $f(x_2) = f(x_3) = 0$, pero nótese que en $\mathbb{Q}_7$ se tiene que para $x = 1, 2, 3, \ldots, 6; x^2 + 1 \not\equiv 0 \mod 7$. Esto implica que el polinomio $x^2 + 1$ es irreducible en $\mathbb{Q}_7$.
Por lo tanto, existen polinomios en $\mathbb{Q}_p$ que no son reducibles, lo cual permite pensar en extensiones algebraicas.
Sea $\mathbb{K}$ un campo tal que $\mathbb{K} = \mathbb{Q}_p(u)$ donde u es raíz del polinomio

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0,$$

entonces se define

$$N_{K/\mathbb{Q}_p}(u) = \prod_{i=1}^{n} u_i,$$

donde u_i son los conjugados de $u = u_1$ sobre $\mathbb{Q}_p$.
La norma algebraica $N_{K/\mathbb{Q}_p}$ cumple las siguientes propiedades

- $N_{K/\mathbb{Q}_p}(uv) = N_{K/\mathbb{Q}_p}(v)N_{K/\mathbb{Q}_p}(v)$.
- Para un cuerpo intermedio E, se tiene que $N_{E/\mathbb{Q}_p}(N_{K/E}(u)) = N_{K/\mathbb{Q}_p}(u)$.
- $N_{K/\mathbb{Q}_p}(a) = a^n$, para $a \in \mathbb{Q}_p$.

esto permite ver el siguiente resultado.

Teorema 8.5. *Sea K una extensión finita de grado n sobre $\mathbb{Q}_p$. Entonces*

$$|x|_K = \left|N_{K/\mathbb{Q}_p}(x)\right|_p^{1/n}.$$

Demostración. La demostración de este resultado se puede consultar en [2]. □

Por último se dará la definición del caracter multiplicativo definido sobre $\mathbb{Q}_p$.

Definición. 1. Sea $e : \mathbb{Q}_p \to \mathbb{C}$ definida de la siguiente forma

$$e(x) = e^{2\pi i \left[\sum_{j=-N}^{-1} a_j p^j\right]},$$

donde x está representado como en el Corolario 1.4. Esta función es conocida como caracter multiplicativo sobre $\mathbb{Q}_p$.

Ejercicios 2

Demuestre que:

1. $\sum_{n=1}^{\infty} n! * n = -1$, en $\mathbb{Q}_p$ para cualquier p.
2. $\sum_{n=1}^{\infty} n^2(n+1)! = 2$, en $\mathbb{Q}_p$ para cualquier p.

9. Integración en $\mathbb{Q}_p$.

Teorema 9.1. *Sea $(G, +)$ un grupo topológico localmente compacto, existe una medida regular de Borel, única salvo multiplicación por constantes positivas, tal que*

1. *$\int_U dx > 0$, para cada conjunto de Borel U, distinto del vacío.*
2. *$\int_{x+U} = \int_U dx$, para cada conjunto de Borel.*

La medida dx descrita en el teorema anterior es una Medida de Haar sobre G.
En las secciones anteriores se vio que $(\mathbb{Q}_p, +)$ es un grupo topológico abeliano localmente compacto, así por el Teorema 1.5 existe una medida de Haar dx sobre $(\mathbb{Q}_p, +)$. Por otro lado, $\mathbb{Z}_p$ es compacto y por ser dx una medida regular se obtiene

$$\int_{\mathbb{Z}_p} dx < \infty.$$

Así, se puede normalizar esta medida por la condición

$$\int_{\mathbb{Z}_p} dx = 1,$$

y así dx es única.
Los abiertos compactos de $\mathbb{Q}_p$, $B_{p^{-m}}(a)$, generan la σ-álgebra de Borel. La medida dx asigna a cada subconjunto abierto compacto U un número real no negativo $\int_U dx$, que además satisface

$$\int_{\bigcup_{n=1}^{\infty} U_n} dx = \sum_{n=1}^{\infty} \int_{U^n} dx,$$

para todos los subconjuntos abiertos compactos U_n en $\mathbb{Q}_p$, que son disjuntos dos a dos, tales que $\bigcup_{n=1}^{\infty} U_n$ es igualmente compacto. También cumple,

$$\int_{x_0+U} dx = \int_U dx.$$

Proposición 9.1. *Sea $d(ax)$ definida por $d(ax)(U) = dx(aU)$, entonces $d(ax)$ es una medida de Haar y*

$$d(ax) = |a|_p dx \qquad a \in \mathbb{Q}_p^{\times}.$$

Es decir,

$$\int_{aU} dx = |a|_p \int_U dx.$$

Demostración. [3] Se define la función

$$T_a : \mathbb{Q}_p \to \mathbb{Q}_p,$$

de la siguiente manera, si $x \in \mathbb{Q}_p$ entonces $T_a(x) = ax$. Es fácil ver que T_a está bien definida y que es biyectiva.
Se tiene que T_a es la restricción de la operación producto al conjunto $\{a\} \times \mathbb{Q}_p$, esto implica que T_a

es continua, además, por la continuidad de la operación "tomar inversos multiplicativos" se obtiene que T_a^{-1} es continua.
Por todas las características anteriores se tiene que T_a es un homeomorfismo de $\mathbb{Q}_p$ en $\mathbb{Q}_p$; entonces $d(ax)$ es una medida de Borel regular sobre $\mathbb{Q}_p$.
Se puede observar que la invarianza de traslación de $d(ax)$ es consecuencia de la invarianza de traslación de dx, esto es, para cualquier $y \in \mathbb{Q}_p$ se tiene

$$d(ax)(y+U) = dx(a(y+U)) = dx(ay+aU) = dx(aU) = d(ax)(U).$$

Por tanto, $d(ax)$ es una medida de Haar sobre $\mathbb{Q}_p$.

Por Teorema 8.5 existe una constante positiva $C(a)$ tal que $\int_{aU} dx = C(a) \int_U dx$. Para calcular $C(a)$ se puede usar cualquier conjunto abierto compacto U, en este caso se toma $U = \mathbb{Z}_p$.
Suponga que $a \in \mathbb{Z}_p$, entonces $|a|_p = p^{-k}$ con $k \in \mathbb{N}$.
Se tiene

$$\mathbb{Z}_p = \bigsqcup_{i=0}^{p^k-1} i + p^k\mathbb{Z}_p,$$

así,

$$1 = \int_{\mathbb{Z}_p} dx = \sum_{i=0}^{p^k-1} \int_{i+p^k\mathbb{Z}_p} dx = \sum_{i=0}^{p^k-1} \int_{p^k\mathbb{Z}_p} dx = p^k \int_{p^k\mathbb{Z}_p} dx,$$

por lo tanto,

$$\int_{p^k\mathbb{Z}_p} dx = p^{-k} = |a|_p.$$

Como $|a|_p = p^{-k}$ entonces $a = p^k u$ con $u \in \mathbb{Z}_p^\times$, usando que $\mathbb{Z}_p = u\mathbb{Z}_p$ se obtiene,

$$\int_{a\mathbb{Z}_p} dx = \int_{p^k u\mathbb{Z}_p} dx = \int_{p^k\mathbb{Z}_p} = |a|_p,$$

y dado que

$$\int_{a\mathbb{Z}_p} dx = C(a) \int_{\mathbb{Z}_p} dx,$$

se concluye que $C(a) = |a|_p$, el caso $a \notin \mathbb{Z}_p$ se trata de manera similar. Por tanto,

$$d(ax) = |a|_p dx \qquad a \in \mathbb{Q}_p^\times.$$

$\square$

En los siguientes ejemplos, se calcula las integrales sobre los conjuntos $B_r(a)$ y $S_r(a)$ con $a \in \mathbb{Q}_p$.

Ejemplo 9.1. *[3]*

$$\int_{B_{p^r}(a)} dx = p^r \;\; y \;\; \int_{S_{p^r}(a)} dx = p^r(1-p^{-1}).$$

En efecto, dado que

$$B_{p^r}(a) = a + p^{-r}\mathbb{Z}_p,$$

se tiene

$$\begin{aligned}\int_{B_{p^r}(a)} dx &= \int_{a+p^{-r}\mathbb{Z}_p} dx,\\ &= \int_{p^{-r}\mathbb{Z}_p} dx.\end{aligned}$$

Entonces para cada $x \in B_{p^r}(a)$ se puede hacer la sustitución $x = p^{-r}y$, donde $y \in \mathbb{Z}_p$, con lo que $dx = |p^{-r}|_p\, dy$, así por el resultado anterior.

$$\begin{aligned}\int_{B_{p^r}(a)} dx &= \int_{p^{-r}\mathbb{Z}_p} dx,\\ &= |p^{-r}|_p \int_{\mathbb{Z}_p} dy,\\ &= p^r.\end{aligned}$$

Ahora bien, para

$$\int_{S_{p^r}(a)} dx.$$

Se tiene en cuenta que

$$B_{p^r}(a) = S_{p^r}(a) \sqcup B_{p^{r-1}}(a),$$

por lo tanto

$$\begin{aligned}\int_{S_{p^r}(a)} dx &= \int_{B_{p^r}(a)} dx - \int_{B_{p^{r-1}}(a)} dx,\\ &= p^r - p^{r-1},\\ &= p^r(1-p^{-1}).\end{aligned}$$

Un último resultado que será de utilidad para el desarrollo de este trabajo, permite calcular la integral sobre la función caracter.

Ejemplo 9.2. *[3]*

$$\int_{B_{p^r}(0)} e(\xi x)dx = \begin{cases} p^r, & si \quad |\xi|_p \leq p^{-r},\\ 0, & si \quad |\xi|_p \geq p^{-r+1}.\end{cases}$$

En efecto, si $|\xi|_p \leq p^{-r}$ *se tiene que* $|\xi x|_p \leq 1$ *por lo tanto* $e(\xi x) = 1$*, así*

$$\begin{aligned}\int_{B_{p^r}(0)} e(\xi x)dx &= \int_{B_{p^r}(0)} dx,\\ &= p^r,\end{aligned}$$

ahora bien, si $|\xi|_p \geq p^{-r+1}$*, entonces para* $x' \in S_{p^r}(0)$*, se cumple que* $B_{p^r}(0) = B_{p^r}(x')$*, luego se tiene que* $|\xi x'|_p \geq p$*, por lo tanto* $e(\xi x') \not\equiv 1$*, así se se hace la sustitución* $x = y - x'$ *y se obtiene que* $dx = dy$*, por lo tanto,*

$$\begin{aligned}\int_{B_{p^r}(0)} e(\xi x)dx &= \int_{B_{p^r}(x')} e(\xi(y-x'))dy,\\ \int_{B_{p^r}(0)} e(\xi x)dx &= \int_{B_{p^r}(x')} e(\xi y)e(-\xi x')dy,\\ \int_{B_{p^r}(0)} e(\xi x)dx &= e(-\xi x')\int_{B_{p^r}(0)} e(\xi y)dy,\\ (1-e(-\xi x'))\int_{B_{p^r}(0)} e(\xi x)dx &= 0,\end{aligned}$$

con lo que se concluye que

$$\int_{B_{p^r}(0)} e(\xi x)dx = 0,$$

con esto se puede ver que

$$\int_{S_{p^r}(0)} e(\xi x) = \begin{cases} p^r(1-p^{-1}) & si \quad |\xi|_p \leq p^{-r},\\ -p^{r-1} & si \quad |\xi|_p = p^{-r+1},\\ 0 & si \quad |\xi|_p \geq p^{-r+2}.\end{cases}$$

Para extender estas idea a dimensión n, se tiene que

$$\mathbb{Q}_p^n = \mathbb{Q}_p \times \mathbb{Q}_p \times \ldots \times \mathbb{Q}_p,$$

y sobre el cual define la norma

$$||x||_p = \text{máx}_{1\leq j\leq n}|x_j|_p.$$

Se puede verificar de manera sencilla que la anterior norma es no arquimediana.

