UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
POSGRADO EN CIENCIAS MATEMÁTICAS

ACERCA DE GRUPOS ABELIANOS QUE NO SON LA PARTE ADITIVA DE UN ANILLO

TESIS
QUE PARA OPTAR POR EL GRADO DE:
MAESTRO EN CIENCIAS

PRESENTA:
SEBASTIÁN PARDO GUERRA

HUGO ALBERTO RINCÓN MEJÍA
FACULTAD DE CIENCIAS

MÉXICO, D. F. 30 DE ABRIL DEL 2014

Acerca de grupos abelianos que no son la parte aditiva de un anillo

Sebastián Pardo Guerra

Índice general

Agradecimientos

Introducción

Un K-espacio vectorial V, sobre el campo K, es una quinteta

$$(V, +, \overrightarrow{0}, K, \bullet : K \times V \longrightarrow V)$$

tal que:

1. $(V, +, \overrightarrow{0})$ es un grupo abeliano.

2. La acción $\bullet : K \times V \longrightarrow V$ satisface:

   a) $1 \bullet \overrightarrow{v} = \overrightarrow{v}$, $\forall \overrightarrow{v} \in V$.

   b) $(cd) \bullet \overrightarrow{v} = c \bullet (d \bullet \overrightarrow{v})$, $\forall c, d \in K$, $\forall \overrightarrow{v} \in V$.

   c) $(c + d) \bullet \overrightarrow{v} = c \bullet \overrightarrow{v} + d \bullet \overrightarrow{v}$, $\forall c, d \in K$, $\forall \overrightarrow{v} \in V$.

   d) $c \bullet (\overrightarrow{v} + \overrightarrow{w}) = c \bullet \overrightarrow{v} + c \bullet \overrightarrow{w}$, $\forall c \in F$, $\forall \overrightarrow{v}, \overrightarrow{w} \in V$.

Notemos que el campo K, como K-espacio vectorial, está sumergido en el espacio vectorial V (el cual asumiremos no nulo) bajo la identificación $k \longmapsto k \bullet v$, donde $v \in V$ es un elemento no nulo que consideraremos fijo. Ahora, si suponemos que $K \subset V$ y que el producto $\bullet$ sólo está definido para $K \times V$, surge la siguiente pregunta:

¿Cúando es posible extender la acción $\bullet : K \times V \longrightarrow V$ a un producto $\overline{\bullet} : V \times V \longrightarrow V$ asociativo de manera que $\overline{\bullet}\ |_K = \bullet$ y que satisfaga las propiedades mencionadas anteriormente?

Por ejemplo, el espacio vectorial $\mathbb{R}^3$ admite la operación $\times : \mathbb{R}^3 \times \mathbb{R}^3 \longrightarrow \mathbb{R}^3$, la cual conocemos como el producto cruz. Notemos que este producto no es asociativo, ya que por una parte $(i \times i) \times j = 0 \times j = 0$; y por otra parte $i \times (i \times j) = i \times k = j$.

Esto nos conduce a la siguiente pregunta

¿Cuándo un grupo abeliano A admite una función producto? Es decir, ¿Para qué grupos abelianos A podemos definir una multiplicación que distribuya a la operación suma del grupo abeliano A?

Todo anillo R está compuesto por un grupo abeliano $(R, +)$ con su operación aditiva, y de una operación producto $\bullet : R \times R \longrightarrow R$ (que también llamamos multiplicación) que distribuye a la operación del grupo abeliano. Si A es un grupo abeliano, entenderemos por una multiplicación en A a cualquier función bilineal $A \times A \longrightarrow A$. Denotamos por $MultA$ a todas las funciones bilineales $A \times A \longrightarrow A$. Como se verá más adelante, el conjunto $MultA$ forma un grupo abeliano bajo cierta operación.

Como cualquier grupo abeliano A es un $\mathbb{Z}$-módulo, usaremos tanto la teoría de módulos como la teoría de categorías para conocer la estructura del conjunto $MultA$. Además, al ser los elementos de $MultA$ funciones bilineales $A \times A \longrightarrow A$, surge de manera directa una asociación entre el grupo $MultA$ y el producto tensorial $A \otimes A$. Esto último nos llevará a identificar al grupo $MultA$ con el gurpo de morfismos entre los grupos $A \otimes A$ y A.

En el trabajo se desarrolla también la teoría de grupos abelianos, donde nuestro principal interés serán los grupos divisibles, así como los grupos puros. Estos nos darán condiciones suficientes para saber cuando un grupo abeliano no puede ser la parte aditiva de un anillo. Así mismo, se verán temas de topología, como la completación de un grupo topológico. Un ejemplo de esto último son los enteros $p-$ádicos, grupo que se mencionará en varias ocasiones a lo largo del trabajo.

Capítulo 1

Preliminares

1.1. Grupos

Definición 1.1.1. *Un monoide es una terna $(M, \cdot, 1)$ tal que M es un conjunto no vacío, $\cdot$ es una operación binaria asociativa en M y 1 es un elemento en M tal que $1 \cdot a = a = a \cdot 1$, $\forall a \in M$. Al elemento 1 se le llama el idéntico (o neutro) de M.*

Definición 1.1.2. *Un elemento u en un monoide M es invertible si existe v en M tal que $v \cdot u = 1 = u \cdot v$.*

Definición 1.1.3. *Un monoide G es un grupo si todos sus elementos son invertibles.*

Definición 1.1.4. *Sean $(G, \cdot, 1)$ un grupo y S un subconjunto no vacío de G. Decimos que S es un subgrupo de G si $(S, \cdot\mid_S, 1)$ es un grupo. En este caso, se denotará por $S \leq G$.*

Definición 1.1.5. *El orden de un grupo G es el número de elementos del conjunto G y se denota por $\mid G \mid$.*

Definición 1.1.6. *Un grupo $(A, \cdot, 1)$ se dice que es abeliano, si la operación $\cdot$ en G es conmutativa. Esto es,*

$$u \cdot v = v \cdot u, \ \forall u, v \in A.$$

En el caso de un grupo abeliano $(A, \cdot, 1)$, se usará preferentemente la notación aditiva $+$ (en lugar de $\cdot$). Usando la notación aditiva, al idéntico se le denota como 0.

Si S es cualquier subconjunto del grupo A, el subgrupo generado por S es la intersección de todos los subgrupos de A que contienen a S, esto es,

$$< S >= \cap\{B \mid S \subset B \text{y } B \leq A\}.$$

Al subgrupo generado por S lo denotamos por $< S >$.

Observación. *Si $S \neq \varnothing$,*

$$< S >= \{a_1^{n_1} \cdot a_2^{n_2} \cdot \dots \cdot a_s^{n_s} \mid s \geq 1,\ a_1, a_2, \dots, a_s \in S,\ n_1, n_2, \dots, n_s \in \mathbb{Z}\}$$

Cuando S consiste de los elementos a_i con $i \in I$, y el grupo A es abeliano, los elementos de $< S >$ son de la forma $n_1a_1 + \cdots + n_ka_k$ con $a_j \in S$, $n_j \in \mathbb{Z}$ y $k \in \mathbb{N}$. A este tipo de elementos les llamamos *combinaciones $\mathbb{Z}$-lineales.*

Definición 1.1.7. *Si $< S >= A$, decimos que S es un conjunto generador de A y a los elementos de S les llamamos generadores de A.*

En particular, cuando $S = \{a\}$, llamamos al subgrupo

$$< a >= \{a^k \mid k \in \mathbb{Z}\}$$

el *grupo cíclico* con generador a.

Observación. *Todo grupo cíclico A es abeliano.*

Definición 1.1.8. *Sea A un grupo. Si $a \in A$, el orden de a es el orden del subgrupo $< a >$, y lo denotamos por $o(a)$.*

Observación. *Si $< a >$ es finito, el orden de a es un número natural. En el caso que $< a >$ no es finito, se dice que a es de orden infinito.*

Observación. *Si B y C son subgrupos de A, el subgrupo generado por B y por C, es el subgrupo de A generado por el conjunto $B \cup C$, y se denota por $< B, C >$.*

Observación. *Nótese que si A es un grupo abeliano, los elementos de $< B, C >$ son de la forma $b + c$, con $b \in B$ y $c \in C$.*

Observación. *En el caso de grupos abelianos, al subgrupo generado por B y C, lo denotaremos por $B + C$. Esta idea se puede generalizar para cualquier familia de subgrupos $\{B_i\}_{i \in I}$ de un grupo abeliano A. En tal caso, si $B = \Sigma_{i \in I} B_i$, cada elemento de B es una suma finita $b_{i_1} + \cdots + b_{i_k}$, donde $b_{i_j} \in B_{i_j}$, para cada $j = 1, \dots, k$.*

Definición 1.1.9. *Sean A y C grupos con operaciones $\cdot$ y $*$, respectivamente. Un morfismo de grupos $\varphi : A \longrightarrow C$ es una función tal que para cualquier $a_1, a_2 \in A$ se tiene*

$$\varphi(a_1 \cdot a_2) = \varphi(a_1) * \varphi(a_2).$$

Note que si A y C son grupos abelianos, usando la notación aditiva, un morfismo $\varphi : A \longrightarrow C$ de grupos abelianos satisface que

$$\varphi(a_1 + a_2) = \varphi(a_1) + \varphi(a_2), \ \forall a_1, a_2 \in A$$

Definición 1.1.10. *Un subgrupo N de G es normal si $aN = Na$ para cualquier $a \in G$.*

Notación. Si N es un subgrupo normal de G, escribimos $N \lhd G$.

Observación. *En cualquier grupo abeliano G todo subgrupo es normal.*

Definición 1.1.11. *Sea G un grupo y $N \lhd G$. El morfismo $\rho : G \longrightarrow G/N$, con regla de correspondencia $g \longmapsto gN$, es el morfismo canónico.*

Teorema 1.1.12. *(Lagrange) Si G es un grupo de orden finito y H un subgrupo, entonces $\mid G \mid = \mid H \mid [G : H]$, donde $[G : H]$ es el índice de H en G.*

Definición 1.1.13. *Sea C un subgrupo cíclico del grupo G. Denotamos por $gen(C)$ al conjunto de todos los generadores del grupo C.*

Definición 1.1.14. *Un grupo finitamente generado es aquel que tiene un conjunto generador finito.*

Definición 1.1.15. *La función φ de Euler se define como:*

$$\varphi(n) = \mid \{k \mid 1 \leq k \leq n \ y \ (k; n) = 1\} \mid.$$

Teorema 1.1.16. *Si n es un entero positivo, entonces $n = \Sigma_{d|n}\varphi(d)$, donde la suma se toma para todos los divisores d de n, con $1 \leq d \leq n$, y φ es la función de Euler.*

Proposición 1.1.17. *Sea G es un grupo cíclico de orden n. Entonces*

$$\mid gen(G) \mid = \varphi(n).$$

Definición 1.1.18. *Sea p un primo. Un p-grupo es un grupo en donde todo elemento tiene como orden una potencia del primo p.*

Ejemplo. *El cociente $\mathbb{Z}/p\mathbb{Z} := \mathbb{Z}(p)$ cumple que todo elemento distinto de 0 tiene orden p.*

Definición 1.1.19. *Sean G un grupo y $a, b \in G$. El conmutador de a y b es*

$$[a; b] = aba^{-1}b^{-1}.$$

El subgrupo conmutador G' de G es el subgrupo generado por los elementos de la forma $[a; b]$ para cualquier $a, b \in G$.

Lema 1.1.20. *Sean G un grupo y N un subgrupo normal de G. Las siguientes proposiciones son equivalentes:*

(i) G/N es un grupo abeliano

(ii) $G' \leq N$.

Demostración. $(i) \implies (ii)$. Sean $a, b \in G$. Como N es un subgrupo normal, se cumple que

$$a^{-1}b^{-1}N = (a^{-1}N)(b^{-1}N), \text{ así como } b^{-1}a^{-1}N = (b^{-1}N)(a^{-1}N).$$

Por ser G/N un grupo abeliano, se sigue que

$$a^{-1}b^{-1}N = (a^{-1}N)(b^{-1}N) = (b^{-1}N)(a^{-1}N) = b^{-1}a^{-1}N,$$

es decir, $aba^{-1}b^{-1}N = N$. Esto muestra que $[a; b] \in N$, para cualquier par de elementos $a, b \in G$. Por lo tanto, $G' \leq N$.

$(ii) \implies (i)$. Sean $a, b \in G$. Como $G' \leq N$, entonces $a^{-1}b^{-1}ab \in G' \leq N$, por lo que $(a^{-1}b^{-1}ab)N = N$. Al ser N un subgrupo normal de G, entonces

$$(aN)(bN) = abN = baN = (bN)(aN),$$

lo cual muestra que G/N es un grupo abeliano. $\square$

Teorema 1.1.21. *Para cualquier morfismo de grupos $\varphi : G \longrightarrow H$ se tiene que $\varphi(G') \subset H'$. Si φ es suprayectiva, se tiene la igualdad. Además, si H es abeliano, se tiene un único morfismo $\tilde{\varphi} : G/G' \longrightarrow H$ que hace conmutativo el diagrama*

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\rho"'] & H \\ G/G' \arrow[ur, "\tilde{\varphi}"'] & \end{tikzcd}$$

donde ρ es el morfismo canónico.

Demostración. Sea $\varphi : G \longrightarrow H$ un morfismo. Si $[a,b] \in G'$, entonces

$$\varphi([a;b]) = \varphi(aba^{-1}b^{-1}) = \varphi(a)\varphi(b)\varphi(a^{-1})\varphi(b^{-1}) = \varphi(a)\varphi(b)\varphi(a)^{-1}\varphi(b)^{-1}.$$

Por lo tanto, cuando φ es un epimorfismo, $\varphi(G') = H'$.

Supongamos ahora que H es un grupo abeliano. En este caso, $H' = 1$, con lo cual $\varphi(G') = 1$. Definimos la función $\tilde{\varphi} : G/G' \longrightarrow H$ con regla de correspondencia $gG' \longmapsto \varphi(g)$. Nótese que $\tilde{\varphi}$ está bien definida. En efecto, si $g_1G' = g_2G'$, entonces $g_2^{-1}g_1 \in G'$, por lo que $\varphi(g_2^{-1}g_1) = \varphi(g_2^{-1})\varphi(g_1) = 1$, es decir, $\varphi(g_1) = \varphi(g_2)$, mostrando así que $\tilde{\varphi}(g_1) = \tilde{\varphi}(g_2)$. Ahora, como G/G' es un grupo abeliano y φ es un morfismo, se tiene que $\tilde{\varphi}$ es un morfismo de grupos que hace conmutativo al diagrama

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\rho"'] & H \\ G/G' \arrow[ur, "\tilde{\varphi}"'] & \end{tikzcd} .$$

Si $\psi : G/G' \longrightarrow H$ es cualquier otro morfismo que hace conmutativo al diagrama anterior, se tiene que para cualquier $gG' \in G'/G$,

$$\psi(gG') = \varphi(g) = \tilde{\varphi}(gG').$$

Por lo tanto, $\tilde{\varphi}$ es única. □

A lo largo del texto, nos interesaremos en grupos abelianos. A menos que se diga otra cosa, los grupos considerados serán abelianos y la operación en el grupo será denotada aditivamente.

Definición 1.1.22. *Si todo elemento de un grupo abeliano A tiene orden finito, decimos que A es un grupo de torsión, mientras que el grupo abeliano A es libre de torsión si el único elemento de orden finito es el* 0.

Definición 1.1.23. *Un grupo abeliano T es de torsión, si todo elemento tiene orden finito.*

Definición 1.1.24. *Decimos que un grupo es mixto si tiene elementos de orden finito y de orden infinito.*

Definición 1.1.25. *Sea A un grupo abeliano. Para cada primo p, el conjunto*

$$A_p = \{a \in A \mid ord(a) = p^k, \text{ para alguna } k \in \mathbb{N}\}$$

es un subgrupo y se le conoce como la p-componente de A.

Definición 1.1.26. *Sean A un grupo abeliano y $E \leq A$. Decimos que E es esencial en A si $E \cap B \neq \{0\}$ para cualquier subgrupo $B \leq A$ con B distinto de cero.*

Teorema 1.1.27 (Teorema Fundamental sobre Grupos Abelianos Finitamente Generados)**.** *Sea G un grupo abeliano finitamente generado. Entonces G es la suma directa de grupos cíclicos.*

Definición 1.1.28. *Un anillo R con 1, es un conjunto no vacío, junto con dos operaciones binarias $+, \cdot$ y dos elementos distintos y distinguidos $0, 1 \in R$ tales que:*

1. *$(R, +, 0)$ es un grupo abeliano.*
2. *$(R, \cdot, 1)$ es un monoide.*
3. *Para cualesquiera $a, b, c \in R$ se cumple*
   - $a(b + c) = ab + ac$.
   - $(b + c)a = ba + ca$.

Definición 1.1.29. *Dado un primo p, el conjunto ${}_p\mathbb{Q} = \{\frac{n}{m} \mid (m, p) = 1\}$ es un subanillo de $\mathbb{Q}$. A este anillo se le llama el anillo localizado en p.*

1.2. Retículas

Definición 1.2.1. *Sea L un conjunto. Una relación en L es un subconjunto $R \subset L \times L$. Decimos que los elementos $a, b \in L$ están relacionados por R si y sólo si $(a, b) \in R$. En este caso, lo denotamos por aRb.*

Definición 1.2.2. *Una relación R, en el conjunto L, es reflexiva si para toda $a \in L$, aRa.*

Definición 1.2.3. *Una relación R, en el conjunto L, es antisimétrica si para cualquier $a, b \in L$,*

$$aRb \text{ y } bRa \text{ implica que } a = b.$$

Definición 1.2.4. *Una relación R, en el conjunto L, es transitiva si para cualesquiera $a, b, c \in L$ se cumple que*

$$aRb \text{ y } bRc \text{ implica que } aRc.$$

Definición 1.2.5. *Un conjunto parcialmente ordenado es un par $(L, \leq)$, donde $\leq$ es una relación en el conjunto L que satisface:*

1. *$\leq$ es reflexiva.*

2. *$\leq$ es antisimétrica.*

3. *$\leq$ es transitiva.*

En un conjunto parcialmente ordenado $(L, \leq)$, no cualquier par de elementos son comparables. Esto es, para $a, b \in L$ no necesariamente se cumple que $a \leq b$ ó $b \leq a$.

Escribimos $a < b$ si $a \leq b$ y $a \neq b$.

Definición 1.2.6. *Sea S un subconjunto del conjunto parcialmente ordenado $(L, \leq)$. Una cota superior de S es un elemento $u \in L$ tal que $a \leq u$ para toda $a \in S$. Una cota inferior del conjunto S es un elemento $u \in L$ tal que $u \leq a$, $\forall a \in S$.*

Definición 1.2.7. *Sean $(L, \leq)$ un conjunto parcialmente ordenado y $S \subset L$. Decimos que $b \in S$ es un primer elemento (o menor) de S si para todo $x \in S$, $b \leq x$. Así mismo, decimos que $b \in S$ es un último elemento (o mayor) de S, si para todo $x \in S$, $x \leq b$.*

Observación. *Sea $(L, \leq)$ un conjunto parcialmente ordenado y S es un subconjunto de L. Si b_1 y b_2 son ambos elementos menores(mayores) de S, entonces son iguales. En efecto, por ser b_1 un primer elemento de S, como $b_2 \in S$, entonces $b_1 \leq b_2$. Análogamente, por ser b_2 un primer elemento de S, como $b_1 \in S$, se sigue que $b_2 \leq b_1$. Por lo tanto, $b_1 = b_2$.*

Definición 1.2.8. *Sea S un subconjunto no vacío de $(L, \leq)$ con cotas superiores. Si el conjunto de cotas superiores tiene un elemento menor, entonces el supremo de S, que denotamos por sup S, es el menor elemento del conjunto de cotas superiores de S. Esto es, $b = sup\ S$ si b es una cota superior de S tal que $b \leq u$ para cualquier otra cota superior $u \in L$ del conjunto S.*

Definición 1.2.9. *Sea S un subconjunto no vacío de $(L, \leq)$ con cotas inferiores. Si el conjunto de cotas inferiores tiene un elemento mayor, el ínfimo de S, que denotamos por $inf\ S$, es el mayor elemento del conjunto de cotas inferiorer del conjunto S. En otras palabras, $l = inf\ S$ si l es una cota inferior de S tal que $v \leq l$ para cualquier otra cota inferior v de S.*

Definición 1.2.10. *Un elemento $m \in S$ es máximo si no existe $s \in S$ para el cual $m < s$.*

Definición 1.2.11. *Un elemento $m \in S$ es mínimo si no existe $s \in S$ para el cual $s < m$.*

Definición 1.2.12. *Una retícula es un conjunto L parcialmente ordenado por $\leq$, tal que para cualquier par de elementos $a, b \in L$, existe un supremo, que denotamos por $a \vee b$, así como un ínfimo, que denotamos por $a \wedge b$.*

Definición 1.2.13. *Una retícula $(L, \leq)$ es completa si todo subconjunto S de L no vacío, tiene un supremo y un ínfimo. De esta manera, el elemento*

$$1 = sup\ \{a \mid a \in L\}$$

satisface que $a \leq 1$, $\forall a \in L$, así como el elemento

$$0 = inf\ \{a \mid a \in L\}$$

es tal que $0 \leq a$, $\forall a \in L$.

Teorema 1.2.14. *Un conjunto parcialmente ordenado $(L, \leq)$ es una retícula completa si y sólo si L contiene un único elemento máximo y si cualquier subconjunto no vacío de L tiene un ínfimo.*

Definición 1.2.15. *Un conjunto parcialmente ordenado $(L \leq)$ está dirigido superiormente si para cualesquiera dos elementos a y b en L, existe $c \in L$ tal que $a \leq c$ y $b \leq c$.*

1.3. Categorías

Definición 1.3.1. *Una categoría $\mathcal{C}$ es una clase de objetos, que denotamos por $Ob(\mathcal{C})$, cuyos elementos los indicaremos por las letras $A, B, C, \ldots$, junto con* *(i) Una clase de conjuntos ajenos, que denotamos por $Hom(A,B)$, uno para cada par de objetos en $\mathcal{C}$. Los elementos en $Hom(A,B)$ se llaman morfismos (o flechas), de A a B, y los expresamos como $f : A \longrightarrow B$ ó $A \xrightarrow{f} B$.*

(ii) Para cada tripleta ordenada (A,B,C), de objetos de $\mathcal{C}$, una función

$$Hom(B,C) \times Hom(A,B) \longrightarrow Hom(A,C);$$

tal que a cada $f : A \longrightarrow B$ y $g : B \longrightarrow C$, le asigna la función

$$g \circ f : A \longrightarrow C.$$

A la función $g \circ f$, se le llama la composición de f y g.

Asociatividad *Si $f : A \longrightarrow B$, $g : B \longrightarrow C$ y $h : C \longrightarrow D$ son morfismos, entonces*

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

Identidad *Para cada objeto B de $\mathcal{C}$, existe un mofrismo $id_B : B \longrightarrow B$, tal que, para cualquier $f : A \longrightarrow B$ y $g : B \longrightarrow C$, se cumple*

$$id_B \circ f = f \text{ y } g \circ id_B = g.$$

Nótese que cada morfismo $f : A \longrightarrow B$ está en un único conjunto $Hom(A,B)$, ya que estos son ajenos entre sí. Además, de la definición anterior, se sigue que una categoría $\mathcal{C}$ está compuesta por tres clases distintas; la primera es la clase de objetos de la categoría, la segunda es la clase de morfismos entre los objetos de la categoría y la tercera es la clase de composiciones entre los morfismos de la categoría.

Ejemplo. *1. **Rng** es la categoría cuyos objetos son anillos asociativos con 1 y las flechas son los morfismos de anillos; cada composición es la composición usual de funciones.*

*2. **Grp** es la categoría donde los objetos son grupos y las flechas son los morfismos de grupos; cada composición es la composición usual de morfismos.*

3. ***Top*** *es la categoría donde los objetos son espacios topológicos, las flechas son las funciones continuas y cada composición es la composición usual de funciones.*

4. ***Set*** *es la categoría que tiene como objetos a todos los conjuntos y como flechas a las funciones entre ellos. Cada composición es la composición usual de funciones.*

5. ***Ab*** *es la categoría donde los objetos son grupos abelianos y las flechas son morfismos de grupos. Cada composición es la composición usual de morfismos.*

Definición 1.3.2. *Una categoría $\mathcal{C}$ es pequeña si la clase de objetos es un conjunto.*

Definición 1.3.3. *Sea $\mathcal{C}$ una categoría. Decimos que $\mathcal{D}$ es una subcategoría de la categoría $\mathcal{C}$ si $Ob\mathcal{D}$ es una subclase de la clase $Ob\mathcal{C}$, tal que para cualquier $A, B \in Ob\mathcal{D}$,*

$$Hom_{\mathcal{D}}(A, B) \subset Hom_{\mathcal{C}}(A, B).$$

Además, se tiene que para cualquier objeto $A \in \mathcal{D}$, id_A es un morfismo en $\mathcal{D}$ y la composición de morfismos en $\mathcal{D}$ es la misma que en $\mathcal{C}$.

Definición 1.3.4. *Sean $\mathcal{C}$ y $\mathcal{D}$ categorías. Un funtor $F : \mathcal{C} \longrightarrow \mathcal{D}$ consiste en dos funciones; una función entre los objetos, que asigna a cada objeto $C \in \mathcal{C}$ el objeto $F(C) \in \mathcal{D}$, y otra función entre morfismos, la cual manda el morfismo $f : X \longrightarrow Y$ en $\mathcal{C}$, al morfismo $F(f) : F(X) \longrightarrow F(Y)$, de tal manera que*

1. *Para cada $X \xrightarrow{f} Y \xrightarrow{g} Z$ en $\mathcal{C}$, $F(g \circ f) = F(g) \circ F(f)$.*

2. *$F(id_X) = id_{F(X)}$ para cualquier $X \in \mathcal{C}$.*

Definición 1.3.5. *Un funtor $F : \mathcal{C} \longrightarrow \mathcal{D}$ es fiel si para cada par de objetos $A, B \in \mathcal{C}$, la correspondencia $f \longmapsto F(f)$ de*

$$Hom_{\mathcal{C}}(A, B) \longrightarrow Hom_{\mathcal{D}}(F(A), F(B))$$

es inyectiva. Decimos también que $F : \mathcal{C} \longrightarrow \mathcal{D}$ es un funtor pleno si la correspondencia $f \longmapsto F(f)$, definida de

$$Hom_{\mathcal{C}}(A,B) \longrightarrow Hom_{\mathcal{D}}(F(A),F(B))$$

es suprayectiva.

Ejemplo. 1. *Un conjunto D está preordenado si existe una relación $\leq$ reflexiva y transitiva en D. Con esto en cuenta, todo conjunto preordenado D determina una categoría. En efecto, la clase de objetos de la categoría son los elementos de D. Además, para cualquier par de objetos (x,y), $Hom(x,y)$ es vacío o consiste en una sola flecha $x \longrightarrow y$, dependiendo si $x \nleq y$ o $x \leq y$. Así, la composición de morfismos $x \longrightarrow y \longrightarrow z$ queda definida por la relación $x \leq y \leq z$. Nótese que esta categoría es pequeña. De esta manera, la categoría de conjunos preordenados tiene como objetos a los conjuntos preordenados y morfismos a las funciones monótonas entre conjuntos preordenados, es decir, funciones que respetan las relaciones.*

2. *Sea $\mathcal{D}$ una subcategoría de la categoría $\mathcal{C}$. El funtor de inclusión de $\mathcal{D}$ a $\mathcal{C}$, que manda a cada objeto en $\mathcal{D}$ al mismo objeto en $\mathcal{C}$, así como a cualquier morfismo en $\mathcal{D}$ al mismo morfismo en $\mathcal{C}$, es un funtor fiel que no es necesariamente pleno.*

Definición 1.3.6. *Un objeto inicial en una categoría $\mathcal{C}$ es un objeto X tal que para cualquier objeto $Y \in \mathcal{C}$ exite un único morfismo $X \longrightarrow Y$. Análogamente, un objeto X es terminal en la categoría $\mathcal{C}$ si para cualquier objeto $Y \in \mathcal{C}$ existe un único morfismo $Y \longrightarrow X$.*

1.4. Conjuntos

Axioma de Elección. Para toda familia no vacía $\mathcal{F}$ de conjuntos no vacíos, existe una función $f : \mathcal{F} \longrightarrow \cup_{X \in \mathcal{F}} X$ tal que $f(S) \in S$ para cada conjunto S en la familia $\mathcal{F}$.

Definición 1.4.1. *Si S es un conjunto parcialmente ordenado por $\leq$, llamamos a un subconjunto T de S una cadena si cualquier par de elementos $a, b \in T$ son comparables, es decir, $a \leq b$ ó $b \leq a$.*

Lema 1.4.2. *(Lema de Zorn) Si S es un conjunto parcialmente ordenado, para el cual toda cadena en S tiene una cota superior en S, entonces S tiene al menos un elemento maximal.*

Definición 1.4.3. *Decimos que una relación $\leq$ en un conjunto S es un buen orden si todo conjunto no vacío $X \subset S$ tiene un primer elemento con respecto al orden $\leq$.*

Principio del Buen Orden. (Zermelo) A todo conjunto S se le puede asignar una relación $\leq$ de buen orden.

Definición 1.4.4. *Sea $\mathcal{F}$ una familia de conjuntos. Se dice que $\mathcal{F}$ es una familia de carácter finito si para cada conjunto A, se tiene que $A \in \mathcal{F}$ si y sólo si cada subconjunto finito de A pertenece a $\mathcal{F}$.*

Lema 1.4.5. *(Lema deTukey). Sea $\mathcal{F}$ una familia no vacía de conjuntos. Si $\mathcal{F}$ es de carácter finito, entonces $\mathcal{F}$ tiene un elemento maximal (con respecto a la inclusión).*

Teorema 1.4.6. *Los siguientes principios son equivalentes:*

1. *El Axioma de Elección.*

2. *Principio del Buen Orden.*

3. *Lema de Zorn.*

4. *Lema de Tukey.*

1.5. Topología

Definición 1.5.1. *Sean X un conjunto y τ un subconjunto del conjunto potencia $\wp(X)$. Decimos que τ es una topología en X si satisface las siguientes propiedades:*

1. *$X, \varnothing \in \tau$.*

2. *Si $U_1, U_2, \ldots, U_n \in \tau$ entonces $\cap_{i=1}^{n} U_i \in \tau$.*

3. *Para cualquier familia $\{U_\alpha\}_{\alpha \in I}$ en τ, se tiene que $\cup_{\alpha \in I} U_\alpha \in \tau$.*

Nótese que la segunda condición es equivalente a que $U \cap V \in \tau$, para cualquier U y V en τ. A los elementos de τ se les conoce como conjuntos abiertos. Decimos que la pareja (X, τ) es un espacio topológico, al cual abreviaremos por X cuando este claro del contexto cual es la topología τ.

Definición 1.5.2. *Un conjunto* $E \subset X$ *es cerrado si* $X \setminus E$ *es abierto en* τ.

Observación. *Una topología* τ *también se puede definir en términos de los conjuntos cerrados. Sea* τ *una topología en* X *definida por los abiertos* $\{U_\alpha\}_{\alpha\in I}$. *Si* $V_\alpha = X \setminus U_\alpha$, *para cada* $\alpha \in I$, *por las Leyes de De Morgan se sigue que la familia de conjuntos* $\tau' = \{V_\alpha\}_{\alpha\in I}$ *satisface:*

1. $X, \varnothing \in \tau'$.
2. *Si* $V_1, V_2, \ldots, V_n \in \tau'$ *entonces* $\cup_{i=1}^n V_i \in \tau'$.
3. *Para cualquier familia* $\{V_\alpha\}_{\alpha\in J}$ *en* τ', *se tiene que* $\cap_{\alpha\in J} V_\alpha \in \tau'$.

Se define también el interior de un conjunto E, denotándolo por E°, como

$$E^\circ = \cup\{G \subset X \mid G \in \tau, G \subset E\},$$

de donde se sigue que, por ser E° unión de abiertos, $E^\circ \in \tau$.

Definición 1.5.3. *Sean* (X, τ) *un espacio topológico y* $Y \subset X$. *La topología inducida en* Y *tiene como abiertos a los conjuntos de la forma* $U \cap Y$, *donde* $U \in \tau$.

Definición 1.5.4. *Sean* (X, τ) *un espacio topológico y* $x \in X$. *Una vecindad de* x *es un conjunto* $V_x \subset X$ *tal que contiene un abierto* U *para el cual* $x \in U$. *A la colección de vecindades* V_x *la llamamos sistema de vecindades de* x.

Definición 1.5.5. *Un filtro* $\mathcal{F}$, *en un conjunto* S, *es una colección no vacía de subconjuntos de* S *con las siguientes propiedades:*

- *Si* $F_1, F_2 \in \mathcal{F}$ *entonces* $F_1 \cap F_2 \in \mathcal{F}$.
- *Si* $F \in \mathcal{F}$ *y* $F \subset G$ *entonces* $G \in \mathcal{F}$

Ejemplo. *Sean* (X, τ) *un espacio topológico y* $A \subset X$. *El conjunto*

$$\{U \subset X \mid A \subset U^\circ\}$$

es un filtro en X. *En particular, cuando* $A = \{x\}$, *este último conjunto es el conjunto de todas las vecindades de* $x \in X$, *por lo que el sistema de vecindades de cualquier punto* $x \in X$ *es un filtro en* X.

Definición 1.5.6. *Sean (X,τ) un espacio topológico y $x \in X$. Una base de vecindades en x es una subcolección β_x, tomada del conjunto de vecindades V_x, tal que para cualquier vecindad U de x, existe $W \in \beta_x$ tal que $W \subset U$.*

Definición 1.5.7. *Dado un espacio topológico (X,τ), decimos que un subconjunto β de τ es una base para τ (o bien para X) si todo conjunto en τ es la unión de elementos de β.*

Observación. *Para cada $x \in X$, si β es una base para (X,τ), entonces el conjunto $\beta_x = \{B \in \beta \mid x \in B\}$ es una base de vecindades en x.*

Definición 1.5.8. *Sea (X,τ) un espacio topológico. Una sub-base de τ (o bien de X) es una colección $\mathcal{C} \subset \tau$ tal que el conjunto de intersecciones finitas de elementos de $\mathcal{C}$ forma una base para τ.*

El siguiente resultado muestra que cualquier colección $\mathcal{F}$ de subconjuntos de un conjunto dado X, induce una topología cuyos abiertos básicos están formados por uniones arbitrarias de intersecciones finitas de elementos de $\mathcal{F}$:

Teorema 1.5.9. *Cualquier colección de subconjuntos de un conjunto X es una sub-base para alguna topología en X.*

Definición 1.5.10. *Si (X,τ) y (Y,σ) son espacios topológicos, decimos que la función $f : X \longrightarrow Y$ es continua si para cualquier abierto $U \in \sigma$, $f^{-1}(U) \in \tau$, es decir, la imagen inversa de abiertos es abierta.*

Proposición 1.5.11. *Si $X \xrightarrow{f} Y$ y $Y \xrightarrow{g} Z$ son funciones continuas, entonces $X \xrightarrow{g \circ f} Z$ es continua.*

Definición 1.5.12. *Decimos que un espacio topológico (X,τ) es T_1 si dados $x, y \in X$ elementos distintos, podemos encontrar dos abiertos U y V en la topología para los cuales $x \in U$ y $y \notin U$, así como $y \in V$ y $x \notin V$.*

Definición 1.5.13. *Si (X,τ) es un espacio topológico tal que, para cualesquiera dos elementos $x, y \in X$ existen abiertos U y V tales que $x \in U$, $y \in V$ y $U \cap V = \varnothing$ decimos que (X,τ) es T_2 o bien de Hausdorff.*

Definición 1.5.14. *Sean (X,τ) un espacio topológico y $\{x_n\}_{n\in\mathbb{N}}$ una sucesión de elementos en X. Decimos que la sucesión converge al elemento x, si para cada vecindad U de x, existe un natural m tal que, para cualquier $k \geq m$ se cumple que $x_k \in U$. Esto último lo denotamos por $\{x_n\}_{n\in\mathbb{N}} \longrightarrow x$.*

Esta última noción se puede generalizar al concepto de redes.

Definición 1.5.15. *Sea I un conjunto parcialmente ordenado y dirigido superiormente. Una red es una función $\alpha : I \longrightarrow X$. Toda red $\alpha : I \longrightarrow X$ la notaremos por $\alpha = \{x_i\}_{i\in I}$, donde $x_i = \alpha(i)$.*

Observación. *Si I es un conjunto dirigido superiormente, se tiene una biyección entre el conjunto de funciones de I a X y el conjunto de familias $\{x_i\}_{i\in I}$ de elementos de X, etiquetadas por el conjunto I. Nótese también que cuando $I = \mathbb{N}$, las redes en X son sucesiones en X.*

Definición 1.5.16. *Una sub-red de la red $\alpha : I \longrightarrow A$ es la red $\alpha\circ\varphi : M \longrightarrow A$, donde $\varphi : M \longrightarrow I$ es una función de un conjunto dirigido M a I tal que:*

- *Si $\lambda \leq \nu$ en M entonces $\varphi(\lambda) \leq \varphi(\nu)$. (Creciente)*
- *Para cada $i \in I$, existe $\mu \in M$ tal que $i \leq \varphi(\mu)$. (Cofinal en I)*

Definición 1.5.17. *Una red $\{x_i\}_{i\in I}$ en (X,τ) converge al elemento $x \in X$, si para cada vecindad U de x, existe $\lambda \in I$ tal que para cualquier $\mu \geq \lambda$ se cumple que $x_\mu \in U$. En este caso, se denota por $\{x_i\}_{i\in I} \longrightarrow x$.*

Dada una red $\{x_i\}_{i\in I}$ en (X,τ), una *cola* de la red $\{x_{i\in I}\}_{i\in I}$ es un conjunto de la forma $\{x_\lambda \mid \lambda \geq \lambda_0\}$ para algún $\lambda_0 \in I$.

Ejemplo. *Sean (X,τ) un espacio topológico y $x \in X$. Si Λ es un sistema básico de vecindades de x en X, al definir la relación en Λ por $U_1 \leq U_2$ si y sólo si $U_2 \subset U_1$ se tiene que Λ es un conjunto dirigido. Más aún, al escoger un elemento $x_U \in U$ para cada $U \in \Lambda$, se obtiene una red $\{x_U\}_{U\in\Lambda}$ convergente a x. En efecto, si V es cualquier vecindad de x, como Λ es un sistema básico de vecindades de x, existe $U_0 \in \Lambda$ tal que $U_0 \subset V$. De esta manera, para cualquier $U \in \Lambda$ con $U_0 \leq U$ se tiene que $U \subset U_0 \subset V$, con lo cual $x_U \in V$ para todo $U \geq U_0$.*

Definición 1.5.18. *Sean (X,τ) un espacio topológico y $E \subset X$. La cerradura de E es el conjunto*

$$\overline{E} = \cap\{K \subset X \mid K \text{ es cerrado y } E \subset K\}.$$

Proposición 1.5.19. *Sean (X,τ) un espacio topológico y $E \subset X$. Entonces, $x \in \overline{E}$ si y sólo si para cualquier abierto U, que contiene a x, se tiene que $U \cap E \neq \varnothing$.*

Proposición 1.5.20. *Sea $E \subset X$. Entonces $x \in \overline{E}$ si y sólo si existe una red $\{x_{i \in I}\}$ en E que converge a x.*

Una propiedad de los espacios topológicos T_2 es la siguiente:

Proposición 1.5.21. *Si (X, τ) es un espacio topológico de Hausdorff, entonces los límites son únicos.*

Demostración. Supongamos que $\{x_i\}_{i \in I}$ es una red que converge a los elementos x_0 y x_1. Como el espacio es de Hausdorff, existen abiertos ajenos U y V tales que $x \in U$ y $y \in V$. Como $\{x_i\}_{i \in I} \longrightarrow x$, para el abierto U existe $\lambda_0 \in I$ para la cual si $\lambda \geq \lambda_0$ entonces $x_\lambda \in U$. Por otra parte, como $\{x_i\}_{i \in I} \longrightarrow x_1$, para el abierto V existe $\lambda_1 \in I$ tal que si $\lambda \geq \lambda_1$ entonces $x_\lambda \in V$. Como el conjunto I es un conjunto dirigido, podemos escoger un $\mu \in I$ tal que $\lambda_0, \lambda_1 \leq \mu$. De esta manera, si $\lambda \geq \mu$ entonces $x_\lambda \in U$ así como $x_\lambda \in V$, lo cual es una contradicción puesto que $U \cap V = \varnothing$. Por lo tanto $x_0 = x_1$. □

Definición 1.5.22. *Sean (X, τ) un espacio topológico y $E \subset X$. La frontera de E es el conjunto*

$$Fr(E) = \overline{E} \cap \overline{(X \setminus E)}.$$

Proposición 1.5.23. *Sean (X, τ) un espacio topológico y $E \subset X$. Entonces, $x \in Fr(E)$ si y sólo si para cualquier abierto U, que contiene a x, se cumple que $U \cap E \neq \varnothing$ y $U \cap (X \setminus E) \neq \varnothing$.*

Proposición 1.5.24. *Sean (X, τ) un espacio topológico y $U \in \tau$. Entonces U es abierto y cerrado si y sólo si, $Fr(U) = \varnothing$.*

A continuación, daremos la definición de dimensión topológica, la cual está definida de manera inductiva. Usaremos la abreviación $dim(X)$ para denotar la dimensión del espacio X; así como $dim_p(X)$ denotará la dimensión del espacio X en un punto p. Para más información, véase [8].

Definición 1.5.25. *(Dimensión Topológica) Sea (X, τ) un espacio topológico de Hausdorff.*

1. *La $dim(X) = -1$ si y sólo si $X = \varnothing$. Además, se entiende que $dim(X) \leq -1$ si $X = \varnothing$.*

2. *Supongamos que hemos definido de manera inductiva lo que significa que* $dim(Y) \leq n-1$*, para cualquier espacio topológico* Y*, y* $n \geq 0$*. Entonces, para cualquier espacio* X *y* $p \in X$*, definimos*

$$dim_p(X) \leq n$$

   si y sólo si p *tiene un sistema de vecindades abiertas en* X *cuyas fronteras tienen* $dim \leq n-1$*.*

3. $dim(X) \leq n$ *si y sólo si* $dim_p(X) \leq n$*, para todo* $p \in X$*.*

4. $dim(X) = n$ *si y sólo si* $dim(X) \leq n$ *y* $dim(X) \nleq n-1$*.*

5. $dim_p(X) = n$ *si y sólo si* $dim_p(X) \leq n$ *y* $dim_p(X) \nleq n-1$

Capítulo 2

Grupos abelianos

2.1. Grupos cíclicos

Definición 2.1.1. *Sea A un grupo. Un subconjunto B de A es un subgrupo si los elementos de B forman un grupo al restringir la operación del grupo A al subconjunto B.*

Lema 2.1.2. *Sea B un subconjunto no vacío de un grupo A. Las siguientes condiciones son equivalentes:*

(a) *B es un subgrupo de A.*

(b) $\forall a, b \in B$, $a + b \in B$ *y* $-a \in B$.

(c) $\forall a, b \in B$, $a - b \in B$.

Demostración. $(a) \Longrightarrow (b)$ Si B es un subgrupo de A entonces la operación $+\,|_B \colon B \times B \longrightarrow B$ es cerrada, por lo que para cualquier $a, b \in B$, $a + b \in B$. Además, al ser B un subgrupo, para cualquier $a \in B$ se tiene que $-a \in B$.

$(b) \Longrightarrow (a)$ Observemos que al ser A un grupo, la operación suma es asociativa en todo A, por lo que también es asociativa en B. Basta demostrar que el elemento neutro está en B. Si $a \in B$, por (b) se tiene que $-a \in B$, teniendo así que $0 = a + (-a) \in B$.

$(b) \Longrightarrow (c)$ Si $a, b \in B$, entonces $-b \in B$, por lo que $a + (-b) = a - b \in B$.

$(c) \Longrightarrow (b)$ Si $a, b \in B$, entonces $a - a = 0 \in B$, de donde se sigue que $-a = 0 - a \in B$. Como $-(-b) = b$, entonces $a + b = a - (-b) \in B$. $\square$

Dado cualquier elemento a del grupo A, se tiene el morfismo de grupos $\varphi : \mathbb{Z} \longrightarrow < a >$ definido por $k \longmapsto ka$. Por como está definido $< a >$, φ es sobre y además, φ es inyectiva si y sólo $na \neq ma$ siempre que $n \neq m$, con lo cual $o(a) = \infty$. Por otro lado, si φ no es inyectiva, entonces $o(a)$ es finito; más aún, $o(a)$ es el menor entero positivo n tal que $na = 0$. En efecto, si k_1 y k_2, con $k_1 > k_2$, son tales que $k_1 a = k_2 a$, entonces $(k_1 - k_2)a = 0$ donde $k_1 - k_2 > 0$. Por el Principio del Buen Orden, el conjunto

$$\{n \in \mathbb{Z}^+ \mid na = 0\}$$

tiene un elemento menor. Si n es tal elemento, afirmamos que

$$< a >= \{0,\ a,\ 2a,\ (n-1)a\}.$$

Como n es el menor entero positivo tal que $na = 0$, los elementos

$$\{a, 2a, \ldots, (n-1)a\}$$

son todos distintos a 0. Más aún, estos son distintos entre sí, ya que si $ra = sa$ con $0 < r < s < n$ entonces $0 < s - r < n$ y es tal que $(s - r)a = 0$, lo cual contradice que n sea mínimo con dicha propiedad. Por lo tanto,

$$< a >= \{0,\ a,\ 2a,\ (n-1)a\}.$$

Esto último implica que $|< a >| = n$.

También es cierto que, si $o(a) = n$ entonces n es el menor entero positivo tal que $na = 0$. En efecto, como los elementos $\{0,\ a,\ 2a,\ (n-1)a\} =< a >$ son distintos entre si y $na \in < a >$, se tiene que $na = sa$, para alguna $s \in \{0, \ldots, n-1\}$. Si $s \neq 0$, como $n > s$ y $0 < n - s < n$ se cumple que $(n - s)a = 0$, lo cual quiere decir que los elementos 0 y $(n - s)a$ son iguales. Esto contradice que el conjunto $< a >$ tenga n elementos distintos. Por lo tanto $s = 0$ y así n es el menor entero positivo tal que $na = 0$.

Nótese también que esto último implica que φ no es inyectiva. Además, bajo las mismas hipótesis, si k es un natural que cumple que $ka = 0$, entonces $n \mid k$ ya que por el algoritmo de la división de Euclides, $k = qn + r$ con $0 \leq r < n$, con lo cual se obtiene que

$$0 = ka = q(na) + ra = ra.$$

Por la minimalidad de n, se sigue que $r = 0$, por lo que $n \mid k$.

Teorema 2.1.3. *Subgrupos de grupos cíclicos son también grupos cíclicos.*

Demostración. Sean $< a >$ un grupo cíclico y B un subgrupo de $< a >$ no trivial. Por ser B un subgrupo de $< a >$, B tiene un elemento de la forma ka, para algún $k \in \mathbb{N}$, con $k > 0$. Por el Principio del Buen Orden, existe un elemento $s \in \mathbb{N}$ con la propiedad de ser el menor natural para el cual $sa \in B$. Obsérvese que $s \neq 0$. Afirmamos que $B =< sa >$. Como $sa \in B$, basta demostrar que $B \subset< sa >$. Si $b \in B \subset< a >$ entonces $b = ta$. Por la elección de s, se tiene que $s \leq t$. Usando el algoritmo de Euclides, se sigue que $t = sq + r$, con $0 \leq r < s$. Notemos que $r = 0$, ya que de lo contrario, se tendría que

$$ra = (t - qs)a = ta - q(sa) \in B,$$

contradiciendo la elección de s. Esto muestra que $B =< sa >$, por lo que B es cíclico. Notemos que por el Teorema de Lagrange, $\mid B \mid=\mid< sa >\mid$ es un divisor de $\mid< a >\mid= n$. □

Proposición 2.1.4. *Sea A un grupo finito. Para cualquier $a \in A$, se tiene que $\mid A \mid a = 0$.*

Demostración. Si $\mid A \mid$ es finito, por el teorema de Lagrange,

$$\mid A \mid=\mid< a >\mid [< a >: A].$$

Como $\mid< a >\mid a = 0$ se tiene que

$$\begin{aligned} \mid A \mid a &= ([< a >: A]\cdot \mid< a >\mid)a \\ &= [< a >: A](\mid< a >\mid a) = [< a >: A]0 = 0. \end{aligned}$$

□

El siguiente resultado caracteriza a los grupos cíclicos:

Teorema 2.1.5. *Un grupo finito A de orden n es cíclico si y sólo si para cada divisor d de n, existe a lo más un único subgrupo cíclico de orden d.*

Demostración. $\Longrightarrow$) Supongamos que $A =< a >$, con $o(a) = n$. Si $d \mid n$ entonces existe $k \in \mathbb{N}$ tal que $dk = n$. Notemos que el elemento ka tiene orden d. En efecto, por una parte, $d(ka) = (dk)a = na = 0$, por lo que $o(ka) \mid d$. Por otra parte, si $s = ord(ka)$, como $o(a) = n$ y $(sk)a = s(ka) = 0$ se tiene que $n \mid sk$, por lo que existe $r \in \mathbb{N}$ tal que $nr = sk$. Como por hipótesis $n = dk$, entonces $(dk)r = sk$, lo cual es equivalente a la igualdad $drk = sk$. Como los naturales distintos de 0 tienen la propiedad de ser cancelables en una igualdad, se sigue que $dr = s$, es decir, $d \mid s$, teniendo así que $d = s = ord(ka)$.

Notemos ahora que si B es un subgrupo de orden d de A, éste tiene que ser cíclico ya que A lo es, por lo que $B =< b >$ con $db = 0$. Además, como $b = ma$ para algún $m \in \{1, \ldots, n\}$, se tiene que

$$0 = db = dma$$

lo cual implica que $n \mid dm$, por lo que $nl = dm$ para algún $l \in \mathbb{N}$. Ahora, como $d \mid n$, entonces n/d es un número natural, con lo cual la igualdad $m = l(n/d)$ tiene sentido. Al tomar el subgrupo generado por $< (n/d)a >$ se cumple que

$$b = ma = l(n/d)a \in < (n/d)a >$$

por lo que $B =< b > \subset < (n/d)a >$. Más aún, como $d(n/d)a = na = 0$ entonces $o((n/d)a) \mid d$. Ahora, si $s = o((n/d)a)$ entonces $s(n/d)a = 0$ por lo que $n \mid s(n/d)$, con lo cual, $nr = s(n/d)$ para algún $r \in \mathbb{N}$. De esto último se sigue que $drn = sn$, por lo que cancelando n en ambos lados de la igualdad, se obtiene $dr = s$, es decir, $d \mid s = ord((n/d)a)$. Por lo tanto, $d = s$ y así $B =< (n/d)a >$, pues ambos subgrupos tienen el mismo orden y el primero está contenido en el otro.

$\Longleftarrow$) Sea G un grupo finito de orden n. Si I es el conjunto formado por los subgrupos cíclicos de G, entonces $G = \dot{\cup}_{C \in I} gen(C)$, es decir, G es la unión ajena de los generadores de todos los subgrupos cíclicos de G. Ahora, si G es un grupo de orden n, entonces el orden de cualquier subgrupo de G divide a n. Por el Teorema 1.1.16, enunciado en la sección de los preliminares, y que, para cada divisor d de n existe un único subgrupo cíclico C_d de orden d, se sigue que

$$n =\mid G \mid = \Sigma_{C \in I} \mid gen(C) \mid \leq \Sigma_{d|n} \mid gen(C_d) \mid = \Sigma_{d|n} \varphi(d) = n.$$

Así, G contiene un subgrupo cíclico de orden d para cada divisor d de n. En particular, G contiene un subgrupo cíclico de orden $d = n$. Por lo tanto G es cíclico. □

Proposición 2.1.6. *Sean A un grupo y $a \in A$ de orden finito. Entonces, para cada $n \in \mathbb{N}$,*

$$o(na) = o(a)/(n; o(a))$$

donde $(n; o(a))$ es el máximo común divisor entre n y $o(a)$.

Demostración. Recordemos que si $l, m, n \in \mathbb{N}$ son tales que $l \mid mn$ y $(l; m) = 1$ entonces $l \mid n$. Sea $a \in A$ y $n \in \mathbb{N}$. Veamos primero que $o(a)/(n; o(a)) \mid o(na)$. Para esto, notemos que

$$\tfrac{o(a)}{(n;o(a))}(na) = \tfrac{no(a)}{(n;o(a))}a = \tfrac{n}{(n;o(a))}o(a)a = \tfrac{n}{(n;o(a))}0 = 0$$

por lo que $o(na) \mid \frac{o(a)}{(n;o(a))}$. Por otra parte, si $s = o(na)$ entonces $0 = s(na) = (sn)a$, por lo que $o(a) \mid sn$. Como $(n; o(a)) \mid n$ y $(n; o(a)) \mid o(a)$ se tiene que $\frac{o(a)}{(n;o(a))} \mid s\frac{n}{(n;o(a))}$, y como $(\frac{o(a)}{(n;o(a))}, \frac{n}{(n;o(a))}) = 1$, podemos concluir que $\frac{o(a)}{(n;o(a))} \mid s = o(na)$. Por lo tanto, $o(na) = o(a)/(n; o(a))$. □

Teorema 2.1.7. *El conjunto T de todos los elementos de orden finito en un grupo A es un subgrupo. Así, T es un grupo de torsión y el grupo cociente abeliano A/T es libre de torsión.*

Demostración. Como $0 \in T$, T es no vacío. Ahora, si $a, b \in T$ entonces existen $n, m \in \mathbb{N}$ tales que $na = 0 = mb$. Así,

$$nm(a - b) = m(na) - n(mb) = 0$$

por lo que $a - b \in T$. Por el Lema 2.1.2, T es un subgrupo de A. Sea $a + T$ un elemento de A/T tal que $m(a + T) \subset T$ para algún $m \in \mathbb{N}$. Esto quiere decir que $ma \in T$, por lo que existe $n \in \mathbb{N}$ tal que $n(ma) = 0$. Así, $(nm)a = 0$ lo cual muestra que a es un elemento de orden finito. Por lo tanto $a \in T$, lo cual implica que $a + T = T$. Esto muestra que A/T no tiene elementos de orden finito salvo el elemento neutro $0 + T = T$. □

El subgrupo T es el mayor subgrupo de torsión de A; se llama la parte de torsión de A. Notemos que si $B \subset A$ es un subgrupo de torsión, entonces $B \leq T$, así como si $C \leq A$ es tal que A/C es libre de torsión, entones $T \leq C$.

