PESQUIMAT 25(1): 50–58 (2022) ISSN:1560-912X/ ISSN-E:1609-8439
https://doi.org/10.15381/pesquimat.v25i1.21522 Facultad de Ciencias Matemáticas – UNMSM

# Los enteros $p$-ádicos como un cociente de un anillo de series de potencias

***Napoleón Caro Tuesta*** [1]***, Alex Molina Sotomayor*** [2]***, Mario Enrique Santiago Saldaña*** [3]

**Resumen:** Sea $p$ un número primo. La construcción más familiar del anillo de los enteros $p$-ádicos $\mathbb{Z}_p$, es como un límite proyectivo de cocientes de potencias del ideal $(p) \lhd \mathbb{Z}$. Existe otra descripción de $\mathbb{Z}_p$ como un cociente del anillo de series de potencias $\mathbb{Z}[[X]]$, que aparece en algunos textos sobre análisis $p$-ádico (ver por ejemplo [3]). Más específicamente, existe un isomorfismo de anillos

$$\Psi : \mathbb{Z}[[X]]/\langle p - X\rangle \longrightarrow \mathbb{Z}_p.$$

Sin embargo, este isomorfismo también es de carácter topológico, pero no existe una demostración de tal hecho en la literatura correspondiente.

En este artículo probaremos, con suficiente detalle, que la descripción citada arriba también es válida en el contexto de los anillos topológicos.
**Palabras clave:** enteros $p$-ádicos, series de potencias, límite proyectivo, isomorfismo, cociente.

## The $p$-adic integers as a quotient of a ring of power series

**Abstract:** Let $p$ a prime number. The most familiar construction of the ring of $p$-adic integers $\mathbb{Z}_p$, is as the projective limit of quotients of powers of the ideal $(p) \lhd \mathbb{Z}$. There is another description of $\mathbb{Z}_p$ as a quotient of the power series ring $\mathbb{Z}[[X]]$, which can be found in some texts of $p$-adic analysis (see e.g. [3]). More specifically, there exists a ring isomorphism

$$\Psi : \mathbb{Z}[[X]]/\langle p - X\rangle \longrightarrow \mathbb{Z}_p.$$

However, this isomorphism is also topological in nature, but there is no proof of this fact in the corresponding literature.

In this article we will prove in sufficient detail that the above description is also valid in the context of topological rings.
**Keywords:** $p$-adic integers, power series, projective limit, isomorphism, quotient.

*Recibido:* 04/11/2021. *Aceptado:* 10/03/2022. *Publicado online:* 30/06/2022.



[1]UFPB, Departamento de Matemática, e-mail: napoleon.caro.tuesta@academico.ufpb.br
[2]UNMSM, Facultad de Ciencias Matemáticas, e-mail: amolinas@unmsm.edu.pe
[3]UNMSM, Facultad de Ciencias Matemáticas. e-mail: msantiagos@unmsm.edu.pe

## 1. Los enteros $p$-ádicos

A lo largo de esta sección, $p$ denotará un número primo. Para cada $n \geq 1$ consideremos el anillo $\mathbb{Z}/p^n\mathbb{Z}$ de enteros residuales mod$p^n$. Indicaremos por

$$\phi_n : \mathbb{Z}/p^n\mathbb{Z} \longrightarrow \mathbb{Z}/p^{n-1}\mathbb{Z}$$

el homomorfismo de anillos natural. La sucesión

$$\cdots \longrightarrow \mathbb{Z}/p^n\mathbb{Z} \xrightarrow{\phi_n} \mathbb{Z}/p^{n-1}\mathbb{Z} \longrightarrow \cdots \longrightarrow \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{\phi_1} \mathbb{Z}/p\mathbb{Z}$$

forma un sistema proyectivo de anillos. El *anillo de los enteros p-ádicos*, denotado por $\mathbb{Z}_p$, es el límite proyectivo del sistema $(\mathbb{Z}_p, \phi_n)$ definido arriba, i.e.,

$$\mathbb{Z}_p := \varprojlim_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z}.$$

Por definición, un elemento de $\mathbb{Z}_p$ es una sucesión $a = (a_1 \text{mod} p\mathbb{Z}, a_2 \text{mod} p^2\mathbb{Z}, ...) \in \prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z}$ tal que $a_n - a_{n-1} \in p^{n-1}\mathbb{Z}$ para todo $n \geq 2$.

