Universidad Nacional Autónoma de México

Facultad de Ciencias

LOS ENTEROS P-ÁDICOS: UN ENFOQUE ALGEBRAICO

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

M A T E M Á T I C O

P R E S E N T A:

MIGUEL ANGEL CORDOBA ORTUÑO

DIRECTOR DE TESIS:

DR. HUGO ALBERTO RINCÓN MEJÍA

CIUDAD UNIVERSITARIA, CD. MX. **2020**

Universidad Nacional Autónoma de México
UNAM
Biblioteca Central
Dirección General de Bibliotecas de la UNAM

UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

1. Datos del alumno	1. Datos del alumno
Apellido Paterno	Cordoba
Apellido Materno	Ortuño
Nombre(s)	Miguel Angel
Correo electrónico	miquelanqel@ciencias.unam.mx
Universidad Nacional Autónoma de México	Universidad Nacional Autónoma de México
Facultad de Ciencias	Facultad de Ciencias
Carrera	Matemáticas
Número de cuenta	401000892
2. Datos del tutor	2. Datos del tutor
Grado	Dr
Nombre(s)	Hugo Alberto
Apellido paterno	Rincón
Apellido materno	Mejía
3. Datos del sinodal 1	3. Datos del sinodal 1
Grado	Dr
Nombre(s)	Manuel Gerardo
Apellido paterno	Zorrilla
Apellido materno	Noriega
4. Datos del sinodal 2	4. Datos del sinodal 2
Grado	Dra
Nombre(s)	Diana
Apellido paterno	Avella
Apellido materno	Alaminos
5. Datos del sinodal 3	5. Datos del sinodal 3
Grado	M en C
Nombre(s)	Patricia
Apellido paterno	Cortés
Apellido materno	Flores
6. Datos del sinodal 4	6. Datos del sinodal 4
Grado	M en C
Nombre(s)	Rodrigo
Apellido paterno	Domínguez
Apellido materno	López
7. Datos del trabajo escrito	7. Datos del trabajo escrito
Título	Los enteros p-ádicos: un enfoque algebraico
Número de páginas	57
Año	2020

VNIVERSIDAD NACIONAL
AVTNOMA DE
MEXICO

FACULTAD DE CIENCIAS
Secretaría General
División de Estudios Profesionales

Votos Aprobatorios

LIC. IVONNE RAMÍREZ WENCE
Directora General
Dirección General de Administración Escolar
Presente

Por este medio hacemos de su conocimiento que hemos revisado el trabajo escrito titulado:

Los enteros p-ádicos: un enfoque algebraico

realizado por **Miguel Angel Cordoba Ortuño** con número de cuenta **401000892** quien ha decidido titularse mediante la opción de **tesis** en la licenciatura en **Matemáticas**. Dicho trabajo cuenta con nuestro voto aprobatorio.

Propietario	Dr. Manuel Gerardo Zorrilla Noriega	
Propietaria	Dra. Diana Avella Alaminos	
Propietario Tutor	Dr. Hugo Alberto Rincón Mejía	
Suplente	M. en C. Patricia Cortés Flores	
Suplente	M. en C. Rodrigo Domínguez López	

Atentamente
"POR MI RAZA HABLARÁ EL ESPÍRITU"
CIUDAD UNIVERSITARIA, CD. MX., A 23 DE OCTUBRE DE 2019

JEFE DE LA DIVISIÓN DE ESTUDIOS PROFESIONALES

ACT. MAURICIO AGUILAR GONZÁLEZ

Señor sinodal: antes de firmar este documento, solicite al estudiante que le muestre la versión digital de su trabajo y verifique que la misma incluya todas las observaciones y correcciones que usted hizo sobre el mismo.

Agradecimientos

A la Sra. Marcela Cordoba Ortuño por haberme dado la vida, por apoyarme incondicionalmente en terminar mi carrera y por no haberse dado por vencida en conseguir siempre motivandome para seguir adelante. ¡Gracias mamá! por tener la convicción de que la educación es la mejor herencia y la herramienta para ser un mejor ser humano día a día y tener una mejor calidad de vida en el futuro.

A la Sra. María de Lourdes Santana Millán, que forma parte también de este momento y por su amistad en momentos difíciles y alentarme en seguir preparándome.

A la M. en C. Patricia Cortés Flores; a quien debo gran parte de mi formación académica si no es que toda (como ayudante-docente). Por su ayuda, comprensión y por confiar en mí para que este trabajo se haya llevado a cabo y por no soltarme de la mano en tiempos difíciles en la realización del proyecto de tesis. También por haber aceptado ser su ayudante en materias como: Álgebra Superior I y II, Teoría de los Números I y II, Geometría Analítica I, Gráficas y Juegos y por supuesto Geometría Moderna I por casi diez años.

Al Dr. Hugo Alberto Rincón Mejía, por haber aceptado dirigir este trabajo, por su apoyo, comprensión, ayuda y sobre todo por su paciencia para que este trabajo sea posible.

Quiero agradecer también a todos aquellos estudiantes (alumnos) que tomaron ayudantía-clase conmigo y con la Mtra Patricia Cortés Flores, pues son parte medular de la práctica docente y mejoramiento de la calidad del trabajo académico.

Al Consejo Departamental de Matemáticas de la Facultad de Ciencias de la U.N.A.M., por haberme dado la oportunidad vía la cláusula 69 (apoyo a la titulación) y así darle el tiempo necesario en la terminación del trabajo.

Gracias a la Facultad de Ciencias de la U.N.A.M., y a todos mis maestros de quienes tuve la oportunidad de aprender algo de sus conocimientos.

A mis sinodales: Dr. Manuel Gerardo Zorrilla Noriega, Dra. Diana Avella Alaminos, Dr. Hugo Alberto Rincón Mejía (tutor), a la M. en C. Patricia Cortés Flores y al M. en C. Rodrigo Domínguez López por la lectura cuidadosa y las observaciones que sin duda ayudaron a mejorar la calidad de la tesis.

Gracias al Dr. Luis Quintanar Robles del departamento de sismología y a la Dra. Ana Lilian Martín del Pozo, del departamento de vulcanología ambos del Instituto de Geofísica de la

UNAM, por haberme dado la oportunidad de trabajar con ellos en proyectos de los cuales aprendí un poquito y obtuve un apoyo para seguir adelante con la tesis.

Agradezco el apoyo del proyecto: Impacto de la Ceniza Volcánica del Popocatépetl en los niveles de la CDMX de la SECITI para el desarrollo de esta tesis.

¡GRACIAS A TODAS Y TODOS!

Dedicatoria

A mi madre:

La Sra. Marcela Cordoba Ortuño. **¡Gracias Mamá!**

A la Sra María de Lourdes Santana Millán. **¡Gracias Amiga!**

A la M. en C. Patricia Cortés Flores. **¡Gracias Maestra!**

Al Dr. Hugo Alberto Rincón Mejía. **¡Gracias Doctor!**

Indudablemente y no exagerado, también lo dedico a todas y todos los que forman parte de los agradecimientos pues son parte importante de este trabajo.

Prólogo

Veremos distintas maneras de describir algebraicamente a los enteros p-ádicos. En el capítulo uno presentamos las nociones básicas para poder desarrollar la teoría que nos ayudará en la descripción de los enteros p-ádicos.

Se demuestra que todo grupo abeliano se puede sumergir en un grupo divisible. Damos la descripción de todos los grupos divisibles.

Se define el anillo de los enteros p-ádicos; como el anillo de endomorfismos de $\mathbb{Z}_{p^\infty}$, la cápsula divisible del grupo simple $\mathbb{Z}_p$.

Se dan otras caracterizaciones algebraicas y se indican algunas de las propiedades interesantes de $\mathbb{Z}_{p^\infty}$.

Índice general

Capítulo 1

Nociones básicas

1.1. Grupos divisibles

Definición 1 *Un grupo abeliano G es divisible si $\forall a \in G$, $\forall n \in \mathbb{Z}^+$ existe $x \in G$ tal que $a = nx$.*

Ejemplo 1 *Sea el grupo aditivo de los números racionales: $(\mathbb{Q}, +)$. Claramente si $\alpha \in \mathbb{Q}$, entonces $\alpha = \frac{a}{b}$ con a, $b \in \mathbb{Z}$ y $b \neq 0$, luego para $n \in \mathbb{Z}^+$ tenemos $n\left(\frac{a}{nb}\right) = \frac{a}{b}$ así que existe $x = \frac{a}{nb} \in \mathbb{Q}$ tal que $\alpha = nx$, por lo tanto $\mathbb{Q}$ es divisible.*

Observación 1 *Si $f : G \longrightarrow H$ es un homomorfismo de grupos, entonces:*

1. *U subgrupo de G implica que $f(U)$ es un subgrupo de H.*
2. *V es un subgrupo de H, implica que $f^{-1}(V)$ es un subgrupo de G.*
3. *la imagen de f es un subgrupo de H.*
4. *$f^{-1}(e_H)$ es un subgrupo de G llamado el núcleo de f.*

Demostración. *1.* Como $e_G \in U$ $(U \leq G)$, entonces $e_H = f(e_G) \in f(U)$.
Si $x, y \in f(U)$,digamos que $x = f(a)$, $y = f(b)$, con $a, b \in U$, entonces $xy = f(a) f(b) = f(ab) \in f(U)$, ya que $ab \in U$ dado que U es cerrado.
Si $x = f(a), a \in U$, entonces $x^{-1} = f(a)^{-1} = f(a^{-1}) \in f(U)$, ya que $a^{-1} \in U$.
2. $f(e_G) = e_H \in V$ $(L \leq H)$, esto equivale a $e_G \in f^{-1}(V)$.
Si $a, b \in f^{-1}(V)$, entonces $f(a) \in$, $f(b) \in L$, por lo que $f(ab) = f(a) f(b) \in V$. Es decir que $ab \in f^{-1}(V)$.
Si $a \in f^{-1}(V)$ entonces $f(a) \in V$, así que $f(a^{-1}) = f(a)^{-1} \in V$. Por lo tanto $a^{-1} \in V$.
3. $Im(f) = f(G) \leq H$ $(G \leq G)$.
4. Como $\{e_H\} \leq H$, entonces $f^{-1}(\{e_H\}) \leq G$.
■

Definición 2 *Sea G un grupo abeliano y n un entero positivo. nG es el conjunto:*

$$\{nx : x \in G\}.$$

Ahora la existencia de la solución $nx = g$ es equivalente a escribir que $g \in nG$. Se sigue del ejemplo 1 que $\alpha \in n\mathbb{Q}$.

Lema 1 *Si G es un grupo abeliano, entonces* $\begin{array}{rcl} G & \xrightarrow{f} & G \\ x & \longmapsto & nx \end{array}$

es un homomorfismo de grupos.

Demostración. Si x_1, x_2 están en G, como $f(x_1 + x_2) = n(x_1 + x_2) = nx_1 + nx_2$ y también $f(x_1) + f(x_2) = nx_1 + nx_2$ entonces $f(x_1 + x_2) = f(x_1) + f(x_2)$. ■

Corolario 1 *$nG \leq G$ y $\{x \in G | nx = 0\} \leq G$.*

Demostración. Se sigue de los incisos *3* y *4* de la observación 1 respectivamente. ■

Definición 3 *Decimos que un subgrupo N de un grupo M es máximo, si N es un submódulo propio máximo de M.*

Lema 2 *Para un grupo abeliano M las siguientes afirmaciones son equivalentes:*

1. *M es divisible.*
2. *Para cada primo p, M=pM.*
3. *M no tiene submódulos (propios) máximos.*

Demostración. *3.* $\Longrightarrow$ *2.* Supongamos que M no tiene subgrupos máximos y que $pM \lneqq M$, entonces M/pM es un grupo abeliano distinto de cero, tal que $p(M/pM)$=(0). Entonces M/pM es un $\mathbb{Z}/p\mathbb{Z}$-módulo, pues se puede comprobar fácilmente que

$$\mathbb{Z}/p\mathbb{Z} \times M \longrightarrow M$$

$$(\overline{a}, m) \longmapsto am$$

es una función bien definida, que hace a M un espacio vectorial sobre $\mathbb{Z}_p$. Como los espacio vectoriales tienen subespacios máximos (una consecuencia de que los espacios vectoriales tienen bases), entonces M tiene un subespacio máximo, y éste es un subgrupo máximo de M. Esta contradicción muestra que $M = pM$, para todo primo p.

2. $\Longrightarrow$ *1.* Queremos ver que $M = nM$, para todo natural n mayor que 0. Sea $n > 0$, y digamos que $n = p_1 ... p_k$ es la factorización en primos de n. Haremos una demostración por inducción sobre k.

Si $k = 1$, entonces n es primo y concluimos directamente de *2.*

Si $k > 1$, entonces $nM = (p_1...p_{k-1})(p_kM) = (p_1...p_{k-1})M = M$, por la base e hipótesis de inducción.

1. $\Longrightarrow$ *3.* Si M tiene un subgrupo máximo N, entonces M/N es isomorfo a $\mathbb{Z}_p$. $\mathbb{Z}_p$ no es divisible pues $p\mathbb{Z}_p = \{\overline{0}\} \neq \mathbb{Z}_p$. Entonces M/N no es divisible, así que M no puede ser divisible, pues como observamos más adelante, cocientes de divisibles son divisibles. ■

Nota 1 *Si para cualquier entero positivo n y para todo homomorfismo $f : n\mathbb{Z} \longrightarrow G$ con G un grupo abeliano, existe un homomorfismo de grupos $\varphi : \mathbb{Z} \longrightarrow G$ (donde consideramos la inmersión de $n\mathbb{Z}$ en $\mathbb{Z}$: $i^{\mathbb{Z}}_{n\mathbb{Z}} : n\mathbb{Z} \hookrightarrow \mathbb{Z}$) tal que el siguiente diagrama conmuta:*

$$\begin{array}{ccc} n\mathbb{Z} & \xrightarrow{i^{\mathbb{Z}}_{n\mathbb{Z}}} & \mathbb{Z} \\ {\scriptstyle f}\downarrow & \swarrow_{\varphi} & \\ G, & & \end{array}$$

entonces G es un grupo divisible: Pues si $n \in \mathbb{Z}^+$ y $g \in G$, como $\mathbb{Z}$ es un dominio entero existe un homomorfismo f de $n\mathbb{Z}$ en G tal que $f(n) = g$; entonces como por hipótesis hay un homomorfismo de grupos $\varphi : \mathbb{Z} \longrightarrow G$ y que extiende a f: $g = f(n) = \varphi(n) = \varphi(n \cdot 1) = \varphi\left(\underbrace{1 + 1 + \cdots + 1}_{n \text{ veces}}\right) = \underbrace{\varphi(1) + \varphi(1) + \cdots + \varphi(1)}_{n \text{ veces}} = n\varphi(1)$, entonces $g = n\varphi(1)$ con $\varphi(1) \in G$, por lo tanto $G \subseteq nG\ \forall n \in \mathbb{Z}^+$. Por el Corolario 1; $nG \subseteq G\ \forall n \in \mathbb{Z}^+$ entonces $G = nG\ \forall n \in \mathbb{Z}^+$ por lo tanto G es divisible.

Ahora por la nota 1 tenemos el siguiente diagrama conmutativo:

$$\begin{array}{ccc} n\mathbb{Z} & \xrightarrow{i^{\mathbb{Z}}_{n\mathbb{Z}}} & \mathbb{Z} \\ {\scriptstyle f}\downarrow & \swarrow_{\varphi} & \\ \mathbb{Q}. & & \end{array}$$

Proposición 1 *(Criterio de Baer) Sea G un grupo abeliano. Entonces G es divisible si y sólo si para todo entero positivo n y todo homomorfismo de grupos $f : n\mathbb{Z} \longrightarrow G$ existe un homomorfismo $\varphi : \mathbb{Z} \longrightarrow G$ tal que el diagrama siguiente conmuta:*

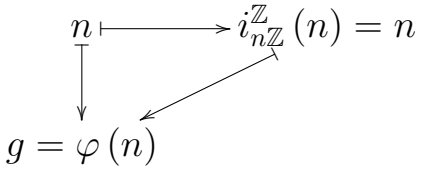
$$\begin{array}{ccc} n\mathbb{Z} & \xrightarrow{i^{\mathbb{Z}}_{n\mathbb{Z}}} & \mathbb{Z} \\ {\scriptstyle f}\downarrow & \swarrow_{\varphi} & \\ G. & & \end{array}$$

Demostración. $\Longrightarrow$) Si G es divisible, entonces existe $\varphi : \mathbb{Z} \longrightarrow G$ homomorfismo de grupos tal que para cualquier homomorfismo de grupos $f : n\mathbb{Z} \longrightarrow G$ tenemos que $\varphi \circ i^{\mathbb{Z}}_{n\mathbb{Z}} = f$.

Por hipótesis tenemos que G es divisible, entonces sea $a \in G$ por tanto existe $x \in G$ tal que $a = nx \ \forall n \in \mathbb{Z}^+$. Ahora sea $f : n\mathbb{Z} \to G$ un homomorfismo tal que $f(n) = a$. Definamos a $\varphi : \mathbb{Z} \to G$ como $\varphi(n) = nx$. Entonces $(\varphi \circ i^{\mathbb{Z}}_{n\mathbb{Z}})(n) = \varphi(i^{\mathbb{Z}}_{n\mathbb{Z}}(n)) = \varphi(n) = nx = a = f(n)$. Por tanto existe φ tal que el diagrama conmuta.

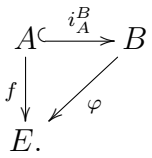
$\Longleftarrow$) Si para todo homomorfismo $f : n\mathbb{Z} \longrightarrow G$ y $\forall\, n \in \mathbb{Z}^+$ existe $\varphi : \mathbb{Z} \longrightarrow G$ homomorfismo tal que el diagrama de la proposición conmuta, entonces el grupo G es divisible.

La demostración está en la Nota 1 y únicamente veremos el siguiente diagrama para completarla.



■

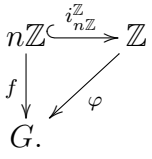
Definición 4 *Sea E un grupo abeliano y $A \subseteq B$ un subgrupo de B. Llamaremos a E grupo inyectivo si para cualquier homomorfismo de grupos $f : A \longrightarrow E$ existe un homomorfismo de grupos $\varphi : B \longrightarrow E$ tal que el diagrama siguiente conmuta:*



También se dice que E tiene la propiedad de inyectividad en la definición anterior.

Ejemplo 2 *El grupo aditivo de los racionales $(\mathbb{Q}, +)$ es inyectivo.*

Nota 2 *Sabemos que para todo homomorfismo $f : n\mathbb{Z} \longrightarrow G$ de grupos con G grupo abeliano, $\exists\ \varphi : \mathbb{Z} \longrightarrow G$ homomorfismo de grupos tal que el diagrama siguiente conmuta:*



Por lo tanto de la Definición 4 (G tiene la propiedad de inyectividad), y usando el criterio de Baer se sigue que un grupo abeliano inyectivo es divisible.

Pero aún tenemos la siguiente pregunta:

¿Un grupo abeliano divisible tiene la propiedad de inyectividad?