Definición 2.1.8. *Dado n un entero positivo, definimos los conjuntos*

$$nA = \{na \mid a \in A\} \text{ y } A[n] = \{a \mid a \in A,\, na = 0\}.$$

Observación. *$g \in nA$ si y solo si la ecuación $g = nx$ tiene solución en A, así como $g \in A[n]$ si y sólo si $o(g) \mid n$.*

Observación. *Los conjuntos nA y como $A[n]$ son subgrupos de A.*

Definición 2.1.9. *Sea $a \in A$ un elemento y p un primo. El mayor entero no negativo r, para el cual la ecuación $p^r x = a$ tiene solución en A, se le llama la p-altura de a y la denotamos por $h_p(a)$. Si $p^r x = a$ tiene solución para cualquier $r \in \mathbb{N}$, decimos que a tiene p-altura infinita y lo escribimos por $h_p(a) = \infty$.*

Observación. *La ecuación $p^r x = a$ siempre tiene solución, ya que*

$$p^0 a = 1a = a.$$

Dado un grupo A, el conjunto $L(A)$ de todos los subgrupos de A es una retícula ya que, para cualquier par de subgrupos B y C de A , $B \cap C$ y $B + C$ son las operaciones para el ínfimo y supremo, respectivamente. Esta retícula también es completa y tiene como máximo al grupo A y como mínimo al subgrupo trivial $\{0\}$, y satisface:

Proposición 2.1.10. *(Ley modular) Si B, C, D son subgrupos de A tales que $B \leq D$ entonces*

$$B + (C \cap D) = (B + C) \cap D.$$

Demostración. Como $B \leq D$, basta demostrar que

$$(B + C) \cap D \subset B + (C \cap D).$$

Si $d \in (B + C) \cap D$ entonces $d = b + c$ donde $b \in B$ y $c \in C$. Así, $d - b = c$ y como $B \leq D$ se tiene que $c = d - b \in D$, por lo que $c \in D \cap C$. Esto implica que $d = b + c \in B + (D \cap C)$. □

2.2. Grupos cocíclicos

Proposición 2.2.1. *Un grupo A es cíclico si y sólo si existe un elemento $a \in A$ tal que, para cualquier morfismo de grupos $\varphi : B \longrightarrow A$, si $a \in Im(\varphi)$ entonces φ es suprayectiva.*

Demostración. $\Longrightarrow$) Supongamos que $A =< a >$ es un grupo cíclico. Sean B un grupo y $\varphi : B \longrightarrow< a >$ un morfismo tal que $a \in Im(\varphi)$. Como $a \in Im(\varphi)$, existe $b \in B$ tal que $\varphi(b) = a$. Ahora, si $c \in< a >$, entonces c es de la forma na, para algún $n \in \mathbb{N}$. Así, el elemento $nb \in B$ cumple que $\varphi(nb) = n\varphi(b) = na$, lo cual muestra que φ es suprayectiva.

$\Longleftarrow$) Sean A un grupo y $a \in A$ tal que, para para cualquier morfismo $\varphi : B \longrightarrow A$, si $a \in Im(\varphi)$, entonces φ es suprayectiva. Consideremos el grupo $B =< a >$ y el morfismo $\varphi :< a >\longrightarrow A$ definido por $a \longmapsto a$. Como $a \in Im(\varphi)$, φ es suprayectiva. Esto quiere decir que cualquier elemento de A es de la forma na, para algún $n \in \mathbb{N}$, con lo cual $A \subset< a >$. Como $< a >\subset A$, se sigue que $A =< a >$. $\square$

Dualizando esta idea, decimos que un grupo C es *cocíclico* si existe un elemento $c \in C$ tal que, para cualquier morfismo $\varphi : C \longrightarrow B$, si $c \notin Ker(\varphi)$, entonces φ es inyectiva. En este caso, llamamos al elemento c un cogenerador de C.

Ejemplo. *Todo grupo cíclico $< a >$ de orden p^k, con p un primo, es un grupo cocíclico. Más aún, todo elemento de orden p es un cogenerador. En efecto, los únicos divisores positivos de p^k, son de la forma p^s, con $1 \leq s \leq k$. Por el Teorema 2.1.5, para cada $s \in \{1, \ldots, k\}$ existe un único subgrupo de $< a >$, de orden p^s. En particular, $< p^{k-1}a >$ es un subgrupo de orden p, por lo que éste es el único subgrupo de $< a >$ de orden p. Ahora, si B es un subgrupo no trivial de $< a >$, entonces B es cíclico, por lo que también contiene un único subgrupo de orden d, por cada divisor d del orden de B. Como los subgrupos de B, son subgrupos de $< a >$, se sigue que $< p^{k-1}a >$ está contenido en cualquier subgrupo B no trivial de $< a >$. Así, si $\varphi :< a >\longrightarrow C$ es un morfismo tal que $p^{k-1}a \notin ker\varphi$, entonces $ker(\varphi) = \{0\}$, ya que $ker(\varphi)$ es un subgrupo de $< a >$ y $p^{k-1}a \notin ker(\varphi)$. Por lo tanto, $< a >$ es un grupo cocíclico. La segunda afirmación se sigue notando que cualquier elemento en $< p^{k-1}a >$, distinto de 0, es un generador.*

Como en cualquier grupo abeliano todo subgrupo es normal, si C es un grupo abeliano cocíclico y $D \leq C$, se tiene el morfismo canónico $C \longrightarrow C/D$, cuyo kernel es el subgrupo D. Esto quiere decir que todo subgrupo de C es el kernel de algún morfismo de grupos. Como estas proyecciones no son inyectivas, salvo el caso trivial $D \cong \{0\}$, el cogenerador c de C debe estar en todos los subgrupos no triviales de C. Por lo tanto, la intersección de todos los subgrupos no triviales de un grupo abeliano cocíclico C es no trivial. Más aún, el subgrupo generado por el elemento cogenerador c es el menor subgrupo no trivial de C; cualquier elemento distinto del 0 en el subgrupo $< c >$, es también un cogenerador, por lo que $< c >$ es de orden primo.

Recíprocamente, si C es un grupo abeliano que contiene un único subgrupo menor no trivial M, entonces C es cocíclico. En efecto, notemos primero que $M =< c >$ para cualquier $c \in M$, ya que la contención $< c >\subset M$ es válida para cualquier $c \in M \setminus \{0\}$ y la condición de ser menor implica que $M =< c >$. De esta manera, si $\varphi : C \longrightarrow B$ es cualquier morfismo de grupos con $c \notin Ker(\varphi)$, como $Ker(\varphi) \leq C$ y $< c >= M$ es el menor subgrupo no trivial de C, se tiene que $Ker(\varphi) = \{0\}$, por lo que φ es inyectiva.

Observación. *Existen grupos cocíclicos no abelianos. Si G es un grupo que tiene un único subgrupo normal no trivial, entonces es G es un grupo cocíclico. Más aún, si $K \lhd G$ es el único subgrupo normal no trivial de G, entonces cualquier elemento $k \in K$ es un cogenerador. En efecto, sean $k \in K$ y $\varphi : G \longrightarrow B$ un morfismo para el cual $k \notin ker(\varphi)$. Como $ker(\varphi) \lhd G$ y $k \notin ker(\varphi)$, se sigue que $ker(\varphi) = \{0\}$.*

Ejemplo. *El grupo S_3 no es abeliano, ya que*

$$(12)(13) = (132) \neq (123) = (13)(12).$$

Más aún, S_3 tiene un único subgrupo normal, a saber, $< (123) >=< (132) >$. Así, los elementos (123) y (132) son cogeneradores del grupo cocíclico S_3.

Definición 2.2.2. *El grupo aditivo de los racionales $(\mathbb{Q}, +)$ es un grupo abeliano y lo denotamos por $\mathbb{Q}$.*

Consideremos ahora al grupo cociente $\mathbb{Q}/\mathbb{Z}$. Notemos que los elementos de $\mathbb{Q}/\mathbb{Z}$ son de la forma $[\overline{\frac{n}{m}}] = \frac{n}{m} + \mathbb{Z}$ donde $\frac{n}{m} \in \mathbb{Q}$. Sin pérdida de generalidad, podemos suponer que $(n, m) = 1$ y tomar, para el elemento $[\overline{\frac{n}{m}}]$, el representante $\frac{n}{m}$. Con esto en cuenta,

$$[\overline{\tfrac{n}{m}}] \in (\mathbb{Q}/\mathbb{Z})_p \text{ si y sólo si } p^k[\overline{\tfrac{n}{m}}] \in \mathbb{Z} \text{ para algún } k \in \mathbb{N},$$

con lo cual $\frac{p^k n}{m} \in \mathbb{Z}$, es decir, $m \mid p^k$. Por lo tanto, $m = p^l$ para algún $l \in \mathbb{N}$, mostrando así que el conjunto $\{[\frac{1}{p}], [\frac{1}{p^2}], \dots, [\frac{1}{p^n}], \dots\}$ es un conjunto generador de $(\mathbb{Q}/\mathbb{Z})_p$.

Proposición 2.2.3. *Sea p un primo. Si $m \geq 1$, existen $n, a_0, a_1, \dots, a_n \in \mathbb{N}$ únicos tales que $0 \leq a_i < p$, $0 \leq n$, $a_n \neq 0$ y*

$$m = a_n p^n + a_{n-1}p^{n-1} + \cdots + a_1 p + a_0 p^0.$$

Demostración. Procederemos por inducción. Si $m = 1$, se sigue que

$$m = 1 + 0p + \cdots + 0p^n$$

donde $n = 0$ y $a_n = a_0 = 1$. Nótese que esta expresión es única ya que cada sumando es positivo. Supongamos que es válida la hipótesis de inducción para cualquier natural $s < m$. Por el algoritmo de la división, existen q y r únicos en $\mathbb{Z}$, tales que $m = qp + r$, donde $0 \leq r < p$. Obsérvese que $q < m$. En efecto, si $\mid q \mid \geq m$, se cumple que $q \geq m$ ó $-q \geq m$. Si $q \geq m$, entonces $pq > m$, con lo cual $pq + r > m$, contradiciendo la igualdad $m = qp + r$. Ahora, si $-q \geq m$, se tiene que $-m = -qp - r$. Como $0 \leq r < p$ y $-qp > p$, entonces $-m = -qp - r > 0$, llegando de nuevo a una contradicción.

Así, por hipótesis de inducción, se sigue que $q = \Sigma_{i=0}^{k} a_i p^i$, por lo que $m = (\Sigma_{i=0}^{k} a_i p^i)p + r$, es decir,

$$m = r + pa_0 + p^2 a_1 + \cdots + p^{k+1} a_k$$

donde $r, a_i \in \{0, \ldots, p-1\}$.

Unicidad. Supongamos que $m = a_0 + a_1 p + \cdots + a_n p^n$ y $m = b_0 + b_1 p + \cdots + b_k p^k$, con $0 \leq a_i < p$ y $0 \leq b_j < p$. Al igualar ambas expresiones, obtenemos

$$b_0 - a_0 = (\Sigma_{i=1}^{n} a_i p^i) - (\Sigma_{j=1}^{k} b_j p^j) = p(\Sigma_{i=1}^{n} a_i p^{i-1} - \Sigma_{j=1}^{k} b_j p^{j-1})$$

es decir, $p \mid b_0 - a_0$. Como tanto a_0 como b_0 son menores que p, se sigue que $b_0 = a_0$. Así,

$$a_1 p + a_2 p^2 + \cdots + a_n p^n = b_1 p + b_2 p^2 + \cdots + b_k p^k < m.$$

Por hipótesis de inducción, se sigue que $n = k$ y que $a_i = b_i$. Por lo tanto, ambas expresiones son iguales. $\square$

Definición 2.2.4. *$\mathbb{Z}(p^\infty)$ es la parte de p-torsión de $\mathbb{Q}/\mathbb{Z}$, es decir,*

$$\mathbb{Z}(p^\infty) = (\mathbb{Q}/\mathbb{Z})_p.$$

Teorema 2.2.5. *Todo elemento no nulo en $\mathbb{Z}(p^\infty)$ se expresa de manera única de la forma $[\frac{a_1}{p} + \frac{a_2}{p^2} + \cdots + \frac{a_n}{p^n}]$ para alguna $n \in \mathbb{N}$ y donde $a_i \in \{0, \ldots p-1\}$, $\forall i \in \{1, \ldots, n\}$.*

Demostración. Un elemento en $\mathbb{Z}(p^\infty)$ es de la forma $\frac{n}{p^k}$, para algún $k \in \mathbb{N}$. Ahora, por la Proposición 2.2.3, $n = a_0 + a_1 p + \cdots + a_s p^s$, donde $0 \leq a_i < p$. Así,

$$\frac{n}{p^k} = \frac{a_0 + a_1 p + \cdots + a_s p^s}{p^k} = \frac{a_0}{p^k} + \frac{a_0}{p^{k-1}} + \cdots + \frac{a_s}{p^{k-s}}.$$

Obsérvese que si $s \geq k$, los términos $\frac{a_k}{p^{k-s}}, \frac{a_{k+1}}{p^{(k+1)-s}}, \cdots, \frac{a_s}{p^{s-s}}$ son todos enteros, por lo que están en la clase del cero en $(\mathbb{Q}/\mathbb{Z})_p$. $\square$

2.3. Grupos cuasicíclicos

Ejemplo. *Sean p un primo y $n \in \mathbb{N}$. Si H_{p^k} es el conjunto de raíces complejas del polinomio $x^{p^k} - 1$, entonces*

$$H_p \leq H_{p^2} \leq \cdots \leq H_{p^n} \leq \cdots.$$

Si $H = \cup_{i=1}^{\infty} H_{p^i}$, entonces H es un subgrupo de $\mathbb{C} \setminus \{0\}$. Más aún, H es un grupo abeliano, no cíclico, con todos sus subgrupos cíclicos finitos.

Observación. *Los grupos $H = \cup_{i=1}^{\infty} H_{p^i}$ y $\mathbb{Z}(p^\infty)$ son isomorfos. En efecto, si c_i es el generador del grupo ciclico H_{p^i}, de orden p^i, definimos la función $\varphi : \mathbb{Z}(p^\infty) \longrightarrow H$ con regla de correspondencia*

$$\tfrac{a_1}{p} + \tfrac{a_2}{p^2} + \cdots + \tfrac{a_n}{p^n} \longmapsto c_1^{a_1} c_2^{a_2} \cdots c_n^{a_n}.$$

Nótese que la unicidad en la expresión de cada elemento de $\mathbb{Z}(p^\infty)$, hace que φ esté bien definida.

Sean $a = a_1 p + a_2 p^2 + \cdots + a_s p^s$ y $b = b_1 p + b_2 p^2 + \cdots + b_r p^r$ dos elementos en $\mathbb{Z}(p^\infty)$. Sin pérdida de generalidad, supongamos que $s < r$, con lo cual

$$\begin{aligned} a + b &= (a_1 p + a_2 p^2 + \cdots + a_s p^s) + (b_1 p + b_2 p^2 + \cdots + b_r p^r) \\ &= (a_1 + b_1)p + (a_2 + b_2)p^2 + \cdots + (a_s + b_s)p^s + b_{s+1}p^{s+1} + \cdots + b_r p^r, \end{aligned}$$

donde cada término $a_i + b_i$ es módulo p. Con esto en cuenta, se sigue que

$$\begin{aligned} \varphi(a+b) &= c_1^{(a_1+b_1)} \cdot c_2^{(a_2+b_2)} \cdots c_s^{(a_s+b_s)} \cdot c_{s+1}^{b_{s+1}} \cdots c_r^{b_r} \\ &= (c_1^{a_1} \cdot c_1^{b_1}) \cdot (c_2^{a_2} \cdot c_2^{b_2}) \cdots (c_s^{a_s} \cdot c_s^{b_s}) \cdot c_{s+1}^{b_{s+1}} \cdots c_r^{b_r} \\ &= (c_1^{a_1} \cdot c_2^{a_2} \cdots c_s^{a_s}) \cdot (c_1^{b_1} \cdot c_2^{b_2} \cdots c_s^{b_s} \cdots c_r^{b_r}) = \varphi(a) \cdot \varphi(b), \end{aligned}$$

mostrando así que φ es un morfismo.

Por otra parte, si $x \in H = \cup_{i=1}^{\infty} H_{p^i}$, entonces $x \in H_{p^n}$, para alguna $n \in \mathbb{N}$. Esto quiere decir que $x = (c_n)^k$, con $1 \leq k \leq p^n - 1$. Ahora, por la Proposición 2.2.3, $k = a_1 p + a_2 p^2 + \cdots + a_s p^s$. Obsérvese que $s < n$, ya que, en caso contrario, si $s \geq n$, entonces $a_s p^s \geq p^n > p^n - 1$, con lo cual, se llega a la contradicción $k > p^n - 1$. Así, se tiene que

$$\begin{aligned} (c_n)^k &= c_n^{(a_1 p + a_2 p^2 + \cdots + a_s p^s)} \\ &= c_n^{(a_1 p)} \cdot c_n^{(a_2 p^2)} \cdot \cdots \cdot c_n^{(a_s p^s)} \\ &= c_{n-1}^{a_1} \cdot c_{n-2}^{a_2} \cdot \cdots \cdot c_{n-s}^{a_s}. \end{aligned}$$

Por lo tanto, el elemento $y = \frac{a_s}{p^{n-s}} + \frac{a_{s-1}}{p^{n-(s-1)}} + \cdots + \frac{a_2}{p^{n-2}} + \frac{a_1}{p^{n-1}} \in \mathbb{Z}(p^\infty)$ *es tal que* $\varphi(y) = x$*, con lo cual* φ *es una función suprayectiva.*

Por otro lado, si $x \in H = \cup_{i=1}^{\infty} H_{p^i}$*, entonces* $x = (c_n)^k$*, para alguna* $n \in \mathbb{N}$*, y* $1 \leq k \leq p^n - 1$*. Así, si* $k = a_1 p + a_2 p^2 + \cdots + a_s p^s$ *entonces* $(c_n)^k = c_{n-1}^{a_1} \cdot c_{n-2}^{a_2} \cdot \cdots \cdot c_{n-s}^{a_s}$*. Con esto en cuenta, la función* $\psi : H \longrightarrow \mathbb{Z}(p^\infty)$*, con regla de correspondencia*

$$(c_n)^k = c_{n-1}^{a_1} \cdot c_{n-2}^{a_2} \cdot \cdots \cdot c_{n-s}^{a_s} \longmapsto \frac{a_s}{p^{n-s}} + \frac{a_{s-1}}{p^{n-(s-1)}} + \cdots + \frac{a_2}{p^{n-2}} + \frac{a_1}{p^{n-1}},$$

satisface $\psi \circ \varphi = id_{\mathbb{Z}(p^\infty)}$*, por lo que* φ *es una función inyectiva. Por lo tanto* $\varphi : \mathbb{Z}(p^\infty) \longrightarrow H$ *es un isomorfismo.*

Definición 2.3.1. *Llamamos a un grupo cuasicíclico o de tipo* p^∞ *si tiene un conjunto generador* $\{c_1, c_2 \ldots, c_n, \ldots,\}$ *tal que*

$$pc_1 = 0,\ pc_2 = c_1, \cdots, pc_n = c_{n-1},\ pc_{n+1} = c_n, \cdots.$$

Observación. $\mathbb{Z}(p^\infty)$ *es un grupo cuasicíclico.*

De la definición anterior, se sigue que para cada c_n, $o(c_n) = p^n$. Si denotamos ahora a los generadores de $\mathbb{Z}(p^\infty)$ por el conjunto

$$\{c_1, c_2 \ldots, c_n, \ldots,\}$$

se tiene que cualquier suma entre dos elementos generadores de $\mathbb{Z}(p^\infty)$, es un múltiplo de algún c_n. En efecto, si sc_m y rc_k son dos elementos de $\mathbb{Z}(p^\infty)$ con $m < k$, como

$$pc_k = c_{k-1},\ pc_{k-1} = c_{k-2}, \ldots,\ pc_{k-(k-m+1)} = pc_{m+1} = c_m$$

se tiene que $p^{(k-m)} c_k = c_m$, por lo que

$$sc_m + rc_k = sp^{(k-m)} c_k + rc_k = (sp^{(k-m)} + r)c_k \in < c_k > .$$

Esto implica que toda suma de elementos de $\mathbb{Z}(p^\infty)$ se encuentra en el subgrupo generado por algún c_n.

Lema 2.3.2. *Los subgrupos de* $\mathbb{Z}(p^\infty)$ *forman una cadena de subgrupos.*

Veamos ahora que $\mathbb{Z}(p^\infty)$ es un grupo cocíclico. Si B es un subgrupo propio de $\mathbb{Z}(p^\infty)$, por el Principio del buen Orden, el conjunto

$$\{i \in \mathbb{N} \mid c_i \text{ es un generador de } \mathbb{Z}(p^\infty) \text{ y } c_i \notin B\}$$

tiene un elemento menor, es decir, existe un generador $c_{n+1} \in \mathbb{Z}(p^\infty)$ tal que $c_{n+1} \notin B$ y cumple ser el de menor índice posible. Afirmamos que $B =< c_n >$. Notemos primero que, por la propiedad de c_{n+1}, se tiene que $c_n \in B$, por lo que $< c_n >\subset B$. Ahora, por lo observado anteriormente, todo elemento $b \in B$ se puede escribir en la forma $b = kc_m$ para alguna k y m enteros positivos con k primo relativo con p. Así, como $(k,p) = 1$ entonces $(k,p^m) = 1$ por lo que existen enteros positivos r y s tales que $rk + sp^m = 1$, lo cual implica que $c_m = rkc_m + sp^m c_m = rkc_m = rb \in B$. Esto a su vez implica que $m \leq n$ ya que de lo contrario, si $n < m$ entonces $n < n+1 \leq m$, por lo que

$$< c_n >\subset< c_{n+1} >\subset< c_m >\subset B$$

lo cual contradice que $c_{n+1} \notin B$. De esta manera, $m \leq n$ por lo que $< c_m >\subseteq< c_n >$. Como

$$b = kc_m \in< c_m >\subset< c_n >$$

se tiene que $B \subset< c_n >$, teniendo así que $B =< c_n >$.

Esto demuestra que todos los subgrupos propios de $\mathbb{Z}(p^\infty)$ son grupos cíclicos finitos de orden p^n con $n \in \mathbb{N}$, los cuales forman una cadena con respecto a la inclusión:

$$0 \subseteq< c_1 >\subseteq \cdots \subseteq< c_n >\subseteq \cdots$$

Lo anterior implica que $< c_1 >\cong \mathbb{Z}(p)$ es el menor subgrupo de $\mathbb{Z}(p^\infty)$, por lo que $\mathbb{Z}(p^\infty)$ es cocíclico.

Teorema 2.3.3. *Un grupo abeliano C es cocíclico si y sólo si $C \cong \mathbb{Z}(p^k)$ con $k \in \mathbb{N}$ ó $k = \infty$.*

Demostración. Por lo visto anteriormente, si $c \in C$ es un cogenerador de C, entonces $< c >$ es el menor subgrupo no trivial de C, por lo que c debe de ser de orden primo. Veamos que C es en realidad un p-grupo. Observemos primero que todo elemento de C tiene orden finito. Si $b \in C$ y $b \neq 0$, al ser $< c >$ el menor subgrupo no trivial de C y $< b >\neq 0$, se tiene que $< c >\leq< b >$, por lo que $c = kb$, para alguna $k \in \mathbb{N}$. Como c tiene orden p, entonces

$$0 = pc = p(kb) = (pk)b,$$

es decir, b es de orden finito. Más aún, el orden de cualquier elemento en C es una potencia del primo p. En efecto, si q es otro primo distinto a p, que divide al orden del elemento $b \in C$, entonces $(qs)b = 0$, para algún $s \in \mathbb{N}$, donde $qs = ord(b)$. Con esto en cuenta, el elemento $(sb) \in C$ tiene orden q. Por la propiedad de c, se tiene que $< c > \leq < sb >$, y por el teorema de Lagrange se sigue que $p \mid q$, lo cual es una contradicción. Por lo tanto, C es un p-grupo, ya que todo elemento tiene orden una potencia de p.

El Teorema de Lagrange nos asegura que todo subgrupo de C es de orden una potencia de p. Usaremos ahora el método de inducción para demostrar que los únicos subgrupos de C son cíclicos y de orden una potencia de p. Para la base de inducción, notemos que $< c >$ es el menor subgrupo de C de orden p, por lo que también es único. Supongamos ahora que la afirmación es válida para m, es decir, C tiene un único subgrupo $C_m =< c_m >$ de orden p^m para cualquier $m < n+1$. Sean A y B subgrupos de C de orden $n+1$ y $a \in A \setminus C_n$, $b \in B \setminus C_n$. Nótese que a y b tienen orden p^{n+1}, pues de lo contrario, tanto $< a >$ como $< b >$ estarían contenidos en $< C_n >$, contradiciendo la elección de a y de b. Como $0 = p^{n+1}a$, entonces $p^n(pa) = 0$, es decir, pa es un elemento de orden p^n, por lo que $pa = rc_n$. Análogamente, como $0 = p^{n+1}b = p^n(pb)$ se tiene que $pb = sc_n$ donde r y s son enteros positivos.

Observemos que $(s, p) = 1 = (r, p)$. Si $r = r'p^k$, con k el mayor exponente posible, entonces

$$pa = (r'p^k)c_n = r'(p^k c_n) = r'(c_{n-k}).$$

Como (r',p)=1 y el orden de c_{n-k} es p^{n-k} entonces

$$p^{n-k+1}a = p^{n-k}(pa) = r'(p^{n-k}c_{n-k}) = 0.$$

Como $o(a) = p^{n+1}$, se tiene que $k = 0$. El razonamiento es análogo para s. Con esto en cuenta, $(r, p) = 1$ y $(s, p) = 1$, por lo que también $(r, p^n) = 1$ y $(s, p^n) = 1$, con lo cual, en $\mathbb{Z}(p^n)$, podemos encontrar enteros positivos r' y s' tales que $rr' \equiv 1 \ (modp^n)$ así como $ss' \equiv 1 \ (modp^n)$. Así, $(r', p^n) = 1 = (s', p^n)$, lo cual a su vez implica que $(r', p) = 1 = (s', p)$.

Veamos que los elementos $a' = r'a$ y $b' = s'b$ cumplen que $< a' >=< a >$ con $pa' = c_n$, así como $< b' >=< b >$ con $pb' = c_n$. Como a' es un múltiplo de a, entonces $< a' > \subseteq < a >$. Ahora, como $a' = r'a$ entonces

$$o(a') = o(r'a) = o(a)/(r', o(a)).$$

Como $(r', p) = 1$ y $o(a) = p^{n+1}$ entonces $(r', p^n) = 1$ por lo que $o(a') = p^{n+1}/1 = p^{n+1}$. Esto implica que $< a' >=< a >$. Para la segunda observación, notemos que, por la elección de r', existe un entero t tal que $rr' + p^n t = 1$, lo cual equivale a la igualdad $rr' = 1 - tp^n$. Como $pa = rc_n$ entonces

$$pa' = p(r'a) = r'(pa) = r'rc_n = 1c_n - tp^n c_n = c_n - t0 = c_n.$$

La afirmación para b y b' es totalmente análoga.

Con esto en cuenta, se tiene que $pa' - pb' = c_n - c_n = 0$, por lo que $p(a' - b') = 0$. Esto quiere decir que $a' - b'$ es un elemento de orden p, y como en particular $< c_1 >\subseteq< c_n >$, tenemos que $a' - b' = qc_n$, para algún número entero q. De esta manera, se sigue que

$$a' = b' + qc_n = b' + qpb' \in< b' >$$

como

$$b' = a' - qc_n = a' - qpa' \in< a' >,$$

lo cual implica que $< a' >=< b' >$. Esto a su vez, implica que $< a >=< b >$.

Ahora, como C contiene un único subgrupo de orden p^n y $\mid B \mid= p^{n+1}$, entonces B tiene un subgrupo de orden p^n, por lo que $C_n \subseteq B$. Así, si $a \in A$ es tal que $a \in C_n$, entonces $a \in B$. Si $a \notin C_n$, entonces $< a >=< b >$ para cualquier $b \in B \setminus C_n$, por lo que $a \in< b >\subseteq B$, es decir, $A \subseteq B$. Con un razonamiento análogo para los elementos $b \in B$, se tiene que $B \subseteq A$, mostrando así que $A = B$. Esto demuestra la unicidad de los subgrupos de orden p^n, para cualquier $n \in \mathbb{N}$. Por otra parte, como $\mid A \mid= p^{n+1}$, existe $a \in A \backslash C_n$ para el cual se cumple que $o(a) = p^{n+1} =\mid A \mid$, lo cual implica que $A =< a >$. Por lo tanto, C es la unión finita o infinita de una cadena ascendente de subgrupos de orden p^n, para cada $n \in \mathbb{N}$. Además, cada subgrupo es isomorfo a $\mathbb{Z}(p^n)$. □

Lo anterior muestra que cualquier par de grupos cuasicíclicos de tipo p^∞, son isomorfos.

Observación. *Como $\mathbb{Z}(p^\infty) \cong H = \cup_{i=1}^{\infty} H_{p^i}$, y los únicos subgrupos propios de $\mathbb{Z}(p^\infty)$ son cíclicos y de orden p^k, con $k \in \mathbb{N}$, entonces el conjunto de subgrupos $\{H_{p^k} \mid k \in \mathbb{N}\}$, son todos los subgrupos de H.*

Definamos a la función $\varphi_1 : H \longrightarrow H$ con regla de correspondencia

$$(c_m)^i \longmapsto (c_m^i)^p = (c_m)^{pi}.$$

Afirmamos que φ_1 *es un morfismo. En efecto, si* $(c_m)^i, (c_k)^j \in H$, *con* $k < m$, *entonces* $\varphi_1((c_m)^i) = (c_m)^{pi}$, *así como* $\varphi_1((c_k)^j) = (c_k)^{pj}$. *Ahora, como* $k < m$, *entonces* $(c_k)^j = (c_m)^{jp^{m-k}}$, *por lo que* $(c_m)^i \cdot (c_k)^j = (c_m)^{i+jp^{m-k}}$. *Así, se sigue que*

$$\begin{gathered}\varphi_1((c_m)^i \cdot (c_k)^j) = \varphi_1((c_m)^{i+jp^{m-k}}) \\ = ((c_m)^{i+jp^{m-k}})^p = (c_m)^{pi+pjp^{m-k}} \\ = (c_m)^{pi} \cdot (c_m)^{pjp^{m-k}} = (c_m)^{pi} \cdot ((c_m)^{jp^{m-k}})^p \\ = (c_m)^{pi} \cdot ((c_k)^j)^p = (c_m)^{pi} \cdot (c_k)^{pj} \\ = \varphi_1((c_m)^i) \cdot \varphi_1((c_k)^j).\end{gathered}$$

Por lo tanto, φ_1 *es un morfismo.*

Por otra parte, notemos que φ_1 *es una función suprayectiva. Si* $x \in H$, *entonces* $x = (c_k)^j$, *para algún* $k \in \mathbb{N}$. *Así, el elemento* $(c_{k+1})^j$ *es tal que*

$$\varphi_1((c_{k+1})^j) = ((c_{k+1})^j)^p = ((c_{k+1})^{pj}) = (c_k)^j.$$

Obsérvese también que $ker(\varphi_1) =< c_1 >= H_{p^1}$.

De manera análoga, se demuestra que la función $\varphi_n : H \longrightarrow H$, *con regla de correspondencia* $x \longmapsto x^{p^n}$, *es un morfismo suprayectivo con* $ker(\varphi_n) = H_{p^n}$. *Esto muestra que para cualquier* $n \in \mathbb{N}$, *se tiene el isomorfismo*

$$H/H_{p^n} \cong H,$$

es decir, los grupos cocientes formados por H *y cualquier subgrupo de* H, *son todos isomorfos a* H.

Observación. $\mathbb{Z}(p^\infty)$ *es un grupo abeliano no cíclico. En efecto, como*

$$\mathbb{Z}(p^\infty) \cong H = \cup_{i\in\mathbb{N}} H_{p^n},$$

si g *fuera un elemento generador de* $\mathbb{Z}(p^\infty)$, *entonces* H *tendría un elemento* g' *generador. Ahora, como* $H = \cup_{i\in\mathbb{N}} H_{p^n}$, $g' \in H_{p^n}$, *para alguna* $n \in \mathbb{N}$, *lo cual implica que* $o(g') \leq p^n$. *Ahora, por la manera en que se construyó* H, *existe un natural* $m > n$, *tal que* $H_{p^m} \leq H$. *Si* c_m *es un elemento generador del grupo cíclico* H_{p^m} *de orden* p^m, *se llega a la contradicción*

$$p^m = o(c_m) \leq\mid H \mid= o(g') \leq p^n.$$

Por lo tanto, $\mathbb{Z}(p^\infty)$ *no es un grupo cíclico.*

Observación. $\mathbb{Z}(p^\infty)$ *es un grupo abeliano infinito, no cíclico, tal que todo subgrupo propio es cíclico y de órden* p^n*, con* $n \in \mathbb{N}$*. Esto no sucede para cualquier grupo abeliano, no cíclico y finito. En efecto, si* G *es un grupo abeliano finito y no cíclico, entonces* G *es un grupo finitamente generado. Más aún, por ser* G *un grupo abeliano finitamente generado y no cíclico, el Teorema Fundamental sobre Grupos Abelianos Finitamente Generados, nos asegura que*

$$G =< c_1 > \oplus < c_2 > \oplus \cdots < c_s >, \text{ donde } s \geq 2.$$

Así, si p *es un primo para el cual* $p \mid o(c_i)$ *y* $p \mid o(c_j)$*, con* $i \neq j$*, entonces* G *contiene un subgrupo isomorfo a* $\mathbb{Z}(p) \oplus \mathbb{Z}(p)$*, el cual no es cíclico.*

Al igual que $\mathbb{Z}(p^\infty)$, $\mathbb{Q}$ puede obtenerse mediante una unión infinita ascendente de cadenas de grupos cíclicos:

$$\mathbb{Z} =< 1 >\subseteq< \frac{1}{2!} >\subseteq< \frac{1}{3!} >\subseteq \cdots \subseteq< \frac{1}{n!} > \cdots$$

puesto que, para cualquier racional $\frac{n}{m}$, se tiene

$$\tfrac{n}{m} = n(m-1)!\tfrac{1}{m!} \in< \tfrac{1}{m!} > .$$

Observación. $\mathbb{Q}$ *no es un grupo cocíclico ya que no contiene un subgrupo menor. Aún así, por lo observado anteriormente, se tiene que*

$$2c_2 = c_1,\ 3c_3 = c_2,\ \cdots,\ (n+1)c_{n+1} = c_n,\ \cdots$$

2.4. El Grupo de los enteros p-ádicos

Tomemos ahora al grupo de endomorfismos de $\mathbb{Z}(p^\infty)$, donde la operación del grupo es la suma de morfismos. A este grupo lo denotamos por $End(\mathbb{Z}(p^\infty))$.

Observación. *Para cualquier grupo abeliano* A*,* $End(A)$ *es un grupo abeliano, cuya operación aditiva* $\tilde{+} : End(A) \times End(A) \longrightarrow End(A)$ *está definida por*

$$(f \tilde{+} g)(x) = f(x) + g(x),$$

donde $+$ es la operación aditiva del gurpo A.

Definición 2.4.1. *$J_p = End(\mathbb{Z}(p^\infty))$. A este grupo lo llamaremos el grupo de los enteros p- ádicos.*

Proposición 2.4.2. *Todo elemento en $End(\mathbb{Z}(p^\infty))$ define una sucesión $\{a_i\}_{i\in\mathbb{N}}$ donde $a_i \in \mathbb{Z}_p$ para toda $i \in \mathbb{N}$.*

Demostración. Sea $\varphi \in End(\mathbb{Z}(p^\infty))$. Como φ está determinada por los valores que toma en el conjunto generador $\{\frac{1}{p}, \frac{1}{p^2}, \cdots\}$ de $\mathbb{Z}(p^\infty)$, basta analizar qué elemento le asigna φ en $\mathbb{Z}(p^\infty)$ a cada $\frac{1}{p^n}$. Notemos que, como $o(\frac{1}{p}) = p$, entonces

$$o(\varphi(\tfrac{1}{p})) \leq p,$$

por lo que $\varphi(\frac{1}{p}) = \frac{a_0}{p}$ con $a_0 \in \{0, 1, \ldots, p-1\}$. Análogamente, como $o(\frac{1}{p^2}) = p^2$, entonces $o(\varphi(\frac{1}{p^2})) \leq p^2$, por lo que

$$\varphi(\tfrac{1}{p^2}) = \tfrac{a_1}{p} + \tfrac{b_0}{p^2},$$

donde $b_0, a_1 \in \{0, 1, \ldots, p-1\}$. Afirmamos que $b_0 = a_0$. Como $p\frac{1}{p^2} = \frac{1}{p}$, se tienen las igualdades

$$\tfrac{a_0}{p} = \varphi(\tfrac{1}{p}) = p\varphi(\tfrac{1}{p^2}) = p(\tfrac{b_1}{p} + \tfrac{b_0}{p^2}) = \tfrac{b_0}{p}.$$

La unicidad en la expresión de cada elemento no nulo en $\mathbb{Z}(p^\infty)$ implica que que $a_0 = b_0$. Notemos que, de esta manera, vamos construyendo una sucesión $\{s_i\}_{i\in\mathbb{N}}$ donde $s_0 = a_0$ y $s_1 = a_1$.

Supongamos que hemos definido los primeros m términos de la sucesión $\{s_i\}_{i\in\mathbb{N}}$, donde

$$\{s_0 = a_0, s_1 = a_1, \ldots, s_m = a_m\}$$

con $a_0, a_1, \ldots, a_m \in \{0, 1, \ldots, p-1\}$ y

$$\varphi(\tfrac{1}{k}) = \tfrac{a_k}{p} + \tfrac{a_{k-1}}{p^2} + \cdots + \tfrac{a_0}{p^k},$$

para toda $k \leq m$. Ahora, si

$$\varphi(\tfrac{1}{p^{m+1}}) = \tfrac{a_{m+1}}{p} + \tfrac{b_m}{p^2} + \cdots + \tfrac{b_0}{p^{m+1}},$$

como $p\frac{1}{p^{m+1}} = \frac{1}{p^m}$, entonces

$$\frac{a_m}{p} + \frac{a_{m-1}}{p^2} + \cdots + \frac{a_0}{p^m} = \varphi(\tfrac{1}{p^m}) = p\varphi(\tfrac{1}{p^{m+1}})$$
$$= p(\tfrac{a_{m+1}}{p} + \tfrac{b_m}{p^2} + \cdots + \tfrac{b_0}{p^{m+1}}) = \frac{b_m}{p} + \frac{b_{m-1}}{p^2} + \cdots + \frac{b_0}{p^m}.$$

De nuevo, la unicidad en la expresión de cada elemento no nulo de $\mathbb{Z}(p^\infty)$, implica que $a_m = b_m, \ldots, a_0 = b_0$, de donde podemos concluir que el término $m+1$- ésimo de la sucesión $\{s_i\}_{i\in\mathbb{N}}$ es $s_{m+1} = a_{m+1}$. Por lo tanto, cada endomorfismo φ define una sucesión $\{a_i\}_{i\in\mathbb{N}}$ donde $a_i \in \{0, 1, \ldots, p-1\}$, $\forall i \in \mathbb{N}$. □

Recíprocamente, se tiene la siguiente

Proposición 2.4.3. *Toda sucesión $S = \{s_i\}_{i\in\mathbb{N}}$ con $s_i \in \{0, 1, \ldots, p-1\}$ define un morfismo $\varphi_S : \mathbb{Z}(p^\infty) \longrightarrow \mathbb{Z}(p^\infty)$.*

Demostración. Sea $S = \{a_i\}_{i\in\mathbb{N}}$, donde $a_i \in \{0, 1, \ldots, p-1\}$. Definamos la función $\varphi_S : \mathbb{Z}(p^\infty) \longrightarrow \mathbb{Z}(p^\infty)$ en cada elemento generador de la siguiente manera: para cada $k \in \mathbb{N}$,

$$\varphi_S(\tfrac{1}{p^k}) = \frac{a_k}{p} + \frac{a_{k-1}}{p^2} + \cdots + \frac{a_0}{p^k}.$$

Además, definimos a φ_S de tal manera que respete las sumas, es decir, que para cualquier generador $\frac{1}{p^k}$ y $b \in \mathbb{Z}$ se cumple que $\varphi_S(\frac{b}{p^k}) = b \cdot \varphi_S(\frac{1}{p^k})$.

Veamos que φ_S está bien definida. Notemos primero que si $z = \frac{b}{p} \in \mathbb{Z}$ entonces $p \mid b$. De esta manera, se tiene que

$$\varphi_S(\tfrac{b}{p}) = b\frac{a_0}{p} = \frac{b}{p} \cdot a_0 = 0$$

en $\mathbb{Z}(p^\infty)$. Observemos también el caso cuando $z = \frac{b_1}{p} + \frac{b_2}{p^2} \in \mathbb{Z}$. Ahora se cumple que $p^2 \mid pb_1 + b_2$. Como $p \mid p^2$ y $p \mid pb_1$, podemos concluir que $p \mid b_2$. Por lo tanto,

$$\varphi_S(z) = \varphi_S(\tfrac{b_1}{p} + \tfrac{b_2}{p^2}) = b_1 \cdot \tfrac{a_0}{p} + b_2 \cdot (\tfrac{a_1}{p} + \tfrac{a_0}{p^2})$$
$$= (\tfrac{b_1}{p} + \tfrac{b_2}{p^2}) \cdot a_0 + b_2 \cdot \tfrac{a_1}{p} = \tfrac{pb_1+b_2}{p^2} \cdot a_0 + \tfrac{b_2}{p} \cdot a_1$$

de donde se sigue que $\varphi_S(z) \in \mathbb{Z}$, ya que tanto $p \mid b_2$ como $p^2 \mid pb_1 + b_2$.

En general, si $z = \frac{b_1}{p} + \frac{b_2}{p^2} + \cdots + \frac{b_n}{p^n} \in \mathbb{Z}$ se tiene que

$$p^n \mid p^{n-1}b_1 + p^{n-2}b_2 + \cdots + pb_{n-1} + b_n.$$

De lo anterior, podemos concluir que, para cada $i \in \{1, \ldots, n-1\}$,

$$p^i \mid p^{i-1}b_{n-i+1} + p^{i-2}b_{n-i+2} + \cdots + pb_{n-1} + b_n$$

ya que $p^i \mid p^n$ y

$$p^i \mid p^i(p^{n-1-i}b_1 + \cdots + pb_{n-i-1} + b_{n-i}).$$

De esta manera, se tiene que

$$\begin{aligned}\varphi_S(z) &= \varphi_S(\tfrac{b_1}{p} + \tfrac{b_2}{p^2} + \cdots + \tfrac{b_n}{p^n}) = \varphi(\tfrac{b_1}{p}) + \cdots + \varphi(\tfrac{b_n}{p^n})\\ &= b_1 \cdot \tfrac{a_0}{p} + b_2 \cdot (\tfrac{a_1}{p} + \tfrac{a_0}{p^2}) + \cdots + b_n \cdot (\tfrac{a_n}{p} + \tfrac{a_{n-1}}{p^2} + \cdots + \tfrac{a_0}{p^n})\\ &= (\tfrac{b_1}{p} + \tfrac{b_2}{p^2} + \cdots + \tfrac{b_n}{p^n}) \cdot a_0 + (\tfrac{b_2}{p} + \tfrac{b_3}{p^2} + \cdots + \tfrac{b_n}{p^{n-1}}) \cdot a_1 + \cdots + \tfrac{b_n}{p} \cdot a_n\\ &= (\tfrac{p^{n-1}b_1 + p^{n-2}b_2 + \cdots + b_n}{p^n}) \cdot a_0 + (\tfrac{p^{n-2}b_2 + p^{n-3}b_3 + \cdots + b_n}{p^{n-1}}) \cdot a_1 + \cdots + \tfrac{b_n}{p} \cdot a_n.\end{aligned}$$

Por lo notado anteriormente, cada sumando de la forma

$$(\tfrac{p^{i-1}b_1 + p^{i-2}b_2 + \cdots + b_n}{p^i}) \in \mathbb{Z} \text{ para } i \in \{1, \ldots, n\}$$

por lo que $\varphi_S(z) = 0$.

Por lo tanto, si $\overline{z} = \overline{w}$ en $\mathbb{Z}(p^\infty)$ entonces $\overline{z} - \overline{w} = 0$ teniendo así que

$$0 = \varphi_S(\overline{z} - \overline{w}) = \varphi_S(\overline{z}) - \varphi_S(\overline{w})$$

con lo cual $\varphi_S(\overline{z}) = \varphi_S(\overline{w})$. Esto demuestra que φ_S está bien definida. □

Definición 2.4.4. *Sean $\alpha, \beta \in \mathbb{Z}$. El intervalo $[\alpha, \beta]_{\mathbb{Z}}$ es el conjunto*

$$\{c \in \mathbb{Z} \mid \alpha \leq c \leq \beta\}.$$

Observación. *Por las Proposiciones 2.4.2 y 2.4.3, se sigue que la función*

$$End(\mathbb{Z}(p^\infty)) \longrightarrow \Pi_{i\in\mathbb{N}}[0, p-1]_{\mathbb{Z}}$$

con regla de correspondencia $\varphi \longmapsto \varphi_S = \{a_i\}_{i\in\mathbb{N}}$ es biyectiva.

Capítulo 3

Módulos

3.1. Definición

Definición 3.1.1. *Sea R un anillo asociativo con 1. Decimos que un grupo abeliano M es un R-módulo derecho si existe una función $\varphi : M \times R \longrightarrow M$, con regla de correspondencia $(x, a) \longmapsto xa$ tal que para toda $x, y \in M$ y $a, b \in R$ se satisfacen las siguientes propiedades:*

1. $(x + y)a = xa + ya$
2. $x(a + b) = xa + xb$
3. $x(ab) = (xa)b$
4. $x1 = x$

A la función $\varphi : M \times R \longrightarrow M$ mencionada anteriormente se le llama una acción por la derecha del anillo R en el grupo M.

De manera análoga, definimos un R-módulo izquierdo como un grupo abeliano M junto con la función $\varphi : R \times M \longrightarrow M$ que cumple las propiedades anteriores salvo que ahora R actúa por la izquierda. Denotaremos a un módulo derecho por M_R y a un módulo izquierdo por ${}_RM$.

Observación. *Cuando R es un anillo conmutativo, cualquier M módulo derecho es también un M módulo izquierdo y viceversa.*

En lo que sigue de la sección, nos referiremos a un módulo M como un R-módulo derecho, a menos que se especifique lo contrario.

Definición 3.1.2. *Sea M un R-módulo. Decimos que $L \subset M$ es un R-submódulo de M si L es un subgrupo de M tal que para cualquier $x \in L$ y $a \in R$ se tiene que $xa \in L$. En otras palabras, L es un R-submódulo de M si L es un R-módulo con la operación heredada por M, a saber, la acción $\varphi\,|_L \colon L \times R \longrightarrow L$.*

Definición 3.1.3. *Sea L un R-submódulo de M. Definimos al R-módulo cociente M/L, como el grupo cociente M/L junto con la acción*

$$\phi : M/L \times R \longrightarrow M/L$$

dada por $(\bar{x}, a) \longmapsto \overline{xa}$.

Observación. *La operación $\phi : M/L \times R \longrightarrow M/L$ está bien definida. En efecto, como $\overline{x} = \overline{y}$ en M/L si y sólo si $x - y \in L$, si $x - y \in L$ entonces $xa - ya = (x - y)a \in L$. Así,*

$$\overline{x}a = \overline{xa} = \overline{ya} = \overline{y}a,$$

para cualquier $a \in R$. Se sigue que la operación ϕ hace de M/L un R-módulo.

Definición 3.1.4. *Sean M y N dos R-módulos. Decimos que $\alpha : M \longrightarrow N$ es un morfismo entre los módulos M y N, o una función R- lineal, si*

$$\alpha(x + y) = \alpha(x) + \alpha(y) \text{ y } \alpha(xa) = \alpha(x)a,$$

para cualquier $x, y \in M$ y $a \in R$.

Al igual que en la teoría de grupos, si $\alpha : M \longrightarrow N$ y $\beta : N \longrightarrow P$ son dos morfismos entre módulos, entonces la composición $\beta \circ \alpha : M \longrightarrow P$ también es un morfismo entre los módulos M y P. Además, para cada módulo M, se tiene el morfismo identidad id_M.

Definición 3.1.5. *Sea $\alpha : M \longrightarrow N$ un morfismo de R-módulos. El kernel de α es el conjunto*

$$Ker(\alpha) = \{x \in M \mid \alpha(x) = 0\}.$$

La imagen de α es el conjunto

$$Im(\alpha) = \{\alpha(x) \mid x \in M\}.$$

Observación. *Los conjuntos $Ker(\alpha)$ y $Im(\alpha)$ son R-submódulos de M y N, respectivamente.*

Definición 3.1.6. *Sea $\alpha : M \longrightarrow N$ un morfismo de módulos. Decimos que α es un monomorfismo, si para cualesquiera $x, y \in M$, $\alpha(x) = \alpha(y)$ implica que $x = y$. El morfismo α es un epimorfismo si $Im(\alpha) = N$.*

Definición 3.1.7. *Sea $\alpha : M \longrightarrow N$ un morfismo de módulos. Decimos que α es un isomorfismo, si α es tanto un monomorfismo como un epimorfismo.*

Observación. *El morfismo α es un monomorfismo si y sólo si*

$$Ker(\alpha) = \{0\}.$$

Por otra parte, para cualquier submódulo L de M, se tienen el morfismo de inclusión, que denotamos por $\iota : L \hookrightarrow M$ y la proyección canónica que denotamos por $\rho : M \longrightarrow M/L$. Nótese que ι es un monomorfismo y ρ es un epimorfismo.

Teorema 3.1.8. *El morfismo $\alpha : M \longrightarrow N$ es un isomorfismo si existe un morfismo $\beta : N \longrightarrow M$ tal que*

$$\beta \circ \alpha = id_M \text{ y } \alpha \circ \beta = Id_N.$$

Algunos ejemplos son los siguientes:

1. Todo grupo abeliano G es un $\mathbb{Z}$-módulo. La función $\varphi : G \times \mathbb{Z} \longrightarrow G$ definida por $(x, n) \longmapsto nx$, donde $xn = (x + x + \cdots + x)$ (n veces), hace de G un $\mathbb{Z}$-módulo. Como todo $\mathbb{Z}$-módulo es un grupo abeliano, se sigue que los grupos abelianos y los $\mathbb{Z}$-módulo están en correspondencia uno a uno.

2. Si R es el anillo $\mathbb{Q}_p$ de números racionales cuyos denominadores son primos relativos con el primo p, entonces cualquier p-grupo abeliano A es un $\mathbb{Q}_p$-módulo.

   Veamos que la función $\varphi : A \times \mathbb{Q}_p \longrightarrow A$ con regla de correspondencia $(a, \frac{m}{n}) \longmapsto (n^{-1}a)m$ está bien definida. Para esto, basta ver que los elementos de la forma $n^{-1}a = \frac{a}{n}$ están únicamente determinados, que equivale a decir que exista una única $x \in A$ tal que $nx = a$. Como A es un p-grupo, si $a \in A$, el orden de a es una potencia de p, digamos p^k. Dado cualquier $\frac{m}{n} \in \mathbb{Q}_p$, como $(n; p) = 1$, entonces también $(n; p^k) = 1$, por lo que existen $s, t \in \mathbb{Z}$ tales que $sn + tp^k = 1$. De esta manera,

   $$a = [sn + tp^k]a = sna + tp^k a = sna.$$

Por lo tanto, $x = sa$ cumple la propiedad mencionada. Ahora, si $x \in A$ también satisface $nx = a$, entonces $nsa = a = nx$, por lo que

$$n(sa - x) = nsa - nx = 0.$$

Como $sa - x \in A$, se tiene que $o(sa - x) = p^l$ para aglún $l \in \mathbb{N}$, con lo cual $p^l \mid n$. Esto implica que $l = 0$, ya que $(n, p) = 1$. Por lo tanto el orden de $sa - x$ es 1, teniendo así que $sa - x = 0$, es decir, $x = sa$. Es claro que φ cumple las poropiedades de una acción.

Definición 3.1.9. *Una sucesión de morfismos entre A-módulos de la forma*

$$\cdots \longrightarrow M_{i-1} \xrightarrow{\alpha_{i-1}} M_i \xrightarrow{\alpha_i} M_{i+i} \longrightarrow \cdots$$

es exacta en M_i si $Ker(\alpha_i) = Im(\alpha_{i-1})$. Decimos que la sucesión es exacta si es exacta en cada M_i.

Ejemplo. *Sea L un submódulo de M. Entonces la sucesión*

$$0 \hookrightarrow L \overset{\iota}{\hookrightarrow} M \xrightarrow{\rho} M/L \longrightarrow 0,$$

es exacta, donde ι es la inclusión y ρ la proyección natural. A las sucesiones de esta forma, las llamamos sucesiones exactas cortas.

3.2. Suma directa interna y externa

Sean I un conjunto y $\{M_i\}_{i\in I}$ una familia de A-módulos.

Definición 3.2.1. *El producto cartesiano de la familia $\{M_i\}_{i\in I}$ es el conjunto*

$$\Pi_{i\in I} M_i = \{f : I \longrightarrow \cup_{i\in I} M_i \mid f(i) \in M_i, \forall i \in I\}.$$

Observación. *El conjunto $\Pi_{i\in I} M_i$ es un A-módulo si definimos la operación suma por $(f + g)(i) = f(i) + g(i)$ para cada $i \in I$, así como el producto por un escalar por $(fa)(i) = f(i)a$.*

Definición 3.2.2. *Al módulo $\Pi_{i\in I} M_i$ se le llama el producto directo de los módulos $\{M_i\}_{i\in I}$.*

Definición 3.2.3. *Sea $\{M_i\}_{i\in I}$ una familia de módulos. El conjunto*

$$\{f \in \Pi_{i\in I} M_i \mid f(i) = 0, \textit{ salvo para una cantidad finita de índices } i \in I\},$$

es un submódulo del producto $\Pi_{i\in I} M_i$*, y se le llama la suma directa (exterma) de los módulos* $\{M_i\}_{i\in I}$*. A este submódulo lo denotamos por*

$$\oplus_{i\in I} M_i.$$

Definición 3.2.4. *Una función* $f : I \longrightarrow \cup_{i\in I} M_i$ *es de soporte finito si* $f(i) = 0$ *para casi toda* $i \in I$*.*

Por otra parte, cada función $f : I \longrightarrow \cup_{i\in I} M_i$ en el producto directo, define al conjunto $(x_i)_{i\in I}$ donde $x_i = f(i)$. Notemos que $(x_i)_{i\in I}$ es tal que $x_i \in M_i$, $\forall i \in I$. Ahora, todo conjunto de la forma $(x_i)_{i\in I}$ tal que $x_i \in M_i$, $\forall i \in I$ induce una función $f : I \longrightarrow \cup_{i\in I} M_i$ con regla de correspondencia $f(i) = x_i$, $\forall i \in I$. Por la manera en que se define a f, se sigue que $f \in \Pi_{i\in I} M_i$, mostrando así que el conjunto de funciones $f : I \longrightarrow \cup_{i\in I} M_i$ está en correspondencia con el conjunto de colecciones de la forma $(x_i)_{i\in I}$ tales que $x_i \in M_i$, para cada $i \in I$.