Notemos el (único) homomorfismo de anillos $j : \mathbb{Z} \longrightarrow \mathbb{Z}_p$, i.e., el homomorfismo definido por $j(r) = (r \text{mod} p\mathbb{Z}, r \text{mod} p^2\mathbb{Z}, ...)$, es inyectivo. Esto permite identificar $\mathbb{Z}$ con un subanillo de $\mathbb{Z}_p$. Si equipamos cada $\mathbb{Z}/p^n\mathbb{Z}$ con la topología discreta y $\prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z}$ con la topología producto, el anillo $\mathbb{Z}_p$ hereda una topología que lo convierte en un espacio compacto.

**Lema 1.** *Todo elemento no nulo de $\mathbb{Z}_p$ puede ser escrito de manera única en la forma $p^n u$, donde $n$ es un entero no negativo e $u$, una unidad de $\mathbb{Z}_p$.*

Prueba. Ver [4, Proposition 2]. ■

Sea $a$ entero $p$-ádico no nulo escrito en la forma $p^n u$. El entero no negativo $n$ es llamado *valuación p-ádica* de $a$ y es denotado por $\upsilon_p(a)$. Si definimos $\upsilon_p(0) = +\infty$, valen las siguientes propiedades:

$$\upsilon_p(ab) = \upsilon_p(a) + \upsilon_p(b), \quad \upsilon_p(a+b) \geq \text{mín}(\upsilon_p(a), \upsilon_p(b)).$$

Tales fórmulas implican que $\mathbb{Z}_p$ es un dominio de integridad.

**Lema 2.** *La topología sobre $\mathbb{Z}_p$ puede ser definida por la distancia*

$$d_p(a,b) := 2^{-\upsilon(a-b)}.$$

*Más aún, $(\mathbb{Z}_p, d_p)$ es un anillo topológico completo.*

Prueba. Ver [4, Proposition 3]. ■

A partir del homomorfismo inyectivo $j : \mathbb{Z} \longrightarrow \mathbb{Z}_p$ podemos definir una métrica sobre $\mathbb{Z}$ de la siguiente manera:

$$d'(r,s) := d_p(j(r), j(s)), \quad \text{para todo par } \ r, s \in \mathbb{Z}.$$

Es importante observar que $d'(r,s) = 2^{-n}$, si y solo si, $r - s = p^n t$, para algún número entero $t$ tal que $(t,p) = 1$. En la literatura, es común llamar a la distancia $d'$ de *métrica p-ádica*, e inclusive, denotarla también por $d_p$.

**Lema 3.** *$(\mathbb{Z}_p, d_p)$ es el completamiento del espacio métrico $(\mathbb{Z}, d')$.*

Prueba. Ver [4, Proposition 3]. ■

## 2. Anillos de series de potencias

Dado un anillo conmutativo con unidad $A$, denotemos por $S$ el conjunto de todas las sucesiones $(a_n)$ de elementos de $A$. El conjunto $S$ equipado con las operaciones

$$((a_n),(b_n)) \longmapsto (c_n), \text{ donde } c_n = a_n + b_n$$

y

$$((a_n),(b_n)) \longmapsto (d_n), \text{ donde } d_n = \sum_{i=0}^{n} a_i b_{n-i},$$

es un anillo conmutativo con unidad, donde la sucesión nula $0 = (0,0,0,\ldots)$ y la sucesión $1 = (1,0,0,\ldots)$ son los elementos cero e identidad, respectivamente.

