UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

# "CLASIFICACIÓN DE P-GRUPOS ABELIANOS NUMERABLES."

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

**M A T E M Á T I C O**

P R E S E N T A :

**ERNESTO MAYORGA SAUCEDO**


FACULTAD DE CIENCIAS
UNAM

DIRECTORA DE TESIS: DRA. MARÍA DEL CARMEN GÓMEZ LAVEAGA

2006

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

**UNAM – Dirección General de Bibliotecas**
**Tesis Digitales**
**Restricciones de uso**

**DERECHOS RESERVADOS ©**
**PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL**

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

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

Mayorga
Saucedo
Ernesto
11-14-14-82
Universidad Nacional Autónoma de México
Facultad de Ciencias
Matemáticas

## Jurado

Dra.
María del Carmen
Gómez
Laveaga

Dr.
Hugo Alberto
Rincón
Mejía

Dr.
Juan
Morales
Rodríguez

Dra.
Bertha María
Tome
Arreola

Dr.
Alejandro
Alvarado
García

Clasificación de $p$-Grupos Abelianos Numerables
97
2006

*A Julia y Ernesto*

*A Edith y Edgar*

*A Richy, Dany y Rocío*

*A Gregorio*

*A mi familia*

# Agradecimientos

Cómo agradecer a quienes no sólo te dan la vida si no que además te brindan parte de la suya... A mi mamá y a mi papá Julia y Ernesto, gracias por apoyarme en todas mis "locuras", ustedes son parte fundamental de lo mucho o poco que he logrado hasta hoy.

A mis herman@s Edith, Roció y Edgar; y a mis sobrinos Dany y Richy por su amor, fortaleza e inteligencia que me inspira.

A mi tía Lourdes, mi tío Rafael y mis prim@s (herman@s) Erika, Jesús y Rafael, por ser mi "segunda" familia.

A mi abuelo Gregorio por su protección y enseñanzas.

A mi maestra Carmen Gómez Laveaga por haber aceptado dirigir esta tesis; por su comprensión, paciencia y por todas las charlas que me ayudan a reflexionar no sólo en matemáticas. Sobre todo le agradezco su gran sentido humanista el cual me ayudó seguir adelante.

A mis sinodales Hugo Rincón Mejía, Juan Morales Rodríguez, Bertha Tome Arreola y Alejandro Alvarado García por su apoyo, comentarios y correcciones.

A los profesores Alejandro Alvarado y Hugo Rincón con lo que he tenido la oportunidad de trabajar como su ayudante, realmente es un orgullo colaborar con ustedes.

A mi maestra Ana Irene Ramírez Galarza quien fue, y es, una de mis primeras fuentes de inspiración para seguir en esta aventura de ser matemático. Gracias por todo el apoyo y los consejos.

A los profesores Cesar Rincón Orta, Emilio Lluis Riera, Cesar Guevara Bravo, Luis Colavita Ferreyra y Javier Páez Cárdenas, mis otras grandes fuentes de inspiración en el deseo de ser matemático.

A los profesores con los que tuve la fortuna de llevar cursos; a todos ellos mi más profundo agradecimiento por haberme mostrado este mundo tan espectacular que conforma la Matemática.

A mis amig@s con los que inicie esta aventura: Nadia Castillo, Oscar Valderrama, Miguel Ángel López, Victor Mellado.

A Rolando Gómez Macedo con quien compartí una importante parte de la carrera y quien soportó y corrigió muchas de mis necedades. Realmente es un orgullo contarme entre tus amigos.

A Leopoldo Morales, por sus consejos y las charlas siempre interesantes y divertidas.

A mis amigos del "Ciencias Adventure Teem": Leo, Daniel, Checo, Yuri, Lu.

A Sele y Paulo, definitivamente fuera de serie.

A Abraham, con el que siempre es gratificante trabajar. Será inolvidable ese EGA.

A los de la Fac: Alejandro, John, Julio, Rafita, Luis, Alvaro, Ale, Idalia, Lupis, Rebe y Guillermo.

A la bandera del Instituto: José, Chávez, Yesenia, Pietra, Daniel, Frank, y Artico.
A tod@s ell@s gracias por brindarme su amistad.

Finalmente, agradezco a la Universidad Nacional Autónoma de México, mi segunda casa; la cual cambió mi vida al haberme otorgado la oportunidad de haber realizado mis estudios de bachillerato y licenciatura.

*... Al fin y al cabo, somos lo que hacemos para cambiar lo que somos.*
*Eduardo Galeano*

# Índice general

# Introducción

En este trabajo de tesis presentamos una clasificación de los Grupos Abelianos de Torsión Numerables mediante la noción de *invariante completo*, para ello seguiremos el esquema planteado por I. Kaplansky en *Infinite Abelian Groups* [Kap]. Dicho planteamiento no requiere de conceptos sofisticados de la teoría de grupos y en general de álgebra, bastará con la noción de *divisibilidad* y "variantes" de la misma, no esta de más decir que estas variantes sorprenden por su sencillez de comprensión e ingenio.

> *... Así como los objetos más fáciles de ver no son los demasiado grandes ni los demasiado pequeños, también las ideas más fáciles en matemáticas no son las demasiado complejas ni las demasiado simples.*
>
> *Bertrand Russell*

Gracias al concepto de *grupo divisible* es posible reducir el trabajo de clasificación a grupos $p$-primarios reducidos, para un número primo $p$ dado. En 1933 H.Ulm demuestra que, un grupo abeliano $G$ $p$-primario reducido y numerable esta completamente determinado salvo isomorfismo por una "sucesión" de cardinales, bien definidos por $G$, llamados invariantes de Ulm de $G$. Para encontrar dichos invariantes será necesario hacer uso de las nociones básicas de la teoría de ordinales y cardinales así como del principio de inducción trasfinita y el Lema de Zorn.

En la búsqueda de invariantes para un grupo dado, y en general para cualquier estructura, sea algebraica o de otra naturaleza, hay que tener presente que dichos invariantes tienen que ser tangibles, es decir,"calculables" y "eficaces" en el sentido de que con ellos podamos decidir si una cierta propiedad se cumple o no y que dicho trabajo sea menos complicado que el grupo mismo. En el capítulo 6 de [Kap], Kaplanski propone que, una forma de solucionar esto es resolviendo un problema explícito; es así que sugiere los siguientes tres problemas, que dentro de la teoría de grupos abelianos en general son preguntas abiertas:

**Problema 1.** *Si $G$ es isomorfo a un sumando directo de $H$ y $H$ es isomorfo a un sumando directo de $G$, ¿necesariamente $G$ y $H$ son isomorfos?*

**Problema 2.** *Si $G \oplus G \cong H \oplus H$, entonces $G \cong H$.*

**Problema 3.** *Si $\mathcal{F}$ es finitamente generado y $\mathcal{F} \oplus G \cong \mathcal{F} \oplus H$, entonces $G \cong H$.*

Veremos que para el caso de grupos abelianos divisibles las tres preguntas tienen respuesta y estas son afirmativas, lo mismo para grupos abelianos de torsión numerables.

El material que presentamos esta dividido en 3 capítulos. Con el fin de hacer autocontenido este trabajo, en el capítulo 1 establecemos algunas de las nociones básicas de la teoría de grupos abeliano como son definiciones y ejemplos, estos últimos servirán de herramienta o "modelos" que motivan ciertas definiciones, un ejemplo es el grupo $\mathcal{Z}_{p^\infty}$ del cual damos varias equivalencias; también introducimos la noción de invariante e invariantes completo dando algunos ejemplos de ellos. En el capítulo 2 se encuentran los temas centrales respecto a resultados de estructura.

*... divide las dificultades que examines en tantas partes como sea posible, para su mejor solución.*

*René Descartes*

La primera sección esta dedicada al estudio de grupos divisibles, presentamos el teorema de clasificación de esta clase de grupos e introducimos los invariantes que los clasifican, con ayuda de ello damos respuesta a los tres problemas anteriores para el caso de grupos divisibles. En la segunda sección se introduce la noción de *grupo puro* con el fin de obtener resultados semejantes a los obtenidos con los subgrupos divisibles, es decir, lograr dar una descomposición de un grupo dado en subgrupos más "manejables". Con la noción de *grupo de orden acotado*, la cual es introducida en la tercera sección, es posible dar condiciones necesarias y suficientes para que un grupo sea una suma directa de grupos cíclicos; también en esta sección se combinan las nociones de grupo puro y de orden acotado para decidir bajo qué condiciones un subgrupo de un grupo dado es sumando directo. En la sección cuatro introducimos el concepto de *altura*, la definición que damos aquí esta motivada por la divisibilidad, posteriormente será generalizada dando una definición más rigurosa; dicho concepto es pieza fundamental para definir los invariantes de Ulm. En la quinta sección estudiamos las sumas directas de grupos cíclicos con la ayuda del concepto de altura y se dan condiciones necesarias y suficientes para que un grupo sea suma directa de grupos cíclicos, en dichas condiciones esta involucrado el *zoclo* del grupo, que si bien en algunas de las secciones anteriores se ve su importancia, en esta es contundente. El capítulo tres

está dedicado a la demostración del teorema de Ulm, cabe mencionar que la demostración que presentamos no es la dada por Ulm, dicha demostración se debe a W. Mackey. En la primera sección retomamos el concepto de altura dando una definición rigurosa de ella; aquí introducimos los invariantes de Ulm de un grupo dado y analizamos su significado en el caso de grupos que son suma directa de grupos cíclicos. En la ultima sección damos la demostración del Teorema de Ulm y con el fin de hacerla más clara comenzamos esta sección dando el esquema que seguirá dicha prueba.

Agradezco a la Dra. Carmen Gómez Laveaga, directora de esta tesis, y al Prof. Luis Colavita Ferreyra su interés, profesionalismo y paciencia que llevaron a buen termino este trabajo, sobre todo les agradezco el haber compartido conmigo su gusto por descubrir cómo surgen las ideas en matemáticas.

Ernesto Mayorga Saucedo

# Capítulo 1

# Preliminares

## 1.1. Definiciones y Ejemplos

A lo largo del presente trabajo, la palabra "grupo", significará grupo abeliano (conmutativo) y su operación será escrita en forma aditiva. Utilizaremos el mismo símbolo para denotar un grupo y el conjunto de sus elementos. Dado un grupo $G$, denotaremos por 0 al elemento neutro del grupo $G$.

Una característica natural de un grupo, abeliano o no, es el numero de elementos que tiene. El ***orden de un grupo*** $G$, que denotaremos como $\boldsymbol{o(G)}$, es al cardinal del conjunto $G$, esto es, si $G$ es un conjunto finito con $n$ elementos, $o(G) = n$ y en este caso diremos que $G$ es un ***grupo finito*** de orden $n$. Por otra parte, si el conjunto $G$ es infinito, $o(G)$ será infinito y en este caso diremos que $G$ es un ***grupo infinito***. Un subconjunto $H$ de un grupo $G$ es un ***subgrupo***, y lo denotamos $\boldsymbol{H \leq G}$, si $H$ con la operación de $G$ restringida a $H$, $+|_H$, es un grupo; si $H$ es un subgrupo de $G$ y $H \subsetneq G$ diremos que $H$ es un ***subgrupo propio*** de $G$ y será denotado por $\boldsymbol{H < G}$. Los ***subgrupos triviales*** de un grupo $G$ son $G$ y el subgrupo que consta sólo del neutro 0, el cual también será denotado por 0.

Existen varias equivalencias de la definición de subgrupo. A continuación presentamos la que utilizaremos a lo largo del trabajo.

**Proposición 1.1.1.** *Si $G$ es un grupo y $H \subseteq G$. Las siguientes afirmaciones son equivalentes*

1. *$H$ es subgrupo de $G$.*
2. *a) $0 \in H$,*

   *b) Si $a, b \in H$ entonces $(a - b) \in H$.*

Dada una familia $\mathscr{F} = \{S_i\}_{i\in I}$ de subgrupos de $G$, a partir de ella podemos obtener un subgrupo en forma sencilla. Esto es, no es difícil demostrar que $\bigcap_{i\in I} S_i$ (la intersección conjuntista de los $S_i$'s, $i \in I$) es un subgrupo de $G$. Teniendo esto en cuenta, dado un subconjunto $X$ de $G$ sea $\mathcal{A} = \{H \leq G \mid X \subseteq H\}$, definimos

$$\langle \boldsymbol{X} \rangle = \bigcap_{H\in\mathcal{A}} H,$$

el cual es un subgrupo de $G$ que contiene a $X$ y claramente es el menor subgrupo de $G$ (respecto a $\subseteq$) con esta propiedad. Llamamos a $\langle X\rangle$ el ***subgrupo generado*** por $X$.

En el caso de la unión $\bigcup_{i\in I} S_i$, este en general no es un subgrupo, sin embargo, dado que $S_i \leq G$ para toda $i \in I$, se puede considerar el subgrupo de $G$ que contiene a todos los $S_i$'s, esto es, si $\mathcal{B} = \{S \leq G \mid S_i \leq S \text{ para toda } i \in I\}$,

$$\langle \mathscr{F} \rangle = \bigcap_{S\in\mathcal{B}} S$$

es el mínimo subgrupo de $G$ que contiene a cada $S_i$, $i \in I$, al que llamaremos el subgrupo generado por la familia $\mathscr{F}$ y del que tenemos una descripción. Definimos

$$\sum_{\boldsymbol{i\in I}} \boldsymbol{S_i} = \left\{ \sum_{j=1}^{k} s_{i_j} \mid s_{i_j} \in S_{i_j},\ i_j \in I,\ k \in \mathbb{N} \right\},$$

no es difícil demostrar que $\sum_{i\in I} S_i$ es un subgrupo de $G$. Además se tiene la siguiente igualdad

$$\langle \mathscr{F} \rangle = \sum_{i\in I} S_i. \tag{1.1}$$

En efecto, como $\sum_{i\in I} S_i$ es un subgrupo de $G$ que contiene a cada $S_j$, $j \in I$, entonces

$$\langle \mathscr{F} \rangle \leq \sum_{i\in I} S_i.$$

Por otro lado, dado $s_{i_j} \in S_{i_j}$, para $j = 1, \ldots, k$ arbitrarios, como pertenecen a $\langle \mathscr{F}\rangle$, entonces $\sum_{j=1}^{k} s_{i_j} \in \langle \mathscr{F}\rangle$, lo que cual muestra

$$\sum_{i\in I} S_i \leq \langle \mathscr{F} \rangle,$$

y de aquí se obtiene la igualdad.

Si $S = \{a_i\}_{i\in I}$ escribimos $\langle S\rangle = \langle a_i\rangle_{i\in I}$. En el caso de que $S = \varnothing$, $\langle S\rangle = 0$. Si $S \neq \varnothing$, $\langle S\rangle = \{n_1 a_{i_1} + \cdots + n_k a_{i_k} \mid i_1, \ldots, i_k \in I;\ k \in \mathbb{N}\}$.

En el caso en que $\langle S\rangle = G$ diremos que $S$ un ***conjunto generador*** de $G$ o simplemente que $S$ genera $G$. Si existe un conjunto finito que genera a $G$, diremos que $G$ es un ***grupo finitamente generado***. Para un elemento $a \in G$, $\langle a\rangle$ se llama el ***subgrupo cíclico*** generado por $a$ y si $G = \langle a\rangle$ diremos que $G$ es un ***grupo cíclico***.

El orden de un elemento $a$ de un grupo $G$, que denotaremos como $\boldsymbol{o(a)}$, está definido como el orden del subgrupo generado por $a$, es decir, $o(a) = o(\langle a\rangle)$. En caso de que $o(a)$ sea finito se puede demostrar haciendo uso del algoritmo de la división en los enteros que, $o(a)$ es el menor entero positivo $n$ tal que $na = 0$. Cabe mencionar que para un elemento $a$ de orden finito $n$, se tiene que $ra = sa$ si y sólo si $r \equiv s \pmod{n}$. Además en este caso se pueden determinar todos los generadores de $\langle a\rangle$ que son los elementos $ma$ con $(m, n) = 1$. Esto es $\langle a\rangle = \langle ma\rangle$ si y sólo si $(m, n) = 1$.

Dado un grupo $G$ el **zoclo** de $G$ denotado por $S(G)$ es el conjunto de elementos de $G$ que son anulados por un entero libre de cuadrados. Consideremos $x_1, x_2 \in S(G)$, entonces existen $m_1$ y $m_2$ enteros libres de cuadrados tales que $m_1x_1 = 0$ y $m_2x_2 = 0$. Como $[m_1, m_2] = \frac{m_1m_2}{(m_1,m_2)}$ es libre de cuadrados y $[m_1, m_2](x_1 - x_2) = 0$ entonces $x_1 - x_2 \in S(G)$, además $0 \in S(G)$. Podemos resumir lo anterior en la siguiente proposición.

**Proposición 1.1.2.** *Sea $G$ es un grupo, entonces $S(G) \leq G$.*

Note que en la demostración es necesaria la conmutatividad del grupo.

### 1.1.1. Suma Directa Externa

Sea $\mathscr{F} = \{G_i\}_{i\in I}$ una familia no vacía de grupos. Consideremos el producto cartesiano de $\mathscr{F}$,

$$\underset{i\in I}{\times} G_i = \left\{ f : I \longrightarrow \bigcup_{i\in I} G_i \mid f(i) \in G_i \text{ para cada } i \in I \right\},$$

la manera natural de dar a $\underset{i\in I}{\times} G_i$ una estructura de grupo, es definir la "suma" de funciones en forma puntual. No es difícil probar que efectivamente esta operación proporciona a $\underset{i\in I}{\times} G_i$ una estructura de grupo conmutativo llamado **producto directo** el cual será denotado como $\prod_{\boldsymbol{i\in I}} \boldsymbol{G_i}$, el elemento neutro de dicho grupo esta dado por $0(i) = 0_i$, donde $0_i$ es el neutro en $G_i$,.

Un subgrupo importante de este grupo es el grupo llamado *suma directa externa*. Consideremos el conjunto

$$\bigoplus_{\boldsymbol{i\in I}} \boldsymbol{G_i} = \left\{ f \in \prod_{i\in I} G_i \mid sop(f) \text{ es finito} \right\},$$

donde $\boldsymbol{sop(f)}= \{i \in I \mid f(i) \neq 0_i\}$. Claramente $0 \in \bigoplus_{i\in I} G_i$; además $sop(f) = sop(-f)$ para cada $f \in \bigoplus_{i\in I} G_i$, y si $f, g \in \bigoplus_{i\in I} G_i$ entonces $Sop(f + g) \subseteq Sop(f) \cup Sop(g)$ que es finito. Así tenemos que $\bigoplus_{i\in I} G_i \leq \prod_{i\in I} G_i$.

**Definición 1.1.3.** *La **Suma Directa Externa** de la familia $\mathscr{F}$ es el subgrupo $\bigoplus_{i\in I} G_i$ del producto directo $\prod_{i\in I} G_i$.*

Dado $f \in \prod_{i\in I} G_i$, como una función queda determinada por la imagen de cada uno de los elementos en su dominio, los elementos de $\prod_{i\in I} G_i$ serán denotados de la forma $(a_i)_{i\in I}$, donde $a_i = f(i) \in G$ para toda $i \in I$; así los elementos de $\prod_{i\in I} G_i$ son aquellas $(x_i)_{i\in I}$ donde todas las $x_i$'$s$ son cero salvo un número finito. Si $I$ es finito, entonces

$$\prod_{i\in I} G_i = \bigoplus_{i\in I} G_i.$$

Si $I$ es infinito, la suma directa y el producto directo en general son distintos, salvo en casos raros.

### 1.1.2. Suma Directa Interna

Sea $G$ un grupo y $\mathscr{F} = \{S_i\}_{i\in I}$ una familia de subgrupos de $G$. Considerando la suma directa externa $\bigoplus_{i\in I} S_i$, tenemos que en cada elemento $(x_i)_{i\in I} \in \bigoplus_{i\in I} S_i$, $x_i = 0$ para todo $i \in I$ salvo un número finito, *denotaremos la suma de dichos elementos como* $\sum_{i\in I} x_i$. Esto determina de manera natural una función $\bigoplus_{i\in I} S_i \xrightarrow{\phi} G$ definida como

$$\phi((x_i)_{i\in I}) = \sum_{i\in I} x_i. \tag{1.2}$$

Como $(x_i)_{i\in I} + (y_i)_{i\in I} = (x_i + y_i)_{i\in I}$ y $G$ es abeliano, entonces

$$\phi((x_i)_{i\in I} + (y_i)_{i\in I}) = \phi((x_i)_{i\in I}) + \phi((y_i)_{i\in I}),$$

es decir, $\phi$ es un homomorfismo natural entre los grupos $\bigoplus_{i\in I} S_i$ y $G$. Veamos qué necesitamos pedir a la familia $\mathscr{F}$ para que $\phi$ sea un isomorfismo. Vayamos por partes y respondamos primero que condiciones imponemos a $\mathscr{F}$ para que $\ker \phi = 0$.

Si $\ker\phi = 0$; en caso de que $(x_i)_{i\in I} \in \bigoplus_{i\in I} S_i$ satisfaga que $\sum_{i\in I} x_i = 0$ debemos tener que $x_i = 0$ para toda $i \in I$ y además para cada $j \in I$ tenemos las identidades $x_j = \sum_{i\in I-\{j\}} (-x_i)$; así necesariamente

$$S_j \bigcap \left( \sum_{i\in I-\{j\}} S_i \right) = 0 \text{ para toda } j \in I. \tag{1.3}$$

Recíprocamente, si $\mathscr{F}$ satisface (1.3) y $(y_i)_{i\in I} \in \ker\phi$ entonces $\sum_{i\in I} y_i = 0$ y por consiguiente

$$y_j = \sum_{i\in I-\{j\}} (-y_i) \in S_j \bigcap \left( \sum_{i\in I-\{j\}} S_i \right) = 0,$$

para cada $j \in I$, es decir, $(y_i)_{i\in I} = 0$ y por lo tanto $\ker\phi = 0$. Así una condición necesaria y suficiente para que $\phi$ sea inyectiva en que $\mathscr{F}$ satisfaga (1.3).

Por otra parte, si $\phi$ es suprayectiva, entonces cada elemento $y \in G$ se puede expresar como

$$y = \sum_{i\in I} x_i,$$

donde $x_i \in S_i$, para cada $i \in I$, y todas las $x_i$'s, son cero salvo un número finito. Así, una condición necesaria para que $\phi$ sea suprayectiva es que

$$G = \sum_{i\in I} S_i. \tag{1.4}$$

Pero también (1.4) es suficiente, ya que si $\mathscr{F}$ satisface esta propiedad, dado $y \in G$ existen $x_{i_1} \in S_{i_1}, \ldots, x_{i_k} \in S_{i_k}$ tales que $y = \sum_{j=1}^{k} x_{i_j}$; considerando $(x_i)_{i\in I}$ donde

$$x_i = \begin{cases} x_{i_j} \text{ si } i = i_j \text{ para algún } j = 1, \ldots, k \\ 0 \quad \text{si } i \neq i_j \text{ para todo } j = 1, \ldots, k \end{cases}$$

tenemos que $\phi((x_i)_{i\in I}) = y$ y así $\phi$ es suprayectiva. Por lo tanto (1.4) determina una condición necesaria y suficiente para que $\phi$ sea suprayectiva. Finalmente tenemos la siguiente definición.

**Definición 1.1.4.** *Sea $\mathscr{F}$ una familia de subgrupos de un grupo $G$. Si $\mathscr{F}$ es una familia que satisface (1.3) y (1.4), decimos que $G$ es la **suma directa interna** de $\mathscr{F}$ y lo denotamos como $G = \bigoplus_{\imath\in I} S_i$.*

Una familia $\mathscr{F} = \{S_i\}_{i\in I}$ de subgrupos de un grupo $G$ que satisface (1.3) se llama **independiente**.

**Nota 1.1.5.** *Si bien ya lo mencionamos, dado $(a_i)_{i\in I}$ un elemento de una suma directa de grupos $\bigoplus_{i\in I} G_i$, en algunas ocasiones, por comodidad, $\sum_{i\in I} a_i$ denotará la suma de aquellas $a_i$'s distintas de cero.*

Una definición equivalente de suma directa interna se muestra en la siguiente proposición.

**Proposición 1.1.6.** *Si $\mathscr{F} = \{S_i\}_{i\in I}$ es una familia de subgrupos de $G$, entonces son equivalentes las siguientes afirmaciones*

1. *$G$ es la suma directa de la familia $\mathscr{F}$.*

2. a) $G = \sum_{i\in I} S_i$.

   b) *Cada elemento $x \in G$ tiene una única expresión*

$$x = \sum_{i\in I} s_i, \tag{1.5}$$

*donde $s_i \in S_i$, para toda $i \in I$ con $s_i = 0$ salvo un número finito de índices.*

*Demostración.* Para verificar la equivalencia basta mostrar que la condición (1.3) es equivalente a al inciso $(b)$ de la Proposición 1.1.6. En efecto si $\mathscr{F}$ satisface (1.3) y $x \in G$ satisface que

$$x = \sum_{i\in I} x_i = \sum_{i\in I} y_i,$$

entonces para toda $j \in I$ se tiene que

$$y_j - x_j = \sum_{i\in I-\{j\}} (x_i - y_i) \in S_j \bigcap_{i\in I-\{j\}} S_i = 0$$

y por lo tanto, para toda $j \in I$, $y_j = x_j$ mostrando que la expresión de $x$ es única.

Recíprocamente si $\mathscr{F}$ satisface Proposición 1.1.6, *2* ,$(b)$ y $x \in S_j \bigcap_{i\in I-\{j\}} S_i$, entonces

$$x = z_j = \sum_{i\in I-\{j\}} z_i,$$

de donde $-z_j + \sum_{i\in I-\{j\}} z_i = 0$, y como la expresión de 0 es única tenemos que $z_i = 0$ para todo $i \in I$, es decir, $\mathscr{F}$ satisface (1.3). ■

**Nota 1.1.7.** *Sea* $G = \bigoplus_{i\in I} G_i$ *la suma directa externa de la familia* $\{G_i\}_{i\in I}$. *Cada* $G_i$ *determina un subgrupo* $\widetilde{G}_i$ *de* $G$, *isomorfo a* $G_i$, *tal que* $G$ *es la suma directa interna de la familia* $\{\widetilde{G}_i\}_{i\in I}$ *de la siguiente manera. Definimos, para cada* $j \in I$,

$$\widetilde{G}_j = \{(x_i)_{i\in I} \mid x_i = 0 \text{ si } i \neq j\}$$

*Claramente* $\widetilde{G}_j \leq G$ *para cada* $j \in I$. *Veamos que* $G$ *es la suma directa interna de la familia de subgrupos* $\{\widetilde{G}_i\}_{i\in I}$. *Dado* $\widetilde{x} = (x_i)_{\imath\in I} \in G$, *sólo un número finito de* $x_i$*'s son distintas de cero, si* $x_{i_1}, \ldots, x_{i_n}$ *son tales términos, consideramos* $\widetilde{x}_{i_j} \in \widetilde{G}_{i_j}$ *con* $j = 1, \ldots, n$, *donde el término* $i_j$ *de* $\widetilde{x}_j$ *es* $x_{i_j}$ *y cero en los demás términos, así tenemos que*

$$\widetilde{x} = \widetilde{x}_{i_1} + \widetilde{x}_{i_2} + \cdots + \widetilde{x}_{i_n},$$

*y por lo tanto* $G = \sum_{i\in I} \widetilde{G}_i$. *Por otra parte, si* $\widetilde{x} = (x_i)_{i\in I} \in G_j \cap \sum_{i\in I-\{j\}} \widetilde{G}_i$ *entonces al ser* $\widetilde{x}$ *elemento de* $\widetilde{G}_j$ *sólo el término* $x_j$ *puede ser distinto de cero, pero como* $\widetilde{x} \in \sum_{i\in I-\{j\}} \widetilde{G}_i$ *el término* $x_j$ *es* $0_j$, *es decir* $\widetilde{x} = 0$ *y por lo tanto*

$$\widetilde{G}_j \cap \sum_{i\in I-\{j\}} \widetilde{G}_i = 0 \text{ para todo } j \in I.$$

*De esta manera tenemos que* $G = \bigoplus_{i\in I} \widetilde{G}_i$ *es la suma directa interna. Claramente existe un isomorfismo de* $G_i$ *con* $\widetilde{G}_i$, *para cada* $i \in I$, *que asocia a cada elemento* $x_i \in G_i$ *el elemento* $\widetilde{x}_i \in \widetilde{G}_i$, *construido como los* $\widetilde{x}_{i_j}$*'s dadas anteriormente. Así, abusando de la notación, dado un elemento* $x \in G$ *éste tiene una única expresión*

$$x = \sum_{j=1}^{n} x_{i_j},$$

*donde estamos identificando* $x_{i_j}$ *con* $\widetilde{x}_{i_j}$.

A continuación damos una definición que de cierta manera es un caso particular de familia independiente de subgrupos.

Sea $\beta = \{x_i\} \subseteq G$. Diremos que $\beta$ es un **conjunto independiente** si $\{\langle x_i\rangle\}_{i\in I}$ es una familia independiente de subgrupos de $G$.

Lo equivalente respecto a la condición (1.3) para conjuntos independientes es la siguiente caracterización, que no es mas que una reformulación de (1.3) para una familia de subgrupos cíclicos.

**Definición 1.1.8.** *Un subconjunto $\beta = \{x_i\}_{i\in I}$ de un grupo $G$ es un* ***subconjunto independiente*** *si y sólo si, cada vez que se tenga*

$$n_{i_1}x_{i_1} + n_{i_2}x_{i_2} + \cdots + n_{i_m}x_{i_m} = 0$$

*entonces*

$$n_{i_j}x_{i_j} = 0,$$

*para todo $j = 1, 2, \ldots, m$; donde $n_{i_j} \in \mathbb{Z}$ $(1 \leq j \leq m)$.*

Si $G = \bigoplus_{i\in I} G_i$ y $H_i$ es un subgrupo de $G_i$, para cada $i \in I$, entonces $H = \bigoplus_{i\in I} H_i$ es un subgrupo de $G$. Es posible obtener una descripción del grupo $G/H$ a través de los grupos $G_i/H_i$ 's como afirma la siguiente proposición.

**Proposición 1.1.9.** *Sean $G = \bigoplus_{i\in I} G_i$ y $H_i$ un subgrupo de $G_i$, para cada $i \in I$, entonces $H = \sum_{i\in I} H_i$ es una suma directa y $H$ es un subgrupo de $G$. Además*

$$G/H \cong \bigoplus_{i\in I} (G_i/H_i)\,.$$

*Demostración.* Claramente $\sum_{i\in I} H_i$ es un subgrupo de $G$. Además, en vista de que $H_j \subseteq G_j$ para todo $j \in I$ obtenemos tenemos que

$$H_j \bigcap \left( \sum_{i\in I-\{j\}} H_i \right) \subseteq G_j \bigcap \left( \sum_{i\in I-\{j\}} G_i \right) = 0$$

y por lo tanto $\sum_{i\in I} H_i = \bigoplus_{i\in I} H_i$. La idea en lo que resta de la demostración es utilizar el primer teorema de isomorfismos, así definimos $\varphi : \bigoplus_{i\in I} G_i \longrightarrow \bigoplus_{i\in I} (G_i/H_i)$ como

$$\varphi((x_i)_{i\in I}) = (\overline{x}_i)_{i\in I},$$

donde $\overline{x_i}$ denota la clase lateral de $x_i \in G_i$ módulo $H_i$. $\varphi$ esta bien definida ya que si $x_i = 0$ para toda $i \in I$ salvo un número finito, entonces $\overline{x_i} = \overline{0}$ para casi toda $i \in I$ excepto un número finito. Veamos que $\varphi$ es un homomorfismo; para esto, sean $(x_i)_{i\in I}, (y_i)_{i\in I} \in G$, entonces

$$\begin{aligned}
\varphi((x_i)_{i\in I} + (y_i)_{i\in I}) &= \varphi((x_i + y_i)_{i\in I}) \\
&= (\overline{x_i + y_i})_{i\in I} \\
&= (\overline{x}_i + \overline{y}_i)_{i\in I} \\
&= (\overline{x}_i)_{i\in I} + (\overline{y}_i)_{i\in I} \\
&= \varphi((x_i)_{i\in I}) + \varphi((y_i)_{i\in I}).
\end{aligned}$$

Supongamos ahora que $(x_i)_{i\in I} \in \ker\varphi$, entonces $\varphi((x_i)_{i\in I}) = (\overline{0}_i)_{i\in I}$ implica que

$$(\overline{x}_i)_{i\in I} = (\overline{0}_i)_{i\in I},$$

y por consiguiente $\overline{x}_i = \overline{0}_i$ para toda $i \in I$, es decir, $x_i \in H_i$ para toda $i \in I$ obteniendo así que $(x_i)_{i\in I} \in \bigoplus_{i\in I} H_i$; por lo tanto $\ker\varphi \subseteq \bigoplus_{i\in I} H_i$.

Recíprocamente, si $(x_i)_{i\in I} \in \bigoplus_{i\in I} H_i$, entonces $\varphi((x_i)_{i\in I}) = (\overline{x}_i)_{i\in I} = (\overline{0}_i)_{i\in I}$, es decir, $\bigoplus_{i\in I} H_i \subseteq \ker\varphi$ y por lo tanto $\bigoplus_{i\in I} H_i = \ker\varphi$.

Por otra parte, dado $y \in \bigoplus_{i\in I} (G_i/H_i)$, $y = (\overline{y}_i)_{i\in I}$ donde $\overline{y}_i \in G_i/H_i$ para cada $i \in I$ y todas son cero salvo un número finito. Suponiendo que $\overline{y}_{i_1}, \ldots, \overline{y}_{i_k}$ son todos los términos distintos de cero, consideramos $(x_i)_{i\in I}$, definido como sigue

$$x_i = \begin{cases} y_{i_j} \text{ si } i = i_j \text{ para algún } j = 1, \ldots, k \\ 0 \quad \text{si } i \neq i_j \text{ para todo } j = 1, \ldots, k. \end{cases}$$

Entonces $(x_i)_{i\in I} \in G$ y además $(\overline{x}_i)_{i\in I} = (\overline{y}_i)_{i\in I}$, es decir, $\varphi((x_i)_{i\in I}) = y$ y por lo tanto $\varphi$ es suprayectiva. Finalmente, por el primer teorema de isomorfismos

$$G/H \cong \bigoplus_{i\in I} (G_i/H_i)\,.$$

■

## 1.2. Invariantes en la Teoría de Grupos

Una gran parte de los trabajos que se desarrollan en matemáticas están dirigidos hacia la clasificación de sus objetos de estudio; curvas, superficies o variedades en Geometría, espacios topológicos en Topología, y estructuras algebraicas en Álgebra son algunos ejemplos. Inclusive con el fin de resolver estos problemas algunos de estos tópicos se ven relacionados y dan lugar a nuevas ramas de la Matemática como son la Geometría Algebraica o la Topología Algebraica. La idea en esta relación es asociar a un objeto de cierta naturaleza A, otro de diferente naturaleza B, y a través de las propiedades de B poder obtener información acerca de A. En ciertas ocasiones esta asociación es recíproca y es así que surge la noción de invariante. Pues bien, en este trabajo se presenta una clasificación de una clase particular de grupos mediante invariantes, estableciendo una correspondencia entre ciertos tipos de grupos y cierta clase de conjuntos. La idea básica de los invariantes en la teoría de grupos es asociar a un grupo dado $G$ un objeto $f(G)$ que puede ser un número, un conjunto de números o una función de tal manera que:

$$G \cong H \Longrightarrow f(G) = f(H)\,. \tag{1.6}$$

Si se cumple (1.6) diremos que $f(G)$ es un **invariante** del grupo $G$; y en caso de tener:

$$G \cong H \Longleftrightarrow f(G) = f(H) \tag{1.7}$$

diremos que $f(G)$ es un **invariante completo** del grupo $G$.