Para investigar la respuesta usaremos el Lema de Zorn (Si $(\mathcal{A}, \preceq)$ es un conjunto no vacío con un orden $\preceq$, y toda cadena en $\mathcal{A}$ (un subconjunto C de $\mathcal{A}$ en donde cualesquiera dos elementos son comparables: si x, $y \in C$ implica $x \preceq y$ ó $y \preceq x$) tiene una cota superior en $\mathcal{A}$, entonces $\mathcal{A}$ tiene elementos máximos).

Ahora sea D un grupo divisible y $f : A \longrightarrow D$ un homomorfismo de grupos donde A es un subgrupo de B, en esta situación nuestro diagrama es:

$$\begin{array}{ccc} A & \xhookrightarrow{i_A^B} & B \\ \downarrow{\scriptstyle f} & & \\ D. & & \end{array}$$

Queremos ver si existe un homomorfismo de grupos $\varphi : B \longrightarrow D$ tal que $\varphi_{|_A} = f$.

Vamos a considerar un conjunto ordenado relacionado con la situación anterior. Para empezar consideremos el conjunto de los subgrupos de B que contienen a A, es decir; los grupos que están entre A y B:

$$A \xhookrightarrow{i_A^C} C \xhookrightarrow{i_C^B} B.$$

Teorema 1 *Son equivalentes:*

1. *D es un grupo abeliano divisible.*

2. $\forall$ $\begin{array}{c} n\mathbb{Z} \\ \downarrow{\scriptstyle f} \\ D \end{array}$ $\exists$ $\begin{array}{ccc} \mathbb{Z} & & \\ & \swarrow{\scriptstyle \varphi} & \\ D & & \end{array}$ *tal que* $\begin{array}{ccc} n\mathbb{Z} & \xhookrightarrow{i_{n\mathbb{Z}}^{\mathbb{Z}}} & \mathbb{Z} \\ \downarrow{\scriptstyle f} & \swarrow{\scriptstyle \varphi} & \\ D & & \end{array}$ *conmuta.*

3. *D es inyectivo, es decir;* $\forall$ $\begin{array}{ccc} A & \xhookrightarrow{i_A^B} & B \\ \downarrow{\scriptstyle f} & & \\ D & & \end{array}$ $\exists\, \varphi$: $\begin{array}{c} B \\ \downarrow{\scriptstyle \varphi} \\ D \end{array}$ *tal que* $\begin{array}{ccc} A & \xhookrightarrow{i_A^B} & B \\ \downarrow{\scriptstyle f} & \swarrow{\scriptstyle \varphi} & \\ D & & \end{array}$ *conmuta.*

Demostración.

1. $\iff$ *2.* es la Proposición 1.

3. $\implies$ *2.* Es claro.

1. $\implies$ *3.* Usaremos el Lema de Zorn.

Supongamos que tenemos $\begin{array}{ccc} A & \overset{i_A^B}{\hookrightarrow} & B \\ \downarrow{\scriptstyle f} & & \\ D & & \end{array}$ donde f es un morfismo de grupos y donde A es un subgrupo de B.

Consideremos el conjunto siguiente:

$$\mathcal{A} := \{\Big(C,\ C \xrightarrow{f_C} D\Big) \mid\ A \leq C \leq B\ \ y\ \ f_C\ \text{extiende a}\ f\}.$$

Observemos que $\mathcal{A}$ es no vacío, pues contiene a $(A,\ A \xrightarrow{f} D\ )$.

Definimos un orden parcial en $\mathcal{A}$ de la manera siguiente:

$$(X,\ f_X : X \longrightarrow D\ ) \preceq (Y,\ f_Y : Y \longrightarrow D\ )$$

si $X \overset{i_X^Y}{\hookrightarrow} Y$ y f_Y extiende a f_X, de manera que $\begin{array}{ccc} X & \overset{i_X^Y}{\hookrightarrow} & Y \\ {\scriptstyle f_X}\downarrow & \swarrow{\scriptstyle f_Y} & \\ D & & \end{array}$ conmuta.

Es inmediato que $\preceq$ es una relación reflexiva y transitiva. Ahora veamos que es antisimétrica:

Si $(X, f_X) \preceq (Y, f_Y) \preceq (X, f_X)$, entonces $X \preceq Y \preceq X$. Por lo que $X = Y$.

Además, como $\begin{array}{ccc} X & \overset{i_X^Y}{\hookrightarrow} & Y \\ {\scriptstyle f_X}\downarrow & = \swarrow{\scriptstyle f_Y} & \\ D & & \end{array}$ y $X = Y$, entonces $\begin{array}{l} f_{Y|_X} = f_X. \text{ Así } (X, f_X) = (Y, f_Y). \\ \quad\quad || \\ f_{X|_Y} = f_Y \end{array}$

Lo que sigue es ver que el conjunto parcialmente ordenado $(\mathcal{A}, \preceq)$ satisface las hipótesis del Lema de Zorn.

Supongamos que $\{(C_i, f_i)\}_{i\in I}$ es una cadena en $\mathcal{A}$. En particular $\{C_i\}_{i\in I}$ es una cadena de subgrupos de B que contiene a A. Entonces $\bigcup_{i\in I} C_i$ es un subgrupo de B que contiene a A.

Definimos ahora $\begin{array}{c} \bigcup_{i\in I} C_i \\ \downarrow{\scriptstyle h} \\ D \end{array}$ por $h(x) := f_j(x)$ si $x \in C_j$. Veamos que h está bien definida.

En efecto, si $x \in C_j \bigcap C_k$ con $j,\ k \in I$, entonces $(C_j, f_j) \preceq (C_k, f_k)$ ó $(C_k, f_k) \preceq (C_j, f_j)$, pues $\{(C_i, f_i)\}_{i\in I}$ es una cadena. Supongamos que $(C_j, f_j) \preceq (C_k, f_k)$. Vemos lo siguiente:

$$x \in C_j,\ \begin{array}{ccc} C_j & \overset{i_{C_j}^{C_k}}{\hookrightarrow} & C_k\ ,\ C_k \ni x \\ & = & \\ {\scriptstyle f_j}\searrow & & \swarrow{\scriptstyle f_k} \\ & D & \end{array} \qquad\qquad \begin{array}{ccc} x & \longmapsto & x \\ \searrow & & \swarrow \\ & f_j(x) = f_k(x) & \end{array}$$

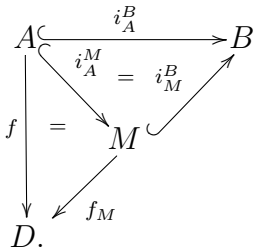
Así $\bigcup_{i\in I} C_i$ está bien definida y por construcción $(\bigcup_{i\in I} C_i, h)$ es una cota superior para la

$$\begin{array}{c} \bigcup_{i\in I} C_i \\ \big\downarrow h \\ D \end{array}$$

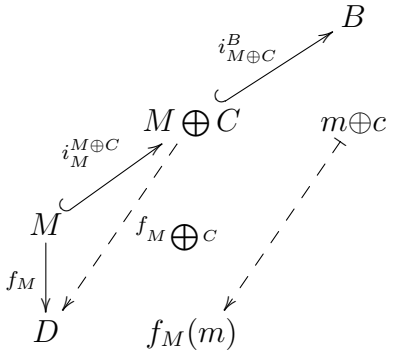
cadena en $\mathcal{A}$:

$$\{(C_i, f_i)\}_{i\in I}.$$

Por el Lema de Zorn, $\mathcal{A}$ tiene un elemento máximo, (M, f_M) digamos.



No puede haber un subgrupo $C \neq \{0\}$ de B tal que $M \bigcap C = \{0\}$, pues en ese caso tenemos el diagrama siguiente:

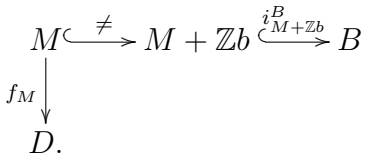


y $(M \bigoplus C, f_{M \bigoplus C})$ sería una extensión propia de (M, f_M), contradiciendo la maximidad de (M, f_M).

Si $M \subsetneqq B$, entonces $\forall b \in B \setminus M$, $\mathbb{Z}b \bigcap M \neq \{0\}$, por la observación anterior. Por lo tanto $\forall b \in B \setminus M$, $\{z | zb \in M\} \neq \{0\}$.

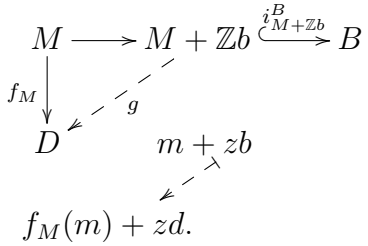
Notemos que $\{z | zb \in M\}$ es un subgrupo de $\mathbb{Z}$ (tiene al 0, es cerrado bajo la suma y es cerrado bajo inversos aditivos).

Todo subgrupo diferente de $\{0\}$ de $\mathbb{Z}$ es de la forma $n\mathbb{Z}$ para alguna $n \in \mathbb{N} \setminus \{0\}$. Así, si $b \in B \setminus M$ tenemos $\{z | zb \in M\} = n\mathbb{Z}$. Notemos también que $zb \in M \iff n \mid z$. Si $M \subsetneqq B$ y $b \in B \setminus M$, entonces veamos lo siguiente:



Definimos ahora $g : M + \mathbb{Z}b \longrightarrow D$ una extensión de f_M a fin de obtener una contradicción.

Sea $n\mathbb{Z} = \{z \in \mathbb{Z} | zb \in M\}$. Tenemos que $nb \in M$, $f_M(nb) \in D$. Como D es divisible, $f_M(nb) = nd$, para alguna $d \in D$. Definamos g por: $g(m + zb) = f_M(m) + zd$ como en el diagrama siguiente:



Veamos que g está bien definida:

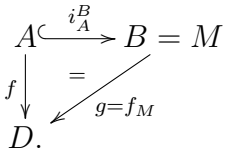
Si $m+zb = m'+z'b$, entonces $m-m' = (z'-z)b$. Entonces $n \mid z'-z$. Digamos que $z'-z = ns$ con $s \in \mathbb{Z}$. Ahora $m - m' = nsb$. Así vemos lo siguiente:

$$f_M(m - m') = f_M(nsb) = f_M(snb) = sf_M(nb) = snd = (z' - z)d.$$

Por lo tanto $f_M(m) - f_M(m') = z'd - zd$, es decir; que $f_M(m) + zd = f_M(m') + z'd$.

Esto muestra que g está bien definida. Es claro que g es un homomorfismo de grupos que extiende a f_M.

Como (M, f_M) es máximo, concluímos que $M = B$, entonces tenemos el diagrama siguiente:



Esto muestra que f se puede extender a un morfismo $B \xrightarrow{g} D$. Es decir D es inyectivo.

■

1.2. El producto cartesiano de una familia de grupos

Definición 5 *Si $\{G_i\}_{i\in I}$ es una familia de grupos, definimos el producto de la familia, como*

$$\Pi_{i\in I}G_i = \{f : I \longrightarrow \cup_{i\in I}G_i | f(i) \in G_i\}$$

Se puede pensar un elemento de $\Pi_{i\in I}G_i$ como una "I-ada" $(f(i))_{i\in I}$, en donde $f(i)$ es el elemento en la coordenada i-ésima de f.

Lema 3 *El producto cartesiano es un grupo con la operación definida por la suma por coordenadas, es decir; $(f + g)(i) = f(i) + g(i) \in G_i \ \forall i \in I$.*

Demostración. Sea $\{G_i\}_{i\in I}$ una familia de grupos y veamos que $\Pi_{i\in I}G_i$ es un grupo. En efecto: sabemos que cada G_i de la familia dada es un grupo y por lo tanto en cada G_i la suma es asociativa, luego la suma en el $\Pi_{i\in I}G_i$ lo es:

Asociatividad: $((f+g)+h)(i) = (f+g)(i)+h(i) = (f(i)+g(i))+h(i) = f(i)+((g(i)+h(i)) = f(i) + (g+h)(i) = (f + (g + h))(i)$.

Existencia de neutro: Sea $f \in \Pi_{i\in I}G_i$. Veamos que existe $g = 0 \in \Pi_{i\in I}G_i$ tal que $f(i) + 0(i) = f(i)\ \forall i \in I$. Sea $0_{\Pi_{i\in I}G_i} = g = 0_{G_i}$.

Existencia de inverso: Sea $h \in \Pi_{i\in I}G_i$. Vemos que $-h(i)$ es el opuesto de $h(i)$, pues $h(i) + (-h(i)) = (h + (-h))(i) = (h - h)(i) = 0(i) \in G_i\ \forall i \in I$.

■

Teorema 2 *El producto cartesiano de una familia de grupos divisibles es un grupo divisible.*

Demostración. Supongamos que $f \in \Pi_{i\in I}G_i$, y sea $n \in \mathbb{Z}^+$, entonces $f(i) = ng_i$ para alguna $g_i \in G_i$, pues G_i es divisible por hipótesis. Definamos $g \in \Pi_{i\in I}G_i$ por: $g(i) = g_i$, entonces $(ng)(i) = ng_i = f(i)$, $\forall i \in I$ por lo tanto $ng = f$. Es decir, $\Pi_{i\in I}G_i$ es divisible. ■

Teorema 3 *Un cociente de un grupo divisible es divisible.*

Demostración. Supongamos que G es un grupo abeliano divisible y que $G \xrightarrow{f} \!\!\!\!\rightarrow H$ es un homomorfismo suprayectivo de grupos. Si $n > 0$, $n \in \mathbb{N}$, tenemos que $nH = nf(G) = f(nG) = f(G) = H$. ■

Observación 2 *Si $M_i = M\ \forall i \in I$,*

$$\Pi_{i\in I}M_i = \{f : I \longrightarrow \cup M_i | f(i) \in M_i\} = \{f : I \longrightarrow M\} = M^I.$$

M^I es el producto de $|I|$ copias de M.

Corolario 2 *$\mathbb{Q}/\mathbb{Z}$ es divisible y para cada conjunto X, $(\mathbb{Q}/\mathbb{Z})^X$ es divisible.*

Demostración. Se sigue inmediatamente de los dos resultados previos y del hecho de que $\mathbb{Q}$ es divisible. ■

Lema 4 *Si $\mathbb{Z}x$ es un grupo abeliano cíclico no trivial, entonces existe un morfismo distinto de cero $\mathbb{Z}x \to \mathbb{Q}/\mathbb{Z}$.*

Demostración. Si el orden de x es finito, y p es un primo que divide al ordende x, entonces $\frac{o(x)}{p}x$ tiene orden p. Hagamos $y = \frac{o(x)}{p}x$. Definamos f como sigue:

$$\mathbb{Z}y \xrightarrow{f} \mathbb{Q}/\mathbb{Z}$$

$$y \longmapsto \overline{1/p}\,,$$

entonces f es un morfismo distinto de cero que se puede extender a un morfismo distinto de cero desde $\mathbb{Z}x$, pues como $\mathbb{Q}/\mathbb{Z}$ es divisible, es también inyectivo. Como en el diagrama:

$$\begin{array}{ccc} \mathbb{Z}y & \longrightarrow & \mathbb{Z}x \\ & \searrow^{f} & \downarrow{\scriptstyle \varphi} \\ & & \mathbb{Q}/\mathbb{Z}. \end{array}$$

Si el orden de x es infinito, podemos definir $\mathbb{Z}x \longrightarrow \mathbb{Q}/\mathbb{Z}$ por: $f(xz) = z(\overline{1/2})$ que es un morfismo distinto de cero.

■

Lema 5 *Todo grupo abeliano M se puede sumergir en un grupo divisible.*

Demostración. Como el grupo trivial es divisible, podemos considerar solamente el caso en que M es distinto del grupo trivial. Por el lema anterior, para cada x no cero en M tenemos un morfismo no nulo f_x de $\mathbb{Z}x$ a $\mathbb{Q}/\mathbb{Z}$. Consideremos ahora el grupo divisible $(\mathbb{Q}/\mathbb{Z})^{M\setminus\{0\}}$ (un producto directo de $|M \setminus \{0\}|$ copias de $\mathbb{Q}/\mathbb{Z}$). Como $\mathbb{Q}/\mathbb{Z}$ es inyectivo, cada f_x se extiende a un morfismo no nulo $\varphi_x : M \longrightarrow \mathbb{Q}/\mathbb{Z}$. Definamos ahora θ, de manera que el siguiente diagrama conmute:

$$\begin{array}{ccc} M & \xrightarrow{\theta} & (\mathbb{Q}/\mathbb{Z})^{|M\setminus\{0\}|} \\ & \searrow^{\varphi_y} & \downarrow{\scriptstyle \pi_y} \\ & & \mathbb{Q}/\mathbb{Z}. \end{array}$$

Es decir, $(\theta(x))(y) = \varphi_y(x)$. Es claro que θ es un morfismo de grupos:

$$\theta(x+y)(z) = \varphi_z(x+y) = \varphi_z(x) + \varphi_z(y) = \theta(x)(z) + \theta(y)(z)\,.$$

De aquí que $\theta(x+y) = \theta(x) + \theta(y)$.

Notemos que $(\theta(x))(x) = \varphi_x(x) = f_x(x) \neq 0$. Por lo que ninguna x no nula pertenece al núcleo de θ. Por lo tanto $Nuc(\theta) = \{0\}$. Es decir que θ es una inmersión de M en un grupo divisible. ■

Definición 6 *Un grupo divisible D es un cogenerador divisible si cualquier grupo abeliano M se puede sumergir en un producto de copias de D.*

El resultado anterior dice que $\mathbb{Q}/\mathbb{Z}$ es un cogenerador divisible (o cogenerador inyectivo para $\mathbb{Z} - mod$).

Definición 7 *Sean* $A \xrightarrow{f} B \xrightarrow{g} C$ *morfismos de grupos. Decimos que la sucesión* f, g *es exacta si* $Im(f) = Nuc(g)$.

Observación 3 $A \xrightarrow{f} B \xrightarrow{g} C$ *es exacta* $\iff$ 1) $g \circ f = 0$ *y* 2) $Nuc(g) \subseteq Im(f)$.

Demostración.
($\Longrightarrow$) Es claro que si la sucesión es exacta, $g \circ f = 0$ pues $Nuc(g) = Im(f)$ y además tenemos que $Nuc(g) \subseteq Im(f)$.
($\Longleftarrow$) Recíprocamente, si 1) y 2) se tienen, entonces $g \circ f = 0 \Longrightarrow Im(f) \subseteq Nuc(g)$. Como estamos suponiendo la otra inclusión, tenemos que $Im(f) = Nuc(g)$. ■

Ejemplo 3 *Sea* $A \xrightarrow{f} B$ *un homomorfismo de grupos.*

Entonces $0 \xrightarrow{\overline{0}} A \xrightarrow{f} B$ *es exacta* $\iff$ f *es un monomorfismo.*

Demostración. $Im(\overline{0}) = \{0\} = Nuc(f) \iff f$ es un monomorfismo. ■

Ejemplo 4 $A \xrightarrow{f} B \xrightarrow{\overline{0}} 0$ *es exacta* $\iff$ f *es un epimorfismo.*

Demostración. En efecto:

($\Longleftarrow$) Si f es un epimorfismo, entonces $Im(f) = B = Nuc(\overline{0})$.
($\Longrightarrow$) Si $Nuc(\overline{0}) = B = f(A)$, entonces f es un epimorfismo. ■

Ejemplo 5 $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ *es exacta* $\iff$

1. f *es un monomorfismo (pues* $0 \longrightarrow A \xrightarrow{f} B$ *es exacta).*
2. g *es un epimorfismo.*
3. $g \circ f = 0$.
4. $Nuc(g) \subseteq Im(f)$.