La aplicación $A \longrightarrow S$ definida por $a \longmapsto (a,0,0,\ldots)$ es un homomorfismo inyetivo de anillos. Por lo tanto, podemos identificar $A$ con su imagen homomorfa en $S$ y escribir $a$ en lugar de $(a,0,0,\ldots)$.

Para cada elemento no nulo $a = (a_n)$ de $S$, indicaremos por $v(a)$ el entero no negativo definido por $v(a) := \text{ínf}\,\{n \in \mathbb{N}_0 \mid a_n \neq 0\}$.

**Lema 4.** *La función* $|\ |: S \longrightarrow \mathbb{R}$ *definida por*

$$|\ a\ | = \begin{cases} 2^{-v(a)}, & \text{si } a \neq 0 \\ 0, & \text{si } a = 0 \end{cases}$$

*posee las siguientes propiedades:*

(i) $|\ a\ | = 0$, *si y solo si,* $a = 0$.

(ii) $|\ ab\ | \leq |\ a\ ||\ b\ |$. *La igualdad es válida cuando* $A$ *es un dominio de integridad.*

(iii) $|\ a + b\ | \leq$ *máx*$\{|\ a\ |, |\ b\ |\}$.

Prueba. Sean $a = (a_n)$ y $b = (b_n)$ elementos de $S$. La propriedad (i) sigue directamente de la definición.

Ahora vamos probar (ii). Si $ab = 0$, no hay nada que demostrar. Sean $m = v(a)$ y $p = v(b)$. Escribimos $ab = (c_n)$, donde $c_n = \sum_{k=0}^{n} a_k b_{n-k}$. Para cada $n < m + p$ observamos lo siguiente: $a_k = 0$ si $0 \leq k < m$, y cuando $m \leq k \leq n$, $b_{n-k} = 0$, pues $n - k \leq n - m < p$. Por lo tanto, $c_n = 0$ para todo $n < m + p$. Esto implica que $v(ab) \geq m + p$. Luego, $|\ ab\ | = 2^{-v(ab)} \leq 2^{-v(a)} 2^{-v(b)} = |\ a\ ||\ b\ |$. Por otro lado, $c_{m+p} = a_m b_p$. En el caso que $A$ es un dominio de integridad, $c_{m+p} \neq 0$ pues $a_m \neq 0$ y $b_p \neq 0$, y en consecuencia, $v(ab) = m + p = v(a) + v(b)$. Ahora la igualdad requerida sigue fácilmente.

Finalmente, probemos (iii): Si $a + b = 0$, la propriedad se cumple trivialmente. Supongamos entonces que $a + b \neq 0$ y que máx$\{|\ a\ |, |\ b\ |\} = |\ a\ |$, o de manera equivalente, $v(b) \geq v(a)$. Esto implica que $a_n + b_n = 0$ para todo $n < v(a)$. Por lo tanto, $v(a+b) \geq v(a)$. Luego, $|\ a+b\ | \leq |\ a\ |$. ■

Ahora es fácil ver que si $A$ es un dominio de integridad, entonces $S$ también lo es. En efecto, sean $a, b \in S$ tales que $a \neq 0$ y $b \neq 0$. Por el Lema 4, $|\ ab\ | = |\ a\ ||\ b\ | \neq 0$ y, por lo tanto, $ab \neq 0$. Por otra parte, resulta claro que la aplicación

$$\begin{array}{rccc} d & : & S \times S & \longrightarrow & \mathbb{R} \\ & & (a,b) & \longmapsto & |\ a - b\ | \end{array}$$

define una métrica sobre $S$.

Si denotamos por $X$ el elemento $(a_n) \in S$ tal que $a_1 = 1$ y $a_n = 0$ para todo $n \neq 1$, entonces $aX = (a, 0, 0, \ldots)(0, 1, 0, \ldots) = (0, a, 0, \ldots)$ para todo $a \in A$. En general, por inducción sobre $m \in \mathbb{N}$, podemos probar que $aX^m = (b_n)$, onde $b_m = a$ e $b_n = 0$ para todo $n \neq m$. Además, por convención, asumiremos que $aX^0 = a$ para todo $a \in A$.