Para facilitar la notación, usaremos $(x_i)_{i\in I}$ para describir a los elementos del producto directo.

Observación. *Para cada* $j \in I$*, se tiene el morfismo proyección*

$$\rho_j : \Pi_{i\in I} M_i \longrightarrow M_j$$

donde a cada elemento $(x_i)_{i\in I}$ *se le asigna su término* j*-ésimo. Así mismo, para cada* $j \in I$*, se tiene el morfismo inclusión*

$$\iota_j : M_j \longrightarrow \Pi_{i\in I} M_i,$$

donde a cada $m \in M_j$ *se le asigna el elemento* $(x_i)_{i\in I}$ *tal que todos sus términos son cero excepto el* j*-ésimo, en el cuál* $x_j = m$*. Nótese que* $Im(\iota_j) \subset \oplus_{i\in I} M_i$ *para cada* $j \in I$*.*

Además, cuando I *es un conjunto finito, si* $I = \{1, \ldots, n\}$ *entonces* $\Pi_{i\in I} M_i = \oplus_{i\in I} M_i$*.*

Definición 3.2.5. *Sean* M *un* A*-módulo y* $\{M_i\}_{i\in I}$ *una familia de submódulos. Definimos*

$$\Sigma_{i\in I} M_i = \{\Sigma_{i\in I} x_i \in M \mid x_i \in M_i \textit{ y } x_i = 0 \textit{ para casi toda } i \in I\}.$$

Observación. *El submódulo $\Sigma_{i\in I}M_i$ es el menor submódulo de M que contiene a cada M_i. Además, se tiene el morfismo $\alpha : \oplus_{i\in I}M_i \longrightarrow M$, con regla de correspondencia $(x_i)_{i\in I} \longmapsto \Sigma_{i\in I}x_i$. Nótese que la imágen de α es el conjunto $\Sigma_{i\in I}M_i$.*

Definición 3.2.6. *Si el morfismo $\alpha : \oplus_{i\in I}M_i \longrightarrow M$ es inyectivo, decimos que el módulo $\Sigma_{i\in I}M_i$ es la suma directa (interna) de los submódulos M_i. En esta caso, se tiene que $\oplus_{i\in I}M_i \cong \Sigma_{i\in I}M_i$.*

Notación. Cuando $M_i = M$ para toda $i \in I$, usaremos $\Pi_{i\in I}A_i = A^I$ y $\oplus_{i\in I}A_i = A^{(I)}$.

Observación. *Como todo grupo abeliano M es un $\mathbb{Z}$-módulo, los conceptos anteriores son válidos para cualquier grupo abeliano.*

3.3. Módulos libres

Definición 3.3.1. *Sea M un A-módulo. Decimos que M está generado por la familia $(x_i)_{i\in I}$ de elementos de M si cada $x \in M$ se puede escribir de la forma $\Sigma_{i\in I}x_ia_i$, donde $a_i \in A$ y $a_i = 0$ salvo para una cantidad finita de índices.*

Definición 3.3.2. *Si los coeficientes a_i de la expresión $x = \Sigma_{i\in I}x_ia_i$ están determinados de manera única por x, decimos que la familia $(x_i)_{i\in I}$ es una base para M.*

Definición 3.3.3. *Un módulo M es libre si existe una base $\{x_i\}_{i\in I}$ para M.*

Proposición 3.3.4. *Un módulo M es libre si y sólo si $M \cong A^{(I)}$ para algún conjunto I.*

Demostración. Notemos que $A^{(I)}$ es un A-módulo libre que tiene como base al conjunto $\{e_i\}_{i\in I}$, donde e_i es 1 en la componente j-ésima 1 y cero en cualquier otro caso. Ahora, si M es un grupo libre, tal que la familia $\{x_i\}_{i\in I}$ de elementos de M es una base, entonces la función $\varphi : A^{(I)} \longrightarrow M$ definida por $(a_i)_{i\in I} \longmapsto \Sigma_{i\in I}x_ia_i$ es un isomorfismo. En efecto, claramente φ es sobre y la unicidad en la expresión de cada elemento $x = \Sigma_{i\in I}x_ia_i \in M$ hacen de φ una función inyectiva. □

Observación. *Por la equivalencia entre $\mathbb{Z}$-módulos y grupos abelianos, se sigue que un grupo abeliano G es libre si y sólo si $G \cong \mathbb{Z}^{(I)}$, es decir, G es la suma directa de grupos cíclicos infinitos.*

Capítulo 4

Sumas Directas

4.1. Definición

La definición de suma directa interna que hemos dado ha sido para módulos. Esta definición es válida para grupos abelianos, ya que estos son $\mathbb{Z}$-módulos. Veremos ahora otra forma de describir a la suma directa (interna) para grupos abelianos:

Definición 4.1.1. *Sean A un grupo y $B, C \leq A$. Si $A = B{+}C$ y $B{\cap}C = \{0\}$, decimos que A es la suma directa interna de los subgrupos B y C.*

Observación. *La primera condición equivale a decir que todo elementen A se puede expresar como una suma de la forma $b + c$ con $b \in B$ y $c \in C$. La segunda condición, nos asegura la unicidad de dichas expresiones. En efecto, si $b_1 + c_1 = a = b_2 + c_2$ entonces $b_1 - b_2 = c_2 - c_1$, con lo cual $b_1 - b_2 \in B \cap C = \{0\}$, así como $c_2 - c_1 \in B \cap C = \{0\}$, teniendo así que $b_1 = b_2$ y $c_1 = c_2$.*

Definición 4.1.2. *Sean A un grupo y $\{B_i\}_{i \in I}$ una familia de subgrupos de A. Si se satisfacen las siguientes condiciones:*

i) $A = \Sigma_{i \in I} B_i$,

ii) *para cada* $i \in I$, $B_i \cap \Sigma_{j \neq i} B_j = \{0\}$,

decimos que A es la suma directa (interna) de los subgrupos B_i.

Proposición 4.1.3. *Las definiciones 3.2.6 y 4.1.2 de suma directa (interna) son equivalentes.*

Demostración. Sean A un grupo y $\{B_i\}_{i\in I}$ una familia de subgrupos de A tales que $A = \Sigma_{i\in I} B_i$. Supongamos que A es la suma directa interna bajo la definición 3.2.6. Ahora, como el morfismo $\alpha : \oplus_{i\in I} B_i \longrightarrow A$ es un monomorfismo y $Im(\alpha) = \Sigma_{i\in I} B_i = A$, entonces α es un isomorfismo. Esto implica que para cada $i \in I$, $B_i \cap \Sigma_{j\neq i} B_j = \{0\}$. En efecto, en caso contrario, si $b_i = b = b_{j_1} + \cdots + b_{j_n}$ con $b_i \in B_i$, $b_{j_s} \in B_{j_s}$ y $j_s \neq j_r$, para cada $s \neq r \in \{1, \ldots n\}$, entonces los elementos

$$(x_i)_{i\in I} = \{x_i \mid x_j = 0, \text{ para } j \neq i, \text{ y } x_i = b_i\}$$

y

$$(y_i)_{i\in I} = \{y_i \mid y_{j_s} = b_{j_s} \text{ para } s \in \{1, \ldots, n\} \text{ y } y_i = 0 \text{ en cualquier otro caso}\}$$

son distintos en $\oplus_{i\in I} B_i$, y además, son tales que $\alpha((x_i)_{i\in I}) = b = \alpha((y_i)_{i\in I})$, contradiciendo que α sea un monomorfismo. Por lo tanto, se cumple la definición 4.1.2.

Supongamos ahora que se cumplen las condiciones $i)$ y $ii)$ de la definición 4.1.2. Por la condición $i)$, se tiene que $Im(\alpha) = \Sigma_{i\in I} B_i = A$, por lo que α es un epimorfismo. La condición $ii)$ asegura que la expresión de cada elemento de A, como una sumas de la forma $b_{j_1} + \cdots + b_{j_n}$ con $b_{j_s} \in B_{j_s}$ y $j_s \neq j_r$, para cada $s \neq r \in \{1, \ldots n\}$, sea única. Esto quiere decir que α es una función inyectiva, por lo que $\oplus_{i\in I} B_i \cong \Sigma_{i\in I} B_i$, es decir, se satisface la definición 3.2.6. □

4.2. Propiedades

Recordemos que si A es un grupo abeliano y p un primo, el conjunto

$$A_p = \{a \in A \mid o(a) = p^k, k \in \mathbb{N}\}.$$

es la p-componente del grupo A. Además, éste es un subgrupo de A en el cual todo elemento tiene orden una potencia del primo p.

Teorema 4.2.1. *Todo grupo abeliano de torsión A es la suma directa de sus p-componente A_p, donde p es un primo.*

Demostración. Sea Π el conjunto de todos los primos. Veamos primero que $A = \Sigma_{p\in\Pi} A_p$. Si $a \in A$, como A es un grupo de torsión, entonces $o(a) = m$, para algún natural m. Ahora, si $m = p_1^{n_1} \cdot p_2^{n_2} \cdot \cdots \cdot p_k^{n_k}$ es la descomposición en números primos, para cada $i \in \{1, \ldots, k\}$, definimos los números

$$m_i = m \cdot p_i^{-n_i} = m/p_i^{n_i}.$$

Con esto en cuenta, se tiene que $(m_1, m_2, \ldots, m_k) = 1$ por lo que existen enteros $s_1, s_2, \ldots s_k$ tales que $s_1m_1 + s_2m_2 + \cdots + s_km_k = 1$. Esto nos lleva a la igualdad

$$a = s_1m_1a + s_2m_2a + \cdots + s_km_ka,$$

donde $m_ia \in A_{p_i}$, pues $p_i^{n_i}(m_ia) = ma = 0$, para cada i. Esto muestra que $A = \Sigma_{p\in\Pi}A_p$.

Veamos ahora que $A_q \cap (A_{p_1} + A_{p_2} + \cdots + A_{p_s}) = \{0\}$, donde $q, p_1, p_2, \ldots, p_s$ son primos distintos. Si $a \in A_q \cap (A_{p_1} + A_{p_2} + \cdots + A_{p_s})$, entonces a tendría orden q^r, para algún $r \in \mathbb{N}$, y además, $a = a_{p_1} + a_{p_2} + \cdots + a_{p_s}$, con $p_i^{n_i}a_{p_i} = 0$, para alguna $n_i \in \mathbb{N}$. De esto último, se sigue que $(p_1^{n_1} \cdot p_2^{n_2} \cdot \cdots \cdot p_s^{n_s})a = 0$, con lo cual se tiene que

$$q^r \mid p_1^{n_1} \cdot p_2^{n_2} \cdot \cdots \cdot p_s^{n_s}.$$

La propiedad de ser números primos nos lleva a que $q \mid p_i$, para alguna $i \in \{1, \ldots s\}$, contradiciendo la elección de q. Por lo tanto,

$$A_q \cap (A_{p_1} + A_{p_2} + \cdots + A_{p_s}) = \{0\},$$

y así, $A = \oplus_{p\in\Pi}A_p$. □

Ejemplo. *Sea $A =< a >$ un grupo cíclico de orden m. Si $m = p_1^{r_1} \cdot p_2^{r_2} \cdot \cdots \cdot p_s^{r_s}$ es la factorización completa de m en primos, y $m_i = m/p_i^{r_i}$, entonces*

$$A = \oplus_{i=1}^{k} < m_ia >.$$

Nótese que $< m_ia >$ es un grupo cíclico de orden $p_i^{r_i}$.

Ejemplo. *La p-componente del grupo $\mathbb{Q}/\mathbb{Z}$ es $\mathbb{Z}(p^\infty)$. Así, se sigue que*

$$\mathbb{Q}/\mathbb{Z} = \oplus_{p\in\Pi}\mathbb{Z}(p^\infty),$$

donde Π es el conjunto de todos los primos.

Definición 4.2.2. *Sea $B \leq A$. Decimos que B es un subgrupo totalmente invariante, si para cualquier endomorfismo $\eta : A \longrightarrow A$ se cumple que $\eta(B) = B$.*

Notemos que las p-componentes son subgrupos totalmente invariantes de A. Si $\eta : A \longrightarrow A$ es un endomorfismo y $a \in A_p$, entonces $o(a) = p^k$, con lo cual se sigue que

$$0 = \eta(p^k a) = p^k \eta(a),$$

es decir, $\eta(a)$ tiene orden una potencia de p.

Proposición 4.2.3. *Sean A, B, C grupos y*

$$0 \hookrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0.$$

una sucesión exacta corta. Las siguientes condiciones son equivalentes:

(a) Existe $f : B \longrightarrow A$ morfismo tal que $f \circ \alpha = id_A$.

(b) B es de la forma $\alpha(A) \oplus D$ con $D \leq B$, y $\beta\mid_D : D \longrightarrow C$ es un isomorfismo.

(c) Existe $g : C \longrightarrow B$ morfismo tal que $\beta \circ g = id_C$.

Demostración. $(a) \Longrightarrow (b)$. Supongamos que $f : B \longrightarrow A$ es un morfismo tal que $f \circ \alpha = id_A$. Veamos que $B = \alpha(A) \oplus D$, para algún $D \leq B$. Si $b \in B$ entonces $f(b) \in A$, por lo que $(\alpha \circ f)(b) = \alpha(f(b)) \in B$. Así,

$$(f \circ \alpha)(f(b)) = (f \circ \alpha \circ f)(b) = f(\alpha(f(b))) \in A.$$

Como por hipótesis $f \circ \alpha = id_A$, de lo anterior se sigue que

$$f(b) = f(\alpha(f(b))),$$

con lo que $f(\alpha(f(b)) - b) = 0$. Esto implica que $\alpha(f(b)) - b \in Ker(f)$, con lo cual $b \in \alpha(f(b)) + Ker(f)$, es decir, $B = \alpha(A) + Ker(f)$. Por lo tanto, si definimos a $D = Ker(f)$, bastaría demostrar que $\alpha(A) \cap Kerf = \{0\}$.

Sea $b \in \alpha(A) \cap Ker(f)$. Entonces $f(b) = 0$ y $b = \alpha(a)$, para alguna $a \in A$. Como $f \circ \alpha = id_A$, se tiene que

$$0 = f(b) = f(\alpha(a)) = (f \circ \alpha)(a) = a.$$

Así, $\alpha(a) = 0$ y $b = f(b) = f(\alpha(a)) = f(0) = 0$. Por lo tanto $\alpha(A) \cap Ker(f) = \{0\}$.

Por otra parte, notemos que $\beta\mid_{Ker(f)} : Ker(f) \longrightarrow C$ es un isomorfismo. En efecto, como $B = \alpha(A) \oplus Ker(f)$ y β es suprayectiva, entonces

$$C = \beta(B) = \beta(\alpha(A)) + \beta(Kerf).$$

Como la sucesión es exacta, $\alpha(A) = Im\alpha = Ker\beta$, por lo que $\beta(\alpha(A)) = 0$, con lo cual, se tiene que $C = \beta(Ker(f))$. Esto quiere decir que $\beta\mid_{Ker(f)}$ es un epimorfismo. Ahora,

$$Ker(\beta\mid_{Kerf}) = Ker(\beta) \cap Ker(f) = \alpha(A) \cap Ker(f) = \{0\},$$

por lo que $\beta\mid_{Ker(f)}$ es inyectiva. Esto muestra que $\beta\mid_{Ker(f)}$ es un isomorfismo.

$(b) \Longrightarrow (a)$. Como $B = \alpha(A) \oplus D$, para cualquier $b \in B$ existen únicos $\alpha(a) \in \alpha(A)$ y $d \in D$ tales que $b = \alpha(a) + d$. Esto implica también que el elemento $a \in A$ para el cual $b = \alpha(a) + d$ sea único. Con esto en cuenta, definimos la función $f : B \longrightarrow A$ por $b \longmapsto a$. Por la unicidad mencionada anteriormente, f está bien definida. Más aún, si

$$b_1 = \alpha(a_1) + d_1 \text{ y } b_2 = \alpha(a_2) + d_2 \text{ entonces}$$

$$b_1 + b_2 = \alpha(a_1 + a_2) + (d_1 + d_2),$$

por lo que

$$f(b_1 + b_2) = a_1 + a_2 = f(b_1) + f(b_2),$$

lo cual muestra que f es un morfismo. Ahora, si $a \in A$, se tiene que $\alpha(a)+0 \in B$ y $f(\alpha(a)) = a$, teniendo así que $f \circ \alpha = id_A$.

$(b) \Longrightarrow (c)$. Sean $B = \alpha(A) \oplus D$ y $D \leq B$, con $\beta\mid_D : D \longrightarrow C$ un isomorfismo. Como $D \cong C$, dada $c \in C$ hay una única $d \in D$ tal que $\beta\mid_D(d) = c$. Esta unicidad nos permite definir la función $g : C \longrightarrow D$ con regla de correspondencia $g(c) = d$. Ahora, si $g(c_1) = d_1$ y $g(c_2) = d_2$, es decir, d_1 y d_2 son tales que $\beta\mid_D(d_1) = c_1$ y $\beta\mid_D(d_2) = c_2$, entonces por ser $\beta\mid_D$ un morfismo se tiene que

$$\beta\mid_D(d_1 + d_2) = \beta\mid_D(d_1) + \beta\mid_D(d_2) = c_1 + c_2,$$

teniendo así que

$$g(c_1 + c_2) = d_1 + d_2 = g(c_1) + g(c_2).$$

Por lo tanto, g es un morfismo.

Por otra parte, por como está definida la función g, para cualquier $c \in C$, se tiene que

$$\beta \circ g(c) = \beta \mid_D (g(c)) = \beta \mid_D (d) = c$$

mostrando así que $\beta \circ g = id_C$.

$(c) \Longrightarrow (b)$. Sea $b \in B$. Como $\beta(b) \in C$, entonces $g(\beta(b)) = g \circ \beta(b)$ es un elemento en B. Al volver a evaluar por β a esta última igualdad, se tiene que

$$\beta(g(\beta(b))) = \beta \circ g(\beta(b)).$$

Como $\beta \circ g = id_C$, esto último implica que $\beta(g(\beta(b))) = \beta(b)$, por lo que

$$g(\beta(b)) - b \in Ker\beta = \alpha(A).$$

Esto equivale a decir que

$$b \in g(\beta(b)) + \alpha(A) \in Img + \alpha(A)$$

es decir, $B = \alpha(A) + Im(g)$. Ahora, si $b \in \alpha(A) \cap Im(g)$, entonces $b = \alpha(a)$ para alguna $a \in A$ y $g(c) = b$ para alguna $c \in C$. Como $\alpha(A) = Ker(\beta)$, entonces $\beta(b) = 0$ por lo que

$$0 = \beta(b) = \beta(g(c)) = \beta \circ g(c) = c.$$

Así, $b = g(c) = g(0) = 0$, por lo que $\alpha(A) \cap Im(g) = \{0\}$. Por lo tanto $B = \alpha(A) \oplus Im(g)$.

Por último, como β es suprayectiva y $B = \alpha(A) \oplus Im(g)$, entonces

$$C = \beta(B) = \beta(\alpha(A)) + \beta(Img).$$

Además, como $\alpha(A) = Ker(\beta)$, se sigue que $C = \beta(Im(g))$, es decir, $\beta \mid_{Im(g)}$ es suprayectiva. Notemos también que

$$Ker(\beta \mid_{Im(g)}) = Ker(\beta) \cap Im(g) = \alpha(A) \cap Im(g) = \{0\},$$

por lo que el morfismo $\beta \mid_{Im(g)}$ es inyectivo. Por lo tanto, $\beta \mid_{Im(g)}$ es un isomorfismo. □

Definición 4.2.4. *Sea B un subgrupo de A. Decimos que B es un sumando directo de A, si existe un subgrupo C de A tal que $A = B \oplus C$. En este caso, llamamos a C un complemento de B en A. Decimos también que C es un seudocomplemento de B si $B + C = B \oplus C$, es decir, si $C \cap B = \{0\}$ y C es maximal con esta propiedad.*

Observación. *Para demostrar que un subgrupo B de A es un sumando directo, basta encontrar un complemento C de B en A entre el conjunto de subgrupos $G \leq A$ tales que $G \cap B = \{0\}$.*

Observación. *De la Proposición 4.2.3, se sigue que D es un sumando directo de A si y sólo si existe $\eta : A \longrightarrow D$ tal que el siguiente diagrama conmuta:*

$$\begin{tikzcd} D \arrow[r, "\iota"] \arrow[d, "id_D"'] & A \arrow[dl, "\eta"'] \\ D & \end{tikzcd}$$

Una característica de cualquier subgrupo G de A totalmente invariante es la siguiente:

Teorema 4.2.5. *Sea $A = B \oplus C$ y G un subgrupo totalmente invariante de A. Entonces $G = (G \cap B) \oplus (G \cap C)$.*

Demostración. Sean $A = B \oplus C$ y $G \leq A$ totalmente invariante. Como A es la suma directa de B y C, surgen de manera natural los morfismos $\rho_B : A \longrightarrow B$ y $\rho_C : A \longrightarrow C$ tales que hacen conmutativos a los diagramas siguientes:

$$\begin{tikzcd} B \arrow[r, "\iota"] \arrow[d, "id_B"'] & A \arrow[dl, "\rho_B"] \\ B & \end{tikzcd} \text{ y } \begin{tikzcd} C \arrow[r, "\iota"] \arrow[d, "id_C"'] & A \arrow[dl, "\rho_C"] \\ C & \end{tikzcd}.$$

Ahora, como G es totalmente invariante, se tiene que

$$\rho_C(G) \leq G \text{ y } \rho_B(G) \leq G,$$

así como

$$\rho_C(G) \leq C \text{ y } \rho_B(G) \leq B.$$

De esto último, se sigue que $\rho_C(G) \cap \rho_B(G) \subset B \cap C = \{0\}$. Más aún, al ser $A = B \oplus C$, cada $g \in G$ se escribe de manera única como $g = b + c$ con $b \in B$ y $c \in C$. Así, $\rho_C(g) = c$ y $\rho_B(g) = b$, es decir, $g = \rho_B(g) + \rho_C(g)$. Esto implica que $G = \rho_B(G) + \rho_C(G)$. Además, como $\rho_C(G) \cap \rho_B(G) = \{0\}$, se sigue que $G = \rho_B(G) \oplus \rho_C(G)$.

Ahora, como $\rho_B(G)$ es un subgrupo, tanto de G como de B, se tiene que $\rho_B(G) \leq G \cap B$, al igual que $\rho_C(G) \leq G \cap C$. Más aún, si $h \in G \cap C$, entonces $h = \rho_C(h) \in \rho_C(G)$, por lo que $\rho_C(G) = G \cap C$. Análogamente se cumple que $\rho_B(G) = G \cap B$, con lo cual concluimos que

$$G = (G \cap B) \oplus (G \cap C).$$

□

Definición 4.2.6. *Sea $B \leq A$. Decimos que un subgrupo H de A es B-alto si $H \cap B = \{0\}$ y si $H \lneqq H' \leq A$ implica que $H' \cap B \neq \{0\}$.*

Observación. *Esto último equivale a decir que H es maximal con respecto a la propiedad de ser independiente del subgrupo B, es decir, que H es un seudocomplemento de B. El lema de Zorn garantiza la existencia de subgrupos B-altos. Obsérvese que si H es un subgrupo B-alto de A, se tiene que $H+B = H \oplus B$.*

Observación. *Cualquier complemento C de B en A es un subgrupo B-alto. Más aún, C contiene a cualquier subgrupo X totalmente invariante en A, con $X \cap B = \{0\}$. En efecto, si $A = B \oplus C$, para cualquier endomorfismo φ de A, se tiene que*

$$\varphi(X) = X \leq A = B \oplus C.$$

Sea ψ la composición de morfismos

$$\psi = A \xrightarrow{\rho} C \xhookrightarrow{\iota} A,$$

donde ρ es la proyección. Como $X \cap B = \{0\}$, se cumple que $\psi(X) = X \subset C$.

Lema 4.2.7. *Sean B un subgrupo de A y C un subgrupo B-alto de A. Para cualquier primo p y cualquier $a \in A$, si $pa \in C$ entonces $a \in B \oplus C$.*

Demostración. Notemos primero que, por ser C un subgrupo B-alto de A, $B+C = B \oplus C$. Sean $a \in A$ y p un primo tales que $pa \in C$. Si $a \in C$, entonces $a \in B \oplus C$, por lo que supongamos que $a \notin C$. Como C es un subgrupo B-alto, el subgrupo $< C, a >$ contiene un elemento $0 \neq b \in B$, ya que $C \lneqq < C, a >$. Así, podemos escribir al elemento b como $b = c + ka$, para alguna $c \in C$ y $k \in \mathbb{Z}$. Más aún, $(k, p) = 1$, pues de lo contrario, si $p \mid k$, entonces $k = ps$ para alguna $s \in \mathbb{Z}$. Esto implicaría que $b = c + ka = c + s(pa) \in C$, contradiciendo la hipótesis de $B \cap C = \{0\}$. Por lo tanto, existen r y s tales que $rk + sp = 1$, con lo cual

$$a = rka + spa = r(b - c) + spa = rb + (spa - rc).$$

Como $pa \in C$, se sigue que $spa - rc \in C$, demostrando así que $a \in B \oplus C$. □

Lema 4.2.8. *Sean B un subgrupo de A y C un subgrupo B-alto de A. Entonces $A = B \oplus C$ si y sólo si, siempre que $pa = b + c$ con $a \in A$, $b \in B$ y $c \in C$ implique que $b = pb'$ para alguna $b' \in B$.*

Demostración. $\Longrightarrow$) Supongamos que $A = B \oplus C$ y que $pa = b + c$. Si $a = b' + c'$ con $b' \in B$ y $c' \in C$, entonces

$$b + c = pa = pb' + pc'.$$

Por ser A la suma directa de B y de C, la expresión de cada elemento es única, de donde se sigue que $b = pb'$.

($\Longleftarrow$ Supongamos ahora que, para cualquier primo p, cada vez que se cumpla $pa = b + c$, se tiene que $b = pb'$ para algún $b' \in B$. Bajo estas hipótesis, el elemento $a - b'$ satisface las condiciones del lema anterior. En efecto,

$$p(a - b') = pa - pb' = (b + c) - b = c \in C,$$

teniendo así que $a - b' \in A \oplus B$. Como $B \oplus C$ es un subgrupo de A y $b' \in B \oplus C$, se sigue que $a = (a - b') + b' \in B \oplus C$. Notemos que esto implica que el grupo cociente $A/(B \oplus C)$ no tiene elementos de orden el primo p. En caso de que $p(a + B \oplus C) \in B \oplus C$, se sigue que $pa = b + c$ con $b \in B$ y $c \in C$. Por hipótesis, esto implica que $b = pb'$ y por el lema anterior se tiene que $a - b' \in B \oplus C$, con lo cual $a \in B \oplus C$. Más aún, $A/(B \oplus C)$ no tiene elementos de orden finito. En efecto, en caso de tener uno, tendría un elemento de orden primo. Por lo tanto, $A/(B \oplus C)$ es un grupo libre de torsión.

Por otra parte, si $x \in A$ es cualquier elemento, por la elección de C, se tiene que el subgrupo $< C, x >$ interseca a B en un elemento b'' distinto de cero. Al elemento b'' lo podemos escribir de la forma $b'' = c'' + lx$. Nótese que $l \neq 0$, pues $B \cap C = \{0\}$ y $b'' \neq 0$. Por lo tanto,

$$lx = b'' - c'' \in B \oplus C.$$

Esto último muestra que cualquier elemento $x + B \oplus C$, en el grupo $A/(B \oplus C)$, tiene orden finito, por lo que $A/(B \oplus C)$ es también un grupo de torsión.

Por lo tanto, la única manera en que el grupo $A/(B \oplus C)$ sea tanto un grupo de torsión, como un grupo libre de torsión, es cuando $A/(B \oplus C) = 0$, lo cual nos lleva a que $A = B \oplus C$. $\square$

Capítulo 5

Límites Directos

5.1. Definición

Definición 5.1.1. *Sean* $\{A_i\}_{i\in I}$ *una familia de grupos abelianos e* I *un conjunto parcialmente ordenado, dirigido superiormente, tal que para cualquier par de elementos* $i, j \in I$*, con* $i \leq j$*, existen homomorfismos* $\pi_i^j : A_i \longrightarrow A_j$ *que satisfacen las siguientes condiciones*

1. $\pi_i^i : A_i \longrightarrow A_i$ *es la identidad* $\forall i \in I$.
2. $\pi_i^k = \pi_j^k \circ \pi_i^j$*, para* $i \leq j \leq k$*, esto es,*

$$\pi_i^k : A_i \xrightarrow{\pi_i^j} A_j \xrightarrow{\pi_j^k} A_k.$$

En tal caso, diremos que el par $\{\{A_{i\in I}\}, \{\pi_i^j\}_{i\leq j}\}$ *forma un sistema dirigido.*

Si $\{\{A_{i\in I}\}, \{\pi_i^j\}_{i\leq j}\}$ es un sistema dirigido, consideremos a la suma directa $A = \oplus_{i\in I} A_i$, de los grupos A_i que conforman al sistema dirigido. Así, el grupo A contiene un subgrupo B, el cual está generado por todos los elementos de la forma $a_i - \pi_i^j(a_i)$ con $i \leq j$.

Proposición 5.1.2. *Todo elemento del subgrupo* B *es de la forma*

$$a = a_{i_1} + a_{i_2} + \cdots + a_{i_n},$$

donde $a_{i_j} \in A_{i_j}$*. Además, para cualquier* $i \in I$ *con* $i \geq i_1, i_2, \ldots, i_n$*, se cumple que*

$$\pi^i_{i_1}(a_{i_1}) + \pi^i_{i_2}(a_{i_2}) + \cdots + \pi^i_{i_n}(a_{i_n}) = 0.$$

Demostración. Sean a un elemento de la forma $a = a_{i_1} + a_{i_2} + \cdots + a_{i_n}$ e $i \geq i_1, i_2, \ldots, i_n$. Como $\pi^i_{i_1}(a_{i_1}) + \pi^i_{i_2}(a_{i_2}) + \cdots + \pi^i_{i_n}(a_{i_n}) = 0$ entonces

$$\begin{aligned} a = a - 0 = a_{i_1} + a_{i_2} + \cdots + a_{i_n} - (\pi^i_{i_1}(a_{i_1}) + \pi^i_{i_2}(a_{i_2}) + \cdots + \pi^i_{i_n}(a_{i_n})) \\ = (a_{i_1} - \pi^i_{i_1}(a_{i_1})) + \cdots + (a_{i_n} - \pi^i_{i_n}(a_{i_n})) \end{aligned}$$

el cual es un elemento en B, ya que cada diferencia es un generador.

Por otra parte, notemos que cada elemento generador de B cumple la propiedad. En efecto, si $a = a_i - \pi^j_i(a_i) \in B$, para $j \geq i$ (o $i \leq j$) se tiene

$$\pi^j_i(a) = \pi^j_i(a_i) - \pi^j_j(\pi^j_i(a_i)) = \pi^j_i(a_i) - \pi^j_i(a_i) = 0,$$

Así, como todo elemento de B es una suma finita de generadores y A es un sistema dirigido, podemos dar una k suficientemente grande tal que, si $a' \in B$ es de la forma

$$a' = (a_{i_1} - \pi^{j_1}_{i_1}(a_{i_1})) + \cdots + (a_{i_n} - \pi^{j_n}_{i_n}(a_{i_n}))$$

y $k \geq i_1, \ldots, i_n, j_1, \ldots, j_n$ entonces

$$\begin{aligned} (\pi^k_{i_1}(a_{i_1}) - \pi^k_{j_1}(\pi^{j_1}_{i_1}(a_{i_1})) + \cdots + (\pi^k_{i_n}(a_{i_n}) - \pi^k_{j_n}(\pi^{j_n}_{i_n}(a_{i_n})) \\ = \pi^k_{i_1}(a_{i_1}) - \pi^k_{i_1}(a_{i_1}) + \cdots + \pi^k_{i_n}(a_{i_n}) - \pi^k_{i_n}(a_{i_n}) = 0 \end{aligned}$$

□

Definición 5.1.3. *El límite directo del sistema dirigido* $\{\{A_{i\in I}\}, \{\pi^j_i\}_{i\leq j}\}$ *está definido por el cociente de los grupos* $A = \oplus_{i\in I} A_i$ *y* B*, esto es:*

$$\varinjlim A_i = \oplus_{i\in I} A_i / B = A_*$$

.

5.2. Propiedades

Observación. *Para cada* $i \in I$*, existe un morfismo* $\pi_i : A_i \longrightarrow A_*$ *tal que, para cualquier* j *con* $i \leq j$*, el diagrama*

$$\begin{tikzcd} A_i \arrow[r, "\pi^j_i"] \arrow[d, "\pi_i"'] & A_j \arrow[dl, "\pi_j"] \\ A_* & \end{tikzcd}$$

conmuta. Esto se sigue notando que, como $a_i - \pi^j_i(a_i) \in B$ *entonces*

$$a_i + B = \pi_i^j(a_i) + B.$$

Al morfismo $\pi_i : A_i \longrightarrow A_*$ con regla de correspondencia $a_i \longmapsto a_i + B$, se le conoce como el morfismo canónico.

Veremos ahora que todo elemento $a_* \in A_*$ está representado por una clase en A/B de la forma $a_j + B$, con $a_j \in A_j$. Cualquier $a_* \in A/B$ es de la forma $a_* = a + B$, donde $a = a_{i_1} + a_{i_2} + \cdots + a_{i_n}$, y $a_{i_m} \in A_{i_m}$ para $m = 1, \ldots, n$. Con esto en cuenta, podemos escoger una $j \geq i_1, \ldots, i_n$ de manera que

$$a - \Sigma_{m=1}^n \pi_{i_m}^j(a_{i_m}) \in B,$$

ya que esto último es igual a

$$a_{i_1} - \pi_{i_1}^j(a_{i_1}) + \cdots + a_{i_n} - \pi_{i_n}^j(a_{i_n}) \in B.$$

Esto implica que $a + B = \Sigma_{m=1}^n \pi_{i_m}^j(a_{i_m}) + B$, por lo que al definir a a_j como la suma $\Sigma_{m=1}^n \pi_{i_m}^j(a_{i_m}) \in A_j$, se tiene que

$$a_* = a + B = a_j + B.$$

Nótese que la j elejida no es única. De hecho, cualquier $j \geq i_1, \ldots, i_n$ cumple lo anterior.

Observación. *Por la manera en que se definió a cada $\pi_i : A_i \longrightarrow A_*$, y que cada elemento $a_* \in A_*$ es de la forma $a_j + B$, para algún $a_j \in A_j$, se tiene que el conjunto de grupos $Im(\pi_i)$, con $i \in I$, cubre a A_*.*

Notemos también que si $\pi_i(a_i) = 0$, para alguna $a_i \in A_i$, entonces $a_i \in B$. En efecto, por la Proposición 5.1.2, para cualquier $j \geq i$, se cumple que $\pi_i^j(a_i) = 0$. Como consecuencia, se tiene la siguiente

Observación. *Si π_i^j es un monomorfismos para toda $i, j \in I$, con $i \leq j$, entonces π_i es también un monomorfismos, $\forall i \in I$.*

Observación. *Análogamente, si π_i^j es un epimorfismo $\forall i \leq j$, entonces π_i también lo es, para toda $i \in I$. En efecto, hemos visto que cualquier $a_* \in A_*$ está representado por alguna clase de la forma $a_j + B$, para algún $j \in I$, y $a_j \in A_j$. Esto último implica que $\pi_j(a_j) = a_*$. Ahora, dado cualquier morfismo π_i, existe $k \in I$, con $i, j \leq k$, para la cual los siguientes diagramas conmutan*

$$\begin{tikzcd} A_i \arrow[d, "\pi_i^k"'] \arrow[dr, "\pi_i"] & \\ A_k \arrow[r, "\pi_k"'] & A_* \end{tikzcd} \quad y \quad \begin{tikzcd} A_j \arrow[d, "\pi_j^k"'] \arrow[dr, "\pi_j"] & \\ A_k \arrow[r, "\pi_k"'] & A_* \end{tikzcd}$$

Como por hipótesis $\pi_i^k : A_i \longrightarrow A_k$ es suprayectiva y $\pi_j^k(a_j) \in A_k$, existe $a_i \in A_i$ tal que $\pi_i^k(a_i) = \pi_j^k(a_j)$. Esto implica que

$$a_* = \pi_j(a_j) = \pi_k(\pi_j^k(a_j)) = \pi_k(\pi_i^k(a_i)) = \pi_i(a_i) \in Im\pi_i$$

teniendo así que cada π_i es un epimorfismo.

Los límites directos cumplen una propiedad universal en el siguiente sentido:

Teorema 5.2.1. *El límite directo A_* del sistema dirigido $\{\{A_{i\in I}\}, \{\pi_i^j\}_{i\leq j}\}$, satisface lo siguiente: si G es cualquier otro grupo para el cual existen morfismos $\sigma_i : A_i \longrightarrow G$ tales que, para cada $i \leq j$, los diagramas*

$$\begin{tikzcd} A_i \arrow[d, "\pi_i^j"'] \arrow[dr, "\sigma_i"] & \\ A_j \arrow[r, "\sigma_j"'] & G \end{tikzcd} \tag{5.1}$$

son conmutativos, entonces existe un único morfismo $\sigma : A_* \longrightarrow G$ tal que todos los diagramas de la forma

$$\begin{tikzcd} A_i \arrow[d, "\pi_i"'] \arrow[dr, "\sigma_i"] & \\ A_* \arrow[r, "\sigma"'] & G \end{tikzcd}$$

conmutan. El grupo A_*, junto con los morfismos π_i, están determinados por esta propiedad, salvo isomorfismos.

Demostración. Sean G un grupo y $\{\sigma_i\}_{i\in I}$ una familia de morfismos tales que hacen de los diagramas (5.1) conmutativos. Por lo notado anteriormente, si $a_* \in A_*$, entonces $a_* = a_i + B$, para alguna $a_i \in A_i$ e $i \in I$. La conmutatividad de los diagramas (5.1) hacen que la función $\sigma : A_* \longrightarrow G$ con regla de correspondencia $\sigma(a_*) = \sigma_i(a_i)$ esté bien definida. En efecto, si $a_* = a + B$ con $a = a_{i_1} + \cdots + a_{i_n}$, $i_1, \ldots, i_n \in I$, para cualquier $i \geq i_1, \ldots, i_n$ se tiene que $a_* = a_i + B$, donde

$$a_i = \pi_{i_1}^i(a_{i_1}) + \cdots + \pi_{i_n}^i(a_{i_n}) \in A_i.$$

Ahora, si $j \geq i$, entonces

$$\pi_i^j(a_i) = \pi_i^j[\pi_{i_1}^i(a_{i_1}) + \cdots + \pi_{i_n}^i(a_{i_n})] = \pi_{i_1}^j(a_{i_1}) + \cdots + \pi_{i_n}^j(a_{i_n}),$$

donde $\pi_{i_1}^j(a_{i_1}) + \cdots + \pi_{i_n}^j(a_{i_n}) = a_j$ satisface que $a_j + B = a_*$. Como los diagramas (5.1) conmutan, se tiene que

$$\sigma_i(a_i) = \sigma_j(\pi_i^j(a_i)) = \sigma_j(a_j).$$

Veamos ahora que σ abre sumas. Sean $a_*, c_* \in A_*$ dos elementos tales que $a_* = a + B$ con $a = a_{i_1} + \cdots + a_{i_n}$ y $a_{i_s} \in A_{i_s}$ para $s \in \{1, \ldots, n\}$, así como $c_* = c + B$ con $c = c_{j_1} + \cdots + c_{j_m}$ y $c_{j_r} \in A_{j_r}$ para cada $r \in \{1, \ldots, m\}$. Con esto en cuenta, para cualquier $l \geq i_1, \ldots, i_n, j_1, \ldots, j_m$, se satisface que

$$a_* = a_l + B \text{ y } c_* = c_l + B, \text{ y } a_l, c_l \in A_l.$$

Ahora, por ser π_l y σ_l morfismos, como $l \geq i_1, \ldots, i_n$ y $l \geq j_1, \ldots, j_m$, se sigue del diagrama

$$\begin{tikzcd} A_l \arrow[r, "\sigma_l"] \arrow[d, "\pi_l"'] & G \\ A_* \arrow[ur, "\sigma"'] & \end{tikzcd}$$

que

$$\sigma(a_* + c_*) = \sigma_l(a_l) + \sigma_l(c_l).$$

Así, como σ preserva la suma, σ es un morfismo tal que

$$\sigma \circ \pi_i(a_i) = \sigma(a_*) = \sigma_i(a_i),$$

lo cual equivale a decir que, para cada $i \in I$, el diagrama

$$\begin{tikzcd} A_i \arrow[r, "\sigma_i"] \arrow[dr, "\pi_i"'] & G \\ & A_* \arrow[u, "\sigma"'] \end{tikzcd}$$

conmuta.

Supongamos ahora que $\eta : A_* \longrightarrow G$ es un morfismo tal que hace conmutativos a los diagramas de la forma

$$\begin{tikzcd} A_i \arrow[r, "\sigma_i"] \arrow[dr, "\pi_i"'] & G \\ & A_* \arrow[u, "\eta"'] \end{tikzcd}$$

para cada $i \in I$. Observemos que para toda $a_i \in A_i$ e $i \in I$,

$$(\sigma - \eta)(\pi_i(a_i)) = \sigma(\pi_i(a_i)) - \eta(\pi_i(a_i)) = \sigma_i(a_i) - \sigma_i(a_i) = 0.$$

Esto quiere decir que el morfismo $\sigma - \eta$ manda a cada $Im(\pi_i)$ al elemento 0. Como el conjunto de imágenes $Im(\pi_i)$ cubre a A_*, se tiene que

$$(\sigma - \eta)(A_*) = 0,$$

es decir, $\sigma = \eta$. Por lo tanto, σ es única.

Veamos ahora la segunda afirmación. Supongamos que el grupo A_0 y los morfismos $\tau_i : A_i \longrightarrow A_0$ tienen la propiedad mencionada, es decir, si G es un grupo para el cual existen morfismos $\sigma_i : A_i \longrightarrow G$ que hacen conmtativos a los diagramas

$$\begin{tikzcd} A_i \arrow[r, "\pi_i^j"] \arrow[dr, "\sigma_i"'] & A_j \arrow[d, "\sigma_j"] \\ & G \end{tikzcd}$$

para cada $i \leq j$, entonces se tiene un único morfismo $\tau : A_0 \longrightarrow G$ tal que los diagramas

$$\begin{tikzcd} A_i \arrow[r, "\sigma_i"] \arrow[dr, "\tau_i"'] & G \\ & A_0 \arrow[u, "\tau"'] \end{tikzcd}$$

conmutan $\forall i \in I$.

Ahora, por la conmutatividad de los diagramas

$$\begin{tikzcd} A_i \arrow[r, "\pi_i^j"] \arrow[dr, "\pi_i"'] & A_j \arrow[d, "\pi_j"] \\ & A_* \end{tikzcd}$$

y por cumplir A_0 y $\{\tau_i\}_{i \in I}$ las hipótesis, tenemos para cualquier $i \in I$, los diagramas

$$\begin{tikzcd} A_i \arrow[r, "\pi_i"] \arrow[dr, "\tau_i"'] & A_* \\ & A_0 \arrow[u, "\tau"'] \end{tikzcd}$$

conmutan, por lo que $\pi_i = \tau \circ \tau_i$, $\forall i \in I$.

Por otra parte, como A_* también cumple la propiedad universal, se tiene un único morfismo $\sigma : A_* \longrightarrow A_0$ tal que los diagramas de la forma

$$\begin{tikzcd} A_i \arrow[r, "\tau_i"] \arrow[dr, "\pi_i"'] & A_0 \\ & A_* \arrow[u, "\sigma"'] \end{tikzcd}$$

son conmutativos para cada $i \in I$, de donde se sigue que $\tau_i = \sigma \circ \pi_i$. De estas dos últimas igualdades, se obtiene que

$$\pi_i = \tau \circ \tau_i = \tau \circ (\sigma \circ \pi_i) = (\tau \circ \sigma) \circ \pi_i$$

así como

$$\tau_i = \sigma \circ \pi_i = \sigma \circ (\tau \circ \tau_i) = (\sigma \circ \tau) \circ \tau_i,$$

para toda $i \in I$. Esto quiere decir que la función $\tau \circ \sigma : A_* \longrightarrow A_*$ satisface $\tau \circ \sigma(\pi_i(A_i)) = \pi_i(A_i)$ para cada $i \in I$. Como el conjunto $\{\pi_i(A_i)\}_{i \in I}$, con $i \in I$, cubre en su totalidad al límite directo A_*, se tiene que $\tau \circ \sigma = id_{A_*}$. Esto implica que σ es inyectiva.

Por ser σ una función inyectiva, la sucesión

$$0 \hookrightarrow A_* \xrightarrow{\sigma} A_0 \xrightarrow{\rho} A_0/\sigma(A) \longrightarrow 0$$

es una sucesión exacta corta y además, $\tau : A_0 \longrightarrow A_*$ es tal que $\tau \circ \sigma = id_{A_*}$. Por la Proposición 4.2.3, se tiene que $\sigma(A_*)$ es un sumando directo de A_0, con lo cual, $A_0 = \sigma(A_*) \oplus C$ donde $C \cong A_0/\sigma(A)$ y $\rho\mid_C : C \longrightarrow A_0/\sigma(A_0)$ es un isomorfismo. La unicidad del sistema $\{A_0, \{\tau_i\}_{\in I}\}$, implica que $C = 0$, teniendo así que $\sigma(A_*) = A_0$. Por lo tanto, σ es un isomorfismo entre A_* y A_0. $\square$

5.3. Ejemplos

Ejemplo. *Consideremos un grupo A junto con todos sus subgrupos finitamente generados a los cuales denotaremos por A_i, con i en el conjunto de índices I. Si definimos la relación $\leq$ en I por $i \leq j$ si y sólo si A_i es un subgrupo de A_j, tenemos que I es un conjunto parcialmente ordenado por $\leq$. Más aún, si $\pi_i^j : A_i \longrightarrow A_j$ son las inclusiones para $i \leq j$, entonces $\{\{A_{i\in I}\}, \{\pi_i^j\}_{i\leq j}\}$ es un sistema directo. Afirmamos que*

$$\varinjlim A_i = A_* \cong A.$$

Para cada $i \in I$, si $\iota_i : A_i \hookrightarrow A$ es la inclusión de A_i en A, se cumple que los diagramas de la forma

$$\begin{tikzcd} A_i \arrow[r, "\pi_i^j"] \arrow[dr, "\iota_i"'] & A_j \arrow[d, "\iota_j"] \\ & A \end{tikzcd}$$

son conmutativos $\forall i \leq j$. Así existe un único morfismo $\sigma : A_* \longrightarrow A$ tal que los diagramas

$$\begin{tikzcd} A_i \arrow[r, "\pi_i"] \arrow[dr, "\iota_i"'] & A_j \arrow[d, "\sigma"] \\ & A \end{tikzcd}$$

conmutan, para cada $i \in I$, donde $\pi_i : A_i \longrightarrow A_*$ es el morfismo canónico. Con esto en cuenta, se tiene que $\sigma \circ \pi_i = \iota_i$ para toda $i \in I$.

Notemos ahora que cada $a \in A$ tiene asignado un subgrupo menor finitamente generado, a saber, el subgrupo $< a >$. Si a este subgrupo lo denotamos por A_k, para alguna $k \in I$, afirmamos que la función

$$\varphi : A \longrightarrow A_*$$

definida por $a \longmapsto \pi_k(a)$ es un morfismo. Observemos primero que, para cada $a \in A$ el subgrupo $< a >$ es único, por lo que la función φ está bien definida. Sean $a, b, a+b \in A$ y $< a >= A_k$, $< b >= A_l$ y $< a+b >= A_n$ para $k, l, n \in I$. Así, $< a, b >$ es un elemento de nuestro conjunto de subgrupos de A finitamente generados, por lo que también tiene asignado un A_m. Nótese que

$$< a >, < b >, < a+b > \subset < a, b >,$$

teniendo así que $k, l, n \leq m$. Con esto en cuenta, se tienen los siguientes diagramas conmutativos

$$\begin{tikzcd} A_n \arrow[r, "\pi_n^m"] \arrow[d, "\pi_n"'] & A_m \arrow[dl, "\pi_m"] \\ A_* \end{tikzcd}, \quad \begin{tikzcd} A_l \arrow[r, "\pi_l^m"] \arrow[d, "\pi_l"'] & A_m \arrow[dl, "\pi_m"] \\ A_* \end{tikzcd}, \quad y \quad \begin{tikzcd} A_k \arrow[r, "\pi_k^m"] \arrow[d, "\pi_k"'] & A_m \arrow[dl, "\pi_m"] \\ A_* \end{tikzcd}.$$

Como las funciones π_n^m, π_l^m, y π_k^m son las inclusiones entre los subgrupos correspondientes, del primer diagrama se obtiene

$$\pi_n(a+b) = \pi_m \circ \pi_n^m(a+b) = \pi_m(a+b) = \pi_m(a) + \pi_m(b),$$

pues π_m es un morfismo. Por otra parte, del segundo y tercer diagrama, se sigue que

$$\pi_l(b) = \pi_m \circ \pi_l^m(b) = \pi_m(b) \text{ y } \pi_k(a) = \pi_m \circ \pi_k^m(a) = \pi_m(a),$$

respectivamente. Por lo tanto, $\pi_m(a) = \pi_k(a)$ y $\pi_m(b) = \pi_l(b)$, por lo que

$$\varphi(a+b) = \pi_n(a+b) = \pi_m(a) + \pi_m(b) = \pi_k(a) + \pi_l(b) = \varphi(a) + \varphi(b).$$

Finalmente, veamos que σ y φ son funciones inversas. Si $a \in A$, entonces existe un $k \in I$ tal que $< a >= A_k$. Así, como $\sigma \circ \pi_k = \iota_k$, donde $\iota_k : A_k \hookrightarrow A$ es la función inclusión, se tiene que

$$\sigma \circ \varphi(a) = \sigma(\pi_k(a)) = \sigma \circ \pi_k(a) = \iota_k(a) = a,$$

es decir, $\sigma \circ \varphi = id_A$. Para demostrar que $\varphi \circ \sigma = Id_{A_*}$, observemos que, como cada $a_* \in A_*$ tiene la forma $a_j + B$ con $a_j \in A_j$, para alguna $j \in I$, se cumple que $a_* = \pi_j(a_j)$. Ahora, como los diagramas de la forma

$$\begin{tikzcd} A_j \arrow[r, "\pi_j"] \arrow[d, "\iota"'] & A_* \arrow[dl, "\sigma"] \\ A & \end{tikzcd}$$

son conmutativos para cualquier $j \in I$, se sigue que $\sigma(a_*) = a_j$. Así, si $a_* = a_j + B$, con $a_j \in A_j$, entonces $\varphi \circ \sigma(a_*) = \varphi(a_j) = \pi_j(a_j) = a_*$. Por lo tanto, φ y σ son funciones inversas, con lo que $A_* \cong A$

Ejemplo. *Sea $C_n =< c_n >$ el grupo cíclico de orden p^n, con $n = 1, 2, \ldots$. Si $n \leq m$, definimos los morfismos $\pi_n^m : C_n \longrightarrow C_m$ con regla de correspondencia*

$$\pi_n^m(b_n) = p^{(m-n)} b_m.$$

Esto nos define el sistema directo $\{\{C_{n \in \mathbb{N}}\}, \{\pi_n^m\}_{n \leq m}\}$, el cual tiene asignado el límite directo C_*.

Por otra parte, notemos que $\mathbb{Z}(p^\infty)$ es un grupo donde todos sus subgrupos propios son finitamente generados y éstos son de la forma $\mathbb{Z}(p^k)$, para alguna $k \in \mathbb{N}$; es decir, los subgrupos de $\mathbb{Z}(p^\infty)$ son grupos cíclicos de orden p^k. Por lo notado y demostrado en el ejemplo anterior, se tiene que

$$C_* \cong \mathbb{Z}(p^\infty).$$

Capítulo 6

Límites Inversos

6.1. Definición

Definición 6.1.1. *Sean* $\{A_i\}_{i\in I}$ *una familia de grupos abelianos e* I *un conjunto parcialmente ordenado, dirigido superiormente, tal que para cualquier par de elementos* $i, j \in I$, *con* $i \leq j$, *existen morfismos* $\pi_i^j : A_j \longrightarrow A_i$ *que satisfacen las siguientes condiciones:*

1. $\pi_i^i : A_i \longrightarrow A_i$ *es la identidad* $\forall i \in I$.

2. $\pi_i^k = \pi_i^j \circ \pi_k^j$, *para* $i \leq j \leq k$, *esto es,*

$$\pi_i^k : A_k \xrightarrow{\pi_k^j} A_j \xrightarrow{\pi_j^i} A_i.$$

En tal caso, diremos que el par $\{\{A_{i\in I}\}, \{\pi_i^j\}_{i\leq j}\}$ *forma un sistema inverso.*

Definición 6.1.2. *El límite inverso del sistema inverso* $\{\{A_{i\in I}\}, \{\pi_i^j\}_{i\leq j}\}$, *que escribimos como*

$$A^* = \underleftarrow{Lím}_I,$$

es el conjunto de coordenadas $(\cdots, a_i, \cdots,)$ *en el producto directo* $\Pi_{i\in I} A_i$, *tales que* $\pi_i^j(a_j) = a_i$, *para cualquier* $i \leq j$.

Observación. *Si denotamos al producto directo* $\Pi_{i\in I} A_i$ *por* A, *se tiene que* A^* *es un subgrupo de* A. *En efecto, si* $a, b \in A^*$, *entonces para cada* $i \leq j$, *las coordenadas tanto de* a *como de* b, *satisfacen que* $\pi_i^j(a_j) = a_i$ *y* $\pi_i^j(b_j) = b_i$, *con lo cual* $\pi_i^j(a_j - b_j) = a_i - b_i$, *para cada* $i \leq j$, *es decir* $a - b \in A^*$.