Este espacio hereda de $\mathbb{Q}_p$ varias características, entre ellas tener une medida de Haar que se notará por $d^n x$ y hasta se puede normalizar de la siguiente manera.

$$\int_{\mathbb{Z}_p^n} d^n x = 1.$$

Un último resultado importante en este trabajo es el siguiente.

Teorema 9.2. *Teorema de Fubini. Sea* $f(x,y)$ *con* $x \in \mathbb{Q}_p^n$ *e* $y \in \mathbb{Q}_p^m$ *tal que la integral iterada*

$$\int_{\mathbb{Q}_p^n}\left(\int_{\mathbb{Q}_p^m} f(x,y)dy\right)dx,$$

existe, entonces la función f *es integrable sobre* $\mathbb{Q}_p^{n+m}$ *y todas las integrales iteradas de* f *existen, y*

$$\int_{\mathbb{Q}_p^n}\left(\int_{\mathbb{Q}_p^m} f(x,y)dy\right)dx = \int_{\mathbb{Q}_p^{n+m}} f(x,y)dydx = \int_{\mathbb{Q}_p^m}\left(\int_{\mathbb{Q}_p^n} f(x,y)dx\right)dy,$$

de forma contraria, si una función f *es (absolutamente) integrable sobre* $\mathbb{Q}_p^{n+m}$ *entonces todas las integrales iteradas existen y son iguales entre ellas.*

Ejercicios 3

1. Escribir el número entero 2351 en base 5.

2. Escriba la operación $60 - 16$ en base 3.

3. Escribir el desarrollo 7-ádico de -12.

4. Pruebe que si $p \neq 2$, una unidad p-ádica $u = c_0 + c_1 p + c_2 p^2 + \ldots$ es un cuadrado en $\mathbb{Z}_p$ si y solo si c_0 es un residuo cuadrático módulo p.

5. Muestre que
$$\int_{\mathbb{Z}_p} \ln(|x|_p)dx = -\frac{\ln(p)}{p-1}.$$

10. La fórmula de la fase estacionaria

La fórmula de la fase estacionaria es un método elemental para calcular integrales $p-$ádicas.

Definición 10.1. *Se dice que* $f(x) = \sum c_i x^i \in \mathbb{Q}_p[[x_1, \cdots, x_n]]$ *es una* ***serie de potencias especial restringida****, abreviada SRP, si* $f(0) = 0$*, es decir* $c_0 = 0$*, y* $c_i \equiv 0 \pmod{p^{|i|-1}}$ *para cualquier* $i \in \mathbb{N}^n, i \neq 0$*, donde* $|i| = i_1 + \cdots + i_n$.

Lema. 1. Sea $f_i(x) \in \mathbb{Z}_p[[x_1, \cdots, x_n]]$, para $i = 1, \cdots, n$, si cada $f_i(x)$ en $f(x) = (f_1(x), \cdots, f_n(x))$ es SRP en $x_1, \cdots, x_n$ y $det \left[\frac{\partial f_i}{x_j}\right] \not\equiv 0 \pmod{p}$, entonces la función bicontinua de $\mathbb{Z}_p^n$ en $\mathbb{Z}_p^n$ definida por $y = f(x)$ preserva la medida de Haar de $\mathbb{Q}_p^n$.

Se identifica al conjunto $\mathbb{F}_p$ con $\{0, 1, \cdots, p-1\}$. Sea "$-$" la función reducción módulo p, es decir, la función

$$\begin{array}{rcl} \mathbb{Z}_p & \longrightarrow & \mathbb{F}_p \\ x_0 + p(\cdots) & \longrightarrow & x_0. \end{array}$$

Esta función puede extenderse a $\mathbb{Z}_p^n \longrightarrow \mathbb{F}_p^n$. La reducción módulo p de un subconjunto $E \subset \mathbb{Z}_p^n$ será denotado por $\overline{E} \subset \mathbb{F}_p^n$. Si $f(x) \in \mathbb{Z}_p[x_1, \cdots, x_n] \setminus p\mathbb{Z}_p[x_1, \cdots, x_n]$ entonces $\overline{f}$ denota su reducción módulo p.
Si A es un conjunto finito $\#A$ denota su número de elementos.

Fórmula de la fase estacionaria

Sea $\overline{E} \subset \mathbb{F}_p^n$ y se denota por $\overline{S}$ el subconjunto de $\overline{E}$ que consiste en todos los $\overline{a} \in \overline{E}$ tales que $\overline{f}(\overline{a}) = \frac{\partial \overline{f}}{\partial x_i}(\overline{a}) = 0$ para $1 \leq i \leq n$. Sean S y E las pre-imagenes de $\overline{S}$ y $\overline{E}$ bajo $\mathbb{Z}_p^n \longrightarrow \mathbb{F}_p^n$ y sea N el número de ceros de $\overline{f}(x)$ en $\overline{E}$. Entonces la función zeta asociada al polinomio $f(x)$ está dada por:

$$\int_E |f(x)|_p^s d^n x = p^{-n}(\#\overline{E} - N) + \frac{p^{-n-s}(1-p^{-1})(N - \#\overline{S})}{1-p^{-1-s}} + \int_S |f(x)|_p^s d^n x.$$

Demostración. Por definición

$$E = \bigsqcup_{\overline{a} \in \overline{E}} a + (p\mathbb{Z}_p)^n.$$

Luego,

$$\begin{aligned}
\int_E |f(x)|_p^s d^n x &= \sum_{\overline{a} \in \overline{E}} \int_{a+(p\mathbb{Z}_p)^n} |f(x)|_p^s d^n x, \\
&= \sum_{\overline{a} \in \overline{E} \setminus \overline{S}} \int_{a+(p\mathbb{Z}_p)^n} |f(x)|_p^s d^n x + \sum_{\overline{a} \in \overline{S}} \int_{a+(p\mathbb{Z}_p)^n} |f(x)|_p^s d^n x, \\
&= \sum_{\overline{a} \in \overline{E} \setminus \overline{S}} \int_{a+(p\mathbb{Z}_p)^n} |f(x)|_p^s d^n x + \int_S |f(x)|_p^s d^n x, \\
&= \sum_{\overline{a} \in \overline{E} \setminus \overline{S}} \int_{\mathbb{Z}_p^n} |f(a+px)|_p^s |p^n|_p d^n x + \int_S |f(x)|_p^s d^n x, \\
&= p^{-n} \sum_{\overline{a} \in \overline{E} \setminus \overline{S}} \int_{\mathbb{Z}_p^n} |f(a+px)|_p^s d^n x + \int_S |f(x)|_p^s d^n x.
\end{aligned}$$

Tomando $\overline{a} \in \overline{E} - \overline{S}$ tal que $\overline{f}(\overline{a}) \neq 0$ se tiene $|f(a+px)|_p = 1$, en este caso

$$\int_{\mathbb{Z}_p^n} |f(a+px)|_p^s d^n x = \int_{\mathbb{Z}_p^n} d^n x = 1.$$

El número de estos $\overline{a}$ es $\#\overline{E} - N$. Así, la contribución de estos $\overline{a}$ es $p^{-n}(\#\overline{E} - N)$.

Sea ahora $\overline{a} \in \overline{E} - \overline{S}$ tal que $\overline{f}(\overline{a}) = 0$, $\frac{\partial \overline{f}}{\partial x_i}(\overline{a}) \neq 0$ para algún i, sin pérdida de generalidad se puede suponer que $i = 1$.
Se define

$$g_i(x) = \begin{cases} \frac{f(a+px)-f(a)}{p}, & \text{si } i = 1, \\ \\ x_i, & \text{si } i > 1. \end{cases}$$

Se tiene que las funciones $g_1(x), \cdots, g_n(x)$ son SRP's en $x_1, \cdots, x_n$ y
$det[\frac{\partial g_i}{\partial x_j}(0)] = \frac{\partial f}{\partial x_1}(0) \not\equiv 0 \pmod{p}$.
Por el Lema 1 $(y_1, \cdots, y_n) = (g_1(x), \cdots, g_n(x))$ es una función de $\mathbb{Z}_p^n$ en $\mathbb{Z}_p^n$ que preserva la medida de Haar.
Así,

$$\begin{aligned}
\int_{\mathbb{Z}_p^n} |f(a+px)|_p^s d^n x &= \int_{\mathbb{Z}_p} |py_1 + f(a)|_p^s dy_1, \\
&= p^{-s} \int_{\mathbb{Z}_p} \left| y_1 + \frac{f(a)}{p} \right|_p^s dy_1, \\
&= p^{-s} \int_{\mathbb{Z}_p} |y_1|_p^s dy_1 = p^{-s} \frac{1-p^{-1}}{1-p^{-1-s}}.
\end{aligned}$$

Está última integral ya se calculó, el número de estos $\overline{a}$ es $N - \#\overline{S}$. Así, la contribución de estos $\overline{a}$ es

$$\frac{p^{-n-s}(1-p^{-1})(N-\#\overline{S})}{1-p^{-1-s}}.$$

Por tanto,

$$\int_E |f(x)|_p^s d^n x = p^{-n}(\#\overline{E}-N) + \frac{p^{-n-s}(1-p^{-1})(N-\#\overline{S})}{1-p^{-1-s}} + \int_S |f(x)|_p^s d^n x.$$

$\square$

Observación 6

Tomando

$$f(a+px) := p^{e_a}\widetilde{f}(x) \qquad con \qquad \widetilde{f}(x) \in \mathbb{Z}_p[x_1,\cdots,x_n] \setminus p\mathbb{Z}_p[x_1,\cdots,x_n]$$

y

$$L(p^{-s}) = (1-p^{-1-s})(p^{-n}(\#\overline{E}-N)) + p^{-n-s}(1-p^{-1})(N-\#\overline{S}).$$

La fórmula de la fase estacionaria, abreviada FFE, puede ser re-escrita como

$$\begin{aligned}
\int_E |f(x)|_p^s d^n x &= \frac{L(p^{-s})}{1-p^{-1-s}} + \int_S |f(x)|_p^s d^n x, \\
&= \frac{L(p^{-s})}{1-p^{-1-s}} + p^{-n}\sum_{\overline{a}\in\overline{S}} \int_{\mathbb{Z}_p^n} |f(a+px)|_p^s d^n x, \\
&= \frac{L(p^{-s})}{1-p^{-1-s}} + p^{-n-e_a s}\sum_{\overline{a}\in\overline{S}} \int_{\mathbb{Z}_p^n} |\widetilde{f}(x)|_p^s d^n x.
\end{aligned}$$

Se puede aplicar nuevamente FFE a cada una de las integrales $\int_{\mathbb{Z}_p^n} |\widetilde{f}(x)|_p^s d^n x$.
Igusa conjeturó que aplicando recursivamente FFE es posible establecer la racionalidad de integrales del tipo $\int_E |f(x)|_p^s d^n x$, en el caso en que el polinomio f tiene coeficientes en un campo completo no arquimediano de característica arbitraria.