Ejemplo 6 *Si* $A \xrightarrow{f} B$ *es morfismo de grupos, entonces:*

$$0 \longrightarrow Nuc(f) \xrightarrow{f} A \xrightarrow{g|} f(A) \longrightarrow 0 \quad es \quad exacta.$$

Ejemplo 7 *Si* $A \xrightarrow{f} B$ *es morfismo de grupos, entonces:*

$$0 \longrightarrow f(A) \longrightarrow B \longrightarrow B/f(A) \longrightarrow 0 \quad es \quad exacta.$$

$$b \longmapsto b + f(A)$$

Definición 8 *Una sucesión exacta* $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ *se llama sucesión exacta corta.*

Definición 9 *La sucesión exacta* $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ *se escinde por la izquierda si* $\exists \beta : B \longrightarrow A$ *morfismo de grupos tal que* $\beta \circ f = 1_A$.

Definición 10 *La sucesión exacta* $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ *se escinde por la derecha si* $\exists \alpha : C \longrightarrow B$ *morfismo de grupos tal que* $g \circ \alpha = 1_C$.

Definición 11 *Una sucesión exacta corta se escinde si se escinde por la izquierda y se escinde por la derecha.*

Teorema 4 *Son equivalentes para* $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ *sucesión exacta corta:*

1. $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ *se escinde por la izquierda.*
2. $B = f(A) \bigoplus C'$ *(es decir;* $\exists C' \subseteq B$ *tal que* $f(A) + C' = B$ *y* $f(A) \cap C' = \{0\}$*), con* $C' \xrightarrow{g_|} C$ *isomorfismo.*
3. $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ *se escinde por la derecha.*
4. $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ *se escinde.*

Demostración.

Basta ver que *1.*, *2.* y *3.* son equivalentes.

1. $\Longrightarrow$ *2.* Si β es una escisión para f, es decir, $\beta \circ f = 1_A$, entonces:

$$\forall b \in B, \ \ (\beta \circ f)(\beta(b)) = 1_A(\beta(b)) = \beta(b)$$

por lo tanto $(\beta f \beta)(b) - \beta(b) = 0$ y así $\beta(f(\beta(b) - b)) = 0$. Entonces $(f \circ \beta)(b) - b \in Nuc(\beta)$ y $b = (b - (f \circ \beta)(b)) + (f \circ \beta)(b)$ (donde $b - (f \circ \beta)(b) \in Nuc(\beta)$ y $(f \circ \beta)(b) \in f(A)$) por lo tanto $B \subseteq Nuc(\beta) + f(A) \subseteq B$. Asi $B = Nuc(\beta) + f(A)$.

Si $x \in Nuc(\beta) \cap f(A)$, entonces $x = f(a)$ para algún $a \in A$ y algún $x \in Nuc(\beta)$. Entonces $0 = \beta(x) = \beta(f(a)) = 1_A(a) = a$. Como $a = 0$ entonces $x = f(0) = 0$ por lo tanto $Nuc(\beta) \cap f(A) = \{0\}$. Así $B = Nuc(\beta) \oplus f(A)$.

Como $f(A) = Nuc(g)$ entonces

$$g(B) = g(Nuc(\beta))$$

luego

$$Nuc(\beta) \xrightarrow{g_|} g(B) = C$$

y

$$Nuc\left(g_|\right) = Nuc(\beta) \cap Nuc(g) = Nuc(\beta) \cap f(A) = \{0\}$$

por lo tanto $g_| : Nuc(\beta) \xrightarrow[]{\sim} g(B)$ es un isomorfismo.

2. $\Longrightarrow$ *3.* Supongamos $0 \longrightarrow A \xrightarrow{f} f(A) \oplus C' \xrightarrow{g} C \longrightarrow 0$ es una sucesión exacta con lo siguiente:

$$C' \xrightarrow[\cong]{g_|} C\ .$$

Sea $C \xrightarrow{h} C'$ el inverso de $g_|$ y consideremos lo que sigue:

$$\underbrace{C \xrightarrow{h} C' \overset{i_{C'}^{f(A)\oplus C'}}{\hookrightarrow} f(A) \oplus C'}_{\alpha}\ .$$

Veamos que $g \circ \alpha = 1_C$. En efecto:

$$(g \circ \alpha)(C) = g \circ i \circ h(C) = (g \circ h)(C) = C$$

por lo tanto $g \circ \alpha = 1_C$.

3. $\Longrightarrow$ *2.* Por hipótesis $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ se escinde por la derecha.
Si $g \circ \alpha = 1_C$ donde $\alpha : C \longrightarrow B$, entonces $(g \circ \alpha \circ g)(b) = (g \circ \alpha)(g(b)) = g(b)$ por lo tanto $(g\alpha g - g)(b) = g(\alpha g(b) - b) = 0$ donde $\alpha g(b) - b \in Nuc(g) = f(A)$. Por lo tanto $b = (-\alpha g(b) + b) + ag(b)$ con $(-\alpha g(b) + b) \in f(A)$ y $ag(b) \in \alpha(C)$ ahora $B = f(A) + \alpha(C)$.
Si $x \in f(A) \cap \alpha(C)$, entonces $x = f(a) = \alpha(c)$ con $a \in A$ y $c \in C$ por lo tanto $g(x) = gf(a) = (g\alpha)(c) = 1_C(c) = c$ por tanto $c = 0$ ahora $\alpha(c) = x = 0$. Así que $B = f(A) \oplus \alpha(C)$ ahora $g(B) = gf(A) + g\alpha(C) = C$ por lo tanto vemos lo siguiente:

$$\alpha(C) \xrightarrow{g_|} C \quad \text{y} \quad Nuc\left(g_|\right) = Nuc(g) \cap \alpha(C) = 0.$$

Por lo tanto $\alpha(C) \xrightarrow[\cong]{g_|} C$.

2. $\Longrightarrow$ *1.* Si $0 \longrightarrow A \xrightarrow{f} f(A) \oplus C' \xrightarrow{g} C \longrightarrow 0$ con $C' \xrightarrow[]{\sim} C$ cualquier elemento $x \in f(A) \oplus C'$ se puede escribir de manera única como $x = f(a) + c'$ con $a \in A$ y $c' \in C'$. Ahora

$$A \xrightarrow{\beta} f(A) \oplus C'$$

$$a \longmapsto f(a) + c'$$

β es un homomorfismo bien definido y $(\beta \circ f)(a) = \beta(f(a)) = a$ es decir, $\beta \circ f = 1_A$.

■

Lema 6 *Un sumando directo de un grupo divisible es divisible.*

Demostración. Supongamos que $D = A \oplus B$ con D divisible y A, B subgrupos de D.

Si $p \in \mathbb{P}$, entonces $A \oplus B = D = pD = pA + pB = pA \oplus pB$.

Si $a \in A$, entonces $a = pa' + pb \in A \oplus B$ donde $a' \in A$. Entonces $a - pa' = pb \in A \cap B = \{0\}$. Entonces $a = pa'$ y por lo tanto $A \subseteq pA \subseteq A$.

■

Lema 7 *Son equivalentes para un grupo abeliano M:*

1) M es divisible.

2) M es un sumando de cualquier grupo que lo contenga.

Demostración. *1) $\Longrightarrow$ 2)* Supongamos que $M \overset{i_M^N}{\hookrightarrow} N$ es un homomorfismo de grupos con M divisible. Veamos el siguente diagrama:

$$\begin{array}{ccc} M & \overset{i_M^N}{\hookrightarrow} & N \\ {\scriptstyle I_M}\downarrow & \swarrow_{\varphi} & \\ M. & & \end{array}$$

Como M es inyectivo entonces se extiende a un homomorfismo φ tal que $\varphi \circ i = I_M$. Entonces φ es una escisión para i_M^N y así M es sumando directo de N.

2) $\Longrightarrow$ 1) Como $\mathbb{Q}/\mathbb{Z}$ es un cogenerador inyectivo $\exists$ $M \overset{\varphi}{\twoheadrightarrow} (\mathbb{Q}/\mathbb{Z})^X$ un monomorfismo para algún conjunto X.

Podemos suponer que φ es la inclusión, entonces M es sumando directo de $(\mathbb{Q}/\mathbb{Z})^X$. Sabemos que $(\mathbb{Q}/\mathbb{Z})^X$ es divisible y un sumando directo de un divisible es divisible.

■

En el siguiente corolario veremos que en efecto, todo grupo abeliano es un subgrupo de un grupo divisible. Antes unas observaciones:

Observación 4 *Si G es un grupo y $f : G \overset{}{\twoheadleftarrow\!\!\!\twoheadrightarrow} X$ es una biyección, X es un grupo y f es un isomorfismo si definimos la suma en X por:*

$$x + y =: f\left(f^{-1}(x) + f^{-1}(y)\right).$$
$$f$$

Demostración. Veamos que se cumple la asociatividad:

$$\begin{array}{l}(1)\ \underset{f}{(x+y)}+\underset{f}{z}=f(f^{-1}(x+y)+f^{-1}(z)).\\ \qquad\qquad\quad =f(f^{-1}(\underset{f}{f}(f^{-1}(x)+f^{-1}(y)))+f^{-1}(z)).\\ \qquad\qquad\quad =f(f^{-1}(x)+f^{-1}(y)+f^{-1}(z)).\end{array}$$

$$\begin{array}{l}(2)\ \underset{f}{x}+\underset{f}{(y+z)}=f\left(f^{-1}\left(x\right)+f^{-1}\left(y+z\right)\right).\\ \qquad\qquad\quad =f\left(f^{-1}\left(x\right)+f^{-1}\left(\underset{f}{f}\left(f^{-1}\left(y\right)+f^{-1}\left(z\right)\right)\right)\right).\\ \qquad\qquad\quad =f\left(f^{-1}\left(x\right)+f^{-1}\left(y\right)+f^{-1}\left(z\right)\right).\end{array}$$

Ahora (1) y (2) coinciden pues $\left(f^{-1}\left(x\right)+f^{-1}\left(y\right)\right)+f^{-1}\left(z\right)=f^{-1}\left(x\right)+\left(f^{-1}\left(y\right)+f^{-1}\left(z\right)\right)$.

Veamos que $0_G=f\left(0_G\right)$:

$$\begin{array}{l}\underset{f}{0_G}+x=:f\left(f^{-1}\left(0_G\right)+f^{-1}\left(x\right)\right)\\ \qquad\quad =f\left(f^{-1}\left(f\left(0_G\right)\right)+f^{-1}\left(x\right)\right)\\ \qquad\quad =f\left(0_G+f^{-1}\left(x\right)\right)=ff^{-1}\left(x\right)=x.\end{array}$$

Veamos que $-x=f\left(-f^{-1}\left(x\right)\right)$:

$$\begin{array}{l}\underset{f}{x}+(-x)=:f\left(f^{-1}\left(x\right)+f^{-1}\left(f\left(-\left(f^{-1}\left(x\right)\right)\right)\right)\right)\\ \qquad\qquad =f\left(f^{-1}\left(x\right)+\left(-f^{-1}\left(x\right)\right)\right)\\ \qquad\qquad =f\left(0_G\right)\\ \qquad\qquad =0_G.\end{array}$$

Por consiguiente X es un grupo.

Ahora veamos que si G es abeliano, entonces X es abeliano.

$$\underset{f}{x}+y=:f\left(f^{-1}\left(x\right)+f^{-1}\left(y\right)\right)=f\left(f^{-1}\left(y\right)+f^{-1}\left(x\right)\right):=\underset{f}{y}+x.$$

Claramente f es un homomorfismo de grupos:

$$f\left(a\right)+f\left(b\right)=f\left(f^{-1}\left(f\left(a\right)\right)+f^{-1}\left(f\left(b\right)\right)\right)=f\left(a+b\right).$$

Como f es un morfismo biyectivo entonces f es un isomorfismo. ■

Nota 3 *Se puede hacer la misma observación si G es un anillo, o espacio vectorial o un R-módulo.*

Observación 5 *Si $H \overset{\varphi}{\twoheadrightarrow} G$ es un monomorfismo de grupos, entonces existe un conjunto X ajeno con $G \cup H$ y tal que $|X| = |G \cup H|$.*

Demostración. Como $G \cup H$ es un conjunto, entonces $|G \cup H| < |\mathcal{P}(G \cup H)|$.
Ahora tenemos lo siguiente:

$$\mathcal{P}(G \cup H) = (\mathcal{P}(G \cup H) \cap (G \cup H)) \overset{\bullet}{\cup} \mathcal{P}(G \cup H) \setminus (G \cup H)$$

por lo tanto

$$\mathcal{P}(G \cup H) = |\, \mathcal{P}(G \cup H) \setminus (G \cup H) \,|\,.$$

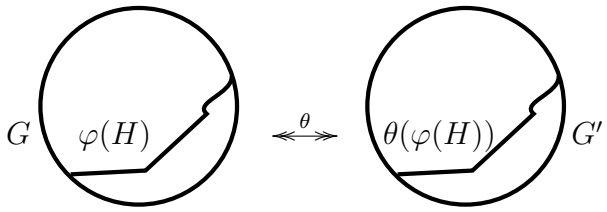
Pues $|\, A \,| + |\, B \,| = \text{máx}\{|\, A \,|, |\, B \,|\}$ si uno de ellos es infinito, entonces:

$$|\, \mathcal{P}(G \cup H) \setminus (G \cup H) \,| \geq |\, G \cup H \,|$$

y $\mathcal{P}(G \cup H) \setminus (G \cup H)$ es un conjunto ajeno con $G \cup H$. Por lo tanto $\mathcal{P}(G \cup H)$ tiene un subconjunto de cardinalidad $|\, G \cup H \,|$ ajeno con $G \cup H$.

Supongamos que X es un conjunto ajeno con $G \cup H$ y con tantos elementos como $G \cup H$ y sea $H \overset{\varphi}{\twoheadrightarrow} G$ un monomorfismo de grupos:

X contiene un subconjunto G' con tantos elementos como G. Sea $G \overset{\theta}{\twoheadleftarrow} G'$ una biyección.



Tenemos que $(G' \setminus \theta(\varphi(H))) \cup H$ es un conjunto con tantos elementos como G que contiene a H. Ahora veamos lo siguiente:

$$H \overset{i_H^{(G' \setminus \theta(\varphi(H))) \cup H}}{\hookrightarrow} \underbrace{(G' \setminus \theta(\varphi(H))) \cup H}$$

$$\begin{array}{ccc} (G' \setminus \theta(\varphi(H))) \ni x & \Big\downarrow & h \in H \\ \Big\downarrow \theta^{-1} & G & \Big\downarrow \varphi \\ \theta^{-1}(x) & & \varphi(h) \end{array}$$

Así que $H \leq (G' \setminus \theta(\varphi(H))) \cup H$ y $(G' \setminus \theta(\varphi(H))) \cup H \cong G$. ■

Corolario 3 *Todo grupo abeliano es un subgrupo de un grupo divisible.*

Demostración. Sea G un grupo y $\varphi\colon G \rightarrowtail D$ un monomorfismo de G en D, donde D es un grupo divisible. Con la construcción anterior, $G \leq D'$ con $D' \cong D$.

D divisible y $D' \cong D \Longrightarrow D'$ es divisible. (si $D \overset{f}{\rightarrowtail} D'$ es isomorfismo, entonces $pD' = pf(D) = f(pD) = f(D) = D'$). ■

Definición 12 *A es un subgrupo esencial de B si $A \cap C \neq \{0\}$ para cualquier subgrupo C de B con $C \neq \{0\}$ y lo denotaremos por $A \leq_{es} B$.*

Observación 6 *Son equivalentes para $A \leq B$:*

1) A es esencial en B

2) $\forall\ 0 \neq b \in B\ \exists\ 0 \neq z \in \mathbb{Z}$ tal que $0 \neq zb \in A$.

Demostración.

1) $\Longrightarrow$ 2) $A \cap \mathbb{Z}b \neq \{0\}$ por lo tanto $\exists\ 0 \neq zb \in A$.

2) $\Longrightarrow$ 1) Si $\{0\} \neq C \leq B$ y $0 \neq c \in C$, entonces $\exists z \in \mathbb{Z}$ tal que $0 \neq zc \in A$. Entonces $zc \in A \cap C$ y por lo tanto $A \cap C \neq \{0\}$.

■

Definición 13 *Si B es máximo en $\{N \leq M | A \cap N = \{0\}\}$ decimos que B es un seudocomplemento de A en M.*

Lema 8 *Si $A \leq M$, entonces A tiene un seudocomplemento B en M.*

Demostración. Sea $\mathcal{S} = \{B \leq G | A \cap B = \{0\}\}$. Si $\mathcal{C}$ es una cadena en $\mathcal{S}$, $\mathcal{C} = \{B_i\}_{i \in I}$, entonces $\cup\mathcal{C} \leq G$ y si $x \in A \cap (\cup\mathcal{C})$, entonces $x \in A$ y $x \in B_i$ para alguna $i \in I$, por lo tanto $x \in A \cap B_i = \{0\}$ luego $x = 0$. Ahora $A \cap (\cup\mathcal{C}) = \{0\}$. Por el Lema de Zorn $\exists B$ máximo en $\mathcal{S}$; así B es un seudocomplemento de A. ■

Lema 9 *Sea G un grupo abeliano. Si B es un seudocomplemento de A, entonces:*

$$A \cap B = \{0\} \quad \vee \quad A \oplus B \leq_{es} G.$$

Demostración. Si no ocurriese que $A \oplus B \leq_{es} G$, entonces $\exists g$ no cero en G tal que $(A \oplus B) \cap \mathbb{Z}g = \{0\}$. Entonces $(A \oplus B) \oplus \mathbb{Z}g \leq G$. Pero tenemos que $(A \oplus B) \oplus \mathbb{Z}g = A \oplus (B \oplus \mathbb{Z}g)$. Ahora $B < (B \oplus \mathbb{Z}g)$ y vemos que $A \cap (B \oplus \mathbb{Z}g) = \{0\}$: $a = b + zg$ por lo tanto $a - b = zg$ y como $(A \oplus B) \cap \mathbb{Z}g = \{0\}$ se sigue que $a = b$ y $zg = 0$, luego $a = b \in A \cap B = \{0\}$ entonces $a = 0 \wedge b = 0$.