6.2. Propiedades

Observación. *Para cada $i \in I$, podemos considerar el morfismo canónico $\rho_i : \Pi_{j\in I} A_j \longrightarrow A_i$ que a cada elemento del producto directo, le asigna su coordenada i-ésima. Esto nos permite definir los morfismos*

$$\pi_i = \rho_i \mid_{A^*} : A^* \longrightarrow A_i,$$

para cada $i \in I$. Estos morfismos hacen que los diagramas

$$\begin{tikzcd} A^* \arrow[r, "\pi_i"] \arrow[d, "\pi_j"'] & A_i \\ A_j \arrow[ur, "\pi_i^j"'] & \end{tikzcd}$$

sean conmutativos $\forall i \leq j$, ya que, para cualquier $i \leq j$, si

$$a = (\cdots, a_i, \ldots, a_j, \cdots) \in A^*,$$

entonces $\pi_i^j(a_j) = a_i$, por lo que

$$\pi_i^j \circ \pi_j(a) = \pi_i^j(a_j) = a_i = \pi_i(a).$$

Observación. *Si todo morfismo π_i^j, con $i \leq j$, es inyectivo, entonces π_i es un monomorfismo para cualquier $i \in I$. En efecto, supongamos que cada π_i^j es una función inyectiva y que $\pi_i(a) = 0$, para alguna $a \in A^*$. Dada cualquier $j \in I$, podemos escoger $k \in I$ tal que $i, j \leq k$. Ahora, como $i \leq k$, entonces el diagrama*

$$\begin{tikzcd} A^* \arrow[r, "\pi_i"] \arrow[d, "\pi_k"'] & A_i \\ A_k \arrow[ur, "\pi_i^k"'] & \end{tikzcd}$$

conmuta, por lo que

$$\pi_i^k \circ \pi_k(a) = \pi_i(a) = 0.$$

Por ser π_i^k una función inyectiva, se sigue que $\pi_k(a) = 0$. Por otra parte, como también $j \leq k$, se tiene el diagrama conmutativo

$$\begin{tikzcd} A^* \arrow[r, "\pi_j"] \arrow[d, "\pi_k"'] & A_j \\ A_k \arrow[ur, "\pi_j^k"'] & \end{tikzcd}$$

de donde se concluye que

$$\pi_j(a) = \pi_j^k \circ \pi_k(a) = \pi_j^k(0) = 0.$$

Como este argumento es para cualquier $j \in I$, tenemos que la coordenada j-ésima de a es 0, es decir, $a = 0$.

Observación. *Para cada $i, j \in I$, con $i \leq j$, podemos definir el endomorfismo*

$$\theta_{i,j} : \Pi_{\alpha \in I} A_\alpha \longrightarrow \Pi_{\alpha \in I} A_\alpha$$

dado por

$$(\cdots, a_i, \ldots, a_j, \cdots) \longmapsto (\cdots, 0, a_i - \pi_i^j(a_j), 0, \cdots),$$

es decir, donde a lo más la i-ésima coordenada no es cero. Al comparar esto último con la definición de límites inversos, podemos ver que

$$\cap_{i,j} Ker(\theta_{i,j}) = A^*,$$

donde i, j corren sobre todas las parejas en I tales que $i \leq j$. En efecto, si $a \in A^*$, con $a = (\cdots, a_i, \ldots, a_j, \cdots)$ e $i \leq j$, se tiene que $a_i = \pi_i^j(a_j)$. Esto implica que $a_i - \pi_i^j(a_j) = 0$, siempre que $i \leq j$, por lo que

$$\begin{aligned} \theta_{i,j}(a) = \theta_{i,j}(\cdots, a_i, \ldots, a_j, \cdots) &= (0, \ldots, a_i - \pi_i^j(a_j), 0, \cdots) \\ &= (0, \ldots, 0, \ldots), \end{aligned}$$

es decir, $a \in Ker(\theta_{i,j})$. Como este argumento fue $\forall i \leq j$, se sigue que

$$a \in \cap Ker(\theta_{i,j}).$$

Por otra parte, si $a \in \cap Ker(\theta_{i,j})$, al fijar una $i \in I$, se cumple que cualquier $j \geq i$ satisface que la coordenada i-ésima de $\theta_{i,j}(a)$ es $a_i - \pi_i^j(a_j) = 0$, por lo que $a \in A^*$.

Proposición 6.2.1. *Sea un sistema inverso $\{\{A_{i \in I}\}, \{\pi_i^j\}_{i \leq j}\}$ tal que cada A_i es un grupo topológico T_2 y donde cada π_i^j es un morfismo continuo. Entonces, el límite inverso del sistema es un subgrupo cerrado en el producto directo $\Pi_{i \in I} A_i$, dotado por la topología producto, y donde cada proyección $\pi_i : A^* \longrightarrow A_i$ es una función continua.*

Demostración. Notemos primero que al dotar con la topología producto a $\Pi_{i\in I}A_i$, cada proyección $\rho_j : \Pi_{i\in I}A_i \longrightarrow A_j$ es continua. Ahora, si $(\cdots, a_i, \cdots) \in \Pi_{i\in I}A_i$ no está en en A^*, entonces existe $i < j$ tal que $a_i \neq \pi_i^j(a_j)$. Como cada espacio es Hausdorff, existen abiertos ajenos, U y V en A_i, tales que $a_i \in U$ y $\pi_i^j(a_j) \in V$. Como las proyecciones $\rho_i : \Pi_{i\in I}A_i \longrightarrow A_i$ son funciones continuas, $(\rho_i)^{-1}(U)$ es un abierto en $\Pi_{i\in I}A_i$.

Por otra parte, como V es un abierto en A_i y $\pi_i^j : A_j \longrightarrow A_i$ es una función continua, $Z = (\pi_i^j)^{-1}(V)$ es un abierto en A_j. Con esto en cuenta, $(\rho_j)^{-1}(Z)$ es un abierto en $\Pi_{i\in I}A_i$, con lo cual, el conjunto $W = (\rho_i)^{-1}(U) \cap (\rho_j)^{-1}(Z)$ es un abierto en $\Pi_{i\in I}A_i$. Más aún,

$$W = \{(\cdots, b_i, \cdots, b_j, \cdots) \in \Pi_{i\in I}A_i \mid b_i \in U \text{ y } \pi_i^j(a_j) \in V\},$$

de donde se sigue que $(\cdots, a_i, \cdots) \in W$. Además, como todo

$$(\cdots, b_i, \cdots, b_j, \cdots) \in W$$

cumple que $b_i \in U$ y $\pi_i^j(b_j) \in V$, por ser U y V ajenos, se tiene que $b_i \neq \pi_i^j(b_j)$, es decir, $A^* \cap W = \varnothing$. Esto muestra que el conjunto $\Pi_{i\in I}A_i \setminus A^*$ es un conjunto abierto en $\Pi_{i\in I}A_i$, ya que todo elemento $(\cdots, a_i, \cdots) \in \Pi_{i\in I}A_i \setminus A^*$ tiene un abierto que lo contiene y es ajeno a A^*. De esta manera, A^* es un conjunto cerrado.

Como cada proyección $\rho_i : \Pi_{i\in I}A_i \longmapsto A_i$ es continua, satisface que si F es un cerrado en A_i, entonces $(\rho_i)^{-1}(F)$ es un cerrado. De esta manera, para cualquier cerrado F en A_i,

$$(\pi_i)^{-1}(F) = A^* \cap (\rho_i)^{-1}(F),$$

con lo cual $(\pi_i)^{-1}(F)$ resulta ser cerrado por ser una intersección finita de cerrados. Por lo tanto, cada π_i es una función continua. $\square$

Por otra parte, al igual que los límites directos, los límites inversos tienen la siguiente propiedad universal:

Teorema 6.2.2. *El límite inverso A^* del sistema inverso $\{\{A_{i\in I}\}, \{\pi_i^j\}_{i\leq j}\}$ satisface la siguiente propiedad: si G es un grupo para el cual existen morfismos $\sigma_i : G \longrightarrow A_i$ tales que, para cada $i \leq j$ los diagramas*

$$\begin{tikzcd} G \arrow[r, "\sigma_j"] \arrow[dr, "\sigma_i"'] & A_j \arrow[d, "\pi_i^j"] \\ & A_i \end{tikzcd} \tag{6.1}$$

son conmutativos, entonces existe un único morfismo $\sigma : G \longrightarrow A^*$ *tal que los diagramas*

$$\begin{tikzcd} G \arrow[r, "\sigma"] \arrow[dr, "\sigma_i"'] & A^* \arrow[d, "\pi_i"] \\ & A_i \end{tikzcd} \tag{6.2}$$

conmutan para cada $i \in I$*. Esta propiedad es única salvo por isomorfismos.*

Demostración. Sean G un grupo y $\sigma_i : G \longrightarrow A_i$ una familia de morfismos tales que, los diagramas de la forma (6.1), son conmutativos para toda $i \leq j$. Definimos la función $\sigma : G \longrightarrow \Pi_{i\in I} A_i$ por

$$\sigma(g) = (\cdots, \sigma_i(g), \cdots, \sigma_k(g), \cdots) \in \Pi_{i\in I} A_i,$$

es decir, $\sigma(g)$ es el elemento en el producto directo $\Pi_{i\in I} A_i$ tal que la coordenada i-ésima de $\sigma(g)$ es $\sigma_i(g)$. Como los diagramas de la forma (6.1) conmutan para toda $i \leq j$, se sigue que

$$\sigma_i(g) = \pi_i^j(\sigma_j(g)), \ \forall i \leq j,$$

lo cual muestra que $\sigma(g) \in A^*$. Además, $\sigma : G \longrightarrow A^*$ es un morfismo ya que, por ser cada σ_i un morfismo, se satisface que

$$\begin{gathered} \sigma(g_1 + g_2) = (\cdots, \sigma_i(g_1 + g_2), \cdots, \sigma_k(g_1 + g_2), \cdots) \\ = (\cdots, \sigma_i(g_1) + \sigma_i(g_2), \cdots, \sigma_k(g_1) + \sigma_k(g_2), \cdots) \\ = (\cdots, \sigma_i(g_1), \cdots, \sigma_k(g_1), \cdots) + (\cdots, \sigma_i(g_2), \cdots, \sigma_k(g_2), \cdots) \\ = \sigma(g_1) + \sigma(g_2). \end{gathered}$$

Por otra parte, para cada $g \in G$ e $i \in I$ se cumple que $\pi_i(\sigma(g)) = \sigma_i(g)$, es decir, los diagramas de la forma (6.2) conmutan para cualquier $i \in I$.

Supongamos ahora que $\sigma' : G \longrightarrow A^*$ es otro morfismo que hace conmutativo a los diagramas de la forma (6.2). Así, para cada $g \in G$, se tiene que

$$\pi_i(\sigma'(g)) = \sigma_i(g) = \pi_i(\sigma(g)),$$

lo cual quiere decir que

$$\pi_i \circ (\sigma - \sigma'(g)) = 0,$$

para toda $i \in I$. Esto muestra que $\sigma_i(g) = \sigma_i'(g)$. Como éstos valores son los términos i-ésimos de $\sigma(g)$ y $\sigma'(g)$, respectivamente, se sigue que $\sigma(g) = \sigma'(g)$, por lo que σ es única.

Sean A_0 un grupo y $\{\tau_i\}_{i\in I}$ una familia de morfismos que cumplen las propiedades mencionadas. Con esto en cuenta, se tienen dos únicos morfismos $\sigma : A_0 \longrightarrow A^*$ y $\sigma_0 : A^* \longrightarrow A_0$ tales que, para cada $i \in I$, se cumple que $\tau_i = \pi_i \circ \sigma$, así como $\pi_i = \tau_i \circ \sigma_0$. Esto nos lleva a que $\pi_i = \pi_i \circ (\sigma \circ \sigma_0)$ para cada $i \in I$, por lo que $\sigma \circ \sigma_0$ se comporta como la identidad en A^*. Como $\sigma \circ \sigma_0 = id_{A^*}$, σ_0 es inyectiva, por lo que la sucesión

$$0 \hookrightarrow A_0 \xrightarrow{\sigma_0} A^* \xrightarrow{\rho} (A/ker(\sigma_0)) \longrightarrow 0$$

es exacta corta. Además, por la Proposición 4.2.3, se sigue que el grupo $\sigma_0(A^*)$ es un sumando directo de A_0. La unicidad del morfismo $G \longrightarrow A_0$, para cualquier grupo G, implica que $\sigma_0(A^*) = A_0$, con lo cual A_0 y A^* son isomorfos. $\square$

Capítulo 7

Grupos Topológicos

7.1. Definición

El Axioma de Elección nos asegura que el producto cartesiano $\Pi_{i\in I}X_i$ es no vacío si cada conjunto X_i es distinto del vacío. De esta manera, si $\{X_i\}_{i\in I}$ es una familia de conjuntos y $\Pi_{i\in I}X_i$ su producto cartesiano, se tienen de manera natural las funciones proyecciones $\pi_j : \Pi_{i\in I}X_i \longrightarrow X_j$ para cada $j \in I$. Notemos que las definiciones de producto cartesiano para grupos y para conjuntos coinciden. Ahora, si cada X_i es un espacio topológico, podemos dotar al producto cartesiano de una topología τ_p, que haga a cada proyección una función continua. Esta topología tiene como sub-base al los conjuntos de la forma $\pi_\alpha^{-1}(U)$, donde U es un abierto en X_α. A esta topología se le conoce como la *topología producto*. Nótese que la topología producto es la topología más chica en el producto cartesian $\Pi_{i\in I}X_i$ que hace a cada proyección continua. En efecto, si τ es una topología en $\Pi_{i\in I}X_i$ para la cual cada proyección es continua, entonces por definición, τ contiene a los conjuntos de la forma $\pi_\alpha^{-1}(U)$ para cualquier abierto U en X_α, y cualquier $\alpha \in I$. Obsérvese que los abiertos básicos en τ_c son de la forma

$$\Pi_{i\in I}U_i,$$

donde $U_i = X_i$, salvo para una cantidad finita.

Otra topología en el producto cartesiano se obtiene al considerar los conjuntos de la forma $\Pi_{\alpha\in I}U_\alpha$, donde U_α es un abierto en X_α. A esta topología se le conoce como la *topología caja*, y la denotamos por τ_c.

Observación. *Cuando se tiene una cantidad finita de espacios topológicos*

X_1, $X_2, \ldots,$ X_n, las topologías caja y producto coinciden. Como cada $\pi_i^{-1}(U_i)$ es equivalente al subconjunto

$$X_1 \times \cdots \times X_{i-1} \times U_i \times X_{i+1} \times \cdots \times X_n,$$

en el producto cartesiano $\Pi_{i=1}^n X_i$. Se sigue que $\pi_i^{-1}(U_i)$ es un abierto de la topología caja, por lo que $\tau_p \subset \tau_c$. Por otra parte, cualquier producto de la forma $\Pi_{i=1}^n U_i$ es la intersección finita de los conjuntos $\pi_i^{-1}(U_i)$, es decir, $\Pi_{i=1}^n U_i = \cap_{i=1}^n \pi_i^{-1}(U_i)$, con lo cual $\tau_c \subset \tau_p$. Por lo tanto, las topologías caja y producto coinciden.

Definición 7.1.1. *Un grupo abeliano A es un grupo topológico si tiene asignada una topología τ para la cual las operaciones del grupo*

$$(a, b) \longmapsto a + b \text{ y } a \longmapsto -a,$$

son funciones continuas. En este caso, $A \times A$ tiene la topología producto o caja.

Observación. *Si A es un grupo topológico y $a \in A$ es un elemento fijo, entonces tanto la función constante $x \longmapsto a$ como la función identidad $x \longmapsto x$ son funciones continuas de A en A. Ahora, estas funciones inducen la función continua $T : A \longrightarrow A \times A$ con regla de correspondencia $x \longmapsto (a, x)$. Al componer la función T con la operación aditiva del grupo, obtenemos la función continua $T_a : A \longrightarrow A$ con regla de correspondencia*

$$x \longmapsto a + x.$$

Nótese que por el mismo argumento, T_{-a} es también una función continua y es inversa de T_a, lo cual muestra que T_a es un homeomorfismo. Así, las traslaciones en un grupo topológico abeliano son homeomorfismos.

Por la observación anterior, decimos que un grupo topológico A es un espacio homogéneo; esto es, para cualquier $a, b \in A$ existe un homeomorfismo $T : A \longrightarrow A$ tal que $T(a) = b$. Además, por lo notado anteriormente, para cualquier $a \in A$, se cumple que:

U es un abierto de a si y sólo si $U - a$ es un abierto del elemento 0.

Esto quiere decir que la topología en A queda definida por el filtro de vecindades abiertas del 0. Este filtro sigue haciendo a las operaciones del grupo continuas en el $(0, 0)$ y 0, respectivamente, es decir, el filtro satisface:

(G1) Para cada $U \in \mathcal{F}$, existe $V \in \mathcal{F}$ tal que $V + V \subset U$.

(G2) Si $U \in \mathcal{F}$ entonces $-U \in \mathcal{F}$.

Recíprocamente, si $\mathcal{F}$ es un filtro en el grupo abeliano A, para el cual $0 \in U$, $\forall U \in \mathcal{F}$ y $\mathcal{F}$ satisface las condiciones $(G1)$ y $(G2)$ antes mencionadas, entonces existe una única topología en A, tal que A es un grupo topológico y $\mathcal{F}$ es un sistema de vecindades del 0. Supongamos que $\mathcal{F}$ es un filtro que satisface que $0 \in U$, para cualquier $U \in \mathcal{F}$, y las propiedades $(G1)$ y $(G2)$. Definamos al conjunto $\tau = \{a + U \mid a \in A, U \in \mathcal{F}\}$, junto con el conjunto $\varnothing$. Notemos primero que $\mathcal{F} \subset \tau$ y que, por ser $\mathcal{F}$ un filtro, se tiene que $A \in \mathcal{F}$, es decir, $A \in \tau$. Veamos que, en efecto, τ cumple las propiedades de ser una topología. Si $a+U$ y $b+V$ son dos abiertos, afirmamos que $(a+U) \cap (b+V)$ es vacía o es de la forma $c + U \cap V$. Si la intersección es no vacía, entonces existe $c \in A$ tal que $a + u_1 = c = b + v_1$, con $u_1 \in U$ y $v_1 \in V$. Ahora, si d es cualquier otro elemento en la intersección, entonces $a + u_2 = d = b + v_2$, con $u_2 \in U$ y $v_2 \in V$. Nótese que $u_2 - u_1 = d - c = v_2 - v_1$, donde $u_2 - u_1 \in U$ y $v_2 - v_1 \in V$, lo cual implica que $d - c \in U \cap V$, es decir, $d \in c + U \cap V$. Como $U \cap V \in \mathcal{F}$, siempre que $U, V \in \mathcal{F}$, entonces

$$(a + U) \cap (b + V) = c + U \cap V.$$

Por lo tanto, $(a + U) \cap (b + V)$ es un elemento en τ, con lo cual, cualquier intersección finita $\cap_{i=1}^{k} a_i + U_i$ es vacía o es de la forma $a + U$. Obervemos que esto último implica que la intersección de dos uniones de abiertos de la forma $\cup_{i \in I} a_i + U_i$ y $\cup_{i \in J} b_i + U_i$, vuelve a ser un conjunto de la forma $\cup_{i \in K} c_i + U_i$.

Por otra parte, al considerar la unión de elementos $\cup_{i \in J}(a_i + U_i)$, si tomamos una $j \in J$ fija, tenemos que $a_j + U_j \subset \cup_{i \in J}(a_i + U_i)$, por lo que $U_j \subset \cup_{i \in J}([a_i - a_j] + U_i)$. Como $\mathcal{F}$ es un filtro, $\cup_{i \in J}(a_i - a_j) + U_i \in \mathcal{F}$, de donde se sigue que

$$\cup_{i \in J}(a_i + U_i) = a_j + (\cup_{i \in J}(a_i - a_j) + U_i) \in \tau.$$

Lo anterior muestra que τ es cerrado bajo intersecciones finitas y uniones, teniendo así que τ es una topología en A.

En vista de lo anterior, el conjunto $a + U$, con $U \in \mathcal{F}$, es un sistema fundamental de vecindades de a. Como el filtro $\mathcal{F}$ cumple la propiedad $(G2)$, la operación de tomar el inverso en el grupo es continua en cualquier elemento $a \in A$, por lo que también es continua en todo A. Ahora, la operación aditiva del grupo $A \times A \longrightarrow A$, con regla de correspondencia $(a, b) \longmapsto a + b$ es continua si y sólo si cada proyección π_A, en cada entrada del producto, es una función continua. Como el filtro $\mathcal{F}$ cumple la propiedad $(G1)$, ambas proyecciones son continuas, por lo que la operación aditiva del grupo es continua. Por lo tanto, A es un grupo topológico y $\mathcal{F}$ es un sistema de vecindades del 0.

Observación. *De lo anterior, podemos decir que todo grupo topológico es un espacio homogéneo, ya que las vecindad en cualquier punto $a \in A$ son vecindades homeomorfas a las vecindades básicas del* 0.

Observación. *Si H es un subgrupo de un grupo topológico A, entonces H es abierto si y sólo si contiene un punto interior. Esto se debe a que, como las traslaciones son homeomorfismos, si un punto en H está en el interior de H, entonces cualquier otro punto en H también lo está.*

7.2. Topologías lineales

A continuación, veremos que en cualquier grupo abeliano A, todo filtro en la retícula de todos los subgrupos de A, donde la relación de orden está dada por la inclusión, da lugar a una topología en el grupo A. Además, bajo estas condiciones, las operaciones del grupo son funciones continuas. De esta manera, si A es un grupo y $L(A)$ es el conjunto de todos los subgrupos de A, al tomar la contención $\subseteq$ como orden parcial, se tiene que $L(A)$ es una retícula completa, ya que para cualquier par de subgrupos B y C de A, $B \cap C$ y $B \vee C$ son los mínimos y máximos, respectivamente, donde la yunta significa el subgrupo generado por B y por C.

Sea $\mathcal{F}$ un filtro en la retícula $L(A)$. Como todo subgrupo tiene al elemento neutro 0, veremos que podemos tomar a los subgrupos $U \in \mathcal{F}$ como una base de vecindades abiertas del 0, con lo cual, la topología quedaría determinada por los abiertos de la forma $a + U$, con $U \in \mathcal{F}$ y $a \in A$. Esto quiere decir que las clases laterales de los subgrupos U en $\mathcal{F}$ son conjuntos abiertos. Si $U_1, U_2 \in \mathcal{F}$, la intersección de dos clases $(a_1 + U_1) \cap (a_2 + U_2)$ es vacía o es una clase de la forma $a + U_1 \cap U_2$, por lo que vuelve a ser un abierto de la topología, así como la unión arbitraria de abiertos de la forma $a + U$, vuelve a ser un elemento en $\mathcal{F}$. Basta demostrar que se cumplen las propiedades $(G1)$ y $(G2)$ antes mencionadas.

Sea $(a,b) \in A \times A$ tal que $(a,b) \longmapsto a+b$. Al tomar la vecindad $(a+b)+U$, con $U \in \mathcal{F}$, se tiene que, para las vecindades $a+U$ y $b+U$, de a y b respectivamente, se cumple que $(a+U, b+U) \longmapsto (a+b)+U$, puesto que U es un subgrupo de A. Esto muestra que la operación aditiva del grupo es continua. Por otra parte, como la operación de tomar inversos en el grupo es un morfismo de $A \longrightarrow A$, para cualquier subgrupo $U \in \mathcal{F}$, se tiene que $-U \subset U$. Así, si $a \in A$ y $U \in \mathcal{F}$, al tomar la vecindad $-a+U$, se sigue que $(a+U) \longmapsto -a+U$. Por lo tanto, la operación de tomar inversos es continua, con lo cual A es un grupo topológico. A esta topología se le llama la *topología lineal* en A, generada por el filtro $\mathcal{F}$.

Proposición 7.2.1. *Sea $\mathcal{F}$ un sistema fundamental de vecindades abiertas del cero en A. Entonces, para cualquier $U \in \mathcal{F}$ existe $V \in \mathcal{F}$ tal que*

$$V + (-V) \subset U.$$

Demostración. Como el grupo A es un grupo topológico, la función $f : A \times A \longrightarrow A$ definida por $(a,b) \longmapsto a-b$ es continua, puesto que las proyecciones en cada entrada del producto, es decir, las funciones de $A \times A \longrightarrow A$ y $A \longrightarrow A$, con regla de correspondencia $(a,b) \longmapsto a$ y $(a,b) \longmapsto -b$, respectivamente, son funciones continuas. De esta manera, si $U \in \mathcal{F}$ es una vecindad abierta del 0, por la continuidad de f, se tiene que $f^{-1}(U)$ es un abierto que contiene al $(0,0)$. Por lo tanto, existen abiertos A y B del 0 tales que $A \times B \subset f^{-1}(U)$. Por otra parte, como $A \cap B$ es un abierto que contiene al 0, existe una vecindad $V \in \mathcal{F}$ tal que $V \subset A \cap B$, lo cual implica que

$$V \times V \subset A \times B \subset f^{-1}(U),$$

esto es, $V + (-V) \subset U$. □

Definición 7.2.2. *Un anillo topológico es un anillo A dotado de una topología que hace del grupo aditivo de A un grupo topológico y tal que la multiplicación $(a,b) \longmapsto ab$ es una función continua de $A \times A \longrightarrow A$.*

Observación. *Como en cualquier anillo A, podemos escribir*

$$ab - a_0b_0 = (a-a_0)(b-b_0) + (a-a_0)b_0 + a_0(b-b_0),$$

para que la multiplicación sea una función continua en el anillo topológico A, basta pedir que

- *Para cada $a \in A$, las funciones $x \longmapsto xa$ y $x \longmapsto ax$ sean continuas en el* 0.
- *La función $(a, b) \longmapsto ab$ sea continua en el* $(0, 0)$.

Por lo tanto, en cualquier anillo topológico A, el filtro $\mathcal{F}$ de vecindades del 0 además de satisfacer $(G1)$ y $(G2)$, satisface:

(R1) Para cada $a \in A$ y $U \in \mathcal{F}$ existe $V \in \mathcal{F}$ tal que $aV \subset U$ y $Va \subset U$.

(R2) Para cada $U \in \mathcal{F}$, existe $V \in \mathcal{F}$ tal que $V \cdot V \subset U$.

Así mismo, si A es un anillo con un filtro $\mathcal{F}$ de subconjuntos, los cuales todos contienen al 0 y $\mathcal{F}$ satisface $(G1)$, $(G2)$, $(R1)$, $(R2)$, entonces existe una única topología en A, que lo hace un anillo topológico, en donde $\mathcal{F}$ es un sistema de vecindades de abiertos del cero.

7.3. Propiedades

Proposición 7.3.1. *Sean A un grupo topológico y $\mathcal{F}$ un filtro de $L(A)$. Para la topología en A generada por $\mathcal{F}$, los siguientes enunciados son equivalentes:*

i) La topología es de Hausdorff.

ii) $\cap_{U\in\mathcal{F}} U = \{0\}$.

iii) $\{0\}$ es un subgrupo cerrado.

Demostración. $i) \Longrightarrow ii)$. Como $\mathcal{F}$ es un sistema de vecindades del 0, lo podemos dirigir con la relación $\leq$ definida por $U \leq V$ si y sólo si $V \subset U$. De esta manera, se tiene que cualquier red de la forma $\{x_U\}_{U\in\mathcal{F}}$, con $x_U \in U$, converge al 0. Ahora, si $a \in \cap_{U\in\mathcal{F}} U$, entonces la red constante $\{y_U\}_{U\in\mathcal{F}}$, donde $y_U = a$, $\forall U \in \mathcal{F}$ converge tanto a a, como al 0. Al ser el grupo topológico de Hausdorff, se tiene que $a = 0$.

$ii) \Longrightarrow i)$. Sea $\mathcal{F}$ un sistema de vecindades abiertas del 0, tal que $\cap_{U\in\mathcal{F}} U = \{0\}$. Sean $a, b \in A$, con $a \neq b$. Entonces $a - b \notin \cap_{U\in\mathcal{F}} U$, por lo que existe una vecindad $U \in \mathcal{F}$ del 0 para la cual $a - b \notin U$. Por la Proposición 7.2.1, existe $V \in \mathcal{F}$ una vecindad abierta del 0 tal que $V^{-1} + V \subset U$. Ahora, como $a - b \notin U$, entonces $a - b \notin V^{-1} + V$, por lo que $(a - b + V) \cap V = \varnothing$. Como las traslaciones son homeomorfismos, se tiene que al aplicar la traslación T_b a los abiertos $a-b+V$ y V, se obtienen los abiertos $a+V$ y $b+V$, respectivamente. Nótese que $(a+V)\cap(b+V)=\varnothing$ y que $a+V$ y $b+V$ son vecindades abiertas de a y de b, respectivamente. Por lo tanto, el espacio es de Hausdorff.

ii) $\Longrightarrow$ *iii)* Sea $a \in A$, con $a \neq 0$. Entonces existe $U \in \mathcal{F}$ para el cual $a \notin U$. Por la Proposición 7.2.1, existe $V \in \mathcal{F}$ tal que $V+(-V) \subset U$, por lo que $a \notin V+(-V)$. Esto implica que $(a+V)\cap V=\varnothing$. Por lo tanto, $a+V$ es un abierto que contiene a a y es tal que $0 \notin a+V$, pues $0 \in V$. Esto muestra que $A \setminus \{0\}$ es abierto, teniendo así que $\{0\}$ es un subgrupo cerrado.

iii) $\Longrightarrow$ *ii)*. Como el grupo topológico A es homogeneo, si $\{0\}$ es un subgrupo cerrado, entonces para cualquier $a \in A$, el conjunto $\{a\}$ es cerrado en A. Esto muestra que el grupo topológico A es T_1. Ahora, si $a \neq 0$, existe un abierto $U \in \mathcal{F}$ tal que $0 \in U$ y $a \notin U$, por lo que $a \notin \cap_{U \in F} U$. Por lo tanto, $\cap_{U \in F} U = \{0\}$. □

Definición 7.3.2. *Decimos que un espacio topológico es primero numerable si todo elemento tiene una base local de cardinal numerable.*

En este caso, si $U_1, U_2, \ldots, U_n, \ldots$ es un sistema de vecindades, entonces $U_1, U_1 \cap U_2, \ldots, U_1 \cap \cdots \cap U_n, \ldots$ también es un sistema de vecindades abiertas locales, por lo que sin pérdida de generalidad podemos suponer que el sistema de vecindades de abiertos forma una sucesión decreciente.

Observación. *Todo subgrupo abierto B de A es también cerrado. En efecto, el complemento de B en A es de la forma $\cup_{a \notin B} a + B$, donde cada $a + B$ es un abierto en la topología. Esto quiere decir que el complemento de B es una unión de abiertos, teniendo así que $\cup_{a \notin B} a + B$ es un conjunto abierto. Por lo tanto, B es cerrado.*

En particular, si $\mathcal{F}$ es un sistema de vecindades abiertas del cero, cualquier $U \in \mathcal{F}$ es tanto abierto como cerrado, lo cual nos lleva al siguiente

Teorema 7.3.3. *Sea $\mathcal{F}$ un filtro en $L(A)$. Si la topología generada por $\mathcal{F}$ en A es de Hausdorff, entonces A es un espacio topológico 0-dimensional.*

Demostración. Sean A un grupo topológico T_2 y $\mathcal{F}$ un sistema de vecindades abiertas del 0. Como el grupo topológico es homogéneo, basta ver la dimensión en el elemento 0. Ahora, por la observación anterior, cada $U \in \mathcal{F}$ es abierto y cerrado, por lo que $Fr(U)=\varnothing$, $\forall U \in \mathcal{F}$. De esta manera, la $dim_0(A)=0$, teniendo así que $dim(A)=0$. □

7.4. Ejemplos

Ejemplo. *Si A es un grupo abeliano, la topología $\mathbb{Z}$-ádica en A tiene como sistema de vecindades abiertas del 0 a los subgrupos de la forma nA, donde $n \in \mathbb{Z} \setminus \{0\}$. Esto muestra que la topología $\mathbb{Z}$-ádica es primero numerable. Notemos también que, para los subgrupos nA, se cumple que $n(A/nA) = \{0\}$.*

Definición 7.4.1. *Decimos que un grupo U es acotado, si existe $m \in \mathbb{N}$ tal que $m(A/U) = \{0\}$.*

Observación. *La topología $\mathbb{Z}$-ádica es la topología lineal generada por los subgrupos U de A tal que U es un subgrupo acotado. Además, la topología $\mathbb{Z}$-ádica es de Hausdorff si y sólo si $\cap_{n\in\mathbb{N}} nA = \{0\}$. A esta última intersección se le conoce como el* ***subgrupo de Ulm***. *Por lo tanto, la topología generada por los subgrupos nA es T_2 si y sólo si el subgrupo de Ulm es trivial.*

Ejemplo. *La topología p-ádica en el grupo A tiene como base fundamental de vecindades del 0 a los subgrupos de la forma $p^k A$, con $k \in \mathbb{N}$. En este caso, el filtro $\mathcal{F}$ en $L(A)$ está formado por los subgrupos U de A tales que A/U es un p-grupo.*

Capítulo 8

Completación Topológica

En esta sección, daremos una construcción de la completación topológica de un grupo topológico A en términos de redes de Cauchy y otra usando límites inversos.

8.1. Redes convergentes y de Cauchy

Sean A un grupo topológico y $\mathcal{F}$ un filtro en $L(A)$. Como vimos anteriormente, $\mathcal{F}$ es un sistema básico de vecindades del 0, el cual define una topología lineal en A. Si etiquetamos a cada elemento de $\mathcal{F}$ con un elemento del conjunto I, y definimos la relación en I por $i \leq j$ si y sólo si $U_j \leq U_i$, entonces I es un conjunto parcialmente ordenado por $\leq$. Más aún, I es un conjunto dirigido ya que los elementos de $\mathcal{F}$ forman un sistema de vecindades del 0. Por lo observado en los preliminares, se tiene una biyección entre el conjunto de redes en A, etiquetadas por el índice I, y funciones de I en A. Esto nos lleva a la siguiente

Definición 8.1.1. *La red $\{a_i\}_{i\in I}$ en el grupo topológico A converge al límite $a \in A$ si para cada $i \in I$ existe $j \in I$ tal que $a_k \in a + U_i$, para toda $k \geq j$. En este caso, lo denotamos por $\{a_i\}_{i\in I} \longrightarrow a$.*

Observación. *Como cada U_i es un subgrupo de A, son equivalentes $a_k \in a + U_i$ y $a_k - a \in U_i$, por lo que usaremos esta última notación a lo largo de la sección. Se sigue también que, si $\{a_i\}_{i\in I}$ converge al elemento $a \in A$, entonces cualquier subred cofinal es convergente y converge a a.*

En este capítulo, nos interesaremos en redes convergentes $\{b_i\}_{i\in I} \longrightarrow a$ tales que, para cualquier $i \in I$, se tiene que $b_k - a \in U_i$ para toda $k \geq i$. A estas redes las llamaremos *nítidas* y diremos que la red converge de manera nítida.

Definición 8.1.2. *Una red $\{a_i\}_{i\in I}$ en el grupo topológico A es de Cauchy si para cualquier $i \in I$, existe $j \in I$ tal que $a_k - a_l \in U_i$, $\forall l, k \geq j$.*

Observación. *Como los conjuntos U_i son subgrupos de A, se tiene que $a_k - a_j \in U_i$ y $a_l - a_j \in U_i$ implican que $a_k - a_l \in U_i$, por lo que ser de Cauchy es equivalente a que $a_k - a_j \in U_i$, para toda $k \geq j$. De manera similar, toda subred cofinal de una red de Cauchy es también de Cauchy. Además, si una subred cofinal, de una red de Cauchy converge, entonces la misma red de Cauchy converge y ambas convergen al mismo valor.*

Consideraremos redes de Cauchy $\{b_i\}_{i\in I}$ tales que, para cada $i \in I$, $b_k - b_i \in U_i$, $\forall k \geq i$, es decir, j coincide con i. A este tipo de redes, las llamaremos redes nítidas de Cauchy.

Observación. *Si $\{b_i\}_{i\in I}$ es una red de Cauchy y converge al límite b, entonces la red converge de manera nítida a b. En efecto, si $i \in I$, como la red $\{b_i\}_{i\in I}$ es de Cauchy, se tiene que $b_k - b_i \in U_i$, $\forall k \geq i$. Por otra parte, como $\{b_i\}_{i\in I} \longrightarrow b$, para $i \in I$, existe $j \in I$ tal que $b_k - b \in U_i$ para toda $k \geq j$. Además, como el conjunto I está dirigido, existe j_0 tal que $i \leq j_0$ y $j \leq j_0$. Con esto en cuenta, se sigue que $b_{j_0} - b \in U_i$, así como $b_{j_0} - b_i \in U_i$. Al ser U_i un subgrupo de A, se cumple que*

$$b_i - b = (b_{j_0} - b) - (b_{j_0} - b_i) \in U_i.$$

De esta manera, si $k \geq i$ entonces $b_k - b_i \in U_i$, por lo que

$$b_k - b = (b_k - b_i) - (b_i - b) \in U_i.$$

Notemos que esto último implica que $b_k - b_i \in U_i$, $\forall k \geq i$. Por lo tanto, la red converge de manera nítida a b.

Definición 8.1.3. *Un grupo topológico A es completo si la topología es de Hausdorff y si toda red de Cauchy en A tiene un punto límite en A.*

8.2. Topologías producto y caja

Sean $\{A_t\}_{t\in J}$ una familia de grupos topológicos, cada uno dotado por la topología lineal definida por el filtro $\mathcal{F}_t$ en $L(A_t)$ y el producto directo $G = \Pi_{t\in J}A_t$, junto con las proyecciones canónicas $\pi_s : \Pi_{t\in J}A_t \longrightarrow A_s$. La topología *producto* τ_p en G es la topología que tiene como sub-base a los conjuntos de la forma $\pi_s^{-1}(U_s)$, donde $U_s \in \mathcal{F}_s$ y $s \in J$. Esto quiere decir que los abiertos de la topología producto son uniones de abiertos básicos de la forma

$$\pi_{s_1}^{-1}(U_{s_1}) \cap \cdots \cap \pi_{s_n}^{-1}(U_{s_n}),$$

donde $U_{s_i} \in \mathcal{F}_{s_i}$ y $s_1, \ldots, s_n \in J$. Obsérvese que, como cada proyección π_s es un morfismo, los conjuntos $\pi_s^{-1}(U_j)$ son subgrupos de G, para cualquier $U_j \in \mathcal{F}_j$, por lo que estos subgrupos forman un sistema de vecindades del 0 que cumple las dos propiedades que hacen a τ_p ser una topología lineal en G. Claramente, τ_p hace de cada proyección π_s un morfismo continuo y abierto. Más aún, τ_p es la topología más chica que hace de las proyecciones funciones continuas y abiertas.

Otra topología que podemos asignar al producto directo $G = \Pi_{t\in J}A_j$ es la que llamamos *topología caja*, la cual denotamos por τ_c. Observemos que, sin perdida de generalidad, podemos usar un conjunto I para etiquetar a los elementos de cada filtro $\mathcal{F}_s$, con $s \in J$, ya que, en caso de ser necesario, se pueden repetir las elecciones de elementos en I hasta cubrir de manera total a cada sistema de vecindades. Así, para cada $t \in J$, denotaremos a su sistema de vecindades del 0 por $\{U_{t_i}\}_{i\in I}$. Notemos que si $j \geq i$, entonces $U_{t_j} \leq U_{t_i}$, para cada $t \in J$, pero puede suceder que $U_{t_i} = U_{t_j}$ para j e i no comparables. Con esto en cuenta, la topología caja tiene como base fundamental de vecindades del 0, a los subgrupos de G de la forma $\Pi_{t\in J}U_{t_i} := U_i^*$, con $i \in I$. Esta topología vuelve a ser lineal y además, como $U_i^* \leq \pi_t^{-1}(U_{t_i})$, para cada $t \in J$, podemos partir al subgrupo $\pi_t^{-1}(U_{t_i})$ en clases laterales inducidas por U_i^*, es decir,

$$\pi_t^{-1}(U_{t_i}) = \cup_{x\in\pi_t^{-1}(U_{t_i})} x + U_i^*.$$

Como τ_c es una topología lineal, cada clase lateral, de un básico, es un abierto, por lo que esta última unión resulta ser también abierta. Esto muestra que $\tau_p \subset \tau_c$, lo cual implica que las proyecciones π_s son también continuas y abiertas con la topología τ_c.

Observación. *Cuando cada A_t está dotado de la topología $\mathbb{Z}$-ádica (p-ádica), la topología caja del producto $\Pi_{t\in J}A_t$ coincide con la topología $\mathbb{Z}$-ádica (p-ádica) de $\Pi_{t\in J}A_t$.*

Nótese también que en la topología caja, puede depender la manera en la que los U_{t_i} se han etiquetado.

La ventaja de la topología caja en el producto directo, es que podemos usar un mismo conjunto I para etiquetar a las redes. Con esto en cuenta, si $G = \Pi_{t\in J}A_t$ tiene la topología caja y $\{(g_i)\}_{i\in I}$ es una red de Cauchy (nítida) en G, entonces cada proyección $\{\pi_t((g_i))\}_{i\in I}$ forma una red de Cauchy (nítida) en A_t. El converso también es cierto, $\{(g_i)\}_{i\in I}$ es una red nítida de Cauchy si para cada $t \in J$, $\{\pi_t((g_i))\}_{i\in I}$ es una red nítida de Cauchy. Este argumento demuestra la siguiente

Proposición 8.2.1. *Un producto directo $\Pi_{t\in J}A_t$ es completo en la topología caja si y sólo si toda componente A_t es completo en su topología lineal.*

8.3. Completación topológica por filtros

Sean A un grupo topológico y $\{U_i\}_{i\in I}$ una base de vecindades del cero. Cada red $\{a_i\}_{i\in I}$ en A se puede identificar de manera única con un elemento del producto directo $G = A^I = \Pi_{i\in I}A_i$, con $A_i = A$ para toda i, bajo la correspondencia

$$\{a_i\}_{i\in I} \longmapsto (\cdots, a_j, \cdots, a_i, \cdots).$$

Como estamos considerando redes nítidas de Cauchy, denotaremos por C a la imagen de todas las redes nítidas de Cauchy bajo esta ultima correspondencia. Nótese que $C \leq G$, donde la suma de dos redes nítidas de Cauchy está definida en cada término i-ésimo; el inverso aditivo de $\{a_i\}_{i\in I}$ es la red $\{-a_i\}_{i\in I}$. Por otra parte, denotaremos por E a la imagen del conjunto de todas las redes nítidas en A que convergen a 0, bajo la correspondencia antes mencionada. Nótese que E es un subgrupo de C, ya que como se vio anteriormente, toda red de Cauchy convergentente, es una red nítida de Cauchy. En este caso, la suma de dos redes nítidas convergentes al 0, convergen a la suma $0 + 0 = 0$, de los puntos límites.

Proposición 8.3.1. *El conjunto E es cerrado en C, con la topología producto y la topología caja.*

Demostración. Basta demostrar que toda red convergente de elementos en E, converge a un elemento en E. Sea $\{g_j\}_{j\in J} \longrightarrow \{b_i\}_{i\in I}$ una red de redes convergentes, es decir, cada $g_j = \{g_{j_i}\}_{i\in I}$ es una red nítida de Cauchy convergente a 0.

Consideremos primero a C con la topología caja. Como $\{g_j\}_{j\in J}$ converge a $\{b_i\}_{i\in I}$, para $i \in I$ y el abierto básico U_i^*, existe $j_1 \in J$ tal que

$$\{g_k\}_{k\in J} - \{b_i\}_{i\in I} \in U_i^*, \ \forall k \geq j_1,$$

lo cual implica que $g_{k_s} - b_s \in U_i$, para cualquier $s \in I$ y $\forall k \geq j_1$. Ahora, como cada $\{g_{j_i}\}_{i\in I}$ converge de manera nítida a 0, si $l \geq i$, para cada $\{g_{j_i}\}_{i\in I}$ se tiene que $g_{j_l} - 0 = g_{j_l} \in U_i$. Por lo tanto, si escogemos $m \geq j_1$, de lo anterior se sigue que, $\forall j \geq i$, $g_{m_j} \in U_i$ y $g_{m_j} - b_j \in U_i$. Como U_i es un subgrupo, se sigue que

$$b_j = g_{m_j} - (b_{m_j} - b_j) \in U_i, \ \forall j \geq i,$$

lo cual muestra que $\{b_i\}_{i\in I}$ converge de manera nítida al 0, es decir, $\{b_i\}_{i\in I} \in E$.

Consideremos ahora a C con la topología producto. Sea $i \in I$ y el abierto básico $\pi_i^{-1}(U_i)$. Como la red $\{g_j\}_{j\in J}$ converge a $\{b_i\}_{i\in I}$, para $j_0 \in J$ existe $k_0 \in J$ tal que

$$\{g_j\}_{j\in J} - \{b_i\}_{i\in I} \in \pi_i^{-1}(U_i), \text{ para cualquier } j \geq k_0.$$

Esto quiere decir que, para toda red $\{g_j\}_{j\in J}$, con $j \geq k_0$, se satisface

$$\{g_{j_i}\}_{i\in I} - \{b_i\}_{i\in I} \in \pi_i^{-1}(U_i),$$

lo cual implica que $\pi_i(\{g_{j_i}\}_{i\in I} - \{b_i\}_{i\in I}) \in U_i$, es decir, $g_{j_i} - b_i \in U_i$. Por otra parte, como cada red $\{g_j\}_{j\in J}$ converge de manera nítida al 0, si $l \geq i$, entonces $g_{j_l} - 0 = g_{j_l} \in U_i$. En particular, para cualquier $j \geq k_0$, se cumple que $g_{j_i} - b_i$, $g_{j_i} \in U_i$. Por ser U_i un subgrupo, se tiene que

$$b_i = g_{j_i} - (g_{j_i} - b_i) \in U_i.$$

Finalmente, como $\{b_i\}_{i\in I}$ es una red nítida de Cauchy, si $l \geq i$ entonces $b_l - b_i \in U_i$. Estas dos últimas observaciones implican que $b_l \in U_i$, para toda $l \geq i$. Por lo tanto, $\{b_i\}_{i\in I} \in E$. $\square$

Esta proposición implica que el espacio cociente $\widehat{A} = C/E$ resulta ser un espacio topológico de Hausdorff, con cualquiera de las dos topologías inducidas por G. Más aún, se tiene el siguiente

Lema 8.3.2. *Las topologías producto y caja en $G = \Pi_{i\in I} A_i$ inducen la misma topología en $\widehat{A}$.*

Demostración. Como $U_i^* \leq \pi_t^{-1}(U_{t_i})$ para toda t, entonces

$$C \cap U_i^* + E \leq C \cap \pi_t^{-1}(U_{t_i}) + E,$$

por lo que basta ver que para cualquier abierto $U_i^* \in \tau_c$, en la topología inducida en $\widehat{A}$ por τ_c, existe un abierto $\pi_j^{-1}(U_k) \in \tau_p$, en la topología inducida en $\widehat{A}$ por τ_p, tal que

$$C \cap \pi_j^{-1}(U_k) + E \leq C \cap U_i^* + E.$$

Por la ley modular, para los grupos $E \leq C$ y $\pi_j^{-1}(U_k)$ de A^I, se tiene que

$$E + (C \cap \pi_j^{-1}(U_k)) = (E + C) \cap \pi_j^{-1}(U_k) = C \cap \pi_j^{-1}(U_k),$$

por lo que basta demostrar que $C \cap \pi_j^{-1}(U_k) \leq C \cap U_i^* + E$.

Sea U_i^* un abierto básico de τ_c y $\{a_i\}_{i\in I}$ una red nítida de Cauchy contenida en $\pi_i^{-1}(U_i)$. Como $\{a_i\}_{i\in I} \in C \cap \pi_i^{-1}(U_i)$, $\{a_i\}_{i\in I}$ es una red nítida de Cauchy y $a_i = (\pi_i\{a_i\}_{i\in I}) \in U_i$. Más aún, como $a_j - a_i \in U_i$ para toda $j \geq i$ y U_i es un subgrupo, entonces $a_j = a_i + (a_j + a_i) \in U_i$. Con esto en cuenta, definamos las redes $\{b_i\}_{i\in I}$ y $\{c_i\}_{i\in I}$ por

$$\{b_i\}_{i\in I} = \begin{cases} b_j = a_j & \text{si } j \geq i \\ b_j = 0 & \text{si } j < i \end{cases} \text{ y } \{c_i\}_{i\in I} = \begin{cases} c_j = a_j & \text{si } j < i \\ c_j = 0 & \text{si } j \geq i \end{cases}.$$

Notemos que $\{b_i\}_{i\in I}$ es una red de Cauchy contenida en U_i^*. En efecto, como la red $\{a_i\}_{i\in I}$ es nítida, dada $s \in I$, se tiene que $\forall k \geq s$, la resta $a_k - a_s \in U_s$. Ahora, por ser I un conjunto dirigido, para i y s, existe $j \in I$ tal que $j \geq i$ y $j \geq s$. De esta manera, para cualquier $k \geq j$, se cumple que $k \geq j \geq i$, por lo que $b_k = a_k$, así como $b_j = a_j$. También, al ser $j \geq s$ y $k \geq s$, se cumple que $a_j - a_s \in U_s$, al igual que $a_k - a_s \in U_s$. Por lo tanto,

$$b_k - b_j = a_k - a_j = (a_k - a_s) - (a_j - a_s) \in U_s,$$

mostrando así que $\{b_j\}_{j\in I}$ es una red de Cauchy. La segunda afirmación se sigue observando que $a_j \in U_i$, para toda $j \geq i$.

Para la red $\{c_i\}_{i\in I}$, el razonamiento es totalmente análogo salvo que en este caso, la existencia de $j \in I$, tal que $j \geq s$ y $j \geq i$, implica que para cualquier $k \geq j$, los términos $c_k = 0$ y $c_j = 0$, de donde se sigue que $c_k - c_j = 0 - 0 = 0 \in U_s$. Esto último muestra que la red $\{c_i\}_{i\in I}$ converge al 0, ya que para cualquier $j \in I$ y $k \geq j$, se cumple que $c_k - 0 = 0 - 0 = 0 \in U_s$. Por lo tanto, $\{c_i\}_{i\in I} \in E$ y $\{b_i\}_{i\in I} \in U_i^* \cap C$. Se sigue que

$$\{a_i\}_{i\in I} = \{b_i\}_{i\in I} + \{c_i\}_{i\in I} \in C \cap U_i^* + E,$$

por lo que $C \cap \pi_j^{-1}(U_k) \leq C \cap U_i^* + E$. □

Observación. *Una consecuencia del lema anterior es que para el grupo topológico A, el conjunto de proyecciones de los subgrupos $\widetilde{U}_l$ de $\widehat{A}$, que constan de todas las redes nítidas de Cauchy $\{a_i\}_{i\in I}$ tales que $a_l \in U_l$, $\forall l \in I$, forman una base de vecindades del 0. Por otra parte, la función $\mu : A \longrightarrow \widehat{A}$ definida por $a \longmapsto (a, \cdots, a, \cdots) + E$ es continua y es un homomorfismo abierto, pues $\mu^{-1}([(a, \cdots, a, \cdots) + U_i^*] + E) = a + U_i$. Esto implica que a todo elemento $a \in A$ lo podemos identificar con la red de Cauchy constante $\{a_i\}_{i\in I}$, es decir, $a_i = a$, $\forall i \in I$. Más aún, si A es de Hausdorff, μ es un isomorfismo topológico entre A y $\mu(A)$, donde $\mu(A)$ tiene la topología inducida por $\widehat{A}$.*

Teorema 8.3.3. *El grupo $\widehat{A}$ es completo y $\mu(A)$ es un subgrupo denso de $\widehat{A}$.*

Demostración. Para ver que $\mu(A)$ es un subgrupo denso de $\widehat{A}$, tomemos $a = \{a_i\}_{i\in I} + E$ un elemento en $\widehat{A}$ y U_i^* una vecindad básica del 0 en $G = A^I$. Por el teorema anterior, podemos suponer que

$$\{a_i\}_{i\in I} \in U_i + E = C \cap \pi_i^{-1}(U_i) + E,$$

por lo que $a_i \in U_i$. Afirmamos que $\mu(a_i) \in (\{a_i\}_{i\in I} + U_i^*) + E$. Como $\{a_i\}_{i\in I}$ es una red nítida de Cauchy, para cualquier $s \in I$, se tiene que $a_k - a_s \in U_s$, $\forall k \geq s$. Con esto en cuenta, al estar $a_i \in U_i$, para cualquier $k \geq i$ se cumple que $a_k = (a_k - a_i) + a_i \in U_i$. De esta manera, podemos definir las redes $\{b_i\}_{i\in I}$ y $\{c_i\}_{i\in I}$ por:

$$\{b_i\}_{i\in I} = \begin{cases} b_j = a_j - a_i & \text{si } j \geq i \\ b_j = 0 & \text{si } j < i \end{cases}, \quad \text{y} \quad \{c_i\}_{i\in I} = \begin{cases} c_j = a_j - a_i & \text{si } j < i \\ c_j = 0 & \text{si } j \geq i \end{cases}.$$

Nótese que $\{b_i\}_{i\in I}$ es una red de Cauchy, pues para cualquier $s \in I$, existe $j \in I$ tal que $j \geq s$ y $j \geq i$. De esta manera, $\forall k \geq j$ se cumple que

$$b_k - b_{j_s} = (a_k - a_i) - (a_{j_s} - a_i) = a_k - a_{j_s},$$

ya que tanto k como j son mayores que i. Además, por cumplirse también que $k \geq j \geq s$, se sigue que $a_k - a_s \in U_s$, como $a_{j_s} - a_s \in U_s$, lo cual implica que

$$a_k - a_j = (a_k - a_s) - (a_j - a_s) \in U_s.$$

Por la manera en que se definió a la red $\{b_i\}_{i\in I}$, se tiene que $\{b_i\}_{i\in I} \in U_i^*$. Por un razonamiento análogo al del lema anterior, la red $\{c_i\}_{i\in I}$ es de Cauchy y converge al 0. Por lo tanto,

$$\{a_i\}_{i\in I} = \{b_i\}_{i\in I} + \mu(a_i) + \{c_i\}_{i\in I},$$

de donde concluimos que $\mu(a_i) \in (\{a_i\}_{i\in I} + U_i^*) + E$. Esto muestra que $\mu(A)$ es denso en $\widehat{A}$.