Observación 7

Sea $f(x) \in \mathbb{Z}_p[x_1,\cdots,x_n] \setminus p\mathbb{Z}_p[x_1,\cdots,x_n]$. Si el sistema de ecuaciones

$$\overline{f}(\overline{a}) = \frac{\partial \overline{f}}{\partial x_i}(\overline{a}) = 0, \quad 1 \le i \le n,$$

no tiene soluciones en $\mathbb{F}_p^n$ entonces $S = \emptyset$ y por FFE,

$$Z(s,f) = p^{-n}(\#\overline{E}-N) + \frac{p^{-n-s}(1-p^{-1})(N)}{1-p^{-1-s}}.$$

Ejemplo 10.1. *1. Sea $f(x,y) = x^4 + bx^2y^2 + y^4 \in \mathbb{Z}_p[x,y]$ donde $b^2 \not\equiv 4 \pmod p$ y $p \neq 2$.*

Para calcular la función zeta asociada a este polinomio se procede a utilizar la FFE.

Se tiene $\overline{E} = \mathbb{F}_p^2$ y $E = \mathbb{Z}_p^2$. Para calcular S se tiene que resolver el sistema

$$\begin{aligned}
\overline{f}(x,y) &= x^4 + \overline{b}x^2y^2 + y^4 = 0, \\
\frac{\partial \overline{f}(x,y)}{\partial x} &= 4x^3 + 2\overline{b}y^2x = 0, \\
\frac{\partial \overline{f}(x,y)}{\partial y} &= 4y^3 + 2\overline{b}x^2y = 0,
\end{aligned}$$

en $\mathbb{F}_p$. Una solución es $x = y = 0$ y se cumple $x = 0$ si y sólo $y = 0$. Suponiendo que $x, y \neq 0$ entonces

$$\begin{aligned}
4x^3 + 2\overline{b}y^2x = 0 &\Longrightarrow 2x(2x^2 + \overline{b}y^2) = 0 \Longrightarrow 2x^2 + \overline{b}y^2 = 0, \\
4y^3 + 2\overline{b}x^2y = 0 &\Longrightarrow 2y(2y^2 + \overline{b}x^2) = 0 \Longrightarrow 2y^2 + \overline{b}x^2 = 0, \\
&\Longrightarrow x^2 = -2^{-1}\overline{b}y^2 \ \wedge y^2 = -2^{-1}\overline{b}x^2 \\
&\Longrightarrow x^2 = -2^{-1}\overline{b}(-2^{-1}\overline{b}x^2) = 4^{-1}\overline{b}^2x^2 \\
&\Longrightarrow 4 = \overline{b}^2 \qquad \textit{contradicción a la hipótesis.}
\end{aligned}$$

Así, $\overline{S} = \{(0,0)\}$ y $S = p\mathbb{Z}_p \times p\mathbb{Z}_p$.
Aplicando FFE se obtiene

$$\begin{aligned}
Z(s,f) &= p^{-2}(p^2 - N) + \frac{p^{-2-s}(1-p^{-1})(N-1)}{1-p^{-1-s}} \\
&+ \int_{p\mathbb{Z}_p \times p\mathbb{Z}_p} |x^4 + bx^2y^2 + y^4|_p^s dxdy.
\end{aligned}$$

Haciendo el cambio de variables $x = pu$, $y = pv$ donde $u, v \in \mathbb{Z}_p$ se obtiene $dxdy = p^{-2}dudv$ y entonces

$$\begin{aligned}
Z(s,f) &= p^{-2}(p^2 - N) + \frac{p^{-2-s}(1-p^{-1})(N-1)}{1-p^{-1-s}} + \\
&\quad + \int_{\mathbb{Z}_p \times \mathbb{Z}_p} |p^4u^4 + bp^4u^2v^2 + p^4v^4|_p^s p^{-2} dudv, \\
&= p^{-2}(p^2 - N) + \frac{p^{-2-s}(1-p^{-1})(N-1)}{1-p^{-1-s}} + \\
&\quad + p^{-4s-2} \int_{\mathbb{Z}_p \times \mathbb{Z}_p} |u^4 + bu^2v^2 + v^4|_p^s dudv, \\
&= p^{-2}(p^2 - N) + \frac{p^{-2-s}(1-p^{-1})(N-1)}{1-p^{-1-s}} + p^{-4s-2} Z(s,f).
\end{aligned}$$

Por lo tanto,

$$Z(s,f) = \frac{1}{1-p^{-4s-2}} \left\{ p^{-2}(p^2 - N) + \frac{p^{-2-s}(1-p^{-1})(N-1)}{1-p^{-1-s}} \right\}.$$

2. *Sea $f(x,y) = px + x^2 - y^3 \in \mathbb{Z}_p$ donde $p \neq 2, 3$. Con la notación de la FFE se tiene $\overline{E} = \mathbb{F}_p^2$ y $E = \mathbb{Z}_p^2$.*
   Para encontrar $\overline{S}$ se tiene que resolver el sistema de ecuaciones

$$\begin{aligned}
\overline{f}(x,y) &= x^2 - y^3 = 0, \\
\frac{\partial \overline{f}(x,y)}{\partial x} &= 2x = 0, \\
\frac{\partial \overline{f}(x,y)}{\partial y} &= -3y^2 = 0,
\end{aligned}$$

   sobre $\mathbb{F}_p$. Se tiene

$$\begin{aligned}
2x = 0 &\Longrightarrow x = 0, \\
-3y^2 = 0 &\Longrightarrow y = 0.
\end{aligned}$$

   Así, $\overline{S} = \{(0,0)\}$ y entonces $S = p\mathbb{Z}_p \times p\mathbb{Z}_p$.

   Para encontrar N, hay que resolver $x^2 - y^3 = 0$ en $\mathbb{F}_p$. Una solución es $x = 0$ y $y = 0$, además se cumple que $x = 0$ si y sólo si $y = 0$. Por otro lado, sea g un generador de $(\mathbb{Z}/p\mathbb{Z})^\times$, escribiendo $x = g^t$ y $y = g^k$ donde t y k pertenecen al conjunto $\{1, 2, \cdots, p-1\}$, la ecuación $x^2 - y^3 = 0$ es equivalente a la ecuación $g^{3k} \equiv g^{2t} \pmod{p}$, que se convierte en la ecuación sobre los exponentes $3k \equiv 2t \pmod{p-1}$. Para la última ecuación se distinguen dos casos:

a) *Si m.c.d*$(3, p-1) = 1$ *entonces* $3k \equiv 2t \pmod{p-1}$ *tiene solución única en la variable* k *para cada* $t \in \{1, 2, \cdots, p-1\}$. *Así, hay* $p-1$ *soluciones.*

b) *Si m.c.d.*$(3, p-1) = 3$ *entonces la ecuación* $3k \equiv 2t \pmod{p}$ *tiene solución para* k *si y sólo si* $2t \equiv 0 \pmod{3}$, *hay exactamente* $\frac{p-1}{3}$ *valores de* t *que son múltiplos de* 3. *Luego, fijando* t *tal que* $2t \equiv 0 \pmod{3}$ *hay exactamente m.c.d.*$(3, 2t) = 3$ *soluciones de* $3k \equiv 2t \pmod{p} - 1$ *en la variable* k. *Así, hay* $3(\frac{p-1}{3}) = p-1$ *soluciones.*

Por tanto, hay p *soluciones de* $x^2 - y^3 = 0$ *en* $\mathbb{F}_p$, *es decir,* $N = p$.

Aplicando la FFE se obtiene

$$\begin{aligned} Z(s,f) &= p^{-2}(p^{-2}-p) + \frac{p^{-2-s}(1-p^{-1})(p-1)}{1-p^{-1-s}} \\ &+ \int_{p\mathbb{Z}_p \times p\mathbb{Z}_p} |px + x^2 - y^3|_p^s dxdy. \end{aligned}$$

Haciendo el cambio de variables $x = pu$ *y* $y = pv$ *con* $u, v \in \mathbb{Z}_p$ *en la última integral, se obtiene*

$$\begin{aligned} Z(s,f) &= p^{-2}(p^{-2}-p) + \frac{p^{-2-s}(1-p^{-1})(p-1)}{1-p^{-1-s}} + \\ &+ p^{-2}\int_{\mathbb{Z}_p^2} |p^2u + p^2u^2 - p^3v^3|_p^s dudv, \\ &= p^{-2}(p^{-2}-p) + \frac{p^{-2-s}(1-p^{-1})(p-1)}{1-p^{-1-s}} + \\ &+ p^{-2-2s}\int_{\mathbb{Z}_p^2} |u + u^2 - pv^3|_p^s dudv. \end{aligned}$$

Para aplicar la FFE al polinomio $g(u,v) = u + u^2 - pv^3$ *se tiene* $\overline{E} = \mathbb{F}_p^2$ *y* $E = \mathbb{Z}_p^2$.