Esto contradice que B es un seudocomplemento de A. Por lo tanto $A \oplus B \leq_{es} G$. ■

Definición 14 *A es esencialmente cerrado en G un grupo abeliano, si A no está contenido esencialmente en un subgrupo de G que contenga propiamente a A.*

Nota 4 *La definición anterior simbólicamente significa lo siguiente:*

$$A \leq_{es} B \leq G \Longrightarrow A = B.$$

Lema 10

$$i) A \leq_{es} B \leq_{es} G \Longrightarrow A \leq_{es} G.$$
$$ii) A \leq_{es} G \text{ y } A \subseteq B \subseteq G \Longrightarrow B \leq_{es} G.$$

Demostración. *i)* Si $A \leq_{es} B \leq_{es} G$ y $0 \neq x \in G$, entonces $\exists z \in \mathbb{Z}$ tal que $0 \neq zx \in B$. Como $A \leq_{es} B$ $\exists$ $w \in \mathbb{Z}$ tal que $0 \neq w(zx) \in A$ y como $w(zx) = (wz)x$ entonces $A \leq_{es} G$. *ii)* Si $A \leq B \leq G$, $A \leq_{es} G$, $\forall$ $0 \neq g \in G$ $\exists$ $0 \neq zg \in A \subseteq B$ por lo tanto $B \leq_{es} G$. ■

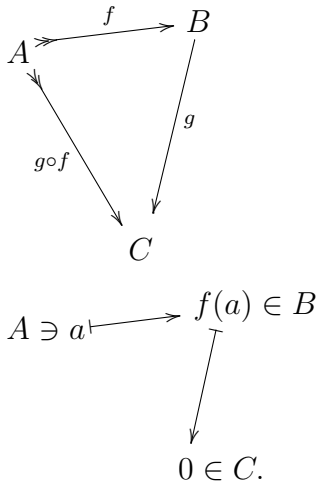
Definición 15 *Un monomorfismo de grupos abelianos* $A \overset{f}{\twoheadrightarrow} B$ *es esencial si*

$$f(A) \leq_{es} B.$$

Lema 11 *Son equivalentes para* $A \overset{f}{\twoheadrightarrow} B$ *monomorfismo:*

1. $f(A) \leq_{es} B$.
2. $g \circ f$ *es monomorfismo* $\Longrightarrow$ g *es monomorfismo.*

Demostración. *1.* $\Longrightarrow$ *2.* Veamos el siguiente diagrama:



Sabemos que $Nuc(g \circ f) = \{0\}$ y como $f^{-1}(Nuc(g)) = Nuc(g \circ f)$ entonces es claro que $f^{-1}(Nuc(g)) = \{0\}$. Si $Nuc(g) \neq \{0\}$, entonces $f(A) \cap Nuc(g) \neq \{0\}$ pues f es un monomorfismo esencial, es decir; $f(A) \leq_{es} B$. Por lo tanto $\exists a \in A$ tal que $0 \neq f(a) \in Nuc(g)$ así que $g(f(a)) = 0$ luego $0 \neq a \in Nuc(g \circ f) = \{0\}$ que es una contradicción.

2. $\Longrightarrow$ *1.* Supongamos que $g \circ f$ es monomorfismo $\Longrightarrow g$ es monomorfismo. Si $A \xrightarrow{f} B$ no fuera esencial: no sucede que $f(A) \leq_{es} B$, entonces hay un seudocomplemento de $f(A)$ que no es $\{0\}$. Sea C un seudocomplemento de $f(A)$ en B entonces $f(A) \oplus C \leq B$.

Por consiguiente

$$\frac{f(A) \oplus C}{C} \leq B/C.$$

Ahora del diagrama siguiente $A \xrightarrow{f} B \xrightarrow{\rho} B/C$ vemos que ρ no es monomorfismo pues $Nuc(\rho) = C \neq \{0\}$. Pero $A \xrightarrow{\rho \circ f} B/C$ sí es monomorfismo: Si $a \in Nuc(\rho \circ f)$, entonces $\rho(f(a)) = 0$ por lo tanto $f(a) \in Nuc(\rho) = C$ ahora $f(a) \in f(A) \cap C = \{0\}$. Entonces $\rho \circ f$ es monomorfismo pero ρ no es monomorfismo lo que contradice a *2.* ■

Lema 12 *Todo subgrupo A de M es esencial en un subgrupo B de M, que es máximo con esta propiedad.*

Demostración. Sea $\mathcal{E} = \{\mathcal{U} \leq M | A \leq_{es} \mathcal{U}\}$. Si $\mathcal{C}$ es una cadena en $\mathcal{E}$, veamos que $A \leq_{es} \cup\mathcal{C}$ donde $\mathcal{C} = \{C_i\}_{i \in I}$. Si $0 \neq x \in \cup\mathcal{C}$, entonces $x \in C_i$ para alguna $i \in I$. Como $A \leq_{es} C_i$ entonces $\exists z \in \mathbb{Z}$ con $z \neq 0$ tal que $0 \neq zx \in A$. Por lo tanto $A \leq_{es} \cup\mathcal{C}$.

Por el Lema de Zorn $\mathcal{E}$ tiene un elemento máximo B. Entonces $A \leq_{es} B$ y si $A \leq_{es} B < C \leq M$ entonces $A \leq_{\not es} C$, en particular $B \leq_{\not es} C \ \forall \ B < C$.

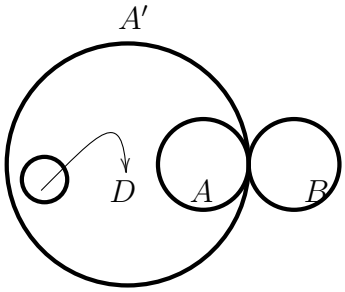
Así que B es esencialmente cerrado (la única extensión de B dentro de M, donde B es esencial es B misma). ■

Teorema 5 *Son equivalentes para $A \leq M$:*

1) A es esencialmente cerrado en M.

2) A es el seudocomplemento de un subgrupo B de M.

Demostración. *1)* $\Longrightarrow$ *2)* Supongamos que A es esencialmente cerrado. Sea B un seudocomplemento de A. Entonces B es máximo tal que $A \cap B = \{0\}$. Sea A' que contiene a A máximo tal que $A' \cap B = \{0\}$. A' es un seudocomplemento de B que contiene a A.



Notemos que $A \leq_{es} A'$: No $\exists\{0\} \neq D \leq A'$ tal que $A \cap D = \{0\}$. Entonces $A \oplus D \subseteq A'$ por lo tanto $(A \oplus D) \oplus B = A \oplus (D \oplus B) \leq M$. Pero entonces $A \cap (D \oplus B) = \{0\}$ y $B < D \oplus B$

contradiciendo que B es un seudocomplemento de A. Por lo tanto tenemos ahora que $A \leq_{es} A'$ pero como A es esencialmente cerrado, entonces $A = A'$ que es seudocomplemento de B.

2) $\Longrightarrow$ *1)* Supongamos que A es seudocomplemento de B.

Si $A \leq_{es} X \leq M$, entonces $B \cap X \leq X$ y $A \cap (B \cap X) = A \cap B = \{0\}$. Como $A \leq_{es} X$ entonces $B \cap X = \{0\}$ $(A \leq X \Longrightarrow A \cap X = A)$ y como A es seudocomplemento de B, entonces $A = X$. Así que $A \leq_{es} X \Longrightarrow A = X$. Es decir; A es esencialmente cerrado. ■

Lema 13 *Un subgrupo esencialmente cerrado de un grupo abeliano divisible es un sumando directo.*

Demostración. Supongamos que A es esencialmente cerrado en D divisible. A es el seudocomplemento de B un subgrupo de D, entonces $A \oplus B \leq_{es} D$. Podemos suponer que B también es esencialmente cerrado, pues lo podemos cambiar por B' un seudocomplemento de A que contenga a B. Así que $A \oplus B \leq_{es} D$ y A, B son esencialmente cerrados, B es un seudocomplemento de A.

Veamos que

$$\frac{A \oplus B}{B} \leq_{es} D/B.$$

Si $C/B \leq D/B$ y $\dfrac{A \oplus B}{B} \cap C/B = \{0\}$, entonces $(A \oplus B) \cap C = B$ y como $B \leq C$ por la propiedad modular:

$$B = (A \oplus B) \cap C = (A \cap C) \oplus B$$

por lo tanto $A \cap C = \{0\}$ pero B seudocomplemento de A y $B \leq C$ implican $B = C$. Por lo tanto $C/B = B/B = \{0\}$. Ahora tenemos el siguiente diagrama:

$$\begin{array}{ccc} A \cong \dfrac{A \oplus B}{B} & \xhookrightarrow[es]{i} & D/B \\ {\scriptstyle i_A^D}\big\downarrow & & \\ D & & \end{array}$$

Como D es divisible, $\exists\ \varphi :\ D/B \longrightarrow D$ tal que conmuta el diagrama siguiente:

$$\begin{array}{ccc} A & \overset{m}{\underset{es}{\twoheadrightarrow}} & D/B \\ {\scriptstyle i_A^D}\big\downarrow & \swarrow_{\varphi} & \\ D. & & \end{array}$$

Como m es esencial e i_A^D es monomorfismo, entonces φ es monomorfismo, $A \leq Im(\varphi)$ y $A \leq_{es} Im(\varphi)$. Como A es esencialmente cerrado, entonces $A = Im(\varphi)$ por lo tanto φ es una escisión para m. Ahora $m(A)$ es sumando directo esencial de D/B. $m(A)$ es esencial y un sumando directo solamente puede pasar si $m(A) = D/B$. Por lo tanto $\dfrac{A \oplus B}{B} = \dfrac{D}{B}$ por tanto $A \oplus B = D$. ■

Definición 16 *Si E es una extensión esencial de M y E es inyectivo, entonces E se llama cápsula inyectiva de M.*

Teorema 6 *Todo grupo abeliano tiene cápsulas divisibles.*

Demostración. Si M es un grupo abeliano; M es un subgrupo de un grupo divisible E por el Corolario 3, pues como $\mathbb{Q}/\mathbb{Z}$ es un cogenerador divisible hay un conjunto X tal que existe

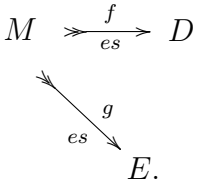
$$M \overset{f}{\rightarrowtail} (\mathbb{Q}/\mathbb{Z})^X \ .$$

Ahora por el Corolario 3 podemos suponer que $M \hookrightarrow E$ con E un grupo divisible.

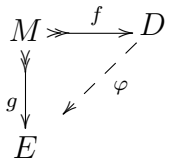
M está contenido en una extensión esencial máxima D, $D \leq E$ por el Lema 12, así que claramente D es esencialmente cerrado en E. Así que D es divisible por el Lema 13. Entonces D es un grupo divisible que contiene esencialmente a M. ■

Teorema 7 *Las cápsulas divisibles de un grupo abeliano M son isomorfas.*

Demostración. Sean



Como E es divisible y f es monomorfismo $\exists\ \varphi$: $D \overset{}{\rightarrowtail} E$ tal que el diagrama siguiente



conmuta. Entonces $\varphi(D)$ es un divisible contenido en E. Entonces $\varphi(D)$ es un sumando directo de E ($E = \varphi(D) \oplus E'$ para algún subgrupo E' de E). Ahora como $\varphi \circ f = g$, entonces $Im(g) \leq Im(\varphi)$.

Como g es monomorfismo esencial, entonces $Im(g) \leq_{es} E$, como $Im(g) \leq Im(\varphi) \leq E$, entonces $Im(\varphi) \leq_{es} E$ por el Lema 10 inciso *ii)*. Entonces $Im(\varphi)$ es un sumando directo esencial de E; así que $E = \varphi(D) \oplus E'$ por lo que $E' = \{0\}$. Por lo tanto $E = \varphi(D)$ y así φ es epimorfismo.

Como $\varphi \circ f = g$ es un monomorfismo y f es un monomorfismo esencial, entonces φ es un monomorfismo por el Lema 11 por lo tanto φ es un isomorfismo. ■

Observación 7 $\mathbb{Q}$ *es la cápsula divisible de* $\mathbb{Z}$.

Tenemos que $\mathbb{Z} \overset{i_{\mathbb{Z}}^{\mathbb{Q}}}{\hookrightarrow} \mathbb{Q}$ *es un monomorfismo esencial: todo racional distinto de cero tiene un múltiplo distinto de cero:* $(b\frac{a}{b} = a \in \mathbb{Z})$.

Recuerde que:

Definición 17 *Un grupo abeliano T es de torsión si todos sus elementos son de orden finito.*

Si M es un grupo abeliano y $n > 0$ es un natural, entonces $M \xrightarrow{n\cdot -} M$ es un homomorfismo de grupos: $n(x+y) = nx+ny$. Ahora $Im(n\cdot -) = nM$ es un subgrupo de M y el $Nuc(n\cdot -)$ donde tenemos que $Nuc(n\cdot -) = \{x \in M | nx = 0\}$ también es un subgrupo de M. Luego:

$$Nuc(n\cdot -) = \{x \in M |\ o(x) \mid n\}.$$

Si $n = p^k$, entonces $(0 : p^k) := \{x \in M \mid p^k \cdot x = 0\}$ es un subgrupo de M.

Observación 8 *$\{(0 : p^k) \mid k \in \mathbb{N}\}$ es una cadena de subgrupos de M. Tenemos que si $k < l$, entonces $p^k \cdot x = 0 \Longrightarrow p^l \cdot x = 0$ por lo tanto $k < l \Longrightarrow (0 : p^k) \subseteq (0 : p^l)$.*

Como la unión de una cadena de subgrupos de M es un subgrupo de M entonces

$$\cup_{k\in\mathbb{N}}\{(0 : p^k)\} = \{x \in M \mid o(x) \text{ es una potencia de } p\} \leq M.$$

Notación 1 *Denotaremos este grupo $t_p(M)$. $t_p(M)$ es la parte p-primaria de M, y coincide con el p-subgrupo de Sylow de M.*

Definición 18 *Sea G un grupo abeliano y $\{A_i \leq G\}_{i\in I}$ una familia de subgrupos de G. La familia de subgrupos es independiente si $\forall i \in I$, $A_i \cap (\sum_{j\in I\setminus\{i\}} A_j) = \{0\}$; en ese caso escribimos*

$$\sum A_i = \bigoplus_I A.$$

Teorema 8 *Un grupo abeliano de torsión T es la suma directa de sus partes p-primarias:*

$$T = \bigoplus_{p\in\mathbb{P}} t_p(T).$$

Demostración. Veamos primero que $\{t_p(T)\}_{p\in\mathbb{P}}$ es una familia independiente de subgrupos de T, es decir que para cada primo p, $t_p(T) \cap (\sum_{q\in\mathbb{P}\setminus\{p\}} t_q(T)) = \{0\}$. Sea $x \in t_p(T) \cap (\sum_{q\in\mathbb{P}\setminus\{p\}} t_q(T))$, entonces $o(x) = p^m$ para alguna m. Además $x = y_1 + \cdots + y_n$ con $y_i \in t_{q_i}(T)$ donde $q_1, ..., q_n$ son primos distintos de p.

Digamos que $o(y_i) = q_i^{s_i}$ con $s_i \in \mathbb{Z}^+$. Entonces

$$q_1^{s_1} \cdots q_n^{s_n}(y_1 + \cdots + y_n) = 0.$$

Así que $o(x) \mid q_1^{s_1} \cdots q_n^{s_n}$. Ahora $p \mid q_i$ para alguna i. Como q_i y p son primos, esto sólo es posible si $p = q_i$, lo que contradice la hipótesis. Por lo tanto

$$t_p(T) \cap \sum_{q\in\mathbb{P}\setminus\{p\}} t_q(T) = \{0\}.$$

Veamos ahora que

$$T = \sum_p t_p(T).$$

Si $0 \neq x \in T$, entonces $o(x) = p_1^{n_1} \cdots p_k^k$, para algún conjunto finito de primos y algunos $n_1, ..., n_k$ enteros positivos.

Definamos $p_i^{'} = \dfrac{o(x)}{p_i^{n_i}} = p_1^{n_1} \cdots \not{p}_i^{n_i} \cdots p_k^{n_k}$ para $i \in \{1, ..., k\}$.

Notemos que p_i no divide a $p_i^{'}$. Veamos a continuación que $\{p_1^{'}, p_2^{'}, ..., p_k^{'}\}$ es un conjunto cuyo máximo común divisor es 1. Denotemos por $(p_1^{'};\ ...\ ; p_k^{'})$ al máximo común divisor de $\{p_1^{'}, ..., p_k^{'}\}$.

Ahora lo siguiente:

$$(p_1^{'};\ ...\ ; p_k^{'}) \mid p_1^{'} \ \wedge \ p_1^{'} \mid o(x) = p_1^{n_1} \cdots p_k^{n_k}.$$

Por lo tanto

$$(p_1^{'};\ ...\ ; p_k^{'}) = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \quad \text{con} \quad \alpha_i \leq n_i.$$

Como p_1 no divide a $p_1^{'}$ entonces $\alpha_i = 0$. Lo mismo se puede decir de cada i por lo tanto

$$(p_1^{'};\ ...\ ; p_k^{'}) = p_1^0 \cdots p_k^0 = 1.$$

Entonces hay una combinación entera $z_1 p_1^{'} + \cdots + z_k p_k^{'} = 1$ ahora

$$x = z_1 p_1^{'} x + \cdots + z_k p_k^{'} x.$$

Notemos ahora que

$$p_i^{n_i}(p_i^{'} x) = (p_i^{n_i} p_i^{'}) x = o(x) \cdot x = 0.$$

Así que

$$p_i^{'} x \in t_{p_i}(T) \quad y \quad x \in t_{p_1}(T) \oplus t_{p_2}(T) \oplus \cdots \oplus t_{p_k}(T).$$

Por lo tanto

$$T = \sum t_p(T) = \bigoplus t_p(T).$$

■

Definición 19

$$\mathbb{Z}_{p^\infty} := t_p(\mathbb{Q}/\mathbb{Z}).$$

Nota 5 *$\mathbb{Z}_{p^\infty}$ es un grupo divisible de torsión pues es un sumando directo de $\mathbb{Q}/\mathbb{Z}$ que es divisible y de torsión: Como $\mathbb{Q}$ es divisible, entonces $\mathbb{Q}/\mathbb{Z}$ es divisible. Ahora como $\mathbb{Z}_{p^\infty} := t_p(\mathbb{Q}/\mathbb{Z})$ tenemos que*

$$\mathbb{Q}/\mathbb{Z} = \bigoplus_{p \in \mathbb{P}} \mathbb{Z}_{p^\infty}.$$

A continuación describiremos $\mathbb{Z}_{p^\infty}$ y sus subgrupos.

Notación 2 $\overline{a/b} = \frac{a}{b} + \mathbb{Z}$. *Ahora*

$$\mathbb{Z}_{p^\infty} = \{\frac{a}{b} + \mathbb{Z} \quad | \quad o(\overline{a/b}) = p^n \text{ para alguna } n\}.$$

Observación 9 *Si* $o(\overline{a/b}) = p^n$, *entonces* $\overline{a/b} = \overline{z/p^n}$ *para alguna* $z \in \mathbb{Z}$ *tal que* $p \nmid z$. *En efecto,* $p^n a = bz$, *para algún entero* z. *Vemos que* p^n *es mínima con la propiedad anterior, por lo que* p *no divide a* z. *Entonces* $\overline{a/b} = \overline{z/p^n}$.