Para fijar ideas consideremos el siguiente ejemplo.

**Ejemplo 1.2.1.** *Sea $K$ un campo. Consideremos $V$ y $W$ dos $K$-espacios vectoriales. La equivalencia*

$$V \cong W \iff \dim_K V = \dim_K W, \tag{1.8}$$

*asegura que $\dim_K V$ es un invariante completo para $V$. Así, desde este punto de vista, la teoría de espacios vectoriales tiene totalmente clasificados gran parte de sus objetos de estudio, los espacios vectoriales, y el teorema de clasificación es el dado en (1.8). De hecho podemos exhibir un representante por cada dimensión y que es, de cierta manera, fácil de manejar, a saber, $\bigoplus_\alpha K$ la suma directa de $\alpha$ copias de $K$, para cada dimensión $\alpha$. En caso de que $\alpha$ sea un cardinal finito tenemos que*

$$\bigoplus_\alpha K = K^\alpha,$$

*donde $K^\alpha$ denota el producto cartesiano de $\alpha$ copias de $K$.*

Dentro de la teoría de grupos esta tarea es más complicada pero para cierta clase de grupos es posible encontrar invariantes completos que no resultan ser tan complicados. El siguiente ejemplo da muestra de ello.

**Ejemplo 1.2.2.** *Sean $G = \langle a \rangle$ y $H = \langle b \rangle$ grupos cíclicos. Es claro que*

$$G \cong H \iff o(G) = o(H). \tag{1.9}$$

*Así el orden resulta ser un invariante completo para el grupo cíclico $G$. De esta manera tenemos que la clase de los grupos cíclicos está completamente clasificada y el teorema de clasificación es el dado por la equivalencia (1.9). Como en el caso de espacios vectoriales, para este tipo de grupos se tienen representantes muy especiales.*

*El grupo aditivo de los números enteros, y que a lo largo del trabajo denotaremos por $\mathcal{Z}$, es un grupo cíclico infinito. De manera que si $o(G)$ es infinito entonces $G \cong \mathcal{Z}$. Para los grupos cíclicos finitos, los representantes son $\mathcal{Z}_n$, los grupos aditivos de las clases de residuos módulo $n$. El grupo $\mathcal{Z}_n$ es cíclico y $\mathcal{Z}_n = \langle \overline{m} \rangle$ donde $(m, n) = 1$. Así, en caso de que $o(G) = n$ entonces $G \cong \mathcal{Z}_n$.*

El ejemplo anterior muestra un invariante completo sumamente sencillo, pero para grupos más generales que los cíclicos éste deja de ser completo, una muestra sencilla de esto es el siguiente ejemplo. Sea $G = \mathcal{Z}_2 \times \mathcal{Z}_2$ y $H = \mathcal{Z}_4$, claramente $o(G) = o(H)$ y sin embargo $G \ncong H$ pues $G$ no es cíclico y $H$ si lo es. Esto nos lleva a considerar otras propiedades que puedan poseer los grupos y que arrojen información de estos.

## 1.3. Grupos de Torsión

Consideremos un grupo $G$ y sea $x \in G$. Diremos que que $x$ es de **torsión** si existe $n \in \mathbb{Z}^+$ tal que $nx = 0$, y en caso de que $nx \neq 0$ para todo $n \in \mathbb{Z}^+$ diremos que $x$ es **libre de torsión**. Denotaremos por $\boldsymbol{t(G)}$ al conjunto de todos los elementos de $G$ que son de torsión. Nótese que los elementos de torsión son precisamente los de orden es finito.

**Proposición 1.3.1.** *Dado un grupo $G$, el conjunto $t(G)$ es un subgrupo de $G$.*

*Demostración.* Claramente $0 \in t(G)$. Sean $x, y \in t(G)$ con $mx = 0$ y $ny = 0$, $m, n \in \mathbb{Z}^+$ entonces

$$\begin{aligned} mn(x-y) &= (mn)x - (mn)y \\ &= n(mx) - m(ny) \\ &= 0 - 0 \\ &= 0, \end{aligned}$$

y como $mn \in \mathbb{Z}^+$ tenemos que $x - y \in t(G)$ y por lo tanto $t(G) \leq G$. ■

**Nota 1.3.2.** *En general si $G$ no es abeliano $t(G)$ no tine porque ser un subgrupo. Consideremos el grupo lineal general con entradas racionales $G = GL(2, \mathbb{Q})$; $GL(2, \mathbb{Q})$ es el grupo multiplicativo de las unidades del anillo $M(2, \mathbb{Q})$. Sean $A, B$ las siguientes matrices en $GL(2, \mathbb{Q})$*

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad y \quad B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

*Un calculo sencillo muestra que $A^4 = E = B^3$, donde $E$ denota la matriz identidad en $M(2, \mathbb{Q})$. Sin embargo, para toda $n \in \mathbb{Z}^+$*

$$(AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \neq E.$$

*Es decir, $AB$ es libre de torsión, a pasar de que $A$ y $B$ son de torsión.*

**Definición 1.3.3.** *Sea $G$ un grupo, $t(G)$ se llama el **subgrupo de torsión** de $G$.*

A $t(G)$ también se le conoce como "*la parte de torsión*" del grupo $G$. Si $t(G) = G$ diremos que $G$ es un ***grupo de torsión***. Si $t(G) = 0$ diremos que $G$ es un ***grupo libre de torsión***. Cabe mencionar que las nociones de torsión y libre de torsión no son complementarias, es decir, podemos encontrar grupos que no son de torsión que tienen parte de torsión no trivial; un grupo con estas características es llamado ***grupo mixto***.

**Ejemplo 1.3.4.** (*a*) *Todo grupo finito es de torsión.*

(*b*) *Como caso particular del ejemplo anterior tenemos que para cada $n \in \mathbb{Z}^+$, $\mathcal{Z}_n$ es un grupo de torsión.*

(*c*) *El grupo aditivo de los números enteros $\mathcal{Z}$ y el grupo aditivo de los números racionales, que a lo largo del trabajo denotaremos por $\mathcal{Q}$, son grupos libres de torsión.*

Los incisos (*a*) y (*b*) del ejemplo anterior sólo muestran grupos finitos, sin embargo hay grupos de torsión infinitos, como lo muestra el siguiente ejemplo.

**Ejemplo 1.3.5.** *El grupo cociente $\mathcal{Q}/\mathcal{Z}$ se conoce como **los racionales módulo uno**. Geométricamente, $\mathcal{Q}/\mathcal{Z}$ puede identificarse con los números racionales contenidos en el intervalo $[0, 1) \subset \mathbb{R}$.*

*Si $\overline{x} \in \mathcal{Q}/\mathcal{Z}$ y $\overline{x} = \frac{\overline{a}}{b}$, entonces*

$$b\overline{x} = b\frac{\overline{a}}{b} = \frac{\overline{ba}}{b} = \overline{a} = \overline{0}.$$

*Es decir $x$ es de torsión, y por lo tanto $\mathcal{Q}/\mathcal{Z}$ es un grupo de torsión.*

El siguiente ejemplo muestra un grupo mixto.

**Ejemplo 1.3.6.** *Sean $L$ un grupo libre de torsión y $T$ un grupo de torsión no trivial. Consideremos el grupo $G = L \oplus T$; no es difícil verificar que*

$$0 < t(G) = 0 \oplus T < G.$$

Antes de continuar con los ejemplos veamos cómo la parte de torsión es invariante bajo isomorfismos.

**Proposición 1.3.7.** *Si $G$ y $H$ son grupos isomorfos. Entonces $t(G)$ es isomorfo a $t(H)$.*

*Demostración.* Sea $\varphi : G \longrightarrow H$ un isomorfismo. Afirmamos que $\varphi|_{t(G)} : t(G) \longrightarrow t(H)$ es un isomorfismo, en efecto si $x \in t(G)$ entonces existe $m \in \mathbb{Z}^+$ tal que $mx = 0$, entonces $m\varphi(x) = \varphi(mx) = 0$ y que indica que $\varphi(x) \in t(H)$ y por lo tanto $\varphi(G) \subseteq t(H)$. Como $\varphi|_{t(G)}$ es la restricción de una función inyectiva, ella es inyectiva. Finalmente dado $y \in t(H)$

existe $x \in G$ tal que $\varphi(x) = y$; si $ny = 0$ entonces $\varphi(nx) = n\varphi(x) = 0$, como $\varphi|_{t(G)}$ es inyectiva $nx = 0$, es decir $x \in t(G)$ mostrando que $\varphi(t(G)) = t(H)$ y por lo tanto $t(G)$ es isomorfo a $t(H)$. ■

La proposición anterior hace ver $t(G)$ es un invariante, pero no es completo como lo muestra el siguiente ejemplo. Sean $G = \mathcal{Z}_n \oplus \mathcal{Z}$ y $H = \mathcal{Z}_n \oplus \mathcal{Q}$, entonces

$$t(G) = \mathcal{Z}_n \oplus 0 = t(H),$$

no obstante $G \ncong H$.

Regresando al grupo del Ejemplo 1.3.6, e identificando $0 \oplus \mathcal{Q}/\mathcal{Z}$ con $\mathcal{Q}/\mathcal{Z}$, tenemos que $G/(\mathcal{Q}/\mathcal{Z}) \cong \mathcal{Z}$ y como $t(\mathcal{Z}) = 0$, por la Proposición 1.3.7, tenemos que $t(G/(\mathcal{Q}/\mathcal{Z})) = 0$. Lo anterior es un caso particular de la siguiente proposición.

**Proposición 1.3.8.** *Sea $G$ un grupo, entonces $G/t(G)$ es libre de torsión*

*Demostración.* Si $\overline{x} \in G/t(G)$ es anulado por $m \in \mathbb{Z}^+$ entonces $\overline{0} = m\overline{x} = \overline{mx}$, de donde $mx \in t(G)$. Entonces existe $n \in \mathbb{Z}^+$ tal que $n(mx) = 0$, es decir, $(nm)x = 0$ mostrando que $x \in t(G)$ y por lo tanto $\overline{x} = \overline{0}$. ■

Dado un número primo $p \in \mathbb{Z}^+$, $x$ y $y$ elementos de un grupo $G$ tales que $p^m x = 0$ y $p^n y = 0$, se tiene que $p^{m+n}(x-y) = p^{m+n}(x) - p^{m+n}(y) = p^n p^m(x) - p^m p^n(y) = 0$, además como $0 = p0$, hemos demostrado que, para cada primo $p \in \mathbb{Z}^+$ el conjunto

$$\boldsymbol{G_p} = \{x \in G \mid p^m x = 0 \text{ para alguna } m \in \mathbb{N}\},$$

es un subgrupo de $t(G)$. Esta clase de subgrupos de la parte de torsión de un grupo $G$ resulta de gran importancia. Así tenemos las siguientes definiciones.

**Definición 1.3.9.** *Sea $p$ un número primo, un grupo $G$ se llama **$p$-primario** (o **$p$-grupo** en el caso no abeliano) si $G = G_p$.*

En particular si $G$ es $p$-primario, cada elemento de $G$ tiene orden una potencia de $p$.

**Definición 1.3.10.** *Sea $G$ un grupo. Para cada número primo $p \in \mathbb{Z}^+$, la **parte $p$-primaria** de $G$ es el subgrupo $G_p$.*

**Nota 1.3.11.** *Cuando $G$ es libre de torsión $t(G) = 0$ y por lo tanto $G_p = 0$ para todo número primo $p$. En caso de que $G$ no sea libre de torsión y $G$ no contenga elementos, no triviales, de orden $p$, entonces $G_p = 0$.*

**Ejemplo 1.3.12.** *Consideremos el grupo $\mathcal{Z}_n$ y supongamos que $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r}$ es su descomposición en primos, entonces $(\mathcal{Z}_n)_{p_i} \cong \mathcal{Z}_{p_i^{\alpha_i}}$. En efecto basta demostrar que $(\mathcal{Z}_n)_{p_i}$ es un grupo cíclico de orden $p_i^{\alpha_i}$. Claramente $(\mathcal{Z}_n)_{p_i}$ es cíclico, supongamos que $o((\mathcal{Z}_n)_{p_i}) = p_i^{\beta}$, como $p_i^{\beta} \mid n$ necesariamente $\beta \leq \alpha_i$; ahora bien $\overline{(\frac{n}{p^{\alpha_i}})}$ es un elemento de $\mathcal{Z}_n$ de orden $p^{\alpha_i}$ y por consiguiente $p^{\alpha_i} \mid p^{\beta}$; así, $\alpha_i \leq \beta$ y $o((\mathcal{Z}_n)_{p_i}) = p^{\alpha_i}$. Por lo tanto $(\mathcal{Z}_n)_{p_i} \cong \mathcal{Z}_{p^{\alpha_i}}$.*

De hecho se conoce más acerca del grupo $\mathcal{Z}_n$ del ejemplo 1.3.12. Se sabe que si $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r}$ entonces $\mathcal{Z}_n \cong \bigoplus_{i=1}^{r} \mathcal{Z}_{p_i^{\alpha_i}}$. Esto no es más que una muestra del hecho de que el estudio de grupos de torsión se reduce al siguiente teorema, cuya demostración está basada en la propiedad de factorización de los números enteros en producto de primos; así como en la ecuación de Bezout la cual expresa al máximo común divisor de ciertos números como una combinación entera de ellos.

**Teorema 1.3.13.** *Todo grupo de torsión es la suma directa de sus partes p-primarias.*

*Demostración.* Sea $G$ un grupo de torsión y $x \in G$ con $o(x) = n$. Consideramos la descomposición de $n$ en producto de primos $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r}$ y sea $n_i = \frac{n}{p_i^{\alpha_i}} \in \mathbb{Z}^+$, con $1 \leq i \leq r$. Como $(n_1, \ldots, n_r) = 1$ existen $m_i \in \mathbb{Z}^+$, $1 \leq i \leq r$, tales que

$$1 = m_1 n_1 + \cdots + m_r n_r,$$

de donde

$$x = m_1(n_1 x) + \cdots + m_r(n_r x).$$

Ahora bien, para cada $i$ $(1 \leq i \leq r)$ $p_i^{\alpha_i}(n_i x) = nx = 0$ y por lo tanto $n_i x \in G_{p_i}$ $(1 \leq i \leq r)$. Con esto hemos demostrado que

$$G = \sum_{p \in \mathscr{P}} G_p \tag{1.10}$$

donde $\mathscr{P}$ denota el conjunto de todos los números primos, cabe hacer notar aquí lo dicho al final de la Nota 1.3.11. Veamos que la suma en (1.10) es directa. Si $x \in G_{p'} \cap \sum_{p \in \mathscr{P} \setminus \{p'\}} G_p$ entonces $x = x_{i_1} + \cdots + x_{i_k}$, con $x_{i_j} \in G_{p_{i_j}}$. Supongamos que $p_{i_j}^{\alpha_{i_j}} x_{i_j} = 0$ para cada $j = i, \ldots, k$. Como $(p_{i_1}^{\alpha_{i_1}} \cdot \ldots \cdot p_{i_k}^{\alpha_{i_k}})x = 0$ necesariamente $p' \mid p_{i_1}^{\alpha_{i_1}} \cdot \ldots \cdot p_{i_k}^{\alpha_{i_k}}$, [1] lo cual es absurdo pues $p' \neq p_{i_j}$ para cada $j$. Por lo tanto para todo primo $p' \in \mathscr{P}$

$$G_{p'} \bigcap \sum_{p \in \mathscr{P} \setminus \{p'\}} G_p = 0. \tag{1.11}$$

[1] Al ser $x$ elemento de $G_{p'}$, $p' \mid o(x)$

A partir de (1.10) y (1.11) obtenemos que

$$G = \bigoplus_{p \in \mathscr{P}} G_p. \tag{1.12}$$

Como en todo teorema de descomposición, es importante verificar la unicidad. En este caso la unicidad es "estricta", es decir, no puede suceder que en (1.12) se tengan dos descomposiciones donde en una $G_q = 0$ y en otra $G_q \neq 0$ para algún número primo $q$. Así la descomposición en (1.12) es única. ■

Examinamos ahora cómo es la parte de torsión de un grupo $G$, así como de sus subgrupos $p$-primarios cuando $G$ es una suma directa de grupos.

**Proposición 1.3.14.** *Si $G$ y $H$ son grupos isomorfos, entonces para cada primo $p \in \mathbb{Z}^+$, $G_p$ es isomorfo a $H_p$.*

*Demostración.* Sea $\varphi : G \longrightarrow H$ un isomorfismo y $p \in \mathbb{Z}$ un numero primo. Afirmamos que

$$\varphi|_{G_p} : G_p \longrightarrow H_p$$

es un isomorfismo. En efecto si $x \in G_p$ y $p^n x = 0$ entonces por ser $\varphi$ un morfismo $0 = \varphi(p^n x) = p^n \varphi(x)$, de donde $\varphi(x) \in H_p$ y en consecuencia $\varphi(G_p) \subseteq H_p$. Además $\varphi|_{G_p}$ es inyectiva ya que es la restricción de una función inyectiva. Finalmente dado $y \in H_p$ por ser $\varphi$ epimorfismo existe $x \in G$ tal que $y = \varphi(x)$, si $p^r y = 0$ entonces $\varphi(p^r x) = p^r \varphi(x) = p^r y = 0$ de donde $p^r x = 0$, pues $\varphi$ es monomorfismo, por lo tanto $x \in G_p$ y $G_p \overset{\varphi|_{G_p}}{\cong} H_p$. ■

**Teorema 1.3.15.** *Sea $G = \bigoplus_{i \in I} G_i$, donde cada $G_i$ es un grupo. Entonces*

(1) $t(G) = \bigoplus_{i \in I} t(G_i)$.

(2) $G_p = \bigoplus_{i \in I} (G_i)_p$.

*Demostración.* (1) [$\supseteq$] Sean $x_{i_k} \in t(G_{i_k})$ y $= m_{i_k} \in \mathbb{Z}^+$ tales que $m_{i_k} x_{i_k} = 0$, $1 \leq k \leq n$. Si $x = \sum_{j=1}^{n} x_{i_j} \in G$, entonces $[m_{i_1}, \ldots, m_{i_n}]x = 0$, por lo tanto $x \in t(G)$.

[$\subseteq$] Sean $y \in t(G)$ y $m \in \mathbb{Z}^+$ tal que $my = 0$, como $y = \sum_{j=1}^{r} y_{i_j}$ entonces $\sum_{j=1}^{r} m y_{i_j} = m(\sum_{j=1}^{r} y_{i_j}) = my = 0$ de donde $my_{i_j} = 0$ para toda $j = 1, \ldots, r$, ya que la suma es directa, por lo tanto $y_{i_j} \in t(G_{i_j})$ para toda $j = 1, \ldots, r$; así $y \in \bigoplus_{i \in I} t(G_i)$.

(2) [$\subseteq$] Sea $x \in G_p$ entonces $p^r x = 0$ para alguna $r \in \mathbb{Z}^+$, si $x = \sum_{j=1}^{m} x_{i_j}$, como en el inciso anterior, tenemos que $p^r x_{i_j} = 0$ para cada $j = 1 \ldots, m$. Por lo tanto $x \in \bigoplus_{i \in I}(G_i)_p$

[$\supseteq$] Dado $y = \sum_{j=1}^{k} y_{i_j} \in \bigoplus_{i \in I}(G_i)_p$ sean $p^{r_j} \in \mathbb{Z}^+$ tales que $p^{r_j} y_{i_j} = 0$ para $j = 1, \ldots, k$, entonces $p^{(\sum_{j=1}^{k} r_j)} y = 0$ y por lo tanto $y \in G_p$. ■

**Nota 1.3.16.** *Con los tres resultados previos podemos dar condiciones suficientes para poder resolver los problemas 1, 2 y 3 dados en la introducción para grupos de torsión.*

(1) *Sean $G$ y $H$ grupos de torsión tales que $G = K \oplus H'$ y $H = L \oplus G'$ donde $H' \cong H$ y $G' \cong G$, por el Teorema 1.3.15, (2) $G_p = K_p \oplus H'_p$ y $H_p = L_p \oplus G'_p$ para todo numero primo $p \in \mathbb{Z}^+$. Considerando el Teorema 1.3.13 tenemos que $G = \bigoplus_{p \in \mathscr{P}} G_p$ y como $K \oplus H' = \bigoplus_{p \in \mathscr{P}} (K_p \oplus H'_p)$ es la descomposición en grupos primarios, por la unicidad fuerte tenemos que $G_p = K_p \oplus H'_p$ para toda $p \in \mathscr{P}$. Análogamente obtenemos que $H_p = L_p \oplus G'_p$ para toda $p \in \mathscr{P}$. Por la Proposición 1.3.14 sabemos que $G'_p \cong G_p$ y $H'_p \cong H_p$ para toda $p \in \mathscr{P}$. Así que el problema planteado para grupos de torsión se reduce a solucionar el mismo problema pero para grupos primarios. Así, una condición suficiente para resolver el problema 1 para grupos de torsión es que dicho problema sea válido para grupos primarios.*

(2) *Para el problema 2, suponemos que $G$ y $H$ son grupos de torsión tales que $G \oplus G \cong H \oplus H$. Dado un número primo $p$, la parte $p$-primaria de $G \oplus G$ y $H \oplus H$ es $G_p \oplus G_p$ y $H_p \oplus H_p$ respectivamente, por la Proposición 1.3.14 tenemos que $G_p \oplus G_p \cong H_p \oplus H_p$ para todo número primo. Nuevamente el problema que fue planteado para grupos de torsión se reduce a resolverlo para grupos primarios; al igual que en el problema 1, esto resulta ser una condición suficiente para resolver el caso para grupos de torsión.*

(3) *En el caso del problema 3 supondremos que $G$ y $H$ son grupos de torsión tales que $\mathcal{F} \oplus G \cong \mathcal{F} \oplus H$, donde $\mathcal{F}$ es un grupo finitamente generado. Por el Teorema 1.3.15, (2) sabemos que $\mathcal{F}_p \oplus G_p \cong \mathcal{F}_p \oplus H_p$ y en vista de que $\mathcal{F}$ es finitamente generado, $\mathcal{F}_p$ también lo es para todo primo $p$; así que nuestro problema se ve reducido nuevamente al caso de grupos primarios.*

*En resumen, para resolver los problemas 1,2 y 3, dados en la introducción, para grupos de torsión será suficiente resolverlos para grupos primarios.*

Dado un grupo $G$ y un número primo $p$, definimos

$$\boldsymbol{G[p]} = G_p \cap S(G),$$

recuérdese que $S(G)$ denota el zoclo de $G$ (véase la página 3). En caso de que $G$ sea un grupo $p$-primario, $G[p]$ es el zoclo de $G$. Es claro, a partir de la definición, que

$$G[p] = \{x \in G \mid px = 0\}, \tag{1.13}$$

es decir, $G[p]$ es el conjunto de todos los elementos de $G$ que son anulados por $p$. Como veremos eventualmente, este subgrupo de $G$ "codifica" una gran cantidad de información acerca del grupo $G$. La siguiente proposición proporciona parte de la herramienta que no ayudará a "decodificar" la información que guarda el grupo $G[p]$.

**Proposición 1.3.17.** *Sea $G$ un grupo, entonces el subgrupo $G[p]$ admite una estructura de $\mathbb{Z}_p$-espacio vectorial.*

*Demostración.* Para darle a $G[p]$ la estructura de $\mathbb{Z}_p$-espacio vectorial definimos la multiplicación por escalares $\mathbb{Z}_p \times G[p] \longrightarrow G[p]$ como sigue: $\overline{m}x = mx$, para cada $\overline{m} \in \mathbb{Z}_p$ y cada $x \in G[p]$. Este producto está bien definido, en el sentido de que no depende del representante de $\overline{m}$. En efecto, sean $m, n \in \mathbb{Z}$ tales que $(m - n) = ps$ entonces para cada $x \in G[p]$ $(m - n)x = (ps)x = 0$ y en consecuencia $mx = nx$. Esta forma tan natural de definir la multiplicación hace que sea fácil verificar que $G[p]$ es un $\mathbb{Z}_p$-espacio vectorial. ■

La siguiente proposición nos dice, como es de esperar, que para buscar elementos en un grupo $G$ que son anulados por $p$ basta buscarlos en su parte $p$ primaria.

**Proposición 1.3.18.** *Sea $G$ un grupo, entonces $G[p] = G_p[p]$.*

*Demostración.* [$\subseteq$] Sea $x \in G[p]$, entonces $px = 0$ y por consiguiente $x \in G_p$, más aún $x \in G_p[p]$.

[$\supseteq$] Sea $y \in G_p[p]$, entonces $y \in G_p$ y $py = 0$ por lo tanto $y \in G[p]$. ■

**Teorema 1.3.19.** *Sea $G = \bigoplus_{i \in I} G_i$, donde cada $G_i$ es un grupo. Entonces $G[p] = \bigoplus_{i \in I} G_i[p]$.*

*Demostración.* Que $\sum_{i \in I} G_i[p]$ sea una suma directa es consecuencia de la primera afirmación de la Proposición 1.1.9

[$\subseteq$] Sea $x \in G[p]$, como $G = \bigoplus_{i \in I} G_i$ tenemos que $x = x_{i_1} + x_{i_2} + \cdots + x_{i_m}$ donde $x_{i_k} \in G_{i_k}$, $i_k \in I$ $(1 \leq k \leq m)$, entonces

$$\begin{aligned} px = 0 &\Longrightarrow px_{i_1} + px_{i_2} + \cdots + px_{i_m} = 0 \\ &\Longrightarrow px_{i_j} = 0 \text{ para cada } 1 \leq j \leq m, \end{aligned}$$

esta última implicación se debe a que la suma es directa; así $x_{i_j} \in G_{i_j}[p]$ para cada $i_j$ $(1 \leq j \leq m)$, es decir $x \in \bigoplus_{i \in I} G_i[p]$.

[$\supseteq$] Supongamos que $y_{i_j} \in G_{i_j}[p]$ con $1 \leq j \leq n$ y sea $y = y_{i_1} + \ldots + y_{i_n}$, entonces

$$\begin{aligned} py &= p(y_{i_1} + \ldots + y_{i_n}) \\ &= py_{i_1} + \ldots + py_{i_n} = 0, \end{aligned}$$

por lo tanto $y \in G[p]$. ■

El siguiente teorema muestra el carácter de invariante del zoclo de un grupo.

**Teorema 1.3.20.** *Si $G$ y $H$ son grupos isomorfos. Entonces $S(G)$ es isomorfo a $S(H)$.*

*Demostración.* Sea $\varphi : G \longrightarrow H$ el isomorfismo entre $G$ y $H$. Afirmamos que

$$\varphi|_{S(G)} : S(G) \longrightarrow S(H)$$

es un isomorfismo, en efecto sean $x \in S(G)$ y $m \in \mathbb{Z}^+$ libre de cuadrados tal que $mx = 0$. Como $m\varphi(x) = \varphi(mx) = \varphi(0) = 0$ entonces $\varphi(x) \in S(H)$, lo que implica que $\varphi(S(G)) \subseteq S(H)$. Además $\ker \varphi|_{S(G)}$ es inyectiva pues es la restricción de una función inyectiva; finalmente dado $h \in S(H)$ existe $x \in G$ tal que $\varphi(x) = h$. Si $nh = 0$, con $n \in \mathbb{Z}^+$ libre de cuadrados, entonces $\varphi(nx) = n\varphi(x) = nh = 0$ y como $\varphi$ es inyectiva, $nx = 0$; así $x \in S(G)$. Por lo tanto $S(G) \overset{\varphi|_{S(G)}}{\cong} S(H)$. ■

Como caso particular tenemos el siguiente corolario.

**Corolario 1.3.21.** *Sean $G$ y $H$ grupos $p$-primarios. Si $G$ es isomorfo a $H$ entonces $G[p]$ es isomorfo a $H[p]$.*

Con lo anterior hemos visto que el zoclo de un $p$-grupo es un invariante, sin embargo éste no es completo como lo muestra el siguiente ejemplo.

**Ejemplo 1.3.22.** *Sean $G = \mathbb{Z}_p \oplus \mathbb{Z}_{p^2}$ y $H = \mathbb{Z}_p \oplus \mathbb{Z}_p$. Entonces $G[p] = H = H[p]$; sin embargo $G \ncong H$.*

Continuando con los ejemplos de grupos de torsión, los siguientes forma parte fundamental en el desarrollo de nuestro trabajo; parte de su importancia radica en su naturaleza y como veremos ellos motivarán nuevas definiciones.

## 1.4. Tipos Especiales de Grupos

### 1.4.1. El Grupo Aditivo de los Números Racionales

Comenzamos enunciando un resultado conocido e importante, que en ocasiones se puede ver en un curso de Algebra Moderna I. La demostración puede encontrarse en el capítulo 9, §4 de [Rot].

**Teorema 1.4.1.** *Cualquier grupo finitamente generado tiene una única descomposición, salvo isomorfismos, en una suma directa de grupos cíclicos primarios y grupos cíclicos infinitos, donde el número de factores de grupos cíclicos primarios, para cada primo que aparece en la descomposición, así como el número de factores de grupos cíclicos infinitos sólo dependen de $G$.*

Podríamos conjeturar que, todo grupo es una suma directa de grupos cíclicos, con un número infinito de sumandos posiblemente. No obstante esta proposición tiene una respuesta negativa. El contraejemplo es el grupo aditivo de los números racionales y recordemos que este grupo es denotado por $\mathcal{Q}$. Como $\mathcal{Q}$ no tiene elementos de orden finito, salvo 0, de ser una suma directa de grupos cíclicos, ésta sería de grupos cíclicos libres de torsión, que como sabemos, cada uno de ellos debe ser isomorfo a $\mathcal{Z}$, así necesariamente $\mathcal{Q} \cong \bigoplus_{r_f} \mathcal{Z}$, sin embargo, los números racionales tienen una propiedad que no se cumple en $\bigoplus_{r_f} \mathcal{Z}$. La propiedad en cuestión es la siguiente:

Dado $y \in \mathcal{Q}$ y $m \in \mathbb{Z} - \{0\}$, existe $x \in \mathcal{Q}$ tal que

$$mx = y.$$

En efecto, si $y = \frac{a}{b}$, basta considera $x = \frac{a}{mb}$. Así $\frac{a}{mb}$ es solución de la ecuación anterior, y de hecho es única. De esta manera, cualquier número racional $y$ tiene la propiedad de que para cualquier número entero $m$ la ecuación $mX = y$ siempre tiene una solución en $\mathcal{Q}$, es decir, cualquier número racional es divisible por cualquier entero.

Veamos ahora que dicha propiedad no se cumple en $\bigoplus_{r_f} \mathcal{Z}$. Consideramos primero el grupo $\mathcal{Z}$. Dado el entero $m \neq 0$, éste tiene sólo un número finito de divisores, esto es, existen $x_1, \ldots, x_k \in \mathcal{Z}$ tales que $n_i x_i = m$. Así que el número de enteros que dividen a $m$ en $\mathcal{Z}$ es $k$ que es finito. Por otra parte, el elemento

$$y = m_1 + n_2 + \cdots + m_k \in \bigoplus_{r_f} \mathcal{Z},$$

es divisible por un número entero $n$ si y sólo si $n \mid m_i$ para cada $i = 1, \ldots, k$. Como el número de divisores de cada $m_i$ es finito, suponiendo que cada uno de ellos es distinto de

cero, el número de enteros que pueden dividir a $y$ es finito y por lo tanto $y$ no es divisible por cualquier número entero. Por lo tanto, $\mathcal{Q}$ no es suma directa de copias de $\mathcal{Z}$.

En la sección 2.1 hablaremos con detalle de la propiedad de "divisibilidad" y de los grupos que la poseen.

### 1.4.2. El grupo $\mathcal{Z}_{p^\infty}$

Denotemos por $\mathcal{Q}_p$ al conjunto de todos los números racionales cuyo denominador es una potencia del número primo $p \in \mathbb{Z}^+$. Es decir

$$\mathcal{Q}_p = \left\{ \tfrac{m}{p^r} \mid m \in \mathcal{Z} \text{ y } r \in \mathbb{N} \right\}.$$

**Proposición 1.4.2.** *$\mathcal{Q}_p \leq \mathcal{Q}$.*

*Demostración.* Claramente $0 \in \mathcal{Q}_p$. Sean $\frac{m}{p^r}, \frac{n}{p^s} \in \mathcal{Q}_p$, entonces

$$\tfrac{m}{p^r} - \tfrac{n}{p^s} = \tfrac{mp^s - np^r}{p^{r+s}} \in \mathcal{Q}_p.$$

Por lo tanto $\mathcal{Q}_p \leq \mathcal{Q}$. ■

En virtud de que, para cada número primo $p$ tenemos la inclusión, $\mathcal{Z} \hookrightarrow \mathcal{Q}_p$ , definimos

$$\mathcal{Z}_{p^\infty} = \mathcal{Q}_p/\mathcal{Z}.$$

Echemos un vistazo a este grupo. La primera observación que hacemos es que cada elemento en $\mathcal{Z}_{p^\infty}$ es de orden finito, esto es claro pues $\mathcal{Z}_{p^\infty} < \mathcal{Q}/\mathcal{Z}$ (véase el ejemplo 1.3.5), más aún, su orden es una potencia de $p$, es decir, $\mathcal{Z}_{p^\infty}$ es un grupo $p$-primario. Recíprocamente, supongamos que $\overline{\frac{m}{n}} \in \mathcal{Q}/\mathcal{Z}$, con $(m,n) = 1$, tiene orden $o(\overline{\frac{m}{n}}) = p^r$, entonces

$$\begin{aligned} \overline{0} &= p^r \overline{\tfrac{m}{n}} \\ &= \overline{\tfrac{p^r m}{n}} \end{aligned}$$

de donde $\frac{p^r m}{n} \in \mathcal{Z}$, por lo que $n \mid p^r m$. Así $p^r m = nm$' para algún $m' \in \mathcal{Z}$. Como $(m,n) = 1$ necesariamente $n = p^s$, con $s \leq r$, y por lo tanto $\overline{\frac{m}{n}} = \overline{\frac{m}{p^s}} \in \mathcal{Z}_{p^\infty}$.