Ahora, el sistema de ecuaciones

$$\begin{aligned} \overline{g}(u,v) &= u + u^2 = 0, \\ \frac{\partial \overline{g}(u,v)}{\partial u} &= 1 + 2u = 0, \\ \frac{\partial \overline{g}(u,v)}{\partial v} &= 0. \end{aligned}$$

no tiene soluciones, entonces $\overline{S} = \emptyset$.
Además, $\{(m,n) \in \mathbb{F}_p^2 : u + u^2 = 0\} = \{(0,n) : n \in \mathbb{F}_p\} \cup \{(-1,m) : m \in \mathbb{F}_p\}$, *luego el número de ceros de* $u + u^2 = 0$ *en* $\mathbb{F}_p$ *es* $2p$.
Aplicando la FFE al polinomio g *se obtiene*

$$Z(s,g) = \int_{\mathbb{Z}_p^2} |u + u^2 - pv^3|_p^s dudv = p^{-2}(p^2 - 2p) + \frac{p^{-2-s}(1-p^{-1})2p}{1-p^{-1-s}}.$$

Por tanto,

$$\begin{aligned} Z(s,f) &= p^{-2}(p^{-2}-p) + \frac{p^{-2-s}(1-p^{-1})(p-1)}{1-p^{-1-s}} \\ &+p^{-2-2s}\left\{p^{-2}(p^2-2p) + \frac{2p^{-1-s}(1-p^{-1})}{1-p^{-1-s}}\right\}. \end{aligned}$$

Ejercicios 4

1. Calcular la integral $\int_E |f(x)|_p^s d^n x$, si $f(x) = x^2 - p$.
.
2. Calcular la integral $\int_E |f(x)|_p^s d^n x$, si $f(x,y) = px + x^2 - y^3 \in \mathbb{Z}_p$ donde $p \neq 2, 3$.

11. Solución

Ejercicios 1:

1. Escribiendo 18 en sus factores primos se tiene que
$$18 = 2 * 3^2,$$
por lo tanto
$$\nu_3(18) = 3.$$
Escribiendo 1728 en sus factores primos se tiene que
$$1728 = 2^6 * 3^3,$$
por lo tanto
$$\nu_2(1728) = 6.$$
Teniendo en cuenta que cuando $x \in \mathbb{Q}$ con $x = a/b$ entonces
$$\nu_p(x) = \nu_p(a) - \nu_p(b),$$
ahora bien, escribiendo 49 en sus factores primos se tiene que
$$49 = 7^2,$$
además, escribiendo 50 en sus factores primos se tiene que
$$50 = 2 * 5^2,$$
por lo tanto
$$\begin{aligned} \nu_5\left(\frac{49}{50}\right) &= \nu_5(49) - \nu_5(50), \\ &= 0 - 2, \\ &= -2. \end{aligned}$$

2. Teniendo en cuenta que si $x \in \mathbb{Q}$ se tiene
$$|x|_p = p^{-\nu_p(x)},$$
entonces.
Escribiendo 9 en sus factores primos se tiene
$$9 = 3^3,$$
así $\nu_3(9) = 2$, por lo tanto
$$|9|_3 = 3^{-2}.$$
Escribiendo 24 en sus factores primos se tiene
$$24 = 2^3 * 3,$$
así $\nu_2(24) = 3$, por lo tanto
$$|24|_2 = 2^{-3}.$$
Escribiendo 24 en sus factores primos se tiene
$$24 = 2^3 * 3,$$
así $\nu_2(24) = 3$, por lo tanto
$$|24|_2 = 2^{-3}.$$
Escribiendo 15 en sus factores primos se tiene
$$24 = 3 * 5,$$
además, escribiendo 28 en sus factores primos se tiene
$$24 = 2^2 * 7,$$
se tiene entonces
$$\begin{aligned} \nu_7\left(\frac{15}{28}\right) &= \nu_7(15) - \nu_7(28), \\ &= 0 - 1. \\ &= -1. \end{aligned}$$
por lo tanto
$$\left|\frac{15}{28}\right|_7 = 7^{-1}.$$

3. El enunciado de este problema se puede leer como. Sea $\mathbb{F}$ un campo, entonces $\mathbb{F}$ no tiene divisores de cero. Esta demostración será efectuada por reducción al absurdo. Suponga que $\mathbb{F}$ es un campo y que existen $a, b \in \mathbb{F}$ tal que $a, b \neq 0$ y $a * b = 0$, como $a * b = 0$ y $\mathbb{F}$ es un campo entonces se tiene que

$$\begin{aligned} a * b &= 0, \\ a^{-1} * a * b &= a^{-1} * 0, \\ e * b &= 0, \\ b &= 0. \end{aligned}$$

lo cual es una contradicción.

4. Teniendo en cuenta que si $x \in \mathbb{Q}_p$ entonces

$$x = \sum_{i=-n_0}^{\infty} a_i p^i,$$

donde, $n_0 \in \mathbb{N}$, $0 < a_{-n_0} \leq p-1$, $0 \leq a_i \leq p-1$ para $i = -n_0, -n_0+1, \ldots, 0, 1, \ldots$ y $\nu_p(x) = -n_0$, por lo tanto $|x|_p = p^{n_0}$, es bastante sencillo ver que la expresión $p-$ádica de $1/p$ se escribe tomando $n_0 = 1$, $a_{-n_0} = 1$ y $a_i = 0$ para $i = 0, 1, \ldots$.
Ahora bien, se quiere hallar la expresión $p-$ádica de $1/2$ para p primo, $p \neq 2$, es fácil notar que $\nu_p(1/2) = 0$ por lo tanto se tiene que

$$\frac{1}{2} = \sum_{i=0}^{\infty} b_i p^i$$

ahora bien, se tiene que

$$2 = \sum_{i=0} a_i p^i,$$

donde $a_0 = 2$ y $a_i = 0$, para $i = 1, 2, \ldots$, además

$$1 = \sum_{i=0} a_i p^i,$$

donde $a_0 = 1$ y $a_i = 0$ para $i = 1, 2, \ldots$, ahora bien como

$$2 * \frac{1}{2} = 1,$$

por la definición del producto en números $p-$ádicos se debe tener que

$$2 * b_0 \equiv 1 \mod p$$

esto implica que b_0 es congruente al inverso multiplicativo de 2 en el campo de p elementos, para calcularlo note lo siguiente

$$\begin{aligned} p+1 &\equiv 1 \mod p, \\ \frac{p+1}{2} &\equiv \frac{1}{2} \mod p, \end{aligned}$$

en la anterior ecuación modular se esta abusando de la notación, pero esta ecuación dice que el inverso multiplicativo de 2 en el campo de p elementos es congruente con $(p+1)/2$, como $0 < (p+1)/2 < p-1$ se tiene que

$$b_0 = \frac{p+1}{2}$$

de nuevo por la definición de la multiplicación en los números $p-$ádicos se tiene que ahora se debe cumplir la ecuación

$$2b_1 + 1 \equiv 0 \mod p$$

esto implica que

$$\begin{aligned} 2b_1 + 1 &\equiv 0 \mod p, \\ 2b_1 &\equiv -1 \mod p, \\ 2b_1 &\equiv p-1 \mod p, \\ b_1 &\equiv \frac{p-1}{2} \mod p, \end{aligned}$$

como $0 < \frac{p-1}{2} < p-1$ se tiene que

$$b_1 = \frac{p-1}{2},$$

de aquí en adelante, por la definición de multiplicación en los números $p-$ ádicos se deberá siempre resolver la ecuación modular

$$2b_i + 1 \equiv 0 \mod p,$$

donde $i = 2, 3, \ldots$ por lo tanto se tendrá que

$$b_i = \frac{p-1}{2},$$

para $i = 2, 3, \ldots$, así

$$\frac{1}{2} = \frac{p+1}{2} + \frac{p-1}{2}\sum_{i=1}^{\infty} p^i.$$

5. Dado la expresión que se tiene de a se tiene que $\nu_p(a) = -m$, y dado que $|a|_p = |-a|_p$ se tiene que $\nu_p(-a) = -m$ por lo tanto

$$-a = \sum_{i=-m}^{\infty} b_i p^i$$

donde $0 < b_{-m} \leq p-1$ y $0 \leq b_i \leq p-1$, ahora bien, como $a + (-a) = 0$ se tiene por la definición de la suma en los números complejos que se debe cumplir que

$$a_{-m} + b_{-m} \equiv p \mod p,$$

esto implica que

$$b_{-m} \equiv p - a_{-m} \mod p,$$

como $0 < p - a_{-m} \leq p-1$ se tiene que

$$b_{-m} = p - a_{-m}.$$

Continuando, por la definición de la suma de números $p-$ ádicos se puede ver que para $i = -m+1, \ldots, 0, 1, \ldots, n$ se debe cumplir la ecuación modular

$$a_i + b_i + 1 \equiv p \mod p,$$

esto implica que

$$b_i \equiv p - a_i - 1 \mod p,$$

como

$$0 \leq p - a_i - 1 \leq p-1,$$

se tiene que

$$b_i = p - a_i - 1,$$

por último, de nuevo por la definición de la suma de los números $p-$ ádicos se tiene que para $i > n$ se debe cumplir la ecuación modular

$$b_i + 1 \equiv p \mod p,$$

lo que implica

$$b_i \equiv p - 1 \mod p,$$

por lo cual $b_i = p-1$, por lo tanto

$$-a = (p - a_{-m})p^{-m} + \sum_{i=-m+1}^{n} (p - a_i - 1)p^i + (p-1)\sum_{i=n+1}^{\infty} p^i.$$

6. Para resolver este ejercicio se toman los siguientes conjuntos

$$\begin{aligned} A_1 &= \{k \in \mathbb{N} : kp = p^n\}, \\ A_2 &= \{k \in \mathbb{N} : kp^2 = p^n\}, \\ A_3 &= \{k \in \mathbb{N} : kp^3 = p^n\}, \\ &\vdots \\ A_n &= \{k \in \mathbb{N} : kp^n = p^n\}. \end{aligned}$$

Se puede notar que el cardinal de cada uno de estos conjuntos es igual al aporte de cada múltiplo de $p, p^2, \ldots, p^n$ a la valuación $p-$ ádica de $p^n!$, ahora bien, se tiene que

$$\begin{aligned} \#(A_1) &= p^{n-1}, \\ \#(A_2) &= p^{n-2}, \\ \#(A_3) &= p^{n-3}, \\ &\vdots \\ \#(A_n) &= 1. \end{aligned}$$

por lo cual

$$\nu_p(p^n!) = \sum_{i=1}^{n} p^{n-i}.$$

7. Es claro que si $n < p$ entonces

$$\nu_p(n!) = 0$$

ahora bien, si $n > p$, sea $K = \max\{s \in \mathbb{N} : p^s \leq n\}$, entonces defina los siguientes conjuntos

$$\begin{aligned} A_1 &= \{k \in \mathbb{N} : kp \leq n\}, \\ A_2 &= \{k \in \mathbb{N} : kp^2 \leq n\}, \\ A_3 &= \{k \in \mathbb{N} : kp^3 \leq n\}, \\ &\vdots \\ A_K &= \{k \in \mathbb{N} : kp^K \leq n\}. \end{aligned}$$