Corolario 4 $\mathbb{Z}_{p^\infty} = \{\frac{a'}{p^n} + \mathbb{Z} \quad | \quad (p; a') = 1 \text{ con } a' \in \mathbb{Z}\}$.

Demostración. Se sigue de la observación previa. ■

Ahora todo elemento $\overline{a/p^n} + \mathbb{Z}$ pertenece a $< \{\overline{1/p^n}\} >$. Entonces:

$$\{\overline{1/p}, \overline{1/p^2}, \overline{1/p^3}, \overline{1/p^4}, \overline{1/p^5}, ...\} \quad \text{genera } \mathbb{Z}_{p^\infty}.$$

Notemos que $\overline{1/p^m} \notin < \overline{1/p^n} >$ si $m > n$. En efecto, supongamos lo contrario.

Si $\overline{1/p^m} \in < \overline{1/p^n} >$ entonces $p^m = o(\overline{1/p^m})$ y $p^m \mid o(\overline{1/p^n}) = p^n$ por lo tanto $p^m \mid p^n$ lo cual implica $m \leq n$. Entonces $\mathbb{Z}_{p^\infty}$ no está generado por un número finito de $\{\overline{1/p^i}\}_{i \in \mathbb{Z}^+}$.

Notemos también que $\mathbb{Z}_{p^\infty}$ no tiene subgrupos máximos porque es divisible.

Los grupos abelianos finitamente generados no triviales tienen subgrupos máximos, (recordemos que convenimos en que máximo es máximo propio) como se puede verificar por inducción matemática.

Lema 14 *Si* $\{0\} \neq {}_{\mathbb{Z}}M =< \{x_1, x_2, x_3, ..., x_n\} >$, *entonces* M *tiene un subgrupo máximo.*

Demostración. Por inducción sobre n:

Base:
Si $n = 1$, entonces $M = \mathbb{Z}x_1$ y tenemos el epimorfismo:

$$\mathbb{Z} \xrightarrow{-x_1} \mathbb{Z}x_1$$

cuyo núcleo es $(0 : x_1) = \{z \in \mathbb{Z} \quad | \quad zx_1 = 0\}$. Ahora por el Teorema de la correspondencia (Si dos grupos son isomorfos, entonces sus respectivos conjuntos de subgrupos son conjuntos ordenados isomorfos), tenemos lo siguiente: $[(0 : x_1), \mathbb{Z}]$ y $[\{0\}, \mathbb{Z}x_1]$ son conjuntos ordenados isomorfos. Notemos que $(0 : x_1) = \mathbb{Z}o(x_1)$ donde $o(x_1)$ denota el orden de x_1.

Como $x_1 \neq 0$ porque $\mathbb{Z}x_1 \neq 0$, entonces $o(x_1) \neq 1$, y existe $p \in \mathbb{P}$ tal que $p \mid o(x_1)$, entonces $\mathbb{Z}o(x_1) \subseteq \mathbb{Z}p$ y $\mathbb{Z}p$ es máximo en $\mathbb{Z}$ ($\mathbb{Z}/p\mathbb{Z} \cong {}_{\mathbb{Z}}\mathbb{Z}_p$ que es simple).

Entonces $[\mathbb{Z}o(x_1), \mathbb{Z}]$ tiene un máximo, así que $[\{0\}, \mathbb{Z}x_1]$ también lo tiene.

Paso inductivo:

Supongamos que $n > 1$ y que un grupo $N \neq \{0\}$ generado por menos de n elementos tiene máximos. Así, $M = \mathbb{Z}x_1 + \cdots + \mathbb{Z}x_n$. Si escribimos $N = \mathbb{Z}x_1 + \cdots + \mathbb{Z}x_{n-1}$, entonces N tiene máximos por la hipótesis de inducción. Así que si $N = M$ ya acabamos.

Si $N < M$, entonces $\{0\} \neq M/N = N + \mathbb{Z}x_n/N \cong \mathbb{Z}x_n/N \cap \mathbb{Z}x_n$ es un grupo generado por $x_n + (N \cap \mathbb{Z}x_n)$, así que por la base de la inducción, $\mathbb{Z}x_n/N \cap \mathbb{Z}x_n$ tiene máximos.

Por el Teorema de la correspondencia vemos que M/N tiene un subgrupo máximo L/N, digamos. Por el Teorema de la correspondencia, L es un subgrupo máximo de M. Esto completa la inducción. ■

Corolario 5 *Un grupo divisible $D \neq \{0\}$ no es finitamente generado, porque D no tiene máximos.*

Demostración. Un grupo abeliano es divisible si y sólo si no tiene máximos. Aplicamos el lema anterior para concluir. ■

Corolario 6 *$\mathbb{Z}_{p^\infty}$ no tiene máximos.*

Demostración. Se sigue del corolario previo, pues $\mathbb{Z}_{p^\infty}$ es divisible. ■

Lema 15 *Si $\{0\} \neq H < \mathbb{Z}_{p^\infty}$, entonces $H =< \overline{1/p^n} >$ para cierto $n \in \mathbb{Z}^+$.*

Demostración. Tenemos $\{0\} \neq H < \mathbb{Z}_{p^\infty} =< \{\overline{1/p}, \overline{1/p^2}, \overline{1/p^3}, \overline{1/p^4}, \overline{1/p^5}, ...\} >$.

Como H es propio, entonces H no contiene a todos los $\overline{1/p^n}$. Sea $\overline{1/p^m} \notin H$ $(m \geq 1)$ con m mínimo.

Ahora $p^k \cdot \overline{1/p^{m+k}} = \overline{1/p^m} \notin H$. Entonces $\overline{1/p^{m+1}}$, $\overline{1/p^{m+2}}$, $\overline{1/p^{m+3}}$, $\overline{1/p^{m+4}}$, ... $\notin H$.

Por la elección de m vemos que $\overline{1/p}$, $\overline{1/p^2}$, $\overline{1/p^3}$,...,$\overline{1/p^{m-1}} \in H$. Así $< \overline{1/p^{m-1}} > \leq H$ y sabemos que $\overline{1/p^m} \notin H$.

Si la inclusión fuera propia, sea $\overline{a/p^l} \in H \setminus < \overline{1/p^{m-1}} >$ con $l > 0$ y p no divide a a. Entonces $l > m - 1$ ya que $\overline{1/p}$,...,$\overline{1/p^{m-1}} \in H$. Por lo tanto $\overline{a/p^l} \in H \setminus < \overline{1/p^{m-1}} >$, $l \geq m$.

Como p no divide a a entonces $(p^l; a) = 1$, por lo tanto $\exists \alpha, \beta \in \mathbb{Z}$ tales que $\alpha a + \beta p^l = 1$. Entonces $\alpha(\overline{a/p^l}) = \overline{\alpha a/p^l} = \overline{1 - \beta p^l/p^l} = \overline{1/p^l} - \overline{\beta \not{p}^l/\not{p}^l} = \overline{1/p^l} \in H$ con $l \geq m$, contradicción.

Esta contradicción prueba que $H = < \overline{1/p^{m-1}} >$.

Entonces los subgrupos propios de $\mathbb{Z}_{p^\infty}$ son los siguientes:

$$< \overline{1/p} > \leq < \overline{1/p^2} > \leq < \overline{1/p^3} > \leq < \overline{1/p^4} > \leq .$$

Es decir que los subgrupos de $\mathbb{Z}_{p^\infty}$ son un conjunto totalmente ordenado, es decir forman una cadena.

Como en un grupo cuyo conjunto de subgrupos es una cadena, todo subgrupo distinto de $\{0\}$ es esencial, entonces todo subgrupo distinto de $\{0\}$ de $\mathbb{Z}_{p^\infty}$ es esencial.

Entonces tenemos el diagrama siguiente:

$$\begin{array}{ccc} < \overline{1/p^n} > & \cong & \mathbb{Z}_{p^n} \overset{i^{\mathbb{Z}_{p^\infty}}_{\mathbb{Z}_{p^n}}}{\underset{es}{\hookrightarrow}} \mathbb{Z}_{p^\infty} \\ \| \wr & & \\ \mathbb{Z}_{p^n} \ . & & \end{array}$$

Así; $\mathbb{Z}_{p^\infty}$ es la cápsula divisible de $\mathbb{Z}_p$, $\mathbb{Z}_{p^2}$, $\mathbb{Z}_{p^3}$, $\mathbb{Z}_{p^4}$,..., $\mathbb{Z}_{p^n}$,... . ■

Corolario 7 *Todo grupo divisible que tenga un elemento distinto de* 0 *de orden finito contiene una copia de* $\mathbb{Z}_{p^\infty}$ *para algún primo* p.

Demostración. Si $0 \neq x \in D$, D divisible y $o(x)$ finito, entonces $o(x) \neq 1$, y así $\exists\, p \in \mathbb{P}$ tal que $p \mid o(x)$ por lo tanto $o(x^{o(x)/p}) = p$. Entonces D contiene un elemento de orden p y entonces D contiene una copia de $\mathbb{Z}_p$. Ahora existe un monomorfismo $f\colon\ \mathbb{Z}_p \rightarrowtail D$ y como D es divisible, $\exists\, \varphi\colon \mathbb{Z}_{p^\infty} \longrightarrow D$ tal que $\varphi \circ i = f$, es decir; el diagrama siguiente conmuta:

$$\begin{array}{ccc} \mathbb{Z}_p & \overset{f}{\rightarrowtail} & D \\ {\scriptstyle es}\downarrow & \nearrow_{\varphi} & \\ \mathbb{Z}_{p^\infty} \ . & {\scriptstyle i} & \end{array}$$

Como i es monomorfismo esencial y f es monomorfismo, entonces φ es monomorfismo.

Ahora tenemos el diagrama siguiente:

$$\begin{array}{ccc} \varphi(\mathbb{Z}_{p^\infty}) & \overset{i^D_{\varphi(\mathbb{Z}_{p^\infty})}}{\hookrightarrow} & D \\ \wr \| & & \\ \mathbb{Z}_{p^\infty} \ . & & \end{array}$$

Como podemos ver $\varphi(\mathbb{Z}_{p^\infty})$ es una copia de $\mathbb{Z}_{p^\infty}$ contenida en D.
Notemos que $\mathbb{Z}_{p^\infty} \cong \varphi(\mathbb{Z}_{p^\infty}) \leq D$. ■

Nota 6 *Si* D *es un grupo divisible con un elemento de orden infinito, entonces* D *contiene una copia de* $\mathbb{Q}$. *En efecto: si* $x \in D$ *es de orden infinito, entonces* $\mathbb{Z}x \cong \mathbb{Z}$. *Así existe el siguiente diagrama:*

$$\begin{array}{ccc} \mathbb{Z} & \overset{f}{\rightarrowtail} & D \\ {\scriptstyle es}\downarrow & \nearrow_{\varphi} & \\ \mathbb{Q}. & {\scriptstyle i^{\mathbb{Q}}_{\mathbb{Z}}} & \end{array}$$

Como D es divisible e $i_{\mathbb{Z}}^{\mathbb{Q}}$ es monomorfismo, $\exists\ \varphi\colon \mathbb{Q} \longrightarrow D$ tal que $\varphi \circ i_{\mathbb{Z}}^{\mathbb{Q}} = f$.

Como $i_{\mathbb{Z}}^{\mathbb{Q}}$ es un monomorfismo esencial y f es monomorfismo, entonces φ es monomorfismo. Por lo tanto:

$$\begin{array}{ccc} \varphi(\mathbb{Q}) & \xrightarrow{i^{D}_{\varphi(\mathbb{Q})}} & D \\ \wr\| & & \\ \mathbb{Q}\,. & & \end{array}$$

Además $\varphi(\mathbb{Q})$ es sumando directo de D porque $\varphi(\mathbb{Q})$ es divisible.

Lema 16 *El subgrupo de torsión de un grupo divisible D es divisible.*

Demostración. Sea D divisible y $t(D) \leq D$. Si $p \in \mathbb{P}$ y $0 \neq x \in t(D)$, entonces $x = py$ con $y \in D$. Ahora $o(x) = o(py) = \frac{o(y)}{(p;o(y))}$ por lo tanto

$$o(y) = o(x)(p; o(y))$$

que es un número natural. Entonces $o(y)$ es finito. Así $x = py$ con $y \in t(D)$ luego

$$t(D) \leq p(t(D)).$$

Por lo tanto $t(D) = p(t(D))$, $\forall\ p \in \mathbb{P}$. Por lo tanto $t(D)$ es divisible. ■

Notación 3 *$A \trianglelefteq B$ denotará que A es un sumando directo de B.*

Corolario 8 *$t(D) \trianglelefteq D$ si D es divisible.*

Demostración. $t(D)$ es un subgrupo divisible de D también se debe al Lema 7. ■

Observación 10 *Sea $D \cong \mathbb{Q}^{(X)} \oplus (\bigoplus_{p\in\mathbb{P}} \mathbb{Z}_{p^\infty}^{(X_p)})$ donde X, X_p son conjuntos y $p \in \mathbb{P}$. Entonces D es un grupo divisible.*

Demostración. Sabemos que una suma directa de grupos divisibles es divisible. ■

Proposición 2 *D grupo divisible $\Longrightarrow D \cong \mathbb{Q}^{(X)} \oplus (\bigoplus_{p\in\mathbb{P}} \mathbb{Z}_{p^\infty}^{(X_p)})$.*

Demostración. Tenemos que la parte de torsión de D:

$$t(D) = \{x \in D \ \mid o(x) \text{ es finito}\}$$

es divisible, entonces $D = t(D) \oplus F$ con F un subgrupo de D tal que $t(F) = 0$. Es decir F no tiene elementos de orden finito y entonces todos sus elementos son de orden infinito. Digamos que $t(D) = T$, entonces $D = T \oplus F$ la suma directa de un divisible de torsión y un divisible libre de torsión.

$$T = \bigoplus_{p\in\mathbb{P}} t_p(T).$$

Basta ver que $F \cong \mathbb{Q}^{(X)}$ para algún conjunto X y que $t_p(T) \cong \mathbb{Z}_{p^\infty}^{(X_p)}$ para algún conjunto X_p.

Supongamos que F es divisible libre de torsión.

Caso 1) Si $F = \{0\}$, podemos tomar $X = \emptyset$ ($\mathbb{Q}^\emptyset \cong \{0\}$).

Caso 2) Supongamos que $F \neq \{0\}$. Por la Nota 6 F contiene una copia de $\mathbb{Q}$. Sea $\{Q_i\}_{i\in I}$ una familia independiente máxima (estamos usando el Lema de Tukey) de subgrupos de F cada uno isomorfo a $\mathbb{Q}$. Ahora

$$\bigoplus_{i\in I} Q_i \leq F,$$

$\bigoplus_{i\in I} Q_i$ es divisible, así que $\bigoplus_{i\in I} Q_i \trianglelefteq F$ y entonces $F = (\bigoplus_{i\in I} Q_i)\oplus\mathfrak{U}$ con $\mathfrak{U}$ un subgrupo de F divisible, por ser un sumando directo. Si $\mathfrak{U} \neq \{0\}$, entonces $\mathfrak{U}$ contendría una copia de $\mathbb{Q}$, con lo que podriamos extender a la familia $\{Q_i\}_{i\in I}$: $\{Q_i\}_{i\in I} \cup \{p\}$, que es una contradicción. Por lo tanto $\mathfrak{U} = \{0\}$ y entonces $F = \bigoplus_{i\in I} Q_i \cong \mathbb{Q}^{(I)}$.

Ahora $t_p(T) \trianglelefteq T$, es un p-grupo divisible.

Caso i) Si $t_p(T) = \{0\}$, entonces $t_p(T) \cong \mathbb{Z}_{p^\infty}^{\emptyset}$.

Caso ii) Si $t_p(T) \neq \{0\}$, entonces $t_p(T)$ contiene una copia de $\mathbb{Z}_{p^\infty}$ por Corolario 7. De nuevo si $\{L_i\}_{i\in I}$ es una familia independiente máxima de subgrupos de $t_p(T)$, con cada $L_i \cong \mathbb{Z}_{p^\infty}$, entonces

$$\bigoplus_{i\in I} L_i \leq t_p(T),$$

$\bigoplus_{i\in I} L_i$ es divisible, así que $\bigoplus_{i\in I} L_i \trianglelefteq t_p(T)$. $t_p(T) = (\bigoplus_{i\in I} L_i)\oplus\mathfrak{U}$ con $\mathfrak{U}$ divisible de p-torsión. Si fuera $\mathfrak{U} \neq \{0\}$, entonces $\mathfrak{U}$ contendría una copia de $\mathbb{Z}_{p^\infty}$ con lo que podríamos extender $\{L_i\}_{i\in I}$, lo que sería una contradicción. Por lo tanto $\mathfrak{U} = \{0\}$ y así

$$t_p(T) = \bigoplus_{i\in I} L_i \cong \mathbb{Z}_{p^\infty}.$$

■

Teorema 9 *Un grupo D es divisible si y sólo si*

$$D \cong \mathbb{Q}^{(X)}\oplus(\bigoplus_{p\in\mathbb{P}} \mathbb{Z}_{p^\infty}^{(X_p)})$$

donde X, X_p son conjuntos y $p \in \mathbb{P}$.

Demostración. Ver la observación 10 y la proposición 2. ■

Observemos que un grupo divisible con todos sus elementos de orden infinito es isomorfo a $\mathbb{Q}^{(X)}$, para algún conjunto X.

Un p-grupo divisible es isomorfo a $\mathbb{Z}_p^{(Y)}$ para algún conjunto Y.

Capítulo 2

Los enteros p-ádicos

Si p es un entero primo definimos el anillo de los enteros p-ádicos como $End(\mathbb{Z}_{p^\infty})$. Mas adelante daremos construcciones de anillos isomorfos con éste.

Notemos que $\mathbb{Z}_{p^\infty} =< \{\overline{1/p}, \overline{1/p^2}, \overline{1/p^3}, \overline{1/p^4}, \overline{1/p^5}, ...\} >$, así que si $\mathbb{Z}_{p^\infty} \xrightarrow{f} \mathbb{Z}_{p^\infty}$ es un endomorfismo, entonces f está determinado por $f(\overline{1/p})$, $f(\overline{1/p^2})$, $f(\overline{1/p^3})$, $f(\overline{1/p^4})$, $f(\overline{1/p^5})$, ...(un elemento de $\mathbb{Z}_{p^\infty}$ es de la forma $\overline{a/p^n}$ con $(a;p) = 1$).

Nota 7 *Notemos que $f(\overline{1/p^k})$ debe ser un elemento de $\mathbb{Z}_{p^\infty}$ tal que $o(f(\overline{1/p^k})) \mid p^k$, por lo que $f(\overline{1/p^k}) = \overline{a/p^l}$ con $l \leq k$.*

Definamos

$$\mathbb{S} = \{a_0 + a_1p + a_2p^2 + a_3p^3 + a_4p^4 + a_5p^5 + \cdots \quad | \quad 0 \leq a_i < p\}.$$

Veremos que hay una correspondencia biyectiva entre los conjuntos $\mathbb{S}$ y $\mathbb{Z}_p[[p]] = End(\mathbb{Z}_{p^\infty})$. Un elemento de $\mathbb{Z}_{p^\infty}$ es de la forma $\overline{b/p^m}$ donde $(p;b) = 1$. Así pues como $\overline{b/p^m}$ es una clase módulo $\mathbb{Z}$, podemos suponer que $b < p^m$: ($b = b'p^m + r$ con $0 \leq r < p^m$ por lo tanto concluimos que $\overline{b/p^m} = \overline{b' \not{p}^m/\not{p}^m} + \overline{r/p^m} = \overline{b'} + \overline{r/p^m} = \overline{0} + \overline{r/p^m} = \overline{r/p^m}$ luego $\overline{b/p^m} = \overline{r/p^m}$).