**Nota 1.4.3.** *De hecho, podemos decir más acerca de el elemento $\frac{m}{n}$ del párrafo de arriba. Considerando lo anterior y como $p^s(\overline{\frac{m}{n}}) = 0$ entonces $p^r \mid p^s$ y por consiguiente $r \leq s$, es decir, $r = s$. Por lo tanto*

$$n = p^s = p^r \ y \ \frac{m}{n} = \frac{m}{p^r} \ en \ \mathcal{Q}. \tag{1.14}$$

De esta manera, hemos demostrado la siguiente proposición.

**Proposición 1.4.4.** *Para cada número primo $p \in \mathbb{Z}^+$, $(\mathcal{Q}/\mathcal{Z})_p = \mathcal{Z}_{p\infty}$.*

Como corolario de esta proposición y del Teorema 1.3.13 tenemos que

$$\mathcal{Q}/\mathcal{Z} = \bigoplus_{p\in\mathscr{P}} \mathcal{Z}_{p^\infty}, \tag{1.15}$$

donde $\mathscr{P}$ denota al conjunto de todos los números primos.

Continuando con la descripción del grupo $\mathcal{Z}_{p^\infty}$, lo que haremos a continuación es describir todos sus subgrupos.

Los subgrupos más sencillos que podemos encontrar en cualquier subgrupo son lo cíclicos. Consideremos $\overline{\frac{1}{p^r}} \in \mathcal{Z}_{p^\infty}$, el grupo cíclico generado por este elemento es

$$\left\langle \overline{\tfrac{1}{p^r}} \right\rangle = \left\{ \overline{\tfrac{m}{p^r}} \mid m \in \mathbb{Z} \right\}.$$

Una de las características sorprendentes del grupo $\mathcal{Z}_{p\infty}$ es que todos sus subgrupos son como el anterior; para ver esto comenzamos notando lo siguiente. Sean $\overline{\frac{1}{p^r}}, \overline{\frac{1}{p^s}} \in \mathcal{Z}_{p^\infty}$, supongamos sin perdida de generalidad que $r \leq s$, entonces

$$\overline{\tfrac{1}{p^r}} = \overline{\tfrac{p^{s-r}}{p^s}} = p^{s-r}\left(\overline{\tfrac{1}{p^s}}\right),$$

es decir, $\overline{\frac{1}{p^r}} \in \left\langle \overline{\frac{1}{p^s}} \right\rangle$ y por lo tanto

$$\left\langle \overline{\tfrac{1}{p^r}} \right\rangle \leq \left\langle \overline{\tfrac{1}{p^s}} \right\rangle.$$

Recíprocamente, si $\left\langle \overline{\frac{1}{p^r}} \right\rangle \leq \left\langle \overline{\frac{1}{p^s}} \right\rangle$ entonces

$$\overline{\tfrac{1}{p^r}} = m\overline{\tfrac{1}{p^s}} = \overline{\tfrac{m}{p^s}},$$

de donde $\frac{1}{p^r} - \frac{m}{p^s} \in \mathcal{Z}$. Sea $n \in \mathcal{Z}$ tal que $\frac{1}{p^r} - \frac{m}{p^s} = n$, entonces $p^s - p^r m = p^{r+s}n$ lo que implica que $p^s = p^r(p^s n + m)$; así $r \leq s$. De lo anterior se sigue que,

$$\left\langle \overline{\tfrac{1}{p^r}} \right\rangle \leq \left\langle \overline{\tfrac{1}{p^s}} \right\rangle \text{ si y sólo si } r \leq s. \tag{1.16}$$

De este hecho se obtiene que

$$\left\langle \overline{\tfrac{1}{p^r}} \right\rangle < \left\langle \overline{\tfrac{1}{p^s}} \right\rangle \text{ si y sólo si } r < s. \tag{1.17}$$

Consideremos ahora un subgrupo propio $H$ de $\mathcal{Z}_{p^\infty}$. Por ser $H$ propio, existe $a \in \mathcal{Z}_{p^\infty}$, de orden $p^s$, tal que $a \notin H$. Supóngase que $a = \overline{\frac{m}{p^s}} = m\left(\overline{\frac{1}{p^s}}\right)$, esto lo podemos hacer por lo

visto en la Nota 1.4.3. Si $\overline{\frac{1}{p^s}} \in H$ entonces $a = m\left(\overline{\frac{1}{p^s}}\right) \in H$ lo cual es absurdo; así $\overline{\frac{1}{p^s}} \notin H$. Sea

$$p^r = \text{máx}\{o(x) \mid x \in H\},$$

$p^r$ existe ya que si $\{o(x) \mid x \in H\}$ no tiene máximo entonces $H$ tendría elementos de orden cualquier potencia de $p$, en particular de orden $p^s$. Si $y \in H$ es de orden $p^s$, entonces de la Nota 1.4.3, $y = \overline{\frac{b}{p^s}} = b\left(\overline{\frac{1}{p^s}}\right)$ para algún $b \in \mathcal{Z}$, con $(b, p) = 1$. Sean $m_1, m_2 \in \mathbb{Z}$ tales que $1 = m_1 b + m_2 p^s$, entonces

$$\begin{aligned}\overline{\frac{1}{p^s}} &= \overline{\frac{m_1 b + m_2 p^s}{p^s}} \\ &= \overline{\frac{m_1 b}{p^s}} + \overline{\frac{m_2 p^s}{p^s}} \\ &= \overline{\frac{m_1 b}{p^s}} \\ &= m_1\left(\overline{\frac{b}{p^s}}\right),\end{aligned}$$

es decir, $\overline{\frac{1}{p^s}} \in H$ lo cual es absurdo. Por lo tanto $p^r$ sí existe.

Sea $\overline{\frac{c}{p^r}} \in H$, de orden $p^r$. Nuevamente, como $(c, p) = 1$, $\overline{\frac{1}{p^r}} \in H$ y por lo tanto $\left\langle \overline{\frac{1}{p^r}} \right\rangle \leq H$. Si $\left\langle \overline{\frac{1}{p^r}} \right\rangle < H$, debe existir $y \in H$ tal que $y \notin \left\langle \overline{\frac{1}{p^r}} \right\rangle$. Si $o(y) = p^t$, de la Nota 1.4.3 y de (1.17) tendríamos que $r < t$ y por consiguiente $p^r < p^t = o(y)$ lo que contradice la elección de $p^r$. Por lo tanto debe ser $H = \left\langle \overline{\frac{1}{p^r}} \right\rangle$.

Resumimos estos resultados en la siguiente proposición.

**Proposición 1.4.5.** *Todos los subgrupos propios de $\mathcal{Z}_{p^\infty}$ son de la forma $\left\langle \overline{\frac{1}{p^n}} \right\rangle$, con $n \in \mathbb{N}$ y estos subgrupos forman la siguiente sucesión ascendente*

$$0 < \left\langle \overline{\tfrac{1}{p}} \right\rangle < \left\langle \overline{\tfrac{1}{p^2}} \right\rangle < \cdots < \left\langle \overline{\tfrac{1}{p^n}} \right\rangle < \cdots < \mathcal{Z}_{p^\infty}. \tag{1.18}$$

En virtud de (1.18) tenemos que $\bigcup_{n\in\mathbb{N}} \left\langle \overline{\frac{1}{p^n}} \right\rangle \leq \mathcal{Z}_{p^\infty}$, más aún, dado $x \in \mathcal{Z}_{p^\infty}$, como $\langle x \rangle \leq \mathcal{Z}_{p^\infty}$, entonces $\langle x \rangle = \left\langle \overline{\frac{1}{p^r}} \right\rangle$ para algún $r \in \mathbb{N}$ y por consiguiente $x \in \left\langle \overline{\frac{1}{p^r}} \right\rangle \subset \bigcup_{n\in\mathbb{N}} \left\langle \overline{\frac{1}{p^n}} \right\rangle$. Por lo tanto

$$\mathcal{Z}_{p^\infty} = \bigcup_{n\in\mathbb{N}} \left\langle \overline{\tfrac{1}{p^n}} \right\rangle. \tag{1.19}$$

Hemos dado varias propiedades del grupo $\mathcal{Z}_{p^\infty}$, la primera es que es un grupo $p$-primario y que cada subgrupo es de la forma $\left\langle \overline{\frac{1}{p^n}} \right\rangle$ para alguna $n \in \mathbb{N}$. Además ellos forma la cadena ascendente dada en (1.18) y de este hecho pudimos comprobar la igualdad (1.19). De lo anterior podemos verificar las siguientes relaciones:

$$p(\overline{\tfrac{1}{p}}) = \overline{0}, \text{ y } p(\overline{\tfrac{1}{p^{n+1}}}) = \overline{\tfrac{1}{p^n}} \text{ para toda } n \in \mathbb{N}.$$

No obstante tenemos otra caracterización de este grupo, que en realidad es una abstracción de las propiedades antes mencionadas.

**Proposición 1.4.6.** *Sea $G$ el grupo generado por la familia $\{x_n\}_{n\in\mathbb{N}}$ cuyos elementos satisfacen las siguientes relaciones*

$$x_1 \neq 0,\ px_1 = 0,$$

$$\textit{en forma recursiva, } px_{n+1} = x_n \textit{ para } n > 0.$$

*Entonces $G$ es isomorfo a $\mathcal{Z}_{p^\infty}$.*

*Demostración.* Consideremos $n \in \mathbb{N}$ con $n > 1$. De las relaciones tenemos que para cada $m \leq n$

$$p^{n-m}x_n = x_m. \tag{1.20}$$

Además, $p^n x_n = p^{1+n-1}x_n = p(p^{n-1}x_n) = px_1 = 0$; así para cada $n \in \mathbb{N}$,

$$o(x_n) \mid p^n.$$

Como $o(x_n)x_n = 0$ multiplicando esta igualdad por $p^{n-1}$, y considerando (1.20), tenemos que $o(x_n)x_1 = o(x_n)p^{n-1}x_n = 0$ lo cual sólo es posible si $p \mid o(x_n)$; así $o(x_n) = q_1 p$ para algún $q_1 \in \mathbb{Z}$, y por lo tanto $q_1 x_{n-1} = q_1(px_n) = o(x_n)x_n = 0$. Nuevamente, multiplicando $q_1 x_{n-1} = 0$ por $p^{n-2}$ obtenemos que $q_1 x_1 = 0$ y en consecuencia $p \mid q_1$, entonces $q_1 = q_2 p$ para algún $q_2 \in \mathbb{Z}$ y $o(x_n) = q_2 p^2$. Siguiendo con este razonamiento encontramos que

$$p^n \mid o(x_n),$$

y por lo tanto $o(x_n) = p^n$.

Sea $x \in G - \{0\}$, entonces

$$x = m_1 x_{i_1} + m_2 x_{i_2} + \cdots + m_k x_{i_k},$$

donde estamos suponer que $p \nmid m_j$ para cada $j = 1, \ldots, k$. Sin pérdida de generalidad podemos admitir que $n = i_k = \text{máx}\{i_l \mid 1 \leq l \leq k\}$, por (1.20) tenemos que

$$x = (m_1 p^{n-i_1} + \cdot + m_{k-1}p^{n-i_{k-1}} + m_k)x_n.$$

Sea $m = \sum_{l=1}^{k-1} m_l p^{n-i_l}$; $p \nmid m$ pues de lo contrario, necesariamente $p \mid m_k$ lo cual es absurdo. Hemos visto que para cada $x \in G - \{0\}$ existen $n \in \mathbb{N}$ y $m \in \mathbb{Z}$ con $(m, p) = 1$ tales que

$$x = mx_n. \tag{1.21}$$

Si existe $m' \in \mathbb{Z}$, $(m', p) = 1$, tal que $x = m'x_n$ entonces $(m' - m)x_n = 0$ y en consecuencia $p^n \mid (m' - m)$, es decir, $m' = m + qp^n$ para algún $q \in \mathbb{Z}$. Esto es, $m$ está unívocamente determinada salvo un múltiplo entero de $p^n$. Por otra parte $x \notin \langle x_{n-1} \rangle$, pues de no ser así $x = rx_{n-1}$ y entonces $mx_n = rx_{n-1} = rpx_n$, de donde $(m - rp)x_n = 0$, es decir, $p^n \mid (m - rp)$ y por lo tanto $p \mid m$, lo cual es absurdo. Por lo tanto $x \in \langle x_n \rangle - \langle x_{n-1} \rangle$.

Resumiendo, cada $x \in G$ se puede escribir de forma única como $x = mx_n$ para alguna $n \in \mathbb{N}$, con $0 \leq m < p$ y si $x \neq 0$ entonces

$$x \in \langle x_n \rangle - \langle x_{n-1} \rangle \,. \tag{1.22}$$

De la discusión anterior resulta natural definir $\varphi : G \longrightarrow \mathcal{Z}_{p^\infty}$ en los generadores como $\varphi(x_n) = \overline{\frac{1}{p^n}}$. Veamos que $\varphi$ esta bien definida, en el sentido de que las relaciones se mantienen bajo $\varphi$. Sea $n > 1$, claramente $\varphi(x) \neq \overline{0}$. Por otra parte,

$$p\varphi(x_n) = p\overline{\tfrac{1}{p^n}} = \overline{\tfrac{p}{p^n}} = \overline{\tfrac{1}{p^{n-1}}} = \varphi(x_{n-1}).$$

Además $\overline{0} = \overline{1} = \overline{\frac{p}{p}} = p\overline{\frac{1}{p}} = p\varphi(x_1)$. Así, hemos visto que

$$\varphi(x_1) \neq \overline{0},\ p\varphi(x_1) = \overline{0},$$

$$\text{en forma recursiva, } p\varphi(x_{n+1}) = \varphi(x_n) \text{ para } n > 0.$$

Por lo tanto $\varphi$ manda generadores en generadores y relaciones en relaciones. Veamos ahora que $\varphi$ es un isomorfismo. Sea $x \in \ker \varphi$ y supongamos que $x = mx_n$, entonces $\overline{\frac{m}{p^n}} = \overline{0}$ y por consiguiente existe $r \in \mathbb{Z}$ tal que $\frac{m}{p^n} = r$, es decir $m = rp^n$ y por lo tanto $x = mx_n = (rp^n)x_n = n(p^n x_n) = 0$ y así $\ker \varphi = 0$. Para verificar que $\varphi$ es suprayectiva basta mostrar que los generadores $\overline{\frac{1}{p^n}} \in \mathcal{Z}_{p^\infty}$ están en la imagen de $\varphi$ para cada $n \in \mathbb{N}$. Dado $\overline{\frac{1}{p^n}} \in \mathcal{Z}_{p^\infty}$, $x_n \in G$ satisface que $\varphi(x_n) = \overline{\frac{1}{p^n}}$ y por lo tanto $\varphi$ es suprayectiva; note que aquí se usa fuertemente la igualdad (1.19). Por lo tanto $G \overset{\varphi}{\cong} \mathcal{Z}_{p^\infty}$. ■

La caracterización anterior del grupo $\mathcal{Z}_{p^\infty}$ será de gran utilidad en el teorema de clasificación de grupos abelianos divisibles, lo cual veremos a continuación.

# Capítulo 2

# Descomposición de Grupos

En la primera sección del presente capítulo abordamos la noción de *grupo divisible*, un clase de grupos sumamente importante en el estudio de clasificación de grupos abelianos, entre otras cosas veremos que, *dado un grupo (abeliano) existe un grupo divisible que lo contiene*. Este resultado tiene una consecuencia que es parte fundamental en la caracterización de grupo divisible, dicho resultado afirma que, *un grupo divisible es sumando directo de cualquier grupo que lo contiene*. También daremos el teorema de clasificación de dichos grupos, e introducimos los invariantes que los determinan. Las siguientes tres secciones están dedicadas a encontrar condiciones bajo las cuales un grupo puede ser descrito como una suma directa de cierta clase de subgrupos. Como mencionamos antes, un grupo divisible es sumando directo de cualquier grupo en el cual este contenido; una de las metas de dichas secciones será encontrar algo equivalente para poder encontrar sumandos directos de un grupo dado. Es así que en la sección 2.2 introducimos una noción de subgrupo más débil a la de subgrupo divisible, a saber la de *subgrupo puro*. Estudiaremos bajo qué condiciones esta clase de subgrupos son sumandos directos. En la sección 2.3 estudiamos las condiciones que debe cumplir un grupo para que éste sea una suma directa de grupos cíclicos; así como las relaciones que debe tener dicho grupo con sus subgrupos puros para producir sumandos directos. En la sección 2.4 se retoma la noción de divisibilidad introduciendo una medida numérica de dicha propiedad, a saber la *altura*, y como veremos ésta resulta ser crucial en nuestro estudio de clasificación. En la sección 2.5, como su nombre lo dice, estudiamos las sumas directas de grupos cíclicos, logrando dar condiciones necesarias y suficientes para que un grupo pueda ser expresado como una suma directa de grupos cíclicos.

## 2.1. Grupos Divisibles

En esta sección estudiaremos aquellos grupos que como $\mathcal{Q}$ tienen la propiedad de que cada uno de sus elementos es "divisible" por cualquier número entero (véase la Sección 1.4.1).

**Definición 2.1.1.** *Sea $y$ un elemento de un grupo $G$ y $n \in \mathbb{Z}^+$; decimos que* ***n divide a y*** *ó que* ***y es divisible por n*** *si existe $x \in G$ tal que*

$$nx = y. \tag{2.1}$$

Es claro que (2.1) es equivalente a que $y \in nG$.[1]

**Ejemplo 2.1.2.**

*a) Sea $G$ un grupo. El elemento neutro $0 \in G$ es divisible por cualquier entero.*

*b) Todo elemento de $\mathcal{Q}$ es divisible por cualquier número entero.*

La siguiente proposición enlista algunas consecuencias inmediatas de la definición 2.1.1.

**Proposición 2.1.3.** *(a) Si $n \in \mathbb{Z}^+$ divide a $y \in G$ entonces $-n$ divide a $y$.*

*(b) Si $x = w$ es una solución de (2.1) entonces la clase lateral $a + G[n]$ [2] es el conjunto de todas las soluciones de (2.1).*

*(c) Si $G$ es libre de torsión entonces la ecuación (2.1) tiene a lo más una solución.*

*(d) Si $y \in G$ y $o(y) = m$, entonces cualquier entero $n$ primo con $m$ divide a $y$.*

*(e) Sean $G$ un grupo, $y \in G$. Si $m$ y $n$ dividen a $y$ entonces $[m, n]$, el mínimo común múltiplo de $m$ y $n$, divide a $y$.*

*Demostración.* (a) Sea $a' \in G$ tal que $na' = y$; considerando $a = -a' \in G$ tenemos que

$$(-n)a = (-n)(-a') = (-(-n))a' = na' = y.$$

(b) Claramente si $a' \in a + G[n]$ entonces $a'$ es solución de (2.1). Recíprocamente, si $a'$ es una solución de (2.1) entonces $na' = na$ y por consiguiente $n(a' - a) = 0$, es decir $(a' - a) \in G[n]$ y por lo tanto $a' \in a + G[n]$.

[1] $nG = \{nx \mid x \in G\}$.

[2] Análogo a la Definición 1.13, $G[n] = \{x \in G \mid nx = 0\}$, es un subgrupo de $G$.

($c$) Si $a$ y $a$' son soluciones de (2.1) entonces $na$' $= na$ y por consiguiente $n(a' - a) = 0$. Como $G$ es libre de torsión y $(a' - a) \in G[n] = 0$ entonces $a' = a$.

($d$) Al ser $(m, n) = 1$ existen enteros $a, b$ tales que

$$am + bn = 1, \tag{2.2}$$

multiplicando por $y$ la identidad (2.2), y considerando que $my = 0$, tenemos que $n(by) = y$.

($e$) Sean $a, a' \in G$ tales que $ma = y$ y $na' = y$ y sea $d = (m, n) = r_1 m + r_2 n$, entonces

$$\begin{aligned}
[m, n](r_1 a' + r_2 a) &= \tfrac{mn}{d}(r_1 a' + r_2 a) \\
&= \tfrac{r_1 m}{d} na' + \tfrac{r_2 n}{d} ma \\
&= (\tfrac{r_1 m}{d} + \tfrac{r_2 n}{d}) y \\
&= \tfrac{r_1 m + r_2 n}{d} y \\
&= y.
\end{aligned}$$

■

**Definición 2.1.4.** *Un grupo $G$ se llama **divisible** si para cada elemento $x \in G$ y cada $n \in \mathbb{Z}^+$, $n$ divide a $x$.*

**Nota 2.1.5.** *El inciso ($a$) de la Proposición 2.1.3 asegura que, si $G$ es divisible entonces para todo $n \in \mathbb{Z} - \{0\}$, $nG = G$.*

**Proposición 2.1.6.** *La imagen bajo un homomorfismo de un grupo divisible es un grupo divisible.*

*Demostración.* Sea $\varphi : D \longrightarrow G$ un homomorfismo de grupos, donde $D$ es divisible. Sea $y \in \varphi(D)$ y $n \in \mathbb{Z}$. Sea $x \in D$ tal que $\varphi(x) = y$, como $D$ es divisible existe $a \in D$ tal que $na = x$, entonces $n\varphi(a) = \varphi(na) = \varphi(x) = y$. Como $\varphi(a) \in \varphi(D)$ se sigue que $\varphi(D)$ es un grupo divisible. ■

Como un corolario de esta proposición tenemos:

**Corolario 2.1.7.** *Si $G$ es un grupo divisible y $H \leq G$ entonces $G/H$ es divisible.*

*Demostración.* $G/H$ es la imagen del homomorfismo canónico $p : G \longrightarrow G/H$ . Por la Proposición 2.1.6 $G/H$ es divisible. ■

A su vez, este corolario nos muestra que los racionales módulo uno $\mathcal{Q}/\mathcal{Z}$ del ejemplo 1.3.5 forman un grupo divisible.

La Proposición 2.1.6 sugiere la siguiente definición.

**Definición 2.1.8.** *Un subgrupo $H$ de un grupo $G$ es **divisible** si al considerar a $H$ como grupo éste es divisible. Es decir, para todo $h \in H$ y todo $n \in \mathbb{Z}$ existe $h' \in H$ tal que $nh' = h$.*

**Nota 2.1.9.** *Ni $\mathcal{Z}$ ni $\mathcal{Z}_n$, para toda $n \in \mathbb{N}$, son grupos divisibles. Así, una consecuencia más de la Proposición 2.1.6, es que los grupos cíclicos no son grupos divisibles.*

De hecho, tampoco la suma directa de grupos cíclicos es un grupo divisible; el siguiente resultado así lo muestra; más aún da condiciones necesarias y suficientes para que una suma directa de grupos sea divisible.

**Teorema 2.1.10.** *Sea $\mathscr{F} = \{G_i\}_{i\in I}$ una familia de grupos. El grupo $G = \bigoplus_{i\in I} G_i$ es divisible si y solo sí $G_i$ es divisible para cada $i \in I$.*

*Demostración.* Supóngase que $\mathscr{F}$ es una familia de grupos divisibles. Sea $n \in \mathbb{Z}$ y $y \in G = \bigoplus_{i\in I} G_i$, supongamos que $y = \sum_{j=1}^{k} y_{i_j}$. Como cada $G_{i_j}$ es divisible, para cada $1 \leq j \leq k$, dado $n \in \mathbb{Z}$ existen $x_{i_j} \in G_{i_j}$ tales que $nx_{i_j} = y_{i_j}$, $1 \leq j \leq k$, considerando $x = \sum_{j=1}^{k} x_{i_j} \in G$ tenemos que $nx = y$. Por lo tanto $G$ es un grupo divisible.

Recíprocamente, supongamos que $G$ es un grupo divisible y sean $y \in G_j$, con $j \in I$ y $n \in \mathbb{Z}$. Consideremos $(y_i)_{i\in I} \in G$ definido como sigue:

$$y_i = \begin{cases} y \text{ si } i = j \\ \\ 0 \text{ si } i \neq j \end{cases}$$

Como $G$ es divisible, dado $(y_i)_{i\in I} \in G$ y $n \in \mathbb{Z}$, existe $(x_i)_{i\in I} \in G$ tal que $n(x_i)_{i\in I} = (y_i)_{i\in I}$, es decir, $(nx_i)_{i\in I} = (y_i)_{i\in I}$; así existe $n_j \in G_j$ tal que $nx_j = y$ y por lo tanto $G_j$ es divisible para cada $j \in I$. ■

Este teorema proporciona una demostración más del hecho de que el grupo $\bigoplus_{r_f} \mathcal{Z}$ del primer ejemplo en 1.4.1 no es divisible. Además, a partir del Teorema 2.1.10 y de (1.15) obtenemos que $\mathcal{Z}_{p^\infty}$ es un grupo divisible para cada número primo $p$.

Para hacer más clara la demostración del siguiente teorema, el cual proporcionará parte de una caracterización de los grupos divisibles, presentamos el siguiente lema preliminar.

**Lema 2.1.11.** *Sea $H$ un subgrupo divisible de un grupo $G$ y $L$ un subgrupo de $G$ tal que $H \oplus L < G$. Sea $x \in G - (H + L)$. Si existe un número primo $p \in \mathbb{Z}^+$ tal que $px \in L$, entonces $H \cap (L + \langle x \rangle) = 0$.*

*Demostración.* Denotamos por $L' = L + \langle x \rangle$. Sea $p \in \mathbb{Z}^+$ un número primo tal que $px \in L$ y sea $h \in H \cap L'$. Por ser $h$ un elemento de $L'$, tenemos que, para alguna $n \in \mathbb{Z}$

$$h = l + nx. \tag{2.3}$$

Si $p \mid n$, entonces $n = rp$ para alguna $r \in \mathbb{Z}^+$; así $h = l + r(px) \in L$ y por lo tanto $h = 0$. Si $(n, p) = 1$ entonces, por la identidad de Bezout, $1 = sn + tp$, con $s, t \in \mathbb{Z}$, de donde

$$\begin{aligned} x &= s(nx) + t(px) \\ &= sh + (-sl + t(px)) \in H + L \end{aligned}$$

que es una contradicción, pues $x \notin H + L$. Por lo tanto $(n, p) \neq 1$ y

$$H \cap L' = (0).$$

■

**Teorema 2.1.12.** *Cualquier subgrupo divisible de un grupo es un sumando directo.*

*Demostración.* Sea $G$ un grupo y $H \leq G$ un subgrupo divisible. En la demostración utilizaremos el Lema de Zorn para poder encontrar un complemento directo para $H$. Sea $\mathscr{A} = \{L \leq G \mid H \cap L = 0\}$. $\mathscr{A} \neq \varnothing$ pues $0 \in \mathscr{A}$. $(\mathscr{A}, \subseteq)$ es entonces un conjunto parcialmente ordena al cual aplicaremos el Lema de Zorn. Si $\mathscr{C}$ es una cadena en $\mathscr{A}$ considerando $M = \bigcup_{L \in \mathscr{C}} L$ tenemos que $H \cap M = \bigcup_{L \in \mathscr{C}} (H \cap L) = 0$, es decir, $M \in \mathscr{A}$ y como $L \subseteq M$ para toda $L \in \mathscr{C}$ entonces $M$ es una cota superior en $\mathscr{A}$.

Así, por el Lema de Zorn, existe $K$ un elemento maximal en $\mathscr{A}$; veamos que $H + K = G$. Si $H + K < G$ y $x \in G - (H + K)$, como $x \notin K$, sí $K' = K + \langle x \rangle$ entonces $K \subsetneq K'$ y por la maximalidad de $K$ tenemos que $H \cap K' \neq 0$. Sea $h \in H \cap K'$, $h \neq 0$, entonces al ser $h$ un elemento de $K'$ existe $n \in \mathbb{Z} - \{0\}$ tal que

$$h = k + nx, \tag{2.4}$$

es decir,

$$nx = h - k \in H + K. \tag{2.5}$$

Sea $m \in \mathbb{Z}^+$ el mínimo con la propiedad de que $mx$ satisface (2.5) y sea $p \in \mathbb{Z}^+$ un primo tal que $p \mid m$, entonces por la elección de $m$

$$y = \left(\frac{m}{p}\right) x \notin H + K. \tag{2.6}$$

Sin embargo $py = mx \in H + K$. Ahora como $H$ es divisible, existe $h' \in H$ tal que $ph' = h$ y por (2.4), $p(y - h') = -k$. Si $z = h' - y$, entonces $pz \in K$ y $z \notin H + K$, pues de lo contrario $y - h' \in H + K$ lo que implica que $y \in H + K$ contradiciendo (2.6). Así hemos construido un elemento $z \in G - (H + K)$ para el cual existe un número primo $p$ con la propiedad de que $pz \in K$. Luego considerando $K'' = K + \langle z \rangle$ tenemos que $K \subsetneq K''$ y por el Lema 2.1.11 $K'' \in \mathscr{A}$ que es absurdo pues $K$ es maximal en $\mathscr{A}$. Por lo tanto no existe $x \in G - (H + K)$ y tenemos así que $H + K = G$. Por lo tanto $G = H \oplus K$. ■

Es posible dar demostraciones más "elegantes" del Teorema 2.1.12 pero hemos elegido la anterior pues en ella se muestra cómo se trabaja con los elementos del grupo, así como con el Lema de Zorn.

A continuación damos algunas equivalencias de grupo divisible. Para lo cual será necesaria la siguiente definición y los siguiente resultados.

**Definición 2.1.13.** *Un grupo $F$ es **libre** si es una suma directa de grupos cíclicos infinitos. Si estos grupos cíclicos están generados por los elementos $x_i$ $(i \in I)$, entonces el grupos libre es*

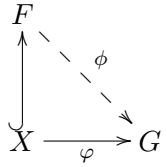
$$F = \bigoplus_{i \in I} \langle x_i \rangle .$$

El conjunto $X = \{x_i\}_{i \in I}$ se llama *conjunto libre de generadores* de $F$ o *base* de $F$. Así $F$ también es llamado *el grupo libre en el conjunto $X$ o con base $X$.*

**Nota 2.1.14.** *Denotamos como $F_{\mathfrak{m}}$ al grupo libre abeliano $F$ con $\mathfrak{m}$ generadores, ($\mathfrak{m}$ un cardinal). Se verifica que dos grupos libres abelianos $F_{\mathfrak{m}}$ y $F_{\mathfrak{n}}$ son isomorfos si y sólo si $\mathfrak{m} = \mathfrak{n}$ (véase por ejemplo [Fu], Cap. 3). Como consecuencia de esto tenemos que, cualesquiera dos bases de un grupos libre abeliano $F$ tienen al misma cardinalidad. Así, se sigue inmediatamente de la definición 2.1.13 que, si $F$ es un grupo libre abeliano entonces $F \cong \bigoplus_{r_l} \mathcal{Z}$, donde $r_l$ es el cardinal de una base.*

La siguiente proposición caracteriza los grupos libres.

**Proposición 2.1.15.** *Sea $F$ un grupo libre abeliano con base $X$. Si $G$ es un grupo y $\varphi : X \longrightarrow G$ una función, entonces existe un único homomorfismo $\phi : F \longrightarrow G$ tal que $\phi|_X = \varphi$, es decir, el siguiente diagrama conmuta.*



*Demostración.* Cada elemento $x \in F$ se escribe de forma única como $x = \sum_{j=1}^{k} m_j x_{i_j}$; así definimos $\phi(x) = \sum_{j=1}^{k} m_j \varphi(x_{i_j})$. Nuevamente, la unicidad de la expresión de $x$ garantiza que $\phi$ esta bien definida y satisface las condiciones que afirmamos. Finalmente $\phi$ es única pues si $\phi$' es una homomorfismo con la propiedad de que $\phi'|_X = \varphi$ entonces para cada $x \in F$ tenemos que

$$\begin{aligned} \phi'(x) &= \phi'(\sum_{j=1}^{k} m_j x_{i_j}) \\ &= \sum_{j=1}^{k} m_j \phi'(x_{i_j}) \\ &= \sum_{j=1}^{k} m_j \varphi(x_{i_j}) \\ &= \phi(x) \end{aligned}$$

es decir, $\phi(x)' = \phi(x)$ para toda $x \in F$. Por lo tanto $\phi' = \phi$. ■

La clase de grupos libres abelianos resulta importante entre otras cosas porque con ella podemos comenzar a estudiar la estructura de los grupos abelianos, como lo muestra el siguiente teorema.

**Teorema 2.1.16.** (*i*) *Cualquier grupo abeliano $G$ es isomorfo a un grupo cociente de la forma $F/K$ donde $F$ es un grupo libre abeliano.*

(*ii*) *Cualquier grupo abeliano $G$ está incluido en un grupo divisible.*

*Demostración.* [(*i*)] Para ver esto consideremos un grupo $G$ y $X$ un subconjunto de $G$, denotaremos al conjunto de todas las funciones $f : X \longrightarrow \mathcal{Z}$ tal que $sop(f)$ es finito (véase la página 4) como $\mathcal{Z}^{(X)}$. No es difícil verificar que $\mathcal{Z}^{(X)}$, con la suma puntual de funciones, es un grupo abeliano. Consideremos a $X \subseteq G$ como un conjunto de generadores de $G$ (es posible que $X = G$), sea $\delta_x : X \longrightarrow \mathcal{Z}$ definida como

$$\delta_x(y) = \begin{cases} 1 \text{ si } y = x \\ \\ 0 \text{ si } y \neq x, \end{cases}$$

claramente $\delta_x \in \mathcal{Z}^{(X)}$ para toda $x \in X$. Veamos que $\{\delta_x\}_{x \in X}$ genera $\mathcal{Z}^{(X)}$. Sea $\varphi \in \mathcal{Z}^{(X)}$, como queremos demostrar que $\varphi \in \langle \delta_x \rangle_{x \in X}$, basta encontrar enteros $m_x$, casi todos cero, tales que $\varphi = \sum m_x \delta_x$. Suponiendo que esto sucede, para $y \in X$ se debe tener $\varphi(y) = \sum m_x \delta_x(y) = m_y$. Por lo tanto

$$\varphi = \sum_{x \in X} \varphi(x) \delta_x \in \langle \delta_x \rangle_{x \in X},$$

y así $\langle \delta_x \rangle_{x\in X} = \mathcal{Z}^{(X)}$. No es difícil ver que, $\mathcal{Z}^{(X)}$ es un grupo libre con base $\{\delta_x\}_{x\in X}$ ($\mathcal{Z}^{(X)} = \bigoplus_{x\in X} \langle \delta_x \rangle$).