Ahora, sea $a = (a_n)$ un elemento diferente de cero de $S$. Consideremos la sucesión $(s_m)$ de elementos de $S$, donde $s_m = a_0 + a_1X + \cdots + a_mX^m = \sum_{i=0}^{m} a_iX^i$, para cada $m \in \mathbb{N}_0$. Desde que $v(a - s_m) \geq m + 1$ obtenemos que $\mid a - s_m \mid = 2^{-v(a-s_m)} \leq 2^{-(m+1)} \to 0$. Por lo tanto, $a = \lim_{m\to\infty} s_m = \lim_{m\to\infty} \sum_{i=0}^{m} a_iX^i = \sum_{m=0}^{\infty} a_mX^m$ em $S$. Así, cada elemento $a = (a_n)$ puede ser escrito, de manera única, como una serie

$$a = a_0 + a_1X + a_2X^2 + \cdots = \sum_{n=0}^{\infty} a_nX^n.$$

Por tal motivo, $S$ es conocido como *anillo de series de potencias con coeficientes en* $A$ y es usualmente denotado por $A[[X]]$.

**Proposición 1.** *$(A[[X]],\ d)$ es un anillo topológico completo.*

Prueba. Para mostrar que $A[[X]]$ es un anillo topológico, debemos verificar que la adición y la multiplicación son aplicaciones continuas. La continuidad de la adición es consecuencia de la desigualdad

$$\left|(a + b) - \left(a' + b'\right)\right| \leq máx\left(\left|a - a'\right|, \left|b - b'\right|\right),$$

en tanto que la continuidad de la multiplicación se infiere de la desigualdad

$$\mid ab - a'b' \mid \leq \text{máx}\left(\mid a \mid\mid b - b' \mid,\ \mid a - a' \mid\mid b' \mid\right).$$

Ahora veamos que el espacio métrico $(A[[X]],\ d)$ es completo. Sea $(a(j))_{j\geq 1}$ una sucesión de Cauchy en $A[[X]]$. Entonces, dado un entero no negativo $s \geq 0$, existe un entero positivo $j_s$ tal que $|a(j) - a(k)| \leq 2^{-(s+1)}$ siempre que $j, k \geq j_s$. Si para cada $j \geq 1$ escribimos

$$a(j) = \sum_{n\geq 0} a_n(j)\, X^n,$$

entonces $|a(j) - a(k)| \leq 2^{-(s+1)}$, si y solo si, $a_n(j) = a_n(k)$ para todo $0 \leq n \leq s$. Por lo tanto,

$$a_n(j) = a_n(j_s) \quad \text{para todo} \quad j \geq j_s \quad \text{y} \quad \text{para todo} \quad 0 \leq n \leq s.$$

Sea $q_s := \text{máx}\{j_n |\ 0 \leq n \leq s\}$. Notemos que para $0 \leq n \leq s$ se tiene que $q_s \geq q_n \geq j_n$. Luego,

$$a_n(j) = a_n(j_n) \quad \text{para todo} \quad j \geq q_s.$$

Ahora consideremos el elemento

$$a = \sum_{n\geq 0} a_n(j_n)\, X^n \in A[[X]].$$

Entonces

$$\mid a(j) - a \mid = \mid \sum_{n\geq s+1} \left(a_n(j) - a_n(j_n)\right) X^n \mid \leq 2^{-(s+1)} \quad \text{para todo} \quad j \geq q_s.$$

En consecuencia, $\lim_{j\to+\infty} a(j) = a$. Esto prueba el resultado requerido. ■