Ahora, como $\mu(A)$ es denso en $\widehat{A}$, para ver que $\widehat{A}$ es completo, basta demostrar que toda red de Cauchy en $\mu(A)$ converge a un elemento en $\widehat{A}$. Una red nítida de Cauchy en $\mu(A)$ es de la forma $\{\mu(a_i)\}_{i\in I}$, lo cual implica que, para cualquier $s \in I$, se tiene que $\mu(a_k) - \mu(a_s) \in U_s^*$, $\forall k \geq s$. De lo anterior, se sigue que $a_k - a_s \in U_s$, es decir, $\{a_i\}_{i\in I}$ es una red nítida de Cauchy. Más aún, afirmamos que

$$\{\mu(a_i)\}_{i\in I} \longrightarrow \{a_i\}_{i\in I} + E.$$

Sean $i \in I$ y U_i^* una vecindad del 0 en $G = A^I$. Como $\forall j \geq i$ se cumple que $a_j - a_i \in U_i$, entonces $a_k - a_j \in U_i$, $k, j \geq i$. De esta manera, si fijamos $j \geq i$, podemos definir las redes

$$\{b_i\}_{i\in I} = \begin{cases} b_k = a_j - a_k & \text{si } k \geq i \\ b_k = 0 & \text{si } k < i \end{cases} \text{ y } \{e_i\}_{i\in I} = \begin{cases} e_k = a_j - a_k & \text{si } k < i \\ e_k = 0 & \text{si } k \geq i \end{cases}.$$

Observemos que $\{b_i\}_{i\in I}$ como $\{e_i\}_{i\in I}$ son redes de Cauchy tales que $\{b_i\}_{i\in I} \in U_i^*$ y $\{e_i\}_{i\in I} \longrightarrow 0$. Así,

$$\mu(a_j) = \{a_i\}_{i\in I} + \{b_i\}_{i\in I} + \{e_i\}_{i\in I},$$

es decir, $\mu(a_j) \in [\{a_i\}_{i\in I} + U_i^*] + E$, para cualquier $j \geq i$. Esto demuestra que $\{\mu(a_i)\}_{i\in I}$ converge de manera nítida a $\{a_i\}_{i\in I} + E \in \widehat{A}$. □

8.4. Enteros p-ádicos como la completación topológica

Veremos ahora que los enteros p-ádicos son la completación topológica del anillo ${}_p\mathbb{Q}$. Sean p un primo y ${}_p\mathbb{Q}$ el anillo de los números racionales cuyos denominadores son primos relativos con p.

Observación. *Notemos que* ${}_p\mathbb{Q}$ *es un anillo de ideales principales, generados por los ideales* $p^k_p\mathbb{Q}$*, con* $k = 1, 2, \ldots$*. En efecto, en primer lugar, para cada* $k \in \mathbb{N}$*, el conjunto* $p^k({}_p\mathbb{Q}) := (p^k)$ *es un ideal de* ${}_p\mathbb{Q}$*. Por otra parte, si* $I \subsetneqq ({}_p\mathbb{Q})$ *es un ideal propio, entonces* I *contiene un menor entero positivo: si* $\frac{n}{m} \in I$*, entonces* $m\frac{n}{m} = n \in I$*, por lo que tanto* n *como* $-n$ *son elementos de* I*. De esta manera,* $I \cap \mathbb{N} \neq \varnothing$*. Por el principio del Buen Orden,* I *contiene un menor entero positivo* k*. Con esto en cuenta, se tiene que* $< k > \subseteq I$*.*

Afirmamos que $k = p^s$, para alguna $s \in \mathbb{N}$. Notemos primero que $(k, p) \neq 1$, pues en caso contrario, se tendría que

$$\tfrac{1}{k}k = 1 \in < k > \subseteq I \subsetneqq ({}_p\mathbb{Q}),$$

lo cual es una contradicción. Ahora, si $k = p^r l$, donde r es la mayor potencia de p que divide a k y $(l, p) = 1$, entonces $\frac{1}{l}k = p^r \in < k >$, por lo que $< p^r > \subseteq < k > \subseteq I$. La elección de k implica que $k = p^r$. Por otra parte, dado $\frac{n}{l} \in I$, se tiene que $n \in I$, por lo que sin pérdida de generalidad, podemos suponer que $n > 0$. Como p^r es el menor natural en I, del algoritmo de la división de Euclides se obtiene que $n = p^r a + b$, con $0 \leqq b < p^r$. En caso de que $b \neq 0$, se sigue que $n - p^r a = b \in I$, lo cual contradice la elección de p^r. Por lo tanto, $b = 0$ y así, todo elemento $\frac{n}{l} \in I$ se puede escribir de la forma $\frac{a}{l}p^r = \frac{ap^r}{l} \in < p^r >$, teniendo que $I = < (p^r) >$.

Con esto en cuenta, podemos dotar a ${}_p\mathbb{Q}$ con la topología inducida por los ideales (p^k) como sistema fundamental de vecindades del 0.

Observación. *Nótese que la topología definida por los ideales* (p^k) *como sistema fundamental de vecindades del* 0 *es la topología p-ádica del conjunto* ${}_p\mathbb{Q}$*.*

Como veremos a continuación, esta topología nos permitirá completar nuestro anillo ${}_p\mathbb{Q}$ a un anillo en el cual toda sucesión de Cauchy es convergente, al cual denotaremos por ${}_p\mathbb{Q}^*$. Además, ${}_p\mathbb{Q}^*$ seguirá cumpliendo que sus ideales son de la forma (p^k).

Veamos ahora la manera en que podemos representar a los elementos de ${}_p\mathbb{Q}^*$. De la cadena de ideales y de subgrupos

$$\cdots \subseteq (p^k) \subseteq \cdots \subseteq (p^2) \subseteq (p) \subseteq ({}_p\mathbb{Q}),$$

se tiene que ${}_p\mathbb{Q}/(p) \cong \mathbb{Z}(p)$, ya que (p) es un ideal máximo. Notemos también que

$$p^k({}_p\mathbb{Q})/p^{k+1}({}_p\mathbb{Q}) \cong \mathbb{Z}(p).$$

Así, si $\{t_0, t_1, \ldots, t_{p-1}\}$ es un sistema completo de representantes de ${}_p\mathbb{Q}$ módulo $(p) = p({}_p\mathbb{Q})$,(por ejemplo, el conjunto $\{0, 1, \ldots, p-1\}$), entonces el conjunto $\{p^k t_0, p^k t_1, \ldots, p^k t_{p-1}\}$ lo es de $p^k({}_p\mathbb{Q})$ módulo $p^{k+1}({}_p\mathbb{Q})$.

Sean $\pi \in ({}_p\mathbb{Q})^*$ y $\{a_n\}_{n=0}^{\infty}$ una sucesión de Cauchy convergente a π. Por como se definió la topología en ${}_p\mathbb{Q}$, cada subgrupo $p^k({}_p\mathbb{Q})$ es un abierto, por lo que cualquier clase lateral de estos subgrupos también lo es. De esta manera, como la sucesión $\{a_n\}_{n=0}^{\infty} \longrightarrow \pi$, casi todas las a_n pertenecen a la misma clase lateral módulo $p({}_p\mathbb{Q})$, la cual denotaremos por s_0. De nuevo por la convergencia, casi todas las diferencias de la forma $a_n - s_0$, con $n \in \mathbb{N}$ y que pertenecen a $p({}_p\mathbb{Q})$, se encuentran en la misma clase lateral de $p({}_p\mathbb{Q})$ módulo $p^2({}_p\mathbb{Q})$, digamos, a la representada por ps_1. Procediendo de esta manera, π va determinando una sucesión de elementos s_0, ps_1, $p^2 s_2, \ldots$, por lo que podemos hacer la asignación

$$\pi \longmapsto s_0 + ps_1 + p^2 s_2 + \cdots,$$

donde las sumas parciales tienen la forma $b_n = s_0 + ps_1 + p^2 s_2 + \cdots + p^n s_n$, para $n = 1, 2, 3, \ldots$. Notemos que estas sumas parciales forman una sucesión de Cauchy en ${}_p\mathbb{Q}$ que converge en ${}_p\mathbb{Q}^*$, ya que, para cualquier abierto básico que contenga a π, de la forma $p^k({}_p\mathbb{Q})$, podemos escoger una $n \in \mathbb{N}$, con $n \geqslant k$ tal que $\pi - b_n \in p^k({}_p\mathbb{Q})$. Por la unicidad de los límites, se sigue que límites distintos en ${}_p\mathbb{Q}^*$, dan lugar a distintas series convergentes. Como toda serie de la forma $s_0 + ps_1 + p^2 s_2 + \cdots$, con coeficientes en un sistema fijo de representantes, define un elemento en ${}_p\mathbb{Q}^*$, podemos identificar a los elementos de ${}_p\mathbb{Q}^*$ con las series formales $s_0 + ps_1 + p^2 s_2 + \cdots$, con coeficientes en $\{t_0, t_1, \ldots, t_{p-1}\}$. Preferentemente tomaremos el conjunto $\{0, 1, 2, \ldots, p-1\}$. Así, podemos escribir $\pi = s_0 + ps_1 + p^2 s_2 + \cdots$, donde $s_n = 0, 1, 2, \ldots, p-1$. Obsérvese que ${}_p\mathbb{Q}^*$ tiene cardinalidad del continuo.

Definición 8.4.1. *El anillo ${}_p\mathbb{Q}^*$ es el anillo de los enteros p-ádicos. El grupo aditivo de ${}_p\mathbb{Q}^*$ lo denotaremos por J_p.*

Observación. *De la misma manera en que demostramos que todo p-grupo A es un ${}_p\mathbb{Q}$-módulo, podemos concluir que todo p-grupo A es un ${}_p\mathbb{Q}^*$-módulo de la siguiente manera: si $\pi = s_0 + s_1 p + \cdots + s_n p^n + \cdots \in \mathbb{Q}_p^*$ y $a \in A$ tiene orden p^n, definimos a*

$$\pi a = (s_0 + s_1 p + \cdots + s_{n-1} p^{n-1})a.$$

Observación. *El espacio topológico ${}_p\mathbb{Q}^*$ es primero numerable.*

8.5. Completación topológica por límites inversos

Sean A un grupo topológico y $\{U_i\}_{i\in I}$ un sistema de vecindades abiertas de subgrupos del 0. Para cada $i \in I$, definimos a $C_i = A/U_i$. Como las vecindades están ordenadas por $\leq$, donde $i \leq j$ si y sólo si $U_j \leq U_i$, se tiene que, para $i \leq j$, la función $\rho_i^j : C_j \longrightarrow C_i$ con regla de correspondencia $(a + U_j) \longmapsto (a + U_i)$ está bien definida. En efecto, si $a + U_j = b + U_j$, entonces $a - b \in U_j \subset U_i$, por lo que $a + U_i = b + U_i$. Es claro que cada ρ_i^j es un morfismo, y que la familia $\{\rho_i^j\}_{i\leq j}$ satisface las propiedades de ser un sistema inverso, por lo que el sistema $\{C_i, i \in I; \rho_i^j\}$ define un límite inverso $\widehat{C}$. Nótese que por ser cada U_i un subgrupo abierto en la topología, también es un conjunto cerrado. Esto implica que cada grupo $C_i = A/U_i$ es un grupo discreto. Además, obsérvese que $\widehat{C}$ tiene la topología inducida por la topología caja en el producto directo $\Pi_{i\in I}C_i$, con lo cual, las vecindades abiertas $\{V_i\}_{i\in I}$ del cero en $\widehat{C}$ son los subgrupos de la forma $\widehat{C} \cap \pi_j^{-1}(0)$, donde $\pi_j : \Pi_{i\in I}C_i \longrightarrow C_j$ es el morfismo proyección en el término j-ésimo.

Por otra parte, definimos la función $\alpha : A \longrightarrow \widehat{C}$ con regla de correspondencia

$$a \longmapsto (\cdots, a + U_i, \cdots),$$

es decir, $(\cdots, a+U_i, \cdots)$ es tal que su entrada j-ésima es de la forma $a+U_j$. Nótese que

$$(\cdots, a + U_i, \cdots) \in \widehat{C},$$

ya que, si $j \geq i$, entonces $\rho_i^j(a + U_j) = a + U_i$. Además, α es un morfismo puesto que para cualquier $i \in I$ se cumple que

$$(a + b) + U_i = (a + U_i) + (b + U_i),$$

con lo cual, se sigue que

$$a + b \longmapsto (\cdots, (a + b) + U_i, \cdots) = (\cdots, a + U_i, \cdots) + (\cdots, b + U_i, \cdots).$$

Por otro lado, al tener $\widehat{C}$ la topología inducida por los abiertos sub-básicos de la forma $\pi_j^{-1}(0)$, donde el cero en C_j es la clase del subgrupo U_j en A, se tiene que α es un morfismo abierto y continuo. En efecto, basta ver que para cada subbásico $\pi_i^{-1}(0)$, $\alpha(\pi_i^{-1}(0))$ es un abierto. Si $a \in A$ y $(\cdots, a + U_i, \cdots) \in \widehat{C} \cap \pi_i^{-1}(0)$, entonces $a \in U_i$, por lo que

$$\alpha(a+U_i) \subset \widehat{C} \cap \pi_i^{-1}(0).$$

Más aún, $\alpha^{-1}(\widehat{C} \cap \pi_i^{-1}(0)) = U_i$, teniendo así que α es abierta y continua.

Proposición 8.5.1. *Existe un morfismo $\lambda : \widehat{A} \longrightarrow \widehat{C}$ continuo y abierto tal que $\lambda \circ \mu = \alpha$.*

Demostración. Sea $\{a_i\}_{i\in I}$ una red nítida de Cauchy, representante de la clase $\{a_i\}_{i\in I} + E$ en $\widehat{A}$. Definimos la función $\lambda : \widehat{A} \longrightarrow \widehat{C}$ por

$$\{a_i\}_{i\in I} + E \longmapsto (\cdots, a_i + U_i, \cdots),$$

es decir, donde el término j-ésimo de la imagen es $a_j + U_j$. Nótese que el elemento $(\cdots, a_i + U_i, \cdots) \in \widehat{C}$, ya que, por ser $\{a_i\}_{i\in I}$ una red nítida de Cauchy, se cumple que $\forall j \geq i$, $a_j - a_i \in U_i$, , es decir, $a_j + U_i = a_i + U_i$, lo cual implica que

$$\rho_i^j(a_j + U_j) = a_j + U_i = a_i + U_i.$$

Por otro lado, λ es un morfismo pues

$$\begin{gathered}\lambda([\{a_i\}_{i\in I} + E] + [\{b_i\}_{i\in I} + E]) = \lambda(\{a_i + b_i\}_{i\in I} + E)\\ = (\cdots, (a_i + b_i) + U_i, \cdots) = (\cdots, a_i + U_i, \cdots) + (\cdots, b_i + U_i, \cdots)\\ = \lambda(\{a_i\}_{i\in I} + E) + \lambda(\{b_i\}_{i\in I} + E).\end{gathered}$$

Veamos ahora que λ está bien definida. Supongamos que

$$\{a_i\}_{i\in I} + E = \{b_i\}_{i\in I} + E.$$

Esto quiere decir que $\{a_i\}_{i\in I} - \{b_i\}_{i\in I} = \{a_i - b_i\}_{i\in I} \in E$. Como E es el conjunto de las redes nítidas de Cauchy en A que convergen al cero, dada cualquier $i \in I$, para $j \geq i$, se cumple tanto $(a_j - b_j) - (a_i - b_i) \in U_i$, por ser $\{a_i - b_i\}_{i\in I}$ una red de Cauchy, así como $a_j - b_j \in U_i$, por la convergencia de $\{a_i - b_i\}_{i\in I}$ a 0. Por ser U_i un subgrupo, se sigue que $a_i - b_i \in U_i$. Como este argumento es para cualquier $i \in I$, tenemos que

$$\begin{gathered}\lambda([\{a_i\}_{i\in I} - \{b_i\}_{i\in I}] + E) = \lambda([\{a_i - b_i\}_{i\in I}] + E)\\ = (\cdots, (a_i - b_i) + U_i, \cdots) = 0 \in \widehat{C},\end{gathered}$$

puesto que $a_i - b_i \in U_i$, $\forall i \in I$. Esto implica que

$$\lambda(\{a_i\}_{i\in I} + E) = \lambda(\{b_i\}_{i\in I} + E).$$

Obsérvese que, de este argumento, se sigue también que si

$$\lambda(\{a_i\}_{i\in I} + E) \neq \lambda(\{b_i\}_{i\in I} + E),$$

entonces $\{a_i\}_{i\in I}+E \neq \{b_i\}_{i\in I}+E$, mostrando así que λ es un monomorfismo.

Por otra parte, si $(\cdots, a_i + U_i, \cdots) \in \widehat{C}$, entonces el conjunto $\{a_i\}_{i\in I}$ es una red nítida de Cauchy. En efecto, para cualquier $i \in I$, si $j \geq i$ entonces

$$a_i + U_i = \rho_i^j(a_j + U_j) = a_j + U_i,$$

donde la primera igualdad es debido a que $(\cdots, a_i + U_i, \cdots)$ es un elemento del límite inverso $\widehat{C}$, y la segunda se sigue por la definición de ρ_i^j. Por lo tanto, se cumple que $a_j - a_i \in U_i$, $\forall j \geq i$. Esto también implica que λ es un epimorfismo. Además, notemos que si $(\cdots, b_i + U_i, \cdots)$ es otro elemento que representa a $(\cdots, a_i + U_i, \cdots)$, entonces las redes $\{a_i\}_{i\in I}$ y $\{b_i\}_{i\in I}$, asociadas a cada elemento respectivamente, satisfacen que

$$\lambda(\{a_i\}_{i\in I} + E) = \lambda(\{b_i\}_{i\in I} + E),$$

que por lo visto anteriormente, implica que $\{a_i\}_{i\in I} + E = \{b_i\}_{i\in I} + E$. Por lo tanto, λ es un isomorfismo.

Por otra parte, observemos que para cualquier básico de la forma $\pi_i^{-1}(0)$ en $\Pi_{i\in I} C_i$, se tiene que

$$\lambda^{-1}(\widehat{C} \cap \pi_i^{-1}(0)) = [C \cap \pi_i^{-1}(U_i)] + E,$$

ya que los elementos $(\cdots, a_i + U_i, \cdots)$ en $\widehat{C} \cap \pi_i^{-1}(0)$ son aquellos que en su término i-ésimo cumplen que $a_i \in U_i$, así como los elementos de $C \cap \pi_i^{-1}(U_i)$ son redes $\{a_i\}_{i\in I}$ tales que $a_i \in U_i$. Esto muestra que λ manda vecindades básicas en vecindades básicas, con lo cual, λ es un morfismo tanto abierto como continuo. Por lo tanto, λ es un isomorfismo topológico. $\square$

Ahora, como $\widehat{C}$ fue construido usando límites inversos, éste posé la propiedad universal de los límites inversos. Esto demuestra que la completación $\widehat{A}$ de un grupo A es única salvo isomorfismos, con lo cual conlcuimos que $\widehat{A} \cong \widehat{C}$.

Teorema 8.5.2. *Sean A un grupo y G un grupo completo. Para cualquier morfismo continuo $\varphi : A \longrightarrow G$, existe un único morfismo continuo $\widehat{\varphi} : \widehat{A} \longrightarrow G$ tal que $\widehat{\varphi} \circ \mu = \varphi$.*

Demostración. Como $A \subset \widehat{A}$, podemos considerar a la red $\{a_i\}_{i\in I}$ de Cauchy en A con límite $\widehat{a} \in \widehat{A}$. Como la función φ es continua, el conjunto $\{\varphi(a_i)\}_{i\in I}$ es una red de Cauchy en G. Por ser G un grupo completo, la red $\{\varphi(a_i)\}_{i\in I}$ converge a un elemento $g \in G$. Con esto en cuenta, definimos la función $\widehat{\varphi} : \widehat{A} \longrightarrow \widehat{C}$ por $\widehat{a} \longmapsto g$. Se sigue que $\widehat{\varphi}$ es un morfismo de grupos continuo.

Por otra parte, si $a \in A$ es tal que $\varphi(a) = g \in G$, como

$$\mu(a) = ((\cdots, a, \cdots, a, \cdots) + E) = \{a_i\}_{i\in I} + E,$$

con $a_i = a$, para toda $i \in I$, se tiene que

$$\widehat{\varphi} \circ \mu(a) = \widehat{\varphi}(\{a_i\}_{i\in I} + E) = \{\varphi(a_i)\}_{i\in I} = \varphi(a)_{i\in I} = \{g_i\}_{i\in I},$$

donde $g_i = g$, para toda $i \in I$. Como la red constante $\{g_i\}_{i\in I}$, con $g_i = g$, converge al elemento $g \in G$, concluimos que $\widehat{\varphi} \circ \mu = \varphi$. $\square$

Observación. *De los dos últimos teoremas, se sigue que $\widehat{A}$ es único salvo isomorfismos topológicos.*

Observación. *Cuando construimos los enteros p-ádicos, concideramos al conjunto de ideales $\{p^k\mathbb{Q}_p \mid k \in \mathbb{N}\}$ de $\mathbb{Q}_p$, como el sistema de vecindades básicas del 0. Por lo visto anteriormente, podemos concluir que J_p es el límite inverso del sistema inverso, formado por los cocientes $C_i = \mathbb{Q}_p/p^i\mathbb{Q}_p$ y los morfismos $\rho_i^j : C_j \longrightarrow C_i$, cuya regla de correspondencia es*

$$a + \mathbb{Q}_p/p^j\mathbb{Q}_p \longmapsto a + \mathbb{Q}_p/p^i\mathbb{Q}_p, \text{ para } j \geq i.$$

Notemos que dichos morfismos están bien definidos. En efecto, si

$$a + \mathbb{Q}_p/p^j\mathbb{Q}_p = b + \mathbb{Q}_p/p^j\mathbb{Q}_p,$$

se tiene que $a - b \in p^j\mathbb{Q}_p$, es decir, $a - b = p^j s$, para algún $s \in \mathbb{N}$. Como $j \geq i$ en el orden de $\mathbb{N}$, se tiene que $a - b = p^i(p^{j-i}s)$, por lo que $a - b \in p^i\mathbb{Q}_p$, con lo cual,

$$a + \mathbb{Q}_p/p^i\mathbb{Q}_p = b + \mathbb{Q}_p/p^i\mathbb{Q}_p.$$

Notemos también que cada C_i es un grupo de orden p^i. En efecto, para cualquier $a + \mathbb{Q}_p/p^i\mathbb{Q}_p \in C_i$ se cumple que

$$p^i(a + \mathbb{Q}_p/p^i\mathbb{Q}_p) = p^i a + \mathbb{Q}_p/p^i\mathbb{Q}_p \in p^i\mathbb{Q}_p.$$

Así, el límite inverso del sistema inverso, formado por los grupos $< c_i >$, *donde* c_i *tiene orden* p^i, *junto con la familia de morfismos*

$$\rho_i^j :< c_j > \longrightarrow < c_i >,$$

definidos por $c_j \longmapsto c_i$, *para cada* $j \geq i$, *es isomorfo al grupo aditivo del anillo de los enteros p-ádicos, es decir,*

$$J_p \cong \varprojlim_{i \in \mathbb{N}} < c_i > .$$

Capítulo 9

Categorías

9.1. Propiedades

A lo largo del capítulo, usaremos las letras mayúsculas A, B, C, D, X, Y, Z, junto con $A', B', C', D', X', Y', Z'$, para referirnos a los objetos de una categoría; las letras minúsculas f, g, h, representarán morfismos entre objetos. Además, si $F : \mathcal{C} \longrightarrow \mathcal{D}$ es un funtor, entonces $F(X)$ y $F(f)$ representarán objetos y morfismos, respectivamente, en la categoría $\mathcal{D}$.

Ejemplo. *Sean Top y Set, las categorías de espacios topológicos y de conjuntos, respectivamente. La asignación $U : Top \longrightarrow Set$, que manda a cada espacio topológico X a su conjunto X es un funtor. En este caso, decimos que el funtor U se olvida de la estructura matemática de cada objeto.*

Sean $\mathcal{C}$, $\mathcal{D}$, $\mathcal{E}$ categorías y $F : \mathcal{C} \longrightarrow \mathcal{D}$, $G : \mathcal{D} \longrightarrow \mathcal{E}$ funtores entre ellas. Si $X, Y \in \mathcal{C}$ y $f : X \longrightarrow Y$, la composición $GF : \mathcal{C} \longrightarrow \mathcal{E}$, definida por:

$$GF(X) = G(F(X)) \text{ y } GF(f) = G(F(f)) : G(F(X)) \longrightarrow G(F(Y)),$$

es un funtor. En efecto, si $X \xrightarrow{f} Y \xrightarrow{g} Z$ son elementos en $\mathcal{C}$, entonces

$$GF(g \circ f) = G(F(g) \circ F(f)) = GF(g) \circ GF(f).$$

Además, como F y G son funtores, también se cumple que

$$GF(Id_X) = G(Id_{F(X)}) = Id_{GF(X)}.$$

Nótese que la composición de funtores es asociativa.

Observación. *Como para cada categoría $\mathcal{C}$, se tiene el funtor identidad*

$$Id : \mathcal{C} \longrightarrow \mathcal{C},$$

obtenemos la categoría Cat, que tiene como objetos a categorías y morfismos a los funtores entre categorías.

Por otra parte, cada categoría $\mathcal{C}$, define una categoría, que llamamos la categoría dual de $\mathcal{C}$ y la denotamos por $\mathcal{C}^{op}$. Los objetos de $\mathcal{C}^{op}$ son los mismos que los de la categoría $\mathcal{C}$, pero los morfismos están invertidos en el siguiente sentido:

$$Hom_{\mathcal{C}^{op}}(X,Y) = Hom_{\mathcal{C}}(Y,X),$$

es decir, si $f : X \longrightarrow Y$ es un morfismo en $\mathcal{C}$, entonces $f \in Hom_{\mathcal{C}^{op}}(Y,X)$. A este último morfismo, lo escribimos como $\bar{f}$. Ahora, si $\bar{f} : Y \longrightarrow X$ y $\bar{g} : Z \longrightarrow Y$ son dos morfismos en $\mathcal{C}^{op}$, la composición en $\mathcal{C}^{op}$ está dada por

$$\bar{f} \circ \bar{g} = \overline{g \circ f}.$$

Con esto en cuenta, se obtiene el funtor $F : \mathcal{C} \longrightarrow \mathcal{C}^{op}$, donde para cada objeto $C \in \mathcal{C}$, $F(C) = C$ y para cada morfismo $C \xrightarrow{g} D$ en $\mathcal{C}$, $F(g) = \bar{g}$. De esta manera, se tienen los diagramas conmutativos

$$\begin{tikzcd} C \arrow[r] \arrow[d, "g"'] & C \\ D \arrow[r] & D \arrow[u, "\bar{g}"'] \end{tikzcd}.$$

Esto nos lleva al siguiente concepto:

Definición 9.1.1. *Decimos que un funtor $F : \mathcal{C} \longrightarrow \mathcal{D}$ es contravariante si invierte la dirección de las flechas o morfismos, es decir, si $f : X \longrightarrow Y$ es un morfismo en $\mathcal{C}$, entonces $F(f) : F(Y) \longrightarrow F(X)$. Un funtor F es covariante, si preserva la dirección de los morfismos.*

Notemos también que cualquier funtor $F : \mathcal{C} \longrightarrow \mathcal{D}$ induce otro funtor $F^{op} : \mathcal{C}^{op} \longrightarrow \mathcal{D}^{op}$, tal que, a cada objecto $X \in \mathcal{C}^{op}$ le asigna el objeto $F(X) \in \mathcal{D}^{op}$, y a cada morfismo $\bar{f}$ en $\mathcal{C}^{op}$, le asigna la flecha $\overline{F(f)}$ en $\mathcal{D}^{op}$. De esta manera, se obtienen los diagramas conmutativos de la forma

$$\begin{tikzcd} C \arrow[r] \arrow[d, "\bar{f}"'] & F(C) \arrow[d, "\overline{F(f)}"] \\ D \arrow[r] & F(D) \end{tikzcd}.$$

Más aún, esto nos define el funtor $(-)^{op} : Cat \longrightarrow Cat$, donde a cada $\mathcal{C} \in Cat$, se le asocia su categoría dual $\mathcal{C}^{op} \in Cat$, y a cada funtor $F : \mathcal{C} \longrightarrow \mathcal{D}$, el funtor $F^{op} : \mathcal{C}^{op} \longrightarrow \mathcal{D}^{op}$.

Ejemplo. *Sean G un grupo y G' el subgrupo conmutador de G. Ahora, en los preliminares se demuestra que G/G' es un grupo abeliano. A este proceso lo llamamos la abelianización del grupo G. Además, si H es cualquier otro grupo y $\varphi : G \longrightarrow H$ es un morfismo de grupos, entonces se tiene que $\varphi(G') \subset H'$. Más aún, cuando φ es un epimorfismo, se obtiene la igualdad $\varphi(G') = H'$.*

Esto nos permite definir la función $\overline{\varphi} : G/G' \longrightarrow H/H'$, con regla de correspondencia $a + G' \longmapsto \varphi(a) + H'$, la cual está bien definida. En efecto, si $a_1 + G' = a_2 + G'$, entonces $a_1 - a_2 \in G'$, por lo que $\varphi(a_1 - a_2) \in H'$, es decir, $\varphi(a_1) + H' = \varphi(a_2) + H'$. Lo anterior muestra que se tiene un funtor de la categoría Grp a la categoría Ab, tal que a cada grupo G se le asocia el grupo abeliano G/G', y a cada morfismo de grupos $\varphi : G \longrightarrow H$, el morfismo $\overline{\varphi} : G/G' \longrightarrow H/H'$. Por obvias razones, a este funtor se le llama el funtor de abelianización.

Definición 9.1.2. *Sean I un conjunto y $\{\mathcal{C}_i\}_{i\in I}$ una familia de categorías. La categoría producto $\Pi_{i\in I}\mathcal{C}_i$ tiene como objetos a los conjuntos de la forma $\Pi_{i\in I}Ob(\mathcal{C}_i)$ y*

$$Hom((\mathcal{C}_i)_{i\in I}, (D_i)_{i\in I}) = \Pi_{i\in I}Hom(\mathcal{C}_i, \mathcal{D}_i),$$

donde la composición se define componente a componente.

Observación. *En caso de que I sea finito, a la categoría producto la denotamos por $\mathcal{C}_1 \times \cdots \times \mathcal{C}_n$.*

Para cada $i \in I$, surge de manera natural el funtor $\rho_i : \Pi_{i\in I}\mathcal{C}_i \longrightarrow \mathcal{C}_i$, donde a cada objeto $\Pi_{i\in I}Ob(\mathcal{C}_i)$ en la categoría producto, se le asocia el i-ésimo objeto $Ob(\mathcal{C}_i)$, y a cada morfismo $Hom((\mathcal{C}_i)_{i\in I}, (D_i)_{i\in I})$ se le asigna el correspondiente $Hom(\mathcal{C}_i, \mathcal{D}_i)$.

Definición 9.1.3. *Una categoría $\mathcal{C}$ es preaditiva si cada conjunto $Hom_{\mathcal{C}}(C, C')$ es un grupo abeliano y la composición de funciones*

$$Hom_{\mathcal{C}}(C', C'') \times Hom_{\mathcal{C}}(C, C') \longrightarrow Hom_{\mathcal{C}}(C, C'')$$

resulta ser bilineal.

Definición 9.1.4. *Sean $\mathcal{C}$ y $\mathcal{D}$ dos categorías preaditivas. Decimos que un funtor $T : \mathcal{D} \longrightarrow \mathcal{C}$ es aditivo si satisface que $T(\alpha+\alpha') = T(\alpha)+T(\alpha')$, para cualquier $\alpha, \alpha' : C \longrightarrow C'$.*

Observación. *Un funtor $T : \mathcal{D} \longrightarrow \mathcal{C}$ es aditivo si y sólo si las funciones*

$$Hom_{\mathcal{D}}(D, D') \longrightarrow Hom_{\mathcal{C}}(T(D), T(D'))$$

son morfismos de grupos.

Sea $\mathcal{C}$ una categoría chica. Definimos el funtor

$$Hom_{\mathcal{C}} : (\mathcal{C}^{op} \times \mathcal{C}) \longrightarrow Sets$$

de la siguiente manera: a cada objeto (C, D) en el producto $\mathcal{C}^{op} \times \mathcal{C}$ le asignamos el conjunto $Hom_{\mathcal{C}}(C, D)$, y al par $f : C' \longrightarrow C$, $g : D \longrightarrow D'$ de morfismos en $\mathcal{C}$, se le asigna la flecha

$$Hom(f, g) : Hom(C, D) \longrightarrow Hom(C', D'),$$

con regla de correspondencia $\varphi \longmapsto g \circ \varphi \circ f$. De esta manera, se obtienen los diagramas conmutativos

$$\begin{tikzcd}
(C, D) \arrow[r] \arrow[d, "(\overline{f},g)"'] & Hom_{\mathcal{C}}(C, D) \arrow[d, "Hom(\overline{f},g)"] \\
(C', D') \arrow[r] & Hom_{\mathcal{C}}(C', D')
\end{tikzcd} .$$

Observación. *El funtor $Hom_{\mathcal{C}}$ es un funtor covariante.*

Observación. *. Cuando $\mathcal{C}$ es una categoría preaditiva, $Hom(f, g)$ es un morfismo de grupos, por lo que en este caso, $Hom_{\mathcal{C}}$ es un funtor de $\mathcal{C}^{op} \times \mathcal{C} \longrightarrow Ab$.*

Definición 9.1.5. *Sean A, B anillos y $T : Mod-A \longrightarrow Mod-B$ un funtor aditivo. Decimos que T es un funtor exacto si manda sucesiones exactas en la categoría $Mod - A$ a sucesiones exactas en la categoría $Mod - B$. Así mismo, T es un funtor exacto izquierdo si manda sucesiones exactas*

$$0 \hookrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

en $Mod - A$, a sucesiones exactas en $Mod - B$ de la forma

$$0 \hookrightarrow T(M') \longrightarrow T(M) \longrightarrow T(M'').$$

De manera similar, se define lo que es un funtor exacto derecho.

9.2. Transformaciones naturales

Definición 9.2.1. *Una transformación natural entre los funtores* $F, G : \mathcal{C} \longrightarrow \mathcal{D}$*, consiste en una familia de morfismos* $\{\mu_C : F(C) \longrightarrow G(C)\}_{C \in \mathcal{C}}$ *en* $\mathcal{D}$*, etiquetados por los objetos de* $\mathcal{C}$*, tales que para cada morfismo* $f : C \longrightarrow C'$ *en* $\mathcal{C}$*, se tienen los diagramas conmutativos:*

$$\begin{tikzcd} F(C) \arrow[r, "\mu_C"] \arrow[d, "F(f)"'] & G(C) \arrow[d, "G(f)"] \\ F(C') \arrow[r, "\mu_{C'}"] & G(C') \end{tikzcd} .$$

Además, cuando cada μ_C *es un isomorfismo, llamamos a la transformación natural un isomorfismo natural o equivalencia natural.*

Notación. Denotaremos por $\mu = \{\mu_C\}_{C \in \mathcal{C}} : F \Longrightarrow G$ a la transformación natural entre los funtores F y G.

Observación. *Si* $\mu : F \Longrightarrow G$ *y* $\nu : G \Longrightarrow H$ *son dos transformaciones naturales, se obtiene la transformación natural* $\nu\mu = \{\nu_C \mu_C\}_{C \in \mathcal{C}} : F \Longrightarrow H$*, de tal manera que para cualquier morfismo* $f : C \longrightarrow C'$*, se tienen los diagramas conmutativos*

$$\begin{tikzcd} F(C) \arrow[r, "\mu_C"] \arrow[d, "F(f)"'] & G(C) \arrow[r, "\nu_C"] \arrow[d, "G(f)"] & H(C) \arrow[d, "H(f)"] \\ F(C') \arrow[r, "\mu_{C'}"] & G(C') \arrow[r, "\nu_{C'}"] & H(C') \end{tikzcd} .$$

Esta composición es asociativa.

Observación (Categoría de funtores)**.** *Si* $\mathcal{B}$ *es una categoría y* $\mathcal{A}$ *es una categoría pequeña, entonces* $\mathcal{B}^{\mathcal{A}}$ *es la categoría cuyos objetos son funtores* $F : \mathcal{A} \longrightarrow \mathcal{B}$ *y los morfismos son transformaciones naturales entre funtores.*

Ejemplo. *Sean* $\mathcal{C}$ *una categoría chica y* $C \in \mathcal{C}$ *un objeto. Definimos la función* $h_C : \mathcal{C}^{op} \longrightarrow Sets$ *por* $h_C(D) = Hom_{\mathcal{C}^{op}}(C, D)$*. Así, para cada* $C' \overset{\overline{g}}{\longrightarrow} C''$ *en* $\mathcal{C}^{op}$*, se tiene la función*

$$h_C(\overline{g}) : Hom_{\mathcal{C}^{op}}(C, C') \longrightarrow Hom_{\mathcal{C}^{op}}(C, C'')$$

con regla de correspondencia $\overline{\varphi} \longmapsto \overline{\varphi \circ g} = \overline{g} \circ \overline{\varphi}$. *Con esto en cuenta, se obtienen los diagramas*

$$\begin{tikzcd} C' \arrow[r] \arrow[d, "\overline{g}"'] & Hom_{\mathcal{C}^{op}}(C, C') \arrow[d, "h_C(\overline{g})"] \\ C'' \arrow[r] & Hom_{\mathcal{C}^{op}}(C, C'') \end{tikzcd} .$$

Esto muestra que h_C *es un funtor covariante. Obsérvese que cada* $C \in \mathcal{C}$, *define un functor* h_C.

Por otra parte, sean $C \xrightarrow{g} D$ *un morfismo en* $\mathcal{C}$ *y* $X, \in \mathcal{C}$. *Definimos la función*

$$\eta_{g,X} : Hom_{\mathcal{C}^{op}}(C, X) \longrightarrow Hom_{\mathcal{C}^{op}}(D, X)$$

con regla de correspondencia $\overline{\varphi} \longmapsto \overline{g \circ \varphi} = \overline{\varphi} \circ \overline{g}$. *Ahora, si* $X \xrightarrow{\overline{\alpha}} Y$, *las funciones* $\eta_{g,X}$ *y* $\eta_{g,Y}$ *inducen los diagramas conmutativos*

$$\begin{tikzcd} Hom_{\mathcal{C}^{op}}(C, X) \arrow[r, "\eta_{g,X}"] \arrow[d, "h_C(\overline{\alpha})"'] & Hom_{\mathcal{C}^{op}}(D, X) \arrow[d, "h_D(\overline{\alpha})"] \\ Hom_{\mathcal{C}^{op}}(C, Y) \arrow[r, "\eta_{g,Y}"] & Hom_{\mathcal{C}^{op}}(D, Y) \end{tikzcd} .$$

En efecto, para cualquier $\overline{\xi} \in Hom_{\mathcal{C}^{op}}(C, X)$, *se tiene que*

$$h_D(\overline{\alpha}) \circ \eta_{g,X}(\overline{\xi}) = h_D(\overline{\alpha})(\overline{\xi} \circ \overline{g}) = \overline{\alpha} \circ (\overline{\xi} \circ \overline{g}),$$

así como

$$\eta_{g,Y} \circ h_C(\overline{\alpha})(\overline{\xi}) = \eta_{g,Y}(\overline{\alpha} \circ \overline{\xi}) = (\overline{\alpha} \circ \overline{\xi}) \circ \overline{g}.$$

La conmutatividad del diagrama se sigue de la asociatividad de la operación en $Hom_{\mathcal{C}^{op}}(D, Y)$. *Nótese que para cada* $C \xrightarrow{g} D$, *las funciones* $\eta_{g,X}$ *son morfismos en Sets, etiquetadas por los objetos de* $\mathcal{C}$, *mostrando así que* $\eta_g = \{\eta_{g,X}\}_{X \in \mathcal{C}}$ *es una transformación natural entre los funtores* h_D *y* h_C.

Por lo tanto, la función $Y : \mathcal{C} \longrightarrow Sets^{\mathcal{C}^{op}}$, *donde a cada objeto* $C \in \mathcal{C}$ *le asocia el funtor* h_C, *y a cada morfismo* $C \xrightarrow{g} D$ *en* $\mathcal{C}$, *la transformación natural* η_g, *es un funtor.*

9.3. Funtores adjuntos

Dados los funtores $F : \mathcal{C} \longrightarrow \mathcal{D}$ y $G : \mathcal{D} \longrightarrow \mathcal{C}$, nos podemos preguntar ¿qué tanto se parecen las composiciones, en ambos sentidos, a los funtores identidad? En otras palabras, ¿de qué manera podemos comparar FG con $Id_{\mathcal{D}}$, así como GF con $Id_{\mathcal{C}}$? El siguiente ejemplo nos dará una idea sobre la noción de funtores adjuntos.

Ejemplo. *Para cualquier conjunto X, podemos formar el espacio vectorial $V(X)_K$, sobre el campo K, el cual tiene como base al conjunto X. Así, todo vector es una combinación lineal de la forma $\Sigma_{i\in I} r_i x_i$, con I un conjunto finito, $r_i \in K$ y $x_i \in X$. Además, por ser K un campo, el conjunto X está sumergido en $V(X)_K$ de la siguiente manera: $x \hookrightarrow 1x$, donde $1 \in K$ es el neutro multiplicativo. Ahora, si K es un campo fijo, al considerar la categoría Vct_K de todos los espacios vectoriales sobre el campo K, y la categoría $Sets$ de todos los conjuntos, se tiene el funtor $U : Vct_K \longrightarrow Sets$, donde a cada espacio vectorial W le asocia el conjunto $U(W)$ formado por todos los vectores de W, es decir, el funtor U se olvida de la estructura de los objetos en la categoría Vct_K.*

Por otro lado, definimos la función $V : Sets \longrightarrow Vct_K$, tal que a cada conjunto X le asocia el espacio vectorial $V(X)_K$. Observemos que la función V es un funtor. En efecto, cada función $g : X \longrightarrow Y$, se extiende de manera única a una transformación lineal $\hat{g} : V(X)_K \longrightarrow V(Y)_K$, a saber, la que tiene regla de correspondencia

$$\hat{g}(\Sigma_{i\in I} r_i x_i) = \Sigma_{i\in I} r_i g(x_i).$$

De esta manera, si $W \in Vct_K$ y $X \in Sets$, se tiene la correspondencia

$$\varphi_{X,W} : Hom_{Sets}(X, U(W)) \longrightarrow Hom_{Vct_K}(V(X)_K, W),$$

donde a cada $g : X \longrightarrow U(W)$ se le asigna la función $\hat{g} : V(X)_K \longrightarrow W$. Nótese también que la función

$$\psi_{X,W} : Hom_{Vcts_K}(V(X)_K, W) \longrightarrow Hom_{Sets}(X, U(W))$$

definida por

$$\psi_{X,W}(g) = g\mid_X$$

es inversa de $\varphi_{X,W}$. En efecto, si $X \xrightarrow{g} U(W)$, como $X \subset V(X)_K$, se cumple que

$$\hat{g}(x) = \hat{g}(1x) = 1g(x) = g(x),$$

por lo que

$$[\psi_{X,W} \circ \varphi_{X,W}](g) = \psi_{X,W}(\hat{g}) = \hat{g} \mid_X = g,$$

es decir, $\psi_{X,W} \circ \varphi_{X,W} = Id_{Hom(X,U(W))}$. *Ahora, como todo elemento en* $V(X)_K$ *se expresa de manera única en términos de la base* X, *y cualquier función lineal entre espacios vectoriales está determinada por los valores que toma en dicha base, si* $V(X)_K \xrightarrow{f} W$, *se sigue que*

$$\varphi_{X,W} \circ \psi_{X,W}(f) = \varphi_{X,W}(f \mid_X) = f,$$

por lo que $\varphi_{X,W} \circ \psi_{X,W} = Id_{Hom(V(X),W)}$. *Esto muestra que hay una biyección entre los conjuntos*

$$Hom_{Vct_K}(V(X), W) \text{ y } Hom_{Sets}(X, U(W)).$$

Obsérvese que las funciones $\varphi_{X,W}$ *y* $\psi_{X,W}$ *se definieron para cada* $X \in Sets$ *y* $W \in Vcts_K$, *por lo que en realidad, tenemos una familia de funciones biyectivas*

$$\psi_{X,W} : Hom_{Sets}(X, U(W)) \longrightarrow Hom_{Vct_K}(V(X), W).$$

Consideremos ahora a los funtores $F_U : Sets^{op} \times Vcts_K \longrightarrow Sets$, *definido por*

$$F_U(X, W) = Hom_{Sets}(X, U(W)),$$

y $F_V : Sets^{op} \times Vcts_K \longrightarrow Sets$ *con regla de correspondencia*

$$F_V(X, W) = Hom_{Vct_K}(V(X)_K, W),$$

Con esto en cuenta, la familia de morfismos $\{\psi_{X,W}\}_{X,W \in Sets^{op} \times Vcts_K}$ *es una transformación natural entre los funtores* F_V *y* F_U. *Más aún, si* $h : X' \longrightarrow X$, *el diagrama siguiente conmuta:*

$$\begin{tikzcd}
Hom_{Vct_K}(V(X), W) \arrow[r, "\psi_{X,W}"] \arrow[d, "\eta=()\circ\hat{h}"'] & Hom_{Sets}(X, U(W)) \arrow[d, "\nu=()\circ h"] \\
Hom_{Vct_K}(V(X'), W) \arrow[r, "\psi_{X',W}"] & Hom_{Sets}(X', W)
\end{tikzcd}$$

En efecto, para cada $\alpha \in Hom_{Vcts_K}(V(X)_K, W)$, *se tiene la función*

$$(\psi_{X',W} \circ \eta)(\alpha) = \psi_{X',W}(\eta(\alpha)) = \psi_{X',W}(\alpha \circ \hat{h}),$$

tal que, al evaluarla en el elemento $x' \in X'$ *(visto como un elemento en* $V(X')_K$*) se obtiene*

$$[\psi_{X',W}(\alpha \circ \hat{h})](x') = (\alpha \circ \hat{h}) \mid_{X'} (x') = \alpha(\hat{h}(1x')) = \alpha(1h(x')) = \alpha(h(x')).$$

Por otra parte, la función $\nu \circ \psi_{X,W}(\alpha) = \psi_{X,W}(\alpha) \circ h$*, evaluada en el elemento* $x' \in X'$ *es*

$$[\psi_{X,W}(\alpha) \circ h](x') = [\psi_{X,W}(\alpha)](h(x')) = \alpha \mid_X (h(x')) = \alpha(h(x')).$$

Análogamente, si $W \xrightarrow{f} Z$ *es una transformación lineal entre los espacios vectoriales sobre el campo* K*, se tiene que el diagrama*

$$\begin{tikzcd} Hom_{Vct_K}(V(X)_K, W) \arrow[r, "\psi_{X,W}"] \arrow[d, "\eta = f\circ()"'] & Hom_{Sets}(X, U(W)) \arrow[d, "\nu = U(f)\circ()"] \\ Hom_{Vct_K}(V(X)_K, Z) \arrow[r, "\psi_{X,Z}"] & Hom_{Sets}(X, U(Z)) \end{tikzcd} .$$

conmuta. En efecto, si $\alpha \in Hom_{Vct_K}(V(X)_K, W)$*, por una parte obtenemos la función*

$$(\nu \circ \psi_{X,W})(\alpha) = U(f) \circ (\psi_{X,W}(\alpha)) = U(f) \circ \alpha \mid_X$$

la cual, evaluada en $x \in X \subset V(X)_K$*, nos da*

$$(U(f) \circ \alpha)(x) = U(f)(\alpha(1x)) = f(\alpha(x)) = (f \circ \alpha)(x).$$

Por otra parte, se tiene la función

$$[\psi_{X,Z} \circ \eta](\alpha) = \psi_{X,Z}(f \circ \alpha) = f \circ \alpha \mid_X,$$

la cual satisface que $f \circ \alpha \mid_X (x) = (f \circ \alpha)(x)$*, para cualquier* $x \in X$*. Estos dos últimos diagramas conmutativos expresan la idea de naturalidad, en cada* $X \in Sets$ *y* $W \in Vcts_K$*, de dos funtores adjuntos.*

Observación. *Sean* $\mathcal{C}$*,* $\mathcal{D}$ *dos categorías preaditivas y* $T : \mathcal{C} \longrightarrow \mathcal{D}$*,* $S : \mathcal{D} \longrightarrow \mathcal{C}$ *dos funtores aditivos. Definimos el funtor*

$$F : \mathcal{C}^{op} \times \mathcal{D} \longrightarrow Ab$$

por

$$(C, D) \longmapsto Hom_{\mathcal{C}}(C, S(D)).$$

Así, si $\overline{g} : C \longrightarrow C'$, *(es decir,* $g : C' \longrightarrow C$ *en* $\mathcal{C}$*) y* $f : D \longrightarrow D'$, *obtenemos los diagramas*

$$\begin{tikzcd}
(C, D) \arrow[r] \arrow[d, "(\overline{g},f)"'] & Hom_{\mathcal{C}}(C, S(D)) \arrow[d, "F(\overline{g},f)"] \\
(C', D') \arrow[r] & Hom_{\mathcal{C}}(C', S(D'))
\end{tikzcd}$$

donde para cada $\alpha \in Hom_{\mathcal{C}}(C, S(D))$,

$$F(\overline{g}, f)(\alpha) = S(f) \circ \alpha \circ g.$$

Análogamente, se tiene el funtor

$$G : \mathcal{C}^{op} \times \mathcal{D} \longrightarrow Ab$$

definido por $(C, D) \longmapsto Hom_{\mathcal{D}}(T(C), D)$. *En este caso, se obtienen los diagramas*

$$\begin{tikzcd}
(C, D) \arrow[r] \arrow[d, "(\overline{g},f)"'] & Hom_{\mathcal{C}}(T(C), D) \arrow[d, "G(\overline{g},f)"] \\
(C', D') \arrow[r] & Hom_{\mathcal{C}}(T(C'), D')
\end{tikzcd} .$$

tal que, para cada $\alpha \in Hom_{\mathcal{C}}(T(C), D)$,

$$G(\overline{g}, f)(\alpha) = f \circ \alpha \circ T(g).$$

Con esto en cuenta, se tiene la siguiente

Definición 9.3.1. *Sean* $\mathcal{C}$ *y* $\mathcal{D}$ *dos categorías preaditivas. Decimos que el funtor* $T : \mathcal{C} \longrightarrow \mathcal{D}$ *es adjunto izquierdo del funtor* $S : \mathcal{D} \longrightarrow \mathcal{C}$, *(y simétricamente* S *es adjunto derecho de* T*), si los funtores* F *y* G *antes mencionados, son naturalmente equivalentes. Esto es, para cada* $(C, D) \in \mathcal{C}^{op} \times \mathcal{D}$, *se tiene un isomorfismo*

$$\eta_{C,D} : Hom_{\mathcal{C}}(C, S(D)) \longrightarrow Hom_{\mathcal{D}}(T(C), D)$$

tal que, si $g : C' \longrightarrow C$ *y* $f : D \longrightarrow D'$, *los diagramas*

$$\begin{tikzcd}
Hom_{\mathcal{C}}(C, S(D)) \arrow[r, "\eta_{C,D}"] \arrow[d, "F(\overline{g},f)"'] & Hom_{\mathcal{D}}(T(C), D) \arrow[d, "G(\overline{g},f)"] \\
Hom_{\mathcal{C}}(C', S(D')) \arrow[r, "\eta_{C',D'}"] & Hom_{\mathcal{D}}(T(C'), D')
\end{tikzcd}$$

conmutan. Además, para cada objeto $C \in \mathcal{C}$ y $D \in \mathcal{D}$, esta equivalencia natural es natural en C y en D, en el siguiente sentido: si $D \in \mathcal{D}$, la asignación $C \longmapsto \eta_{C,D}$ es una equivalencia natural entre los funtores

$$F_D : \mathcal{C} \longrightarrow Ab \text{ y } G_D : \mathcal{C} \longrightarrow Ab$$

definidos por

$$C \longmapsto Hom_{\mathcal{C}}(C, S(D)) \text{ y } C \longmapsto Hom_{\mathcal{D}}(T(C), D),$$

respectivamente.

Análogamente, la naturalidad en D se refiere a que, para cada objeto $C \in \mathcal{C}$, la asignación $D \longmapsto \eta_{C,D}$ es una equivalencia natural entre los funtores

$$F_C : \mathcal{D} \longrightarrow Ab \text{ y } G_C : \mathcal{D} \longrightarrow Ab$$

definidos por

$$D \longmapsto Hom_{\mathcal{C}}(C, S(D)) \text{ y } D \longmapsto Hom_{\mathcal{D}}(T(C), D),$$

respectivamente.

9.4. Algunas propiedades de funtores adjuntos

Sean $T : \mathcal{C} \longrightarrow \mathcal{D}$ y $S : \mathcal{D} \longrightarrow \mathcal{C}$ dos functores adjuntos, donde $\eta_{C,D}$ es el isomorfismo entre $Hom_{\mathcal{C}}(C, S(D))$ y $Hom_{\mathcal{D}}(T(C), D)$, para cada $C \in \mathcal{C}$, $D \in \mathcal{D}$. Ahora, si $D \in \mathcal{D}$ y $C = S(D)$, entonces se obtiene el isomorfismo

$$\eta_{S(D),D} : Hom_{\mathcal{C}}(S(D), S(D)) \longrightarrow Hom_{\mathcal{D}}(TS(D), D).$$

Como $Id_{S(D)} \in Hom_{\mathcal{C}}(S(D), S(D))$, definimos a la función

$$\xi_D = \eta_{S(D),D}(Id_D) : (TS)(D) \longrightarrow D.$$

Afirmamos que el conjunto $\{\xi_D\}_{D \in \mathcal{D}}$ es una transformación natural entre los funtores TS y Id_D. En efecto, si $f : D \longrightarrow D'$, entonces la condición de naturalidad en D nos garantiza que el diagrama

$$\begin{tikzcd} Hom_{\mathcal{C}}(S(D), S(D)) \arrow[r, "\eta_{S(D),D}"] \arrow[d, "S(f)\circ()"'] & Hom_{\mathcal{D}}(TS(D), D) \arrow[d, "f\circ()"] \\ Hom_{\mathcal{C}}(S(D), S(D')) \arrow[r, "\eta_{S(D),D'}"] & Hom_{\mathcal{D}}(TS(D), D') \end{tikzcd} .$$

sea conmutativo.

Así, para $Id_{S(D)} \in Hom_{\mathcal{C}}(S(D), S(D))$, se tiene que

$$\begin{aligned} f\circ \xi_D &= f\circ \eta_{S(D),D}(Id_{S(D)})\\ &= \eta_{S(D),D'}\circ S(f)\circ Id_{S(D)} = \eta_{S(D),D'}(S(f)). \end{aligned}$$

Por otra parte, por la naturalidad de la transformación natural, ahora en C, para $D' \in \mathcal{D}$, se tiene el diagrama conutativo

$$\begin{tikzcd} Hom_{\mathcal{C}}(S(D'),S(D')) \arrow[r, "\eta_{S(D'),D'}"] \arrow[d, "()\circ S(f)"'] & Hom_{\mathcal{D}}(TS(D),D') \arrow[d, "()\circ TS(f)"] \\ Hom_{\mathcal{C}}(S(D),S(D')) \arrow[r, "\eta_{S(D),D'}"] & Hom_{\mathcal{D}}(TS(D),D') \end{tikzcd}$$

de donde se siguen las igualdades

$$\begin{aligned} \xi_{D'}\circ TS(f) &= \eta_{S(D'),D'}(Id_{S(D')})\circ TS(f)\\ &= \eta_{S(D),D'}(Id_{S(D')}\circ S(f)) = \eta_{S(D),D'}(S(f)) \end{aligned}$$

De esta manera, se obtiene que

$$f\circ \xi_D = \eta_{S(D),D'}(S(f)) = \xi_{D'}\circ TS(f),$$

mostrando así que para cualquier $f : D \longrightarrow D'$ en $\mathcal{D}$, se tiene el diagrama conmutativo

$$\begin{tikzcd} TS(D) \arrow[r, "\xi_D"] \arrow[d, "TS(f)"'] & D \arrow[d, "f"] \\ TS(D') \arrow[r, "\xi_{D'}"'] & D' \end{tikzcd}$$

es decir, $TS \Longrightarrow Id_{\mathcal{D}}$.