Se puede notar que el cardinal de cada uno de estos conjuntos es igual al aporte de cada múltiplo de $p, p^2, \ldots, p^n$ a la valuación $p-$ ádica de $n!$, ahora bien, se tiene que

$$\begin{aligned} \#(A_1) &= \left\lfloor \frac{n}{p} \right\rfloor, \\ \#(A_2) &= \left\lfloor \frac{n}{p^2} \right\rfloor, \\ \#(A_3) &= \left\lfloor \frac{n}{p^3} \right\rfloor, \\ &\vdots \\ \#(A_K) &= \left\lfloor \frac{n}{p^K} \right\rfloor, \end{aligned}$$

por lo cual

$$\nu_p(n!) = \sum_{i=1}^{K} \left\lfloor \frac{n}{p^i} \right\rfloor.$$

8. Sea $x \in \mathbb{Z}_p \cap \mathbb{Q}$ por lo tanto $|x|_p \leq 1$ y $x = a/b$ con $(a, b) = 1$, como $|x|_p \leq 1$ se tiene que $\nu_p(x) \geq 0$, además $\nu_p(x) = \nu_p(a) - \nu_p(b)$, por lo cual, $\nu_p(a) - \nu_p(b) \geq 0$ como $(a, b) = 1$ se debe tener que $p|a$ o $p|b$ pero no ambas a la vez, si $p \nmid a$ entonces $p|b$ con lo que se tendrá que $\nu_p(x) = -\nu_p(b) < 0$, lo cual no es posible, por lo cual $p \mid b$, por lo tanto $x \in \{a/b : p \nmid b\}$.
   Sea $x \in \mathbb{Z}_p^\times \cap \mathbb{Q}$ por lo tanto $|x|_p = 1$ y $x = a/b$ con $(a, b) = 1$, como $|x|_p = 1$ se tiene que $\nu_p(x) = 0$, ademÃ¡s $\nu_p(x) = \nu_p(a) - \nu_p(b)$, por lo cual, $\nu_p(a) - \nu_p(b) = 0$, o lo que es lo mismo $\nu_p(a) = \nu_p(b)$ como $(a, b) = 1$ se debe tener que $p \nmid a$ y $p \nmid b$, por lo tanto $x \in \{a/b : \ p \nmid a \ \text{ y } \ p \nmid b\}$.

Ejercicios 2:

1. Note que

$$\begin{aligned} n! * n &= n! * ((n+1) - 1), \\ &= (n+1)! - n!, \end{aligned}$$

por lo tanto

$$\begin{aligned} \sum_{n=1}^{N} n! * n &= \sum_{n=1}^{N} ((n+1)! - n!) \\ &= (N+1)! - 1 \end{aligned}$$

ahora bien, sea $\epsilon > 0$, se tiene que

$$\begin{aligned} \left| \sum_{n=1}^{N} n! * n - (-1) \right|_p &= \left| \sum_{n=1}^{N} n! * n + 1 \right|_p, \\ &= |(N+1)! - 1 + 1|_p, \\ &= |(N+1)!|_p, \\ &= p^{-\nu_p((N+1)!)}. \end{aligned}$$

como

$$\lim_{N\to\infty} \nu_p((N+1)!) = \infty$$

se puede encontrar N tal que

$$p^{-\nu_p((N+1)!)} < \epsilon,$$

por lo cual

$$\left| \sum_{n=1}^{N} n! * n - (-1) \right|_p < \epsilon,$$

esto implica que

$$\sum_{n=1}^{\infty} n! * n = -1,$$

2. Note que

$$n^2(n+1)! = (n-1)(n+2)! - (n-2)(n+1)!.$$

por lo tanto

$$\begin{aligned}\sum_{n=1}^{N} n^2(n+1)! &= \sum_{n=1}^{N}((n-1)(n+2)! - (n-2)(n+1)!),\\ &= (N-1)(N+2)! + 2.\end{aligned}$$

ahora bien, sea $\epsilon > 0$, se tiene que

$$\begin{aligned}\left| \sum_{n=1}^{N} n^2(n+1)! - 2 \right|_p &= \left|((N-1)(N+2)! + 2 - 2\right|_p,\\ &= \left|((N-1)(N+2)!\right|_p,\\ &= p^{-\nu_p((N-1)(N+2)!)}.\end{aligned}$$

como

$$\lim_{N\to\infty} \nu_p((N-1)(N+2)!) = \infty$$

se puede encontrar N tal que

$$p^{-\nu_p((N-1)(N+2)!)} < \epsilon,$$

por lo cual

$$\left| \sum_{n=1}^{N} n^2(n+1)! - 2 \right|_p < \epsilon,$$

esto implica que

$$\sum_{n=1}^{\infty} n^2(n+1)! = 2.$$

Ejercicios 3

1. Se tiene que

$$\begin{aligned}2351 &= (470)(5) + 1\\ 470 &= (94)(5) + 0\\ 94 &= (18)(5) + 4\\ 18 &= (3)(5) + 3\end{aligned}$$

por lo cual nuestra expansión en base 5 es

$$2351 = 1 + 0 * 5 + 4 * 5^2 + 3 * 5^3 + 3 * 5^4.$$

2. Se tienen las expresiones $(\cdots 251453)_7$ y $(\cdots 121132)_7$ estas representan

$$\begin{aligned}(\cdots 251453)_7 &= 3 + 5 * 7 + 4 * 7^2 + 1 * 7^3 + 5 * 7^4 + 2 * 7^5,\\ (\cdots 121132)_7 &= 2 + 3 * 7 + 1 * 7^2 + 1 * 7^3 + 2 * 7^4 + 1 * 7^5,\end{aligned}$$

por lo cual

$$\begin{aligned}(\cdots 251453)_7+(\cdots 121132)_7 =&(3+2)+(5+3)*7+(4+1)*7^2+(1+1)*7^3+\\&+(5+2)*7^4+(2+1)*7^5,\\=&5+1*7+6*7^2+2*7^3+0*7^4+4*7^5.\end{aligned}$$

se obtiene que

$$(\cdots 251453)_7+(\cdots 121132)_7=(\cdots 402615)_7$$

.

3. Se tiene que

$$\begin{aligned}60&=20*3+0\\20&=6*3+2\\6&=3*2+0\end{aligned}$$

así $60=(\cdots 2020)_3$, ahora bien,

$$\begin{aligned}16&=5*3+1\\5&=1*3+2\end{aligned}$$

así $16=(\cdots 0121)_3$ por lo que se tiene que $-16=(\cdots 2102)_3$ así

$$\begin{aligned}60-16&=(\cdots 2020)_3+(\cdots 2102)_3\\&=(\cdots 1122)_3\end{aligned}$$

4. Se tiene que $(\cdots 0121)_3\times(\cdots 2020)_3$, y

$$\begin{aligned}(\cdots 0121)_3\times(\cdots 2020)_3 =&(0*1)+(0*2+2*1)*3+(0*1+2*2+0*1)*3^2\\&+(0*0+2*1+0*1+2*1)*3^3\\&+(0*0+2*0+0*1+2*2)*3^4\\&+(0*0+2*0+0*0+2*1)*3^5\\&+(0*0+2*0+0*0+2*0)*3^6\\=&2*3+1*3^2+2*3^3+2*3^4+0*3^5+1*3^6\end{aligned}$$

por lo tanto,

$$(\cdots 0121)_3\times(\cdots 2020)_3=(\cdots 01022120)_3.$$

5. Se tiene que

$$12=7*1+5.$$

por lo tanto $12=(\cdots 00015)_7$ por lo cual $-12=(\cdots 6652)_7$.

6. Note primero que $\sqrt{3}\notin\mathbb{Q}_2$, en efecto, se busca un elemento

$$a=\sum_{i=0}^{\infty}a_i2^i$$

tal que

$$a^2=1+1*2+0*2^2+0*2^3+\cdots$$

de ahí que

$$a_0^2\cong 1(\text{mod }2),$$

por lo cual $a_0=1$ por lo que se tiene

$$\begin{aligned}(1+a_1*2)*(1+a_1*2)&=1+(a_1+a_1)*2+a_1^2*2^2,\\&=1+2a_1*2+a_1^2*2^2,\end{aligned}$$

se puede notar que aunque se tome $a_1=1$, no se podría cumplir la la igualdad.
ahora bien, se tiene el polinomio

$$f(x)=x^2-3,$$

entonces

$$\begin{aligned}x^2-3&\cong 0(\text{mod }2),\\x^2&\cong 1(\text{mod }2).\end{aligned}$$

así se tiene que $x=1$ es una raíz de $f(x)$ módulo 2, pero no tiene raíz en $\mathbb{Q}_2$, ya que $\sqrt{3}\notin\mathbb{Q}_2$.

7. Como u es un cuadrado en $\mathbb{Z}_p$ se tiene que la ecuación
$$x^2 - u = 0$$
tiene solución es $\mathbb{Z}_p$. Esto implica que
$$\begin{aligned} x^2 - u &\equiv 0(\text{mod } p) \\ x^2 &\equiv u(\text{mod } p) \end{aligned}$$
y dado que $c_0 \equiv u(\text{mod } p)$ se tiene
$$x^2 \equiv c_0(\text{mod } p)$$
por lo cual c_0 es un residuo cuadrático.
Ahora suponga que c_0 es un residuo cuadrático, entonces
$$x^2 \equiv c_0(\text{mod } p)$$
además
$$2c_0 \not\equiv 0(\text{mod } p)$$
por Lema de Hensel, el polinomio
$$f(x) = x^2 - u$$
tiene solución y además, esa solución es congruente con c_0 por lo tanto debe tener la forma
$$a = a_0 + a_1p + a_2p^2 + \dots$$
y cumple que
$$a_0^2 \equiv c_0(\text{mod } p)$$
por lo tanto u tiene la forma $u = c_0 + c_1p + c_2p^2 + \dots$