**Corolario 1.** *Si $A$ es un dominio de integridad, entonces todo ideal principal de $A[[X]]$ es cerrado.*

Prueba. Sea $J$ un ideal principal de $A[[X]]$. Si $J$ es el ideal nulo, no hay nada que probar. Supongamos entonces que $J = \langle a \rangle$ para algún elemento no nulo $a \in A[[X]]$. Sea $b$ un punto de adherencia de $J$, entonces existe una sucesión $(b_n)$ de elementos de $J$ tal que $b = \lim_{n\to+\infty} b_n$. Para cada $n \geq 1$ existe $c_n \in A[[X]]$ tal que $b_n = c_n a$. Desde que $a \neq 0$, la igualdad $\mid b_n - b_m \mid = \mid a \mid\mid c_n - c_m \mid$ implica que $(c_n)$ es una sucesión de Cauchy en $A[[X]]$. La completitud de $A[[X]]$ garantiza la existencia de un elemento $c \in A[[X]]$ tal que $\lim_{n\to+\infty} c_n = c$. Finalmente, la igualdad

$$\mid b_n - ca \mid = \mid c_n a - ca \mid = \mid a \mid\mid c_n - c \mid$$

implica que $b = ca \in J$. ■

A partir de ahora asumiremos que $A$ es un dominio de integridad y que $J = \langle a \rangle$ es un ideal principal no nulo de $A[[X]]$. Desde que $J$ es cerrado (Corolario 1), no es difícil ver que la aplicación

$$\widetilde{d} : A[[X]]/J \times A[[X]]/J \longrightarrow \mathbb{R} \text{ definida por } \widetilde{d}(b \bmod J,\ c \bmod J) := \inf_{e\in J} \mid b - c - e \mid$$

es una métrica sobre el anillo $A[[X]]/J$ tal que la aplicación cociente $\pi : A[[X]] \longrightarrow A[[X]]/J$ es (uniformente) continua. En efecto, dado un número real $\epsilon > 0$ existe $\delta = \epsilon$ tal que si $b, c \in A[[X]]$ con $\mid b - c \mid < \delta$, entonces $\widetilde{d}(b \bmod J,\ c \bmod J) = \inf_{e\in J} \mid b - c - e \mid \leq \mid b - c \mid < \epsilon$.

Denotemos por $\mathcal{T}_m$ la topología inducida por la métrica $\widetilde{d}$ y por $\mathcal{T}_c$, la topología cociente.

**Lema 5.** *Las topologías $\mathcal{T}_m$ y $\mathcal{T}_c$ coinciden.*

Prueba. Desde que $\pi$ es continua (cuando $A[[X]]/J$ está equipado con la métrica $\widetilde{d}$), $\mathcal{T}_c$ es más fina que $\mathcal{T}_m$, i.e., $\mathcal{T}_m \subseteq \mathcal{T}_c$. Recíprocamemte, sean $U \in \mathcal{T}_c$ y $b \bmod J \in U$. Como $\pi^{-1}(U)$ es un abierto de $A[[X]]$ y $b \in \pi^{-1}(U)$, existe $r > 0$ tal que $B(b, r) \subseteq \pi^{-1}(U)$. Afirmamos que $B(b \bmod J, r) \subseteq U$. En efecto, sea $t \bmod J$ un elemento de $A[[X]]/J$ tal que $\widetilde{d}(t \bmod J,\ b \bmod J) = \inf_{c\in J} \mid t - b - c \mid < r$. Entonces existe $c' \in J$ de modo que $\mid t - b - c' \mid < r$. Esto implica que $t - c' \in B(b, r) \subseteq \pi^{-1}(U)$. Por lo tanto, $t \bmod J = \pi(t) = \pi(t - c') \in U$. ■

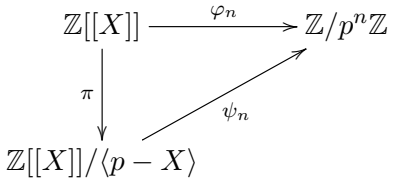
## 3. $\mathbb{Z}_p$ como un cociente de $\mathbb{Z}[[X]]$