Observación. *Para cada $\alpha : C \longrightarrow S(D)$, se satisface que*

$$\eta_{C,D}(\alpha) = \xi_D\circ T(\alpha).$$

En efecto, del diagrama conmutativo, dado por la naturalidad de η en C, se obtiene

$$\begin{tikzcd} Hom_{\mathcal{C}}(S(D),S(D)) \arrow[r, "\eta_{S(D),D}"] \arrow[d, "()\circ\alpha"'] & Hom_{\mathcal{D}}(TS(D),D) \arrow[d, "()\circ T(\alpha)"] \\ Hom_{\mathcal{C}}(C,S(D)) \arrow[r, "\eta_{C,D}"] & Hom_{\mathcal{D}}(T(C),D) \end{tikzcd}$$

de donde se sigue que

$$\eta_{C,D}(\alpha) = \eta_{C,D}(Id_{S(D)} \circ \alpha) = \eta_{S(D),D}(Id_{S(D)}) \circ T(\alpha) = \xi_D \circ T(\alpha).$$

Observación. *Análogamente, al definir*

$$\zeta_C = \eta^{-1}_{C,T(C)}(Id_{T(C)}) : C \longrightarrow ST(C),$$

se tiene que $\zeta : Id_{\mathcal{C}} \Longrightarrow ST$. *En efecto, como para cada* $C \in \mathcal{C}$ *y* $D \in \mathcal{D}$, *se tiene el isomorfismo*

$$\eta_{C,D} : Hom_{\mathcal{C}}(C, S(D)) \longrightarrow Hom_{\mathcal{D}}(T(C), D),$$

entonces

$$(\eta_{C,D})^{-1} : Hom_{\mathcal{D}}(T(C), D) \longrightarrow Hom_{\mathcal{C}}(C, S(D))$$

es un isomorfismo. En particular, al fijar $C \in \mathcal{C}$, *como* $T(C) \in \mathcal{D}$, *se tiene el isomorfismo*

$$(\eta_{C,T(C)})^{-1} : Hom_{\mathcal{D}}(T(C), T(C)) \longrightarrow Hom_{\mathcal{C}}(C, ST(C)).$$

Con esto en cuenta,

$$\zeta_C := (\eta_{C,T(C)})^{-1}(Id_{T(C)}) : C \longrightarrow ST(C).$$

Ahora, si $C' \xrightarrow{f} C$, *la naturalidad en* C *y en* D, *hacen conmutativo al diagrama*

$$\begin{tikzcd}
Hom_{\mathcal{D}}(T(C),T(C)) \arrow[r, "(\eta_{C,T(C)})^{-1}"] \arrow[d, "()\circ T(f)"'] & Hom_{\mathcal{C}}(C,ST(C)) \arrow[d, "()\circ f"] \\
Hom_{\mathcal{D}}(T(C'),T(C)) \arrow[r, "(\eta_{C',T(C)})^{-1}"] & Hom_{\mathcal{C}}(C',ST(C)) \\
Hom_{\mathcal{D}}(T(C'),T(C')) \arrow[r, "(\eta_{C',T(C')})^{-1}"] \arrow[u, "T(f)\circ()"] & Hom_{\mathcal{C}}(C',ST(C')) \arrow[u, "ST(f)\circ()"']
\end{tikzcd}.$$

Por lo tanto, tenemos que

$$\begin{gathered}
\zeta_C \circ f = (\eta_{C,T(C)})^{-1}(Id_{T(C)}) \circ f \\
= (\eta_{C',T(C)})^{-1} \circ (Id_{T(C)} \circ T(f)) = (\eta_{C',T(C)})^{-1}(T(f)) \\
= (\eta_{C',T(C)})^{-1}(T(f) \circ Id_{T(C')}) \\
= ST(f) \circ (\eta_{C',T(C')})^{-1}(Id_{T(C')}) \\
= ST(f) \circ \zeta_{C'}.
\end{gathered}$$

Así, para cada $C' \xrightarrow{f} C$*, los diagramas*

$$\begin{tikzcd} C' \arrow[r, "\zeta_{C'}"] \arrow[d, "f"'] & ST(C') \arrow[d, "ST(f)"] \\ C \arrow[r, "\zeta_C"] & ST(C) \end{tikzcd}$$

conmutan, mostrando que $\zeta : Id_{\mathcal{C}} \Longrightarrow ST$.

Observación. *Si* $\beta : T(C) \longrightarrow D$*, entonces* $(\eta_{C,D})^{-1}(\beta) = S(\beta) \circ \zeta_C$*. En efecto, por la naturalidad de* η *en* D*, se obtiene el diagrama conmutativo*

$$\begin{tikzcd} Hom_{\mathcal{D}}(T(C), T(C)) \arrow[r, "(\eta_{C,T(C)})^{-1}"] \arrow[d, "\beta\circ()"'] & Hom_{\mathcal{C}}(C, ST(C)) \arrow[d, "S(\beta)\circ()"] \\ Hom_{\mathcal{D}}(T(C), D) \arrow[r, "(\eta_{C,D})^{-1}"] & Hom_{\mathcal{C}}(C, S(D)) \end{tikzcd},$$

con lo cual

$$\begin{gathered} (\eta_{C,D})^{-1}(\beta) = (\eta_{C,D})^{-1}(\beta \circ Id_{T(C)}) \\ = S(\beta) \circ (\eta_{C,T(C)})^{-1}(Id_{T(C)}) = S(\beta) \circ \zeta_C. \end{gathered}$$

El siguiente resultado muestra que los funtores adjuntos derechos, como izquierdos, no son únicos pero sí equivalentes en el siguiente sentido:

Proposición 9.4.1. *Si* $S, S' : \mathcal{D} \longrightarrow \mathcal{C}$ *son ambos funtores adjuntos derechos de* $T : \mathcal{C} \longrightarrow \mathcal{D}$*, entonces* S *y* S' *son naturalmente equivalentes.*

Demostración. Sean $T : \mathcal{C} \longrightarrow \mathcal{D}$, $S' : \mathcal{D} \longrightarrow \mathcal{C}$ y $S : \mathcal{D} \longrightarrow \mathcal{C}$ funtores tales que S y S' son adjuntos derechos de T. Por la definición de ser adjunto derecho, para cada $C \in \mathcal{C}$ y $D \in \mathcal{D}$, se tienen los isomorfismos

$$\begin{gathered} \eta_{C,D} : Hom_{\mathcal{C}}(C, S(D)) \longrightarrow Hom_{\mathcal{D}}(T(C), D) \text{ y} \\ \eta'_{C,D} : Hom_{\mathcal{C}}(C, S'(D)) \longrightarrow Hom_{\mathcal{D}}(T(C), D). \end{gathered}$$

Así, para cada $C \in \mathcal{C}$ y $D \in \mathcal{D}$, la función

$$\lambda_{C,D} := (\eta'_{C,D})^{-1} \circ \eta_{C,D}$$

es un isomorfismo de

$$Hom_{\mathcal{C}}(C, S(D)) \longrightarrow Hom_{\mathcal{C}}(C, S'(D)),$$

con lo cual, se sigue que $\lambda = \{\lambda_{C,D}\}_{C,D \in \mathcal{C}^{op} \times \mathcal{D}}$ es una equivalencia natural entre los funtores $F : \mathcal{C}^{op} \times \mathcal{D} \longrightarrow Sets$, definido por

$$(C, D) \longrightarrow Hom_{\mathcal{C}}(C, S(D)),$$

y $F' : F : \mathcal{C}^{op} \times \mathcal{D} \longrightarrow Sets$, con regla de correspondencia

$$(C, D) \longrightarrow Hom_{\mathcal{C}}(C, S'(D)).$$

Además, si $C' \xrightarrow{f} C$, entonces el diagrama

$$\begin{tikzcd}
Hom_{\mathcal{C}}(C, S(D)) \arrow[r, "\eta_{C,D}"] \arrow[d, "()\circ f"'] & Hom_{\mathcal{D}}(T(C), D) \arrow[r, "(\eta'_{C,D})^{-1}"] \arrow[d, "()\circ T(f)"] & Hom_{\mathcal{C}}(C, S'(D)) \arrow[d, "()\circ f"] \\
Hom_{\mathcal{C}}(C', S(D)) \arrow[r, "\eta_{C',D}"] & Hom_{\mathcal{D}}(T(C'), D) \arrow[r, "(\eta'_{C',D})^{-1}"] & Hom_{\mathcal{C}}(C', S'(D))
\end{tikzcd},$$

conmuta debido a la conmutatividad de los dos diagramas pequeños. Esto muestra que λ es natural en C.

Análogamente, si $D \xrightarrow{g} D'$, la naturalidad en D se sigue del diagrama

$$\begin{tikzcd}
Hom_{\mathcal{C}}(C, S(D)) \arrow[r, "\eta_{C,D}"] \arrow[d, "S(g)\circ()"'] & Hom_{\mathcal{D}}(T(C), D) \arrow[r, "(\eta'_{C,D})^{-1}"] \arrow[d, "g\circ()"] & Hom_{\mathcal{C}}(C, S'(D)) \arrow[d, "S'(g)\circ()"] \\
Hom_{\mathcal{C}}(C, S(D')) \arrow[r, "\eta_{C,D'}"] & Hom_{\mathcal{D}}(T(C), D') \arrow[r, "(\eta'_{C,D'})^{-1}"] & Hom_{\mathcal{C}}(C, S'(D'))
\end{tikzcd},$$

que resulta ser conmutativo por la conmutatividad de los diagramas pequeños.

En particular, si $D \xrightarrow{g} D'$ es un morfismo en $\mathcal{D}$, se tienen los elementos

$$S(D), S(D'), S'(D), S'(D') \in \mathcal{C},$$

con los cuales, se obtienen los diagramas conmutativos

$$\begin{tikzcd}
Hom_{\mathcal{C}}(S(D), S(D)) \arrow[r, "\lambda_{S(D),D}"] \arrow[d, "S(g)\circ()"'] & Hom_{\mathcal{C}}(S(D), S'(D)) \arrow[d, "S'(g)\circ()"] \\
Hom_{\mathcal{C}}(S(D), S(D')) \arrow[r, "\lambda_{S(D),D'}"] & Hom_{\mathcal{C}}(S(D), S'(D')) \\
Hom_{\mathcal{C}}(S(D'), S(D')) \arrow[r, "\lambda_{S(D'),D'}"] \arrow[u, "()\circ S(g)"] & Hom_{\mathcal{C}}(S(D'), S'(D')) \arrow[u, "()\circ S(g)"']
\end{tikzcd}.$$

Si ahora definimos a $\varphi_D := \lambda_{S(D),D}(Id_{S(D)})$, entonces

$$\begin{aligned} S'(g)\circ\varphi_D = S'(g)\circ\lambda_{S(D),D}(Id_{S(D)}) &= \lambda_{S(D),D'}(S(g)\circ Id_{S(D)}) \\ = \lambda_{S(D),D'}(S(g)) &= \lambda_{S(D),D'}(Id_{S(D')}\circ S(g)) \\ = \lambda_{S(D'),D'}(Id_{S(D')})\circ S(g) &= \varphi_{D'}\circ S(g). \end{aligned}$$

Esto último quiere decir que los diagramas

$$\begin{tikzcd} S(D) \arrow[r, "\varphi_D"] \arrow[d, "S(g)"'] & S'(D) \arrow[d, "S'(g)"] \\ S(D') \arrow[r, "\varphi_{D'}"] & S'(D') \end{tikzcd} \quad ,$$

conmutan para cualquier $D \in \mathcal{D}$ y $D \xrightarrow{g} D'$. Por lo tanto, S y S' son naturalmente equivalentes. □

Como se vio anteriormente, $\eta_{C,D}$ queda expresada en términos de las funciones ξ y ζ antes mencionadas. El siguiente resultado da una condición para la naturalidad de η, en términos de una transformación natural ξ:

Proposición 9.4.2. *Sea $T : \mathcal{C} \longrightarrow \mathcal{D}$ y $S : \mathcal{D} \longrightarrow \mathcal{C}$ dos funtores para los cuales se tiene la transformación natural $\xi : TS \Longrightarrow Id_{\mathcal{D}}$. Para cada $C \in \mathcal{C}$ y $D \in \mathcal{D}$, definimos*

$$\eta_{C,D} : Hom_{\mathcal{C}}(C, S(D)) \longrightarrow Hom_{\mathcal{D}}(T(C), D)$$

por $\eta_{C,D}(\alpha) = \xi_D \circ T(\alpha)$. Si para cualquier $C \in \mathcal{C}$ y cada $D \in \mathcal{D}$, $\eta_{C,D}$ es un isomorfismo, entonces $\eta = \{\eta_{C,D}\}$ hace de S un adjunto derecho de T.

Demostración. Como $\xi : TS \Longrightarrow Id_{\mathcal{D}}$, si $D \xrightarrow{g} D'$ es un morfismo en $\mathcal{D}$, entonces

$$\begin{tikzcd} TS(D) \arrow[r, "\xi_D"] \arrow[d, "TS(g)"'] & D \arrow[d, "g"] \\ TS(D') \arrow[r, "\xi_{D'}"] & D' \end{tikzcd} \quad .$$

Así, si $C \xrightarrow{\alpha} S(D)$ es un morfismo en $\mathcal{C}$, se sigue que

$$\xi_D \circ T(\alpha) : T(C) \longrightarrow D.$$

Basta demostrar que η es natural en C y en D. Sea $D \in \mathcal{D}$ un elemento fijo y $C' \xrightarrow{\gamma} C$. El diagrama

$$\begin{tikzcd} Hom_{\mathcal{C}}(C, S(D)) \arrow[r, "\eta_{C,D}"] \arrow[d, "()\circ\gamma"'] & Hom_{\mathcal{D}}(T(C), D) \arrow[d, "()\circ T(\gamma)"] \\ Hom_{\mathcal{C}}(C', S(D)) \arrow[r, "\eta_{C',D}"] & Hom_{\mathcal{D}}(T(C'), D) \end{tikzcd},$$

conmuta ya que, por una parte, si $\alpha \in Hom_{\mathcal{C}}(C, S(D))$, entonces

$\eta_{C,D}(\alpha) \circ T(\gamma) = (\xi_D \circ T(\alpha)) \circ T(\gamma) = \xi_D \circ (T(\alpha) \circ T(\gamma)) = \xi_D \circ (T(\alpha \circ \gamma))$;

por otra parte se tiene que $\eta_{C',D}(\alpha \circ \gamma) = \xi_D \circ T(\alpha \circ \gamma)$.

Sea ahora $D \xrightarrow{\gamma} D'$ un morfismo en $\mathcal{D}$ y $C \in \mathcal{C}$ un objeto fijo. Por hipótesis, para $D \xrightarrow{\gamma} D'$, se tiene el diagrama conmutativo

$$\begin{tikzcd} TS(D) \arrow[r, "\xi_D"] \arrow[d, "TS(\gamma)"'] & D \arrow[d, "\gamma"] \\ TS(D') \arrow[r, "\xi_{D'}"] & D' \end{tikzcd},$$

el cual garantiza la conmutatividad del diagrama

$$\begin{tikzcd} Hom_{\mathcal{D}}(T(C), TS(D)) \arrow[r, "\xi_D"] \arrow[d, "TS(\gamma)\circ()"'] & Hom_{\mathcal{D}}(T(C), D) \arrow[d, "\gamma\circ()"] \\ Hom_{\mathcal{D}}(T(C), TS(D')) \arrow[r, "\xi_{D'}"] & Hom_{\mathcal{D}}(T(C), D') \end{tikzcd}.$$

Además, el funtor T nos asegura que el siguiente diagrama sea conmutativo

$$\begin{tikzcd} Hom_{\mathcal{C}}(C, S(D)) \arrow[r, "T(-)"] \arrow[d, "S(\gamma)\circ()"'] & Hom_{\mathcal{D}}(T(C), TS(D)) \arrow[d, "TS(\gamma)\circ()"] \\ Hom_{\mathcal{C}}(C, S(D')) \arrow[r, "T(-)"] & Hom_{\mathcal{D}}(T(C), TS(D')) \end{tikzcd}.$$

Este último diagrama implica la conmutatividad del diagrama

$$\begin{tikzcd} Hom_{\mathcal{C}}(C, S(D)) \arrow[r, "T(-)"] \arrow[d, "S(\gamma)\circ()"'] & Hom_{\mathcal{D}}(T(C), TS(D)) \arrow[r, "\xi_D"] \arrow[d, "TS(\gamma)\circ()"] & Hom_{\mathcal{D}}(T(C), D) \arrow[d, "\gamma\circ()"] \\ Hom_{\mathcal{C}}(C, S(D')) \arrow[r, "T(-)"] & Hom_{\mathcal{D}}(T(C), TS(D')) \arrow[r, "\xi_{D'}"] & Hom_{\mathcal{D}}(T(C), D') \end{tikzcd}.$$

de donde se sigue la naturalidad en D.

9.5. Ejemplos de funtores adjuntos

Ejemplo. *Los funtores $V : Sets \longrightarrow Vct_K$, que a cada conjunto X le asocia el espacio vectorial $V(X)_K$, y $U : Vct_K \longrightarrow Sets$, donde a cada espacio vectorial W le asocia el conjunto $U(W)$ formado por todos los vectores de W, son adjuntos izquierdo y derechos, respectivamente.*

Ejemplo. *El funtor abelianización $r : Grp \longrightarrow Ab$ es adjunto izquierdo del funtor inclusión $\iota : Ab \longrightarrow Grp$. Así mismo, el funtor inclusión es adjunto derecho del funtor abelianización.*

Cualquier morfismo de grupos $\varphi : G \longrightarrow H$ induce un único morfismo $\widetilde{\varphi} : G/G' \longrightarrow H/H'$. Cuando además suponemos que el grupo H es abeliano, esto nos define un morfismo de grupos $\widetilde{\varphi}$ de tal manera que el diagrama siguiente conmuta:

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\rho"'] & H , \\ G/G' \arrow[ur, "\widetilde{\varphi}"] & \end{tikzcd}$$

Así, se tiene una biyección

$$\eta_{G,H} : Hom_{Grp}(G, \iota(H)) \longrightarrow Hom_{Ab}(G/G', H),$$

definida por

$$\varphi \longmapsto \widetilde{\varphi}.$$

Más aún, esta última correspondencia nos garantiza la noción de naturalidad en G. En efecto, si $G_2 \xrightarrow{f} G_1$ es un morfismo de grupos, el diagrama

$$\begin{tikzcd} Hom_{Grp}(G_1, \iota(H)) \arrow[r, "\eta_{G_1,H}"] \arrow[d, "()\circ f"'] & Hom_{Ab}(G_1/(G_1)', H) . \arrow[d, "()\circ\widetilde{f}"] \\ Hom_{Grp}(G_2, \iota(H)) \arrow[r, "\eta_{G_2,H}"] & Hom_{Ab}(G_2/(G_2)', H) \end{tikzcd}$$

es conmutativo: si $\alpha : G_1 \longrightarrow H$, se tiene la función $\alpha \circ f : G_2 \longrightarrow H$, con la cual $\eta_{G_2,H}(\alpha \circ f) = \widetilde{\alpha \circ f}$ es la única función que hace conmutativo al diagrama

$$\begin{tikzcd} G_2 \arrow[r, "\alpha\circ f"] \arrow[d, "\rho"'] & H . \\ G_2/(G_2)' \arrow[ur, "\widetilde{\alpha\circ f}"'] & \end{tikzcd}$$

Por otra parte, por la definición de $\widetilde{f}$ *y de* $\widetilde{\alpha}$*, la función*

$$\eta_{G_1,H}(\alpha) \circ \widetilde{f} = \widetilde{\alpha} \circ \widetilde{f} : G_2/(G_2)' \longrightarrow H$$

es tal que, para cualquier $g \in G_2$*, se cumple que*

$$[\widetilde{\alpha} \circ \widetilde{f}](g + (G_2)') = \widetilde{\alpha}(f(g) + (G_1)') = \alpha(f(g)) = \alpha \circ f(g).$$

Esto implica que el diagrama

$$\begin{tikzcd} G_2 \arrow[r, "\alpha\circ f"] \arrow[d, "\rho"'] & H \\ G_2/(G_2)' \arrow[ur, "\widetilde{\alpha}\circ\widetilde{f}"'] & \end{tikzcd} ,$$

conmuta. Por la unicidad de la función que hace conmutativo al diagrama anterior, se sigue que

$$\widetilde{\alpha} \circ \widetilde{f} = \widetilde{\alpha \circ f}.$$

Análogamente, sean G *un grupo arbitrario,* H_1 *un grupo abeliano y* $\varphi : G \longrightarrow H_1$ *un morfismo de grupos. Por lo notado anteriormente, existe un único morfismo* $\widetilde{\varphi}$ *tal que*

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\rho"'] & H_1 \\ G/G' \arrow[ur, "\widetilde{\varphi}"'] & \end{tikzcd}$$

es un diagrama conmutativo. Ahora, si $H_1 \xrightarrow{f} H_2$ *es un morfismo entre grupos abelianos, entonces la función* $f \circ \widetilde{\varphi} : G/G' \longrightarrow H_2$ *satisface que, para cualquier* $g \in G$*,*

$$f \circ \widetilde{\varphi}(g + G') = f(\widetilde{\varphi}(g + G')) = f(\varphi(g)) = (f \circ \varphi)(g),$$

es decir, el diagrama

$$\begin{tikzcd} G \arrow[r, "f\circ\varphi"] \arrow[d, "\rho"'] & H_2 \\ G/G' \arrow[ur, "f\circ\widetilde{\varphi}"'] & \end{tikzcd} ,$$

conmuta. De nuevo, la unicidad de la función que hace conmutativo al diagrama anterior, implica que

$$f \circ \widetilde{\varphi} = \widetilde{f \circ \varphi},$$

con lo cual, se tiene que el siguiente diagrama es conmutativo:

$$\begin{tikzcd}
Hom_{Grp}(G, \iota(H_1)) \arrow[r, "\eta_{G,H_1}"] \arrow[d, "f\circ()"'] & Hom_{Ab}(G/G', H_1) \arrow[d, "f\circ()"] \\
Hom_{Grp}(G, \iota(H_2)) \arrow[r, "\eta_{G,H_2}"] & Hom_{Ab}(G/G', H_2)
\end{tikzcd}.$$

Capítulo 10

Grupos Divisibles

10.1. Grupos divisibles

Como en cualquier grupo abeliano hay una acción de los enteros en el grupo, surge de manera natural la noción de divisibilidad en un grupo.

Definición 10.1.1. *Decimos que un elemento a de un grupo A es divisible por el entero positivo n, si la ecuación $nx = a$ tiene solución en A, es decir, si existe $b \in A$ tal que $nb = a$. En este caso, lo denotamos por $n \mid a$.*

Observación. *Notemos que la existencia de la solución $nx = a$ es equivalente a decir que $a \in nA$. Más aún, si $x = b$ es una solución de $nx = a$, entonces la clase $b + A[n]$ es el conjunto de todas las soluciones de dicha ecuación. En efecto, recordemos que $A[n] = \{a \in A \mid na = 0\}$ es un subgrupo de A, por lo que $A/A[n]$ es un grupo donde el neutro aditivo es la clase del $0 + A[n] = A[n]$. De esta manera, $y - b \in A[n]$ si y sólo si $y = b + A[n]$. Con esto en cuenta, si $c \neq b$ es otra solución de la ecuación $nx = a$, entonces $n(c-b) = nc - nb = a - a = 0$, por lo que $c - b \in A[n]$, es decir, $c = b + A[n]$.*

Por otra parte, de la definición de divisibilidad, se sigue que si $n \mid a$ y $n \mid b$, entonces $n \mid a \pm b$. Esta idea se extiende para el caso cuando el grupo A es una suma directa:

Proposición 10.1.2. *Sea $A = B \oplus C$. Si $a = b + c$, con $b \in B$ y $c \in C$, entonces $n \mid a = b + c$ si y solo si $n \mid b$ y $n \mid c$.*

Demostración. Si $n \mid b$ y $n \mid c$, existen $b_0, c_0 \in A$ tales que $nb_0 = b$ y $nc_0 = c$. De esta manera,

$$n(b_0 + c_0) = nb_0 + nc_0 = b + c = a,$$

es decir, $n \mid a$.

Supongamos ahora que $n \mid a$. Así, existe $a_0 \in A$ tal que $na_0 = a = b + c$. Como $A = B \oplus C$, existen únicos $b_0 \in B$ y $c_0 \in C$ tales que $a_0 = b_0 + c_0$. Por lo tanto, se tiene que

$$b + c = a = na_0 = n(b_0 + c_0) = nb_0 + nc_0.$$

Como la expresión de cada elemento $a \in A$, en términos de B y C es única, se sigue que $nb_0 = b$ y $nc_0 = c$, por lo que $n \mid b$ y $n \mid c$. □

Observación. *Si $(n, ord(a)) = 1$, entonces la ecuación $nx = a$ siempre tiene solución. En efecto, si r y s son enteros tales que $nr + o(a)s = 1$, entonces $x = ra$ satisface que*

$$nx = nra = nra + so(a)a = (nr + so(a))a = 1a = a.$$

Definición 10.1.3. *Un grupo D es divisible si $n \mid a$ para toda $a \in A$ y $\forall n \in \mathbb{N}$.*

Observación. *Un grupo D es divisible si y sólo si $D = nD$ para todo entero positivo n.*

Observación. *De la Proposición 10.1.2, se sigue que subgrupos de un grupo divisible que son sumandos directos de éste, son también divisibles.*

Ejemplo. *(a) El grupo $\mathbb{Z}(p^\infty)$ es divisible. Sea $a \in \mathbb{Z}(p^\infty)$ con $a \neq 0$. Denotemos a los generadores de $\mathbb{Z}(p^\infty)$ por $c_1, c_2, \ldots, c_n, \ldots$, donde $pc_1 = 0$, $pc_2 = p_1, \cdots, pc_{n+1} = c_n$ y para cada $l \in \mathbb{N}$, $ord(c_l) = p^l$. Nótese que cada $< c_l >$ es un grupo cíclico de orden p^l y que*

$$\mathbb{Z}(p^\infty) = \cup_{n\in\mathbb{N}} < c_n >.$$

Ahora, como $a \in \mathbb{Z}(p^\infty)$, entonces existe un menor $l \in \mathbb{N}$ para el cual $a = kc_l$, con $1 \leq k < p^l$. Más aún, podemos suponer que $(k, p) = 1$. En efecto, si $s \geq 1$ es la mayor potencia de p que divide a k, es decir, $k = p^s m$ con $(m, p) = 1$, entonces

$$a = kc_l = m(p^s c_l) = mc_{l-s},$$

con $(m,p) = 1$. Esto contradice la elección de l. Por lo tanto, todo elemento $a \in \mathbb{Z}(p^\infty)$ se puede escribir de la forma $a = kc_l$, donde $(k,p) = 1$ y l es el menor natural para el cual $a \in < c_l >$. Esto implica que $ord(a) = p^l$. Así, por lo observado anteriormente, basta demostrar que $n \mid a$ para aquellas $n \in \mathbb{N}$ tales que $(n, ord(a)) \neq 1$.

Supongamos que $n = p^r m$, con $(m,p) = 1$. Como m y k son ambos primos relativos con p, entonces $(mk,p) = 1$, por lo que también $(mk, p^{l+r}) = 1$. Con esto en cuenta, existen enteros α y β tales que $1 = km\alpha + p^{l+r}\beta$, de donde se sigue que

$$c_{r+l} = mk\alpha c_{r+l} + \beta p^{r+l} c_{r+l} = mk\alpha c_{r+l}.$$

Como $p^r c_{r+l} = c_l$, al multiplicar por p^r esta última igualdad, se obtiene

$$c_l = p^r c_{r+l} = p^r mk\alpha c_{r+l} = nk\alpha c_{r+l},$$

con lo cual, se sigue que

$$a = kc_l = nk^2\alpha c_{r+l},$$

es decir, $x = (k^2\alpha)c_{r+l}$ es solución de $a = nx$.

(b) El grupo $\mathbb{Q}$ es claramente divisible.

(c) Una suma directa (producto directo) de grupos es divisible si y sólo si cada sumando directo (cada factor del producto directo) es un grupo divisible.

(d) $\mathbb{Q}/\mathbb{Q}_p \cong \mathbb{Z}(p^\infty)$.

Definición 10.1.4. *Decimos que un grupo D es p-divisible si $p^k D = D$ para todo entero positivo k.*

Notemos que $pD = D$ implica que

$$p^k D = p \cdot p \cdot \dots \cdot pD = D,$$

por lo que ser p-divisible es equivalente a que $pD = D$.

Proposición 10.1.5. *Un grupo D es divisible si y sólo si es p-divisible para todo primo p, es decir, $pD = D$ para cualquier primo p.*

Demostración. Sea D un grupo p-divisible, para cualquier primo p. Si $n = p_1^{\alpha_1} \cdot \dots \cdot p_s^{\alpha_s}$ es la factorización en primos, sigue que

$$\begin{aligned} nD &= (p_1^{\alpha_1} \cdot \dots \cdot p_s^{\alpha_s})D = (p_1^{\alpha_1} \cdot \dots \cdot p_{s-1}^{\alpha_{s-1}})p_s^{\alpha_s} D \\ &= (p_1^{\alpha_1} \cdot \dots \cdot p_{s-1}^{\alpha_{s-1}})D = \cdots = p_1^{\alpha_1} D = D. \end{aligned}$$

Por otra parte, si D es divisible, entonces en particular para cualquier primo p, se cumple que $pD = D$, por lo que D es p-divisible para cualquier primo p. □

Notación. Cuando D es un grupo p-divisible, lo denotaremos por $p \mid D$.

Observación. *Un p-grupo D es divisible si y sólo si D es p-divisible.*

Ejemplo. *Veamos ahora que el grupo $J_p/\mathbb{Z}$ es divisible. Notemos primero que, como J_p es la completación topológica de $\mathbb{Q}_p$, todo elemento x en J_p lo podemos escribir como la suma formal $x = s_0 + s_1 p + \cdots + s_n p^n + \cdots$, donde $s_m \in \{1, \dots, p-1\}$, para toda $m \in \mathbb{N}$. De esta manera, al elemento x lo podemos escribir como*

$$x = s_0 + p(s_1 + s_2 p + \cdots + s_n p^{n-1} + \cdots),$$

el cual es claramente un elemento en $\mathbb{Z} + pJ_p$. Esto quiere decir que $J_p = \mathbb{Z} + pJ_p$, y por lo tanto

$$J_p/\mathbb{Z} = (\mathbb{Z} + pJ_p)/\mathbb{Z} = pJ_p/\mathbb{Z} = p(J_p/\mathbb{Z}).$$

Esto muestra que $J_p/\mathbb{Z}$ es p-divisible. Ahora, como $\mathbb{Z}(p)$ es un p-grupo, entonces es q-divisible, por lo que cualquier $s_i \in \mathbb{Z}(p)$ cumple que $s_i = qs_i'$, para algún $s_i' \in \mathbb{Z}(p)$. Con esto en cuenta, dado cualquier elemento

$$x = s_0 + s_1 p + \cdots + s_n p^n + \cdots$$

en J_p, se tiene que $x = q(s_0' + s_1' p + \cdots + s_n' p^n + \cdots)$, es decir, J_p es q-divisible. Así, como $qJ_p = J_p$, entonces

$$q(J_p/\mathbb{Z}) = (\mathbb{Z} + qJ_p)/\mathbb{Z} = (\mathbb{Z} + J_p)/\mathbb{Z} = J_p/\mathbb{Z},$$

por lo que $J_p/\mathbb{Z}$ es q-divisible. Esto demuestra que $J_p/\mathbb{Z}$ es un grupo divisible.

Proposición 10.1.6. *Si en un p-grupo D todo elemento de orden p es de p-altura infinita, entonces D es divisible.*

Demostración. Notemos primero que, para cualquier primo $q \neq p$, como $(p,q) = 1$, la ecuación $qx = a$ tiene solución para cualquier $a \in D$, es decir, $q \mid D$. Veremos ahora que $p \mid D$.

Sea $a \in D$ con $o(a) = p^n$. Procederemos por inducción. Si $n = 1$, entonces a tiene orden p, por lo que $h_p(a) = \infty$, es decir, toda ecuación de la forma $p^k x = a$, con $k \in \mathbb{N}$, tiene solución en D. En particular, la ecuación $px = a$ tiene solución, por lo que $p \mid a$. Supongamos ahora que $n > 1$ y que el resultado es válido para todo elemento $b \in D$, con orden $m < n$. Como $o(a) = p^n$, entonces $o(p^{n-1}a) = p$, por lo que $p^{n-1}a$ tiene p-altura infinita. De esta manera, existe $b \in D$ que satisface la ecuación $p^n x = p^{n-1}a$, con lo cual, se sigue que $a - pb \in D$ es tal que

$$p^{n-1}(a - pb) = p^{n-1}a - p^n b = 0,$$

es decir, $o(a - pb) \leq n - 1$. Por hipótesis de inducción, se tiene que $p \mid a - pb$, lo cual implica que $p \mid a$. Por lo tanto D es p-divisible, y así D es un grupo divisible. $\square$

Observación. *Si $\varphi : A \longrightarrow B$ es un morfismo y $n \mid a$ en A, entonces $n \mid \varphi(a)$ en B. Esto implica que para cualquier epimorfismo $\varphi : A \longrightarrow B$, si A es divisible, entonces B también lo es. Con esto en cuenta, podemos concluir que $\mathbb{Z}$ no es isomorfo a $\mathbb{Q}$, pues $\mathbb{Q}$ es divisible y $\mathbb{Z}$ no lo es.*

Definición 10.1.7. *Decimos que un grupo D es inyectivo, si para cualquier sucesión exacta de la forma $0 \hookrightarrow A \xrightarrow{\alpha} B$ y cualquier morfismo $\xi : A \longrightarrow D$, existe un morfismo $\eta : B \longrightarrow D$ tal que el diagrama*

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "\alpha"] \arrow[d, "\xi"'] & B \arrow[dl, "\eta"] \\ & D & \end{tikzcd}$$

es conmutativo.

De la definición anterior, si identificamos a A con $\alpha(A)$ en B, la condición de ser inyectivo es equivalente a poder extender cualquier morfismo $\xi : A \longrightarrow D$, a un morfismo de cualquier grupo B, que contenga a A, al grupo D. Como veremos más adelante, esta condición caracteriza de manera única a los grupos divisibles.

Teorema 10.1.8. *Todo grupo divisible D es un grupo inyectivo.*

Demostración. Sea D un grupo divisible y $0 \hookrightarrow A \xrightarrow{\alpha} B$ una sucesión exacta. Por lo observado anteriormente, podemos suponer que $A \leq B$. Consideremos ahora a todos los grupos G entre A y B para los cuales cualquier morfismo $\xi : A \longrightarrow D$ tiene una extensión $\theta : G \longrightarrow D$, es decir, al conjunto

$$\mathcal{Z} = \{(G, \theta) \mid G \leq B \,\text{y}\, \theta : G \longrightarrow D \text{ es una extensión de } \xi : A \longrightarrow D\}.$$

Nótese que $\mathcal{Z}$ es no vació pues $(A, \xi) \in \mathcal{Z}$. A continuación, daremos un orden parcial en el conjunto $\mathcal{Z}$ para poder aplicar el lema de Zorn. Para esto, definamos la relación $(G, \theta) \leq (G', \theta')$ por $G \leq G'$ y $\theta = \theta' \mid_G$, que claramente es una relación de orden. Ahora, si $(G_i, \theta_i)_{i \in I}$ es una cadena en $\mathcal{Z}$, como cada par de parejas son comparables, de tal manera que uno de ellos está contenido en el otro, entonces podemos formar el grupo $G = \cup_{i \in I} G_i$ y la función $\theta : G \longrightarrow D$, donde a cada $x_i \in G_i \subset G$ le asigna el valor $\theta_i(x_i)$ en D. Notemos que esta función está bien definida, ya que para cualquier $x_i \in G_k \cap G_j$, se tiene que $k \leq j$ o $j \leq k$, por lo que $G_k \leq G_j$ ó $G_j \leq G_k$. Así, se cumple que $\theta(x_i) = \theta_i(x_i) = \theta_j(x_i)$ puesto que una de ellas extiende a la otra. Por lo tanto, (G, θ) es una cota para la cadena $(G_i, \theta_i)_{i \in I}$. Como $(G, \theta) \in \mathcal{Z}$, por el Lema de Zorn, $\mathcal{Z}$ tiene un elemento máximo (G_0, θ_0). Afirmamos que $G_0 = B$.

Supongamos que $G_0 \neq B$ y que $b \in B \setminus G_0$.

Caso (1) Si $< b > \cap G_0 = \{0\}$, entonces $< G_0, b >= G_0 \oplus < b >$. Como todo elemento en $< G_0, b >$ se escribe de manera única como $g + nb$, con $g \in G_0$ y $n \in \mathbb{N}$, podemos definir la función

$$\varphi :< G_0, b > \longrightarrow D,$$

dada por $g + nb \longmapsto \theta_0(g)$. Notemos que, como φ es un morfismo que extiende a θ_0, entonces extiende también a ξ. Esto implica que $(< G_0, b >, \varphi) \in \mathcal{Z}$, y además, es tal que $(G_0, \theta_0) \leq (< G_0, b >, \varphi)$, lo cual contradice la maximalidad de (G_0, θ_0).

Caso (2) Si $< b > \cap G_0 \neq \{0\}$, entonces el principio del buen Orden nos garantiza que, dentro del conjunto $\{nb \in G_0 \mid n \in \mathbb{N}^+\}$, existe un elemento menor. Más aún, si $k \in \mathbb{N}$ es tal elemento, el algoritmo de la división de Euclides nos caracteriza a todos los elementos en $< b > \cap G_0$, de donde se sigue que $< b > \cap G_0 = \{m(kb) \mid m \in \mathbb{N}^+\}$.

Supongamos que $k \in \mathbb{N}^+$ es el menor natural positivo para el cual $kb \in G_0$. Si $g + sb \in < G_0, b >$, con $k \leq s$, por el algoritmo de la división de Euclides, $s = qk + r$, con $0 \leq r < k$. Así, se tiene que

$$g + sb = g + (qk + r)b = [g + q(kb)] + rb,$$

con $g + q(kb) \in G_0$ y $r < k$. Más aún, todo elemento de $< G_0, b >$ se puede escribir de manera única como $g + sb$, donde $1 \leq s < k$ y $g \in G_0$. En efecto, si $g_1 + n_1 b = g_2 + n_2 b$, con $n_1, n_2 < k$ y $g_1, g_2 \in G_0$, entonces $g_1 - g_2 = (n_2 - n_1)b$. Obsérvese que no puede suceder que $g_1 \neq g_2$, ya que en tal caso, se tendría que $r = n_2 - n_1 < k$ es tal que

$$rb = (n_2 - n_1)b = g_1 - g_2 \in G_0,$$

contradiciendo la minimalidad de k. Por lo tanto, $g_1 = g_2$, con lo cual se sigue que $(n_2 - n_1)b = 0 \in G_0$. Como $n_2 - n_1 < k$, la condición de minimalidad de k implica que $n_2 - n_1 = 0$, es decir, $n_1 = n_2$, lo cual muestra la unicidad de la expresión.

Por otra parte, como $kb \in G_0$, entonces $\theta_0(kb) \in D$. Por ser D un grupo divisible, existe $d \in D$ tal que $kd = \theta_0(kd)$. Esto nos permite definir la función $\mu :< G_0, b > \longrightarrow D$ con regla de correspondencia

$$g + sb \longmapsto \theta_0(g) + sd.$$

Notemos que μ es un morfismo: si $(g_1 + s_1 b)$ y $(g_2 + s_2 b)$ son dos elementos en $< G_0, b >$, con $s_1, s_2 < k$, entonces

$$\begin{gathered}\mu((g_1 + s_1 b) + (g_2 + s_2 b)) = \mu((g_1 + g_2) + (s_1 + s_2)b) \\ = \theta_0(g_1 + g_2) + (s_1 + s_2)d = \theta_0(g_1) + \theta_0(g_2) + s_1 d + s_2 d \\ = [\theta_0(g_1) + s_1 d] + [\theta_0(g_2) + s_2 d] = \mu(g_1 + s_1 b) + \mu(g_2 + s_2 b).\end{gathered}$$

Obsérvese también que μ está bien definida, ya que si $s_1 + s_2 \geq k$, por el algoritmo de la división, se tiene que

$$s_1 + s_2 = qk + r,$$

con $0 \leq r < k$. Por lo observado anteriormente,

$$(g_1 + s_1 b) + (g_2 + s_2 b) = (g_1 + g_2 + q(kb)) + rb,$$

teniendo así que

$$\begin{gathered}\mu((g_1 + s_1 b) + (g_2 + s_2 b)) = \mu((g_1 + g_2 + q(kb)) + rb) \\ = \theta_0(g_1 + g_2 + q(kb)) + rd = \theta_0(g_1 + g_2) + q\theta_0(kb) + rd \\ = \theta_0(g_1 + g_2) + qkd + rd = \theta_0(g_1) + \theta_0(g_2) + (qk + r)d \\ = \theta_0(g_1) + \theta_0(g_2) + (s_1 + s_2)d = [\theta_0(g_1) + s_1 d] + [\theta_0(g_2) + s_2 d] \\ = \mu(g_1 + s_1 b) + \mu(g_2 + s_2 b).\end{gathered}$$

Por lo tanto, $\mu :< G_0, b > \longrightarrow D$ es un morfismo que además extiende a θ_0, por lo que también extiende a ξ. Esto muestra que

$$(G_0, \theta_0) \leq (< G_0, b >, \mu),$$

lo cual contradice la maximalidad de (G_0, θ_0). De esta manera, llegamos a que $G_0 = B$, mostrando así que D es inyectivo.

□

De lo anterior, podemos ver que otra propiedad de los grupos divisibles es la de ser sumandos directos de cualquier grupo que lo contenga:

Teorema 10.1.9. *(Baer) Sea $D \leq A$, con D un grupo divisible. Entonces D es un sumando directo de A. Más aún, si $A = D \oplus C$ y B es cualquier otro subgrupo de A con $B \cap D = 0$, entonces podemos escoger $C \leq A$ de tal manera que $B \leq C$.*

Demostración. Por ser D un subgrupo de A, se tiene la sucesión exacta

$$0 \hookrightarrow D \xrightarrow{\iota} A \longrightarrow A/D \longrightarrow 0.$$

Como D es inyectivo, para la función identidad $id_D : D \longrightarrow D$, se tiene el diagrama conmutativo

$$\begin{tikzcd} D \arrow[r, "\iota"] \arrow[d, "id_D"'] & A \arrow[dl, "\xi"] \\ D & \end{tikzcd},$$

donde $\xi \mid_D = id_D$, es decir, $\xi : A \longrightarrow D$ es tal que $\xi \circ \iota = id_D$. Por la Proposición 4.2.3, se tiene que $A = \iota(D) \oplus Ker\xi$.

Para la segunda afirmación, si B es un subgrupo de A, tal que $B \cap D = \{0\}$, entonces $D + B = D \oplus B$. Si consideramos ahora la inclusión $\iota : D \oplus B \hookrightarrow A$ en el argumento anterior, tenemos que $\xi \circ \iota(D \oplus B) = D$, de donde se sigue que $\xi(D \oplus B) = D$, es decir, $B \leq Ker\xi$, con $A = D \oplus Ker\xi$. $\square$

Observación. *Si* $\{D_i\}_{i \in I}$ *es una familia de grupos divisibles de* A*, entonces la suma* $\Sigma_{i \in I} D_i$ *es un grupo divisible de* A*. En efecto, si* $d_1 + d_2 + \cdots + d_k$ *es un elemento en la suma, donde* $d_i \in D_i$*, entonces para cada* $d_i \in D_i$*, existe* $d_i' \in D_i$ *tal que* $nd_i' = d_i$*. Por lo tanto, se sigue que*

$$n(d_1' + d_2' + \cdots + d_k') = nd_1' + nd_2' + \cdots + nd_k' = d_1 + d_2 + \cdots + d_k,$$

lo cual muestra que $\Sigma_{i \in I} D_i$ *es divisible.*

Por la observación anterior, dado cualquier grupo A, podemos considerar el subgrupo D generado por todos los subgrupos divisibles de A. Más aún, D es el subgrupo máximo divisible de A. Además, el subgrupo máximo divisible D de A, es un subgrupo totalmente invariante de A: para cualquier endomorfismo $\eta : A \longrightarrow A$, $\eta(D) \subset D$ pues $\eta(D)$ es divisible. De esta manera, $A = D \oplus C$, donde C es *reducido*, en el sentido de que no tiene subgrupos divisibles no triviales.

Ejemplo. J_p *es un grupo reducido.*

Teorema 10.1.10. *Todo grupo* A *es la suma directa de un grupo divisible* D *y un grupo reducido* C*. Además, el grupo* D *está determinado por* A*, mientras que* C *es único salvo isomorfismos.*

Demostración. Por lo notado anteriormente, si D es el subgrupo máximo divisible de A, entonces $A = D \oplus C$, con C un grupo reducido. Ahora, si $A = D' \oplus C'$ con D' divisible y C' reducido, entonces por ser D un subgrupo totalmente invariante de A, se cumple que

$$D = (D \cap D') \oplus (D \cap C').$$

Como C' es reducido y D es divisible, $D \cap C'$ es un subgrupo divisible de C', por lo que $D \cap C' = \{0\}$. Esto implica que $D \cap D' = D$, con lo cual se tiene que $D \leq D'$. Como D es el subgrupo máximo divisible, se obtiene la contención $D' \leq D$, teniendo así que $D = D'$. $\square$

A continuación, determinaremos la estructura de los grupos divisibles. Notemos que si A es un grupo divisible y T su parte de torsión, entonces T es un subgrupo divisible. En efecto, si y es solución de $nx = t$, con $t \in T$, entonces $ny = t$. Como t tiene orden finito, entonces y también lo tiene. De esta manera, por ser T un subgrupo divisible, se tiene que T es un sumando directo de A, con lo cual $A = T \oplus E$, donde E es un subgrupo libre de torsión. Notemos también que, por un argumento análogo, E es un subgrupo divisible.

Recordemos que si b es solución de $nx = a$, entonces todas las soluciones de esta ecuación son de la forma $b + A[n]$, donde

$$A[n] = \{c \in A \mid nc = 0\}.$$

Así, si E es libre de torsión, afirmamos que las soluciones a las ecuaciones $nx = a$ son únicas. En efecto, si $b_1 \neq b_2 \in E$ son ambas soluciones de la ecuación $nx = a$, se tiene que $b_1 - b_2 \in A[n]$, con lo cuál se tendría que $n(b_1 - b_2) = 0$, es decir, llegamos a la contradicción de que $0 \neq b_1 - b_2 \in E$ es un elemento de orden finito. Con esto en cuenta, tenemos la siguiente

Proposición 10.1.11. *Si E es un grupo divisible y libre de torsión, entonces E es un espacio vectorial sobre $\mathbb{Q}$.*

Demostración. Sean $b \in E$ y $n > 0$. Por lo visto anteriormente, existe una única $y \in E$ tal que $ny = b$. De esta manera, podemos definir la función $\varphi : \mathbb{Q} \times E \longrightarrow E$, dada por $(\frac{m}{n}, b) \longmapsto my$. Veamos que esta función es una acción de $\mathbb{Q}$ en E, que hacen de E un espacio vectorial sobre $\mathbb{Q}$:

i) Para cualquier $v \in E$, se tiene que $(1, v) \longmapsto 1 \cdot v = v$, pues v es la única solución de $v = 1 \cdot x$.

ii) Sean $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$ y $v \in E$. Por una parte, tenemos que

$$(\tfrac{a}{b} \cdot \tfrac{c}{d}, v) = (\tfrac{ac}{bd}, v) \longmapsto acw,$$

donde w es la única solución de $v = (bd)x$. Ahora, si w_1 es solución de $v = dx$, entonces $(\frac{c}{d}, v) \longmapsto cw_1$, con lo cual se tiene que

$$(\tfrac{a}{b}, cw_1) \longmapsto aw_2,$$

donde w_2 es solución de $cw_1 = bx$. Como las soluciones de las ecuaciones en E, de la forma $a = nx$, son únicas, se sigue que los elementos bw y w_1 son iguales, ya que ambos satisfacen la ecuación $v = dx$. Así, de la igualdad $bw = w_1$, se tiene que $cw_1 = bcw$. Como w_2 es solución de la ecuación $cw_1 = bx$, se sigue también que $w_2 = cw$, con lo cual podemos concluir que $(\frac{a}{b}, (\frac{c}{d}, v)) \longmapsto aw_2 = acw$, es decir, $(\frac{a}{b} \cdot \frac{c}{d}, v) = (\frac{a}{b}, (\frac{c}{d}, v))$.

iii) Sean $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$ y $v \in E$. Por una parte, se tiene que

$$(\tfrac{a}{b} + \tfrac{c}{d}, v) = (\tfrac{ad+bc}{bd}, v) \longmapsto (ad + cb)w,$$

donde w es la solución de $v = (bd)x$. Por otra parte, $(\frac{a}{b}, v) \longmapsto aw_1$, donde w_1 es la solución de $v = bx$ y $(\frac{c}{d}, v) \longmapsto cw_2$, donde w_2 es la solución de $v = dx$. Notemos que como $v = b(dw)$ y $v = d(bw)$, por la unididad de las soluciones, se sigue que $dw = w_1$ así como $bw = w_2$. Con esto en cuenta, llegamos a que

$$(\tfrac{a}{b}, v) + (\tfrac{c}{d}, v) = aw_1 + cw_2 = a(dw) + c(bw) = (ad + cb)w,$$

es decir, $(\frac{a}{b}, v) + (\frac{c}{d}, v) = (\frac{a}{b} + \frac{c}{d}, v)$.

iv) Sean $\frac{a}{b} \in \mathbb{Q}$ y $v, w \in E$. Por definición, $(\frac{a}{b}, v + w) \longmapsto az$, donde z es la solución de la ecuación $(v + w) = bx$. Ahora, $(\frac{a}{b}, v) \longmapsto az_1$, con z_1 solución de $v = bx$ y $(\frac{a}{b}, w) \longmapsto az_2$, donde z_2 es solución de $w = bx$. Obsérvese que $z_1 + z_2$ es solución de $(v + w) = bx$, pues

$$b(z_1 + z_2) = bz_1 + bz_2 = v + w.$$

Como las soluciones de las ecuaciones en E son únicas, se tiene que $z_1 + z_2 = z$, con lo cual se llega a que

$$(\tfrac{a}{b}, v + w) = az = a(z_1 + z_2) = az_1 + az_2 = (\tfrac{a}{b}, v) + (\tfrac{a}{b}, w).$$

Por lo tanto, E es un espacio vectorial sobre $\mathbb{Q}$. $\square$

El siguiente resultado nos caracteriza al grupo aditivo de cualquier espacio vectorial V sobre un campo K:

Proposición 10.1.12. *Si V es un espacio vectorial sobre el campo K, entonces V, como grupo aditivo, es la suma directa de copias de K.*

Demostración. Sea X una base para el espacio vectorial V_K. Para cada $x \in X$, tenemos el subespacio de dimensión uno de la forma $Kx = \{kx \mid k \in K\}$, el cual es claramente isomorfo a K, bajo la correspondencia $kx \longmapsto k$. Como todo elemento en V_K es una combinación lineal de elementos de la base, se tiene que

$$V_K \cong \oplus_{x\in X} Kx = K^{(X)}.$$

$\square$

De lo anterior, si A es un grupo divisible tal que $A = T \oplus E$, donde T y E son de torsión y libre torsión, respectivamente, se sigue que $E = \oplus_{i=1}^{n}\mathbb{Q}_i$, donde n es la dimensión del espacio vectorial $E_{\mathbb{Q}}$. De esta manera, falta caracterizar a la parte de torsión del grupo divisible A. Como todo grupo de torsión es la suma directa de sus p-componentes, basta fijarnos en una p-componente para poder caracterizar a los grupos divisibles.

10.2. Cápsula inyectiva

Teorema 10.2.1. *Todo grupo abeliano G es isomorfo a un cociente de la forma L/N, con L un grupo libre.*

Demostración. Sean G un grupo, $I =\mid G \mid$ y $L = \oplus_{i\in I}\mathbb{Z}_i$. Como I etiqueta al grupo G, se tiene que $G = \{g_i \mid i \in I\}$. Así, si x_{g_i} denota al generador del término i-ésimo de la suma directa $L = \oplus_{i\in I}\mathbb{Z}_i$, (donde $g_i \in G$), entonces L es un grupo libre abeliano, cuyo conjunto generador es $X = \{x_{g_i} \mid g \in G\}$. Con esto en cuenta, definimos la función $\varphi : X \longrightarrow G$ por $x_{g_i} \longmapsto g_i$, la cual se puede extender de manera lineal a la función $\overline{\varphi} : L \longrightarrow G$. Más aún, $\overline{\varphi}$ es un morfismo de grupos suprayectivo, por lo que $L/Ker\varphi \cong G$. $\square$

Observación. *Como $\mathbb{Z} \hookrightarrow \mathbb{Q}$, entonces $\oplus_{i\in I}\mathbb{Z}_i \hookrightarrow \oplus_{i\in I}\mathbb{Q}_i$. Así, por ser $\oplus_{i\in I}\mathbb{Q}_i$ un grupo libre y divisible, puesto que es una suma directa de grupos divisibles, se tiene que*

$$G \cong \oplus_{i\in I}\mathbb{Z}_i/N \hookrightarrow \oplus_{i\in I}\mathbb{Q}_i/N.$$

Notemos también que $\oplus_{i\in I}\mathbb{Q}_i/N$ es divisible por ser la imagen del epimorfismo $\oplus_{i\in I}\mathbb{Q}_i \xrightarrow{\rho_N} \oplus_{i\in I}\mathbb{Q}_i/N$, lo cual muestra que todo grupo abeliano se puede sumergir en un grupo divisible.

De lo anterior, surge la pregunta natural: dado un grupo abeliano A, ¿existe un grupo divisible con la propiedad de ser el menor grupo divisible que contiene a A? Los siguientes lemas nos ayudarán a demostrar la existencia de dicho grupo divisible junto con algunas propiedades.