A partir de lo anterior resulta natural definir $f : \{\delta_x\}_{x\in X} \longrightarrow G$ dada por $f(\delta_x) = x$; la Proposición 2.1.15 asegura que existe un único homomorfismo $\widehat{f} : \mathcal{Z}^{(X)} \longrightarrow G$ tal que el siguiente diagrama conmuta

$$\begin{array}{ccc} \mathcal{Z}^{(X)} & & \\ \uparrow{\scriptstyle i} & \searrow^{\widehat{f}} & \\ \{\delta_x\}_{x\in X} & \xrightarrow[f]{} & G \end{array}$$

es decir, $\widehat{f} \circ i = f$ o bien $\widehat{f}|_{\{\delta_x\}_{x\in X}} = f$. Además es $\widehat{f}$ suprayectiva, ya que $G = \langle X \rangle$. Así, por el primer teorema de isomorfismos tenemos que

$$G \cong \mathcal{Z}^{(X)} / \ker \widehat{f}, \tag{2.7}$$

lo que demuestra $(i)$.

$[(ii)]$ Sin perdida de generalidad suponemos que $G$ satisface (2.7). Así, a partir de el isomorfismo en (2.7) y de la Nota 2.1.14 obtenemos que

$$G \cong (\bigoplus_{|X|} \mathcal{Z})/K,$$

donde $K$ es la imagen de $\ker \widehat{f}$ bajo el isomorfismo de $\mathcal{Z}^{(X)}$ con $\bigoplus_{|X|} \mathcal{Z}$. Como

$$(\bigoplus_{|X|} \mathcal{Z})/K \overset{i}{\hookrightarrow} (\bigoplus_{|X|} \mathcal{Q})/K,$$

($i$ la inclusión natural) finalmente tenemos que

$$G \hookrightarrow (\bigoplus_{|X|} \mathcal{Q})/K, \tag{2.8}$$

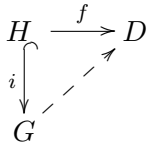
con $(\bigoplus_{|X|} \mathcal{Q})/K$ es un grupo divisible, debido al Teorema 2.1.10 y al Corolario 2.1.7. ■

**Proposición 2.1.17.** *Sea $D$ un grupo, las siguientes condiciones son equivalentes:*

*(a) $D$ es divisible.*

*(b) $D$ es un sumando directo de cualquier grupo que lo contiene.*

*(c) Sea $G$ es un grupo, $H$ un subgrupo de $G$ y $f : H \longrightarrow D$ un homomorfismo, entonces $f$ puede extenderse a un homomorfismo de $G$ en $D$, en diagrama*




*Demostración.* Veremos que $(a) \Rightarrow (c) \Rightarrow (b) \Rightarrow (a)$.

$[(a) \Rightarrow (c)]$ Sean $G$ un grupo y $H$ un subgrupo de $G$ tal que existe un homomorfismo $f : H \longrightarrow D$ . Si $H = G$ no hay nada que demostrar. Sean $x \in G - H$, veremos primero que es posible extender $f$ a $H' = H + \langle x \rangle$. Si $H \cap \langle x \rangle = 0$ entonces $H' = H \oplus \langle x \rangle$ y en este caso definimos

$$f' : H' \longrightarrow D$$
$$h + mx \longmapsto f(h) + ma$$

donde $a \in D$ es un elemento fijo. $f'$ esta bien definida pues la expresión de $h + mx$ es única. Además si $(h + mx), (h' + m'x) \in H'$ entonces $f'((h + mx) + (h' + m'x)) = f'((h + h') + (m + m')x) = f(h + h') + (m + m')a = (f(h) + f(h')) + (ma + m'a) = (f(h) + ma) + (f(h') + m'a) = f'(h + mx) + f'(h' + m'x)$, es decir, $f'$ es un homomorfismo y claramente $f'|_H = f$.

Supongamos ahora que $H \cap \langle x \rangle \neq 0$. Sea $m = \text{mín}\{n \in \mathbb{Z}^+ \mid nx \in H \cap \langle x \rangle\}$. Si $nx \in H \cap \langle x \rangle$ entonces $m$ divide a $n$ (en $\mathbb{Z}$) ya que por el algoritmo de la división, $n = qm + r$ donde $0 \leq r < m$ y como $rx = (n - qm)x = nx - q(mx) \in H \cap \langle x \rangle$ necesariamente $r = 0$. Como $mx \in H$ entonces $f(mx) \in D$; al ser $D$ divisible dados $f(mx)$ y $m$ existe $a \in D$ tal que $ma = f(mx)$. Definimos $f' : H' \longrightarrow D$ dada como sigue. Si $y \in H'$ y $y = h + nx$, $f'(y) = f(h) + na$. Para ver que $f'$ esta bien definida, basta demostrar que $\varphi$ está definida en $H \cap \langle x \rangle$. Supóngase que $h = nx \in H \cap \langle x \rangle$ y que $n = qm$. Considerando $h \in H$ tenemos que $f'(h) = f(h) = f(nx) = f(q(mx)) = qf(mx) = q(ma) = na = f'(nx)$. Por lo tanto $f'$ está bien definida. Claramente $f'$ es un homomorfismo de grupos y además $f'|_H = f$.

Para dar el homomorfismo de $G$ en $D$ consideramos el siguiente conjunto

$$\mathscr{A} = \{(S, \varphi) \mid S \leq G,\ S \supseteq H,\ \ \varphi : S \longrightarrow D \text{ es un homomorfismo de grupos y } \varphi|_H = f\}.$$

$\mathscr{A} \neq \varnothing$ ya que $(H, f) \in \mathscr{A}$. Definimos en $\mathscr{A}$ la siguiente relación:

$$(S_i, \varphi_i) \preccurlyeq (S_j, \varphi_j) \text{ si y sólo si } S_i \subseteq S_j \text{ y } \varphi_j|_{S_i} = \varphi_i.$$

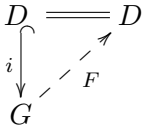
Claramente $(\mathscr{A}, \preccurlyeq)$ es un conjunto parcialmente ordenado. Veamos que $(\mathscr{A}, \preccurlyeq)$ satisface las hipótesis del Lema de Zorn. Sea $\mathscr{C} = \{(S_i, \varphi_i)\}_{i\in I}$ una cadena en $\mathscr{A}$. Consideramos $S = \bigcup_{i\in I} S_i$ el cual es un subgrupo de $G$ pues al ser $\mathscr{C}$ una cadena, $\{S_i\}_{i\in I}$ también lo es. Definimos

$$\begin{aligned} \varphi : S &\longrightarrow D \\ s &\longmapsto \varphi_j(s) \text{ si } s \in S_j. \end{aligned}$$

$\varphi$ esta bien definida ya que si $s \in S_j \cap S_k$, al ser $\mathscr{C}$ una cadena y $(S_j, \varphi_j), (S_k, \varphi_k) \in \mathscr{C}$ necesariamente $(S_j, \varphi_j) \preccurlyeq (S_k, \varphi_k)$ o $(S_k, \varphi_k) \preccurlyeq (S_j, \varphi_j)$; si $(S_j, \varphi_j) \preccurlyeq (S_k, \varphi_k)$ entonces $S_j \subseteq S_k$ y por consiguiente $S_j \cap S_k = S_j$, además $\varphi_k(s) = \varphi_j(s)$ pues $\varphi_k|_{S_j} = \varphi_j$. Veamos ahora que $\varphi$ es un homomorfismo. Sean $s, s' \in S$, supongamos sin perdida de generalidad que $s \in S_j$ y $s' \in S_k$ con $S_j \subseteq S_k$, entonces $s, s' \in S_k$ y por consiguiente $s + s' \in S_k$; así $\varphi(s + s') = \varphi_k(s + s') = \varphi_k(s) + \varphi_k(s') = \varphi_j(s) + \varphi_k(s') = \varphi(s) + \varphi(s')$, la tercera igualdad es debido a que $\varphi_k|_{S_j} = \varphi_j$. Finalmente si $h \in H$, entonces para cada $i \in I$ $\varphi(h) = \varphi_i(h) = f(h)$, donde la segunda igualdad es debido a que $\varphi_i|_H = f$ para cada $i \in I$. Por lo tanto $(S, \varphi) \in \mathscr{A}$ y claramente es cota superior de $\mathscr{C}$. Por el Lema de Zorn existe $(\widetilde{G}, F)$ una elemento maximal en $\mathscr{A}$.

Afirmamos que $\widetilde{G} = G$, en efecto si $\widetilde{G} < G$ entonces existe $y \in G - \widetilde{G}$. Considerando $G' = \widetilde{G} + \langle y\rangle$ podemos repetir la construcción del principio y encontrar un homomorfismo $F' : G' \longrightarrow D$ de tal manera que $F'|_{\widetilde{G}} = F$. Como $H \leq \widetilde{G} < G'$, dado $h \in H$ tenemos que $F'(h) = F(h) = f(h)$ y por consiguiente $(G', F') \in \mathscr{A}$. Es decir $(G', F') \in \mathscr{A}$ y $\widetilde{G} < G'$, que es absurdo pues contradice la elección de $(\widetilde{G}, F)$. Por lo tanto debemos tener que $\widetilde{G} = G$, lo que termina esta parte de la prueba.

$[(c) \Rightarrow (b)]$ Supóngase que $D \leq G$. Consideremos el siguiente diagrama




Por $(c)$, el homomorfismo identidad en $D$ se puede extender a un homomorfismo $F$ de $G$ en $D$. Sea $K = \ker F$; veamos que $G = D \oplus K$. Sea $x \in G$ y $a = F(x) \in D$, entonces $F(a) = Id_D(a) = a$ y por consiguiente $F(x) = F(a)$, así $F(x - a) = 0$ y en consecuencia $(x - a) \in \ker F$, sea $k \in K$ tal que $x - a = k$, entonces $x = a + k \in D + K$ y por lo tanto $G = D + K$. Si $d \in D \cap K$, entonces $d = Id_D(d) = F(d) = 0$ mostrando que $D \cap K = 0$ y por lo tanto $G = D \oplus K$.

$[(b) \Rightarrow (a)]$ Sea $D$ un grupo con la propiedad de ser sumando directo de cualquier grupo

que lo contiene, por el Teorema 2.1.16 (*ii*), existe un grupo divisible $\mathcal{D}$ que lo contiene. Entonces $\mathcal{D} = D \oplus H$ y por el Teorema 2.1.10 tenemos que $D$ es divisible. ■

En la búsqueda de una descripción de un grupo hemos visto que si contiene un subgrupo divisible éste es un sumando directo de dicho grupo. El siguiente teorema muestra que, dado un grupo siempre existe un subgrupo divisible, más aún es posible encontrar el máximo subgrupo divisible de un grupo respecto a $\subseteq$.

**Teorema 2.1.18.** *Un grupo $G$ tiene un subgrupo divisible máximo (resp. a $\subseteq$) $D$, y $G = D \oplus R$, donde $R$ no tiene subgrupos divisibles triviales.*

*Demostración.* Consideramos la familia $\mathscr{D} = \{H \leq G \mid H \text{ es divisible}\}$, el subgrupo buscado es

$$D = \sum_{H \in \mathscr{D}} H.$$

En efecto, sean $n \in \mathbb{Z}$ y $x = h_1 + \cdots + h_k \in D$ donde $h_i \in H_i \in \mathscr{D}$ para $1 \leq i \leq k$. Como cada $H_i$ es divisible existen $h_i' \in H_i$ tales que $nh_i' = h_i$ para $1 \leq i \leq k$. Considerando $y = h_1' + \cdots + h_k' \in D$ tenemos que $ny = x$ y por lo tanto $D$ es un subgrupo divisible. Claramente $D$ es el mayor subgrupo divisible de $G$ (respecto a $\subseteq$); así el Teorema 2.1.12 asegura que $G = D \oplus R$ para algún $R \leq G$. Si $R$ contiene un subgrupo divisible $N$ necesariamente $N \in \mathscr{D}$ y por lo tanto $N \subseteq D$, por lo que $N \subseteq D \cap R = 0$; así el único subgrupo divisible que contiene $R$ es 0. ■

El subgrupo $R$ del teorema anterior será sumamente importante en nuestro trabajo de clasificación. Así tenemos la siguiente definición.

**Definición 2.1.19.** *Decimos que un grupo $G$ es un* ***reducido*** *si el único subgrupo divisible que contiene es* 0.

Es claro a partir de la demostración del Teorema 2.1.18 que, para cada grupo $G$ el subgrupo divisible máximo $D$ que contiene es único. Sin embargo no podemos afirmar lo mismo para el subgrupo reducido $R$ del Teorema 2.1.18, lo que si podemos asegurar es que es único salvo isomorfismos ya que $R \cong G/D$; un ejemplo de esto son los grupos $\mathcal{Q} \oplus \mathcal{Z}_2$ y $\mathcal{Q} \oplus H$ donde $H = \langle 0, 2 \rangle \leq \mathcal{Z}_4$, ambos grupos son isomorfos y su parte divisible es la misma, no así su parte reducida.

**Nota 2.1.20.** *Del Teorema 2.1.18 deducimos que una forma de estudiar grupos abelianos es estudiar, por separado, grupos divisibles y grupos reducidos así como la suma directa de estas dos clases de grupos.*

El estudio de los grupos divisibles ha sido muy satisfactorio en el sentido de que se ha logrado dar un teorema de clasificación de esta clase de grupos.

Comenzaremos la descripción de los grupos divisibles con los siguientes lemas preliminares, posteriormente daremos un teorema que clasifica a estos grupos (abelianos) con la propiedad de divisibilidad.

**Lema 2.1.21.** *Si $G$ es un grupo divisible entonces $t(G)$ es un subgrupo divisible.*

*Demostración.* Sean $n \in \mathbb{Z}^+ - \{0\}$ y $x \in t(G)$ tal que $mx = 0$ con $m \in \mathbb{Z}^+$. Por ser $G$ divisible existe $y \in G$ tal que $ny = x$ y por consiguiente

$$(mn)y = m(ny) = mx = 0,$$

como $mn \in \mathbb{Z}^+$ tenemos que $y \in t(G)$. Es decir, dado $n \in \mathbb{Z}^+$ y $x \in t(G)$, existe $y \in t(G)$ tal que $ny = x$. Por lo tanto $t(G)$ es divisible. ■

Para el siguiente lema, recordamos que para un grupo divisible libre de torsión, cada ecuación $nx = y$ tienen un <u>única</u> solución (ver el inciso $(c)$ de la Proposición 2.1.3)

**Lema 2.1.22.** *Si $F$ es un grupo divisible libre de torsión, entonces $F$ admite una estructura de $\mathbb{Q}$-espacio vectorial.*

*Demostración.* Para dotar a $F$ de una estructura de $\mathbb{Q}$-espacio vectorial sólo basta definir el producto por escalares. Sea $r = \frac{m}{n} \in \mathbb{Q}$ y $y \in F$. Dados $n$ y $y$ tenemos que existe un único $x \in F$ tal que $nx = y$. Lo anterior sugiere definir

$$ry = (\tfrac{m}{n})y = mx \in F. \tag{2.9}$$

Para ver que este producto está bien definido, veamos que no depende de la representación de $r$.

Supongamos que $r = \frac{m}{n} = \frac{m'}{n'}$, entonces $mn' = m'n$. Sea $y \in F$ y supongamos que $nx_1 = y = n'x_2$, luego por definición

$$(\tfrac{m}{n})y = mx_1 \text{ y } (\tfrac{m'}{n'})y = m'x_2.$$

Sea $x \in F$ tal que $(mn')x = y = (m'n)x$, entonces al ser $n(m'x) = y$ por la unicidad tenemos que $(m'x) = x_1$ y en forma análoga $mx = x_2$. De donde $mx_1 = m(m'x) = (mm')x = (m'm)x = m'(mx) = m'x_2$. Por lo tanto $(\frac{m}{n})x = (\frac{m'}{n'})x$.

Veamos ahora que se satisfacen las siguientes propiedades

$(i)$ $r(sy) = (rs)y$.

$(ii)$ $r(y+y') = ry + ry'$.

$(iii)$ $(r+s)y = ry + sy$.

$(iv)$ $1y = y$.

Sean $r = \frac{m}{n}$, $s = \frac{m'}{n'} \in \mathbb{Q}$ y $y, y' \in F$.
$[(i)]$ $rs = \frac{mm'}{nn'}$; sea $x \in F$ tal que $(nn')x = y$ entonces, por definición $(rs)y = (mm')x$, como $n'(nx) = y$, y la solución es única, entonces $sy = m'(nx) = n(m'x)$ y por consiguiente, nuevamente por la unicidad en las soluciones, $r(sy) = m(m'x) = (mm')x$; por lo tanto $r(sy) = (rs)y$.
$[(ii)]$ Sean $x_1, x_2 \in F$ tales que

$$mx_1 = y \quad \text{y} \quad mx_2 = y', \tag{2.10}$$

sumando las igualdades en (2.10) miembro a miembro tenemos que $m(x_1 + x_2) = y + y'$, de donde

$$\begin{aligned} r(y+y') &= m(x_1 + x_2) \\ &= mx_1 + mx_2 \\ &= ry + ry'. \end{aligned}$$

.
$[(iii)]$ Sean $x_1, x_2 \in F$ tales que $nx_1 = y$ y $n'x_2 = y$. Es decir

$$ry = mx_1 \quad \text{y} \quad sy = m'x_2. \tag{2.11}$$

Sea $x \in F$ tal que $(nn')x = y$. Como $n(n'x) = y$ entonces $n'x = x_1$, análogamente $n'(nx) = y$ implica que $nx = x_2$ y por consiguiente

$$mn'x = mx_1 \quad \text{y} \quad m'nx = m'x_2, \tag{2.12}$$

así

$$\begin{aligned} (r+s)y &= (mn' + nm')x \\ &= (mn')x + (nm')x \\ &= ry + sy; \end{aligned}$$

donde la última igualdad es por (2.12) y (2.11). Por lo tanto $(r+s)y = ry + sy$.

Claramente se satisface $(iv)$ y por lo tanto $F$ es un $\mathbb{Q}$-espacio vectorial. ■

**Nota 2.1.23.** *La estructura de $\mathbb{Q}$-espacio vectorial que hemos dado al grupo divisible libre de torsión $F$ es única. En efecto supóngase que se tiene definida una multiplicación por*

*escalares $r*y$ con $r \in \mathbb{Q}$ y $y \in F$ que hace de $F$ un $\mathbb{Q}$-espacio vectorial. Veremos que dichas operaciones son iguales y para lo cual comenzaremos mostraremos que para toda $n \in \mathbb{Z}$*

$$n * y = ny. \tag{2.13}$$

*Sea $y \in F$, de los axiomas de espacio vectorial tenemos que*

$$1 * y = y = 1y.$$

*Supongamos como hipótesis de inducción que (2.13) es válida para $k \in \mathbb{Z}^+$, entonces*

$$\begin{aligned} (k+1) * y &= k * y + 1 * y && \textit{(axioma de espacio vectorial)} \\ &= ky + 1y && \textit{(hipótesis y base de inducción)} \\ &= (k+1)y && \textit{(asociatividad en } F\textit{)} \end{aligned}$$

*por lo tanto (2.13) es válida para toda $n \in \mathbb{Z}^+$. Sea $n \in \mathbb{Z}$ con $n < 0$. Utilizando los axiomas de espacio vectorial tenemos que*

$$0 = 0 * y = (1-1) * y = 1 * y + (-1) * y = y + (-1) * y,$$

*por lo tanto para todo $y \in F$*

$$-((-1) * y) = y. \tag{2.14}$$

*Como $-n \in \mathbb{Z}^+$ tenemos que $(-n) * y = (-ny) = -(ny)$, por otra parte $(-n) * y = (-1n) * y = (-1) * (n * y)$ y así $(-1) * (n * y) = -(ny)$, lo cual implica que $-((-1) * (n * y)) = ny$; así por (2.14) tenemos $n * y = -((-1) * (n * y)) = ny$. Por lo tanto tenemos que (2.13) es válida para todo $n \in \mathbb{Z}$. Nuevamente, de los axiomas de espacio vectorial tenemos que $y = 1 * y = (\frac{n}{n}) * y = (n\frac{1}{n}) * y = n * (\frac{1}{n} * y) = n(\frac{1}{n} * y)$, la última igualdad es debido a (2.13). Es decir, para toda $y \in F$ y para toda $n \in \mathbb{Z}$, la solución de la ecuación $nx = y$ es $x = \frac{1}{n} * y$. Así, de nuestra definición de multiplicación por escalares dada en el Lema 2.1.22, para $r = \frac{m}{n} \in \mathbb{Q}$ y $y \in F$ tenemos que $ry = m(\frac{1}{n} * y) = m * (\frac{1}{n} * y) = (m\frac{1}{n}) * y = \frac{m}{n} * y = r * y$, nuevamente la segunda igualdad es por (2.13). Por lo tanto $r * y = ry$ para toda $y \in F$ y para todo $r \in \mathbb{Q}$.*

**Proposición 2.1.24.** *Sea $T$ un grupo p-primario divisible, entonces $T \cong \bigoplus_{r_p} \mathcal{Z}_{p^\infty}$, donde $r_p$ es un cardinal que sólo depende de $T$.*

*Demostración.* Sea $x_1 \in T[p] - \{0\}$, por ser $T$ un grupo divisible podemos definir $\beta = \{x_n\}_{n \in \mathbb{N}}$ en forma recursiva como sigue

$$px_2 = x_1, \quad \text{en forma recursiva} \quad px_n = x_{n-1} \text{ para } n > 1. \tag{2.15}$$

Sea $\mathscr{Z} = \langle\beta\rangle$, por la Proposición 1.4.6 $\mathscr{Z} \cong \mathcal{Z}_\infty$. De esta manera si $T \neq 0$ entonces $T$ contiene un subgrupo isomorfo a $\mathcal{Z}_{p^\infty}$.

Sea $\mathscr{A} = \{W \leq T \mid W \cong \mathcal{Z}_{p^\infty}\}$, por lo anterior tenemos que $\mathscr{A} \neq \varnothing$ ya que $\mathscr{Z} \in \mathscr{A}$. Sea $\mathfrak{G} = \{\{S_i\}_{i\in I} \mid \{S_i\}_{i\in I} \subset \mathscr{A},\ \text{y } \{S_i\}_{i\in I} \text{ independiente}\}$, como $\mathscr{A} \neq \varnothing$ entonces $\mathfrak{G} \neq \varnothing$, $(\mathfrak{G}, \subseteq)$ determina un conjunto parcialmente ordenado al cual aplicaremos el Lema de Zorn. Sea $\mathscr{C}$ una cadena en $\mathfrak{G}$ y sea $\mathscr{F} = \bigcup_{H\in\mathscr{C}} H$. Claramente $\mathscr{F} \subseteq \mathscr{A}$, así que mostraremos que $\mathscr{F}$ es independiente para probar que $\mathscr{F} \in \mathfrak{G}$.

Sea $S \in \mathscr{F}$ y $s \in S \bigcap \sum_{K\in\mathscr{F}-\{S\}} K$. Entonces $s = k_{i_1} + \cdots + k_{i_m}$, donde $k_{i_j} \in K_{i_j} \in \mathscr{F}$. Sea $\mathscr{L} \in \mathscr{C}$ tal que $S, K_1, \ldots, K_m \in \mathscr{L}$, existe ya que $\mathscr{C}$ es una cadena, como $\mathscr{L}$ es independiente $S \bigcap \sum_{j=1}^{m} K_{i_j} = 0$; así que $s = 0$ y por lo tanto $S \bigcap \sum_{K\in\mathscr{F}-\{S\}} K = 0$ para toda $S \in \mathscr{F}$. Por lo tanto $\mathscr{F} \in \mathfrak{G}$ y claramente es cota superior de $\mathscr{C}$. Por el Lema de Zorn existe $\mathscr{M} = \{S_i\}_{i\in I}$ un elemento maximal de $\mathfrak{G}$.

Sea $T' = \bigoplus_{i\in I} S_i$, veamos que $T' = T$. Por definición $S_i \cong \mathcal{Z}_{p^\infty}$ para toda $i \in I$ y como $\mathcal{Z}_{p^\infty}$ es divisible, entonces cada $S_i$ es un subgrupo divisible de $G$ y por consiguiente, de la Proposición 2.1.10, tenemos que $T'$ es divisible. Por otra parte el Teorema 2.1.12 asegura que $T = T' \oplus R$. Veamos que $R = 0$. Si existe $x_1 \in R - \{0\}$, como $R$ es divisible y de torsión (Teoremas 2.1.12 y 2.1.10), podemos construir $\{y_n\}_{n\in\mathbb{N}} \subset R$ con las siguientes propiedades:

$$py_1 = 0 \text{ y para cada } n \geq 1 \ py_{n+1} = y_n.$$

Sea $R' = \langle\{y_n\}_{n\in\mathbb{N}}\rangle \leq R$, por la Proposición 1.4.6 $R' \cong \mathcal{Z}_{p^\infty}$; consideremos $\mathscr{M}' = \mathscr{M} \cup \{R'\}$. Como $\sum_{i\in I} S_i \bigcap R' \subseteq \sum_{i\in I} S_i \bigcap R = 0$; con un argumento parecido se muestra que $(R' + \sum_{i\neq j} S_i) \cap S_j = 0$, para todo $j \in I$, y por consiguiente tenemos que $\mathscr{M}' \in \mathfrak{G}$; además $\mathscr{M} \subsetneq \mathscr{M}'$, lo cual es absurdo pues contradice la maximalidad de $\mathscr{M}$. Así $R = 0$ y por lo tanto

$$T = T' = \bigoplus_{i\in I} S_i \cong \bigoplus_{|I|} \mathcal{Z}_{p^\infty}. \tag{2.16}$$

A continuación encontraremos cual es el cardinal $|I|$. Considerando el Teorema 1.3.15, tenemos que

$$T[p] \cong \bigoplus_{|I|} \mathcal{Z}_{p^\infty}[p] \tag{2.17}$$

Veamos que $\mathcal{Z}_{p^\infty}[p] \cong \mathcal{Z}_p$. Definimos $\varphi : \mathcal{Z}_p \longrightarrow \mathcal{Z}_{p^\infty}[p]$ como $\varphi(\overline{m}) = \overline{\frac{m}{p}}$. Veamos que $\varphi$ esta bien definida, en el sentido de que no depende del representante elegido. Supongamos

pues que $m - m' = qp$ para algún $q \in \mathbb{Z}$, entonces

$$\begin{aligned}\overline{\frac{m}{p}} - \overline{\frac{m'}{p}} &= m(\overline{\frac{1}{p}}) - m'(\overline{\frac{1}{p}}) \\ &= (m - m')(\overline{\frac{1}{p}}) \\ &= qp(\overline{\frac{1}{p}}) = \overline{0}\end{aligned}$$

Por lo tanto $\varphi(\overline{m}) = \varphi(\overline{m'})$ y $\varphi$ esta bien definida. Claramente $\varphi$ es un homomorfismo de grupos. Si $\overline{m} \in \ker\varphi$ entonces $\frac{m}{p} \in \mathcal{Z}$ y por lo tanto $m = qp$ para algún $q \in \mathcal{Z}$; así $\overline{m} = \overline{qp} = \overline{0}$ y por lo tanto $\ker\varphi = 0$. Finalmente, a partir de la Nota 1.4.3 sabemos los elementos de $\mathcal{Z}_{p^\infty}[p]$ son de la forma $\overline{\frac{n}{p}}$ para alguna $n \in \mathcal{Z}$, con $1 \leq n \leq p$; así, dado $\overline{\frac{n}{p}} \in \mathcal{Z}_{p^\infty}[p]$, $\overline{n} \in \mathcal{Z}_p$ satisface que $\varphi(\overline{n}) = \overline{\frac{n}{p}}$ y por consiguiente $\varphi$ es suprayectiva. Por lo tanto $\mathcal{Z}_{p^\infty}[p] \overset{\varphi}{\cong} \mathcal{Z}_p$ y así (2.17) lo podemos escribir como

$$T[p] \cong \bigoplus_{|I|} \mathcal{Z}_{p^\infty}[p] \cong \bigoplus_{|I|} \mathcal{Z}_p. \tag{2.18}$$

Por otra parte, de la Proposición 1.3.17 tenemos que $T[p]$ es un $\mathbb{Z}_p$-espacio vectorial. Si $r_p = \dim_{\mathbb{Z}_p} T[p]$ entonces tenemos el isomorfismo de $\mathbb{Z}_p$-espacios vectoriales

$$T[p] \cong \bigoplus_{r_p} \mathbb{Z}_p,$$

que en particular es un isomorfismo de grupos (abelianos), y por lo tanto

$$T[p] \cong \bigoplus_{r_p} \mathcal{Z}_p. \tag{2.19}$$

Así por (2.18) y (2.19) tenemos que $\bigoplus_{|I|} \mathcal{Z}_p \cong \bigoplus_{r_p} \mathcal{Z}_p$ y por lo tanto $|I| = r_p = \dim_{\mathbb{Z}_p} T[p]$. ■

El siguiente teorema, así como lo hecho en la sección 1.3, nos permitirá definir un invariante completo para los grupos divisibles.

**Teorema 2.1.25.** *Todo grupo divisible $G$ es una suma directa de grupos cada uno isomorfo al grupo aditivo $\mathcal{Q}$ ó a $\mathcal{Z}_{p^\infty}$ (para varios primos $p$).*

*Demostración.* Sea $G$ un grupo divisible. Por el Lema 2.1.21 $t(G)$ es un subgrupo divisible de $G$ y por el Teorema 2.1.12

$$G = F \oplus t(G). \tag{2.20}$$

Como $F \cong G/t(G)$ la Proposición 1.3.8 asegura que $F$ es libre de torsión, y por el Teorema 2.1.10 tenemos que $F$ es divisible. Así $F$ es un grupo divisible libre de torsión y por el Lema

2.1.22 $F$ es un $\mathbb{Q}$-espacio vectorial. Si $r_{_F} = \dim_{\mathbb{Q}} F$, tenemos el isomorfismo de $\mathbb{Q}$-espacios vectoriales

$$F \cong \bigoplus_{r_{_F}} \mathbb{Q}. \tag{2.21}$$

Ya que todo homomorfismo de espacios vectoriales es en particular un homomorfismo de grupos, el isomorfismo en (2.21) es de grupos; y así tenemos que $F \cong \bigoplus_{r_{_F}} \mathcal{Q}$.

Por otra parte, Como $t(G)$ es divisible, del Teorema 1.3.13 tenemos que

$$t(G) \cong \bigoplus_{p \in \mathscr{P}} t(G)_p. \tag{2.22}$$

Nótese que al ser $t(G)$ divisible y en virtud del Teorema 2.1.10 cada $t(G)_p$ es un grupo divisible y además de torsión; así por la Proposición 2.1.24, para cada $p \in \mathscr{P}$, $t(G)_p \cong \bigoplus_{r_p} \mathcal{Z}_{p^\infty}$; así por el isomorfismo en (2.22) tenemos que

$$t(G) \cong \bigoplus_{p \in \mathscr{P}} (\bigoplus_{r_p} \mathcal{Z}_{p^\infty}). \tag{2.23}$$

Finalmente, a partir de (2.20), (2.21) y (2.23) obtenemos que

$$G \cong \bigoplus_{r_{_F}} \mathcal{Q} \oplus \bigoplus_{p \in \mathscr{P}} (\bigoplus_{r_p} \mathcal{Z}_{p^\infty}).$$

■

Dado un grupo divisible $G$, denotaremos por $\boldsymbol{F(G)}$ al grupo libre de torsión enunciado en la Proposición 1.3.8. En virtud del Teorema 2.1.25, definimos la siguiente asignación

$$G \rightsquigarrow (r_{_{F(G)}}, r_{p_{1(G)}}, r_{p_{2(G)}}, \ldots, r_{p_{n(G)}}, \ldots)\ , \tag{2.24}$$

donde $r_{_{F(G)}} = \dim_{\mathbb{Q}} F(G)$ y para cada $n \in \mathbb{N}$, $r_{p_{n(G)}} = \dim_{\mathbb{Z}_{p_n}} t(G)_{p_n}$. Nótese que si en la descomposición de $t(G)$ no hay elementos de orden $p$ entonces $t(G)_p = 0$ y por lo tanto $r_{p_{(G)}} = 0$.

**Nota 2.1.26.** *De las Proposiciones 1.3.7 y 1.3.14 tenemos que si $G$ y $H$ son grupos isomorfos entonces $t(G) \cong t(H)$ y así $t(G)_p \cong t(H)_p$ para toda $p \in \mathscr{P}$; además $F(G) \cong F(H)$. Por lo tanto*

$$(r_{_{F(G)}}, r_{p_{1(G)}}, r_{p_{2(G)}}, \ldots, r_{p_{n(G)}}, \ldots) = (r_{_{F(H)}}, r_{p_{1(H)}}, r_{p_{2(H)}}, \ldots, r_{p_{n(H)}}, \ldots). \tag{2.25}$$

*Recíprocamente, si $G$ y $H$ son grupos divisibles tales que satisfacen (2.25), entonces*

$$G \cong \bigoplus_{r_{F(G)}} \mathcal{Q} \oplus \bigoplus_{i\in\mathbb{N}} \left( \bigoplus_{r_{p_i(G)}} \mathcal{Z}_{p_i^\infty} \right) \cong H.$$

*De esta manera*

$$(r_{F(G)}, r_{p_1(G)}, r_{p_2(G)}, \ldots, r_{p_n(G)}, \ldots),$$

*determina un invariante completo para un grupo divisible $G$.*

La idea ahora es extender este invariante a grupos más generales que los divisibles. Comenzaremos esta tarea en el siguiente capítulo introduciendo nuevas nociones un poco más débiles que la divisibilidad.

Para finalizar, y como una consecuencia del Teorema 2.1.25, daremos otra caracterización del grupo $\mathcal{Z}_{p^\infty}$. Despues de esto, daremos respuesta a los problemas 1, 2 y 3 planteados en la introducción de la tesis.

**Proposición 2.1.27.** *Si $G$ es un grupo infinito tal que cualquier subgrupo propio es finito. Entonces que $G$ es isomorfo a $\mathcal{Z}_{p^\infty}$.*

*Demostración.* Notemos que $G$ no puede ser cíclico pues de lo contrario $G \cong \mathcal{Z}$ el cual no tiene subgrupos finitos; así dado $x \in G$, como $\langle x \rangle < G$, tenemos que $o(x)$ es finito y por lo tanto $t(G) = G$. Por el Teorema 1.3.13 tenemos que $G$ es la suma directa de sus partes primarias, es decir

$$G = \bigoplus_{p\in\mathscr{P}} G_p.$$

El número de sumandos $G_p$ , con $p \in \mathscr{P}$, distintos de cero es finito; más aún existe sólo un número primo $p \in \mathscr{P}$ tal que $G_p \neq 0$. En efecto ya que si $p, q \in \mathscr{P}$ son dos números primos distintos entonces $G = G_q \oplus \bigoplus_{p\in\mathscr{P}-\{q\}} G_p$ y por ser $G$ infinito ó $G_q$ es infinito ó $\bigoplus_{p\in\mathscr{P}-\{q\}} G_p$ es infinito; sin importar cual de ellos lo sea, hemos encontrado un subgrupo propio de $G$ que no es finito lo que es absurdo. Por lo tanto $G$ es un grupo $p$-primario infinito, para algún número primo $p$.