Veamos cómo un elemento $s \in \mathbb{S}$, induce un endomorfismo de $\mathbb{Z}_{p^\infty}$ por multiplicación. Si $s \in \mathbb{S}$ y multiplicamos s por $\overline{b/p^m}$ entonces

$$s \cdot \overline{b/p^m} = \overline{a_0b/p^m} + \overline{a_1b/p^{m-1}} + \cdots + \overline{a_mb/p^{m-m}} + \overline{0} + \cdots .$$

Denotamos $f_s = s \cdot -$, entonces

$$\begin{array}{ccc}
\mathbb{Z}_{p^\infty} & \xrightarrow{f_s} & \mathbb{Z}_{p^\infty} \\
\overline{1/p} & \longmapsto & \overline{a_0/p} \\
\overline{1/p^2} & \longmapsto & \overline{a_0/p^2} + \overline{a_1/p} = \overline{a_0 + a_1p/p^2} \\
\overline{1/p^3} & \longmapsto & \overline{a_0/p^3} + \overline{a_1/p^2} + \overline{a_2/p} = \overline{a_0 + a_1p + a_2p^2/p^3}
\end{array}$$

$$\begin{array}{rcl}
\overline{1/p^4} & \longmapsto & \overline{a_0/p^4} + \overline{a_1/p^3} + \overline{a_2/p^2} + \overline{a_3/p} = \overline{a_0 + a_1p + a_2p^2 + a_3p^3/p^4} \\
\overline{1/p^5} & \longmapsto & \overline{a_0/p^5} + \overline{a_1/p^4} + \overline{a_2/p^3} + \overline{a_3/p^2} + \overline{a_4/p} = \overline{a_0 + a_1p + a_2p^2 + a_3p^3 + a_4p^4/p^5} \\
\vdots & \longmapsto & \vdots \\
\overline{1/p^{m+1}} & \longmapsto & \overline{a_0/p^{m+1}} + \overline{a_1/p^m} + \overline{a_2/p^{m-1}} + \cdots + \overline{a_m/p} = \overline{a_0 + a_1p + a_2p^2 + \cdots + a_mp^m/p^{m+1}} \, .
\end{array}$$

Después demostraremos formalmente que $f_s : \mathbb{Z}_{p^\infty} \longrightarrow \mathbb{Z}_{p^\infty}$ es un morfismo de grupos.

Lema 17 *Si G es grupo abeliano, entonces $(End(G), +, \circ, 0, 1_G)$ es un anillo.*

Demostración. (i) Si f, $g \in End(G)$, entonces $f + g$ definida por

$$(f + g)(x) := f(x) + g(x)$$

es un endomorfismo de G:

$$\begin{aligned}
(f + g)(x + y) &= f(x + y) + g(x + y) \\
&= f(x) + f(y) + g(x) + g(y) \\
&= f(x) + g(x) + f(y) + g(y) \\
&= (f + g)(x) + (f + g)(y).
\end{aligned}$$

(ii) El neutro es el homomorfismo de grupos $G \xrightarrow{\bar{0}} G$.
$y \longmapsto 0$

(iii) $-f$ es el homomorfismo tal que $(-f)(x) = -f(x)$.

Como la composición de endomorfismos es un endomorfismo entonces $(End(G), \circ, 1_G)$ es un monoide. Además si f, g, h son endomorfismos tenemos lo siguiente:

$$(f + g) \circ h = f \circ h + g \circ h$$

y

$$h \circ (f + g) = h \circ f + h \circ g.$$

■

Lema 18 *Sea $(G, +, 0)$ un grupo abeliano con un subconjunto X que genera a G. Sea H un grupo abeliano. Una función $X \xrightarrow{f} H$ se puede extender a un homomorfismo $\varphi : G \longrightarrow H$ si y sólo si*

$$\sum_{i=1}^{n} z_i x_i = 0, z_i \in \mathbb{Z}, x_i \in X \Longrightarrow \sum_{i=1}^{n} z_i f(x_i) = 0.$$

Demostración. ($\Longleftarrow$) Sea $X = \{x_i\}_{i\in I}$. Que X genera a G significa que $\forall g \neq 0$, $g \in G$ tenemos que g se puede expresar como $g = \sum_{i\in I} z_i x_i$ con $z_i \in \mathbb{Z}$ y casi todos los $z_i = 0$. Así puede definirse toda $G \xrightarrow{\varphi} H$ por $\varphi(g) = \varphi(\sum_{i\in I} z_i x_i) = \sum_{i\in I} z_i f(x_i)$ donde las sumas son finitas, pues por hipótesis casi cada z_i es 0 (es decir todos, salvo un número finito de z_i son 0).

Veamos que φ está bien definida. En efecto:

Supongamos que $g = \sum_{i\in I} z_i x_i = \sum_{i\in I} w_i x_i$ son dos combinaciones de los elementos de $\{x_i\}_{i\in I}$, con casi toda z_i y casi toda w_i son cero. Entonces $0 = g - g = \sum_{i\in I}(z_i - w_i)x_i$. Por hipótesis tenemos que $0 = \sum_{i\in I}(z_i - w_i)f(x_i)$ de donde tenemos que

$$\sum_{i=1}^{n} z_i f(x_i) = \sum_{i=1}^{n} w_i f(x_i).$$

Esto muestra que $\varphi : G \longrightarrow H$ es una función bien definida. Además φ es un morfismo de grupos pues si $u = \sum_{i\in I} z_i x_i$ y $v = \sum_{i\in I} w_i x_i$ donde casi toda x_i es 0 y casi toda w_i es 0, entonces tenemos lo siguiente:

$$\begin{aligned}\varphi(u+v) &= \varphi(\textstyle\sum_{i\in I} z_i x_i + \sum_{i\in I} w_i x_i)\\ &= \varphi(\textstyle\sum_{i\in I}(z_i + w_i)x_i)\\ &= \textstyle\sum_{i\in I} z_i f(x_i) + \sum_{i\in I} w_i f(x_i)\\ &= \varphi(u) + \varphi(v).\end{aligned}$$

($\Longrightarrow$) Como un morfismo de grupos manda el neutro al neutro, y en vista de que $G \xrightarrow{\varphi} H$ manda a $G \ni g = \sum_{i\in I} z_i x_i \longmapsto \sum_{i\in I} z_i f(x_i) \in H$ por ser un morfismo de grupos que extienden a f, tenemos que

$$\sum_{i\in I} z_i x_i = 0 \Longrightarrow \sum_{i\in I} z_i f(x_i) = 0.$$

■

Definición 20 *Definimos* $\mathbb{Z}_p[[p]] := \{\sum_{i=0}^{\infty} a_i p^i | 0 \leq a_i < p\}$.

Definimos una suma y un producto en $\mathbb{Z}_p[[p]]$ por $\sum_{i=0}^{\infty} a_i p^i + \sum_{i=0}^{\infty} b_i p^i =: \sum_{i=0}^{\infty} c_i p^i$, donde definimos los coeficientes c_i de la manera siguiente:

Por el algoritmo de la división

$$\begin{aligned} a_0 + b_0 &= c_0 + pq_0\\ a_1 + b_1 + q_0 &= c_1 + pq_1\\ &\vdots\\ a_{n+1} + b_{n+1} + q_n &= c_{n+1} + pq_{n+1}.\end{aligned}$$

$$\begin{array}{r} q_0 \\ p\overline{|\, a_0 + b_0} \\ c_0 \end{array}$$

Esto define los coeficientes c_0, c_1, c_2,... por inducción.

Análogamente, definimos un producto en $\mathbb{Z}_p[[p]]$, como $(\sum_{i=0}^{\infty} a_i p^i)(\sum_{i=0}^{\infty} b_i p^i) =: \sum_{i=0}^{\infty} m_i p^i$.

Por el algoritmo de la división

$$\begin{array}{rr} a_0b_0 = s_0p + m_0 & s_0 \\ a_0b_1 + a_1b_0 + s_0 = s_1p + m_1 & p\overline{|\,a_0b_0} \\ \vdots \quad \vdots \quad \vdots\ \vdots\ \vdots \quad \vdots & \quad m_0 \end{array}$$

$$\textstyle\sum_{i+j=k+1} a_ib_j + s_k = s_{k+1}p + m_{n+1}.$$

Con esto definimos por inducción los coeficientes $m_i \in \mathbb{N}$.

Entonces $\mathbb{Z}_p[[p]]$ tiene definida una suma y un producto.

Veamos que cada elemento de $\mathbb{Z}_p[[p]]$ induce un endomorfismo de $\mathbb{Z}_{p^\infty}$ por "multiplicación".

Lema 19 *$\forall s \in \mathbb{Z}_p[[p]]$, la función*

$$\begin{array}{rcl} \overline{1/p} & \overset{f}{\longmapsto} & \overline{a_0/p} \\ \overline{1/p^2} & \overset{f}{\longmapsto} & \overline{a_0 + a_1p/p^2} \\ \overline{1/p^3} & \overset{f}{\longmapsto} & \overline{a_0 + a_1p + a_2p^2/p^3} \\ \vdots & \overset{f}{\longmapsto} & \vdots\vdots\vdots\vdots\vdots\vdots\vdots\vdots\vdots\vdots\vdots\vdots\vdots\vdots\vdots\vdots \\ \overline{1/p^m} & \overset{f}{\longmapsto} & \overline{a_0 + a_1p + a_2p^2 + \cdots + a_{m-1}p^{m-1}/p^m} \end{array}$$

induce un morfismo de grupos $\varphi_s : \mathbb{Z}_{p^\infty} \longrightarrow \mathbb{Z}_{p^\infty}$.

Demostración.

Veamos el siguiente diagrama:

$$\begin{array}{ccc} \mathbb{Z}_{p^\infty} & \longrightarrow & \mathbb{Z}_{p^\infty} \\ {\scriptstyle i^{\mathbb{Z}_{p^\infty}}_{\{\overline{1/p^n}\}}}\big\uparrow & & \big\uparrow{\scriptstyle gen} \\ \{\overline{1/p^n}\}. & & \end{array}$$

Si $s = \sum_{i=0}^{\infty} \overline{a_i} \cdot p^i \in \mathbb{Z}_p[[p]]$ con $\overline{a_i} \in \mathbb{Z}_p$, $a_i \in \mathbb{Z}$, tenemos que

$$\begin{aligned} s \cdot \overline{1/p^n} =: \textstyle\sum_{i=0}^{\infty} a_i \cdot \overline{p^i/p^n} = \sum_{i=0}^{n} a_i \cdot \overline{p^i/p^n} &= \overline{a_0/p^n} + \overline{a_1/p^{n-1}} + \cdots + \overline{a_n \not{p}^n/\not{p}^n} \\ &= \overline{a_0 + a_1p + \cdots + a_{n-1}p^{n-1}/p^n} \end{aligned}$$

que está definida en $\{\overline{1/p}, \overline{1/p^2}, ...\}$ que es un conjunto que genera a $\mathbb{Z}_{p^\infty}$. Veamos que se puede extender a un morfismo de grupos

$$\mathbb{Z}_{p^\infty} \xrightarrow{\varphi_s} \mathbb{Z}_{p^\infty} \ .$$

Por el Lema 18 basta ver que si

$$\overline{z_1/p + z_2/p^2 + \cdots + z_m/p^m} = \overline{0},$$

entonces

$$z_1(\overline{a_0/p}) + z_2(\overline{a_0 + a_1p/p^2}) + \cdots + z_m(\overline{a_0 + a_1p + \cdots + a_{m-1}p^{m-1}/p^m}) = \overline{0}.$$

Supongamos que $\overline{z_1/p} + \overline{z_2/p^2} + \cdots + \overline{z_m/p^m} = \overline{0}$, entonces $\frac{z_1}{p} + \frac{z_2}{p^2} + \cdots + \frac{z_m}{p^m} \in \mathbb{Z}$.

Multiplicando por p: $z_1 + \frac{z_2}{p} + \cdots + \frac{z_m}{p^{m-1}} \in \mathbb{Z}$ por lo que $\overline{z_2/p + \cdots + z_m/p^{m-1}} = \overline{0}$. Volviendo a multiplicar por p obtenemos que $z_2 + \frac{z_3}{p} + \cdots + \frac{z_m}{p^{m-2}} \in \mathbb{Z}$ y por lo tanto

$$\overline{z_3/p + \cdots + z_m/p^{m-2}} = \overline{0}.$$

Repitiendo el argumento tenemos que $\overline{z_4/p + \cdots + z_m/p^{m-3}} = \overline{0}$

$$\vdots$$

$\frac{z_m}{p} \in \mathbb{Z}$, es decir $\overline{z_m/p} = \overline{0}$.

Usaremos esto para calcular lo siguiente:

$$z_1(\overline{a_0/p}) + z_2(\overline{a_0 + a_1p/p^2}) + \cdots + z_m(\overline{a_0 + a_1p + \cdots + a_{m-1}p^{m-1}/p^m}).$$

El coeficiente de a_0 en esta expresión es $\overline{z_1/p + z_2/p^2 + \cdots + z_m/p^m}$, que es $\overline{0}$ por hipótesis.

El coeficiente de a_1 es $\overline{z_2/p + z_3/p^2 + \cdots + z_m/p^{m-1}}$, que ya notamos que es $\overline{0}$. Ahora también el coeficiente de a_2 es $\overline{0}$, es decir los coeficientes de a_0, a_1, a_2,...,a_m son todos $\overline{0}$, como ya notamos.

Así que f se extiende a una función $\mathbb{Z}_{p^\infty} \xrightarrow{\varphi_s} \mathbb{Z}_{p^\infty}$ que podemos pensar que es multiplicar por $(a_0 + a_1p + a_2p^2 + \cdots)$.

Además, el Lema 18 muestra que φ_s es un morfismo de grupos. ■

Lema 20 $\quad \mathbb{Z}_p[[p]] \xrightarrow{\mu} End(\mathbb{Z}_{p^\infty})$

$$\textstyle\sum_{i=0}^{\infty} a_ip^i \longmapsto (\sum_{i=0}^{\infty} a_ip^i) \cdot - : \mathbb{Z}_{p^\infty} \longrightarrow \mathbb{Z}_{p^\infty}$$

es una función, que respeta la suma y el producto.

Demostración. Manda sumas en sumas:

Veamos que

$$(\sum_{i=0}^{\infty} a_i p^i + \sum_{i=0}^{\infty} b_i p^i) \cdot - = (\sum_{i=0}^{\infty} a_i p^i \cdot -) + (\sum_{i=0}^{\infty} b_i p^i \cdot -).$$

Para ver esta igualdad, basta ver que tienen el mismo efecto en cada $\overline{1/p^k}$.

Si $(\sum_{i=0}^{\infty} a_i p^i + \sum_{i=0}^{\infty} b_i p^i) = (\sum_{i=0}^{\infty} c_i p^i)$, entonces multiplicando esto por $\overline{1/p^k}$ obtenemos

$$\overline{c_0 + c_1 p + \cdots + c_{k-1} p^{k-1}/p^k}.$$

Así que tenemos que comprobar lo siguiente:

$$\overline{c_0 + c_1 p + \cdots + c_{k-1} p^{k-1}/p^k} = \overline{a_0 + a_1 p + \cdots + a_{k-1} p^{k-1}/p^k} + \overline{b_0 + b_1 p + \cdots + b_{k-1} p^{k-1}/p^k} \quad para \quad cada \quad k.$$

En efecto: Si $k = 1$, entonces $\overline{c_0/p} = \overline{a_0/p} + \overline{b_0/p}$, pues por definición de c_0, $c_0 \overset{p}{\equiv} a_0 + b_0$ así que $\frac{c_0 - a_0 - b_0}{p} = \frac{\not{p} q_0}{\not{p}} \in \mathbb{Z}$.

Recordando que

$$a_0 + b_0 = c_0 + q_0 p$$

$$a_1 + b_1 + q_0 = c_1 + q_1 p$$

tenemos lo siguiente:

$$\begin{aligned} \overline{a_0 + a_1 p/p^2} + \overline{b_0 + b_1 p/p^2} &= \overline{c_0 + q_0 p + a_1 p + b_1 p/p^2} \\ &= \overline{c_0 + (q_0 + a_1 + b_1) p/p^2} \\ &= \overline{c_0 + (c_1 + q_1 p) p/p^2} \\ &= \overline{c_0 + c_1 p/p^2} + \overline{q_1 \ \not{p}^2/ \ \not{p}^2}. \end{aligned}$$

Por definición de la suma en $\mathbb{Z}_p[[p]]$:

$$a_0 + b_0 = c_0 + q_0 p$$

$$a_1 + b_1 + q_0 = c_1 + q_1 p$$

$$a_2 + b_2 + q_1 = c_2 + q_2 p$$

$$\vdots \qquad \vdots \quad \vdots$$

$$a_{k+1} + b_{k+1} + q_k = c_{k+1} + q_{k+1} p,$$

tenemos que

$$\begin{aligned}
\overline{(a_0+b_0)+(a_1+b_1)p+(a_2+b_2)p^2+\cdots+(a_k+b_k)p^k/p^{k+1}} &= \overline{c_0+(q_0+a_1+b_1)p+(a_2+b_2p^2+\cdots/p^{k+1}} \\
&= \overline{c_0+c_1p+(q_1+a_2+b_2p^2)+\cdots/p^{k+1}} \\
&= \overline{c_0+c_1p+c_2p^2+(q_2+a_3+b_3)p^3+\cdots/p^{k+1}} \\
&= \overline{c_0+c_1p+\cdots+(q_{k-1}+a_k+b_k)p^k/p^{k+1}} \\
&= \overline{c_0+c_1p+\cdots+(c_k+q_kp)p^k/p^{k+1}} \\
&= \overline{c_0+c_1p+\cdots+c_kp^k+q_kp^{k+1}/p^{k+1}} \\
&= \overline{c_0+c_1p+\cdots+c_kp^k/p^{k+1}}+\overline{q_k\not{p}^{k+1}/\not{p}^{k+1}}.
\end{aligned}$$

Esto muestra que $\mu : \mathbb{Z}_p[[p]] \longrightarrow End(\mathbb{Z}_{p^\infty})$ manda sumas en sumas.

μ respeta productos:

Demostremos que

$$\mu((\sum_{i=0}^{\infty} a_ip^i)(\sum_{i=0}^{\infty} b_ip^i)) = \mu(\sum_{i=0}^{\infty} a_ip^i)\mu(\sum_{i=0}^{\infty} b_ip^i).$$

De nuevo basta ver que el efecto de ambos endomorfismos de $\mathbb{Z}_{p^\infty}$ es el mismo en cada generador de $\mathbb{Z}_{p^\infty}$.