Lema 10.2.2. *Sea B un subgrupo de A. Entonces B es esencial en A si y sólo si para cualquier grupo G y morfismo $\alpha : A \longrightarrow G$, se cumple que α es inyectiva si $\alpha\mid_B: B \longrightarrow G$ es inyectiva.*

Demostración. $\Longrightarrow$) Supongamos que B es esencial en A y que $\alpha : A \longrightarrow G$ es un morfismo tal que $\alpha\mid_B: B \longrightarrow G$ es inyectivo. Claramente,

$$Ker(\alpha\mid_B) \subset Ker(\alpha).$$

Si $a \in Ker(\alpha) \setminus Ker(\alpha\mid_B)$, entonces a satisface que $\alpha(a) = 0$ y que $a \notin B$. Así, si consideramos al subgrupo generado por a, la esencialidad de B nos asegura que $< a > \cap B \neq \{0\}$.

Caso 1) Si $o(a) = n < \infty$. Como $< a > \cap B \neq \{0\}$, existe $la \in < a > \cap B$, con $l \in \{1, \ldots, n-1\}$. Ahora, como $la \in B$ y $\alpha(a) = 0$, se cumple que $\alpha(la) = l\alpha(a) = l \cdot 0 = 0$. Al ser $\alpha\mid_B$ inyectiva, se tiene que $la = 0$. Esto contradice la hipótesis del orden de a.

Caso 2) Sea $o(a) = \infty$. De manera análoga, la esencialidad de B en A nos asegura que $< a > \cap B \neq \{0\}$, con lo cual existe $la \in < a > \cap B$, para algún $l \in \mathbb{N}$. Por el argumento anterior, como $la \in B$ entonces $\alpha(la) = 0$, de donde se sigue que $la = 0$, es decir, a es de orden finito, contradiciendo la hipótesis.

Por lo tanto, ambas contradicciones surgen de suponer que en el conjunto $Ker(\alpha) \setminus Ker(\alpha\mid_B)$ hay elementos. De esta manera, $Ker(\alpha) \setminus Ker(\alpha\mid_B) = \varnothing$, con lo cual $Ker(\alpha) = Ker(\alpha\mid_B) = \{0\}$

$\Longleftarrow$) Si B no fuera un subgrupo esencial en A, existiría $0 \neq C \leq A$ tal que $C \cap B = \{0\}$. De esta manera, el morfismo canónico $\rho : A \longrightarrow A/C$ cumple que $\rho\mid_B$ es inyectivo. En efecto, si $b_1, b_2 \in B$ son dos elementos, entonces $b_1 + C = b_2 + C$ si y sólo sí $b_1 - b_2 \in C$. Así, si $\rho\mid_B (b_1) = \rho\mid_B (b_2)$, entonces $b_1 - b_2 = 0$, ya que $b_1 - b_2 \in B$ y $C \cap B = \{0\}$. Por lo tanto,

$$b_1 + C = b_2 + C \Longleftrightarrow b_1 = b_2,$$

es decir, si $b_1 \neq b_2$ entonces $b_1 + C \neq b_2 + C$. Notemos también que ρ no es inyectiva, pues claramente $Ker\rho = C$.

Por lo tanto, si para cualquier grupo G y morfismo $\alpha : A \longrightarrow G$, la inyectividad de la función $\alpha\mid_B : B \longrightarrow G$ implica que α sea también inyectiva, entonces B es un subgrupo esencial en A. $\square$

Definición 10.2.3. *Sea A un grupo. Llamamos a un grupo divisible E, que contiene a A, mínimo divisible si no contiene subgrupos propios divisibles que contengan a A.*

Lema 10.2.4. *Un grupo divisible E que contiene a A, es mínimo divisible exactamente cuando A es un subgrupo esencial en E.*

Demostración. $\Longleftarrow$) Si E no fuera un grupo mínimo divisible que contiene a A, entonces se tendría un subgrupo $D \subsetneq E$ divisible para el cual $A \subset D$. Por la divisibilidad de D, se sigue que $E = D \oplus C$, donde $C \neq \{0\}$, ya que $D \subsetneq E$. Así, como $A \subset D$ y $D \cap C = \{0\}$, entonces $A \cap C = \{0\}$, por lo que A no es un subgrupo esencial de E.

$\Longrightarrow$) Sea E un grupo divisible y supongamos que A no es esencial en E. Esto quiere decir que existe un subgrupo C de E tal que $A \cap C = \{0\}$. Sin pérdida de generalidad, podemos suponer que $C =< c >$, con lo cual se tienen los dos casos: *i)* $o(c) = \infty$ o *ii)* $o(c) = p$.

Caso i) Como $o(c) = \infty$, podemos sumergir a $< c >$ en $\mathbb{Q}$ mediante el morfismo $\alpha :< c >\longrightarrow \mathbb{Q}$, donde $\alpha(c) = 1$. Ahora, como E es un grupo divisible, entonces también es inyectivo, por lo que si $\iota :< c >\hookrightarrow E$ es la inclusión, existe $\beta : \mathbb{Q} \longrightarrow E$ tal que hace conmutativo el diagrama

$$\begin{tikzcd} < c > \arrow[r, "\alpha"] \arrow[d, "\iota"'] & \mathbb{Q} \arrow[dl, "\beta"] \\ E & \end{tikzcd}$$

Veamos ahora que β es inyectiva para poder concluir que E contiene un subgrupo isomorfo a $\mathbb{Q}$. Supongamos que $\beta(\frac{l}{m}) = 0$, con $m \neq 0$. Como $\beta(\frac{l}{m}) = 0$, entonces

$$0 = m\beta(\tfrac{l}{m}) = \beta(\tfrac{l}{m} \cdot m) = \beta(l).$$

Así,

$$lc = \iota(lc) = \beta \circ \alpha(lc) = \beta(l) = 0.$$

Como $o(c) = \infty$, se sigue que $l = 0$, por lo que $\frac{l}{m} = 0$, es decir, β es inyectiva.

Afirmamos ahora que $\beta(\mathbb{Q}) \cap A = \{0\}$. Si $a \in A \cap \beta(\mathbb{Q})$, entonces existe $\frac{l}{m} \in \mathbb{Q}$, con $m \neq 0$, tal que $\beta(\frac{l}{m}) = a$. De esta manera,

$$ma = m\beta(\frac{l}{m}) = \beta(\frac{l}{m} \cdot m) = \beta(l) = \beta \circ \alpha(lc) = \iota(lc) = lc.$$

Con esto en cuenta, se tiene que

$$lc \in A \cap < c >= \{0\},$$

con lo cual, $l = 0$. Esto implica que $a = \beta(\frac{0}{m}) = \beta(0) = 0$. Por lo tanto, $A \cap \beta(\mathbb{Q}) = \{0\}$.

De esta manera, como $\beta(\mathbb{Q})$ es divisible, ya que es isomorfo al grupo divisible $\mathbb{Q}$, entonces es un sumando directo de E, con lo cual $E = \beta(\mathbb{Q}) \oplus B$. Notemos que como B es un sumando directo del grupo divisible E, resulta ser también divisible. Por el teorema de Baer, podemos escoger al subgrupo divisible B de manera que $A \subset B$, mostrando así que E no es mínimo divisible sobre A.

Caso ii) Supongamos que $o(c) = p$. Por un razonamiento análogo al del caso anterior, para la función $\alpha :< c > \longrightarrow \mathbb{Z}(p^\infty)$, definida por $\alpha(c) = \frac{a_0}{p}$, con $a_0 \in \{0, \ldots, p-1\}$, existe $\beta : \mathbb{Z}(p^\infty) \longrightarrow E$ tal que el siguiente diagrama conmuta:

$$\begin{tikzcd} < c > \arrow[r, "\alpha"] \arrow[d, "\iota"'] & \mathbb{Z}(p^\infty) \arrow[dl, "\beta"] \\ E & \end{tikzcd} .$$

Notemos que como $< c >$ es un grupo cíclico de orden p, entonces cualquier elemento no nulo de $< c >$ es un generador. Así, si b_0 es el inverso multiplicativo de a_0 en $\mathbb{Z}(p)$, es decir, $a_0 b_0 \cong 1$, (mod$p$), se tiene que $\alpha(b_0 c) = \frac{a_0 b_0}{p} = \frac{1}{p}$. De esta manera, podemos suponer sin pérdida de generalidad que $\alpha(c) = \frac{1}{p}$.

Ahora veamos que β es inyectiva, lo cual mostraría que E tiene un subgrupo isomorfo a $\mathbb{Z}(p^\infty)$. Supongamos que $\beta(\frac{l}{p^k}) = 0$, donde $(l;p) =$

1 y $\frac{l}{p^k}$ es el representante de la clase $\overline{\frac{l}{p^k}}$. Con esto en cuenta, se tiene que

$$\begin{aligned} 0 = p^{k-1} \cdot \beta(\tfrac{l}{p^k}) = \beta(p^{k-1} \cdot \tfrac{l}{p^k}) = \beta(\tfrac{l}{p}) = \beta(l \cdot \tfrac{1}{p}) = \beta \circ \alpha(lc) \\ = \iota(lc) = lc. \end{aligned}$$

Como $o(c) = p$, esto último implica que $p \mid l$, contradiciendo el hecho de que $(l; p) = 1$. Por lo tanto, $l = 0$, y así β es un monomorfismo.

De nuevo, afirmamos que $\beta(\mathbb{Z}(p^\infty)) \cap A = \{0\}$. Si

$$0 \neq a \in \beta(\mathbb{Z}(p^\infty)) \cap A,$$

entonces existe $\frac{l}{p^k} \in \mathbb{Z}(p^\infty)$, con $(l; p) = 1$ tal que $\beta(\frac{l}{p^k}) = a$. Así, se tiene que

$$p^{k-1}a = p^{k-1} \cdot \beta(\tfrac{l}{p^k}) = \beta(p^{k-1} \cdot \tfrac{l}{p^k}) = \beta(\tfrac{l}{p}) = \beta \circ \alpha(lc) = \iota(lc) = lc.$$

Esto último muestra que $p^{k-1}a = lc \in A \cap C = \{0\}$, lo cual implica que $lc = 0$. Como $o(c) = p$, se tiene que $p \mid l$, lo cual contradice la suposición de $(l; p) = 1$. Por lo tanto, $a = 0$, con lo que

$$\beta(\mathbb{Z}(p^\infty)) \cap A = \{0\}.$$

De esta manera, por el teorema de Baer, $E = \beta(\mathbb{Z}(p^\infty) \oplus B$, donde B es un subgrupo divisible no trivial de E que contiene a A, mostrando así que E no es mínimo divisible sobre A.

Por lo tanto, A es un subgrupo esencial en B. □

Teorema 10.2.5. *Sea A un grupo. Todo grupo divisible que contiene al grupo A, contiene un grupo mínimo divisible que contiene a A. Además, dos grupos mínimos divisibles que contienen a A son isomorfos sobre A.*

Demostración. Sea D un grupo divisible que contiene a A. El conjunto

$$\mathcal{F} = \{C \mid C \leq D \,\text{divisible tal que}\; C \cap A = \{0\}\}$$

es no vacío ya que el grupo trivial $\{0\}$ es un elemento de $\mathcal{F}$. Si a $\mathcal{F}$ lo ordenamos por la inclusión, se tiene que $(\mathcal{F}, \subset)$ es un conjunto parcialmente ordenado donde toda cadena tiene una cota superior. En efecto, si $\{C_i\}_{i \in I}$ es una cadena de grupos divisibles, donde cada $C_i \cap A = \{0\}$, entonces el grupo formado por la unión de todos ellos $\cup_{i \in I} C_i$ también es divisible y ajeno a A, puesto que $a \in A \cap (\cup_{i \in I} C_i)$ si y sólo si $a \in A \cap C_j$, para algún $j \in I$. Por el Lema de Zorn, el conjunto $\mathcal{F}$ tiene un elemento maximal. Si M es un elemento maximal de $\mathcal{F}$, por ser divisible se tiene que $D = M \oplus E$, con E de nuevo un subgrupo divisible de D, que contiene a A.

Afirmamos que E es un grupo mínimmo divisible sobre A. Sea B un subgrupo divisible de E que contiene a A. Por ser divisible, $D = B \oplus F$, donde $F \cap B = \{0\}$. Como F es un sumando directo del grupo divisible D, resulta ser también divisible. Más aún, $F \cap A \subset F \cap B = \{0\}$, por lo que $F \in \mathcal{F}$. Ahora, como $B \subsetneq E$ y $M \cap E = \{0\}$, entonces $B \cap M = \{0\}$. Por el teorema de Baer, podemos suponer que $M \subset F$. Así, el hecho de que B sea un subgrupo propio de E nos asegura que $M \subsetneq F$, lo cual contradice la maximalidad del elemento M. Por lo tanto, E es un grupo mínimo divisible sobre A, lo cual demuestra la existencia del grupo mínimo divisible.

Por otra parte, si E_1 y E_2 son dos grupos, cada uno de ellos mínimo divisible sobre A, se tiene que el diagrama

$$\begin{tikzcd} A \arrow[r, "\iota"] \arrow[d, "\iota"'] & E_1 \arrow[dl, "\eta"] \\ E_2 & \end{tikzcd}$$

conmuta, por la divisibilidad e inyectividad de E_2. Esto último equivale a decir que el automorfismo id_A es extendida al morfismo $\eta : E_1 \longrightarrow E_2$. Como $\eta(E_1)$ es divisible en E_2 y contiene a A, la condición de que E_2 sea mínimo divisible sobre A, implica que η es sobre. Así mismo, como A es un grupo esencial de E_1 y $\eta\mid_A = id_A$ es un monomorfismo, por el Lema 10.2.2 se tiene que $\eta : E_1 \longrightarrow E_2$ es inyectiva, teniendo así que η es un isomorfismo entre E_1 y E_2, que además deja fijo a los elementos de A. $\square$

Por el teorema anterior, se tiene la siguiente

Definición 10.2.6. *Dado un grupo A, la cápsula inyectiva de A es un grupo E mínimo divisible que contiene a A.*

Teorema 10.2.7. *Sea D un grupo. Son equivalentes las siguientes proposiciones:*

(i) D es un grupo divisible.

(ii) D es inyectivo.

(iii) D es un sumando directo de cualquier grupo que lo contenga.

Demostración. Hemos visto que todo grupo divisible es inyectivo. Además, si A es un grupo que contiene al grupo inyectivo D, entonces el diagrama

$$\begin{tikzcd} 0 \arrow[r] & D \arrow[r, "\iota"] \arrow[d, "id_D"'] & A \arrow[dl, "\eta"] \\ & D & \end{tikzcd}$$

muestra que D es un sumando directo de A. Por lo tanto, basta demostrar $iii) \Longrightarrow ii)$.

Sea D un grupo tal que D es sumando directo de cualquier grupo que lo contenga. Como vimos anteriormente, podemos sumergir a D en un grupo divisible E. En particular, por ser D un sumando directo del grupo divisible E, se tiene que D también es divisible. □

Observación. *Como $\mathbb{Z}(p^\infty)$ es la cápsula inyectiva de $\mathbb{Z}(p^k)$, para cualquier $k \in \mathbb{N}$, entonces $\oplus_{i\in I}\mathbb{Z}(p^\infty)_i$ es la cápsula inyectiva de $\oplus_{i\in I}\mathbb{Z}(p^{k_i})$.*

Regresando a la cuestión de caracterizar a la parte de torsión de un grupo divisible A, para un p-grupo divisible, se tiene el siguiente resultado:

Teorema 10.2.8. *Sea D un p-grupo divisible. Entonces $D \cong \oplus_{i\in I}(\mathbb{Z}(p^\infty))_i$.*

Demostración. Sea $\mathcal{F}$ una familia independiente de grupos cíclicos de D. Por ser independientes, $< \mathcal{F} >= \oplus_{F\in\mathcal{F}}F$. De esta manera, si

$$\mathcal{I} = \{\mathcal{F} \mid \mathcal{F} \text{ es una familia independiente de subgrupos cíclicos}\},$$

la condición de independencia nos asegura que $\mathcal{I}$ es una familia de carácter finito, por lo que es válido el Lema de Tukey. Así, si $\mathcal{F}_\mathcal{I}$ es máximo con respecto a la inclusión, afirmamos que $< \mathcal{F}_\mathcal{I} >$ es un grupo esencial de D. En efecto, si $a \in D\setminus < \mathcal{F}_\mathcal{I} >$ es tal que $< a > \cap < \mathcal{F}_\mathcal{I} >= \{0\}$, se llega a la contradicción de la maximalidad de $\mathcal{F}_\mathcal{I}$, puesto que $< a > \cup \mathcal{F}_\mathcal{I}$ es una familia independiente de grupos cíclicos.

Para simplificar la notación, supongamos que I es un conjunto que etiqueta a la familia $\mathcal{F}_\mathcal{I}$. Como cada elemento en $\mathcal{F}_\mathcal{I}$ es un p-grupo cíclico, entonces

$$< \mathcal{F}_{\mathcal{I}} >= \oplus_{F\in\mathcal{F}_{\mathcal{I}}} F \cong \oplus_{i\in I}(\mathbb{Z}(p^{k_i})).$$

De esta manera, se tiene el diagrama

$$\begin{tikzcd}
\oplus_{i\in I}(\mathbb{Z}(p^{k_i})) \arrow[r, "\iota"] \arrow[d, "\iota"'] & D \arrow[dl, "\eta"] \\
\oplus_{i\in I}(\mathbb{Z}(p^{\infty}))_i &
\end{tikzcd}$$

donde $\eta : D \longrightarrow \oplus_{i\in I}(\mathbb{Z}(p^{\infty}))_{i\in I}$ es debido a que $\oplus_{i\in I}(\mathbb{Z}(p^{\infty}))_{i\in I}$ es un grupo divisible y por lo tanto inyectivo. Ahora, como $\oplus_{i\in I}(\mathbb{Z}(p^{k_i}))$ es esencial en D y

$$\iota : \oplus_{i\in I}(\mathbb{Z}(p^{k_i})) \longrightarrow \oplus_{i\in I}(\mathbb{Z}(p^{\infty}))_i$$

es inyectiva, entonces η es un monomorfismo.

De esta manera, como $\oplus_{i\in I}(\mathbb{Z}(p^{\infty}))_{i\in I}$ es la cápsula inyectiva de $\oplus_{i\in I}(\mathbb{Z}(p^{k_i}))$ y $\eta(D)$ es un grupo divisible en $\oplus_{i\in I}(\mathbb{Z}(p^{\infty}))_{i\in I}$ que contiene a $\oplus_{i\in I}(\mathbb{Z}(p^{k_i}))$, se tiene que η es un epimorfismo, con lo cual

$$\oplus_{i\in I}(\mathbb{Z}(p^{\infty}) \cong D.$$

$\square$

Observación. *Si A_p es la p-componente del grupo divisible y de torsión T, entonces A_p es también divisible, por ser un sumando directo del grupo T. Como A_p es un p-grupo, del teorema anterior se sigue que*

$$A_p \cong \oplus_{i\in I}(\mathbb{Z}(p^{\infty}))_i.$$

Por lo tanto, tenemos el siguiente

Teorema 10.2.9. *Todo grupo divisible D es de la forma*

$$\oplus_p(\oplus_{i\in I}(\mathbb{Z}(p^{\infty}))_i \oplus_{j\in J} \mathbb{Q}_j.$$

10.3. Grupos puros

Definición 10.3.1. *Sea A un grupo. Decimos que un subgrupo G de A es puro, si cada vez que la ecuación $nx = g$, con $g \in G$, tiene solución en A , la tiene también en G.*

Observación. *Por la definición anterior, si G es un subgrupo puro en A y $n \mid g$ en A, entonces $n \mid g$ en G. Además, como $n \mid g$ en G es equivalente a la condición $g \in nG$, se tiene que*

$$G \text{ es puro en } A \text{ si y solo si } nG = G \cap nA,\ \forall n \in \mathbb{Z}.$$

Nótese también que como G y A son ambos grupos, basta pedir que la condición anterior se cumpla para $n \in \mathbb{N}$.

Observación. *Si al grupo A lo dotamos con la topología $\mathbb{Z}$-ádica y G es un subgrupo puro de A, entonces la topología $\mathbb{Z}$-ádica inducida por A en G, coincide con la topología $\mathbb{Z}$-ádica de G.*

Definición 10.3.2. *Un subgrupo G de A es p-puro (p primo), si*

$$p^k G = G \cap p^k A, \text{ para } k = 1, 2, \ldots.$$

Observación. *De la definición anterior, son equivalentes que un subgrupo G sea p-puro en A y que las p-alturas de los elementos de G son las mismas en G que en A. Además, de manera análoga a la observación anterior, si al grupo A lo dotamos con la topología p-ádica, entonces para cualquier subgrupo G p-puro de A, se cumple que la topología inducida de A en G, coincide con la topología p-ádica del grupo G.*

Proposición 10.3.3. *Sea G un subgrupo de A. Entonces G es p-puro en A, para todo primo p, si y sólo si G es puro.*

Demostración. Si G es un subgrupo puro en A, entonces G es p-puro, para cualquier primo p. En efecto, si p es un primo, como $nG = G \cap nA$ para toda $n \in \mathbb{N}$, en particular se cumple para cualquier p^k, con $k = 1, 2, \ldots$.

Supongamos ahora que el subgrupo G es p-puro para todo primo p. Sea $n \in \mathbb{N}$, con factorización en primos $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_r^{\alpha_r}$. Notemos que como G es p-puro, se tiene que $p^k G = G \cap p^k A$ para cualquier primo p y $k > 0$. Así,

$$\begin{aligned} nG &= (p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_r^{\alpha_r})G \\ &= (p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_{r-1}^{\alpha_{r-1}})(p_r^{\alpha_r} G) \\ &= (p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_{r-1}^{\alpha_{r-1}})(G \cap p_r^{\alpha_r} A) \\ &= (p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_{r-1}^{\alpha_{r-1}})G \cap (p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_{r-1}^{\alpha_{r-1}})p_r^{\alpha_r} A \\ &= (p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_{r-1}^{\alpha_{r-1}})G \cap nA \\ &= (p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_{r-2}^{\alpha_{r-2}})(p_{r-1}^{\alpha_{r-1}} G) \cap nA \\ &= (p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_{r-2}^{\alpha_{r-2}})(G \cap p_{r-1}^{\alpha_{r-1}} A) \cap nA \\ &= (p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_{r-2}^{\alpha_{r-2}})G \cap nA, \end{aligned}$$

donde esta última igualdad es debido a que $nA \subset p_{r-1}^{\alpha_{r-1}}A$. Más aún, $nA \subset p_i^{\alpha_i}A$, por lo que si proseguimos de esta manera, llegamos a la igualdad

$$nG = (p_1^{\alpha_1})G \cap nA = (G \cap p_1^{\alpha_1}A) \cap nA = G \cap nA,$$

lo cual implica que G es un subgrupo puro. □

Veamos algunas propiedades de los subgrupos puros:

- Todo sumando directo de un grupo es un subgrupo puro. Supongamos que $A = B \oplus C$. Sin pérdida de generalidad, demostraremos que $nB = B \cap nA$ para cualquier $n \in \mathbb{N}$. Claramente, $nB \subset B \cap nA$, por lo que basta demostrar la otra contención. Sea n cualquier entero positivo y $b \in B \cap nA$, con $b = na$ para alguna $a \in A$. Como $A = B \oplus C$, existen $b_1 \in B$ y $c \in C$ tales que $a = b_1 + c$. Con esto en cuenta, se tiene que $na = n(b_1 + c) = nb_1 + nc$. Ahora, por ser A la suma directa de B y de C, como $b + 0 = na = nb_1 + nc$, se sigue que $b = nb_1$ y $0 = nc$, con lo cual $b \in nB$.

- La parte de torsión de cualquier grupo mixto G es un subgrupo puro. Sean G un grupo, G_T la parte de torsión del grupo G y $n > 0$. Como $nG_T \subset G_T \cap nG$, basta demostrar que $G_T \cap nG \subset nG_T$. Sea $g \in G_T \cap nG$. Como g está en la parte de torsión de G, tiene orden finito $s = o(g)$. Además, como $g \in nG$, existe $g_1 \in G$ tal que $g = ng_1$, por lo que

$$0 = sg = s(ng_1) = (sn)g_1,$$

  lo cual quiere decir que $g_1 \in G_T$. Por lo tanto $g \in nG_T$.

- Toda p-componente de un grupo G es un subgrupo puro. Sean p un primo y A_p la p-componente de G. Por una parte, $p^k A_p \subset A_p \cap p^k G$. Ahora, si $a \in A_p \cap p^k G$, entonces $o(a) = p^s$ y $a = p^k g$ para alguna $g \in G$. Esto implica que $0 = p^s a = p^{s+k} g$, por lo que $g \in A_p$, con lo cual $a \in p^k A_p$. Por lo tanto, $p^k A_p = A_p \cap p^k G$, para toda $k \in \mathbb{N}$.

  Sea q un primo distinto a p y $k > 0$. Si $b \in A_p \cap q^k G$, entonces la ecuación $q^k x = b$ tiene solución en G, digamos el elemento $g \in G$. Además, como $b \in A_p$, $o(b) = p^s$, teniendo así que $0 = p^s b = p^s(q^k g)$, es decir, el elemento $q^k g$ tiene orden p^s. Como $o(na) = o(a)/(n; o(a))$ para cualquier $a \in A$, al denotar por t al orden de g, se tiene que

$$p^s = ord(q^k g) = t/(q^k, t).$$

Notemos que como q es primo, $(q^k, t) = q^l$, con $0 \leq l \leq k$, con lo cual obtenemos la igualdad $q^l p^s = t$. Obsérvese que si $l = 0$, entonces $t = p^s$, de donde se sigue que $g \in A_p$ y en cuyo caso se tendría que $b \in q^k A_p$. Por lo tanto, consideraremos a $l \in \{1, \ldots, k\}$.

Ahora, como p y q son primos relativos, también lo son p^s y q^l, con lo cual existen α y β enteros tales que $1 = \alpha p^s + \beta q^l$. Nótese que de esta combinación lineal también se deduce que $(p, \beta) = 1$. Así, $g = (\alpha p^s)g + (\beta q^l)g$, por lo que

$$b = q^k g = (\alpha p^s q^k)g + (\beta q^k q^l)g = q^k(\beta q^l g),$$

es decir, $(\beta q^l g)$ es una solución de la ecuación $q^k x = b$, que además satisface que

$$o(\beta q^l g) = t/(\beta q^l, t) = p^s q^l/(\beta q^l, p^s q^l) = q^l p^s / q^l(\beta, p^s) = p^s/(\beta, p^s).$$

Como β y p son primos relativos, $(\beta, p^s) = 1$, por lo que $o(\beta q^l g) = p^s$, es decir, $\beta q^l g \in A_p$. Por lo tanto, para cualquier primo $q \neq p$ y $k > 0$, siempre que la ecuación $q^k x = b$, con $b \in A_p$, tenga solución en G, lo tendrá también en A_p. Esto demuestra que A_p es un subgrupo puro.

Lema 10.3.4. *Sean $B, C \leq A$ tales que $C \leq B \leq A$. Entonces*

(i) Si C es puro en B y B es puro en A, entonces C es puro en A.

(ii) Si B es puro en A, entonces B/C es puro en A/C.

(iii) Si C es puro en A y B/C es puro en A/C, entonces B es puro en A.

Demostración. (i) Si tanto B como C son subgrupos puros en A, entonces $nB = B \cap nA$ y $nC = C \cap nA$, para cada $n \in \mathbb{Z}$. De esta manera,

$$nC = C \cap nB = C \cap (B \cap nA) = (C \cap B) \cap nA = C \cap nA.$$

(ii) Nótese que para cualquier $n \in \mathbb{Z}$, $n(B/C) = nB/C = nB + C$. Así, si $nB = B \cap nA$, entonces

$$n(B/C) = nB + C = (B \cap nA) + C = B \cap (nA + C) = B \cap n(A/C) = (B/C) \cap n(A/C),$$

donde la tercer igualdad es debido a la ley modular con los subgrupos $C \leq B$ y nA de A.

(iii) Veamos que dada cualquier $n \in \mathbb{N}$, si la ecuación $nx = b$, con $b \in B$, tiene solución en A, entonces también la tiene en B. Sean $n \in \mathbb{N}$, $b \in B$ y $a \in A$ una solución de la ecuación $nx = b$. Con esto en cuenta, $n(a + C) = b + C$ es un elemento tanto en B/C como en $n(A/C)$. Al ser B/C un subgrupo puro en A/C se cumple que

$$n(B/C) = (B/C) \cap n(A/C),$$

por lo que existe $b' \in B$ tal que $n(b' + C) = b + C$. Esto quiere decir que $nb' = b + c$, para alguna $c \in C$, con lo cuál se obtiene que

$$n(b' - a) = nb' - na = b + c - b = c,$$

pues $na = b$. Ahora, como C es puro en A y $nx = c$ tiene como solución al elemento $b' - a \in A$, existe $c' \in C$ tal que $nc' = c$. Por lo tanto,

$$n(b' - c') = nb' - nc' = b + c - c = b,$$

donde $b' - c' \in B$. Por lo tanto, B es puro en A.

$\square$

Proposición 10.3.5. *Todo subgrupo infinito puede sumergirse en un subgrupo puro de la misma cardinalidad y todo subgrupo finito en un subgrupo puro numerable.*

Demostración. Sea $B \leq A$ con $\mid B \mid = \mathcal{M}$. Consideremos las ecuaciones de la forma $nx = b$, con $b \in B$, que tengan solución en A. Para cada una de estas ecuaciones, tomemos una solución $a_{n,b} \in A$ y formemos el subgrupo B_1 generado por B y el conjunto

$$\{a_{n,b} \mid b \in B \text{ y } n \in \mathbb{N}\}.$$

Repitiendo este argumento, ahora para ecuaciones de la forma $nx = b$, con $b \in B_1$, obtenemos el subgrupo B_2 generado por B_1 y el conjunto

$$\{a_{n,b} \mid b \in B_1 \text{ y } n \in \mathbb{N}\}$$

de soluciones de dichas ecuaciones. Prosiguiendo de esta manera, el conjunto $G = \cup_{i\in\mathbb{N}} B_i$ es un subgrupo de A. En efecto, notemos primero que si $b \in G$, entonces $b \in B_n$ para algún $n \in \mathbb{N}$. Además, como los subgrupos B_i satisfacen que $B_n \leq B_{n+1}$, para toda $n \in \mathbb{N}$, la suma de dos elementos $a, b \in G$, con $a \in B_j$ y $b \in B_l$ está definido como $a+b \in B_s$ donde $s = max\{j, l\}$. Por otra parte, si la ecuación $nx = b$, con $b \in G$ tiene solución en A, por la manera en que se construyó al conjunto G, $b \in B_m$ para alguna $m \in \mathbb{N}$, por lo que existe $a_{n,b} \in B_{m+1}$ solución de la ecuación $nx = b$. Como $B_{n+1} \subset G$, entonces G es puro en A. Por último, se tiene que $\mid G \mid \leq \mathcal{M}\aleph_0$, de donde se siguen ambas afirmaciones. $\square$

El siguiente resultado nos permite identificar subgrupos puros en un grupo A, que son sumandos directos de éste.

Proposición 10.3.6. *Sea $B \leq A$ con $B = \oplus_{i=1}^{n} < c_i >$, donde cada $< c_i >$ es un grupo cíclico de orden p^k. Las siguientes proposiciones son equivalentes:*

1. *B es un subgrupo puro. (p-puro).*
2. *B satisface $B \cap p^k A = \{0\}$.*
3. *B es un sumando directo de A.*

Demostración. 1. $\Longrightarrow$ 2. Si B es un subgrupo puro, entonces es p-puro. De esta manera, para cualquier $m \in \mathbb{N}$, se tiene que $p^m B = B \cap p^m A$. Como $B = \oplus_{i=1}^{n} < c_i >$, con cada $< c_i >$ un grupo cíclico de orden p^k, se sigue que $0 = p^k B = B \cap p^k A$.

2. $\Longrightarrow$ 3. Supongamos que B satisface que $B \cap p^k A = 0$. Sea C un subgrupo B-alto de A, con $p^k A \subset C$, es decir, un seudocomplemento de B máximo en A que contiene a $p^k A$. Supongamos que $a \in A$ es tal que $pa = b+c$, con $b \in B$ y $c \in C$. Demostraremos que existe $b' \in B$ tal que $pb' = b$, para así usar el Lema 4.2.8. Bajo estas hipótesis, se sigue que $p^k a = p^{k-1}b + p^{k-1}c$. Ahora, tanto $p^k a$ como $p^{k-1}c$ están en C, ya que $p^k A \leq C$, por lo que

$$p^k a - p^{k-1}c = p^{k-1}b \in C.$$

Como $B \cap C = \{0\}$, esta última igualdad implica que $p^{k-1}b = 0$.

Por otra parte, cualquier elemento $b \in B$ se escribe como una combinación lineal de los elementos c_i, es decir, de la forma $b = z_1 c_1 + \cdots + z_n c_n$, con $z_i \in \mathbb{Z}$. Así, si $p^{k-1}b = 0$ y $b = z_1 c_1 + \cdots + z_n c_n$, entonces

$$0 = p^{k-1}b = (z_1p^{k-1})c_1 + \cdots + (z_np^{k-1})c_n.$$

Esto último implica que $p \mid z_i$, para toda $i \in \{1, \ldots, n\}$, ya que c_i tiene orden p^k. De esta manera,

$$b = (pz'_1)c_1 + \cdots + (pz'_n)c_n = p\Sigma_{i=1}^n z'_i c_i,$$

donde $b' = \Sigma_{i=1}^n z'_i c_i \in B$. Por lo tanto, como para cualquier $a \in A$, que satisface $pa = b + c$, con $b \in B$ y $c \in C$, se tiene que $b = pb'$, para algún $b' \in B$, el Lema 4.2.8 nos garantiza que $A = B \oplus C$.

3. $\Longrightarrow$ 1. Todo sumando directo es un subgrupo puro. □

Corolario 10.3.7. *Sea A un grupo. Todo elemento $a \in A$ de orden p y de p-altura finita puede sumergirse en un sumando directo finito y cíclico.*

Demostración. Sea $a \in A$, con $h_p(a) = k < \infty$. Esto quiere decir que existe $b \in A$ que satisface $p^kb = a$. Como a es de orden p, entonces $p^{k+1}b = pa = 0$. Notemos que como $p^{k+1}b = 0$, entonces el orden de b es p^s, con $1 \leq s \leq k+1$. Afirmamos que $s = k+1$. En efecto, como

$$p = o(a) = o(p^kb) = o(b)/(p^k, o(b)),$$

si $s \leq k$, entonces $(o(b), p^k) = o(b)$, con lo cual se tendría que $p = o(b)/o(b) = 1$. De esta manera, $B =< b >$ es un subgrupo cíclico de A, de orden p^{k+1} tal que $a \in B$. Veamos ahora que $B \cap p^{k+1}A = \{0\}$. Como B es un subgrupo cíclico de orden p^{k+1}, sus únicos subgrupos propios son cíclicos y de orden p^m, donde $m \in \{1, \ldots, k\}$. Más aún, estos subgrupos forman la cadena

$$< p^kb > \subset < p^{k-1}b > \subset \cdots \subset < pb >.$$

Así, como $p^{k+1}A$ es un subgrupo de A, entonces $B \cap p^{k+1}A$ es un subgrupo de B. Por lo tanto, si $B \cap p^{k+1}A \neq \{0\}$, entonces $a \in B \cap p^{k+1}A$, ya que $p^kb = a$ es el menor subgrupo de B. Lo anterior implica que existe $a' \in A$ tal que $p^{k+1}a' = a$, lo cual contradice que $h_p(a) = k$. □

Observación. *El subgrupo $B =< b >$ en el cual se sumerge el elemento a de orden p y de p-altura finita, es isomorfo al grupo cocíclico $\mathbb{Z}(p^{k+1})$. Además, B es un sumando directo de A.*

El siguiente resultado generaliza la idea anterior:

Corolario 10.3.8. *Si A es un grupo que tiene elementos de orden finito, entonces tiene un subgrupo cocíclico como sumando directo.*

Demostración. Observemos que como A es un grupo con elementos de orden finito, podemos escoger $a \in A$ de orden un primo p. Ahora, si A tiene algún subgrupo isomorfo a $\mathbb{Z}(p^\infty)$, entonces éste es un sumando directo por ser un grupo divisible. Supóngase que A no contiene a algún subgrupo isomorfo a $\mathbb{Z}(p^\infty)$, para cualquier primo p. Afirmamos que existe un elemento $b \in A_p$, de orden p, tal que $h_p(b) < \infty$. De lo contrario, si todo elemento $c \in A_p$, con $o(c) = p$ tuviera p-altura infinita, entonces por la Proposición 10.1.6, se tiene que A_p es un p-grupo divisible. Esto quiere decir que

$$\mathbb{Z}(p^\infty) \hookrightarrow A_p \hookrightarrow A,$$

lo cual contradice la suposición. Por lo tanto, existe $b \in A_p$, con $o(b) = p$ y $h_p(c) < \infty$, cayendo así en las hipótesis del corolario anterior. $\square$

Capítulo 11

Producto Tensorial

11.1. Definición

Definición 11.1.1. *Sean A, C y G grupos. Decimos que la función $g : A \times C \longrightarrow G$ es bilineal, si para toda $a_1, a_2 \in A$ y $c_1, c_2 \in C$ se satisface:*

1. $g(a_1 + a_2, c_1) = g(a_1, c_1) + g(a_2, c_1)$.

2. $g(a_1, c_1 + c_2) = g(a_1, c_1) + g(a_1, c_2)$.

Algunas propiedades de las funciones bilineal son las siguientes:

(a) $g(a, 0) = 0 = g(0, c)$, pues $g(a, 0) = g(a, 0 + 0) = g(a, 0) + g(a, 0)$, lo cual implica que $g(a, 0) = 0$. Análogamente para $g(0, c)$.

(b) $g(-a, c) = -g(a, c) = g(a, -c)$.

(c) $g(na, c) = ng(a, c) = g(a, nc)$, para cualquier $n \in \mathbb{Z}$.

Sea X el grupo libre generado por las parejas ordenadas (a, c), con $a \in A$ y $c \in C$. Si Y es el subgrupo de X generado por los elementos de la forma

$$(a_1 + a_2, c) - (a_1, c) - (a_2, c) \text{ y } (a, c_1 + c_2) - (a, c_1) - (a, c_2),$$

definimos al subgrupo

$$A \otimes C := X/Y.$$

La clase de $(a,c)+Y$ la denotaremos por $a\otimes c$. A este grupo le llamamos el *producto tensorial* entre A y C. Obsérvese que los elementos de $A\otimes C$ son de la forma $\Sigma k_i(a_i\otimes c_i)$, donde $k_i\in\mathbb{Z}$, $a_i\in A$ y $c_i\in C$.

Por la manera en que definimos al producto tensorial $A\otimes C$, se cumplen las siguientes propiedades:

- $(a_1+a_2)\otimes c = a_1\otimes c + a_2\otimes c.$
- $a\otimes(c_1+c_2) = a\otimes c_1 + a\otimes c_2.$
- $na\otimes c = n(a\otimes c) = a\otimes nc.$

Nótese que estas propiedades implican que la proyección natural

$$e : A\times C \longrightarrow A\otimes C,$$

definida por $(a,c)\longmapsto a\otimes c$, es un homomorfismo, y además

$$a\otimes 0 = 0\otimes 0 = 0\otimes c,$$

ya que

$$a\otimes 0 = a\otimes(0+0) = a\otimes 0 + a\otimes 0,$$

por lo que $a\otimes 0 = 0\otimes 0$. Más aún, e es una función bilineal que satisface la siguiente particularidad: si $g : A\times C\longrightarrow G$ es una función bilineal, existe un único homomorfismo $\theta : A\otimes C\longrightarrow G$ tal que el siguiente diagrama es conmutativo:

$$\begin{tikzcd} A\times C \arrow[r, "e"] \arrow[d, "g"'] & A\otimes C \arrow[dl, "\theta"] \\ G & \end{tikzcd}.$$

En efecto, si $g : A\times C\longrightarrow G$ es una función bilineal, definimos

$$\theta : A\otimes C\longrightarrow G$$

por $\theta(a\otimes c) = g(a,c)$. Como g es bilineal y el producto tensorial distribuye a la suma, se tiene que θ es un homomorfismo de grupos que hace conmutativo al diagrama anterior. Para demostrar la unicidad, supongamos que

$$\Psi : A\otimes C\longrightarrow G$$

es otra función, que hace conmutativo el diagrama

$$\begin{tikzcd} A \times C \arrow[r, "e"] \arrow[d, "g"'] & A \otimes C \arrow[dl, "\Psi"] \\ G & \end{tikzcd} .$$

Como los elementos $a \otimes c$ generan al producto tensorial, se sigue que

$$\Psi(a \otimes c) = g(a, c) = \theta(a \otimes c),$$

lo cual implica que $\Psi = \theta$. De esta manera, tenemos el siguiente

Teorema 11.1.2. *Sean A y C grupos. Entonces, existe un grupo $A \otimes C$ y una función bilineal $e : A \times C \longrightarrow A \otimes C$ tal que, para cualquier otra función bilineal $g : A \times C \longrightarrow G$, existe un único morfismo $\theta : A \otimes C \longrightarrow G$ tal que el siguiente diagrama conmuta:*

$$\begin{tikzcd} A \times C \arrow[r, "e"] \arrow[d, "g"'] & A \otimes C \arrow[dl, "\theta"] \\ G & \end{tikzcd} .$$

Observemos que esta propiedad la determina el grupo $A \otimes C$, salvo isomorfismos. En efecto, si H es otro grupo con esta propiedad, entonces para la función bilineal $e : A \times C \longrightarrow A \otimes C$, se tiene el diagrama conmutativo

$$\begin{tikzcd} A \times C \arrow[r, "h"] \arrow[d, "e"'] & H \arrow[dl, "\theta_H"] \\ A \otimes C & \end{tikzcd} .$$

de donde $e = \theta_H \circ h$. Así mismo, por la propiedad de bilinealidad de h, se tiene que el diagrama

$$\begin{tikzcd} A \times C \arrow[r, "e"] \arrow[d, "h"'] & A \otimes C \arrow[dl, "\theta"] \\ H & \end{tikzcd} .$$

es conmutativo, con lo cual $h = \theta \circ e$. Esto implica que

$$e = \theta_H \circ h = \theta_H \circ (\theta \circ e) = (\theta_H \circ \theta) \circ e \text{ y}$$
$$h = \theta \circ e = \theta \circ (\theta_H \circ h) = (\theta \circ \theta_H) \circ h.$$

Por lo tanto, $\theta_H \circ \theta : A \otimes C \longrightarrow A \otimes C$ es la función $id_{A\otimes C}$, al igual que $\theta \circ \theta_H : H \longrightarrow H$ la función id_H, teniendo así que θ_H y θ son isomorfismos entre H y $A \otimes C$.

Definición 11.1.3. *A la función $e : A \times C \longrightarrow A \otimes C$, con regla de correspondencia $(a, c) \longmapsto a \otimes c$, la llamamos la función tensor.*

11.2. Propiedades y ejemplos

Proposición 11.2.1. *Sean A y C dos grupos. Entonces en el producto tensorial $A \otimes C$ se cumplen las siguientes propiedades:*

(i) Si $m \mid a$ y $n \mid c$, entonces $mn \mid a \otimes c$.

(ii) Si $ma = 0$ y $nc = 0$, entonces $(m; n)[a \otimes c] = 0$.

(iii) Si $n \mid a$ y $nc = 0$, entonces $a \otimes c = 0$.

Demostración. (i) Si $a_0 \in A$ y $c_0 \in C$ son tales que $ma_0 = a$ y $nc_0 = c$, entonces

$$mn(a_0 \otimes c_0) = n(ma_0 \otimes c_0) = (ma_0 \otimes nc_0) = (a \otimes c).$$

(ii) Si $s, t \in \mathbb{Z}$ son tales que $ms + nt = (m; n)$, entonces

$$\begin{aligned}(m; n)(a \otimes c) &= (ms + nt)(a \otimes c) = ms(a \otimes c) + nt(a \otimes c)\\ &= s(ma \otimes c) + t(a \otimes nc) = s(0 \otimes c) + t(a \otimes 0)\\ &= (0 \otimes c) + (a \otimes 0) = (0 \otimes 0) + (0 \otimes 0) = (0 \otimes 0)\end{aligned}$$

(iii) Si $n \mid a$ entonces $na_0 = a$, para alguna $a_0 \in A$. De esta manera,

$$a \otimes c = (na_0 \otimes c) = a_0 \otimes nc = a_0 \otimes 0 = 0 \otimes 0 = 0.$$

□

Ejemplo. *Para cualquier grupo abeliano A, se tiene que*

$$\mathbb{Z} \otimes A \cong A.$$

Consideremos el grupo $\mathbb{Z} \times A$ formado por las parejas (n, a), con $n \in \mathbb{Z}$ y $a \in A$. De esta manera, se tiene la función bilineal $\varphi : \mathbb{Z} \times A \longrightarrow A$, definida por $(n, a) \longmapsto na$. Por la propiedad del producto tensorial, existe una función $\overline{\varphi} : \mathbb{Z} \otimes A \longrightarrow A$ que hace conmutar al diagrama

$$\begin{tikzcd} \mathbb{Z} \times A \arrow[r, "e"] \arrow[d, "\varphi"'] & \mathbb{Z} \otimes A . \arrow[dl, "\overline{\varphi}"] \\ A & \end{tikzcd}$$

Notemos que por las propiedades del producto tensorial, los elementos de la forma $n \otimes a$ satisfacen

$$n \otimes a = 1 \cdot n \otimes a = 1 \otimes na.$$

Esto implica que todo elemento $\Sigma_{i=1}^{m} n_i \otimes a_i$ en el producto tensorial, lo podemos escribir como

$$\Sigma_{i=1}^{m} n_i \otimes a_i = \Sigma_{i=1}^{m} 1 \otimes n_i a_i = 1 \otimes \Sigma_{i=1}^{m} n_i a = 1 \otimes a,$$

para alguna $a \in A$. Con esto en cuenta, $\overline{\varphi}$ está determinada en los elementos de la forma $1 \otimes a$, con $a \in A$. Así, al definir la función $\psi : A \longrightarrow \mathbb{Z} \otimes A$ por $a \longmapsto 1 \otimes a$, se tiene que $\overline{\varphi}$ y ψ satisfacen

$$\psi \circ \overline{\varphi} = id_{\mathbb{Z} \otimes A} \text{ y } \overline{\varphi} \circ \psi = id_A,$$

es decir, $\mathbb{Z} \otimes A \cong A$.

Lo anterior se puede generalizar con la siguiente

Proposición 11.2.2. *Sea A un anillo. Para cualquier A-módulo M,*

$$A \otimes_A M \cong M.$$

Demostración. La acción τ del anillo A en el grupo M es claramente una función bilineal de $A \times M$ en M. Por la propiedad del producto tensorial, existe $\alpha : A \otimes M \longrightarrow M$ tal que $\tau = \alpha \circ e$, donde $e : A \times M \longrightarrow A \otimes M$ es la función tensor. De esta manera,

$$am = \tau(a, m) = \alpha \circ e(a, m) = \alpha(a \otimes m).$$

Por otra parte, notemos que la función $\beta : M \longrightarrow A \otimes M$, definida por $\beta(m) = 1 \otimes m$ es un morfismo de grupos. En efecto, si $m_1, m_2 \in M$, entonces

$$(m_1 + m_2) \longmapsto 1 \otimes (m_1 + m_2) = 1 \otimes m_1 + 1 \otimes m_2.$$

Con esto en cuenta, se tiene que

$$\alpha \circ \beta(m) = \alpha(1 \otimes m) = 1m = m$$

así como

$$\beta \circ \alpha(a \otimes m) = \beta(am) = 1 \otimes am = 1 \cdot a \otimes m = a \otimes m,$$

por lo que α y β son isomorfismos. $\square$

Si ahora tensamos a un grupo A por un grupo cíclico de orden m, se obtiene un grupo isomorfo a A/mA, como lo muestra la siguiente

Proposición 11.2.3. *Para cualquier grupo A, se tiene que*

$$\mathbb{Z}(m) \otimes A \cong A/mA.$$

Demostración. La función $\varphi : \mathbb{Z}(m) \times A \longrightarrow A/mA$, definida por

$$(k, a) \longrightarrow ka + mA,$$

es una función bilineal, por lo que existe una única función

$$\widehat{\varphi} : \mathbb{Z}(m) \otimes A \longrightarrow A/mA$$

que hace conmutativo el diagrama

$$\begin{tikzcd} \mathbb{Z}(m) \times A \arrow[r, "e"] \arrow[d, "\varphi"'] & \mathbb{Z}(m) \otimes A \arrow[dl, "\widehat{\varphi}"] \\ A/mA & \end{tikzcd}.$$

De manera análoga al ejemplo anterior, la función $\psi : A \longrightarrow \mathbb{Z}(m) \otimes A$ definida por $a \longmapsto 1 \otimes a$ es un epimorfismo, tal que $mA \subset Ker\psi$, ya que

$$1 \otimes ma = m \otimes a = 0 \otimes a = 0.$$

Más aún, como φ es un epimorfismo y $\widehat{\varphi}$ hace conmutar el diagrama, entonces $\widehat{\varphi}$ es también un epimorfismo. Esto implica que $\widehat{\varphi} \circ \psi$ es una función de $A \longrightarrow A/mA$ tal que $\widehat{\varphi} \circ \psi(a) = a + mA$, es decir, $\widehat{\varphi} \circ \psi$ es la proyección canónica $\rho : A \longrightarrow A/mA$. Como $ker(\widehat{\varphi} \circ \psi) = ker\rho = mA$, entonces $ker\psi \subset mA$, teniendo así que $ker\psi = mA$. De esta manera, se obtiene que

$$A/ker\psi = A/mA \cong \mathbb{Z}(m) \otimes A.$$

Observación. *En particular $\mathbb{Z}(p^r) \otimes \mathbb{Z}(p^s) \cong \mathbb{Z}(p^t)$, donde $t = min\{s, r\}$.*

11.3. Producto tensorial visto de una manera categórica

A continuación, veremos al producto tensorial entre módulos desde un punto de vista categórico.

Consideremos al funtor $F : Mod_A \times_A Mod \longrightarrow Ab$, donde Mod_A es la categoría de A-módulos derechos, ${}_AMod$ la categoría de A-módulos izquierdos y Ab la categoría de grupos abelianos. Sean L y L' A-módulos izquierdos, M y M' A-módulos derechos, y $\lambda : L \longrightarrow L'$ y $\mu : M \longrightarrow M'$ morfismos de A-módulos. Si $L \times M$ es el producto directo entre los A-módulos , definimos la función $\varphi : L \times M \longrightarrow L' \otimes_A M'$ por

$$\varphi(x, y) = \lambda(x) \otimes \mu(y),$$

que resulta ser bilineal ya que tanto λ como μ son morfismos y el producto tensorial abre sumas. De esta manera, existe una única función

$$\alpha : L \otimes_A M \longrightarrow L' \otimes_A M'$$

tal que

$$\alpha(x \otimes y) = \varphi(x, y) = \lambda(x) \otimes \mu(y).$$

A este morfismo lo denotaremos por $\lambda \otimes \mu$, con lo que

$$\lambda \otimes \mu(x \otimes y) = \lambda(x) \otimes \mu(y).$$

Obsérvese que el morfismo $\lambda \otimes \mu$ es un elemento en

$$Hom(L \otimes_A M, L' \otimes_A M).$$

Ahora, si tenemos los morfismos $L \xrightarrow{\lambda} L' \xrightarrow{\lambda'} L''$ y $M \xrightarrow{\mu} M' \xrightarrow{\mu'} M''$, entonces

$$(\lambda' \otimes \mu')(\lambda \otimes \mu) = \lambda'\lambda \otimes \mu'\mu,$$

ya que en cualquier elemento generador $x \otimes y$ de $L \otimes M$, ambas funciones coinciden. Además, si $\lambda = id_L$ y $\mu = id_M$, entonces

$$\lambda \otimes \mu = id_L \otimes_A id_M = id_{L\otimes M},$$

lo cual muestra que el producto tensorial es un funtor de $Mod_A \times_A Mod$ en Ab. Notemos que este funtor es aditivo en las dos variables, es decir,

$$(\lambda_1 + \lambda_2) \otimes \mu = \lambda_1 \otimes \mu + \lambda_2 \otimes \mu,$$

así como

$$\lambda \otimes (\mu_1 + \mu_2) = \lambda \otimes \mu_1 + \lambda \otimes \mu_2.$$

Por otra parte, el producto tensorial no es un funtor exacto como lo muestra el siguiente

Ejemplo. *Consideremos a $\mathbb{Z} \subset \mathbb{Q}$ como un $\mathbb{Z}$-submódulo de $\mathbb{Q}$. Si tensamos por el grupo $\mathbb{Z}/2\mathbb{Z}$, se tiente*

$$\mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \hookrightarrow \mathbb{Q} \otimes \mathbb{Z}/2\mathbb{Z}.$$

Ahora, como cualquier $\frac{n}{m} \in \mathbb{Q}$ se puede escribir como $\frac{2n}{2m}$, se sigue que

$$\tfrac{n}{m} \otimes \overline{1} = \tfrac{2n}{2m} \otimes \overline{1} = \tfrac{n}{2m} \otimes 2\overline{1} = \tfrac{n}{2m} \otimes \overline{2} = \tfrac{n}{2m} \otimes \overline{0} = 0,$$

por lo que $\mathbb{Q} \otimes \mathbb{Z}/2\mathbb{Z} = 0$.

En cambio, una propiedad del producto tensorial es la siguiente:

Proposición 11.3.1. *El producto tensorial es un funtor exacto derecho en cada una de las dos variables.*

Demostración. Por simetría, basta tomar L_A un A-módulo derecho y una sucesión exacta de A-módulos izquierdos

$$0 \hookrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0.$$

Veamos que $L \otimes M' \xrightarrow{1\otimes\alpha} L \otimes M \xrightarrow{1\otimes\beta} M'' \longrightarrow 0$ es exacta. Notemos que cada generador en $L \otimes M''$ es de la forma $x \otimes y''$, con $x \in L$ y $y'' \in M''$. Como β es un epimorfismo, existe $y \in M$, con $\beta(y) = y''$, por lo que

$$(1 \otimes \beta)(x \otimes y) = x \otimes y''.$$

Además, como $Im\alpha \subset Ker\beta$, entonces para cualquier $x \otimes \alpha(y') \in Im(1 \otimes \alpha)$ se tiene que

$$(1 \otimes \beta)(x \otimes \alpha(y')) = x \otimes \beta(\alpha(y')) = x \otimes 0 = 0,$$

por lo que $Im(1 \otimes \alpha) \subset Ker(1 \otimes \beta)$. Con esto en cuenta, si

$$\xi : L \otimes M/Im(1 \otimes \alpha) \longrightarrow L \otimes M''$$

es tal que $\xi(\overline{x \otimes y}) = x \otimes \beta(y)$, se tiene el diagrama conmutativo

$$\begin{tikzcd} L \otimes M \arrow[r, "1\otimes\beta"] \arrow[d, "\rho"'] & L \otimes M'' . \\ L \otimes M/Im((1 \otimes \alpha) \arrow[ur, "\xi"'] & \end{tikzcd}$$

Así, como $1 \otimes \beta$ es un epimorfismo, también lo es ξ. De esta manera, exhibiremos una función μ inversa de ξ. Para esto, definimos

$$\varphi : L \times M'' \longrightarrow L \otimes M/Im(1 \otimes \alpha)$$

por $\varphi(x, y'') = \overline{x \otimes y}$, donde $\beta(y) = y''$. Notemos que la función φ está bien definida. En efecto, si $y_1 \in M$ es tal que $\beta(y_1) = y''$, entonces $y - y_1 \in Ker\beta = Im\alpha$, por lo que $x \otimes (y - y_1) \in Im(1 \otimes \alpha)$, lo cual implica que

$$x \otimes y + Im(1 \otimes \alpha) = x \otimes y_1 + Im(1 \otimes \alpha),$$

es decir, $\overline{x \otimes y} = \overline{x \otimes y_1}$ en $L \otimes M/Im(1 \otimes \alpha)$. Observemos también que, por como está definida φ, resulta ser una función bilineal. Para $(x_1 + x_2, y'') \in L \times M''$ se tiene que

$$\overline{(x_1 + x_2) \otimes y''} = \overline{x_1 \otimes y'' + x_2 \otimes y''} = \overline{x_1 \otimes y''} + \overline{x_2 \otimes y''}.$$

Este argumento es análogo para la segunda coordenada.