Veamos ahora que $G$ es divisible. De la Proposición 2.1.3, $(d)$ tenemos que para todo $n \in \mathbb{Z}^+$ con $(n, p) = 1$ $nG = G$. Por lo tanto basta demostrar que $p^m G = G$ para toda $m \in \mathbb{Z}^+$. Veamos primero que $pG = G$. Si $pG < G$ entonces $pG$ es finito, es decir, $pG = \{px_1, px_2, \ldots, px_k\}$. Sea $X_i = \{x \in G \mid px = px_i\}$; como $G$ es infinito, para alguna $i$ $(1 \leq i \leq m)$ $X_i$ es infinito; este conjunto garantiza que $G[p] = \{x \in G \mid px = 0\}$ es infinito, ya que $(x - x_i) \in G[p]$ para toda $x \in X_i$ y como $G[p] \leq G$ necesariamente $G[p] = G$. Por la Proposición 1.3.17, $G[p]$ es un $\mathbb{Z}_p$-espacio vectorial, y por ser $G[p]$ infinito, necesariamente $G = G[p] \cong \bigoplus_\alpha \mathbb{Z}_p$, donde $\alpha = \dim_{\mathbb{Z}_p} G[p]$ es infinito. Esto es absurdo pues claramente $\bigoplus_\alpha \mathbb{Z}_p$

contiene subgrupos propios infinitos los cuales producirían subgrupos propios infinitos en $G$. Por lo tanto $pG = G$. Esta última igualdad implica que $p^mG = G$ para toda $m \in \mathbb{Z}^+$ y por lo tanto $G$ es divisible. Por le Teorema 2.1.25 $G \cong \bigoplus_{r_p} \mathcal{Z}_{p^\infty}$. Necesariamente $r_p = 1$ pues si $r_p \geq 2$ es posible encontrar subgrupos propios infinitos en $\bigoplus_{r_p} \mathcal{Z}_{p^\infty}$, por ejemplo una copia isomorfa a $\mathcal{Z}_{p^\infty}$, lo que da lugar a encontrar subgrupos propio infinitos en $G$, vía el isomorfismo que existe por el Teorema 2.1.25, lo que es absurdo. Por lo tanto $G \cong \mathcal{Z}_{p^\infty}$. ■

**Proposición 2.1.28.** *Sean $G$ y $H$ grupos divisible tales que $G$ es isomorfo a un sumando directo de $H$ y $H$ es isomorfo a un sumando directo de $G$, entonces $G$ y $H$ son isomorfos.*

*Demostración.* Supongamos que $G \cong \widetilde{H}$ donde $\widetilde{H}$ es un sumando directo de $H$ y $H \cong \widetilde{G}$ con $\widetilde{G}$ un sumando directo de $G$. Por el Teorema 2.1.25 tenemos que

$$\begin{aligned}(r_{_{F(G)}}, r_{p_1(G)}, r_{p_2(G)}, \ldots, r_{p_n(G)}, \ldots) &= (r_{_{F(\widetilde{H})}}, r_{p_1(\widetilde{H})}, r_{p_2(\widetilde{H})}, \ldots, r_{p_n(\widetilde{H})}, \ldots)\\ (r_{_{F(H)}}, r_{p_1(H)}, r_{p_2(H)}, \ldots, r_{p_n(H)}, \ldots) &= (r_{_{F(\widetilde{G})}}, r_{p_1(\widetilde{G})}, r_{p_2(\widetilde{G})}, \ldots, r_{p_n(\widetilde{G})}, \ldots).\end{aligned}$$

Como $\widetilde{H} \leq H$ y $\widetilde{G} \leq G$ tenemos que $r_{_{F(G)}} = r_{_{F(\widetilde{H})}} \leq r_{_{F(H)}} = r_{_{F(\widetilde{G})}} \leq r_{_{F(G)}}$, por consiguiente $r_{_{F(G)}} = r_{_{F(H)}}$. En forma análoga obtenemos que $r_{p_n(G)} = r_{p_n(H)}$ para toda $n \in \mathbb{Z}^+$; así

$$(r_{_{F(G)}}, r_{p_1(G)}, r_{p_2(G)}, \ldots, r_{p_n(G)}, \ldots) = (r_{_{F(H)}}, r_{p_1(H)}, r_{p_2(H)}, \ldots, r_{p_n(H)}, \ldots),$$

por lo tato, de la Nota 2.1.26, tenemos que $G$ es isomorfo a $H$. ■

**Proposición 2.1.29.** *Sean $G$ y $H$ grupos divisibles. Si $G \oplus G \cong H \oplus H$, entonces $G \cong H$.*

*Demostración.* Sabemos a partir del Teorema 1.3.15 (1) que $t(G \oplus G) = t(G) \oplus t(G)$. Por otra parte $F(G \oplus G) = (G \oplus G)/(t(G) \oplus t(G)) \cong G/t(G) \oplus G/t(G) = F(G) \oplus F(G)$, es decir, $F(G \oplus G) \cong F(G) \oplus F(G)$. Análogamente $F(H \oplus H) \cong F(H) \oplus F(H)$. De lo anterior obtenemos que $r_{_{F(G\oplus G)}} = r_{_{F(G)}} + r_{_{F(G)}}$ y $r_{_{F(H\oplus H)}} = r_{_{F(H)}} + r_{_{F(H)}}$. Como $G \oplus G \cong H \oplus H$ se sigue que $r_{_{F(G)}} + r_{_{F(G)}} = r_{_{F(H)}} + r_{_{F(H)}}$ y por lo tanto $r_{_{F(G)}} = r_{_{F(H)}}$. Nuevamente como $t(G) \oplus t(G) \cong t(H) \oplus t(H)$ se sigue del Teorema 1.3.15 (2) que $t(G)_p \oplus t(G)_p \cong t(H)_p \oplus t(H)_p$ para todo número primo $p$; así $r_{p_{i(G)}} + r_{p_{i(G)}} = r_{p_{i(H)}} + r_{p_{i(H)}}$ para cada $i \in \mathbb{Z}^+$ y por lo tanto $r_{p_{i(G)}} = r_{p_{i(H)}}$ para toda $i \in \mathbb{Z}^+$. Nuevamente la Nota 2.1.26 garantiza que $G$ es isomorfo a $H$. ■

**Proposición 2.1.30.** *Sea $\mathcal{F}$ un grupo abeliano finitamente generado. Si $G$ y $H$ son grupos divisibles tal que $\mathcal{F} \oplus G \cong \mathcal{F} \oplus H$, entonces $G \cong H$.*

*Demostración.* Como $\mathcal{F}$ es finitamente generado, $\mathcal{F} = \bigoplus_{i=1}^{k} \langle a_i \rangle$ donde $a_i \in F$ para $1 \leq i \leq k$ (véase [Fu], Capítulo 3 página 79) y como cada $\langle a_i \rangle$ no es divisible, Nota 2.1.9, el Teorema 2.1.10 asegura que $\mathcal{F}$ no es divisible; por lo tanto los subgrupos máximos divisibles de $\mathcal{F} \oplus G$ y $\mathcal{F} \oplus G$ son $0 \oplus G$ y $0 \oplus H$ respectivamente. En vista de que $\mathcal{F} \oplus G \cong \mathcal{F} \oplus H$, necesariamente $0 \oplus G \cong 0 \oplus H$. Además, claramente $G \cong 0 \oplus G$ y $H \cong 0 \oplus H$; por lo tanto $G \cong H$. ■

**Nota 2.1.31.** *A la luz del Teorema 2.1.18, la Nota 2.1.26 y las proposiciones 2.1.28, 2.1.29 y 2.1.30; es suficiente resolver los problemas 1, 2 y 3 dados en la introducción para el caso de grupos reducidos.*

## 2.2. Subgrupos Puros

Como se mencionó al inicio de este capítulo, la noción de subgrupo puro es más débil que la subgrupo divisible. En el Teorema 2.1.12 se demostró que si un grupo $G$ contiene un subgrupo divisible necesariamente éste es un sumando directo. En el caso de los subgrupos puros esto no necesariamente sucede, al estudiar esta clase de subgrupos entre otras cosas veremos cómo esta noción refleja una de las maneras en que un subgrupo es incluido en un grupo. Se verá que esta noción es suficientemente general como para garantizar la existencia de una cantidad suficiente de subgrupos puros y al mismo tiempo los subgrupos puros poseen varias propiedades que son fáciles de manejar. Su importancia también se verá manifestada en el papel metodológico, demostrando la existencia de sumas directas, a saber, la existencia de subgrupos puros de un tipo u otro se puede establecer con cierta facilidad, así como varios criterios que aseguran el carácter de sumando directo de ciertos subgrupo puros.

Supongamos que $H$ es un subgrupo de un grupo $G$ y que además $G = H \oplus K$. Sean $n \in \mathbb{Z}$ y $h \in H$ tales que $ny = h$ para alguna $y \in G$; como $G = H \oplus K$, existen $h' \in H$ y $k \in K$ de tal manera que $y = h' + k$ y por consiguiente $ny = nh' + nk$; así al ser $H + K$ una suma directa obtenemos que $nh' = h$.

Hemos visto que de existir un subgrupo $H$ de un grupo $G$ con la propiedad de ser sumando directo entonces cada vez que se tenga $ny = h \in H$ para algún $n \in \mathbb{Z}$ y $y \in G$ existe $h' \in H$ que satisface $nh' = h$. Esta propiedad sugiere la siguiente definición.

**Definición 2.2.1.** *Un subgrupo $H$ de un grupo $G$ es llamado **puro** si la ecuación $nx = y \in H$ tiene solución en $H$ cuando esta tiene solución en $G$. Es decir, $H$ es puro en $G$ si cada vez que un entero $n$ divida a un elemento $y \in H$ en $G$ implica que $n$ divide a $y$ en $H$.*

El hecho de que $n$ divida a $y$ en $H$ implica que $y \in nH$; así un subgrupo $H$ de un grupo $G$ es puro si y sólo si para cada $n \in \mathbb{Z}$.

$$nH = nG \cap H. \tag{2.26}$$

**Ejemplo 2.2.2.** *El subgrupo de torsión de un grupo es puro. En efecto ya hemos visto que las soluciones de la ecuación $nx = y$ con $y \in t(G)$ deben pertenecer a $t(G)$.*

El siguiente es un ejemplo de un subgrupo que no es puro.

**Ejemplo 2.2.3.** *Considerando $\mathcal{Z}$ como subgrupo de $\mathcal{Q}$ tenemos que para toda $n \in \mathbb{Z}$, $n\mathcal{Q} = \mathcal{Q}$ ya que $\mathcal{Q}$ es divisible, así $n\mathcal{Q} \cap \mathcal{Z} = \mathcal{Q} \cap \mathcal{Z} = \mathcal{Z} \neq n\mathcal{Z}$. Por lo tanto $\mathcal{Z}$ no es un subgrupo puro de $\mathcal{Q}$.*

**Nota 2.2.4.** *A pesar de que la noción de sumando directo motiva la definición de subgrupo puro, no necesariamente un subgrupo puro es un sumando directo. Consideremos $G = \prod_{\aleph_0} \mathcal{Z}$ el producto de $\aleph_0$[3] copias del grupo $\mathcal{Z}$. Denotamos, para cada $n \in \mathbb{N}$,*

$$\mathcal{H}_n = \{(x_i)_{i\in\mathbb{N}} \in G \mid x_i = 0 \ \forall \ i > n\} \quad y \quad \mathcal{K}_n = \{(x_i)_{i\in\mathbb{N}} \in G \mid x_i = 0 \ \forall \ i \leq n\}.$$

*Se puede verificar fácilmente que para cada $n \in \mathbb{N}$, $G = \mathcal{H}_n \oplus \mathcal{K}_n$ y que $\bigcup_{n\in\mathbb{N}} \mathcal{H}_n = \bigoplus_{\aleph_0} \mathcal{Z}$ es la suma directa de $\aleph_o$ copias del grupo $\mathcal{Z}$. Veamos que $\bigoplus_{\aleph_0} \mathcal{Z}$ es un subgrupo puro de $\prod_{\aleph_0} \mathcal{Z}$.*

*Supongamos que existe $x = (x_i)_{i\in\mathbb{N}} \in \prod_{\aleph_0} \mathcal{Z}$ tal que $nx = y \in \bigoplus_{\aleph_0} \mathcal{Z}$ para algún $n \in \mathbb{Z} - \{0\}$, si $y = (y_i)_{i\in\mathbb{N}}$ entonces para toda $i \in \mathbb{N}$ se tiene que $nx_i = y_i$ y como $y_i \neq 0$ solamente para un número finito de $i$'s, entonces $nx_i \neq 0$ solamente para un número finito de $i$'s. Al ser $n \in \mathbb{Z} - \{0\}$ lo anterior implica que $x \in \bigoplus_{\aleph_0} \mathcal{Z}$, lo que prueba que $\bigoplus_{\aleph_0} \mathcal{Z}$ es un subgrupo puro de $\prod_{\aleph_0} \mathcal{Z}$. Sin embargo $\bigoplus_{\aleph_0} \mathcal{Z}$ no es un sumando directo de $\prod_{\aleph_0} \mathcal{Z}$:*

*Supongamos que $\bigoplus_{\aleph_0} \mathcal{Z}$ es un sumando directo de $\prod_{\aleph_0} \mathcal{Z}$. Entonces*

$$\prod_{\aleph_0} \mathcal{Z}_n = \bigoplus_{\aleph_0} \mathcal{Z} \oplus K,$$

*donde $K \overset{\varphi}{\cong} (\prod_{\aleph_0} \mathcal{Z} / \bigoplus_{\aleph_0} \mathcal{Z})$. Considerando $y = (i!)_{i\in\mathbb{N}} \in \prod_{\aleph_0} \mathcal{Z}$ y $n \in \mathbb{Z}^+$ tenemos que*

$$\begin{aligned} y &= (1!, 2!, \ldots, (n-1)!, 0, 0, \ldots) + (0, 0, \ldots, 0, n!, (n+1)!, \ldots) \\ &= (1!, 2!, \ldots, (n-1)!, 0, 0, \ldots) + n(0, 0, \ldots, 0, (n-1)!, \tfrac{(n+1)!}{n}, \ldots), \end{aligned}$$

[3] $\aleph_0$ denota al cardinal de $\mathbb{N}$, es decir, $|\mathbb{N}| = \aleph_0$.

*tomando clases módulo* $\bigoplus_{\aleph_0}\mathcal{Z}$ *tenemos que* $n(x+\bigoplus_{\aleph_0}\mathcal{Z}) = x+\bigoplus_{\aleph_0}\mathcal{Z}$ *donde*

$$x = (0, 0, \ldots, 0, (n-1)!, \tfrac{(n+1)!}{n}, \ldots),$$

*es decir,* $y+\bigoplus_{\aleph_0}\mathcal{Z}$ *es un elemento en* $\prod_{\aleph_0}\mathcal{Z}/\bigoplus_{\aleph_0}\mathcal{Z}$ *que es divisible por* $n$*; como* $n$ *es arbitraria, entonces* $y+\bigoplus_{\aleph_0}\mathcal{Z}$ *es divisible por cualquier entero positivo y por lo tanto por cualquier entero. Esto implica que* $\varphi^{-1}(y+\bigoplus_{\aleph_0}\mathcal{Z}) \in K \leq \prod_{\aleph_0}\mathcal{Z}$ *es un elemento divisible por cualquier entero lo que es absurdo ya que la divisibilidad en* $\prod_{\aleph_0}\mathcal{Z}$ *se "pasa" a* $\mathcal{Z}$ *y cada número entero sólo tiene un número finito de divisores. Por lo tanto* $\bigoplus_{\aleph_0}\mathcal{Z}$ *no puede ser un sumando directo de* $\prod_{\aleph_0}\mathcal{Z}$.

A continuación tenemos algunas consecuencias inmediatas de la definición 2.2.1.

**Observación 2.2.5.** (*a*) *Si* $K$ *es un subgrupo puro de* $H$ *y* $H$ *es un subgrupo puro de* $G$ *entonces* $K$ *es un subgrupo puro de* $G$*. En efecto, como* $K \leq H$ *es puro tenemos que* $mH \cap K = mK$ *para cada* $m \in \mathbb{Z}$ *y como* $H \leq G$ *es puro entonces* $nG \cap H = nH$ *para cada* $n \in \mathbb{Z}$*; así*

$$\begin{aligned} mG \cap K &= mG \cap (H \cap K) \\ &= (mG \cap H) \cap K \\ &= mH \cap K \\ &= mK. \end{aligned}$$

(*b*) *Un subgrupo divisible es puro. En efecto, si* $H \leq G$ *es un subgrupo divisible entonces para cada* $n \in \mathbb{Z}$*,* $nH = H$ *y por lo tanto*

$$\begin{aligned} nG \cap H &= nG \cap nH \\ &= nH. \end{aligned}$$

(*c*) *Un subgrupo* $H$ *de un grupo divisible* $G$ *es puro si y sólo si* $H$ *es divisible. En efecto, suponga que* $G$ *es un grupo divisible entonces para toda* $n \in \mathbb{Z}$*,* $nG = G$*. Si* $H$ *es puro entonces para cada* $n \in \mathbb{Z}$ $nH = nG \cap H = G \cap H = H$*, es decir, para cada* $n \in \mathbb{Z}$ $nH = H$ *y por lo tanto* $H$ *es divisible. El recíproco no es otra cosa que* (*b*).

(*d*) *Si* $S \leq G$ *satisface que* $G/S$ *es libre de torsión entonces* $S$ *es puro. En efecto, sean* $n \in \mathbb{Z}$ *y* $s \in S$ *tales que* $ny = s$ *para alguna* $y \in G$*, pasando al cociente tenemos que* $\overline{ny} = \overline{s} = \overline{0}$ *lo cual implica que* $n\overline{y} = \overline{0}$*; como* $G/S$ *es libre de torsión necesariamente* $\overline{y} = \overline{0}$ *y por consiguiente* $y \in S$.

(*e*) *Si $G$ es libre de torsión, la pureza de $S \leq G$ simplemente significa que $S$ es cerrado (dentro de $G$) bajo división por enteros, en caso de que se tenga dicha división en $G$, siendo este último único. En efecto suponga que $G$ es libre de torsión y que $S \leq G$ es puro, suponga además que $ny = s \in S$ donde $n \in \mathbb{Z}$ e $y \in G$, entonces por (c) de la Proposición 2.1.3 y la pureza de $S$, $y \in S$. De esta manera es posible definir unívocamente $\frac{1}{n}s = y$.*

*Como consecuencia de (e) tenemos que,*

**Corolario 2.2.6.** *Si $G$ es libre de torsión y $\mathscr{F} = \{S_i\}_{i\in I}$ es una familia de subgrupos puros de $G$. Entonces $S = \bigcap_{i\in I} S_i$ es puro.*

*Demostración.* Sean $n \in \mathbb{Z} - \{0\}$ y $s \in nG \cap S$. Entonces existe $g \in G$ tal que $ng = s$. Como $s \in S_i$ para cada $i \in I$, por el inciso (*e*) de la Observación 2.2.5 tenemos que $g = \frac{1}{n}s \in S_i$ para cada $i \in I$. Así, $g \in S$ y $s = ng \in nS$. ■

*Como una consecuencia del Corolario 2.2.6 tenemos lo siguiente: para cada subgrupo $H$ de $G$ consideramos la familia de subgrupos $\mathscr{A} = \{S \leq G \mid S \text{ es puro y } S \supseteq H\}$, $\mathscr{A} \neq \varnothing$ pues $G \in \mathscr{A}$. Así $K = \bigcap_{S\in\mathscr{A}} S \leq G$ es puro en $G$ y es el mínimo subgrupo puro de $G$ que contiene a $H$. De esta manera hemos demostrado el siguiente corolario.*

**Corolario 2.2.7.** *Cualquier subgrupo de un grupo libre de torsión está contenido en un subgrupo puro mínimo.*

(*f*) *La unión de una cadena ascendente de subgrupos puros es puro. En efecto, sea $G$ un grupo y $\mathscr{C} = \{S_i\}_{i\in I}$ una cadena ascendente de subgrupos puros de $G$. Suponga que $ny = s \in S = \bigcup_{i\in I} S_i$ donde $n \in \mathbb{Z}$ e $y \in G$. Como $s \in S$ existe $j \in I$ tal que $s \in S_j$, por la pureza de $S_j$ existe $s_j \in S_j$ tal que $ns_j = s$; finalmente al ser $s_j \in S$ tenemos que $S$ es puro en $G$.*

**Lema 2.2.8.** *Sean $G$ un grupo, $H$ un subgrupo puro de $G$ y $\overline{y} \in G/H$. Entonces existe $x \in G$ tal que*

*(1)* $\overline{x} = \overline{y}$.

*(2)* $o(x) = o(y)$.

*Demostración.* Denotemos por $\pi : G \longrightarrow G/H$ a la proyección canónica y sea $\overline{y} \in G/H$. Si $o(\overline{y})$ es infinito y $x \in G$ es tal que $\pi(x) = \overline{y}$ necesariamente $o(x)$ es infinito, pues de lo contrario $o(x)\overline{y} = o(x)\pi(x) = \pi(o(x)x) = \pi(0) = \overline{0}$ lo cual es absurdo.

Supongamos ahora que $o(\overline{y}) = m < \infty$ y sea $x' \in G$ tal que $\pi(x') = \overline{y}$. Como $m\overline{y} = \overline{0}$ entonces $\pi(mx') = \overline{0}$ y por lo tanto $mx' = h \in H$, por la pureza de $H$ existe $h' \in H$ tal que $mh' = h$; así $mx' = mh'$ y por consiguiente $m(x' - h') = 0$. Si $x = x' - h' \in G$, entonces $\pi(x) = y$ y como $mx = 0$ tenemos que $o(x) \mid m$, además $o(x)\overline{y} = \overline{0}$ y en consecuencia $m \mid o(x)$; así $o(x) = m$.

■

**Teorema 2.2.9.** *Si $G$ es un grupo y $H$ es un subgrupo puro de $G$ tal que $G/H$ es una suma directa de grupos cíclicos. Entonces $H$ es un sumando directo de $G$.*

*Demostración.* Suponga que $G/H = \bigoplus_{i\in I} \langle \overline{y}_i \rangle$ y sea $\beta = \{x_i\}_{i\in I} \subset G$ tal que para cada $i \in I$ $\pi(x_i) = \overline{y}_i$ y $o(x_i) = o(\overline{y}_i)$ (Lema 2.2.8). Sea $x \in G$ entonces

$$\begin{aligned} \pi(x) &= m_{i_1}\overline{y}_{i_1} + \cdots + m_{i_k}\overline{y}_{i_k} \\ &= m_{i_1}\pi(x_{i_1}) + \cdots + m_{i_k}\pi(x_{i_k}) \\ &= \pi(m_{i_1}x_{i_1}) + \cdots + \pi(m_{i_k}x_{i_k}) \\ &= \pi(m_{i_1}x_{i_1} + \cdots + m_{i_k}x_{i_k}), \end{aligned}$$

así $x - (m_{i_1}x_{i_1} + \cdots + m_{i_k}x_{i_k}) \in H$ y por lo tanto $x \in H + \langle \beta \rangle$.

Suponga ahora que $h \in H \cap \langle \beta \rangle$, entonces $h = m_{i_1}x_{i_1} + \cdots + m_{i_k}x_{i_k}$ y por consiguiente $m_{i_1}\overline{y}_{i_1} + \cdots + m_{i_k}\overline{y}_{i_k} = \overline{0}$, lo que implica que $m_{i_j}\overline{y}_{i_j} = \overline{0}$ para cada $j = 1, \ldots, k$; ya que la suma de los $\langle \overline{y}_i \rangle$'s es directa. Si $o(\overline{y}_{i_j}) = \infty$ entonces $m_{i_j} = 0$; y si $o(\overline{y}_{i_j})$ es finito tenemos que $o(x_{i_j}) = o(\overline{y}_{i_j}) \mid m_{i_j}$ y por lo tanto tenemos que $m_{i_j}x_{i_j} = 0$ para cada $j = 1, \ldots, k$, demostrando que $h = 0$. Por lo tanto $G = H \oplus \langle \beta \rangle$. ■

Concluiremos esta sección con un par de lemas que serán utilizados posteriormente y que tienen que ver con el comportamiento de la noción de pureza bajo homomorfismos.

**Lema 2.2.10.** *Sean $G$ un grupo, $S$ un subgrupo puro de $G$, y $T$ un subgrupo de $G$ tal que $T \supseteq S$ y $T/S$ es puro en $G/S$. Entonces $T$ es puro en $G$.*

*Demostración.* Suponga que

$$ny = t \in T \tag{2.27}$$

con $n \in \mathbb{Z}$, $y \in G$. Pasando al cociente obtenemos $n\overline{y} = \overline{t}$ en $G/S$. Por la pureza de $T/S$ existe $\overline{t}' \in T/S$ tal que $n\overline{t}' = \overline{t}$ y por consiguiente

$$t - nt' = s \in S; \tag{2.28}$$

así, por (2.27), tenemos que $n(y - t') = s$ y por la pureza de $S$ en $T$ existe $s' \in S$ tal que $ns' = s$, sustituyendo en (2.28) obtenemos que $n(s' + t') = t$ donde $s' + t' \in T$ y por lo tanto $T$ es puro en $G$. ■

**Lema 2.2.11.** *Sean $G$ un grupo y $S$ un subgrupo puro de $G$ tal que $nS = 0$. Entonces $(S + nG)/nG$ es puro en $G/nG$.*

*Demostración.* Suponga que $m\overline{y} = \overline{s} \in (S + nG)/nG$ donde $m \in \mathbb{Z}$, $\overline{y} \in G/nG$. Entonces $my - s = nz \in nG$ para algún $z \in G$, y por consiguiente

$$s = my - nz. \tag{2.29}$$

Sea $d = (m, n)$; de (2.29) obtenemos que $s = my - nz = d(m'y - n'z)$ por la pureza de $S$ existe $s' \in S$ tal que $ds' = s$. Sea $d = mr_1 + nr_2$ Entonces

$$\begin{aligned} s &= ds' \\ &= (mr_1 + nr_2)s' \\ &= m(r_1s') + n(r_2s') \end{aligned}$$

pasando al cociente obtenemos que $m\overline{r_1s'} = \overline{s}$ donde $\overline{r_1s'} \in (S + nG)/nG$. Por lo tanto $(S + nG)/nG$ es puro en $G/nG$. ■

## 2.3. Grupos de Orden Acotado

**Definición 2.3.1.** *Un grupo $G$ se llama **de orden acotado** si*

(1) *$G$ es de torsión.*

(2) *Existe $n \in \mathbb{Z}^+$ tal que $nG = 0$.*

**Ejemplo 2.3.2.** (1) *Cualquier grupo finito es de orden acotado.*

(2) *Sea $G = \bigoplus_{\aleph_0} \mathcal{Z}_n$, $\aleph_0$ copias de $\mathcal{Z}_n$. $G$ es un grupo infinito que es de orden acotado, $nG = 0$.*

Veremos en breve que cualquier grupo de orden acotado es un suma directa de grupos cíclicos. De hecho, esta es una generalización del teorema que afirma que un grupo (abeliano) finito es una suma directa de grupos cíclicos.

A priori, no parece haber medios visibles para construir un sumando directo cíclico para un grupo dado de orden acotado. Pero el Lema 2.3.3, que damos a continuación, muestra cómo obtener subgrupos puros cíclicos. Esto ilustra la ventaja que presenta considerar a un subgrupo puro como un substituto temporal para un sumando directo.

**Lema 2.3.3.** *Sea $G$ un grupo $p$-primario, tal que $p^rG = 0$. Si $x \in G$ es de orden $p^r$, entonces $\langle x \rangle$ es puro.*

*Demostración.* Recordamos que en la Proposición 2.1.3 $(d)$ vimos que, si $n \in \mathbb{Z}$ es primo relativo con $p$ entonces $n$ divide a $x$ y por lo tanto a todos los múltiplos enteros de $x$.

Supongamos ahora que

$$ny = mx \in \langle x \rangle ,$$

donde $n, m \in \mathbb{Z}$ y $y \in G$. Resolveremos primero el caso particular $n = p^s$, $m = p^t$ donde $0 < s, t < r$, los restantes casos son consecuencia de éste.

Si $s \leq t$, entonces $p^s \leq p^t$ y

$$p^s(p^{t-s}x) = p^t x$$

con $p^{t-s}x \in \langle x \rangle$.

No puede suceder que $t < s$ pues de lo contrario

$$\begin{aligned} 0 &= p^r y \\ &= p^{r-s}(p^s y) \\ &= p^{r-s}p^t x \\ &= p^{r^{r+t-s}} x \end{aligned}$$

lo cual es absurdo ya que $p^{r+t-s} < p^r = o(x)$.

Hemos demostrado hasta ahora que si $p^s$ divide a $p^t x$ en $G$ entonces $p^s$ divide a $p^t x$ en $\langle x \rangle$. Ahora supongamos que $p^s y = mx$, donde $m = p^\alpha q$ con $(p, q) = 1$. Como $\langle x \rangle = \langle qx \rangle$ (véase la página 3), considerando lo demostrado antes tenemos que como $p^s$ divide a $p^\alpha(qx)$ en $G$ entonces $p^s$ divide a $p^\alpha(qx)$ en $\langle qx \rangle = \langle x \rangle$, es decir, la ecuación $p^s y = mx$ tiene una solución en $\langle x \rangle$. Supóngase ahora que $n = p^s u$ divide a $mx$ en $G$, donde $u$ es primo relativo con $p$. Entonces la ecuación $(p^s u)y = p^s(uy) = mx$ tiene una solución en $\langle x \rangle = \langle ux \rangle$, Supóngase que $w(ux) \in \langle ux \rangle$ es una solución. Entonces $p^s(w(ux)) = mx$, es decir $n(wx) = mx$ con $wx \in \langle x \rangle$. Por lo tanto $\langle x \rangle$ es puro. ■

**Nota 2.3.4.** *Hasta aquí tenemos suficiente información para establecer algunos resultados sobre grupos finitos respecto a su descomposición en suma directa. Consideremos un grupo p-primario finito G; procediendo por inducción sobre el orden del grupo, si $o(G) = 1$ claramente G es una suma directa de grupos cíclicos; así podemos suponer como hipótesis de inducción que todo grupo p-primario finito de orden menor que n es un suma directa de grupos cíclicos, por el Lema 2.3.3 es posible encontrar un subgrupo K de G cíclico y puro, G/K es un grupos p-primario finito de orden menor que n. Entonces, por hipótesis de inducción, G/K es una suma directa de grupos cíclicos; así el Teorema 2.2.9 garantiza que K es un sumando directo de G. De lo anterior concluimos que G es una suma directa de grupos cíclicos.*

Para el caso de grupos infinitos este proceso no es satisfactorio, pues en general en este caso, no podemos garantizar el paso inductivo, ya que muy probablemente $G/K$ es

infinito. La idea entonces es tratar de descomponer al grupo $G$ en una suma directa de subgrupos puros y posteriormente intentar descomponer a los subgrupos puros como una suma directa de subgrupos cíclicos. En este sentido el siguiente lema da condiciones para construir conjuntos independientes.

**Lema 2.3.5.** *Sean $G$ un grupo, $S$ un subgrupo de $G$, $x \in G$ y $\overline{y} \in G/S$ tal que $\overline{x} = \overline{y}$. Suponga que $o(x) = o(\overline{y})$, entonces $S + \langle x \rangle$ es directa.*

*Demostración.* Sea $s \in S \cap \langle x \rangle$ entonces $s = mx$ para alguna $m \in \mathbb{Z}$, pasando al cociente se tiene que $m\overline{y} = \overline{0}$ y por consiguiente $o(x) = o(y) \mid m$, Supóngase que $m = qo(x)$ entonces $s = qo(x)x = 0$ y por lo tanto $S \cap \langle x \rangle = 0$. ■

Para el siguiente Teorema será necesaria la siguiente definición.

**Definición 2.3.6.** *Decimos que un subconjunto $\{x_i\}_{i\in I}$ de un grupo $G$ es un **subconjunto independiente puro** si es independiente y el subgrupo generado $\langle \{x_i\}_{i\in I} \rangle$ es puro (en $G$).*

**Teorema 2.3.7.** *Un grupo de orden acotado es una suma directa de grupos cíclicos.*

*Demostración.* Sea $G$ un grupo de orden acotado. Entonces al ser de torsión, el Teorema 1.3.13 garantiza que $G$ es la suma directa de sus partes $p$-primarias, para varios primos $p$. Sea $G_p$ es la parte $p$-primaria, entonces $p^\alpha G_p = 0$ donde $p^\alpha = \text{máx}\{o(x) \mid x \in G_p\}$, el cual existe pues $G$ es de orden acotado. Así para demostrar el teorema basta verificar que $G_p$ es una suma directa de grupos cíclicos, para cada parte primaria que aparece en la descomposición.

Consideremos el conjunto

$$\mathscr{A} = \{\{x_i\}_{i\in I} \mid \{x_i\}_{i\in I} \text{ es independiente puro}\}.$$

$\mathscr{A} \neq \varnothing$ ya que si $x \in G_p$ es de orden $p^\alpha$ entonces $\langle x \rangle$ es puro (Lema 2.3.3), además $\{x\}$ es independiente y por lo tanto $\{x\} \in \mathscr{A}$.

Claramente $(\mathscr{A}, \subseteq)$ es un conjunto parcialmente ordenado. Veamos que $\mathscr{A}$ verifica las hipótesis del Lema de Zorn. Sea $\mathscr{C} = \{\mathscr{F}_k\}_{k\in K}$ una cadena en $\mathscr{A}$ y consideremos $\mathscr{F} = \bigcup_{k\in K} \mathscr{F}_k$, supongamos que $\mathscr{F} = \{y_{i_k}\}_{i_k \in I_k; k\in K}$. Únicamente mostraremos que $\mathscr{F} \in \mathscr{A}$ pues claramente $\mathscr{F}$ es cota superior en $\mathscr{C}$.