8. Se tiene el polinomio $f(x) = x^3 - 1$, asÃ
$$\begin{aligned} x^3 - 1 &\equiv 0 \mod 7 \\ x^3 &\equiv 1 \mod 7 \end{aligned}$$
se sabe que esta congruencia tiene como soluciones $x = 1$, $x = 2$ y $x = 4$, para resolver este ejercicio se usa $x = 2$, se tiene además que
$$\begin{aligned} f'(2) &= 3(2)^2, \\ &= 12, \\ &\equiv 5 \mod 7. \end{aligned}$$
por lo tanto $f'(2) \not\equiv 0 \mod 7$, así por Lema de Hensel existe un entero p-ádico a tal que $f(a) = 0$ y $a \equiv 2 \mod 7$, se sigue la construcción vista en la demostración del Lema de Hensel para hallar sus primeros tres dígitos p-ádicos.
primero suponga $a_1 = 2 + b_1 * 7$, entonces
$$\begin{aligned} f(a_1) &= (2 + b_1 * 7)^3 - 1, \\ &= (2)^3 + 3(2)^2b_1 * 7 + t + 7^2 - 1, \\ &= (2)^3 - 1 + 3(2)^2b_1 * 7 + t * 7^2, \\ &\equiv (2)^3 - 1 + 3(2)^2b_1 * 7 \mod 7^2, \\ &\equiv 1 * 7 + 3(2)^2b_1 * 7 \mod 7^2, \end{aligned}$$
por lo tanto
$$\begin{aligned} 1 + 3(2)^2b_1 &\equiv 0 \mod 7, \\ 12b_1 &\equiv 6 \mod 7, \\ 5b_1 &\equiv 6 \mod 7, \\ b_1 &\equiv 18 \mod 7, \\ b_1 &\equiv 4 \mod 7, \end{aligned}$$
entonces $a_1 = 2 + 4 * 7$, suponga ahora $a_2 = 2 + 4 * 7 + b_2 * 7^2$, se tiene entonces que
$$\begin{aligned} f(a_2) &\equiv (2 + 4 * 7)^3 - 1 + 3(2 + 4 * 7)^2b_27^2 \mod 7^3, \\ &\equiv 7 + 3(2)^2(4) * 7 + 3(2)(16)7^2 + 3(2 + 4 * 7)^2b_27^2 \mod 7^3, \\ &\equiv (1 + 3(2)^2(4)) * 7 + (96)7^2 + 3(2 + 4 * 7)^2b_27^2 \mod 7^3, \\ &\equiv (49) * 7 + (47 + 7^2)7^2 + 3(2 + 4 * 7)^2b_27^2 \mod 7^3, \\ &\equiv (47) * 7^2 + 3(2 + 4 * 7)^2b_2 * 7^2 \mod 7^3, \\ &\equiv 5 * 7^2 + 3(2 + 4 * 7)^2b_27^2 \mod 7^3. \end{aligned}$$

por lo tanto

$$\begin{aligned} 5+3(2+4*7)^2b_2 &\equiv 0 \quad \text{mód } 7,\\ 3(30)^2b_2 &\equiv 2 \quad \text{mód } 7,\\ 5b_2 &\equiv 2 \quad \text{mód } 7,\\ b_2 &\equiv 6 \quad \text{mód } 7. \end{aligned}$$

así $a_2 = 2+4*7+6*7^2$, y estos son lo tres dígitos p-ádicos que se busca.

9.
$$\int_{\mathbb{Q}_p} f(x)dx = \sum_{-\infty<\gamma<\infty} \int_{S_\gamma} f(x)dx$$

y además

$$\int_{S_\gamma} dx = p^\gamma(1-p^{-1}),$$

entonces se tiene que

$$\int_{\mathbb{Q}_p} f(|x|_p)dx = \sum_{-\infty<\gamma<\infty} \int_{S_\gamma} f(|x|_p)dx,$$

dado que $x \in S_\gamma$ se tiene que $|x|_p = p^\gamma$, así

$$\begin{aligned} \int_{\mathbb{Q}_p} f(|x|_p)dx &= \sum_{-\infty<\gamma<\infty} \int_{S_\gamma} f(|x|_p)dx,\\ &= \sum_{-\infty<\gamma<\infty} \int_{S_\gamma} f(p^\gamma)dx,\\ &= \sum_{-\infty<\gamma<\infty} f(p^\gamma)\int_{S_\gamma} dx,\\ &= \sum_{-\infty<\gamma<\infty} f(p^\gamma)p^\gamma(1-p^{-1}),\\ &= (1-p^{-1}) \sum_{-\infty<\gamma<\infty} f(p^\gamma)p^\gamma, \end{aligned}$$

por lo tanto se tiene que

$$\begin{aligned} \int_{\mathbb{Z}_p} \ln(|x|_p)dx &= (1-p^{-1}) \sum_{0\le\gamma<\infty} \ln(p^{-\gamma})p^{-\gamma},\\ &= -(1-p^{-1}) \sum_{0\le\gamma<\infty} \gamma\ln(p)p^{-\gamma},\\ &= -(1-p^{-1})\ln(p) \sum_{0\le\gamma<\infty} \gamma p^{-\gamma}, \end{aligned}$$

y dado que

$$\sum_{0\le\gamma<\infty} \gamma p^{-\gamma} = \frac{p}{(p-1)^2},$$

se tiene

$$\begin{aligned} \int_{\mathbb{Z}_p} \ln(|x|_p)dx &= (1-p^{-1}) \sum_{0\le\gamma<\infty} \ln(p^{-\gamma})p^{-\gamma},\\ &= -(1-p^{-1}) \sum_{0\le\gamma<\infty} \gamma\ln(p)p^{-\gamma},\\ &= -(1-p^{-1})\ln(p) \sum_{0\le\gamma<\infty} \gamma p^{-\gamma},\\ &= -\left(\frac{p-1}{p}\right)\ln(p)\left(\frac{p}{(p-1)^2}\right),\\ &= -\frac{\ln(p)}{p-1}. \end{aligned}$$

Ejercicios 4

1. $f(x) = x^2 - p \in \mathbb{Z}_p[x]$. Para calcular la función zeta asociada a este polinomio se procede a utilizar la FFE.
   Se tiene $\overline{E} = \mathbb{F}_p$ y $E = \mathbb{Z}_p$. Para calcular S se tiene que resolver el sistema

$$\overline{f}(x) = x^2 = 0$$
$$\frac{\partial \overline{f}}{\partial x}(x) = 2x = 0$$

   en $\mathbb{F}_p$. La única solución es $x = 0$, así $\overline{S} = \{0\}$, $S = p\mathbb{Z}_p$ y $N = 1$, por lo que

$$\begin{aligned} Z(s,f) &= p^{-1}(p-1) + \frac{p^{-1-s}(1-p^{-1})(1-1)}{1-p^{s-1}} + \int_{p\mathbb{Z}_p} |x^2 - p|_s^p dx \\ &= p^{-1}(p-1) + \int_{p\mathbb{Z}_p} |x^2 - p|_p^s dx \end{aligned}$$

   haciendo el cambio de variable $x = pu$ se obtiene $dx = p^{-1}du$ y así

$$\begin{aligned} Z(s,f) &= p^{-1}(p-1) + \frac{p^{-1-s}(1-p)(1-1)}{1-p^{s-1}} + \int_{p\mathbb{Z}_p} |x^2 - p|_s^p dx, \\ &= p^{-1}(p-1) + \int_{p\mathbb{Z}_p} |(pu)^2 - p|_p^s p^{-1} du, \\ &= p^{-1}(p-1) + \int_{\mathbb{Z}_p} |p^2u^2 - p|_p^s p^{-1} du, \\ &= p^{-1}(p-1) + \int_{\mathbb{Z}_p} |p(pu^2 - 1)|_p^s p^{-1} du, \\ &= p^{-1}(p-1) + \int_{\mathbb{Z}_p} |p|_p^s (pu^2 - 1)|_p^s p^{-1} du, \\ &= p^{-1}(p-1) + p^{-s-1} \int_{\mathbb{Z}_p} |pu^2 - 1|_p^s du. \end{aligned}$$

   Ahora bien, aplicando FFE al polinomio $f(u) = pu^2 - 1$, se tiene que $\overline{E} = \mathbb{F}_p$ y $E = \mathbb{Z}_p$. Para calcular S se debe resolver el sistema

$$\overline{f}(u) = -1 = 0,$$
$$\frac{\partial \overline{f}}{\partial u}(u) = 0.$$

   en $\mathbb{F}_p$. Se puede notar que el sistema no tiene solución, así $S = \emptyset$ y además $N = 0$ por lo tanto

$$\int_{\mathbb{Z}_p} |pu^2 - 1|_p^s du = 1,$$

   por lo tanto

$$Z(s,f) = p^{-1}(p-1) + p^{-s-1}.$$

2. $f(x,y,z) = x^4 + y^3 + z^2 \in \mathbb{Z}_p[x,y,z]$, para calcular la función zeta asociada a este polinomio se procede a usar FFE.
   Se tiene que $\overline{E} = \mathbb{F}_p^3$ y $E = \mathbb{Z}_p^3$. Para calcular S se tiene que resolver el sistema

$$\overline{f}(x,y,z) = x^4 + y^3 + z^2 = 0,$$
$$\frac{\partial \overline{f}}{\partial x} = 4x^3 = 0,$$
$$\frac{\partial \overline{f}}{\partial y} = 3y^2 = 0,$$
$$\frac{\partial \overline{f}}{\partial z} = 2z = 0.$$

   en $\mathbb{F}_p$. La única solución es $x = 0$, $y = 0$ y $z = 0$ así $\overline{S} = \{0\}$ y $S = (p\mathbb{Z}_p)^3$, por lo que se obtiene

$$Z(s,f) = p^{-3}(p^3 - N) + \frac{p^{-3-s}(1-p^{-1})(N-1)}{1-p^{s-1}} + \int_{(p\mathbb{Z}_p)^3} |x^4 + y^3 + z^2|_p^s dxdydz,$$

haciendo el cambio de variable $x = pu$, $y = pv$ y $z = pw$ se obtiene $dxdydz = p^{-3}dudvdw$ y así

$$\begin{aligned}
Z(s,f) =& p^{-3}(p^3 - N) + \frac{p^{-3-s}(1-p^{-1})(N-1)}{1-p^{s-1}}, \\
&+ \int_{\mathbb{Z}_p^3} |(pu)^4 + (pv)^3 + (pw)^2|_p^s p^{-3} dudvdw, \\
=& p^{-3}(p^3 - N) + \frac{p^{-3-s}(1-p^{-1})(N-1)}{1-p^{s-1}}, \\
&+ \int_{\mathbb{Z}_p^3} |p^2|_p^s |p^2u^4 + pv^3 + w^2|_p^s p^{-3} dudvdw, \\
=& p^{-3}(p^3 - N) + \frac{p^{-3-s}(1-p^{-1})(N-1)}{1-p^{s-1}}, \\
&+ p^{-2s-3} \int_{\mathbb{Z}_p^3} |p^2u^4 + pv^3 + w^2|_p^s dudvdw.
\end{aligned}$$