Dados un número primo $p$ y un número natural $n \geq 1$, no es difícil verificar que la aplicación

$$\begin{array}{rccc} \varphi_n & : & \mathbb{Z}[[X]] & \longrightarrow & \mathbb{Z}/p^n\mathbb{Z} \\ & & \sum_{i\geq 0} a_i X^i & \longmapsto & (\sum_{i=0}^{n-1} a_i p^i) \bmod p^n \end{array}$$

es un homomorfismo sobreyectivo de anillos. Más aún, $\varphi_n$ es (uniformemente) continua. En efecto, para un número real $\epsilon > 0$ escogemos un número real $0 < \delta < 2^{-n}$. Luego, si $a = \sum_{i\geq 0} a_i X^i$ y $b = \sum_{i\geq 0} b_i X^i$ son elementos de $\mathbb{Z}[[X]]$ tales que $d(a, b) = 2^{-\upsilon(a-b)} < \delta$, entonces $a_i = b_i$ para todo $0 \leq i \leq n - 1$. Por lo tanto, $d''(\varphi_n(a), \varphi_n(b)) = 0 < \epsilon$. (Aquí $d''$ denota la métrica discreta sobre $\mathbb{Z}/p^n\mathbb{Z}$).

Desde que $\varphi_n(p-X)=0$, el homomorfismo $\varphi_n$ induce un homomorfismo (sobreyectivo) de anillos $\psi_n : \mathbb{Z}[[X]]/\langle p-X\rangle \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$ tal que el siguiente diagrama es conmutativo




Si equipamos $\mathbb{Z}[[X]]/\langle p-X\rangle$ con la topología cociente, o equivalentemente con la topología inducida por la métrica $\widetilde{d}$ (Lema 5), el homomorfismo $\psi_n$ también es continuo. Por otro lado, para todo $n\geq 1$, valen las igualdades

$$(\phi_n\circ\psi_n)\circ\pi=\phi_n\circ\varphi_n=\varphi_n=\psi_{n-1}\circ\pi,$$

donde $\phi_n : \mathbb{Z}/p^n\mathbb{Z}\longrightarrow\mathbb{Z}/p^{n-1}\mathbb{Z}$ denota el homomorfismo sobreyectivo natural (como indicado en la Sección 1). Desde que $\pi$ es sobreyectiva, obtenemos que $\phi_n\circ\psi_n=\psi_{n-1}$ para todo $n\geq 1$.

Indiquemos por $\rho_n : \mathbb{Z}_p\longrightarrow\mathbb{Z}/p^n\mathbb{Z}$ el homomorfismo de anillos continuo que asocia a cada entero $p$-ádico $b=(b_1\mathrm{mod}p\mathbb{Z}, b_2\mathrm{mod}p^2\mathbb{Z},...)$ su $n$-ésima componente $b_n\mathrm{mod}p^n\mathbb{Z}$. La propiedad universal del límite proyectivo, garantiza la existencia de un único homomorfismo continuo

$$\Psi : \mathbb{Z}[[X]]/\langle p-X\rangle\longrightarrow\mathbb{Z}_p=\varprojlim_{n\geq 1}\mathbb{Z}/p^n\mathbb{Z}$$

tal que $\rho_n\circ\psi=\psi_n$ para todo $n\geq 1$. De manera más explícita,

$$\Psi(\sum_{i\geq 0}a_iX^i \bmod\langle p-X\rangle)=(a_0\mathrm{mod}\ p\mathbb{Z},(a_0+a_1p)\mathrm{mod}\ p^2\mathbb{Z},(a_0+a_1p+a_2p^2)\mathrm{mod}\ p^3\mathbb{Z},...).$$

En [3, Theorem, pág 35], A. M. Roberts prueba que $\Psi$ es un isomorfismo de anillos. Nosotros demostraremos que $\Psi$ también es un homeomorfismo. Para esto, necesitaremos del siguiente resultado.