$\mathscr{F}$ es independiente ya que si

$$x \in \langle y_{j_k} \rangle \bigcap \sum_{i \in (\bigcup_{k\in K} I_k) - \{j_k\}} \langle y_i \rangle,$$

entonces $x = m_{j_k} y_{j_k} = \sum_{i_k \neq j_k} m_{i_k} y_{i_k}$ (suma finita). Sea $\mathscr{F}_k \in \mathscr{C}$ tal que $y_{j_k}, y_{i_1}, \ldots, y_{i_s} \in \mathscr{F}_k$ y supongamos que $\mathscr{F}_k = \{y_{i_k}\}_{I_k}$, existe pues $\mathscr{C}$ es una cadena. Como $\mathscr{F}_k$ es independiente entonces

$$\langle y_{j_k} \rangle \bigcap \sum_{r=1}^{s} \langle y_{i_r} \rangle \subseteq \langle y_{j_k} \rangle \bigcap \sum_{i \in I_k - \{j_k\}} \langle y_i \rangle = 0$$

y por lo tanto $x = 0$.
Por otra parte como $\left\{ \langle y_{i_k} \rangle_{i_k \in I_k} \right\}_{k \in K}$ es una cadena ascendente de subgrupos puros, de la Observación 2.2.5 $(f)$, tenemos que $\langle \mathscr{F} \rangle = \bigoplus_{i \in I} \langle y_i \rangle$ es puro, y por lo tanto $\mathscr{F} \in \mathscr{A}$.

Por el Lema de Zorn existe $\{x_i\}_{i \in I} \in \mathscr{A}$ un elemento maximal en $\mathscr{A}$. Sea $S = \bigoplus_{i \in I} \langle x_i \rangle$, debemos demostrar que $S = G_p$. Supongamos que $G_p/S \neq \overline{0}$, como $p^\alpha(G_p/S) = \overline{0}$, $G_p/S$ es un grupo $p$-primario de orden acotado, sea $\overline{y} \in G_p/S$ de orden $o(\overline{y}) = p^\alpha$, por el Lema 2.3.3 $\langle \overline{y} \rangle$ es puro en $G_p/S$ y por el Lema 2.2.8 existe $x \in G_p$ una preimagen de $\overline{y}$ con $o(x) = o(\overline{y})$ de tal manera que, por el Lema 2.3.5, la suma $S + \langle x \rangle$ es directa y como $(S \oplus \langle x \rangle)/S \cong \langle \overline{y} \rangle$ entonces $(S \oplus \langle x \rangle)/S$ es puro en $G_p/S$, así el Lema 2.2.10 asegura que $S \oplus \langle x \rangle$ es puro en $G$. Con lo anterior demostramos que $\mathscr{F} \cup \{x\} \in \mathscr{A}$ lo cual es absurdo ya que $\mathscr{F} \subsetneq \mathscr{F} \cup \{x\}$ contradice la maximalidad de $\mathscr{F}$ en $\mathscr{A}$, por lo tanto $G_p = \bigoplus_{i \in I} \langle x_i \rangle$.

En este caso la unicidad en la descomposición se dejará pendiente; esto será una consecuencia del Teorema 3.2.8 (Teorema de Ulm). ■

Con la ayuda del Teorema 2.3.7 demostraremos un resultado que establecerá una relación entre subgrupos puros y sumandos directos; para ello necesitaremos el siguiente lema preliminar.

Ya hemos visto que un subgrupo puro $S$ no necesariamente es sumando directo del grupo, sin embargo es posible pedir algunas condiciones sobre $S$ para garantizar que sea un sumando directo.

**Lema 2.3.8.** *Sean $S$ y $T$ subgrupos de $G$ tales que $S \cap T = 0$. Si $(S+T)/T$ es un sumando directo de $G/T$, entonces $S$ es un sumando directo de $G$.*

*Demostración.* Supóngase que $G/T = R/T \oplus (S+T)/T$. Entonces $R + (S+T) = G$ y $R \cap (S+T) = T$. Como $T \subseteq R$ entonces $R + T = R$ y por consiguiente $R + S = G$, además $R \cap S \subseteq R \cap (S+T) = T$ de donde $R \cap S \subseteq S \cap T = 0$, es decir, $R \cap S = 0$ y por lo tanto $G = R \oplus S$. ■

Como veremos en la siguiente sección, este resultado será de gran importancia.

**Teorema 2.3.9.** *Sean $G$ un grupo y $S$ un subgrupo de $G$ puro y de orden acotado. Entonces $S$ es un sumando directo de $G$.*

*Demostración.* Como $S$ es de orden acotado existe $n \in \mathbb{Z}^+$ tal que $nS = 0$. Por el Lema 2.2.11, $(S + nG)/nG$ es puro en $G/nG$. Notamos además que $G/nG$ es de orden acotado, $n(G/nG) = \overline{0}$; y por el Teorema 2.3.7, $G/nG$ es una suma directa de grupos cíclicos. Además, por el Teorema 2.2.9, $(S+nG)/nG$ es un sumando directo de $G/nG$, ya que al ser $G/nG$ cíclico entonces $(G/nG)/[(S + nG)/nG]$ también lo es. Por otra parte al ser $S$ puro entonces $S \cap nG = nS = 0$, entonces por el Lema 2.3.8, considerando a $T = nG$, tenemos que $S$ es un sumando directo de $G$. ■

Considerando los Teoremas 2.1.12 y 2.3.9 se obtiene el siguiente teorema.

**Teorema 2.3.10.** *Sea $G$ un grupo y suponga que $t(G) = D \oplus S$, donde $D$ es divisible y $S$ es de orden acotado. Entonces $t(G)$ es un sumando directo de $G$.*

*Demostración.* Del ejemplo 2.2.2, sabemos que $t(G)$ es un subgrupo puro de $G$. Veamos que $S$ también lo es. Supongamos que $ng = s \in S$ para algún $n \in \mathbb{Z}$ y $g \in G$. Como $S \subseteq t(G)$ y $t(G)$ es puro existe $x \in t(G)$ tal que $nx = s$, supongamos que $x = d + s$', entonces tenemos que $nd + ns' = s$ y como $t(G) = D \oplus S$ necesariamente $nd = 0$ y $ns' = s$; por lo tanto $S$ es un subgrupo puro de $G$. Por el el Teorema 2.3.9 tenemos que $S$ es un sumando directo de $G$. Sea $G = H \oplus S$ y $m \in \mathbb{Z}^+$ tal que $mS = 0$. Entonces $D = mD \subseteq mG = m(H \oplus S) = mH + mS = mH \subseteq H$; la primera igualdad es por ser $D$ un subgrupo divisible, así $D$ es un subgrupo de $H$ y por el Teorema 2.1.12 $D$ es un sumando directo de $H$. Sea $H = K \oplus D$. Veamos que $G = K \oplus t(G)$. Claramente $G = K + t(G)$, supóngase ahora que $k \in K \cap t(G)$, entonces $k = d + s$, con $d \in D$ y $s \in S$, despejando obtenemos que $s = k + (-d) \in H \cap S = 0$ y por consiguiente $k = d \in K \cap D = 0$. Por lo tanto $K \cap t(G) = 0$ y $t(G)$ es un sumando directo de $G$. ■

## 2.4. Altura

Anteriormente hemos discutido hasta qué punto un elemento dado en un grupo puede ser dividido por números enteros. En esta sección se introducirá una medida numérica de esta divisibilidad. Sólo nos ocupamos del caso de grupos primarios, no obstante cabe mencionar que este concepto se puede definir en cualquier grupo, véase por ejemplo [Rot] Capítulo 9 §5.

**Definición 2.4.1.** *Sea $G$ un grupo $p$-primario y $x \in G$; la **altura** de $x$, denotada como $\boldsymbol{h_G(x)}$, es*

$$h_G(x) = \begin{cases} n \text{ si } x \text{ es dividido en } G \text{ por } p^n \text{ pero no por } p^{n+1}. \\ \\ \infty \text{ si } x \text{ es divisible por } p^n \text{ para toda } n \in \mathbb{N}. \end{cases} \tag{2.30}$$

**Nota 2.4.2.** *Es claro a partir de la definición que, para cualquier grupo p-primario $G$, $h_G(0) = \infty$. Además para cada $x \in G$, $h_G(x) = h_G(-x)$*

Si $S \leq G$, $h_S(x)$ denotará la altura de $x$ en $S$. Por ejemplo si $h_S(x) = m$ entonces $x \in p^m S$ pero $x \notin p^{m+1}S$; sin embargo es posible que $x \in p^{m+1}(G - S)$ y por esta razón, en general

$$h_S(x) \leq h_G(x) \ \forall \ x \in G. \tag{2.31}$$

Un ejemplo de lo anterior es considerar $S = \mathcal{Z}$ y $G = \mathcal{Q}$. Dado $m \in \mathcal{Z} - \{0\}$ tenemos que

$$h_{\mathcal{Z}}(m) = \begin{cases} 0 & \text{si } p \nmid m \quad \text{en } \mathbb{Z} \\ n & \text{si } p^n \nmid m \quad \text{en } \mathbb{Z}. \end{cases}$$

Por otra parte $h_{\mathcal{Q}}(m) = \infty$.

**Observación 2.4.3.** *Tenemos las siguientes relaciones respecto a la altura en un grupo. Sólo algunas de ellas serán demostradas.*

(*a*) (1) *Si $h_G(x) \neq h_G(y)$ entonces $h_G(x + y) = \text{mín}\{h_G(x), h_G(y)\}$.*
(2) *Si $h_G(x) = h_G(y)$ entonces $h_G(x + y) \geq h_G(x)$.*

*Demostración.* (1) Suponemos que $m = h_G(x) < h_G(y) = n$. Sean $y_1, y_2 \in G$ tales que $p^m y_1 = x$ y $p^n y_2 = y$ y por consiguiente $p^m(y_1 + p^{n-m}y_2) = x + y$, así $h_G(x + y) \geq m = \text{mín}\{m, n\}$. Supongamos que $k = h_G(x + y) > m = \text{mín}\{m, n\}$ y que $p^k z = x + y$. Como $k, n \geq m + 1$ tenemos que $p^{m+1}(p^{k-(m+1)}z - p^{n-(m+1)}y) = x$, con $(p^{k-(m+1)}z - p^{n-(m+1)}y) \in \mathbb{Z}$, esto es un absurdo ya que $h_G(x) = m$. Por lo tanto $h_G(x + y) = \text{mín}\{h_G(x), h_G(y)\}$.

(2) Suponga que $m = h_G(x) = h_G(y)$ y sean $y_1, y_2 \in G$ tales que $p^m y_1 = x$ y $p^n y_2 = y$, entonces $p^m(y_1 + y_2) = x + y$ y por lo tanto $h_G(x + y) \geq m = h_G(x)$. ■

*Dado $x \in G$ es fácil encontrar un elemento $y \in G$ tal que $h_G(x) = h_G(y)$ y $h_G(x+y) > h_G(x)$, a saber $y = -x$; $h_G(x + (-x)) = h_G(0) = \infty > h_G(x)$.*

(*b*) *Como $p^{n-1}(py) = p^n y$ para toda $n \in \mathbb{Z}^+$ y toda $y \in G$, se tiene una cadena descendente*

$$G \supset pG \supset p^2G \supset \cdots \supset p^kG \supset p^{k+1}G \supset \cdots \supset \bigcap_{n>0} p^nG \supset p(\bigcap_{n>0} p^nG) \supset \cdots$$

*Si $x \in G$ tiene altura $n$ entonces existe $y \in G$ tal que $p^n y = x$ y $n$ es la máxima potencia de $p$ que divide a $x$; así $x \in p^nG - p^{n+1}G$. Es decir,*

$$h_G(x) = n \text{ si y sólo si } x \in p^nG - p^{n+1}G.$$

*Además*

$$h_G(x) = \infty \text{ si y sólo si } x \in \bigcap_{n>0} p^n G.$$

(c) *Un grupo p-primario $G$ es divisible si y sólo si $h_G(x) = \infty \ \forall\ x \in G$.*

*Demostración.* Es claro a partir de la Proposición 2.1.3, $(d)$ y de la definición de altura. ■

(d) *El conjunto $H = \{x \in G \mid h_G(x) = \infty\}$ es un subgrupo de $G$.*

*Demostración.* Claramente $0 \in H$; sean $x_1, x_2 \in H$ y $n \in \mathbb{Z}^+$. Entonces, por hipótesis, existen $y_1, y_2 \in G$ tales que $p^n y_1 = x_1$ y $p^n y_2 = x_2$; así $p^n(y_1 - y_2) = x_1 - x_2$ y por consiguiente $x_1 - x_2$ es divisible por cualquier entero positivo, es decir, $x_1 - x_2 \in H$. Por lo tanto $H \leq G$. ■

(e) *La Proposición 1.4.5, muestra que el elemento $\overline{\frac{1}{p}} \in \mathbb{Z}_{p^\infty}$, tiene altura infinita, es decir, $h_{\mathbb{Z}_{p^\infty}}\left(\overline{\frac{1}{p}}\right) = \infty$.*

(f) *Una condición necesaria para que un grupo p-primario $G$ sea una suma directa de grupos cíclicos es que no tenga elementos de altura infinita distintos de* 0.

*Demostración.* Supóngase que $G = \bigoplus_{i \in i} \langle x_i \rangle$ y que además existe $x \in G - \{0\}$ de altura infinita. Sea $x = m_{i_1} x_{i_1} + m_{i_2} x_{i_2} + \cdots + m_{i_k} x_{i_k}$. El hecho de que $x \in p^n G$ para toda $n \in \mathbb{Z}^+$ implica que $m_{i_j} x_{i_j} \in p^n \langle x_{i_j} \rangle$ para toda $n \in \mathbb{Z}^+$ y para toda $j = 1, \ldots, k$. Así, por el inciso $(c)$ anterior, $\langle m_{i_j} x_{i_j} \rangle \leq \langle x_{i_j} \rangle$ es un subgrupo divisible para toda $j = 1, \ldots, k$. Pero sabemos que un grupo cíclico no es divisible y por consiguiente el único subgrupo divisible que posee es el cero; así $\langle m_{i_j} x_{i_j} \rangle = 0$ para toda $j = 1, \ldots, k$ y en consecuencia $m_{i_j} x_{i_j} = 0$ para toda $j = 1, \ldots, k$, lo que implica que $x = 0$ que es absurdo ya que $x \neq 0$. Por lo tanto si $G = \bigoplus_{i \in i} \langle x_i \rangle$ entonces $G$ no tiene elementos de altura infinita distintos de cero. ■

En virtud de que la divisibilidad en grupos $p$-primarios se reduce a la divisibilidad por potencias de $p$ hacemos una reformulación de la definición de pureza.

**Definición 2.4.4.** *Sea $G$ un grupo p-primario. Un subgrupo $S$ de $G$ es puro si para toda $s \in S$*

$$h_S(s) = h_G(s).$$

El siguiente lema justifica aún más la Definición 2.4.4 y deja ver, por primera vez, cómo el zoclo de un $p$-grupo determina la naturaleza de todo el grupo.

**Lema 2.4.5.** *Sea $G$ un grupo $p$-primario y $S$ un subgrupo de $G$ sin elementos de altura infinita (salvo 0). Suponga que los elementos de orden $p$ en $S$ tienen la misma altura en $S$ como en $G$. Entonces $S$ es puro.*

*Demostración.* La demostración será por inducción sobre el orden de los elementos de $S$.

Sea $s \in S$ con $o(s) = p^k$. Si $k = 1$, por hipótesis, $h_S(s) = h_G(s)$. Suponemos como hipótesis de inducción que, para todo $s \in S$ de orden $p^k$, $h_S(s) = h_G(s)$. Sea $s \in S$ de orden $p^{k+1}$, entonces $ps$ es de orden $p^k$ y por hipótesis de inducción $h_G(ps) = h_S(ps)$. Sea $h_G(s) = m$, entonces existe $y \in G$ tal que $p^m y = s$, multiplicando tenemos que $p^{m+1}y = ps$, esto implica que $m+1 \leq h_G(ps) = h_S(ps)$, es decir, $m+1 \leq h_S(ps)$ entonces existe $s$'$\in S$ tal que $p^{m+1}s' = ps$, así $p(s - p^m s') = 0$ y por lo tanto $s - p^m s$' es de orden $p$. De aquí tenemos que

$$h_S(s - p^m s') = h_G(s - p^m s'). \tag{2.32}$$

Como $p^m(y - s') = s - p^m s'$, $p^m$ divide a $s - p^m s$' en $G$, por (2.32) tenemos que existe $s$" $\in S$ tal que $p^m s" = s - p^m s'$; por lo tanto $p^m(s' + s") = s$, es decir, $h_G(s) = h_S(s)$. Lo anterior demuestra que para toda $s \in S$, $h_S(s) = h_G(s)$ y por lo tanto $S$ es puro en $G$. ■

El siguiente lema es consecuencia del inciso $(c)$ de la Observación 2.4.3 y muestra un vez más cómo el zoclo de un grupo $p$-primario describe la naturaleza del grupo entero.

**Lema 2.4.6.** *Sea $G$ un grupo $p$-primario y suponga que todos los elementos de orden $p$ en $G$ tienen altura infinita. Entonces $G$ es divisible.*

*Demostración.* Demostraremos por inducción sobre el orden de los elementos de $G$ que todos ellos son de altura infinita.

Si $G = G[p]$, por la Observación 2.4.3 $(c)$ $G$ es divisible. Supongamos como hipótesis de inducción que todos los elementos de $G$ de orden $p^k$ son de altura infinita. Sea $a \in G$ de orden $p^{k+1}$, entonces $pa$ es de orden $p^k$ y por hipótesis de inducción $pa$ tiene altura infinita. Sea $m \in \mathbb{Z}^+$, queremos resolver la ecuación $p^m x = a$. Como $h(pa) = \infty$ existe $y \in G$ tal que $p^{m+1}y = pa$ y por consiguiente $p(a - p^m y) = 0$, es decir, $(a - p^m y) \in G[p]$ y por hipótesis $h(a - p^m y) = \infty$; así existe $y' \in G$ tal que $p^m y' = a - p^m y$ y por lo tanto $p^m(y + y') = a$. Así $h(g) = \infty$ para toda $g \in G$ y por lo tanto, a partir de la Observación 2.4.3 $(c)$, tenemos que $G$ es divisible. ■

El siguiente es un resultado técnico que facilitará la demostración de algunos de los siguientes resultados.

**Proposición 2.4.7.** *Sean $G$ en un grupo $p$-primario y $a \in G[p]$ con altura $h_G(a) = r < \infty$. Si*

$$p^r y = a, \tag{2.33}$$

*y $H = \langle y \rangle$ entonces $H[p] = \langle a \rangle$ y $H$ es puro en $G$.*

*Demostración.* Veamos primero que $H[p] = \langle a \rangle$; claramente $\langle a \rangle \subseteq H[p]$. Para la otra contención notamos a partir de la elección de $y$ que $o(y) = p^{r+1}$. Sea $x = my \in H[p]$, como $(pm)y = px = 0$ entonces $p^{r+1}|pm$ de donde $p^r|m$; así $m = qp^r$ y por consiguiente $x = qp^r y \in \langle a \rangle$. De esta manera tenemos que $H[p] \subseteq \langle a \rangle$ y por lo tanto $H[p] = \langle a \rangle$. Para demostrar la pureza de $H$ veremos que satisface las hipótesis del Lema 2.4.5. $H$ no tiene elementos de altura infinita por ser un grupo cíclico (véase la Observación 2.4.3, $(f)$). Verificaremos ahora que los elementos de $H[p] = \langle a \rangle$ tienen la misma altura en $H$ como en $G$. Observamos, a partir de la definición de $H$, que $h_H(a) = h_G(a) = r$. Sea $x = ma \in H[p]$, donde $(m, p) = 1$, con $h_G(x) = n$. A partir de (2.33) tenemos que $n \geq r$, más aún $h_H(x) \geq r$ ya que $p^r my = ma = x$. Si $m > r$ entonces existe $z \in G$ tal que

$$p^n z = x = ma; \tag{2.34}$$

como $(m, p) = 1$ existen $r_1, r_2 \in \mathbb{Z}$ tales que $r_1 m = 1 + pr_2$, multiplicando (2.34) por $r_1$ tenemos que

$$p^n(r_1 z) = a,$$

que es absurdo ya que $h_G(a) = r < n$. Así, debe ser $n = r$ lo que implica $r \leq h_H(x) \leq h_G(x) = r$ y por lo tanto $h_H(x) = h_G(x) = r$. Finalmente por el Lema 2.4.5 tenemos que $H$ es un subgrupo puro de $G$. ■

**Teorema 2.4.8.** *Sea $G$ un grupo reducido que no es libre de torsion. Entonces $G$ tiene un sumando directo cíclico finito.*

*Demostración.* Comenzaremos demostrando el caso particular en el que $G$ es un grupo $p$-primario. Como $G$ no es divisible necesariamente existe un elemento $x \in G[p]$ de altura $h_G(x) = m$ finita, de lo contrario $G$ sería divisible (Lema 2.4.6) lo que es absurdo ya que $G$ es reducido.

Sean $y \in G$ tal que $p^m y = x$ y $H = \langle y \rangle$. De la Proposición 2.4.7 sabemos que $H$ es puro, y como es de orden acotado, ya que $p^{m+1}H = 0$, entonces por el Teorema 2.3.9 $H$ es un sumando directo de $G$ quedando demostrado el teorema para este caso.

Ahora al caso general; sea $G$ un grupo arbitrario, como $G$ no es libre de torsión $t(G) \neq 0$ y por consiguiente $t(G)$ es la suma directa de sus partes primarias (Teorema 1.3.13). Sea $0 < S < t(G)$ una parte primaria, como $G$ es reducido necesariamente $S$ no es divisible y

por el caso anterior $S$ contiene un subgrupo cíclico finito $H$ que es un sumando directo y por consiguiente un subgrupo puro de $S$ (véase la página 44). De la misma manera, al ser $S$ un sumando directo de $t(G)$, $S$ es puro en $t(G)$; por lo tanto de la Observación 2.2.5 $(a)$ $H$ es puro en $t(G)$, y como $t(G)$ es puro en $G$ finalmente $H$ es puro en $G$, es decir, $H$ es un subgrupo de $G$ puro y de orden acotado, por lo tanto el Teorema 2.3.9 asegura que $H$ es un sumando directo de $G$. ■

Terminamos esta sección con el siguiente teorema consecuencia del Teorema 2.4.8 y para lo cual es necesaria la siguiente definición.

**Definición 2.4.9.** *Un grupo $G \neq 0$ es **inescindible** si*

$$G = H \oplus K \implies (\ H = 0\ \vee\ K = 0).$$

**Ejemplo 2.4.10.** $(a)$ *El grupo aditivo de los números enteros $\mathcal{Z}$ es inescindible pues si sucede que $\mathcal{Z} = m\mathcal{Z} \oplus n\mathcal{Z}$, entonces $(m, n) = 1$ y como $0 = m\mathcal{Z} \cap n\mathcal{Z} = [m, n]\mathcal{Z} = mn\mathcal{Z}$ entonces $mn = 0$ y por lo tanto o $m\mathcal{Z} = 0$ o $n\mathcal{Z} = 0$.*

$(b)$ *El grupo aditivo de las clases residuales módulo un primo $p$ es inescindible ya que cualquier subgrupo de $\mathcal{Z}_p$ necesariamente es cíclico, y si $\mathcal{Z}_p = \langle \overline{h} \rangle \oplus \langle \overline{k} \rangle$ como*

$$(k, p) = \begin{cases} 1 \\ \acute{o} \\ p \end{cases} \quad y \quad (h, p) = \begin{cases} 1 \\ \acute{o} \\ p \end{cases}$$

*no puede suceder que $(h, p) = (k, p) = 1$, pues de lo contrario $\mathcal{Z}_p = \mathcal{Z}_p \oplus \mathcal{Z}_p$ que es absurdo; así o $(h, p) = p$ o $(k, p) = p$ y por lo tanto o $\langle \overline{h} \rangle = 0$ o $\langle \overline{k} \rangle = 0$.*

$(c)$ *El grupo $\mathcal{Z}_{p^\infty}$ es inescindible ya que si $\mathcal{Z}_{p^\infty} = H \oplus K$ entonces al ser $H$ y $K$ subgrupos de $\mathcal{Z}_{p^\infty}$, de la Proposición 1.4.5 sabemos que si ambos son propios entonces $H = \left\langle \overline{\frac{1}{p^{m_1}}} \right\rangle$ y $K = \left\langle \overline{\frac{1}{p^{m_2}}} \right\rangle$, con $m_1 \neq 0 \neq m_2$, y por consiguiente, si $m_1 \leq m_2$, $\mathcal{Z}_{p^\infty} = \left\langle \overline{\frac{1}{p^{m_1}}} \right\rangle \oplus \left\langle \overline{\frac{1}{p^{m_2}}} \right\rangle = \left\langle \overline{\frac{1}{p^{m_2}}} \right\rangle$ lo que es absurdo. Así necesariamente $H = 0$ o $K = 0$.*

**Teorema 2.4.11.** *Un grupo inescindible no puede ser mixto, es decir, o es un grupo de torsión o un grupo libre de torsion. Si es de torsión, es isomorfo a $\mathcal{Z}_{p^n}$ o $\mathcal{Z}_{p^\infty}$ para algún primo $p$.*

*Demostración.* Sea $G$ un grupo inescindible, si $G$ es libre de torsión no tenemos nada que demostrar. Supongamos ahora que $t(G) \neq 0$. Si $G$ es divisible entonces $t(G)$ es un subgrupo divisible (Lema 2.1.21) y por lo tanto un sumando directo de $G$ (Teorema 2.1.12). Por ser $G$ inescindible necesariamente $t(G) = G$. Considerando el Teorema 2.1.25 obtenemos que

$G \cong \mathcal{Z}_{p^\infty}$ para algún número primo $p$. Supongamos ahora que $G$ es reducido, entonces $G$ satisface las hipótesis del Teorema 2.4.8 y por lo tanto $G$ tiene un sumando directo cíclico finito $\langle x \rangle$. Al ser $G$ inescindible necesariamente $G = \langle x \rangle$ y por lo tanto $G \cong \mathcal{Z}_{p^n}$ para algún número primo $p$ y alguna $n \in \mathbb{Z}^+$. ■

## 2.5. Suma Directa de Grupos Cíclicos

**Lema 2.5.1.** *Sean $G$ un grupo $p$-primario sin elementos de altura infinita, $H$ un subgrupo de $G$ puro y finito, y $x \in G$. Entonces existe un subgrupo finito puro de $G$ que contiene a $H$ y $x$.*

*Demostración.* $H$ es de de orden acotado por ser finito y como por hipótesis de puro, el Teorema 2.3.9 asegura que $G = H \oplus K$ para algún subgrupo $K$ de $G$. Sea $x = h + k$ con $h \in H$, $k \in K$ y sea $o(k) = p^m$. Para la demostración procedemos por inducción sobre $m$.

Si $m = 0$, entonces $x \in H$ y no hay nada que demostrar. Suponemos como hipótesis de inducción que si $x = h + k$ con $o(k) = p^m$, entonces existe un subgrupo finito puro que contiene a $H$ y a $x$. Sea $x = h + k$ con $k \in K$ y $o(k) = p^{m+1}$. Entonces $px = ph + pk$, como $ph \in H$ y $pk \in K$ con $o(pk) = p^m$, por hipótesis de inducción existe $H' \leq G$ finito puro que contiene a $H$ y a $px$. Al ser $H'$ finito, es de orden acotado, y nuevamente por el Teorema 2.3.9, $G = H' \oplus K'$. Sea $k = h' + k'$ donde $h' \in H'$ y $k' \in K'$, sustituyendo obtenemos que $x = (h + h') + k'$, así $pk' = px - p(h + h') \in H'$, por lo que $pk' \in H' \cap K' = 0$. Sea $h_G(k') = n < \infty$, esto es porque $G$ no tiene elementos de altura infinita, entonces existe $u \in G$ tal que $p^n u = k'$. Por la Proposición 2.4.7 tenemos que $L = \langle u \rangle$ es puro en $G$.

Sea $H'' = H' + L$, $H''$ es finito y contiene a $H$ y a $x$. Para ver que $H''$ es puro comenzamos mostrando que $H''$ es la suma directa de $H'$ y $L$.

Sea $h' \in H' \cap L$. Si $h' \neq 0$ entonces $h' = mu$, donde $p^n \nmid m$ ya que de lo contrario $h' = m'p^n u = m'k' \in H' \cap K' = 0$ que es absurdo. Sea $m = p^s m'$ con $0 \leq s < n$ y $(m', p) = 1$. Entonces $p^{n-s}h' = m'k' \in H' \cap K' = 0$, es decir, $m'k' = 0$ y por lo tanto $p|m'$ contradiciendo la hipótesis de que $(m', p) = 1$. Así $h' = 0$ y $H'' = H' \oplus L$.

Veamos ahora la pureza de $H''$ en $G$. Sea $t = h_1 + l \in H''$ y supongamos que

$$p^r y = t \tag{2.35}$$

donde $y = h_2 + \widetilde{k} \in G$, con $h_2 \in H'$ y $\widetilde{k} \in K'$ entonces, por ser $H'' = H' \oplus L$, $p^r h_2 = h_1$ y $p^r \widetilde{k} = l$. Por la pureza de $L$ existe $l' \in L$ tal que $p^r l' = l$; así $p^r(h_2 + l') = t$ donde $(h_2 + l') \in H''$. Por lo tanto $H''$ es un subgrupo finito puro de $G$ que contiene a $H$ y a $x$. ■

**Teorema 2.5.2.** *Si $G$ es un grupo p-primario numerable sin elementos de altura infinita, entonces $G$ es una suma directa de grupos cíclicos.*

*Demostración.* Suponemos $G = \{x_i\}_{i=1}^{\infty}$. Aplicaremos repetidamente el Lema 2.5.1, para encontrar una sucesión de subgrupos $H_i$ con las siguientes propiedades:

$(a)$ $H_1 \subseteq H_2 \subseteq H_3 \subseteq \cdots$,

$(b)$ Cada $H_i$ es finito y puro en $G$.

$(c)$ $x_n \in H_n$

En efecto, considerando el subgrupo trivial 0 de $G$ y el Lema 2.5.1, tenemos que existe un subgrupo puro finito $H_1 \leq G$ que contiene a $x_1$. Si $x_2 \in H_1$ definimos $H_2 = H_1$; si no, nuevamente por el Lema 2.5.1 encontramos un subgrupo $H_2 \leq G$ puro y finito que contiene a $H_1$ y a $x_2$. Siguiendo esta idea definimos en forma recursiva

$$H_{i+1} = \begin{cases} H_i & \text{si} \quad x_{i+1} \in H_i \\ \\ \widetilde{H}_{i+1} & \text{si} \quad x_{i+1} \notin H_i, \end{cases}$$

donde $\widetilde{H}_{i+1}$ el subgrupo finito puro, que se obtiene del Lema 2.4.5, y que contiene a $H_i$ y a $x_{i+1}$

Así obtenemos una sucesión de subgrupos finitos puros $\{H_i\}_{i\in\mathbb{Z}^+}$ que satisfacen $(a)$, $(b)$ y $(c)$.

Por el Teorema 2.3.9, cada $H_i$, con $i \in \mathbb{Z}^+$, es sumando directo de $H_{i+1}$. Sea $H_{i+1} = H_i \oplus K_i$, entonces

$$\begin{aligned} H_{i+1} &= H_i \oplus K_i \\ &= H_{i-1} \oplus K_{i-1} \oplus K_i \\ &= H_{i-2} \oplus K_{i-2} \oplus K_{i-1} \oplus K_i \\ &\quad \vdots \qquad \vdots \qquad \vdots \\ &= H_1 \oplus K_1 \oplus K_2 \oplus \ldots \oplus K_{i-1} \oplus K_i \end{aligned}$$

es decir, para toda $i \in \mathbb{Z}^+$

$$H_i = H_1 \oplus K_1 \oplus K_2 \oplus \ldots \oplus K_{i-1}. \tag{2.36}$$

Claramente $G = \bigcup_{i\in\mathbb{Z}^+} H_i$, veamos que $G = H_1 \oplus (\bigoplus_{i\in\mathbb{Z}^+} K_i)$. Sea $x \in G$ entonces $x \in H_j$ para algún $j \in \mathbb{Z}^+$, por (2.36) tenemos que $x \in H_1 \oplus K_1 \oplus K_2 \oplus \ldots \oplus K_{j-1} \subseteq H_1 + \sum_{i\in\mathbb{Z}^+} K_i$. por lo tanto $G = H_1 + \sum_{i\in\mathbb{Z}^+} K_i$. Veamos que la suma $H_1 + \sum_{i\in\mathbb{Z}^+} K_i$ es directa; sea $h \in H_1 \cap \sum_{i\in\mathbb{Z}^+} K_i$

entonces $h = \sum_{j=1}^{l} k_{i_j}$ con $k_{i_j} \in K_{i_j}$. Suponemos sin perdida de generalidad que $i_j < i_{j+1}$ para cada $j = 1, \ldots, l-1$, entonces $h \in H_1 \cap \sum_{i=1}^{i_l} K_i = 0$ (esta igualdad es debido a (2.36)) lo que implica que $h = 0$. Con un argumento similar al anterior obtenemos que $K_j \cap (H_1 + \sum_{i \in \mathbb{Z}^+ - \{j\}} K_i) = 0$ para todo $j \in \mathbb{Z}^+$. Por lo tanto

$$G = H_1 \oplus K_1 \oplus K_2 \oplus \cdots \oplus K_n \oplus \cdots$$

donde cada sumando es finito y por lo tanto cada uno de ellos es una suma directa de grupos cíclicos. ■

**Nota 2.5.3.** *Cabe mencionar que el Teorema 2.5.2 no es válido si se suprime la hipótesis de que $G$ es numerable. Un ejemplo de esto se da en la Proposición 3.2.12 $(b)$.*

**Lema 2.5.4.** *Sean $G$ un grupo p-primario, $H$ un subgrupo puro de $G$ y $x \notin H$ de orden $p$. Supóngase que $h_G(x) = r < \infty$ y que $h_G(x+a) \leq h_G(x)$ para cualquier $a \in H$ con $pa = 0$. Escribiendo $x = p^r y$, y $K = \langle y \rangle$; sea $L = H + K$. Entonces $L$ es la suma directa de $H$ y $K$, y $L$ es puro.*

*Demostración.* Mostraremos primero que $L = H + K$ es directa. Para ello veremos que cualquier subgrupo de $K$ distinto de 0 contiene a $x$. Sea $K$' un subgrupo de $K$ distinto de cero, entones $K' = \langle my \rangle$ donde $p^{r+1} \nmid m$. Supóngase que $m = p^s q$ con $0 \leq s < r+1$ y $(p, q) = 1$. Sean $t_1, t_2 \in \mathbb{Z}$ tales que $1 = t_1 p + t_2 q$, entonces

$$\begin{aligned} x &= p^r y \\ &= p^r(t_1 p + t_2 q)y \\ &= p^{r+1} t_1 y + p^r t_2 q y \\ &= p^r (t_2 q) y \\ &= p^{r-s} t_2 p^s q y \\ &= (p^{r-s} t_2) m y \in K'. \end{aligned}$$

Con esto hemos visto que cualquier subgrupo distinto de cero de $K$ contiene a $x$. Por otra parte, $H \cap K$ es un subgrupo de $K$ y claramente no contiene a $x$; así necesariamente $H \cap K = 0$ y por lo tanto $L = H \oplus K$.