De nuevo se aplica F.F.E, pero ahora a la integral

$$\int_{\mathbb{Z}_p^3} |p^2u^4 + pv^3 + w^2|_p^s dudvdw.$$

Se tiene que $\overline{E} = \mathbb{F}_p^3$, así $E = \mathbb{Z}_p^3$, ahora bien, para calcular S, con $g(u,v,w) = p^2u^4 + pv^3 + w^2$ se debe resolver el sistema

$$\begin{aligned}
\overline{g}(u,v,w) &= w^2 \\
\frac{\partial \overline{g}}{\partial u} &= 0, \\
\frac{\partial \overline{g}}{\partial v} &= 0, \\
\frac{\partial \overline{g}}{\partial w} &= 2w = 0,
\end{aligned}$$

por lo tanto $\overline{S} = \mathbb{F}_p^2 \times \{0\}$, por lo cual $S = \mathbb{Z}_p^2 \times p\mathbb{Z}_p$ y $N = p^2 + 1$, por lo cual

$$\begin{aligned}
\int_{\mathbb{Z}_p^3} |p^2u^4 + pv^3 + w^2|_p^s dudvdw =& p^{-3}(p^3 - (p^2+1)) + \frac{p^{-3-s}(1-p^{-1})((p^2+1)-(p^2+1))}{1-p^{-1-s}}, \\
&+ \int_{\mathbb{Z}_p^2 \times p\mathbb{Z}_p} |p^2u^4 + pv^3 + w^2|_p^s dudvdw, \\
=& p^{-3}(p^3 - (p^2+1)) + \int_{\mathbb{Z}_p^2 \times p\mathbb{Z}_p} |p^2u^4 + pv^3 + w^2|_p^s dudvdw,
\end{aligned}$$

haciendo la sustitución $w = pw_1$ se obtiene $p^{-1}dw_1$, así

$$\begin{aligned}
\int_{\mathbb{Z}_p^3} |p^2u^4 + pv^3 + w^2|_p^s dudvdw =& p^{-3}(p^3 - (p^2+1)) + \int_{\mathbb{Z}_p^2 \times p\mathbb{Z}_p} |p^2u^4 + pv^3 + w^2|_p^s dudvdw, \\
=& p^{-3}(p^3 - (p^2+1)) + \int_{\mathbb{Z}_p^3} |p^2u^4 + pv^3 + (pw_1)^2|_p^s p^{-1} dudvdw_1, \\
=& p^{-3}(p^3 - (p^2+1)) + \int_{\mathbb{Z}_p^3} |p^2u^4 + pv^3 + p^2w_1^2|_p^s p^{-1} dudvdw_1, \\
=& p^{-3}(p^3 - (p^2+1)) + \int_{\mathbb{Z}_p^3} |p|_p^s |pu^4 + v^3 + pw_1^2|_p^s p^{-1} dudvdw_1, \\
=& p^{-3}(p^3 - (p^2+1)) + p^{-s-1} \int_{\mathbb{Z}_p^3} |pu^4 + v^3 + pw_1^2|_p^s dudvdw_1,
\end{aligned}$$

de nuevo se repite el proceso con

$$\int_{\mathbb{Z}_p^3} |pu^4 + v^3 + pw_1^2|_p^s dudvdw_1 -$$

Así se tiene que $\overline{E} = \mathbb{F}_p^3$ así $E = \mathbb{Z}_p^3$, ahora bien, para calcular S, con $g(u,v,w) = pu^4 + v^3 + pw_1^2$ se debe resolver el sistema

$$\begin{aligned}
\overline{g}(u,v,w) &= v^3, \\
\frac{\partial \overline{g}}{\partial u} &= 0, \\
\frac{\partial \overline{g}}{\partial v} &= 3v^2 = 0, \\
\frac{\partial \overline{g}}{\partial w} &= 0,
\end{aligned}$$

por lo tanto $\overline{S} = \mathbb{F}_p \times \{0\} \times \mathbb{F}_p$, por lo cual $S = \mathbb{Z}_p \times p\mathbb{Z}_p \times \mathbb{Z}_p$ y $N = p^2 + 1$, por lo cual

$$\int_{\mathbb{Z}_p^3} |pu^4 + v^3 + pw_1^2|_p^s dudvdw_1 = p^{-3}(p^3 - (p^2+1)) + \int_{\mathbb{Z}_p \times p\mathbb{Z}_p \times \mathbb{Z}_p} |pu^4 + v^3 + pw_1^2|_p^s dudvdw_1$$

haciendo la sustitución $v = pv_1$, se tiene $dv = p^{-1}dv_1$, así

$$\begin{aligned}\int_{\mathbb{Z}_p^3} |pu^4 + v^3 + pw_1^2|_p^s dudvdw_1 &= p^{-3}(p^3 - (p^2+1)) + \int_{\mathbb{Z}_p^3} |pu^4 + (pv_1)^3 + pw_1^2|_p^s p^{-1} dudv_1dw_1 \\ &= p^{-3}(p^3 - (p^2+1)) + \int_{\mathbb{Z}_p^3} |pu^4 + p^3v_1^3 + pw_1^2|_p^s p^{-1} dudv_1dw_1 \\ &= p^{-3}(p^3 - (p^2+1)) + \int_{\mathbb{Z}_p^3} |p|_p^s |u^4 + p^2v_1^3 + w_1^2|_p^s p^{-1} dudv_1dw_1 \\ &= p^{-3}(p^3 - (p^2+1)) + p^{-s-1} \int_{\mathbb{Z}_p^3} |u^4 + p^2v_1^3 + w_1^2|_p^s dudv_1dw_1\end{aligned}$$

de nuevo se repite el proceso con

$$\int_{\mathbb{Z}_p^3} |u^4 + p^2v_1^3 + w_1^2|_p^s dudv_1dw_1.$$

Entonces se tiene que $\overline{E} = \mathbb{F}_p^3$ asÃ $E = \mathbb{Z}_p^3$, ahora bien, para calcular S, con $g(u,v,w) = u^4 + p^2v_1^3 + w_1^2$ se debe resolver el sistema

$$\begin{aligned}\overline{g}(u,v,w) &= u^4 + w_1^2, \\ \frac{\partial \overline{g}}{\partial u} &= 4u^3 = 0, \\ \frac{\partial \overline{g}}{\partial v} &= 0, \\ \frac{\partial \overline{g}}{\partial w} &= 2w_1 = 0,\end{aligned}$$

por lo tanto $\overline{S} = \{0\} \times \mathbb{F}^p \times \{0\}$, por lo cual $S = p\mathbb{Z}_p \times \mathbb{Z}_p \times p\mathbb{Z}_p$ y N_1, luego

$$\begin{aligned}\int_{\mathbb{Z}_p^3} |u^4 + p^2v_1^3 + w_1^2|_p^s dudv_1dw_1 =& p^{-3}(p^3 - N_1) + \frac{p^{-3-s}(1-p^{-1})(N_1 - (p+2))}{1-p^{-1-s}} + \\ &+ \int_{p\mathbb{Z}_p \times \mathbb{Z}_p \times p\mathbb{Z}_p} |u^4 + p^2v_1^3 + w_1^2|_p^s dudv_1dw_1\end{aligned}$$

haciendo la sustitución $u = pu_1$, $w_1 = pw_2$, se tiene $dudw_1 = p^{-2}du_1dw_2$, así

$$\begin{aligned}\int_{\mathbb{Z}_p^3} |u^4 + p^2v_1^3 + w_1^2|_p^s dudv_1dw_1 =& p^{-3}(p^3 - N_1) + \frac{p^{-3-s}(1-p^{-1})(N_1 - (p+2))}{1-p^{-1-s}}, \\ &+ \int_{\mathbb{Z}_p^3} |(pu_1)^4 + p^2v_1^3 + (pw_2)^2|_p^s p^{-2} du_1dv_1dw_2, \\ =& p^{-3}(p^3 - N_1) + \frac{p^{-3-s}(1-p^{-1})(N_1 - (p+2))}{1-p^{-1-s}} + \\ &+ \int_{\mathbb{Z}_p^3} |p^4u_1^4 + p^2v_1^3 + p^2w_2^2|_p^s p^{-2} du_1dv_1dw_2, \\ =& p^{-3}(p^3 - N_1) + \frac{p^{-3-s}(1-p^{-1})(N_1 - (p+2))}{1-p^{-1-s}} + \\ &+ \int_{\mathbb{Z}_p^3} |p^2|_p^s |p^2u_1^4 + v_1^3 + w_2^2|_p^s p^{-2} du_1dv_1dw_2, \\ =& p^{-3}(p^3 - N_1) + \frac{p^{-3-s}(1-p^{-1})(N_1 - (p+2))}{1-p^{-1-s}} + \\ &+ p^{-2s-2} \int_{\mathbb{Z}_p^3} |p^2u_1^4 + v_1^3 + w_2^2|_p^s du_1dv_1dw_2,\end{aligned}$$

de nuevo se repite el proceso con

$$\int_{\mathbb{Z}_p^3} |p^2u_1^4 + v_1^3 + w_2^2|_p^s du_1dv_1dw_2,$$

y se obtiene $\overline{E} = \mathbb{F}_p^3$ así $E = \mathbb{Z}_p^3$, ahora bien, para calcular S, con $g(u, v, w) = p^2u_1^4 + v_1^3 + w_2^2$ se debe resolver el sistema

$$\begin{aligned}\overline{g}(u, v, w) &= v_1^3 + w_2^2,\\ \frac{\partial \overline{g}}{\partial u} &= 0,\\ \frac{\partial \overline{g}}{\partial v} &= 3v_1^2 = 0,\\ \frac{\partial \overline{g}}{\partial w} &= 2w_2 = 0,\end{aligned}$$

por lo tanto $\overline{S} = \mathbb{F}_p \times \{0\} \times \{0\}$, por lo cual $S = \mathbb{Z}_p \times p\mathbb{Z}_p \times p\mathbb{Z}_p$ y N_2, por lo cual

$$\begin{aligned}\int_{\mathbb{Z}_p^3} |p^2u_1^4 + v_1^3 + w_2^2|_p^s du dv_1 dw_2 =& p^{-3}(p^3 - N_2) + \frac{p^{-3-s}(1 - p^{-1})(N_2 - (p + 2))}{1 - p^{1-s}} +\\ &+ \int_{\mathbb{Z}_p \times p\mathbb{Z}_p \times p\mathbb{Z}_p} |p^2u_1^4 + v_1^3 + w_2^2|_p^s du_1 dv_1 dw_2,\end{aligned}$$

haciendo la sustitución $v_1 = pv_2$, $w_2 = pw_3$ se tiene $dv_1dw_2 = p^{-2}dv_2dw_3$, así

$$\begin{aligned}\int_{\mathbb{Z}_p^3} |p^2u_1^4 + v_1^3 + w_2^2|_p^s du dv_1 dw_2 =& p^{-3}(p^3 - N_2) + \frac{p^{-3-s}(1 - p^{-1})(N_2 - (p + 2))}{1 - p^{1-s}} +\\ &+ \int_{\mathbb{Z}_p^3} |p^2u_1^4 + (pv_2)^3 + (pw_3)^2|_p^s p^{-2} du_1 dv_2 dw_3\\ =& p^{-3}(p^3 - N_2) + \frac{p^{-3-s}(1 - p^{-1})(N_2 - (p + 2))}{1 - p^{1-s}} +\\ &+ \int_{\mathbb{Z}_p^3} |p^2u_1^4 + p^3v_2^3 + p^2w_3^2|_p^s p^{-2} du_1 dv_2 dw_3,\\ =& p^{-3}(p^3 - N_2) + \frac{p^{-3-s}(1 - p^{-1})(N_2 - (p + 2))}{1 - p^{1-s}} +\\ &+ \int_{\mathbb{Z}_p^3} |p^2|_p^s |u_1^4 + pv_2^3 + w_3^2|_p^s p^{-2} du_1 dv_2 dw_3,\\ =& p^{-3}(p^3 - N_2) + \frac{p^{-3-s}(1 - p^{-1})(N_2 - (p + 2))}{1 - p^{1-s}} +\\ &+ p^{-2s-2} \int_{\mathbb{Z}_p^3} |u_1^4 + pv_2^3 + w_3^2|_p^s du_1 dv_2 dw_3,\end{aligned}$$