Por lo tanto, por la propiedad universal del producto tensorial, existe

$$\mu : L \otimes M'' \longrightarrow L \otimes M/Im(1 \otimes \alpha)$$

que hace conmutar el diagrama

$$\begin{tikzcd} L \otimes M'' \arrow[r, "e"] \arrow[d, "\varphi"'] & L \otimes M'' . \arrow[dl, "\mu"] \\ L \otimes M/Im((1 \otimes \alpha) & \end{tikzcd}$$

De la conmutatividad de los diagramas anteriores, se sigue que

$$\xi \circ \mu(x \otimes y'') = \xi(\overline{x \otimes y}) = x \otimes \beta(y) = x \otimes y''$$

al igual que

$$\mu \circ \xi(\overline{x \otimes y}) = \mu(x \otimes \beta(y)) = \overline{x \otimes y}.$$

Por lo tanto, ξ y μ son isomorfismos, con lo cual se tiene que

$$Im(1 \otimes \alpha) = Ker(1 \otimes \beta).$$

$\square$

Proposición 11.3.2. *Sean $\{L_i\}_{i \in I}$ una familia de A-módulos derechos y M un A-módulo izquierdo. Entonces se tiene el isomorfismo*

$$(\oplus_{i \in I} L_i) \otimes M \cong \oplus_{i \in I}(L_i \otimes M).$$

Demostración. Para facilitar la notación, denotaremos a un elemento $x \in \oplus_{i \in I} L_i$ por $x = (x_i)_{i \in I}$. Recordemos que bajo esta notación, estamos suponiendo que $x_i = 0$ para casi toda i, es decir, $x_i \neq 0$ para un número finito de índices. Consideremos la función

$$\mu : (\oplus_{i \in I} L_i) \times M \longrightarrow \oplus_{i \in I}(L_i \otimes M)$$

con regla de correspondencia $\mu((x_i)_{i \in I}, m) = (x_i \otimes m)_{i \in I}$. Por como se definió μ, se tiene que es una función bilineal, ya que el producto tensorial distribuye a la suma por ambos lados, y en cada $L_i \otimes M$. Además, por las propiedades del producto tensorial, existe un único morfismo

$$\varphi : (\oplus_{i \in I} L_i) \otimes M \longrightarrow \oplus_{i \in I}(L_i \otimes M)$$

tal que $\varphi((x_i)_{i \in I} \otimes m) = (x_i \otimes m)_{i \in I}$.

Por otra parte, si $\iota_j : A_j \longrightarrow \oplus_{i \in I} A_i$ denota a la función inclusión, para cada $j \in I$, entonces se tiene la función

$$\xi : \oplus_{i \in I}(L_i \otimes M) \longrightarrow (\oplus_{i \in I} L_i) \otimes M,$$

definida por $(x_i \otimes m_i)_{i \in I} \longmapsto \Sigma_{i \in I}(\iota_i(x_i) \otimes m_i)$. Notemos que como cada ι_j es un morfismo y el producto tensorial también abre sumas, se tiene que ξ es un morfismo. Más aún, φ y ξ son funciones inversas. En efecto, si $(x_i)_{i \in I} \otimes m$ es un elemento en $(\oplus_{i \in I} L_i) \otimes M$, entonces

$$\xi \circ \varphi((x_i)_{i \in I} \otimes m) = \xi(x_i \otimes m)_{i \in I}) = \Sigma_{i \in I}(\iota_i(x_i) \otimes m) = (x_i)_{i \in I} \otimes m$$

donde la última igualdad se debe a que $(x_i)_{i \in I} = \Sigma_{i \in I} \iota_i(x_i)$ y que el producto tensorial distribuye a la suma.

Por otra parte, si $(x_i \otimes m_i)_{i \in I} \in \oplus_{i \in I}(L_i \otimes M)$, entonces

$$\varphi \circ \xi((x_i \otimes m_i)_{i\in I}) = \varphi(\Sigma_{i\in I}(\iota_i(x_i) \otimes m_i))$$
$$= \Sigma_{i\in I}\varphi(\iota_i(x_i) \otimes m_i) = \Sigma_{i\in I}(x_i \otimes m_i) = (x_i \otimes m_i)_{i\in I},$$

ya que $\iota_i(x_i)$ es el elemento en $\oplus_{i\in I}L_i$ que tiene como valor x_i en su término i-ésimo y cero en cualquier otro, por lo que $\varphi(\iota_i(x_i) \otimes m_i)$ es el elemento en $\oplus_{i\in I}(L_i \otimes M)$ que tiene en su término i-ésimo el valor $x_i \otimes m_i$ y $0 \otimes m_i = 0$ en cualquier otro, es decir,

$$\varphi(\iota_i(x_i) \otimes m_i) = x_i \otimes m_i,$$

para cada $i \in I$. Por lo tanto $\oplus_{i\in I}(L_i\otimes M)$ y $(\oplus_{i\in I}L_i)\otimes M$ son isomorfos. $\square$

Corolario 11.3.3. *Si $A = \oplus_{i\in I}A_i$ y $C = \oplus_{j\in J}C_j$ entonces*

$$A \otimes C = \oplus_{i,j}(A_i \otimes C_j).$$

Demostración. Por la proposición anterior, como $A_i \otimes C = \oplus_{j\in J}A_i \otimes C_j$, basta demostrar que $A \otimes C = \oplus_{i\in I}(A_i \otimes C)$.

Para cada $i \in I$, sea $\rho_i : \oplus_{s\in I}A_s \longrightarrow A_i$ el morfismo proyección. Ahora, si $G = \oplus_{i\in I}(A_i \otimes C)$, la función $g : A \times C \longrightarrow G$, con regla de correspondencia

$$(a, c) \longmapsto \Sigma_{i\in I}(\rho_i(a) \otimes c),$$

es una función bilineal, puesto que cada proyección es un morfismo y el producto tensorial distribuye a la suma. Por la propiedad del producto tensorial, existe un único morfismo $\theta : A\otimes C \longrightarrow G$ que hace conmutativo el diagrama

$$\begin{tikzcd} A \times C \arrow[r, "e"] \arrow[d, "g"'] & A \otimes C \arrow[dl, "\theta"] \\ G & \end{tikzcd},$$

donde $e : A \times C \longrightarrow A \otimes C$ es la función tensor. Como el conjunto de elementos de la forma $\rho_i(a) \otimes c$, con $i \in I$, $a \in A$ y $c \in C$, generan a $\oplus_{i\in I}(A_i \otimes C)$, la función g es suprayectiva, con lo cual θ es un epimorfismo. Por otra parte, como $A_i = \rho_i(A)$, la función tensor $e : A\times C \longrightarrow A\otimes C$ induce la función $e\mid_{A_i}: A_i\times C \longrightarrow A\otimes C$, la cual tiene como regla de correspondencia $(\rho_i(a), c) \longmapsto \rho_i(a) \otimes c$. Además, al ser e una función bilineal, $e\mid_{A_i}$ también lo es, por lo que existe un único morfismo ψ_i que hace conmutar el diagrama

$$\begin{tikzcd} A_i \times C \arrow[r, "e'"] \arrow[d, "e|_{A_i}"'] & A_i \otimes C \arrow[dl, "\psi_i"] \\ A \otimes C & \end{tikzcd},$$

donde e' es la función tensor de $A_i \times C$ a $A_i \otimes C$. Nótese que para cada $i \in I$, $\psi_i(\rho_i(a) \otimes c) = e\mid_{A_i}(\rho_i(a), c)$. Por lo tanto, si tomamos a la familia $\{\psi_i\}_{i\in I}$, se tiene el morfismo $\Psi : G = \oplus_{i\in I}(A_i \otimes C) \longrightarrow A \otimes C$, donde

$$\Psi[\Sigma_{i\in I}(\rho_i(a) \otimes c)] \longmapsto \Sigma_{i\in I}\Psi_i(\rho_i(a) \otimes c).$$

Con esto en cuenta, $\Psi \circ g : A \times C \longrightarrow A \otimes C$ es una función tal que

$$\begin{gathered}\Psi \circ g(a, c) = \Psi[\Sigma_{i\in I}(\rho_i(a) \otimes c)] \\ = \Sigma_{i\in I}\Psi_i(\rho_i(a) \otimes c) = \Sigma_{i\in I}e\mid_{A_i}(\rho_i(a), c) = e(a, c).\end{gathered}$$

Nótese que los elementos de la forma $\rho_i(a)$, que aparecen en las sumas anteriores, son los elementos en el soporte de a, visto en el grupo $\oplus_{i\in I}A_i$ y donde cada $\rho_i(a) \in A_i$.

Así, como $g(a, c) = \theta \circ e(a, c)$ y $\Psi \circ g(a, c) = e(a, c)$, se tiene que

$$g(a, c) = \theta \circ e(a, c) = \theta \circ (\Psi \circ g(a, c)) = (\theta \circ \Psi) \circ g(a, c),$$

con lo cual, se sigue que θ es un monomorfismo. Por lo tanto

$$\theta : A \otimes C \longrightarrow \oplus_{i\in I}(A_i \otimes C) \text{ es un isomorfismo.}$$

□

Así como el producto tensorial conmuta con las sumas directas, también conmuta con los límites directos, como lo muestra la siguiente

Proposición 11.3.4. *Sean $\{L_i\}_{i\in I}$ un sistema dirigido de A-módulos derechos y M un A-módulo izquierdo. Entonces se tiene el isomorfismo*

$$(\varinjlim L_i) \otimes_A M \cong \varinjlim(L_i \otimes_A M).$$

Demostración. Notemos primero que si $\{L_i, \pi_i^j\}_{i\in I}$ es un sistema dirigido de A-módulos, entonces se tiene el sistema dirigido $\{L_i \otimes M, (\pi_i^j, id_M)\}_{i\in I}$ de grupos abelianos. Además, la conmutatividad de los diagramas de la forma

$$\begin{tikzcd} L_i \arrow[r, "\pi_i^j"] \arrow[d, "\rho_i"'] & L_j \arrow[dl, "\rho_j"] \\ \varinjlim A_k & \end{tikzcd}$$

nos inducen también una familia de homomorfismos $\{(\rho_i, id_M)\}_{i\in I}$ tales que los diagramas

$$\begin{tikzcd} L_i \otimes M \arrow[r, "\pi_i^j{,}id_M"] \arrow[d, "\rho_i{,}id_M"'] & L_j \otimes M \arrow[dl, "\rho_j{,}id_M"] \\ \varinjlim A_k \otimes M & \end{tikzcd}$$

conmutan para toda $i \leq j$.

Por las propiedades del límite directo, se tiene un único morfismo

$$\varphi : \varinjlim(L_i \otimes M) \longrightarrow (\varinjlim L_i) \otimes M,$$

tal que para cualesquier $x_i \in L_i$, $y \in M$ y $\widetilde{x_i \otimes y} \in \varinjlim(L_i \otimes M)$, se tiene que $\varphi(\widetilde{x_i \otimes y}) = \overline{x_i} \otimes y$, donde $\overline{x_i}$ denota la imagen de x_i en $\varinjlim L_i$.

Por otra parte, la función

$$\alpha : (\varinjlim L_i) \times M \longrightarrow \varinjlim(L_i \otimes M)$$

definida por $(\overline{x_i}, y) \longmapsto \widetilde{x_i \otimes y}$ resulta ser bilineal, ya que tanto el producto tensorial como el tomar clases en $\varinjlim(L_i \otimes M)$ distribuyen a la suma. De esta manera, se obtiene la función

$$\xi : (\varinjlim L_i) \otimes M \longrightarrow \varinjlim(L_i \otimes M)$$

tal que $\xi(\overline{x_i} \otimes y) = \widetilde{x_i \otimes y}$. Con esto en cuenta, φ y ξ son funciones inversas, ya que

$$\xi \circ \varphi(\widetilde{x_i \otimes y}) = \xi(\overline{x_i} \otimes y) = \widetilde{x_i \otimes y},$$

así como

$$\varphi \circ \xi(\overline{x_i} \otimes y) = \varphi(\widetilde{x_i \otimes y}) = \overline{x_i} \otimes y,$$

por lo que φ es un isomorfismo. □

Veremos ahora un resultado que nos será de utilidad en la siguiente sección, ya que nos condiciona cuándo un elemento $x \otimes y$ en el producto tensorial $L \otimes_A M$ es cero:

Proposición 11.3.5. *Sean $\{y_i\}_{i\in I}$ una familia de generadores de ${}_AM$ y $\{x_i\}_{i\in I}$ una familia de elementos de L_A tales que $x_i = 0$ para casi toda $i \in I$. Entonces $\Sigma_{i\in I} x_i \otimes y_i = 0$ en $L \otimes_A M$ si y sólo si existen una familia $\{u_j\}_{j\in J}$, con J un conjunto finito de elementos de L y una familia $\{a_{j,i}\}_{j,i\in J\times I}$ de elementos de A tales que:*

1. *$a_{j,i} = 0$ para casi toda $(j, i) \in J \times I$.*
2. *$\Sigma_{i\in I} a_{j,i} y_i = 0$ para cada $j \in J$.*
3. *$x_i = \Sigma_{j\in J} u_j a_{j,i}$ para cada $i \in I$.*

Demostración. $\Longleftarrow$) En caso de cumplirse las tres condiciones, se tiene que

$$\begin{gathered}\Sigma_{i\in I}[x_i \otimes y_i] = \Sigma_{i\in I}[\Sigma_{j\in J}(u_j a_{j,i}) \otimes y_i] \\ = \Sigma_{i\in I, j\in J}[(u_j a_{j,i}) \otimes y_i] = \Sigma_{j\in J}[\Sigma_{i\in I}(u_j \otimes a_{j,i} y_i)] \\ = \Sigma_{j\in J}[u_j \otimes \Sigma_{i\in I} a_{j,i} y_i] = \Sigma_{j\in J} u_j \otimes 0 = 0.\end{gathered}$$

$\Longrightarrow$) Supongamos ahora que $\Sigma_{i\in I} x_i \otimes y_i = 0$ en $L \otimes M$. Observemos que al ser $\{y_i\}_{i\in I}$ una familia de generadores del módulo ${}_AM$, entonces para el grupo libre abeliano $A^{(I)}$, con conjunto base $\{e_i\}_{i\in I}$, se tiene la función $\beta : A^{(I)} \longrightarrow_A M$ con regla de correspondencia $e_i \longmapsto y_i$. Nótese que en realidad β es un morfismo suprayectivo, y que en caso de ser $\{y_i\}_{i\in I}$ una base para ${}_AM$, β es un isomorfismo. De esta manera, si $K = Ker\beta$ y $\iota : K \hookrightarrow A^{(I)}$ es el morfismo inclusión, se obtiene la siguiente sucesión exacta corta

$$0 \hookrightarrow K \overset{\iota}{\hookrightarrow} A^{(I)} \xrightarrow{\beta} M \longrightarrow 0.$$

Si ahora tensamos a la sucesión exacta por L_A, obtenemos la sucesión exacta corta

$$L \otimes K \xrightarrow{Id_L \otimes \iota} L \otimes A^{(I)} \xrightarrow{Id_L \otimes \beta} L \otimes M \longrightarrow 0.$$

Como

$$0 = \Sigma_{i\in I} x_i \otimes y_i = \Sigma_{i\in I} Id_L(x_i) \otimes \beta(e_i) = Id_L \otimes \beta(\Sigma_{i\in I}(x_i \otimes e_i)),$$

entonces

$$\Sigma_{i\in I}(x_i \otimes e_i) \in Ker(Id_L \otimes \beta) = Im(Id_L \otimes \iota),$$

por lo que existe un elemento $\Sigma_{j\in J}(u_j \otimes z_j)$, en $L \otimes K$, con $u_j \in L$ y $z_j \in K$, $\forall j \in J$, tal que $\Sigma_{i\in I}(x_i \otimes e_i) = \Sigma_{j\in J}(u_j \otimes \iota(z_j))$.

Por otro lado, notemos que como cada $\iota(z_j) \in K \subset A^{(I)}$ entonces éste se expresa como combinación de la base $\{e_i\}_{i\in I}$, es decir, $\iota(z_j) = \Sigma_{i\in I} a_{j,i} e_i$, para cada $j \in J$. Así, como $\beta \circ \iota = 0$, entonces

$$0 = \beta \circ \iota(z_j) = \beta(\Sigma_{i\in I} a_{j,i} e_i) = \Sigma_{i\in I} a_{j,i} \beta(e_i) = \Sigma_{i\in I} a_{j,i} y_i$$

para cada $j \in J$, cumpliéndose la segunda propiedad.

Por otra parte,

$$\begin{gathered} \Sigma_{i\in I} x_i \otimes e_i = \Sigma_{j\in J}(u_j \otimes \iota(z_j)) \\ = \Sigma_{j\in J}(u_j \otimes (\Sigma_{i\in I} a_{j,i} e_i)) = \Sigma_{j\in J}[\Sigma_{i\in I}(u_j \otimes a_{j,i} e_i)] \\ = \Sigma_{i\in I, j\in J}(u_j a_{j,i} \otimes e_i) \in L \otimes A^{(I)}. \end{gathered}$$

Como se tiene el isomorfismo $L \otimes A^{(I)} \cong L^{(I)}$ y

$$\Sigma_{i\in I} x_i \otimes e_i = \Sigma_{i\in I}[\Sigma_{,j\in J}(u_j a_{j,i})] \otimes e_i,$$

entonces $\Sigma_{i\in I} x_i = \Sigma_{i\in I}[\Sigma_{j\in J} u_j a_{j,i}]$ en $L^{(I)}$. De esta manera, para cada $i \in I$, $x_i = \Sigma_{j\in J} u_j a_{j,i}$, puesto que éstas son las imágenes de $\rho_i : A^{(I)} \longrightarrow A_i$, cumpliéndose así la tercera condición. $\square$

Ejemplo. *Sea $\mathcal{A}$ un ideal derecho del anillo A y M un A-módulo izquierdo. De la sucesión exacta corta*

$$0 \hookrightarrow \mathcal{A} \xrightarrow{\iota} A \xrightarrow{\rho} A/\mathcal{A} \longrightarrow 0,$$

al tensar por M obtenemos la sucesión exacta corta

$$\mathcal{A} \otimes M \stackrel{\iota\otimes Id_M}{\longrightarrow} A \otimes M \stackrel{\rho\otimes Id_M}{\longrightarrow} (A/\mathcal{A}) \otimes M \longrightarrow 0.$$

Ahora, el segundo miembro de la sucesión, de izquierda a derecha, es isomorfo a M, por lo que se tiene la sucesión exacta corta

$$\mathcal{A} \otimes M \stackrel{alpha}{\longrightarrow} M \longrightarrow (A/\mathcal{A}) \otimes M \longrightarrow 0$$

donde

$$Im\alpha = \{\Sigma_{i\in I} a_i x_i \mid a_i \in \mathcal{A}, x_i \in M \, con \, x_i = 0 \ para\ casi\ toda\ i \in I\} = \mathcal{A}M.$$

Por la exactitud de la sucesión, se sigue que $(A/\mathcal{A}) \otimes M \cong M/\mathcal{A}M$.

Para finalizar esta sección, veremos el isomorfismo en la categoría de grupo abelianos, que hace del funtor tensar y el funtor Hom ser adjuntos izquierdo y derecho, respectivamente.

Proposición 11.3.6. *Para cualesquiera tres grupos abelianos A,B,C, se tiene un isomorfismo*

$$\gamma : Hom(A \otimes B, C) \longrightarrow Hom(A, Hom(B, C))$$

definido de la siguiente manera: a cada $\eta \in Hom(A \otimes B, C)$, se le asigna la función

$$\gamma : A \longrightarrow Hom(B, C)$$

tal que $[\gamma(\eta)(a)](b) = \eta(a \otimes b)$.

Demostración. Notemos primero que la función $\gamma(\eta)$, evaluada en el elemento $a \in A$, tiene como dominio el grupo B y como codominio el grupo C, por lo que $\gamma(\eta)$ asocia a cada elemento $a \in A$, una función de B en C, de tal manera que manda $b \longmapsto \eta(a \otimes b)$. Ahora, como cada η es un morfismo y el producto tensorial distribuye a la suma del grupo, se tiene que

$$\gamma(\eta)(a + a') = \gamma(\eta)(a) + \gamma(\eta)(a'),$$

mostrando así que $\gamma(\eta)$ es un morfismo, para cada $\eta \in Hom(A \otimes B, C)$. Más aún, la función γ es un morfismo. En efecto, si $\eta_1, \eta_2 \in Hom(A \otimes B, C)$, entonces $\gamma(\eta_1 + \eta_2)$ es el morfismo tal que en cualquier $a \in A$ y cualquier $b \in B$ se cumple que

$$\begin{aligned}[\gamma(\eta_1 + \eta_2)(a)](b) &= (\eta_1 + \eta_2)(a \otimes b) = \eta_1(a \otimes b) + \eta_2(a \otimes b) = (\eta_1 + \eta_2)(a \otimes b) \\ &= \eta_1(a \otimes b) + \eta_2(a \otimes b) = [\gamma(\eta_1)(a)](b) + [\gamma(\eta_2)(a)](b).\end{aligned}$$

Veamos ahora que γ tiene una función inversa. Para esto, si

$$\zeta : A \longrightarrow Hom(B, C)$$

es un morfismo, se tiene de manera natural la función $\omega_\zeta : A \times B \longrightarrow C$ definida por $\omega_\zeta(a, b) = [\zeta(a)](b)$. Como ζ es un morfismo, ω_ζ también lo es. Así, por las propiedades del producto tensorial, existe un único morfismo $\xi_\zeta : A \otimes B \longrightarrow C$ tal que

$$\xi_\zeta(a \otimes b) = \omega_\zeta(a, b) = [\zeta(a)](b).$$

Con esto en cuenta, definimos la función

$$\chi : Hom(A, Hom(B, C)) \longrightarrow Hom(A \otimes B, C)$$

con regla de correspondencia $\zeta \longmapsto \xi_\zeta$, donde $\xi_\zeta(a \otimes b) = [\zeta(a)](b)$. Por la unicidad en la existencia de ξ_ζ, se sigue que χ está bien definida. Así mismo, χ es un morfismo ya que $\xi_{\zeta_1} + \xi_{\zeta_2} = \xi_{\zeta_1+\zeta_2}$, donde

$$\zeta_1 + \zeta_2 : A \longrightarrow Hom(B, C)$$

es tal que $(\zeta_1 + \zeta_2)(a) = (\zeta_1(a) + \zeta_2(a)) : B \longrightarrow C$.

Observemos que χ y γ son inversas. Por un lado si $\zeta : A \longrightarrow Hom(B, C)$, entonces $\gamma \circ \chi(\zeta) = \gamma(\xi_\zeta) : A \longrightarrow Hom(B, C)$ es tal que, para cualquier $a \in A$ y $b \in B$,

$$[\gamma(\xi_\zeta)(a)](b) = \xi_\zeta(a \otimes b) = [\zeta(a)](b),$$

es decir, $\gamma(\xi_\zeta) = \zeta$, por lo que $\gamma \circ \chi = id_{Hom(A,Hom(B,C))}$. Por otra parte, si $\eta \in Hom(A \otimes B, C)$, entonces $\gamma(\eta) : A \longrightarrow Hom(B, C)$, con la cual se obtiene la una función $\omega_{\gamma(\eta)}$. Como

$$\omega_{\gamma(\eta)}(a, b) = [\gamma(\eta)(a)](b) = \eta(a \otimes b),$$

se sigue que η hace conmutativo el diagrama

$$\begin{tikzcd} A \times B \arrow[r, "e"] \arrow[d, "\omega_{\gamma(\eta)}"'] & A \otimes B \arrow[dl, "\eta"] \\ C & \end{tikzcd},$$

con lo cual $\xi_{\gamma(\eta)} = \eta$. De esta manera,

$$(\chi \circ \gamma)(\eta) = \chi(\gamma(\eta)) = \xi_{\gamma(\eta)} = \eta,$$

teniendo así que γ y χ son funciones inversas. $\square$

La Proposición 11.3.6 se puede extender para las categorías Mod_R, de R-módulos derechos y ${}_SMod$, de S-módulos izquierdos.

Si ${}_SM_R$ es un bimódulo, definimos el funtor

$$Hom :_S Mod \longrightarrow Mod_R$$

por ${}_SN \longmapsto Hom_{Mod_R}({}_SN, {}_SM_R)$. Observemos que $Hom_{Mod_R}({}_SN, {}_SM_R)$ es un R-módulo derecho. En efecto, para cualquier $f \in Hom_{Mod_R}({}_SN, {}_SM_R)$ y $a \in R$, definimos la operación

$$(f \cdot a)(x) := f(x)a.$$

Se sigue que, bajo esta operación, $Hom_{Mod_R}({}_SN, {}_SM_R)$ es un R-módulo derecho.

Por otra parte, se tiene el funtor

$${}_SM_R \otimes - : Mod_R \longrightarrow {}_S Mod$$

con regla de correspondencia

$$N_R \longmapsto ({}_SM_R) \otimes N_R.$$

En [1], pp. 342, se encuentra la demostración de que los funtores Hom y ${}_SM_R \otimes -$ son funtores adjuntos derechos e izquierdos, respectivamente.

Capítulo 12

Multiplicaciones en un Grupo

12.1. Definición

Sea R un anillo, con grupo aditivo A. Entonces el producto en el anillo es una función bilineal de $A \times A \longrightarrow A$. Con esto en cuenta, surge de manera natural la siguiente

Definición 12.1.1. *Una multiplicación en un grupo A es una función $\mu : A \times A \longrightarrow A$ tal que, $\forall a, b, c \in A$ se satisfacen las siguientes condiciones:*

1. $\mu(a, b + c) = \mu(a, b) + \mu(a, c)$.
2. $\mu(a + b, c) = \mu(a, c) + \mu(b, c)$.

Observación. *Nótese que una multiplicación es una función bilineal de $A \times A$ en A. Así, si μ es una multiplicación, se cumple que*

$$\mu(na, b) = n(\mu(a, b)) = \mu(a, nb),$$

para cualquier $a, b \in A$ y $n \in \mathbb{Z}$.

La manera de acercarnos a la pregunta de cúando un grupo es la parte aditiva de un anillo, será considerando el conjunto de multiplicaciones en el grupo A, ya que, como se verá a continuación, todo producto en un anillo R es en realidad una multiplicación en el grupo aditivo asociado al anillo. En general, consideraremos anillos R cuya función producto no sea necesariamente conmutativa o asociativa. Las propiedades atribuidas al anillo R son aquellas que satisface su grupo abeliano asociado, es decir, un anillo es de torsión, libre de torsión, p-anillo, divisible, etc. si su grupo aditivo lo es.

Diremos que R es un anillo sobre el grupo A, si $R^+ \cong A$. Observemos que a cualquier grupo A, le podemos asignar una estructura de anillo definiendo el producto constante igual a cero para cualquier par de elementos. A este anillo se le conoce como el *anillo cero*.

Ahora, como todo anillo R tiene asociado un grupo abeliano A y una función producto, la cual distribuye a la operación suma asociada al grupo, si A es el grupo aditivo del anillo R, el producto μ en el anillo es una multiplicación en A, cuya regla de correspondencia es $\mu(a,b) = ab$. De manera conversa, si A es un grupo y μ es una multiplicación, entonces la pareja (μ, A) forma un anillo. Esto muestra que la correspondencia entre anillos sobre un grupo A y multiplicaciones en A es biyectiva, con lo cual podemos identificar a R con (A, μ).

Definición 12.1.2. *Sea A un grupo. El conjunto $MultA$ está formado por todas las multiplicaciones en A. En otras palabras,*

$$MultA = \{\mu : A \times A \longrightarrow A \mid \mu \textit{ es una función bilineal } \}$$

Ahora, si μ y ν son dos multiplicaciones en A, podemos definir una operación aditiva en el conjunto $MultA$, de todas las multiplicaciones en A, de la siguiente manera:

$$[\mu + \nu](a,b) = \mu(a,b) + \nu(a,b).$$

Con esto en cuenta, el conjunto $MultA$ es un grupo abeliano con la operación suma antes definida, donde el neutro aditivo es la multiplicación constantes 0, es decir, el anillo cero.

Teorema 12.1.3. *Para un grupo A, se tienen los siguientes isomorfismos:*

(i) $MultA \cong Hom(A \otimes A, A)$.

(ii) $MultA \cong Hom(A, EndA)$.

Demostración. (i) Como cada elemento $\mu \in MultA$ es una función bilineal de $A \times A \longrightarrow A$, se tiene una única función $\varphi_\mu : A \otimes A \longrightarrow A$ tal que $\mu(a,b) = \varphi_\mu(a \otimes b)$. Además, como $MultA$ es un grupo abeliano,

$$[\mu + \nu](a,b) = \mu(a,b) + \nu(a,b),$$

por lo que a la función bilineal $[\mu + \nu]$ le corresponde la función

$$\varphi_\mu + \varphi_\nu : A \otimes A \longrightarrow A$$

tal que

$$[\mu + \nu](a, b) = (\varphi_\mu + \varphi_\nu)(a \otimes b).$$

Con esto en cuenta, se tiene el morfismo

$$\xi : MultA \longrightarrow Hom(A \otimes A, A),$$

con regla de correspondencia $\mu \longmapsto \varphi_\mu$. Notemos que, por la unicidad antes mencionada, ξ es un monomorfismo. Más aún, ξ también es un epimorfismo. En efecto, si $\varphi \in Hom(A \otimes A, A)$, entonces éste induce una función bilineal $\eta_\varphi : A \times A \longrightarrow A$, definida por $\eta_\varphi(a, b) = \varphi(a \otimes b)$, ya que

$$a \otimes (b_1 + b_2) = a \otimes b_1 + a \otimes b_2,$$

así como

$$(a_1 + a_2 \otimes)b = a_1 \otimes b + a_2 \otimes b.$$

Por lo tanto, ξ es un isomorfismo entre $MultA$ y $Hom(A \otimes A, A)$.

(ii) Este isomorfismo se sigue del hecho de que el funtor tensar y el funtor Hom son adjuntos derechos e izquierdos, respectivamente, por lo que

$$Hom(A, EndA) \cong Hom(A \otimes A, A) \cong MultA.$$

□

12.2. Propiedades y ejemplos

Ejemplo. *Sean $F = \oplus_\alpha \mathbb{Z}^+$, para cualquier cardinal α y $\{a_i \mid i \in I\}$ una base para F. Como*

$$MultF \cong Hom(F \otimes F, F),$$

cualquier $\varphi \in Hom(F \otimes F, F)$ define una multiplicación que hace de F un anillo. Al ser $F \otimes F$ un grupo libre abeliano, con base el conjunto de elementos $\{a_i \otimes a_j \mid i, j \in I\}$, toda función de $F \otimes F$ a F queda determinada por los valores que toma en cada básico $a_i \otimes a_j$. Más aún, al definir el valor de la función en cada $a_i \otimes a_j$, podemos extenderlo de manera lineal a cualquier elemento en $F \otimes F$, obteniendo así un homomorfismo de $F \otimes F$ a F. Esto quiere decir que en cualquier anillo R, cuyo grupo aditivo sea F, la multiplicación del anillo se obtiene al determinar los valores $a_i \cdot a_j$, para $i, j \in I$, y después extenderlo de manera lineal.

Ejemplo. *Sean $G = \oplus_\alpha \mathbb{Q}^+$, con α cualquier cardinal y $\{a_i \mid i \in I\}$ una base para G, visto como espacio vectorial sobre $\mathbb{Q}$. Así, el conjunto*

$$\{a_i \otimes a_j \mid i, j \in I\}$$

es una base para $G \otimes G$. El mismo argumento del ejemplo anterior aplica en este, con la observación de que $G \otimes G$ es un objeto libre en la categoría de espacios vectoriales sobre $\mathbb{Q}$, mientras que $F \otimes F$ es libre en la categoría de de grupos abelianos. Por lo tanto, cualquier producto en un anillo R, con grupo aditivo G, se obtiene al definir los valores en los productos de elementos básicos de la forma $a_i \cdot a_j$, para $i, j \in I$, y después extenderlo de manera lineal a todo G.

Por el Teorema 12.1.3, podemos ver que el grupo de los enteros tiene una cantidad numerable de anillos R tales que $R^+ = \mathbb{Z}$:

Ejemplo. *Como $\mathbb{Z} \otimes \mathbb{Z} \cong \mathbb{Z}$, entonces*

$$Mult\mathbb{Z} \cong Hom(\mathbb{Z} \otimes \mathbb{Z}, \mathbb{Z}) \cong Hom(\mathbb{Z}, \mathbb{Z}) \cong \mathbb{Z}.$$

Afirmamos que cada multiplicación en $\mathbb{Z}$ es de la forma

$$\eta_n : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z},$$

donde $\eta_n(a, b) = n^2 ab$. La función η_n es una función bilineal. En efecto; por una parte

$$\eta_n(a_1 + a_2, b) = n^2(a_1 + a_2)b = n^2 a_1 b + n^2 a_2 b;$$

por otra parte

$$\eta_n(a_1, b) + \eta_n(a_2, b) = n^2 a_1 b + n^2 a_2 b.$$

Análogamente se demuestra que $\eta_n(a, b_1 + b_2) = \eta_n(a, b_1) + \eta_n(a, b_2)$. De esta manera, el conjunto $\{\eta_n\}_{n \in \mathbb{N}}$ son todas las multiplicaciones sobre el grupo $\mathbb{Z}$. Observemos que cuando $n = 1$, la multiplicación η_1 corresponde a la multiplicación convencional en el anillo de los enteros. Además, las multiplicaciones η_n y η_m definen anillos isomorfos sobre $\mathbb{Z}$ exactamente cuando $n = \pm m$.

Observación. *Si A y C son grupos tales que $C[n] = \{0\}$, para alguna $n \in \mathbb{N}$, entonces $Hom(A, C)[n] = \{0\}$, donde este último elemento es considerado como la función constante cero. En efecto, supongamos que $\alpha \in Hom(A, C)$ y $n\alpha \equiv 0$. Para cualquier $a \in A$, se tiene que*

$$n(\alpha(a)) = (n\alpha)(a) = 0.$$

Como $\alpha(a) \in C$ *y* $C[n] = \{0\}$, *entonces* $\alpha(a) = 0$, *lo cual implica que* $\alpha \equiv 0$.

Observación. *Por la observación anterior, si* C *es un grupo libre de torsión, se tiene que* $C[n] = \{0\}$, $\forall n \in \mathbb{N}$, *por lo que también se cumple que* $Hom(A, C)[n] = \{0\}$ *para toda* $n \in \mathbb{N}$. *Esto quiere decir que* $Hom(A, C)$ *es un grupo libre de torsión.*

Observación. *Si* A *y* C *son grupos, con* C *divisible, entonces* $Hom(A, C)$ *es divisible. Sea* $\alpha \in Hom(A, C)$ *y* n *cualquier natural. Dado un elemento* $a \in A$, *por la divisibilidad de* C, *existe un único* $c \in C$ *que satisface la ecuación* $\alpha(a) = nx$. *Con esto en cuenta, podemos definir la función* $\beta : A \longrightarrow C$ *por* $a \longmapsto c$. *Veamos que* β *es un morfismo de grupos. Nótese que, si* $a_1 \longmapsto c_1$ *y* $a_2 \longmapsto c_2$, *entonces* $\alpha(a_1) = nc_1$ *y* $\alpha(a_2) = nc_2$. *Esto implica que*

$$n(c_1 + c_2) = \alpha(a_1 + a_2) = \alpha(a_1) + \alpha(a_2),$$

es decir, $a_1 + a_2 \longmapsto c_1 + c_2$. *Además, para cualquier* $a \in A$, *se tiene que*

$$[n\beta](a) = n(\beta(a)) = nc = \alpha(a),$$

por lo que $n\beta = \alpha$, *lo cual muestra que* $Hom(A, C)$ *es un grupo divisible.*

Observación. *Si* A *es un grupo tal que* $nA = A$, *para alguna* $n \in \mathbb{N}$, *entonces* $Hom(A, C)[n] = \{0\}$. *En efecto, sea* $\alpha \in Hom(A, C)$ *tal que* $n\alpha \equiv 0$. *Ahora, para cualquier* $a \in A$, *existe* $b \in A$ *tal que* $a = nb$, *por lo que*

$$\alpha(a) = \alpha(nb) = n\alpha(b) = 0.$$

Como este argumento fue para cualquier $a \in A$, *se sigue que* $\alpha \equiv 0$.

Proposición 12.2.1. *Si* A *y* C *son grupos tales que alguno de ellos es* p*-divisibles, entonces* $A \otimes C$ *es* p*-divisible.*

Demostración. Sea $a \otimes c \in A \otimes C$. Sin pérdida de generalidad, supongamos que A es p-divisible, es decir, $pA = A$. De esta manera, para $a \in A$, existe $a_0 \in A$ tal que $pa_0 = a$. Por las propiedades del producto tensorial, se tiene que $p(a_0 \otimes c) = (pa_0 \otimes c) = a \otimes c$. □

Como consecuencia directa de esta proposición, si alguno de los grupos A o C es divisible, entonces el producto tensorial $A \otimes C$ es divisible.

Obsérvese ahora que si A es p-divisible, entonces $A \otimes A$ es p-divisible, es decir, $p(A \otimes A) = A \otimes A$. De esta manera, $Hom(A \otimes A, A)[p] = \{0\}$, lo cual implica que $MultA$ no tiene elementos de orden p. Además, si A es libre de torsión, entonces $A[n] = \{0\}$, $\forall n \in \mathbb{N}$, por lo que

$$Hom(A \otimes A, A)[n] = \{0\}$$

para cualquier natural n, es decir, $MultA$ es libre de torsión. Notemos también que por el mismo argumento, si A es divisible, entonces $Hom(A \otimes A, A)$ lo es también, teniendo así que $MultA$ es divisible. Esto demuestra la siguiente

Proposición 12.2.2. *Si A es un grupo libre de torsión y divisible entonces $MultA$ también lo es.*

Teorema 12.2.3. *Sean $\{A_i\}_{i \in I}$ una familia de grupos y C un grupo. Entonces*

$$Hom(\oplus_{i \in I} A_i, C) \cong \Pi_{i \in I} Hom(A_i, C).$$

Demostración. Si $\alpha \in Hom(\oplus_{i \in I} A_i, C)$, entonces $\alpha : \oplus_{i \in I} A_i \longrightarrow C$, por lo que si restringimos α a A_i, se obtiene el morfismo $\alpha_i = \alpha \mid_{A_i} : A_i \longrightarrow C$. Con esto en cuenta, podemos descomponer a α en las funciones componentes $\{\alpha_i\}_{i \in I}$ y expresarlo de la forma $(\cdots, \alpha_i, \cdots)$. Como

$$(\alpha + \beta) \mid_{A_i} = \alpha_i + \beta_i,$$

la correspondencia Ψ, definida por $\alpha \longmapsto (\cdots, \alpha_i, \cdots)$ es un morfismo entre $Hom(\oplus_{i \in I} A_i, C)$ y $\Pi_{i \in I} Hom(A_i, C)$. Además, si $\alpha \longmapsto (0, \cdots, 0, \cdots)$, entonces $\alpha \mid_{A_i} = 0$, $\forall i \in I$, por lo que $\alpha \equiv 0$, es decir, Ψ es inyectiva.

Por otra parte, cualquier conjunto $\{\alpha_i\}_{i \in I}$, con $\alpha_i \in Hom(A_i, C)$, define un morfismo $\alpha : \oplus_{i \in I} A_i \longrightarrow C$ que satisface $\alpha \mid_{A_i} = \alpha_i$, mostrando así que Ψ es sobre. Por lo tanto,

$$\Psi : Hom(\oplus_{i \in I} A_i, C) \longrightarrow \Pi_{i \in I} Hom(A_i, C)$$

es un isomorfismo. $\square$

Supongamos ahora que $A = \oplus_{i \in I} A_i$, con cada A_i un subgrupo totalmente invariante de A. Afirmamos que

$$MultA \cong \Pi_{i\in I} MultA_i.$$

Por el Teorema 12,1,2., $MultA \cong Hom(A \otimes A, A)$. Como $A = \oplus_{i\in I} A_i$, entonces $A \otimes A = \oplus_{i,j\in I}(A_i \otimes A_j)$. Además, por el teorema anterior,

$$Hom(\oplus_{i\in J} A_i, C) \cong \Pi_{i\in J} Hom(A_i, C),$$

de donde se sigue que

$$Hom(A \otimes A, A) \cong Hom(\oplus_{i,j\in I}(A_i \otimes A_j), A) \cong \Pi_{i,j\in I} Hom(A_i \otimes A_j, A).$$

Ahora, si $a_j \in A_j$ es un elemento fijo, para la función $\varphi \in Hom(A_i \otimes A_j, A)$, con $i \in I$, se tiene la función $\psi_i : A_i \longrightarrow A$ con regla de correspondencia $a_i \longmapsto \varphi(a_i \otimes a_j)$, la cual resulta ser también un morfismo. Como A_i es un subgrupo totalmente invariante de A, la función $\psi_i \circ \rho_i$ deja fijo a A_i, lo cual implica que $\psi_i(A_i) = A_i$. De manera análoga, si ahora $a_i \in A_i$ es un elemento fijo, la función ψ_j que manda $a_j \longmapsto \varphi(a_i \otimes a_j)$ es un morfismo de A_j en A, que también deja fijo a A_j. Al ser A la suma directa de los subgrupos $\{A_i\}_{i\in I}$, se cumple que $A_i \cap A_j = \{0\}$, para $i \neq j$. Por lo tanto, si $i \neq j$, cualquier morfismo $\varphi \in Hom(A_i \otimes A_j, A)$ se anula en $a_i \otimes a_j$, pues por una parte $\varphi(a_i \otimes a_j) \in A_i$ y por otra parte $\varphi(a_i \otimes a_j) \in A_j$. En cambio, φ no se anula cuando $i = j$. De esta manera, se tiene que

$$\Pi_{i,j\in I} Hom(A_i \otimes A_j, A) = \Pi_{i\in I} Hom(A_i \otimes A_i, A),$$

mostrando así que

$$\Pi_{i\in I} MultA_i \cong \Pi_{i\in I} Hom(A_i \otimes A_i, A) \cong \Pi_{i\in I} MultA_i$$

Como consecuencia de esto último, si A es un grupo de torsión y A_p sus p-componentes, al ser éstas totalmente invariantes, se sigue que

$$MultA \cong \Pi_p MultA_p.$$

Ejemplo. *Sea $A = J_p = C$. Si $\pi \in J_p$ es cualquier elemento, la función $\eta_\pi : J_p \longrightarrow J_p$, definida por $\eta_\pi(x) = \pi x$ es un morfismo, teniendo así que cada $\pi \in J_p$ define el elemento $\eta_\pi \in End(J_p)$. Además, notemos que si $\pi_1 \neq \pi_2$ entonces $\eta_{\pi_1} \neq \eta_{\pi_2}$, ya que $\eta_{\pi_1}(1) = \pi_1 \neq \eta_{\pi_2}(1)$. Con esto en cuenta, se tiene el monomorfismo de grupos $J_p \longrightarrow End(J_p)$, cuya regla de correspondencia es $\pi \longmapsto \eta_\pi$. Por otra parte, observemos que si $\xi \in End(J_p)$ es tal que $\xi(1) = \pi$, entonces $\xi = \eta_\pi$. En efecto, como $\eta_\pi(1) = \pi = \xi(1)$, entonces $(\xi - \eta_\pi)(1) = 0$, por lo que $(\xi - \eta_\pi)(n) = 0$, $\forall n \in \mathbb{Z} \subset J_p$, es decir, $\mathbb{Z} \subset Ker(\xi - \eta_\pi)$. Como $J_p/\mathbb{Z}$ es un grupo divisible y la función $J_p/\mathbb{Z} \longrightarrow J_p/Ker(\xi - \eta_\pi)$ es sobre, entonces el grupo $J_p/Ker(\xi - \eta_\pi)$ es también un grupo divisible.*

Ahora, que $J_p/Ker(\xi - \eta_\pi)$ sea un grupo divisible quiere decir que

$$n(J_p/Ker(\xi - \eta_\pi)) = J_p/Ker(\xi - \eta_\pi),$$

para toda $n \in \mathbb{Z}$. *Así,*

$$J_p/Ker(\xi - \eta_\pi) = n(J_p/Ker(\xi - \eta_\pi)) = [nJ_p + Ker(\xi - \eta_\pi)]/Ker(\xi - \eta_\pi).$$

Esto último implica que $J_p = nJ_p + Ker(\xi - \eta_\pi)$, *por lo que*

$$(\xi - \eta_\pi)(J_p) = (\xi - \eta_\pi)[nJ_p + Ker(\xi - \eta_\pi)] = (\xi - \eta_\pi)(nJ_p).$$

Como para cualquier $n \in \mathbb{Z}$, *se cumple que*

$$(\xi - \eta_\pi)(nJ_p) = n(\xi - \eta_\pi)(J_p),$$

entonces el subgrupo $(\xi - \eta_\pi)(J_p)$ *de* J_p *es divisible. Al ser* J_p *un grupo reducido, se tiene que* $(\xi - \eta_\pi)(J_p) = 0$, *lo cual implica que* $\xi = \eta_\pi$.

De esta manera, cualquier $\xi \in End(J_p)$ *es de la forma* $\xi = \eta_\pi$, *para algún* $\pi \in J_p$, *con lo cual* $J_p \cong End(J_p)$. *Por lo tanto*

$$Mult(J_p) \cong Hom(J_p, End(J_p)) \cong Hom(J_p, J_p) \cong End(J_p) \cong J_p.$$

Observación. *Sean* ${}_p\mathbb{Q}^*$ *y su grupo aditivo* J_p. *Recordemos que la completación topológica del anillo* ${}_p\mathbb{Q}$ *se hizo con la topología determinada por el sistema fundamental de vecindades* $\{p^k({}_p\mathbb{Q}) \mid k \in \mathbb{N}\}$ *del cero. Además, el conjunto* $\{p^k({}_p\mathbb{Q}) \mid k \in \mathbb{N}\}$ *son todos los ideales del anillo* ${}_p\mathbb{Q}^*$. *Más aún, los ideales* $\{p^k({}_p\mathbb{Q})^* \mid k \in \mathbb{N}\}$ *posen una estructura de anillo, heredada por* ${}_p\mathbb{Q}^*$.

Ahora, como cada elemento $\mu \in J_p$ *está en el ideal generado por el mismo, la observación anterior implica que* $\mu \in p^n J_p$, *para algún* $n \in \mathbb{N}$. *Por el Principio del Buen Orden, podemos escoger al menor natural* n, *para el cual* $\mu \in p^n J_p$.

Por otra parte, por el ejemplo anterior, cada elemento $\mu \in J_p$ *define una multiplicación en* J_p. *Con esto en cuenta, al definir la relación en* J_p *por* $\mu \sim \eta$ *si y sólo si* $\mu, \eta \in p^n J_p$, *se tiene que* $\sim$ *es una relación de equivalencia. Esto muestra que los anillos, no isomorfos, sobre* J_p *son de la forma* $p^k({}_p\mathbb{Q})^*$, *con* $k \in \mathbb{N}$. *Nótese que* J_p *tiene una cantidad numerable de anillos* R, *no isomorfos, tales que* $R^+ = J_p$.

Definición 12.2.4. *Un grupo* A *es nil asociativo si el único anillo sobre* A *es el anillo cero. Un grupo* A *es cuasi nil asociativo si existen únicamente una cantidad finita de anillos* R, *no isomorfos, tales que* $R^+ = A$.

Observación. *Un grupo* A *es nil asociativo si y sólo si* $MultA = \{0\}$.

El siguiente resultado caracteriza a los grupos de torsión que son nil asociativos:

Teorema 12.2.5. *Un grupo de torsión A es nil asociativo si y sólo si es divisible.*

Demostración. $\Longleftarrow$) Supongamos que A es un grupo divisible y de torsión. Veamos que $A \otimes A = \{0\}$. Sean $a, b \in A$, con $o(a) = n$. Por ser A un grupo divisible, existe $c \in A$ solución de la ecuación $nx = b$. Así, $nc = b$, con lo que

$$a \otimes b = a \otimes nc = na \otimes c = 0 \otimes c = 0,$$

es decir, todo elemento $a \otimes b$ en $A \otimes A$ es cero. Esto implica que $A \otimes A = \{0\}$. Como $Mult(A) = Hom(A \otimes A, A)$ y $A \otimes A = \{0\}$, se sigue que $MultA = \{0\}$.

$\Longrightarrow$) Supongamos que A es un grupo de torsión nil asociativo. Observemos que, por ser A un grupo nil asociativo y de torsión, cualquier sumando directo de A también es nil asociativo y de torsión. Además, como A es un grupo de torsión, entonces A contiene un subgrupo cocíclico como sumando directo. Nótese que éste no puede ser de la forma $\mathbb{Z}(p^k)$, para k finito, ya que éstos no son nil asociativos. De esta manera, cualquier sumando cocíclico de A es de la forma $\mathbb{Z}(p^\infty)$, con p un primo. Con esto en cuenta, al grupo de torsión A lo podemos escribir como $A = D \oplus E$, donde D es el subgrupo máximo divisible de A y E es un grupo reducido, en el sentido de no contener ningún grupo divisible distinto a $\{0\}$.

Por otra parte, como E es un subgrupo de A, también es de torsión, por lo que E se descompone en sus p-componentes. De manera análoga, E tiene un subgrupo cocíclico como sumando directo. Nótese que si el sumando directo de E es de la forma $\mathbb{Z}(p^\infty)$, se contradice que E es un grupo reducido; si el sumando directo de E es de la forma $\mathbb{Z}(p^k)$, con k finito, se tiene que $\mathbb{Z}(p^k)$ es también sumando directo de A, contradiciendo la observación inicial. Por lo tanto, $E = \{0\}$, teniendo así que A es divisible.

Del teorema anterior podemos concluir la siguiente

Proposición 12.2.6. *Sea A un grupo abeliano. Las siguientes condiciones son equivalentes:*

(i) $A \otimes A = \{0\}$.

(ii) A es un grupo divisible y de torsión.

Demostración. $(i) \Longrightarrow (ii)$ Supongamos que $A \otimes A = \{0\}$, con $A \neq \{0\}$. Consideremos al grupo abeliano A como un $\mathbb{Z}$-módulo. Si $a \in A$ fuera un elemento tal que $o(a) = \infty$, entonces $< a > \cong \mathbb{Z}$, por lo que

$$A \cong \mathbb{Z} \otimes A \cong < a > \otimes A \hookrightarrow A \otimes A.$$

Como $A \otimes A = \{0\}$, se sigue que $A = \{0\}$, contradiciendo que $A \neq \{0\}$. Por lo tanto, A es un grupo de torsión.

Como A es un grupo de torsión, éste se descompone en $A = \oplus_p A_p$, donde cada A_p es la p-componente. Como $A \otimes A = \{0\}$, entonces $A_p \otimes A_p = \{0\}$, para cualquier primo p. Obsérvese que A_p es q-divisible, para todo primo $q \neq p$. Por lo tanto, para demostrar que A es divisible, basta ver que cada p-componente A_p es p-divisible. Si $pA_p \subsetneq A_p$, entonces $A_p/pA_p \neq \{0\}$. Además, podemos escoger $a \in A_p \setminus pA_p$ tal que $o(a) = p$, llegando así a

$$A_p/pA_p \cong \mathbb{Z}/p\mathbb{Z} \otimes A_p \cong \mathbb{Z}_p \otimes A_p \cong < a > \otimes A_p \hookrightarrow A_p \otimes A_p = \{0\},$$

lo cual es una contradicción. Por lo tanto, A_p es p-divisible, con lo cual A también lo es.

$(ii) \Longrightarrow (i)$ Se sigue del teorema anterior.

Los resultados anteriores muestran que cualquier grupo divisible y de torsión no puede ser la parte aditiva de un anillo. Así, si $\mathcal{P}$ es el conjunto de todos los primos, entonces los grupos de la forma

$$\oplus_{p \in \mathcal{P}} (\oplus_{i \in I} (\mathbb{Z}(p^\infty)_i)$$

no admiten una multiplicación que les de una estructura de anillo.

Por otra parte, en [2], se desarrollan los casos para los grupos que son la suma directa de un grupo divisible (como $\mathbb{Z}(p^\infty)$) y uno de torsión. También se analizan los casos cuando el grupo es libre de torsión, como por ejemplo, los subgrupos de $\mathbb{Q}$.

Bibliografía

[1] Dauns, J., *Modules and Rings*, Cambridge University Press, 1994.

[2] Feigelstock S., *Additive groups of rings*, Pitman Publishing Inc, 1983.

[3] Fuchs L., *Infinite Abelian Groups, Vol I*, Academic Press, 1970.

[4] Fuchs L., *Infinite Abelian Groups, Vol II*, Academic Press, 1973.

[5] Higgins P.J, *Introduction to Topological Groups*, Cambridge University Press, 1974.

[6] Hernández F., *Teoría de Conjuntos. Una introducción*, Sociedad Matemática Mexicana, 2003.

[7] Mac Lane S. *Categories for the working mathematician*, Springer-Verlaq, 2^a ed., 1998.

[8] Nadler, S. B, *Dimension Theory: An Introduction with Exercices*, Sociedad Matemática Mexicana, 2002.

[9] Nathan J., *Basic Algebra I*, Dover, 2^a ed., 1985.

[10] Nathan J., *Basic Algebra II*, Dover, 2^a ed., 1989.

[11] Rotman J. J., *An Introduction to the Theory of Groups*, Springer-Verlag, 4^a ed., 1995.

[12] Stenström, B., *Ring of Quotients, An Introduction to Methods of Ring Theory*, Springer-Verlag, 1970.

[13] Van Oosten J., *Basic Category Theory*, Utrecht University, 2002.

[14] Willard S., *General Topology*, Dover, 2004.