Veremos ahora que $L$ es puro; para ello consideraremos nuevamente el Lema 2.4.5 y recordamos además que $L[p] = H[p] \oplus K[p]$.

Sea $l \in L[p]$, entonces $l = \eta + mx$.[4] Si $p \mid m$ entonces $l = \eta \in H[p]$ y por consiguiente

$$h_G(l) = h_G(\eta) = h_H(\eta) = h_H(l).$$

[4]Estamos utilizando la primera parte de la Proposición 2.4.7, a saber, $K[p] = \langle x \rangle$

Supongamos ahora que $l = \eta + mx$ y que $(m, p) = 1$. Veremos primero que en el caso de que $m = 1$, la altura de $l$ en $H$ coincide con la altura de $l$ en $G$. Así, supongamos que $l = \eta + x$ y que $h_G(l) = s$, entonces existe $z \in G$ tal que $p^s z = l = \eta + x = \eta + p^r y$. Si $s \leq r$ tenemos que $p^s(z - p^{r-s}y) = \eta$ y como $H$ es puro, existe $\eta' \in H$ tal que $p^s\eta' = \eta$, entonces $l = \eta + x = p^s\eta' + p^r y = p^s(\eta' + p^{r-s}y)$ donde $\eta' + p^{r-s}y \in L$. El caso $r < s$ no puede suceder ya que de lo contrario $s = h_G(\eta + x) \leq h_G(x) = r < s$ que es absurdo. Por lo tanto, para $l = \eta + x$, $h_G(l) = h_L(l)$.

Para el caso en que

$$l = \eta + mx \tag{2.37}$$

con $(m, p) = 1$, la misma demostración funciona, ya que existen $\alpha, \beta \in \mathbb{Z}$ con la propiedad de que $\alpha m = 1 + \beta p$; multiplicando por $\alpha$ la igualdad (2.37) obtenemos la ecuación

$$\alpha l = \alpha\eta + x.$$

Por el caso anterior, $h_L(\alpha l) = h_G(\alpha l)$. Como $h_G(tz) = h_G(z)$ para todo $z \in G$ de altura finita y $t \in \mathbb{Z}$ (véase en la demostración de la Proposición 2.4.7), tenemos que $h_H(l) = h_H(\alpha l) = h_G(l)$; así hemos demostrado que los elementos de $L[p]$ tienen la misma altura en $L$ como en $G$ y por lo tanto el Lema 2.4.5 asegura que $L$ es puro. ■

**Nota 2.5.5.** *Un caso particular del Lema 2.5.4 es la segunda afirmación que se da en la Proposición 2.4.7 pues basta considerar $H = 0$. Si este es el caso, el Lema 2.5.4 nos dice que, si $x$ es un elemento distinto de cero de orden $p$ en grupo $p$-primario $G$ y de altura $h_G(x) = r < \infty$; y si $p^r y = x$ entonces el grupo $\langle y \rangle$ es puro en $G$.*

Con el fin de facilitar la redacción del siguiente lema así como la escritura de su demostración, entenderemos $\{x_i\}$ como un conjunto donde $i$ pertenece a algún conjunto de índices.

**Lema 2.5.6.** *Sean $G$ un grupo $p$-primario, $Q$ y $R$ subgrupos de $G[p]$ tales que $Q \subseteq R \subseteq G[p]$ y supongamos que $R$ de altura acotada (es decir, existe una constante $k \in \mathbb{Z}^+$ tal que $h_G(a) \leq k$ para toda $a \in R$). Si $\{x_i\}$ un conjunto independiente puro, en $G$, que satisface $\sum \langle x_i \rangle \cap G[p] = Q$. Entonces $\{x_i\}$ puede extenderse a un subconjunto independiente puro (de $G$) $\{y_j\}$ que satisface $\sum \langle y_j \rangle \cap G[p] = R$.*

*Demostración.* Utilizaremos el Lema de Zorn para la demostración. Sea

$$\mathscr{A} = \{\{y_j\} \mid \{y_j\} \supset \{x_i\} \text{ es independiente puro y } \textstyle\sum \langle y_j \rangle \cap G[p] \subseteq R\}$$

$\mathscr{A} \neq \varnothing$ pues $\{x_i\} \in \mathscr{A}$. Claramente $(\mathscr{A}, \subseteq)$ es un conjunto parcialmente ordenado, y si $\mathscr{C}$ es una cadena en $\mathscr{A}$, entonces $\bigcup_{\{y_j\} \in \mathscr{C}} \{y_j\}$ es independiente puro y por lo tanto una cota superior de $\mathscr{C}$ en $\mathscr{A}$.

Sea $\{y_j\}$ un elemento maximal en $\mathscr{A}$. Veamos que $\sum \langle y_j \rangle \cap G[p] = R$. Sea $H = \sum \langle y_j \rangle$, entonces $H[p] = H \cap G[p] = \sum \langle y_j \rangle \cap G[p]$. Supongamos que existe $a \in R - H[p]$, como $R \subseteq G[p]$ necesariamente $a \notin H$. Sea $B = a + H[p] \subset R$. Al ser $R$ de altura acotada existe $x \in B$ tal que $h_G(x) = r$ es máximo en $\{h_G(b) \mid b \in B\}$. En virtud de que $B = x + H[p]$ tenemos que $H$ y $x$ satisfacen las hipótesis del Lema 2.5.4. Sea $y \in G$ tal que $p^r y = x$, entonces $\{y_j\} \cup \{y\}$ es independiente puro y por consiguiente $\{y_j\} \cup \{y\} \in \mathscr{A}$, además $y \notin \{y_j\}$ pues de lo contrario $x = p^r y \in H$ que es absurdo. Así $\{y_j\} \subsetneq \{y_j\} \cup \{y\}$ que nuevamente es absurdo pues contradice la maximalidad de $\{y_j\}$. Por lo tanto $\sum \langle y_j \rangle \cap G[p] = H[p] = R$. ■

**Lema 2.5.7.** *Sea $G$ un grupo p-primario, y $H$ un subgrupo puro que contiene a todos los elementos de orden $p$ en $G$. Entonces $H = G$.*

*Demostración.* Sea $x \in G$ con $o(x) = p^m$. Demostraremos que $x \in H$ por inducción sobre $m$.

Si $m = 1$, $x \in H$ por hipótesis. Supongamos como hipótesis de inducción que, todos los elementos de orden $p^m$ pertenecen a $H$. Sea $x \in G$ con $o(x) = p^{m+1}$, entonces $px$ es de orden $p^m$ y por lo tanto $px \in H$. Por la pureza de $H$, existe $y \in H$ tal que $py = px$ y por consiguiente $p(x - y) = 0$, es decir, $x - y \in H$ lo cual implica que $x \in H$. Por lo tanto $H = G$. ■

**Teorema 2.5.8.** *Sea $G$ un grupo p-primario. Una condición necesaria y suficiente para que $G$ sea una suma directa de grupos cíclicos es que $G[p]$ sea la unión de una sucesión ascendente de subgrupos de altura acotada.*

*Demostración.* Veremos primero la condición necesaria. Supóngase que $G = \bigoplus_{i \in I} \langle x_i \rangle$. Por el Teorema 1.3.19

$$G[p] = \bigoplus_{i \in I} (\langle x_i \rangle [p]). \tag{2.38}$$

Sea $P_n$ la suma de los primero $n$ sumandos directos de $G[p]$ que aparecen en (2.38). Claramente se tiene que

$$P_1 \leq P_2 \leq \cdots \leq P_n \leq \cdots , \quad \bigcup_{n=1}^{\infty} P_n = G[p].$$

Sólo falta verificar que cada $P_n$ es de altura acotada. Sabemos por la Observación 2.4.3, $(f)$ que, $G$ no tiene elementos de altura infinita por ser una suma directa de grupos cíclicos, además, para cada $n \in \mathbb{Z}^+$, $P_n$ es un subgrupo finito de $G$ así que tiene sentido considerar $k_n = \text{máx}\{h_G(x) \mid x \in P_n\}$. Por lo tanto $P_n$ es un subgrupo de $G$ de altura acotada precisamente por $k_n$.

Probaremos ahora la condición suficiente. Supongamos que $G[p] = \bigcup_{i\in I} P_i$ donde

$$P_1 \subset P_2 \subset P_3 \subset \cdots,$$

y cada $P_i$ es de altura acotada;[5] más aún cada $P_i$ es de orden acotado, ya que $pP_i = 0$ para cada $i$. La idea de la demostración es construir un subgrupo puro $H$ de $G$ que sea una suma directa de grupos cíclicos y que contenga a $G[p]$, entonces por el Lema 2.5.7 necesariamente $H = G$ demostrando así la afirmación.

Para comenzar a realizar esta tarea encontraremos, en forma recursiva, subconjuntos independientes puros $X_i$ con las siguientes propiedades:

(1) $X_i \subset X_{i+1}$.

(2) $\langle X_i\rangle \cap G[p] = P_i$.

Sea $x \in P_1$, $x \neq 0$. Como $P_1$ es de altura acotada existe $y \in G$ tal que $p^{h_G(x)}y = x$. por lo dicho en la Nota 2.5.5, $\langle y\rangle$ es un subgrupo puro de $G$. Aplicando el Lema 2.5.6 a los subgrupos $\langle y\rangle \subseteq P_1 \subseteq G[p]$ y al subconjunto independiente puro $\{y\}$ obtenemos un subconjunto independiente puro $X_1$ con la propiedad de que $\langle X_1\rangle \cap G[p] = P_1$. Supongamos ahora que se han construido $X_1, X_2, \ldots, X_r$ subconjuntos independientes puros que satisfacen (1) y (2). Aplicando nuevamente el Lema 2.5.6 ahora al los subgrupos $P_r \subseteq P_{r+1} \subseteq G[p]$ y al subconjunto independiente puro $X_r$, obtenemos una subconjunto independiente puro $X_{r+1}$ que extiende a $X_r$ con la propiedad de que $\langle X_{r+1}\rangle \cap G[p] = P_{r+1}$.

Sea $H = \bigcup_{i\in\mathbb{Z}^+} \langle X_i\rangle$, por construcción, $H$ es un subgrupo puro de $G$ que es una suma directa de grupos cíclicos. Consideremos lo siguiente

$$\begin{aligned} G[p] &= \bigcup_{i\in I} P_i \\ &= \bigcup_{i=1}^{\infty} (\langle X_i\rangle \cap G[p]) \\ &= H \cap G[p], \end{aligned}$$

es decir, $G[p] = H \cap G[p]$ mostrando que $G[p] \subseteq H$. De esta manera, hemos construido un subgrupo puro $H$ que contiene a todos los elementos de orden $p$ y por el Lema 2.5.7 necesariamente $G = H$; por lo tanto $G$ es una suma directa de grupos cíclicos. ■

**Teorema 2.5.9.** *Sea $G$ un grupo $p$-primario que es una suma directa de grupos cíclicos. Entonces cualquier subgrupo $H$ de $G$ es una suma directa de grupos cíclicos.*

[5] Hemos indicado los subgrupos según la cadena ascendente, que existe por hipótesis.

*Demostración.* Sea $G = \bigoplus_{i\in I} \langle x_i \rangle$ y $H$ un subgrupo de $G$. Definimos $P_n$ igual que en el Teorema 2.5.8; así

$$G[p] = \bigcup_{n=1}^{\infty} P_n. \tag{2.39}$$

Consideremos lo siguiente

$$\begin{aligned} H[p] &= H \cap G[p] \\ &= H \cap \bigcup_{n=1}^{\infty} P_n \\ &= \bigcup_{n=1}^{\infty} (H \cap P_n). \end{aligned}$$

Definimos, para cada $n \in \mathbb{Z}^+$, $H_n = H \cap P_n$, entonces

$$H_1 \leq H_2 \leq \cdots \leq H_n \leq \cdots \ , \quad \bigcup_{n=1}^{\infty} H_n = H[p].$$

Además, al ser $P_n$ de altura acotada, para cada $n \in \mathbb{Z}^+$ (en $G$), también $H_n$ es de altura acotada (en $H$); así el Teorema 2.5.8 asegura que $H$ es la suma directa de grupos cíclicos. ■

# Capítulo 3

# El Teorema de Ulm

En esta primer sección damos una definición más rigurosa de la noción de Altura, con la cual definiremos los *invariantes de Ulm*. La segunda sección, como su nombre lo indica, está dedicada a la demostración del Teorema de Ulm, es aquí donde se ve que para lograr dar una clasificación una condición crucial es la numerabilidad del grupo, sin la cual dicho resultado sería falso.

## 3.1. Regreso a la Noción de Altura

Sabemos del Teorema 1.3.13 que un grupo de torsión tiene una descomposición única, en sentido estricto, como suma directa de sus partes primarias; así que para describir a un grupo de torsión numerable basta obtener una descripción para cada parte primaria que aparece en dicha descomposición. Es por esta razón que en la presente sección nos limitamos a estudiar grupos primarios numerables.

Dado un grupo $p$-primario $G$ podemos construir la siguiente cadena descendente de subgrupos

$$pG \supseteq p^2G \supseteq p^3G \supseteq \cdots \supseteq p^nG \supseteq \cdots \tag{3.1}$$

como vimos en la Observación 2.4.3 $(b)$ es claro a partir de la definición que un elemento en $G$ tiene altura $n$ si y sólo si pertenece al conjunto $p^nG - p^{n+1}G$, además un elemento de $G$ es de altura infinita si y sólo si pertenece al subgrupo $\bigcap_{i\in\mathbb{Z}^+} p^iG$.

Por otra parte, sabemos que dado un grupo $G$ existe un subgrupo divisible máximo $D$ y $G = D \oplus R$, donde $R$ es un grupo reducido (Teorema 2.1.18). En general, no es inmediato poder describir con más precisión cómo es $D$ pero para un grupo $p$-primario esto no resulta tan complicado si utilizamos la sucesión (3.1). En general, un grupo $p$-primario $G$ es divisible si y sólo si $pG = G$ ya que un argumento de inducción garantiza

que $p^{n+1}G = p(p^nG) = G$ y por consiguiente $h_G(x) = \infty$ para todo $x \in G$, esto implica que $G$ sea divisible.

Supongamos ahora que existe $n \in \mathbb{Z}^+$ tal que el subgrupo $p^nG$ en la cadena (3.1) satisface que $p^{n+1}G = p(p^nG) = p^nG$ entonces, como vimos antes, $p^nG$ es un grupo divisible y por lo tanto un subgrupo divisible de $G$. A partir de la definición que dimos del subgrupo $D$ en el Teorema 2.1.18 tenemos que $p^nG \subseteq D$. Por otra parte, al ser $D$ un subgrupo divisible y como $D \subseteq G$ tenemos que $D = p^nD \subseteq p^nG$; por lo tanto $p^nG = D$. Así, en caso de que la cadena (3.1) se estacione esta lo hará en el subgrupo divisible máximo del $p$-grupo $G$, pero

$$\text{¿la sucesión (3.1) se estaciona?} \tag{3.2}$$

Hemos visto que un $p$-grupo es divisible si y sólo si todos sus elementos tienen altura infinita; si consideramos el subgrupo $\bigcap_{i\in\mathbb{Z}^+} p^iG$ todos sus elementos tienen altura infinita en $G$ sin embargo $\bigcap_{i\in\mathbb{Z}^+} p^iG$ no necesariamente es un subgrupo divisible, es decir, si $x \in \bigcap_{i\in\mathbb{Z}^+} p^iG$ entonces la ecuación

$$p^nX = y \tag{3.3}$$

tiene una solución en $G$ para toda $n \in \mathbb{Z}^+$ y no hay un argumento general que garantice que se pueda encontrar una solución de (3.3) en $\bigcap_{i\in\mathbb{Z}^+} p^iG$. Nótese que si $\bigcap_{i\in\mathbb{Z}^+} p^iG$ es un subgrupo puro de $G$ siempre se puede encontrar una solución de (3.3) en $\bigcap_{i\in\mathbb{Z}^+} p^iG$. Si $p(\bigcap_{i\in\mathbb{Z}^+} p^iG) \subset \bigcap_{i\in\mathbb{Z}^+} p^iG$ podemos seguir extendiendo la sucesión (3.1) a una sucesión de la forma

$$pG \supseteq p^2G \supseteq \cdots \supseteq p^nG \supseteq p^{n+1}G \supseteq \cdots \supseteq \bigcap_{i\in\mathbb{Z}^+} p^iG \supseteq p(\bigcap_{i\in\mathbb{Z}^+} p^iG) \supseteq \cdots \tag{3.4}$$

Pare llevar esta idea a algo más formal, y entre otras cosas poder responder la pregunta en (3.2), haremos uso de los ordinales transfinitos e introduciremos la siguiente notación: $G_n$ denotará al subgrupo $p^nG$; así definimos para cada ordinal finito $n$, en forma recursiva

$$G_0 = G \quad \text{y} \quad G_{n+1} = pG_n.$$

Sea $\omega$ el primer ordinal infinito, definimos $G_\omega = \bigcap_{n\in\mathbb{N}} p^nG$ y en forma recursiva

$$G_{\omega+(k+1)} = pG_{\omega+k} \quad \text{para toda } k \in \mathbb{N}.$$

En general dado un ordinal $\alpha$ definimos

$$G_\alpha = \begin{cases} pG_\beta & \text{si} \quad \alpha = \beta + 1 \ (\alpha \text{ es un sucesor}) \\ \\ \bigcap_{\beta<\alpha} G_\beta & \text{si} \quad \alpha \text{ es un ordinal límite.} \end{cases} \tag{3.5}$$

De esta manera, obtenemos la siguiente sucesión descendente de subgrupos de $G$

$$G_1 \supseteq G_2 \supseteq \cdots \supseteq G_\omega \supseteq G_{\omega+1} \supseteq \cdots \tag{3.6}$$

Para responder la pregunta hecha en (3.2) notamos que, necesariamente existe un ordinal $\lambda$ con la propiedad de que $G_{\lambda+1} = G_\lambda$, y a partir de aquí la sucesión (3.6) permanecerá constante, este ordinal existe pues en la sucesión (3.6) a lo más pueden haber el cardinal de $G$ subgrupos. Análogo al caso de ordinales finitos, se verifica que $G_\lambda$ es un subgrupo divisible de $G$, más aún, es el máximo subgrupo divisible contenido en $G$ y por lo tanto $G = G_\lambda \oplus R$. En virtud de que los grupos divisibles los tenemos completamente clasificados, es posible considerar el caso en que $G$ es reducido y para tal caso se tiene que $G_\lambda = 0$, debido a que en un grupo reducido el único subgrupo divisible es 0. Así que para un grupo $p$-primario reducido tenemos la siguiente cadena descendente

$$G \supseteq G_1 \supseteq \cdots \supseteq G_\lambda = 0. \tag{3.7}$$

**Definición 3.1.1.** *Sea $G$ un grupo $p$-primario reducido. Llamamos **longitud** del grupo $G$ al ordinal $\lambda$ obtenido como en (3.7).*

Una manera de analizar el comportamiento de la cadena (3.6) es estudiar los grupos $G_\alpha/G_{\alpha+1}$. De la definición de $G_{\alpha+1}$ tenemos que $p(G_\alpha/G_{\alpha+1}) = 0$, lo cual muestra que $G_\alpha/G_{\alpha+1} = (G_\alpha/G_{\alpha+1})[p]$; así, $G_\alpha/G_{\alpha+1}$ admite una estructura de $\mathbb{Z}_p$-espacio vectorial y por lo tanto tiene completamente definida su dimensión, ya sea finita o infinita. Claramente $\dim_{\mathbb{Z}_p}(G_\alpha/G_{\alpha+1})$ es un invariante del grupo $G$, pero como veremos más adelante no es un invariante completo.

Comenzamos examinando el significado de $\dim_{\mathbb{Z}_p}(G_\alpha/G_{\alpha+1})$ en un grupo $p$-primario tal que $G = \bigoplus_{i\in I} \langle a_i\rangle$. Veamos que $G_1 = \bigoplus_{i\in I}(p\langle a_i\rangle)$. Como las operaciones en $\sum_{i\in I}\langle a_i\rangle$ son "coordenada a coordenada" y $G$ es abeliano, es claro que $G_1 = p\sum_{i\in I}\langle a_i\rangle = \sum_{i\in I}(p\langle a_i\rangle)$. Además por la primera afirmación de la Proposición 1.1.9, $\sum_{i\in I}(p\langle a_i\rangle)$ es un suma directa. Por lo tanto $G_1 = \bigoplus_{i\in I}(p\langle a_i\rangle)$. De hecho, en vista de que $p\langle a_i\rangle = \langle pa_i\rangle$, la igualdad anterior puede escribirse como $G_1 = \bigoplus_{i\in I}\langle pa_i\rangle$. Con un argumento de inducción se obtiene que

$$G_n = \bigoplus_{i\in I}(\langle p^n a_i\rangle). \tag{3.8}$$

Sea $\langle a_j\rangle$ un un sumando directo de $G$; si $o(a_j) \leq p^n$ entonces $\langle p^n a_j\rangle = 0$ y dicho sumando "no aparece" en (3.8), es decir, $p^n a_j$ no pertenece al conjunto independiente $\{p^n a_i\}$ que da origen a $G_n$; por otra parte si $o(a_j) > p^n$ entonces $(\langle p^n a_j\rangle / \langle p^{n+1}a_j\rangle) = \langle p^n a_j + \langle p^{n+1}a_j\rangle\rangle$

es un grupo cíclico de orden $p$ (de hecho, como $\mathbb{Z}_p$-espacio vectorial, $(\langle p^n a_j\rangle / \langle p^{n+1}a_j\rangle) \cong \mathbb{Z}_p$); considerando la Proposición 1.1.9 tenemos que, $G_n/G_{n+1} \cong \bigoplus_{i\in\mathbb{N}} (\langle p^n a_i\rangle / \langle p^{n+1}a_i\rangle)$ y por lo tanto

$$\dim_{\mathbb{Z}_p} G_n/G_{n+1} = \#\text{ sumandos directos cíclicos de orden mayor o igual a } p^{n+1}. \quad (3.9)$$

Si $G$ es un grupo finito, la cadena (3.7) tiene un numero finito de términos; así que es posible calcular el número de sumandos directos cíclicos de orden $p^k$ mediante la ecuación

$$\dim_{\mathbb{Z}_p} G_{k-1}/G_k - \dim_{\mathbb{Z}_p} G_k/G_{k+1}. \quad (3.10)$$

Así que, para grupos $p$-primarios reducidos finitos, el conjunto de cardinales

$$(\dim_{\mathbb{Z}_p} G_{k-1}/G_k - \dim_{\mathbb{Z}_p} G_k/G_{k+1})_{k\in\mathbb{Z}^+}$$

es un juego de invariantes completos. Sin embargo este proceso no funciona para grupos infinitos, incluso los infinitos numerables como se muestra a continuación.

Sea $G = \bigoplus_{n\in\mathbb{N}} \mathbb{Z}_{p^n}$; claramente el número de sumandos directos de orden $p^k$ es 1 para cada $k \in \mathbb{N}$; por otra parte, vimos que $\dim_{\mathbb{Z}_p} G_n/G_{n+1}$ determina el "número" de sumandos directos cíclicos de orden mayor o igual a $p^{n+1}$ así es que $\dim_{\mathbb{Z}_p} G_n/G_{n+1} = \aleph_0$ para cada $n \in \mathbb{N}$ y por consiguiente no podemos considerar la ecuación (3.10). Claramente el invariante $\dim_{\mathbb{Z}_p} G_n/G_{n+1}$ no "distingue" los sumandos directos cíclicos de $G$, más aún, para el grupo $H = \bigoplus_{n\in\mathbb{N}} (\mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^n})$, que no es isomorfo a $G$, se tiene que $\dim_{\mathbb{Z}_p} H_n/H_{n+1} = \aleph_0 = \dim_{\mathbb{Z}_p} G_n/G_{n+1}$ para cada $n \in \mathbb{N}$, es decir, $\dim_{\mathbb{Z}_p}(G_n/G_{n+1})$ no es un invariante completo para $G$. Por esta razón es necesario refinar este invariante.

Dado un subgrupo $S$ de un $p$-grupo reducido $G$, definimos para cada ordinal $\alpha$,

$$\boldsymbol{S_\alpha} = S \cap G_\alpha. \quad (3.11)$$

En particular, para el subgrupo $G[p]$ de $G$ tenemos que, $G[p]_\alpha = G[p] \cap G_\alpha$. Nuevamente, a partir de la definición tenemos que $p(G[p]_\alpha/G[p]_{\alpha+1}) = 0$ y por lo tanto $G[p]_\alpha/G[p]_{\alpha+1}$ es un $\mathbb{Z}_p$-espacio vectorial; así es posible establecer una correspondencia entre "cierto" conjunto de ordinales $W$ y el conjunto de cardinales

$$\{\dim_{\mathbb{Z}_p}(G[p]_\alpha/G[p]_{\alpha+1})\}_{\alpha\in W};$$

abusando un poco de la notación, tenemos la siguiente asignación

$$\begin{aligned} f_{p,G} : Ordinales &\longrightarrow Cardinales \\ \alpha &\longmapsto \dim_{\mathbb{Z}_p}(G[p]_\alpha/G[p]_{\alpha+1})\ . \end{aligned} \quad (3.12)$$

**Definición 3.1.2.** *Sea $G$ un $p$-grupo reducido. Llamaremos a*

$$\boldsymbol{f_{p,G}(\alpha)} = \dim_{\mathbb{Z}_p}(G[p]_\alpha / G[p]_{\alpha+1})$$

*el* ***$\alpha$-ésimo invariante de Ulm*** *de $G$.*

Comenzaremos el análisis de este invariante considerando primero el caso en que $G$ es, nuevamente, una suma directa de grupos cíclicos.

Sea $G = \bigoplus_{i\in I} \langle a_i \rangle$ y $\langle a_j \rangle$ un sumando directo tal que $o(a_j) = p^k$. Dado $n \in \mathbb{N}$, y considerando $\langle a_j \rangle$ como un subgrupo de $G$, a partir de (3.11) obtenemos que $\langle a_j \rangle_n = \langle p^n a_j \rangle$. Si $k \leq n$ entonces $\langle a_j \rangle_n = 0$ y por consiguiente $\langle a_j \rangle [p]_n = \langle a_j \rangle [p] \cap \langle a_j \rangle_n = 0$; así que $(\langle a_j \rangle [p]_n)/(\langle a_j \rangle [p]_{n+1}) = 0$ y por lo tanto $f_{p,\langle a_j \rangle}(n) = 0$ para toda $n \geq k$.

Por otra parte, si $k > n$ tenemos dos caso, uno cuando $k \geq n+2$ y el otro es para $k = n+1$. Para el primer caso $\langle a_j \rangle_n$ es cíclico, un generador es $p^n a_j$ y por consiguiente $o(\langle a_j \rangle_n) = p^{k-n}$. Por otra parte, $\langle a_j \rangle [p] = \langle p^{k-1} a_j \rangle = \langle a_j \rangle_{k-1}$ y así tenemos las siguientes igualdades

$$\begin{aligned} \langle a_j \rangle [p]_n &= \langle a_j \rangle [p] \cap \langle a_j \rangle_n \\ &= \langle a_j \rangle_{k-1} \cap \langle a_j \rangle_n \\ &= \langle a_j \rangle_{k-1}. \end{aligned} \tag{3.13}$$

la última igualdad es debida a que $k - 1 \geq n + 1 > n$; así mismo

$$\begin{aligned} \langle a_j \rangle [p]_{n+1} &= \langle a_j \rangle [p] \cap \langle a_j \rangle_{n+1} \\ &= \langle a_j \rangle_{k-1} \cap \langle a_j \rangle_{n+1} \\ &= \langle a_j \rangle_{k-1}. \end{aligned} \tag{3.14}$$

Por lo tanto para $k \geq n+2$, $(\langle a_j \rangle [p]_n)/(\langle a_j \rangle [p]_{n+1}) = 0$ y de aquí se sigue que $f_{p,\langle a_j \rangle}(n) = 0$ para toda $n$ tal que $k \geq n+2$. Por último, en el caso $k = n+1$ las igualdades (3.13) y (3.14) producen las siguientes identidades

$$\langle a_j \rangle [p]_n = \langle a_j \rangle_n \text{ y } \langle a_j \rangle [p]_{n+1} = \langle a_j \rangle_{n+1},$$

por lo tanto $\langle a_j \rangle [p]_n / \langle a_j \rangle [p]_{n+1} = \langle a_j \rangle_n / \langle a_j \rangle_{n+1}$ el cual es un $\mathbb{Z}_p$-espacio vectorial de dimensión uno. En resumen, para un sumando directo $\langle a_j \rangle$ de $G$

$$f_{p,\langle a_j \rangle}(n) = \begin{cases} 0 & \text{si} \quad o(a_j) \leq p^n \\ 1 & \text{si} \quad o(a_j) = p^{n+1} \\ 0 & \text{si} \quad o(a_j) \geq p^{n+2}. \end{cases} \tag{3.15}$$

Para finalizar con el análisis observemos lo siguiente. Sabemos que si $G = \bigoplus_{i\in I} \langle a_i \rangle$ entonces

$$G[p] = \bigoplus_{i\in I}(\langle a_i\rangle\,[p]) \quad \text{y} \quad G_n = \bigoplus_{i\in I}\langle a_i\rangle_n$$

Como $G[p]_n = G[p]\cap G_n$ se tiene que

$$\bigoplus_{i\in I}(\langle a_i\rangle\,[p]) \cap \bigoplus_{i\in I}\langle a_i\rangle_n = \bigoplus_{i\in I}(\langle a_i\rangle\,[p]\cap\langle a_i\rangle_n), \tag{3.16}$$

la demostración de (3.16) no presenta mayor dificultad pues se sigue de la definición de suma directa. Así, $G[p]_n = \bigoplus_{i\in I}(\langle a_i\rangle\,[p]_n)$ y por la Proposición 1.1.9 tenemos que

$$G[p]_n/G[p]_{n+1} \cong \bigoplus_{i\in I}\left(\langle a_i\rangle\,[p]_n/\,\langle a_i\rangle\,[p]_{n+1}\right),$$

por lo tanto

$$\dim(G[p]_n/G[p]_{n+1}) = \#\text{ sumandos directos cíclicos de dimensión } p^{n+1}. \tag{3.17}$$

Lo anterior lo podemos resumir diciendo que,

> *Para un grupo p-primario reducido $G$ que es una suma directa de grupos cíclicos, el $n-$ésimo invariante de Ulm $f_{p,G}(n)$ es el número de sumandos directos cíclicos, de $G$, de orden $p^{n+1}$.*

De esta manera, el invariante de Ulm proporciona una caracterización completa al menos para sumas directas de grupos cíclicos.

**Nota 3.1.3.** *Al suponer que $G = \bigoplus_{i\in I}\langle a_i\rangle$ no se ha impuesto restricción alguna al conjunto de índices $I$, es decir, (3.17) es válido aún cuando $I$ es no numerable.*

Antes de pasar a la demostración del Teorema de Ulm haremos algunas observaciones y refinaremos la definición de altura.

Sea $W(\lambda) = \{\alpha \mid \alpha \text{ es un ordinal y } \alpha < \lambda\}$ el segmento inicial determinado por la longitud de $G$ (véase la Definición 3.1.1). Nótese que $W(\lambda)$ es el conjunto de índices de la cadena (3.7) excepto $\lambda$. Sea $x \in G-\{0\}$, claramente existe $\tau \in W(\lambda)\cup\{\lambda\}$ tal que $x \notin G_\tau$, al menos $\tau = \lambda$ lo satisface. Sea $\mathcal{S} = \{\alpha \in W(\lambda)\cup\{\lambda\} \mid x \notin G_\alpha\}$, como $\mathcal{S} \neq \varnothing$ existe $\tau = \min\mathcal{S}$.

Si $\tau$ es un sucesor existe un <u>único</u> ordinal $\alpha$, necesariamente en $W(\tau)$, tal que $\tau = \alpha+1$. Por la elección de $\tau$ tenemos que $x \in G_\alpha$ y por lo tanto $x \in G_\alpha - G_{\alpha+1}$. Además $\tau$ no puede ser un ordinal límite pues de lo contrario $G_\tau = \bigcap_{\beta<\tau} G_\beta$ y en vista de que $x \notin G_\tau$, existiría $G_\beta$ con $\beta < \tau$ tal que $x \notin G_\beta$ lo cual contradice la elección de $\tau$. De esta manera tenemos la siguiente definición.

**Definición 3.1.4.** *Sea $G$ un grupo $p$-primario reducido y $x \in G - \{0\}$. Definimos la* ***altura generalizada*** *de $x$ como el único ordinal $\alpha$ tal que $x \in G_\alpha - G_{\alpha+1}$. Dicha altura será denotada simplemente como*

$$\boldsymbol{h(x) = \alpha}.$$

Así, cada elemento distinto de cero en un grupo $p$-primario reducido $G$ tiene asignado un ordinal bien definido menor que $\lambda$, la longitud de $G$. Nótese que esta definición coincide con la anterior en los elementos de altura finita. El caso en que $x = 0$ acordamos en denotar $h(x) = \infty$, bajo la convención de que $\infty > \alpha$ para cualquier ordinal $\alpha$. Aún con esta generalización mantenemos la propiedades que vimos en el inciso $(a)$ de la Observación 2.4.3. Es decir, tenemos las siguiente propiedades respecto a la altura generalizada.

**Proposición 3.1.5.** $(a)$ *Si $h(x) < h(y)$, entonces $h(x + y) = h(x)$.*

$(b)$ *Si $h(x) = h(y)$, entonces $h(x + y) \geq h(x)$.*

$(c)$ *Si $x \neq 0$, entonces $h(px) > h(x)$.*

$(d)$ *Si $(m, p) = 1$, entonces $h(mx) = h(x)$.*

*Demostración.* $[(a)]$ Supongamos que $\alpha = h(x) < h(y) = \beta$. Ya que $\alpha + 1 \leq \beta$ tenemos que $G_\beta \subseteq G_{\alpha+1} \subseteq G_\alpha$. Como $x \in G_\alpha$ y $y \in G_\beta$ entonces $x + y \in G_\alpha$; por otra parte si $x + y \in G_{\alpha+1}$ entonces $x \in G_{\alpha+1}$, ya que $y \in G_{\alpha+1}$, y por consiguiente $h(x) \geq \alpha + 1 > \alpha$ lo cual es absurdo, por lo tanto $x + y \in G_\alpha - G_{\alpha+1}$ y así $h(x + y) = \alpha$.

$[(b)]$ Si $h(x) = h(y) = \alpha$ entonces $x, y \in G_\alpha - G_{\alpha+1}$; así $x + y \in G_\alpha$ y por lo tanto $h(x + y) \geq \alpha = h(x)$.

$[(c)]$ Sea $x \in G$ con $x \neq 0$. Supóngase que $h(x) = \alpha$, entonces $x \in G_\alpha - G_{\alpha+1}$ y por consiguiente $px \in pG_\alpha = G_{\alpha+1}$; por lo tanto $h(px) \geq \alpha + 1 > \alpha$.