de nuevo se repite el proceso con

$$\int_{\mathbb{Z}_p^3} |u_1^4 + pv_2^3 + w_3^2|_p^s du dv_2 dw_3$$

Nuevamente se tiene que $\overline{E} = \mathbb{F}_p^3$ así $E = \mathbb{Z}_p^3$, ahora bien, para calcular S, con $g(u, v, w) = u_1^4 + pv_2^3 + w_3^2$ se debe resolver el sistema

$$\begin{aligned}\overline{g}(u, v, w) &= u_1^4 + w_2^2,\\ \frac{\partial \overline{g}}{\partial u} &= 4u_1^3 = 0,\\ \frac{\partial \overline{g}}{\partial v} &= 0,\\ \frac{\partial \overline{g}}{\partial w} &= 2w_2 = 0,\end{aligned}$$

por lo tanto $\overline{S} = \{0\} \times \mathbb{F}_p \times \{0\}$, por lo cual $S = p\mathbb{Z}_p \times \mathbb{Z}_p \times p\mathbb{Z}_p$ y N_3, por lo cual

$$\begin{aligned}\int_{\mathbb{Z}_p^3} |u_1^4 + pv_2^3 + w_3^2|_p^s du dv_2 dw_3 =& p^{-3}(p^3 - N_3) + \frac{p^{-3-s}(1 - p^{-1})(N_3 - (p + 2))}{1 - p^{-1-s}} +\\ &+ \int_{p\mathbb{Z}_p \times \mathbb{Z}_p \times p\mathbb{Z}_p} |u_1^4 + pv_2^3 + w_3^2|_p^s du_1 dv_2 dw_3\end{aligned}$$

haciendo la sustitución $u_1 = pu_2$, $w_3 = pw_4$, se tiene que $du_1dw_3 = p^{-2}du_2dw_4$, así

$$\begin{aligned}
\int_{\mathbb{Z}_p^3} |u_1^4 + pv_2^3 + w_3^2|_p^s dudv_2dw_3 =& p^{-3}(p^3 - N_3) + \frac{p^{-3-s}(1-p^{-1})(N_3-(p+2))}{1-p^{-1-s}} \\
&+ \int_{\mathbb{Z}_p^3} |(pu_2)^4 + pv_2^3 + (pw_4)^2|_p^s p^{-2} du_2dv_2dw_4, \\
=& p^{-3}(p^3 - N_3) + \frac{p^{-3-s}(1-p^{-1})(N_3-(p+2))}{1-p^{-1-s}} + \\
&+ \int_{\mathbb{Z}_p^3} |p^4u_2^4 + pv_2^3 + p^2w_4^2|_p^s p^{-2} du_2dv_2dw_4, \\
=& p^{-3}(p^3 - N_3) + \frac{p^{-3-s}(1-p^{-1})(N_3-(p+2))}{1-p^{-1-s}} + \\
&+ \int_{\mathbb{Z}_p^3} |p|_p^s |p^3u_2^4 + v_2^3 + pw_4^2|_p^s p^{-2} du_2dv_2dw_4, \\
=& p^{-3}(p^3 - N_3) + \frac{p^{-3-s}(1-p^{-1})(N_3-(p+2))}{1-p^{-1-s}} + \\
&+ p^{-s-2} \int_{\mathbb{Z}_p^3} |p^3u_2^4 + v_2^3 + pw_4^2|_p^s du_2dv_2dw_4,
\end{aligned}$$

de nuevo se repite el proceso con

$$\int_{\mathbb{Z}_p^3} |p^3u_2^4 + v_2^3 + pw_4^2|_p^s du_2dv_2dw_4$$

Así que $\overline{E} = \mathbb{F}_p^3$ así $E = \mathbb{Z}_p^3$, ahora bien, para calcular S, con $g(u,v,w) = p^3u_2^4 + v_2^3 + pw_4^2$ se debe resolver el sistema

$$\begin{aligned}
\overline{g}(u,v,w) &= v_2^3, \\
\frac{\partial \overline{g}}{\partial u} &= 0, \\
\frac{\partial \overline{g}}{\partial v} &= 3v_2^2 = 0, \\
\frac{\partial \overline{g}}{\partial w} &= 0,
\end{aligned}$$

por lo tanto $\overline{S} = \mathbb{F}_p \times \{0\} \times \mathbb{F}_p$, por lo cual $S = \mathbb{Z}_p \times p\mathbb{Z}_p \times \mathbb{Z}_p$ y $N_4 = 1$, entonces

$$\begin{aligned}
\int_{\mathbb{Z}_p^3} |p^3u_2^4 + v_2^3 + pw_4^2|_p^s du_2dv_2dw_4 =& p^{-3}(p^3 - 1) + \frac{p^{-3-s}(1-p^{-1})(1-(p+2))}{1-p^{-1-s}} \\
&+ \int_{\mathbb{Z}_p \times p\mathbb{Z}_p \times \mathbb{Z}_p} |p^3u_2^4 + v_2^3 + pw_4^2|_p^s du_1dv_2dw_3
\end{aligned}$$

haciendo la sustitución $v_2 = pv_3$ se tiene que $dv_2 = p^{-1}dv_3$, así

$$\begin{aligned}
\int_{\mathbb{Z}_p^3} |p^3u_2^4 + v_2^3 + pw_4^2|_p^s du_2dv_2dw_4 =& p^{-3}(p^3 - 1) + \frac{p^{-3-s}(1-p^{-1})(1-(p+2))}{1-p^{-1-s}} + \\
&+ \int_{\mathbb{Z}_p^3} |p^3u_2^4 + (pv_3)^3 + pw_4^2|_p^s p^{-1} du_1dv_3dw_4, \\
=& p^{-3}(p^3 - 1) + \frac{p^{-3-s}(1-p^{-1})(1-(p+2))}{1-p^{-1-s}} + \\
&+ \int_{\mathbb{Z}_p^3} |p^3u_2^4 + p^3v_3^3 + pw_4^2|_p^s p^{-1} du_1dv_3dw_4, \\
=& p^{-3}(p^3 - 1) + \frac{p^{-3-s}(1-p^{-1})(1-(p+2))}{1-p^{-1-s}} + \\
&+ \int_{\mathbb{Z}_p^3} |p|_p^s |p^2u_2^4 + p^2v_3^3 + w_4^2|_p^s p^{-1} du_1dv_3dw_4, \\
=& p^{-3}(p^3 - 1) + \frac{p^{-3-s}(1-p^{-1})(1-(p+2))}{1-p^{-1-s}} + \\
&+ p^{-s-1} \int_{\mathbb{Z}_p^3} |p^2u_2^4 + p^2v_3^3 + w_4^2|_p^s du_1dv_3dw_4,
\end{aligned}$$

de nuevo se repite el proceso con

$$\int_{\mathbb{Z}_p^3} |p^2u_2^4 + p^2v_3^3 + w_4^2|_p^s du_1 dv_3 dw_4.$$

Se tiene que $\overline{E} = \mathbb{F}_p^3$ asÃ $E = \mathbb{Z}_p^3$, ahora bien, para calcular S, con $g(u, v, w) = p^2u_2^4 + p^2v_3^3 + w_4^2$ se debe resolver el sistema

$$\begin{aligned}
\overline{g}(u, v, w) &= w_4^2, \\
\frac{\partial \overline{g}}{\partial u} &= 0, \\
\frac{\partial \overline{g}}{\partial v} &= 0, \\
\frac{\partial \overline{g}}{\partial w} &= 2w_4,
\end{aligned}$$

por lo tanto $\overline{S} = \mathbb{F}_p \times \mathbb{F}_p \times \{0\}$, por lo cual $S = \mathbb{Z}_p \times \mathbb{Z}_p \times p\mathbb{Z}_p$ y $N_5 = 1$, por lo cual

$$\begin{aligned}
\int_{\mathbb{Z}_p^3} |p^2u_2^4 + p^2v_3^3 + w_4^2|_p^s du_1 dv_3 dw_4 =& p^{-3}(p^3 - 1) + \frac{p^{-3-s}(1 - p^{-1})(1 - (p^2 + 1))}{1 - p^{-1-s}} + \\
&+ \int_{\mathbb{Z}_p \times \mathbb{Z}_p \times p\mathbb{Z}_p} |p^2u_2^4 + p^2v_3^3 + w_4^2|_p^s du_1 dv_3 dw_4,
\end{aligned}$$

haciendo la sustitución $w_4 = pw_5$, se tiene $dw_4 = p^{-1}dw_5$, así

$$\begin{aligned}
\int_{\mathbb{Z}_p^3} |p^2u_2^4 + p^2v_3^3 + w_4^2|_p^s du_1 dv_3 dw_4 =& p^{-3}(p^3 - 1) + \frac{p^{-3-s}(1 - p^{-1})(1 - (p^2 + 1))}{1 - p^{-1-s}} + \\
&+ \int_{\mathbb{Z}_p^3} |p^2u_2^4 + p^2v_3^3 + (pw_5)^2|_p^s p^{-1} du_1 dv_3 dw_4, \\
=& p^{-3}(p^3 - 1) + \frac{p^{-3-s}(1 - p^{-1})(1 - (p^2 + 1))}{1 - p^{-1-s}} + \\
&+ \int_{\mathbb{Z}_p^3} |p^2u_2^4 + p^2v_3^3 + p^2w_5^2|_p^s p^{-1} du_1 dv_3 dw_4, \\
=& p^{-3}(p^3 - 1) + \frac{p^{-3-s}(1 - p^{-1})(1 - (p^2 + 1))}{1 - p^{-1-s}} + \\
&+ \int_{\mathbb{Z}_p^3} |p^2|_p^s |u_2^4 + v_3^3 + w_5^2|_p^s p^{-1} du_1 dv_3 dw_4, \\
=& p^{-3}(p^3 - 1) + \frac{p^{-3-s}(1 - p^{-1})(1 - (p^2 + 1))}{1 - p^{-1-s}} + \\
&+ p^{-2s-1} \int_{\mathbb{Z}_p^3} |u_2^4 + v_3^3 + w_5^2|_p^s du_1 dv_3 dw_4.
\end{aligned}$$

Referencias

[1] Katok S. *p-adic analysis compared with Real*, Student mathematical library, Volume 37.

[2] Koblitz, N. *p-adic numbers, p-adic analysis, and zeta-functions,* , Springer- Verlag, New York.

[3] Vladimirov V. S, Volovich I. V, Zelenov E. I. *p-adic analysis and mathematical physics*, Series on Soviet and East European Mathematics - Vol. 1.