**Lema 6.** *Sea $m$ un número natural cuyo desarrollo en base $p$ es*

$$m=\sum_{i=0}^{l}\alpha_ip^i,\quad 0\leq\alpha_i\leq p-1.$$

*Entonces existen $q_0,...,q_{l-1}\in\mathbb{Z}$ tales que*

$$m=(p-X)\sum_{i=0}^{l-1}q_iX^i+\sum_{i=0}^{l}\alpha_iX^i\quad en\quad\mathbb{Z}[[X]]. \tag{1}$$

Prueba. Veamos como escoger los enteros $q_k$ para que se cumpla (1). Primero debemos tener $m=pq_0+\alpha_0$, de donde $q_0=\sum_{i=1}^{l}\alpha_ip^{i-1}$. También, $pq_1-q_0+\alpha_1=0$. Por lo tanto, $q_1=\sum_{i=2}^{l}\alpha_ip^{i-2}$. Por inducción, sea $q_{k-1}=\sum_{i=k}^{l}\alpha_ip^{i-k}$ para $1\leq k\leq l-1$. Desde que $pq_k-q_{k-1}+\alpha_k=0$, entonces $q_k=\sum_{i=k+1}^{l}\alpha_ip^{i-(k+1)}$. Reciprocamente, no es difícil verificar que tales números satisfacen (1). ■

**Teorema.** $\Psi$ *es un isomorfismo en la categoría de los anillos topológicos.*

Prueba. Para probar que $\Psi$ es inyectiva, supongamos que $\Psi(\sum_{i\geq 0} a_i X^i \bmod\langle p-X\rangle) = 0$. Entonces $p^i|(a_0 + a_1 p + \cdots + a_{i-1}p^{i-1})$ para todo $i \geq 1$. Luego, existe $r_0 \in \mathbb{Z}$ tal que $a_0 = pr_0$. Desde que $a_0 + a_1 p = p^2 r_1$ para algún $r_1 \in \mathbb{Z}$, obtenemos $a_1 = pr_1 - r_0$. Continuando en este camino, podemos encontrar una sucesión de números enteros $(r_i)$ tal que $a_n = pr_i - r_{i-1}$ para todo $i \geq 1$. Por lo tanto,

$$\sum_{i\geq 0} a_i X^i = (p - X)\sum_{i\geq 0} r_i X^i.$$

En consecuencia, $\sum_{i\geq 0} a_i X^i \bmod\langle p - X\rangle = 0$.

Ahora sea $(b_1 \bmod p\mathbb{Z}, b_2 \bmod p^2\mathbb{Z}, ...)$ un elemento cualquiera de $\mathbb{Z}_p$. Para cada $i \geq 1$, existe un entero $r_i$ tal que $b_{i+1} - b_i = p^i r_i$. Consideremos los números enteros $a_0 = b_1$ y $a_i = r_i$ para $i \geq 1$. Entonces $a_0 + a_1 p + \cdots + a_i p^{i-1} = b_i$ para todo $i \geq 1$. Por lo tanto,

$$\begin{aligned}\Psi(\sum_{i\geq 0} a_i X^i \bmod\langle p - X\rangle) &= (a_0 \bmod p\mathbb{Z}, (a_0 + a_1 p) \bmod p^2\mathbb{Z}, ...)\\ &= (b_1 \bmod p\mathbb{Z}, b_2 \bmod p^2\mathbb{Z}, ...).\end{aligned}$$

Concluimos así, que $\Psi$ es sobreyectiva.