En $\overline{1/p}$:

$$(a_0+a_1p+\cdots)((b_0+b_1p+\cdots)(\overline{1/p})) = (a_0+a_1p+\cdots)(\overline{b_0/p}) = \overline{a_0b_0/p} = \overline{m_0+s_0p/p} = \overline{m_0/p}+\overline{s_0} = (m_0+m_1p+\cdots)\overline{1/p}.$$

En general,

$$\begin{aligned}
((a_0+a_1p+\cdots)(b_0+b_1p+\cdots))(\overline{1/p^k}) &= (a_0+a_1p+\cdots)(\overline{b_0+b_1p+\cdots+b_{k-1}p^{k-1}/p^k}) \\
&= \overline{a_0b_0+(a_0b_1+a_1b_0)p+\cdots+(a_0b_{k-1}+a_1b_{k-2}+\cdots+a_{k-1}b_0)p^{k-1}/p^k} \\
&= \overline{m_0+(s_0+a_0b_1+a_1b_0)p+\cdots/p^k} \\
&= \overline{m_0+m_1p+(s_1+a_0b_2+a_1b_1+a_2b_0)p^2+\cdots/p^k} \\
&= \overline{m_0+m_1p+m_2p^2+(s_2+a_0b_3+\cdots)p^3+\cdots/p^k} \\
&= \overline{m_0+m_1p+\cdots+m_{k-1}p^{k-1}/p^k}+\overline{s_k\not{p}^k/\not{p}^k} \\
&= (m_0+m_1p+m_2p^2+m_3p^3+\cdots)(\overline{1/p^k}).
\end{aligned}$$

Lo que muestra que μ respeta el producto.

Entonces $\mathbb{Z}_p[[p]] \xrightarrow{\mu} End(\mathbb{Z}_{p^\infty})$ es una función que respeta la suma y el producto. ■

Teorema 10 *$\mu : \mathbb{Z}_p[[p]] \longrightarrow End(\mathbb{Z}_{p^\infty})$ es un isomorfismo de anillos.*

Demostración. $\mathbb{Z}_p[[p]] \xrightarrow{\mu} End(\mathbb{Z}_{p^\infty})$ es una función inyectiva:

Supongamos $\sum_{i=0}^{\infty} a_i p^i \neq \sum_{i=0}^{\infty} b_i p^i$, esto quiere decir que a_k es distinto de b_k para alguna $k \in \mathbb{N}$, k-mínimo $\mu(\sum_{i=0}^{\infty} a_i p^i) \neq \mu(\sum_{i=0}^{\infty} b_i p^i)$ porque su efecto en $\overline{1/p^{k+1}}$ son distintos:

$$\mu(\sum_{i=0}^{\infty} a_i p^i)(\overline{1/p^{k+1}}) = \overline{a_0 + a_1 p + \cdots + a_k p^k / p^{k+1}}.$$

Por otra parte

$$\mu(\sum_{i=0}^{\infty} b_i p^i)(\overline{1/p^{k+1}}) = \overline{b_0 + b_1 p + \cdots + b_k p^k / p^{k+1}}.$$

Por hipótesis, $b_0 = a_0$, $b_1 = a_1$, ..., $b_{k-1} = a_{k-1}$, entonces

$$\overline{a_0 + a_1 p + \cdots + a_k p^k / p^{k+1}} \neq \overline{a_0 + \cdots + a_{k-1} p^{k-1} + b_k p^k / p^{k+1}}$$

pues $\overline{a_k p^k / p^{k+1}} \neq \overline{b_k p^k / p^{k+1}}$, porque $\overline{a_k / p} \neq \overline{b_k / p}$.
Si fueran iguales, entonces $\frac{(a_k - b_k)}{p} \in \mathbb{Z}$ y $p \mid |a_k - b_k|$, lo que no es posible pues a_k y b_k son enteros menores que p.

Veremos ahora que $\mu : \mathbb{Z}_p[[p]] \longrightarrow End(\mathbb{Z}_{p^\infty})$ es una función suprayectiva.

Si $\mathbb{Z}_{p^\infty} \xrightarrow{f} \mathbb{Z}_{p^\infty}$ es un morfismo de grupos:

$$\mathbb{Z}_{p^\infty} \xrightarrow{f} \mathbb{Z}_{p^\infty}$$

$$\overline{1/p^k} \longmapsto f(\overline{1/p^k})$$

como $p^k \cdot \overline{1/p^k} = \overline{0}$ vemos que $p^k \cdot f(\overline{1/p^k}) = \overline{0}$.
Entonces $f(\overline{1/p^k})$ es un elemento de $\mathbb{Z}_{p^\infty} =< \{\overline{1/p}, \overline{1/p^2}, \overline{1/p^3}, \overline{1/p^4}, \overline{1/p^5}, ...\} >$ de orden un divisor de p^k, entonces $f(\overline{1/p^k}) = \overline{b/p^k}$ donde podemos tomar $b < p^k$, pues podemos sustituir b por su residuo al dividir entre p^k si hiciera falta.
Entonces $f(\overline{1/p}) = \overline{a_0/p}$ con $0 \leq a_0 < p$, $f(\overline{1/p^2}) = \overline{b/p^2}$ con $0 \leq b < p^2$.

Ahora

$$\begin{array}{c} p \cdot f(\overline{1/p^2}) = f(\overline{1/p}) = \overline{a_0/p}. \\ \| \\ p \cdot \overline{b/p^2} \\ \| \\ \overline{b/p} \ . \end{array}$$

Entonces $p \mid b - a_0$ por lo tanto $b - a_0 = pa$, entonces $b = a_0 + pa$, como $b < p^2$ entonces $a < p$.

Suponiendo que $f(\overline{1/p^k}) = \overline{a_0 + a_1 p + \cdots + a_{k-1} p^{k-1} / p^k}$.

Si $f(\overline{1/p^{k+1}}) = \overline{c/p^{k+1}}$, entonces $\overline{c/p^k} = p(f(\overline{1/p^{k+1}})) = f(\overline{1/p^k}) = \overline{a_0 + a_1 p + \cdots + a_{k-1} p^{k-1} / p^k}$.

Entonces $\overline{c/p^k} = \overline{a_0 + \cdots + a_{k-1}p^{k-1}/p^k}$, es decir, $\frac{c-(a_0+\cdots+a_{k-1}p^{k-1})}{p^k} \in \mathbb{Z}$ por lo tanto

$$c - (a_0 + \cdots + a_{k-1}p^{k-1}) = a_k p^k \text{ con } a_k \in \mathbb{Z}.$$

Entonces $c = a_0 + \cdots + a_{k-1}p^{k-1} + a_k p^k$ como $c < p^{k+1}$ se sigue que $a_k < p$.
El argumento anterior muestra que f es $\mu(a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots)$. Por lo tanto $\mathbb{Z}_p[[p]] \xrightarrow{\mu} End(\mathbb{Z}_{p^\infty})$ es suprayectiva. Como μ es una biyección que respeta la suma y el producto y como $End(\mathbb{Z}_{p^\infty})$ es un anillo, entonces $\mathbb{Z}_p[[p]]$ es un anillo isomorfo a $End(\mathbb{Z}_{p^\infty})$. ■

Lo anterior nos da una alternativa a la definición de los enteros p-ádicos.

Como vimos, podemos identificar un entero p-ádico con una suma formal $\sum_{i=0}^{\infty} a_i p^i$ con coeficientes en $\mathbb{Z}_p$.

2.1. Valuación p-ádica

Definición 21 $\upsilon_p : \mathbb{Z}_p[[p]] \setminus \{\overline{0}\} \longrightarrow \mathbb{N}$

$$\textstyle\sum_{i=0}^{\infty} a_i p^i \longmapsto \text{mín}\{i \in \mathbb{N} | a_i \neq 0\} .$$

υ_p está definida en $\mathbb{Z}_p[[p]] \setminus \{\overline{0}\}$.

Un número p-ádico es distinto de $\overline{0}$ si y sólo si $\upsilon_p(a)$ está definido.

Lema 21 *Si $\sum_{i=0}^{\infty} a_i p^i$ y $\sum_{i=0}^{\infty} b_i p^i$ son dos enteros p-ádicos ambos no cero, entonces*

$$(\sum_{i=0}^{\infty} a_i p^i)(\sum_{i=0}^{\infty} b_i p^i) \neq 0$$

y

$$\upsilon_p((\sum_{i=0}^{\infty} a_i p^i)(\sum_{i=0}^{\infty} b_i p^i)) = \upsilon_p(\sum_{i=0}^{\infty} a_i p^i) + \upsilon_p(\sum_{i=0}^{\infty} b_i p^i).$$

Demostración. Digamos que $\upsilon_p(\sum_{i=0}^{\infty} a_i p^i) = k$ y $\upsilon_p(\sum_{i=0}^{\infty} b_i p^i) = l$. Entonces:

$$a_0 = a_1 = \cdots = a_{k-1} = 0 \text{ y } b_0 = b_1 = \cdots = b_{l-1} = 0.$$

Por definición,

$$(\sum_{i=0}^{\infty} a_i p^i)(\sum_{i=0}^{\infty} b_i p^i) = \sum_{i=0}^{\infty} m_i p^i$$

donde $a_0 b_0 = s_0 p + m_0$ y $s_0 + a_0 b_1 + a_1 b_0 = s_1 p + m_1$.

En general

$$(s_k + \sum_{i+j=k+1}^{\infty} a_i b_j) = s_{k+1}p + m_{k+1} \quad \text{si}$$

$$a_0 = a_1 = \cdots = a_{k-1} = 0 \quad con \quad a_k \neq 0$$

y

$$b_0 = b_1 = \cdots = b_{l-1} = 0 \quad con \quad b_l \neq 0.$$

Entonces

$$a_0 b_0 = 0 \cdot p + 0 \quad (m_0 = 0)$$

$$0 + (a_0 \cdot b + a_1 \cdot b_0) = 0 + (0 \cdot 0 + 0 \cdot 0) = 0 \cdot p + 0 \quad (m_1 = 0).$$

Así tenemos que

$$m_0 = 0 = m_1 = \cdots = m_{k+l-1} = 0$$

y

$$s_0 = s_1 = \cdots = s_{k+l-1} = 0.$$

Ahora

$$s_{k+l-1} + \sum_{i+j=k+l} a_i b_j = a_k b_l.$$

Es decir

$$v_p((\sum_{i=0}^{\infty} a_i p^i)(\sum_{i=0}^{\infty} b_i p^i)) = k + l = v_p(\sum_{i=0}^{\infty} a_i p^i) + v_p(\sum_{i=0}^{\infty} b_i p^i).$$

■

Corolario 9 $\mathbb{Z}_p[[p]]$ *es un dominio entero.*

Demostración. Esto es equivalente a que el producto de dos elementos distintos de cero sea distinto de cero, que se demostró en el lema previo. ■

Definición 22

$$\mathbb{Z}_p[[p]] \xrightarrow{\rho} \mathbb{Z}_p$$

$$\textstyle\sum_{i=0}^{\infty} a_i p^i \longmapsto \overline{a_0}\ .$$

Observación 11 ρ *es un homomorfismo de anillos.*

Demostración. Por definición

$$\sum_{i=0}^{\infty} a_i p^i + \sum_{i=0}^{\infty} b_i p^i = \sum_{i=0}^{\infty} c_i p^i$$

donde $a_0 + b_0 = q_0 p + c_0$. Así que $a_0 + b_0 \overset{p}{\equiv} c_0$. Además $(\sum_{i=0}^{\infty} a_i p^i)(\sum_{i=0}^{\infty} b_i p^i) = \sum_{i=0}^{\infty} m_i p^i$ donde $a_0 b_0 = s_0 p + m_0$ por definición. Por lo tanto $a_0 b_0 \overset{p}{\equiv} m_0$. ■

Observación 12 *1. ρ es un morfismo suprayectivo.*

2. *$Nuc(\rho) = \{\sum_{i=0}^{\infty} a_i p^i | a_0 = 0\}$.*

3. *$\mathbb{Z}_p[[p]]/Nuc(\rho) \cong \mathbb{Z}_p$, por el primer Teorema de isomorfismos.*

De lo anterior tenemos que $Nuc(\rho)$ es un ideal máximo de $\mathbb{Z}_p[[p]]$. (Pues $\mathbb{Z}_p$ es un campo, y sólo tiene dos ideales).

Observación 13 *El neutro multiplicativo para $\mathbb{Z}_p[[p]]$ es*

$$1 + 0 \cdot p + 0 \cdot p^2 + \cdots,$$

que es el elemento que corresponde al neutro en $End(\mathbb{Z}_{p^\infty})$, que es $Id_{\mathbb{Z}_{p^\infty}}$: Notemos que

$$\mathbb{Z}_p[[p]] \xrightarrow{\mu} End(\mathbb{Z}_{p^\infty})$$

$$\textstyle\sum_{i=0}^{\infty} a_i p^i \longmapsto \sum_{i=0}^{\infty} a_i p^i \cdot - \ .$$

Si $a_0 = 1$ y $a_i = 0$, entonces $(\sum_{i=0}^{\infty} a_i p^i) \cdot \overline{1/p^k} = 1 \cdot \overline{1/p^k} = \overline{1/p^k}$.

Observación 14 *$\sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p[[p]]$ tiene inverso multiplicativo $\iff a_0 \neq 0$.*

Demostración. ($\Longrightarrow$) Si $\sum_{i=0}^{\infty} a_i p^i$ tiene inverso multiplicativo $\sum_{i=0}^{\infty} b_i p^i$, entonces

$$(\sum_{i=0}^{\infty} a_i p^i)(\sum_{i=0}^{\infty} b_i p^i) = 1 + 0 \cdot p + 0 \cdot p^2 + \cdots$$

asi que $a_0 b_0 \overset{p}{\equiv} m_0 = 1$. Entonces $a_0 \neq 0$.

($\Longleftarrow$) Recíprocamente, si $a_0 \neq 0$ podemos resolver

$$(\sum_{i=0}^{\infty} a_i p^i)(\sum_{i=0}^{\infty} b_i p^i) = 1 + 0 \cdot p + 0 \cdot p^2 + \cdots .$$

Pues : $a_0 b_0 = s_0 \cdot p + 1$, así que b_0 es el elemento del inverso multiplicativo de a_0 en $\mathbb{Z}_p$ y conocemos s_0.

Ahora, $s_0 + a_0 b_1 + a_1 b_0 = p s_1$, así que $a_0 b_1 = -a_1 b_0 - s_0 + p s_1$ que se puede resolver en $\mathbb{Z}_p$ y conocemos s_1. Si ya hemos encontrado b_0, b_1, ..., b_k, s_0, s_1,..., s_k, entonces como

$$(\sum_{i=0}^{\infty} a_i p^i)(\sum_{i=0}^{\infty} b_i p^i) = 1 + 0 \cdot p + 0 \cdot p^2 + \cdots,$$

entonces

$$s_k + \sum_{i+j=k+1} a_i b_j = s_{k+1}p + m_{k+1}.$$

Es decir,

$$s_k + b_{k+1} + \sum_{i+j=k+1} a_i b_j = s_{k+1}p + m_{k+1}.$$

Así,

$$a_0 b_{k+1} = - \sum_{i+j=k+1 \text{ excepto } (i=0 \text{ y } j=k+1)} a_i b_j + s_{k+1}p - s_k.$$

que se puede resolver en $\mathbb{Z}_p$ porque $\overline{a_0}$ es una unidad en $\mathbb{Z}_p$ y conocemos s_{k+1}. ■

Corolario 10 *$\mathbb{Z}_p[[p]]$ es un dominio entero con ideal propio mayor igual a*

$$\{\sum_{i=0}^{\infty} a_i p^i | a_0 = 0\}.$$

Es decir $\mathbb{Z}_p[[p]]$ es un anillo local.

Demostración. Ya vimos que $\{\sum_{i=0}^{\infty} a_i p^i | a_0 = 0\} = Nuc(\rho)$ y que $\mathbb{Z}_p[[p]]/Nuc(\rho) \cong \mathbb{Z}_p$. Como $\mathbb{Z}_p$ es un campo, solamente tiene dos ideales. Concluimos usando el Teorema de la Correspondencia. ■

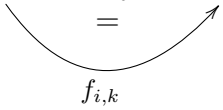
2.2. Los enteros p-ádicos como límite inverso

Definición 23 *Un conjunto dirigido $(I, \leq)$ es un conjunto parcialmente ordenado tal que $\forall i, j \in I \; \exists k \in I$ tal que $k \geq i$, $k \geq j$.*

Un sistema dirigido de grupos (o anillos) es una pareja:

$$(\{M_i\}_{i \in I}, \; \{M_i \xrightarrow{f_{i,j}} M_j \}_{i \geq j}) \text{ tal que } M_i \xrightarrow{f_{i,i}} M_i \text{ es la identidad}$$

en M_i y $M_i \xrightarrow{f_{i,j}} M_j \xrightarrow{f_{j,k}} M_k$ si $i \geq j \geq k$ donde cada $f_{i,j}$ es un morfismo de grupos (o de



anillos) $\forall i \geq j$ con $i, j \in I$.

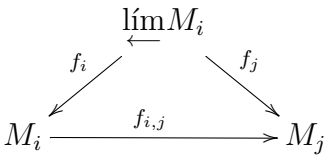
Un límite inverso para el sistema $(\{M_i\}_{i \in I}, \; \{M_i \xrightarrow{f_{i,j}} M_j \}_{i \geq j})$ es un grupo (o anillo) denotado:

$$\varprojlim M_i$$

junto con una familia de morfismos

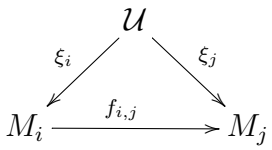
$$\{f_j : \varprojlim M_i \longrightarrow M_j\}_{j \in I}$$

tal que el siguiente diagrama conmuta:

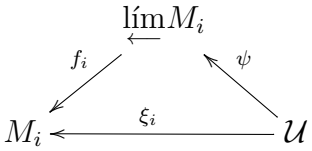


es decir $f_{i,j} \circ f_i = f_j$ y tal que tiene la siguiente propiedad (universal):

$\forall\ (\mathcal{U}, \{\ \mathcal{U} \xrightarrow{\xi_i} M_i\ \}_{i\in I})$ tal que conmuta el diagrama siguiente:



$\exists!\ \psi : \varprojlim M_i \longleftarrow \mathcal{U}$ morfismo de grupos (o anillos) tal que



conmuta $\forall i \in I$.

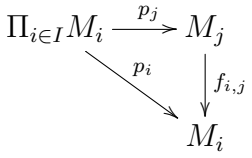
Para grupos o anillos se puede construir el límite inverso de:

$$(\{M_i\}_{i\in I}, \{\ M_i \xrightarrow{f_{i,j}} M_j\ \}_{i,j\in I})$$

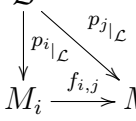
tomando

$$\mathcal{L} = \{x \in \Pi_{i\in I} M_i | \text{ para } i \geq j, f_{i,j}(p_i(x)) = p_j(x)\}$$

donde



(p_i, p_j son las proyecciones canónicas).