A continuación, denotemos por $\iota : \mathbb{Z} \longrightarrow Z[[X]]/\langle p-X\rangle$ la composición de los homomorfismos

$$\mathbb{Z} \hookrightarrow Z[[X]] \xrightarrow{\pi} Z[[X]]/\langle p - X\rangle$$

Observemos que $\Psi \circ \iota = j$. Afirmamos que $\iota$ es uniformemente continua. En efecto, sean $r, s$ dos números enteros diferentes tales que $d'(r, s) = 2^{-k}$. Supongamos que $r > s$. En base $p$ podemos escribir

$$r - s = \alpha_0 p^k + \alpha_1 p^{k+1} + \cdots + \alpha_l p^{k+l},$$

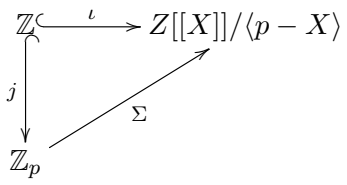
para algún entero no negativo $l$ e algunos enteros $0 \leq \alpha_i \leq p - 1$ con $\alpha_0 \neq 0$. Gracias al Lema 6, existe $q \in Z[[X]]$ tal que

$$r - s = (p - X)q + \sum_{i=0}^{l} \alpha_i X^{k+i} \text{ en } \mathbb{Z}[[X]].$$

Luego,

$$|| \ r \bmod\langle p - X\rangle - s \bmod\langle p - X\rangle \ || = \inf_{a\in\langle p-X\rangle} | \ r - s - a \ | \leq | \sum_{i=0}^{l} \alpha_i X^{k+i} \ | \leq 2^{-k}.$$

En vista que $\mathbb{Z}_p$ es el completamiento de $\mathbb{Z}$, existe un única función (uniformente) continua $\Sigma : \mathbb{Z}_p \longrightarrow Z[[X]]/\langle p - X\rangle$ tal que el siguiente diagrama



es conmutativo. Ahora afirmamos que $\Psi \circ \Sigma = \mathrm{id}_{\mathbb{Z}_p}$. En efecto, sea $a \in \mathbb{Z}_p$ entonces $a = \lim\limits_{n\to+\infty} j(a_n)$ para alguna sucesión $(a_n)$ de números enteros. Por lo tanto,

$$\Psi \circ \Sigma(a) = \Psi(\lim_{n\to+\infty} \Sigma \circ j(a_n)) = \Psi(\lim_{n\to+\infty} \iota(a_n)) = \lim_{n\to+\infty} \Psi \circ \iota(a_n) = \lim_{n\to+\infty} j(a_n) = a.$$

Como $\Psi$ es una biyección, $\Sigma = \Psi^{-1}$. Concluimos así que $\Psi$ es un homeomorfismo. ■

**Corolario 2.** *Son válidas las siguientes afirmaciones:*

(i) $(\mathbb{Z}[[X]]/\langle p - X\rangle, \widetilde{d})$ *es un completamiento de* $(\mathbb{Z}, d')$.

(ii) $\mathbb{Z}[[X]]$ *no es un dominio de ideales principales.*

Prueba. La parte (i) sigue directamente del Teorema y del Lema 3.

Por otro lado, el Teorema muestra que $p - X$ es un elemento primo de $\mathbb{Z}[[X]]$. Por lo tanto, $p - X$ es irreducible. Si $\mathbb{Z}[[X]]$ fuese un DIP, el ideal $\langle p - X\rangle$ sería maximal y en consecuencia, $\mathbb{Z}[[X]]/\langle p - X\rangle$ sería un cuerpo, lo que es una contradicción. Esto demuestra la parte (ii). ■

## Referencias bibliográficas

[1] Dugundji, J. (1966). *Topology.* Allyn and Bacon, Boston.

[2] Fried, Michael D., Jarden, Moshe (2008). *Field Arithmetic.* Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics, Springer-Verlag Berlin Heidelberg.

[3] Roberts, A. M. (2000). *A course in p-adic analysis.* Graduate Texts in Mathematics, Springer-Verlag New York.

[4] Serre, J.P. (1973). *A course in Arithmetic.* Graduate Texts in Mathematics, Springer-Verlag New York.