Así tenemos $(\mathcal{L}, \{\ \mathcal{L} \xrightarrow{p_i} M_i\ \})$ tal que  conmuta. Esto es claro dada la definición

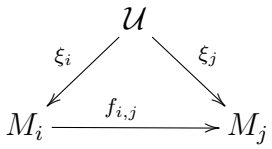
de $\mathcal{L}$.

Que $(\mathcal{L}, \{\ \mathcal{L} \xrightarrow{p_{i|_\mathcal{L}}} M_i\ \})$ es un límite inverso se comprueba de la manera siguiente:

Supongamos que $(\{M_i\}_{i\in I}, \{\ M_i \xrightarrow{f_{i,j}} M_j\ \}_{i,j\in I})$ es un sistema dirigido y sea

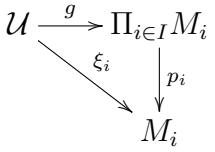
$$(\mathcal{U}, \{\ \mathcal{U} \xrightarrow{\xi_i} M_i\ \}_{i\in I})$$

tal que



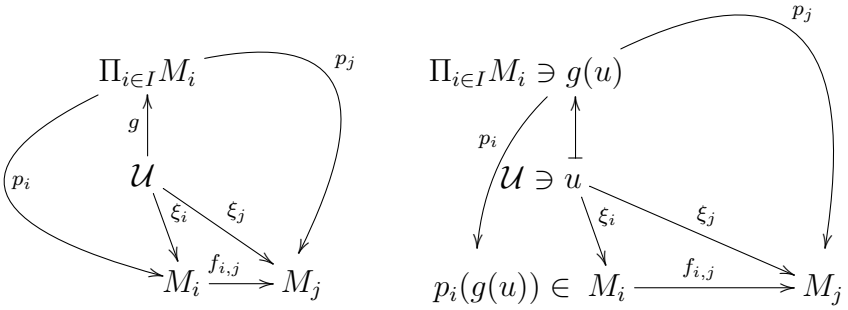
conmuta si $i \geq j$.

Entonces la familia $(\mathcal{U}, \{\ \mathcal{U} \xrightarrow{\xi_i} M_i\ \}_{i\in I})$ induce $\mathcal{U} \xrightarrow{g} \Pi_{i\in I} M_i$ tal que



conmuta para toda i.

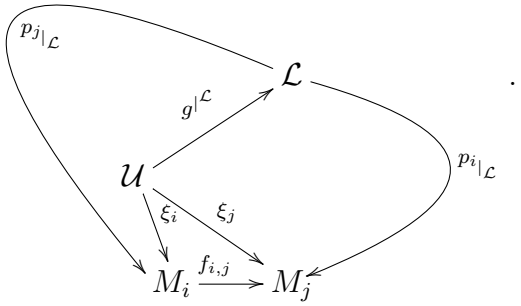
Si $i \geq j$, entonces



conmuta, así que $\forall u \in \mathcal{U}$, $(f_{i,j} \circ p_i)(g(u)) = p_j(g(u))$.

Esto muestra que $g(u) \in \mathcal{L}$.

Así que el diagrama siguiente conmuta:



.

Lo que muestra que $(\mathcal{L}, \{p_{i_{|\mathcal{L}}}\}_{i\in I})$ es un límite inverso para

$$(\{M_i\}_{i\in I}, \{\ M_i \xrightarrow{f_{i,j}} M_j\ \}_{i,j\in I}).$$

(La unicidad de $g^{|\mathcal{L}}$ se sigue fácilmente de las propiedades del producto cartesiano y del diagrama anterior). Esto muestra que existen los límites inversos de sistemas dirigidos de grupos o anillos.

Ejemplo 8 *Si $i \leq j$, entonces $\mathbb{Z}p^j \subseteq \mathbb{Z}p^i$.*

Demostración. Esta inclusión induce un morfismo de anillos

$$\mathbb{Z}/\mathbb{Z}p^j \xrightarrow{f_{j,i}} \mathbb{Z}/\mathbb{Z}p^i$$

podemos ver que $(\mathbb{Z}_p[[p]], \{\ \mathbb{Z}_p[[p]] \xrightarrow{\mu_j} \mathbb{Z}/\mathbb{Z}p^j\ \}_{j\in I})$ es el límite inverso de

$$(\{\mathbb{Z}/\mathbb{Z}p^i\}_{i\in I}, \{\ \mathbb{Z}/\mathbb{Z}p^j \xrightarrow{f_{j,i}} \mathbb{Z}/\mathbb{Z}p^i\ \}_{i\leq j}),$$

donde

$$\mathbb{Z}_p[[p]] \xrightarrow{\mu_j} \mathbb{Z}/\mathbb{Z}p^j$$

$$(a_0 + a_1p + a_2p^2 + \cdots) \longmapsto \overline{a_0 + a_1p + a_2p^2 + \cdots + a_{j-1}p^{j-1}}\ .\ \blacksquare$$

Observación 15

$$\mathbb{Z}_p[[p]] \xrightarrow{\mu_j} \mathbb{Z}/\mathbb{Z}p^j$$

$$(\textstyle\sum_{i=0}^{\infty} a_ip^i) \longmapsto \overline{a_0 + a_1p + a_2p^2 + \cdots + a_{j-1}p^{j-1}}$$

es un homomorfismo de anillos.

Demostración. μ_j es aditiva:

Recordemos que

$$(\sum_{i=0}^{\infty} a_ip^i) + (\sum_{i=0}^{\infty} b_ip^i) = \sum_{i=0}^{\infty} c_ip^i$$

donde

$$\begin{aligned} a_0 + b_0 &= q_0p + c_0 \\ q_0 + a_1 + b_1 &= q_1p + c_1 \\ \vdots \qquad &\vdots \qquad \vdots \\ q_{j-1} + a_j + b_j &= q_jp + c_j \end{aligned}$$

entonces

$$(\overline{a_0 + a_1p + a_2p^2 + \cdots + a_{j-1}p^{j-1}}) + (\overline{b_0 + b_1p + b_2p^2 + \cdots + b_{j-1}p^{j-1}}) =$$
$$= \overline{(a_0 + b_0) + (a_1 + b_1)p + (a_2 + b_2)p^2 + \cdots + (a_{j-1} + b_{j-1})p^{j-1}}$$

$= \overline{c_0 + (q_0 + a_1 + b_1)p + \cdots + (a_{j-1} + b_{j-1})p^{j-1}}$

$= \overline{c_0 + c_1 p + (q_1 + a_2 + b_2)p^2 + (a_3 + b_3)p^3 + \cdots + (a_{j-1} + b_{j-1})p^{j-1}}$

$= \overline{c_0 + c_1 p + c_2 p^2 + \cdots + (q_{j-2} + a_{j-1} + b_{j-1})p^{j-1}}$

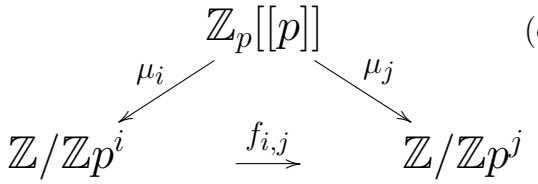
$= \overline{c_0 + c_1 p + \cdots + c_{j-1}p^{j-1} + \not{q}_{j-1}\ \not{p}^j}.$

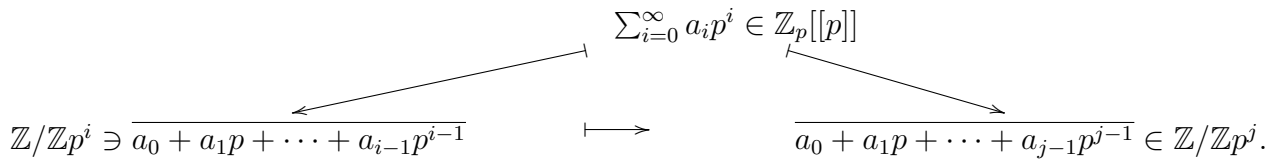
(El último sumando se cancela pues la barra significa clase módulo $\mathbb{Z}p^j$).

La demostración de que μ_j respeta el producto se demuestra usando la definición de producto en $\mathbb{Z}_p[[p]]$ es decir, análogamente como en el caso de que μ es aditiva.

Es claro que μ_j manda el uno de $\mathbb{Z}_p[[p]]$ al uno de $\mathbb{Z}/\mathbb{Z}p^j$. ■

Notemos ahora que



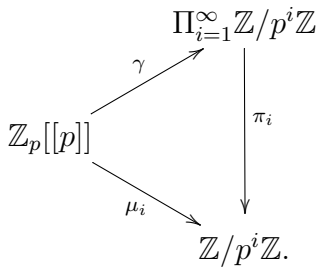


es un diagrama conmutativo, donde μ_i, μ_j, $f_{i,j}$ son homomorfismos de anillos.

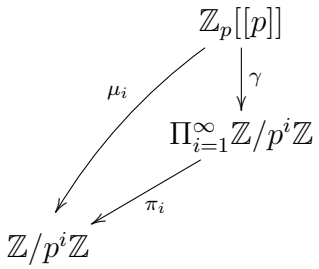
En la situación anterior, la familia $\{\ \mathbb{Z}_p[[p]] \xrightarrow{\mu_i} \mathbb{Z}/p^i\mathbb{Z}\ \}_{i\in I}$ induce el morfismo siguiente:

$$\mathbb{Z}_p[[p]] \xrightarrow{\gamma} \Pi_{i=1}^{\infty}\mathbb{Z}/p^i\mathbb{Z}$$

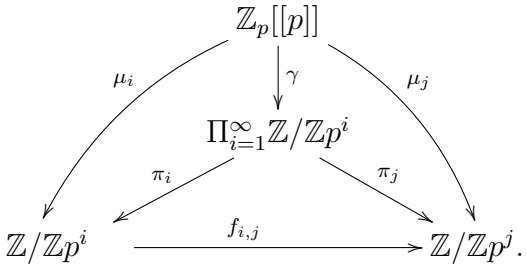
tal que conmuta el siguiente diagrama:



Si consideramos $\{\Pi_{i=1}^{\infty}\mathbb{Z}/p^i\mathbb{Z} \xrightarrow{\pi_i} \mathbb{Z}/p^i\mathbb{Z}\ \}_{i\in\mathbb{N}}$. Como tenemos que el diagrama siguiente:



es conmutativo $\forall i$ entonces también conmuta el siguiente diagrama excepto el triángulo inferior:



Tenemos que

$$\gamma(\mathbb{Z}_p[[p]]) \subseteq \{x \in \Pi_{i=1}^{\infty}\mathbb{Z}/\mathbb{Z}p^i | (f_{i,j} \circ \pi_i)(x) = \pi_j(x)\ \forall i \geq j\}.$$

Por otra parte si $x \in \Pi_{i=1}^{\infty}\mathbb{Z}/\mathbb{Z}p^i$ satisface $(f_{i,j} \circ \pi_i)(x) = \pi_j(x)\ \forall i \geq j$, entonces existe un elemento $\sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p[[p]]$ tal que

$$\gamma(\sum_{i=0}^{\infty} a_i p^i) = x.$$

Esto se demuestra en el Lema siguiente:

Lema 22 *Dada la sucesión $(x_1, x_2, x_3, ...)$ con $x_{i+1} \overset{p^i}{\equiv} x_i$ hay una única sucesión a_0, a_1, a_2,... donde $0 \leq a_i < p$ tal que*

$$a_0 + a_1 p + \cdots + a_{i-1} p^{i-1} \overset{p^i}{\equiv} x_i.$$

Demostración. Para empezar $a_0 \overset{p}{\equiv} x_1$ ($x_1 = s_1 p + a_0$) tiene solución única por el algoritmo de la división.

Ahora necesitamos encontrar a_1 tal que $a_0 + a_1 p \overset{p^2}{\equiv} x_2$. Es decir, $a_1 p \overset{p^2}{\equiv} x_2 - a_0 = x_2 - (x_1 - s_1 p)$. Como $x_2 - x_1$ es un múltiplo de p, denotemos $\frac{x_2 - x_1}{p}$ al entero tal que $\frac{x_2 - x_1}{p} \cdot p = x_2 - x_1$.

Ahora $a_1 p \overset{p^2}{\equiv} (x_2 - x_1) + s_1 p \Longleftrightarrow a_1 \overset{p}{\equiv} \frac{x_2 - x_1}{p} + s_1$.

Esto tiene una única solución mayor o igual que 0 y menor que p. Si ya hemos encontrado a_0, a_1,..., a_k con $0 \leq a_i < p$ tales que

$$\begin{aligned} a_0 &\overset{p}{\equiv} x_1 \\ a_0 + a_1 p &\overset{p^2}{\equiv} x_2 \\ \vdots \quad & \quad \vdots \quad \quad \vdots \\ a_0 + \cdots + a_k p^k &\overset{p^{k+1}}{\equiv} x_{k+1}. \end{aligned}$$

Entonces, como $x_{k+2} \overset{p^{k+1}}{\equiv} x_{k+1}$ entonces $\frac{x_{k+2}-x_{k+1}}{p^{k+1}} \in \mathbb{Z}$.

Queremos encontrar a_{k+1} tal que $a_0 + \cdots + a_{k+1}p^{k+1} \overset{p^{k+2}}{\equiv} x_{k+2}$.
Así

$$\begin{aligned} a_{k+1}p^{k+1} &\overset{p^{k+2}}{\equiv} x_{k+2} - (a_0 + \cdots + a_k p^k) \\ &\overset{p^{k+2}}{\equiv} (x_{k+2} - x_{k+1}) + ap^{k+1} \quad \iff \quad a_{k+1} \overset{p}{\equiv} \tfrac{(x_{k+2}-x_{k+1})}{p^{k+1}} + a. \end{aligned}$$

Esto tiene solución una mayor o igual que cero y menor que p.
Esto muestra que hay una sucesión que satisface las hipótesis. ■
En vista de la inyectividad de γ tenemos que $\mathbb{Z}_p[[p]]$ es isomorfo al límite inverso de

$$(\{\mathbb{Z}/\mathbb{Z}p^i\}_{i\in\mathbb{N}}, \{\ \mathbb{Z}/\mathbb{Z}p^i \xrightarrow{f_{i,j}} \mathbb{Z}/\mathbb{Z}p^j\ \}_{i\geq j})$$

donde $f_{i,j}$ es el morfismo de anillos canónico.
Esto junto con el Teorema 10 nos da otras descripciones del anillo de los enteros p-ádicos.

Conclusiones

Teorema 11 *Los siguientes anillos son isomorfos y cada uno es una copia del anillo de enteros p-ádicos:*

1. *El anillo de endomorfismos de* $\mathbb{Z}_{p^\infty}$.
2. *El anillo* $\{\sum_{i=0}^{\infty} a_i p^i | 0 \leq a_i < p\}$ *con la suma y el producto descrito en el texto.*
3. *El límite inverso del sistema dirigido de anillos*

$$\{(\mathbb{Z}/\mathbb{Z}p^i)_{i\in\mathbb{N}},\ \{\mathbb{Z}/\mathbb{Z}p^i \xrightarrow{f_{i,j}} \mathbb{Z}/\mathbb{Z}p^j\}_{i\geq j}\ ).$$

4. *El anillo de sucesiones* $\{(\overline{x_1}, \overline{x_2}, \overline{x_3}, ...) | \overline{x_i} \in \mathbb{Z}/\mathbb{Z}p^i, x_{i+1} \overset{p^i}{\equiv} x_i\}$, *que es un subanillo de* $\Pi_{i=1}^{\infty}\mathbb{Z}/\mathbb{Z}p^i$.

Demostración. Las demostraciones están incluidas en el texto. ■

Los enteros p-ádicos tienen las siguientes propiedades que se demuestran en la tesis:

a) El anillo de los enteros p-ádicos es conmutativo, es un dominio entero (el producto de elementos distintos de cero es distinto de cero).

b) Es un anillo local: tiene un único ideal máximo: $\{\sum_{i=0}^{\infty} a_i p^i | a_0 = 0\}$.

c) El conjunto de sus unidades (elementos invertibles) es

$$\mathbb{Z}_p^{\bullet}[[p]] = \{\sum_{i=1}^{\infty} a_i p^i | a_0 \neq 0\}.$$

d) Es un dominio de ideales principales, los ideales son de la forma

$$\mathcal{I}_j = \{\sum_{i=0}^{\infty} a_i p^i | v_p(\sum a_i p^j) \geq j\}.$$

e) El conjunto de ideales está totalmente ordenado por la inclusión

$$\mathcal{I}_k \leq \mathcal{I}_j \Longleftrightarrow k \geq j.$$

Bibliografía

[1] Alejandro Bravo, Hugo Rincón, Cesar Rincón, Álgebra Superior, México, Las prensas de Ciencias 2011, Facultad de Ciencias, UNAM.

[2] Anna Devic y Julian Kellerhals, Les nombres p-adiques, 2005-2006.

[3] Enzo Gentile, Estructuras Algebraicas, Buenos Aires, Argentina, Departamento de asuntos científicos Unión Panamericana Secretaría General Organización de los Estados Americanos Washington, D.C.- 1967.

[4] Enzo Gentile, Estructuras Algebraicas II (Álgebra lineal), Buenos Aires, Argentina, Facultad de Ciencias Exactas y Naturales Universidad de Buenos Aires, Argentina Programa Regional Científico y Tecnológico Departamento de asuntos científicos, Secretaría General de la Organización de los Estados Americanos Washington, D.C.- 1971.

[5] N Herstein, Álgebra Abstracta Versión en español de la obra Abstract Algebra por N.Herstein. D.R. 1988 por Grupo Editorial Iberoamérica, S.A. de C.V. La traducción estuvo a cargo del M. en C. Eduardo M. Ojeda Peña University of Arizona, E.U.A. Universidad Autónoma de Guadalajara (UAG), Guadalajara, México.

[6] Horacio O'brien, Estructuras Algebraicas III (Grupos Finitos), Buenos Aires, Argentina, Facultad de Ciencias Exactas y Naturales Universidad de Buenos Aires, Argentina Programa Regional Científico y Tecnológico, Departamento de asuntos científicos, Secretaría General de la Organización de los Estados Americanos Washington, D.C.- 1973.

[7] Enzo Gentile, Notas de Álgebra, Cursos y seminarios de matemática, Serie A Facículo 22 Año 2011, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires.

[8] Sebastian Pardo, Acerca de los grupos abelianos que no son la parte aditiva de un anillo, México, D.F. 30 de Abril del 2014, Tesis dirigida por el Dr. en Ciencias, Hugo Alberto Rincón Mejía.

[9] Hugo Rincón, Álgebra Lineal, México, Las prensas de Ciencias 2001, Facultad de Ciencias, UNAM.

[10] Hugo Rincón, Notas de Álgebra Moderna I.

[11] Hugo Rincón, Notas de Cogeneradores y generadores.

[12] Joseph Rotman, An Introduction to the Theory of Groups, USA Departament of Mathematics University of Illinois at Urbana-Champaign, Springer-Verlag Fourth Edition 1995.