$[(d)]$ Sea $r \in \mathbb{Z}$ tal que $rm \equiv 1 \pmod{o(x)}$ y supóngase que $h(x) = \alpha$. Como $x \in G_\alpha$ entonces $mx \in G_\alpha$; si $mx \in G_{\alpha+1}$ entonces $x = 1x = (rm)x = r(mx) \in G_{\alpha+1}$ lo cual es absurdo. Así $mx \in G_\alpha - G_{\alpha+1}$ y por lo tanto $h(mx) = h(x)$. ■

Terminamos esta sección con unos lemas concernientes a las subgrupos $\mathcal{G}[p]_\alpha$'s de un grupo dado $\mathcal{G} = \bigoplus_{i \in I} G_i$, donde $\alpha$ es un ordinal menor que la longitud de $\mathcal{G}$. Comenzamos con el siguiente lema preliminar.

**Lema 3.1.6.** *Sea $\{G_i\}_{i \in I}$ es una familia de grupos $p$-primarios reducidos y $\mathcal{G} = \bigoplus_{i \in I} G_i$. Sea $\lambda$ la longitud de $\mathcal{G}$, entonces para cada $\alpha < \lambda$,*

$$\mathcal{G}_\alpha = \bigoplus_{i \in I} [(G_i)_\alpha].$$

*Demostración.* La demostración se hará por inducción transfinita sobre $\alpha$. Es claro a partir de la definición de suma directa que $p\mathcal{G} = \bigoplus_{i\in I}(pG_i)$, es decir, $\mathcal{G}_1 = \bigoplus_{i\in I}[(G_i)_1]$. Supongamos ahora como hipótesis de inducción que para toda $\beta < \alpha$ se cumple que $\mathcal{G}_\beta = \bigoplus_{i\in I}[(G_i)_\beta]$. Debemos demostrar que $\mathcal{G}_\alpha = \bigoplus_{i\in I}[(G_i)_\alpha]$. Para esto tenemos dos casos: El primero es cuando $\alpha = \alpha' + 1$ es un sucesor. Para este caso tenemos las siguientes igualdades

$$\begin{aligned}\mathcal{G}_\alpha &= \mathcal{G}_{\alpha'+1}\\ &= p\mathcal{G}_{\alpha'}\\ &= p\bigoplus_{i\in I}[(G_i)_{\alpha'}]\\ &= \bigoplus_{i\in I}[p(G_i)_{\alpha'}]\\ &= \bigoplus_{i\in I}[(G_i)_{\alpha'+1}]\\ &= \bigoplus_{i\in I}[(G_i)_\alpha],\end{aligned}$$

la segunda y quinta igualdad se dan por la definición, y la cuarta es consecuencia de la definición de suma directa.

El segundo y último caso es cuando $\alpha$ es un ordinal límite; en este es el caso, por definición $\mathcal{G}_\alpha = \bigcap_{\beta<\alpha}\mathcal{G}_\beta$; por hipótesis de inducción $\mathcal{G}_\beta = \bigoplus_{i\in I}[(G_i)_\beta]$ para toda $\beta < \alpha$; así

$$\mathcal{G}_\alpha = \bigcap_{\beta<\alpha}(\bigoplus_{i\in I}(G_i)_\beta). \tag{3.18}$$

Dado $x \in \mathcal{G}_\alpha$, $x = a_{i_1} + a_{i_2} + \cdots + a_{i_k}$ con $a_{i_j} \in G_{i_j}$ para $j = 1, \ldots, k$. Se sigue de la unicidad de la escritura en $\mathcal{G}$ y (3.18) que $a_{i_j} \in (G_{i_j})_\beta$ para toda $\beta < \alpha$ y esto es para toda $j = 1, \ldots, k$; por consiguiente $x_{i_j} \in \bigcap_{\beta<\alpha}(G_{i_j})_\beta = (G_{i_j})_\alpha$ para todo $j = 1, \ldots, k$. Así,

$$x \in \bigoplus_{j=1}^{k}[(G_{i_j})_\alpha] \subseteq \bigoplus_{i\in I}[(G_i)_\alpha]$$

y por lo tanto $\mathcal{G}_\alpha \subseteq \bigoplus_{i\in I}[(G_i)_\alpha]$. Por otra parte, dado $y = b_{i_1} + b_{i_2} + \cdots + b_{i_l} \in \bigoplus_{i\in I}[(G_i)_\alpha]$, entonces $b_{i_j} \in (G_{i_j})_\alpha = \bigcap_{\beta<\alpha}[(G_{i_j})_\beta]$ para toda $j = 1, \ldots, l$ lo que implica que $y \in \bigoplus_{j=1}^{l}[(G_{i_j})_\beta] \subseteq \bigoplus_{i\in I}[(G_i)_\beta] = \mathcal{G}_\beta$ para toda $\beta < \alpha$, es decir, $y \in \bigcap_{\beta<\alpha}\mathcal{G}_\beta = \mathcal{G}_\alpha$. De lo anterior concluimos que $\bigoplus_{i\in I}[(G_i)_\alpha] \subseteq \mathcal{G}_\alpha$ y por lo tato

$$\mathcal{G}_\alpha = \bigoplus_{i\in I}[(G_i)_\alpha].$$

Finalmente el principio de inducción trasfinita no da el resultado deseado. ■

**Lema 3.1.7.** *Sea $\mathcal{G} = \bigoplus_{i\in I} G_i$, donde $\{G_i\}_{i\in I}$ es una familia de grupos p-primarios reducidos. Sea $\lambda$ la longitud de $\mathcal{G}$, entonces para cada $\alpha < \lambda$,*

$$\mathcal{G}[p]_\alpha = \bigoplus_{i\in I}[G_i[p]_\alpha].$$

*Demostración.* Sea $\alpha < \lambda$, considerando el Lema 3.1.6 tenemos que

$$\begin{aligned}\mathcal{G}[p]_\alpha &= \mathcal{G}[p] \cap \mathcal{G}_\alpha \\ &= \bigoplus_{i\in I} G_i[p] \cap \bigoplus_{i\in I}[(G_i)_\alpha].\end{aligned}$$

Si $x = a_{i_1} + \cdots + a_{i_k} \in \mathcal{G}[p]_\alpha$, debido a la unicidad en la escritura de $x$ tenemos que $a_{i_j} \in G_{i_j}[p] \cap (G_{i_j})_\alpha = G_{i_j}[p]_\alpha$ para cada $j = 1, \ldots, k$ y por consiguiente $x \in \bigoplus_{j=1}^{k}[G_{i_j}[p]_\alpha] \subseteq \bigoplus_{i\in I}[G_i[p]_\alpha]$, por lo tanto $\mathcal{G}[p]_\alpha \subseteq \bigoplus_{i\in I}[G_i[p]_\alpha]$. Por otra parte, si $y = b_{i_1} + \cdots + b_{i_l} \in \bigoplus_{i\in I}[G_i[p]_\alpha]$ tenemos que $b_{i_j} \in G_{i_j}[p]_\alpha = G_{i_j}[p] \cap (G_{i_j})_\alpha$, por consiguiente $y \in \bigoplus_{j=1}^{l} G_{i_j}[p] \cap \bigoplus_{j=1}^{l}[(G_{i_j})_\alpha] \subseteq \bigoplus_{i\in I} G_i[p] \cap \bigoplus_{i\in I}[(G_i)_\alpha] = \mathcal{G}[p]_\alpha$, esto muestra que $\bigoplus_{i\in I}[G_i[p]_\alpha] \subseteq \mathcal{G}[p]_\alpha$ y por lo tanto $\mathcal{G}[p]_\alpha = \bigoplus_{i\in I}[G_i[p]_\alpha]$.

■

## 3.2. La Demostración del Teorema de Ulm

El teorema presentado en esta sección es sin duda uno de los más sorprendentes que hasta ahora se ha obtenido en grupos abelianos. Este resultado logra clasificar a los grupos de torsión numerables mediante invariantes completos.

En la sección anterior vimos que, para un grupo $p$-primario reducido $G$ que es una suma directa de grupos cíclicos, el $n$-ésimo invariante de Ulm, $f_{p,G}(n)$, es precisamente el número de sumandos directos cíclicos de orden $p^{n+1}$ que tiene $G$. Pues bien, el Teorema de Ulm afirma lo siguiente:

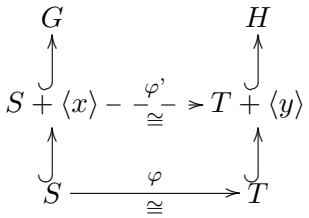
> ***Dos grupos p-primarios reducidos numerables son isomorfos si y sólo si tienen los mismos invariantes de Ulm.***

Con el fin de hacer más clara la demostración del Teorema de Ulm, a continuación haremos algunas observaciones y presentaremos la idea de dicha demostración. Supongamos que $G = \{x_i\}_{i\in\mathbb{N}}$ y $H = \{y_i\}_{i\in\mathbb{N}}$ satisfacen las hipótesis del teorema de Ulm. El isomorfismo que daremos entre $G$ y $H$ será construido a través de extensiones de isomorfismos de

subgrupos finitos de $G$. Supóngase que se tienen los subgrupos $S$ y $T$, finitos, de $G$ y $H$ respectivamente tales que existe un isomorfismo $\varphi : S \longrightarrow T$. Queremos averiguar primero si siempre es posible extender este isomorfismo a algo más grande que los subgrupos $S$ y $T$. Es claro que la altura de cada elemento de $S$, calculada en $S$, es preservada por $\varphi$, es decir, para toda $s \in S$, $h_S(s) = h_T(\varphi(s))$. Pero qué pasa con la altura de los elementos de $S$ calculada en $G$, sabemos que dichas alturas en general no tienen por qué ser las mismas. Si $\phi$ es el isomorfismo de $G$ a $H$ que obtuvimos al extender en algún momento $\varphi$, debe cumplirse que $h_G(x) = h_H(\phi(x))$ para toda $x \in G$, en particular para toda $s \in S$ debemos tener que $h_G(s) = h_H(\phi(s)) = h_H(\varphi(s))$, es decir, si pretendemos extender $\varphi$ será necesario garantizar que dicho isomorfismo preserve la altura global de los elementos de $S$; sin embargo, esto no siempre sucede. Antes de verificar esto consideremos la siguiente situación.

$$x \in G - S,\ y \in H - T,\ h_G(x) = h_H(y) \text{ y } o(x) = o(y). \tag{3.19}$$

Queremos ver si es posible extender $\varphi$ a un isomorfismo entre $S + \langle x \rangle$ y $T + \langle y \rangle$.




Lo natural será definir $\varphi$' como: $\varphi'(s+mx) = \varphi(s)+my$, para ver que $\varphi$' esta bien definida tendremos que garantizar que realmente $\varphi$' es bien definida en $S \cap \langle x \rangle = \langle p^k x \rangle$, donde $p^k$ es la mínima potencia de $p$ con la propiedad de que $p^k x \in S$, es decir, $p^k$ es el orden de $x + S$ calculado en $G/S$. Una condición suficiente es pedir que $\varphi(p^k x) = p^k y$, ya que si $s + mx = s' + nx$ entonces $(m - n)x = s' - s \in S \cap \langle x \rangle$ y por consiguiente $(m - n) = qp^k$, para algún $q \in \mathbb{Z}$. Considerando que $q\varphi(p^k x) = \varphi((m - n)x) = \varphi(s' - s)$ y por otra parte $q\varphi(p^k x) = qp^k y = (m - n)y$, tenemos que $(m - n)y = \varphi(s' - s)$ y por lo tanto $\varphi(s)+my = \varphi(s')+ny$, es decir, $\varphi'(s+mx) = \varphi'(s'+nx)$. Hasta ahora lo único que hemos hecho es definir una función de $S + \langle x \rangle$ en $T + \langle y \rangle$ que claramente es un homomorfismo de grupos, lo que resta es garantizar que este homomorfismo sea un isomorfismo. Veamos ahora que no cualquier isomorfismo puede ser extendido, aún si sabemos que se cumple (3.19). El siguiente ejemplo da luz acerca de esto.

**Ejemplo 3.2.1.** *Sea* $G = \langle x_1 \rangle \oplus \langle x_2 \rangle \oplus \cdots \oplus \langle x_6 \rangle$, *donde* $\langle x_i \rangle \cong \mathcal{Z}$ *para* $1 \leq i \leq 6$ *y* $G' = \langle px_3 - x_2 \rangle + \langle px_4 - x_2 \rangle + \langle x_3 + x_1 + x_2 - px_5 \rangle + \langle x_4 + x_1 + x_2 - p^2 x_6 \rangle + \langle px_1 \rangle + \langle px_2 \rangle$. *Considerando* $G/G'$ *tenemos que* $p\overline{x}_1 = \overline{0} = p\overline{x}_2$ *y como*

$$p\overline{x}_3 = \overline{x}_2,\ p\overline{x}_4 = \overline{x}_2,\ p\overline{x}_5 = \overline{x}_3 + \overline{x}_1 + \overline{x}_2,\ p^2\overline{x}_6 = \overline{x}_4 + \overline{x}_1 + \overline{x}_2, \tag{3.20}$$

*tenemos que:* $p^2\overline{x}_3 = \overline{0}$, $p^2\overline{x}_4 = \overline{0}$ *lo cual implica que* $p^3\overline{x}_5 = \overline{0}$ *y* $p^4\overline{x}_6 = \overline{0}$*; por lo tanto* $G/G'$ *es un grupo p-primario. Consideramos el subgrupo* $S = \langle \overline{x}_1 + \overline{x}_2 \rangle$ *de* $G/G'$ *y el isomorfismo* $Id_S : S \longrightarrow S$*. Elegimos* $\overline{x}_3 \in G/G'$*, veamos si podemos extender* $Id_S$ *a* $S + \langle \overline{x}_3 \rangle$*. Como* $p\overline{x}_3 = \overline{x}_2 \in S$*, queremos encontrar un elemento* $\overline{y} \in G/G' - S$ *tal que* $p\overline{y} = \overline{x}_2$ *y que además* $h_{(G/G')}(\overline{x}_3) = h_{(G/G')}(\overline{y})$*; una solución es* $\overline{x}_4$ *ya que,* $h_{(G/G')}(\overline{x}_4) = h_{(G/G')}(\overline{x}_3) = 0$*. Así* $f(\overline{x}_1 + \overline{x}_2 + \overline{x}_3) = \overline{x}_1 + \overline{x}_2 + \overline{x}_4$*, sin embargo,* $f : S + \langle \overline{x}_3 \rangle \longrightarrow S + \langle \overline{x}_4 \rangle$ *dada por* $f(s + m\overline{x}_3) = s + m\overline{x}_4$ *no es un isomorfismo ya que, como se ve en (3.20),* $h_{(G/G')}(\overline{x}_1 + \overline{x}_2 + \overline{x}_3) = 1$ *y* $h_{(G/G')}(\overline{x}_1 + \overline{x}_2 + \overline{x}_4) = 2$.

Con este ejemplo se ve la necesidad de poder tener control sobre las alturas de las imágenes de los elementos de $S + \langle x \rangle$. La solución a dicho problema consistirá en elegir de manera "apropiada" el elemento $x \in G - S$ y que dicha elección permita obtener las mismas propiedades que posee $x$ respecto a $S$ para $y$ en $T$, donde la existencia de $y$ se verá garantizada por las hipótesis del teorema de Ulm.

Así es que tenemos que resolver el siguiente problema: Dado un subgrupo $S$ de un grupo $G$, ¿cómo deberá ser $x \in G$ para que podamos conocer las alturas de $S + \langle x \rangle$ conociendo las de $h_G(x)$ y $h_G(s)$ para cada $s \in S$? La Proposición 3.1.5 nos proporciona algunas desigualdades que nos serán útiles. Considerando el inciso $(c)$ de dicha proposición sabemos que, para cada $x \in G - \{0\}$, $h(x) < h(px)$ de donde se sigue que

$$h(x) < h(px) < h_(p^2x) < h(p^3x) < \cdots$$

por $(a)$ de la Proposición 3.1.5 tenemos que $h(x + mp^k x) = h(x)$, para toda $k \in \mathbb{N}$ y $m \in \mathbb{Z}$ primo con $p$. Por otra parte si $h(x) \neq h(s)$ sabemos que $h(s + x) = \text{mín}\{h(x), h(s)\}$, que depende de los valores de $h(x)$ y $h(s)$. Cuando $h(x) = h(s)$ lo único que podemos asegurar es que $h(s + x) \geq \text{mín}\{h(x), h(s)\}$; si pedimos a $x \in G$ que $h(s + x) \leq h(x)$ para toda $s \in S$, como veremos en la Nota 3.2.3, garantizaremos que $h(s + x) = \text{mín}\{h(x), h(s)\}$ lo cual depende completamente de las alturas de $x$ y los elementos de $S$. Así tenemos la siguiente definición.

**Definición 3.2.2.** *Sea* $S$ *un subgrupo de un grupo* $G$ *y* $x \in G$*, diremos que* $x$ *es es un* ***elemento propio respecto a*** $S$ *si* $h(x) \geq h(x + s)$ *para todo* $s \in S$.

En otras palabras, un elemento $x \in G$ es propio respecto al subgrupo $S$ de $G$ si $x$ tiene altura maximal con respecto a las alturas de los elementos de $x + S$, la clase lateral de $x$ módulo S. Lo siguiente es una consecuencia de la definición que corrobora la propiedad que buscamos.

**Nota 3.2.3.** (1) *Si $x \in G$ es propio respecto a $S$, entonces*

$$h(x+s) = \text{mín}\{h(x), h(s)\}.$$

*En efecto, sean $x \in G$ un elemento propio respecto a $S$ y $s \in S$. Si $h(x) \neq h(s)$ entonces, por la Proposición 3.1.5 inciso $(a)$, $h(x+s) = \text{mín}\{h(x), h(s)\}$. Si $h(x) = h(s)$ entonces*

$$\text{mín}\{h(x), h(s)\} = h(x) \leq h(x+s) \leq h(x),$$

*donde la primera desigualdad es por la Proposición 3.1.5 inciso $(b)$ y la segunda por ser $x$ propio respecto a $S$; así $h(x+s) = \text{mín}\{h(x), h(s)\}$.*

(2) *En general dado un subgrupos $S$ de un grupo $G$, no podemos garantizar la existencia de elementos propios respecto a $S$; pero es claro que si $S$ es finito entonces cada clase lateral módulo $S$ tiene un elemento propio respecto a $S$, ya que en un conjunto finito de ordinales siempre existe un máximo y cada clase lateral módulo $S$ determina uno de dichos conjuntos.*

Continuando con la idea de la demostración, tenemos la siguiente proposición.

**Proposición 3.2.4.** *Sean $S$ y $T$ subgrupos de $G$ y $H$ respectivamente, $\varphi : S \longrightarrow T$ un isomorfismo tal que $h_G(s) = h_H(\varphi(s))$ para toda $s \in S$. Sean $x \in G - S$ y $y \in H - T$ tales que:*

$(i)$ $h_G(x) = h_H(y)$.

$(ii)$ *$x$ es propio respecto a $S$, $y$ es propio respecto a $T$.*

$(iii)$ $px \in S$, $py \in T$.

$(iv)$ $\varphi(px) = py$.

*Entonces $\widetilde{\varphi} : S + \langle x \rangle \longrightarrow T + \langle y \rangle$ definida como $\widetilde{\varphi}(s + mx) = \varphi(s) + my$ $(s \in S,\ m \in \mathbb{Z})$ es un isomorfismo que preserva altura.*

$$\begin{array}{ccc} G & & H \\ \uparrow & & \uparrow \\ S + \langle x \rangle & \overset{\widetilde{\varphi}}{\underset{\cong}{\twoheadrightarrow}} & T + \langle y \rangle \\ \uparrow & & \uparrow \\ S & \underset{\cong}{\xrightarrow{\varphi}} & T \end{array}$$

*Demostración.* Que $\widetilde{\varphi}$ esta bien definida es una consecuencia de $(iii)$ y $(iv)$, este hecho es un caso particular de lo ya demostrado al iniciar la discusión de la idea de la prueba del teorema de Ulm, considerando $k = 1$, (véase la página 76). Veamos que $\widetilde{\varphi}$ es un isomorfismo. Claramente $\widetilde{\varphi}$ es un homomorfismo. Sea $z = s + mx \in \ker \widetilde{\varphi}$, entonces $\varphi(s) + my = 0$ y por consiguiente $my = -\varphi(s) \in T$, esto implica (por $(iii)$) que $m = qp$, para algún $q \in \mathbb{Z}$; así es que $z = s + qpx \in S$, entonces $\varphi(z) = \widetilde{\varphi}(z) = 0$ y como $\varphi$ es inyectiva necesariamente $z = 0$; lo cual muestra que $\widetilde{\varphi}$ es inyectiva. Para ver que $\widetilde{\varphi}$ es suprayectiva sea $w = t + ny \in T + \langle y \rangle$, considerando $v = \varphi^{-1}(t) + nx \in S + \langle x \rangle$ tenemos que $\widetilde{\varphi}(v) = w$, es decir, $\widetilde{\varphi}$ es suprayectiva y por lo tanto $\widetilde{\varphi}$ es isomorfismo.

Veamos ahora que $\widetilde{\varphi}$ preserva la altura en $G$. Sea $s + nx \in S + \langle x \rangle$, si $p \mid n$ entonces $s + nx \in S$ y en este caso $\widetilde{\varphi}(s + nx) = \varphi(s + nx)$ y por consiguiente $\widetilde{\varphi}$ respeta la altura. Supongamos que $(n, p) = 1$, entonces existe $r \in \mathbb{Z}$ tal que

$$rn \equiv 1 \ (mod\, \text{máx}\{o(x), o(s)\}),$$

multiplicando, $r(s + nx) = rs + rnx = rs + x$, donde $(r, p) = 1$. Tenemos entonces que

$$\begin{aligned}
h_G(s + nx) &= h_G(rs + x) && \text{(Proposición 3.1.5 inciso } (d)) \\
&= \text{mín}\{h_G(x), h_G(rs)\} && \text{(por } (ii)) \\
&= \text{mín}\{h_G(x), h_G(s)\} && \text{(Proposición 3.1.5 inciso } (d)) \\
&= \text{mín}\{h_H(y), h_H(\varphi(s))\} && \text{(por } (i) \text{ y porque } \varphi \text{ preserva orden)} \\
&= \text{mín}\{h_H(y), h_H(r\varphi(s))\} && \text{(Proposición 3.1.5 inciso } (d)) \\
&= h_H(y + r\varphi(s)) && \text{(por}(ii)) \\
&= h_H(ny + \varphi(s)) && \text{(Proposición 3.1.5 inciso } (d)) \\
&= h_H(\widetilde{\varphi}(s + nx)), &&
\end{aligned}$$

es decir, $h_G(s + nx) = h_H(\widetilde{\varphi}(s + nx))$ para toda $s + nx \in S + \langle x \rangle$ y por lo tanto $\widetilde{\varphi}$ preserva altura. ■

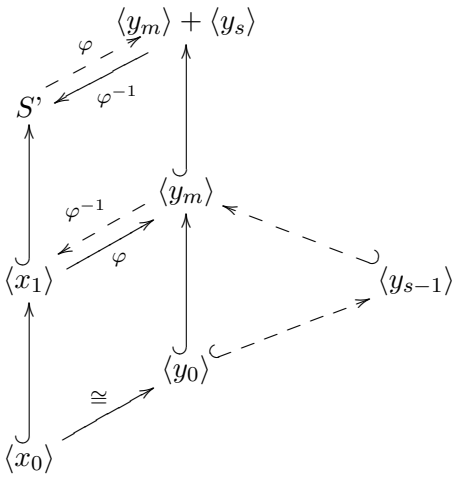
Con la proposición 3.2.4 tenemos un método para extender ciertos isomorfismos entre subgrupos finitos de $G$ y $H$, ahora hay que garantizar que dicho método realmente produce el isomorfismo de $G$ en $H$ que buscamos. Es en esta parte que recurrimos a la hipótesis de que $G$ y $H$ son numerables y que tienen los mismos invariantes de Ulm. El argumento que daremos para dar el isomorfismo de $G$ en $H$ será inductivo. Sean $G = \{x_i\}_{i \in \mathbb{N}}$ y $H = \{y_i\}_{i \in \mathbb{N}}$, supongamos $x_0 = 0_G$ y $y_0 = 0_H$. Comenzamos por extender el isomorfismo trivial $\langle x_0 \rangle \longrightarrow \langle y_0 \rangle$ que claramente preserva altura. Si es necesario volver a numerar los elementos de $G$, podemos suponer que $x_1 \in G[p]$; claramente $x_1$ es propio respecto a $\langle x_0 \rangle$, de hecho cualquier elemento en $G$ es propio respecto a $\langle x_0 \rangle$. Necesitamos encontrar $y \in H[p] - \{0\}$ tal que $h_G(x_1) = h_H(y)$ y así utilizando la Proposición 3.2.4 obtendremos un isomorfismo que preserva altura de $\langle x_1 \rangle$ en $\langle y \rangle$. Sea $h_G(x_1) = \alpha$,

como $G$ y $H$ tienen los mismo invariantes de Ulm, tenemos que $f_{p,G}(\alpha) = f_{p,H}(\alpha)$ y por consiguiente $G[p]_\alpha/G[p]_{\alpha+1} \overset{\psi}{\cong} H[p]_\alpha/H[p]_{\alpha+1}$. Considerando $\overline{x}_1 \in G[p]_\alpha/G[p]_{\alpha+1}$, que es distinto de $\overline{0}$; sea $\overline{y_m} \in H[p]_\alpha/H[p]_{\alpha+1}$ el único elemento tal que $\psi(\overline{x_1}) = (\overline{y_m})$. Veamos que $h_H(y_m) = h_G(x_1)$; como $\overline{y_m}$ es distinto de $\overline{0}$ entonces $y_m \in H[p]_\alpha - H[p]_{\alpha+1}$ lo cual implica que $y_m \in H_\alpha - H_{\alpha+1}$ y por lo tanto $h_H(y_m) = \alpha = h_G(x_1)$. Así, $\langle x_0\rangle$, $\langle y_0\rangle$, $x_1$ y $y_1$ satisfacen las hipótesis de la Proposición 3.2.4 y por lo tanto existe un isomorfismo $\varphi$ de $\langle x_1\rangle$ en $\langle y_m\rangle$ que preserva altura.

Es importante hacer notar que, nada garantiza que $y_1 \in \langle y_m\rangle$. Si $y_1 \notin \langle y_m\rangle$ y logramos extender $\varphi$ a subgrupos finitos $S$ y $T$ que contengan a $\langle x_1\rangle$ y a $\langle y_m\rangle$ respectivamente; de nuevo no hay un argumento general que nos garantice que $y_1 \in T$. Sin embargo, esto lo podemos solucionar si logramos extender $\varphi^{-1}$ a un isomorfismo, y que abusando un poco de la notación seguiremos escribiendo como $\varphi^{-1}$, de $T + \langle y_1\rangle$ a algún subgrupo de $G$ que contenga a $S$. Con más precisión, sea $1 \leq s < m$ el mínimo índice tal que $y_s \notin \langle y_m\rangle$, lo que haremos ahora es extender $\varphi^{-1}$ a un isomorfismo de $\langle y_m\rangle + \langle y_s\rangle$ a un subgrupo finito $S$' de $G$ que contiene a $\langle x_1\rangle$. Nuevamente, no es posible garantizar que $x_2 \in S$' pero procediendo como antes lo que hacemos es extender $\varphi$ (pensado como isomorfismo de $S$' a $\langle y_m\rangle + \langle y_s\rangle$).

Teniendo en cuenta lo anterior, supongamos como hipótesis de inducción que el isomorfismo $\varphi$, de $\langle x_1\rangle$ a $\langle y_m\rangle$, ha sido extendido a un isomorfismo $\varphi : S \longrightarrow T$ que preserva altura y tal que $x_1, \ldots, x_n \in S = \{s_1, \ldots, s_r\}$ y $y_1, \ldots, y_n \in T$. Supongamos además que $x_{n+1} \notin S$; queremos extender este isomorfismo a un grupo que contenga a $S$ y a $x_{n+1}$ y para ello lo primero que haremos es encontrar un elemento en $G$ que satisfaga las hipótesis de la Proposición 3.2.4. Como $G$ es un grupo $p$-primario, $G/S$ también lo es; sean $p^k = o(x_{n+1} + S)$ calculado en $G/S$ con $k > 0$; ya que $p^{k-1}x_{n+1}+S = \{p^{k-1}x_{n+1}+s_1, \ldots, p^{k-1}x_{n+1}+s_r\}$ es finito, existe $\alpha = \text{máx}\{h(w) \mid w \in p^{k-1}x_{n+1}+S\}$. Sea $\mathcal{A} = \{w \in p^{k-1}x_{n+1}+S \mid h(w) = \alpha\}$ y $w_0 \in \mathcal{A}$ tal que $h_G(pw_0) = \text{máx}\{h_G(pw) \mid w \in \mathcal{A}\}$, nuevamente esto es posible debido a que $\mathcal{A}$ es finito. Escribimos $w_0 = p^{k-1}x_{n+1} + s$, para alguna $s \in S$; dado $s_i \in S$, $s + s_i = s_j \in S$; así que $w_0 + s_i = p^{k-1}x_{n+1} + s + s_i = p^{k-1}x_{n+1} + s_j \in p^{k-1}x_{n+1} + S$ y por consiguiente $h_G(w_0 + s_i) \leq h_G(w_0)$, es decir, $w_0$ es propio respecto a $S$, además $pw_0 \in S$. Lo que necesitamos ahora es encontrar un elemento en $H$ el cual nos de finalmente las hipótesis de la Proposición 3.2.4, de esto nos ocuparemos más adelante en la demostración del Teorema de Ulm; una vez hecho esto, el isomorfismo $\varphi$ puede extenderse a un isomorfismo (recordamos que lo denotaremos igual) $\varphi$ de $S + \langle w_0\rangle = S + \langle p^{k-1}x_{n+1}\rangle$ en algún subgrupo de $H$ que contiene a $T$. Aún no podemos asegurar que $x_{n+1}$ pertenezca a este grupo pero si podemos garantizar que $p(p^{k-2}x_{n+1}) \in S + \langle w_0\rangle$. Repitiendo el proceso anterior obtenemos que, $\varphi$ se puede extender a un subgrupo finito $S$', de $G$, que contiene a $S + \langle w_0\rangle = S + \langle p^{k-1}x_{n+1}\rangle$ garantizando además que $p(p^{k-3}x_{n+1}) \in S$'. En un número finito de repeticiones de dicho

proceso finalmente obtenemos que es posible extender $\varphi$ a un isomorfismo $\varphi : \widehat{S} \longrightarrow \widehat{T}$ donde, $\widehat{S}$ y $\widehat{T}$ son subgrupos finitos de $G$ y $H$ respectivamente, con $S \subseteq \widehat{S}$, $x_{n+1} \in \widehat{S}$ y $T \subseteq \widehat{T}$. Como ya lo mencionamos antes, no se puede garantizar que al finial de este proceso $y_{n+1} \in \widehat{T}$, así que el siguiente paso será extender $\varphi^{-1}$ a un subgrupo de $H$ que contenga a $\widehat{T}$ y a $y_{n+1}$; así, por inducción, finalmente obtenemos el isomorfismo de $G$ en $H$ que buscamos.

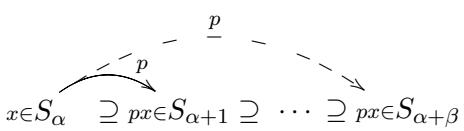



Para finalizar con la idea de la demostración del Teorema de Ulm, y que en realidad forma parte de la misma, el lema que daremos a continuación da condiciones necesarias y suficientes acerca de la existencia de elementos propios, respecto a un subgrupo, con altura dada. Comenzamos esto con la siguiente observación.

**Observación 3.2.5.** *Consideremos $S$ un subgrupo de un grupo $G$ y sea $\alpha$ un ordinal. De la cadena (3.6) obtenemos la cadena*

$$S \supseteq S_1 \supseteq \cdots \supseteq S_\omega \supseteq S_{\omega+1} \supseteq \cdots$$

*Si $x \in S_\alpha$, a partir de la definición de $S_{\alpha+1}$ tenemos que $px \in S_{\alpha+1}$, pero nada prohíbe que $px \in S_{\alpha+\beta}$ para algún ordinal $\beta$;*




*Denotamos como*

$$p^{-1}G_\beta = \{x \in G \mid px \in G_\beta\}.$$

*Supongamos que $x \in S_\alpha$ es tal que $px \in S_{\alpha+2}$, entonces $px \in S \cap G_{\alpha+2}$ y así $x \in p^{-1}G_{\alpha+2}$, es decir $x \in S_\alpha \cap p^{-1}G_{\alpha+2}$. Recíprocamente, si $x \in S_\alpha \cap p^{-1}G_{\alpha+2}$ entonces $px \in G_{\alpha+2}$ y como $x \in S$ tenemos que $px \in S$ y por consiguiente $px \in S \cap G_{\alpha+2} = S_{\alpha+2}$. De esta manera el conjunto*

$$\boldsymbol{S^*_\alpha} = S_\alpha \cap p^{-1}G_{\alpha+2} \tag{3.21}$$

*caracteriza a los elementos en $S_\alpha$ que al ser multiplicados por $p$ caen en $S_{\alpha+2}$.*

Para el siguiente lema será necesario definir un isomorfismo en el cual se ve involucrado el grupo $S^*_\alpha$. A continuación presentamos dicho isomorfismo.

Dado $x \in S^*_\alpha$ tenemos que $px \in G_{\alpha+2}$ y por consiguiente existe $y \in G_{\alpha+1}$ tal que $px = py$; de esta igualdad obtenemos que $p(x-y) = 0$ y como $x, y \in G_\alpha$ se sigue que $(x-y) \in G[p]_\alpha$. Por otra parte, si $y' \in G_{\alpha+1}$ satisface que $py' = px = py$ entonces $p(y'-y) = 0$, así $y'-y \in G[p]_{\alpha+1}$ lo que implica que $y' + G[p]_{\alpha+1} = y + G[p]_{\alpha+1}$ y por lo tanto $(x-y') + G[p]_{\alpha+1} = (x-y) + G[p]_{\alpha+1}$. Por lo anterior, podemos definir una función $\varphi : S^*_\alpha \longrightarrow G[p]_\alpha / G[p]_{\alpha+1}$ como

$$\varphi(x) = (x-y) + G[p]_{\alpha+1}. \tag{3.22}$$

Veremos ahora que $\varphi$ es un homomorfismo. Sean $x, x' \in S^*_\alpha$ y $y, y' \in G_{\alpha+1}$ tales que $xp = py$ y $px' = py'$, entonces $p(x+x') = p(y+y')$ y por la manera en que fue definida $\varphi$ , tenemos que

$$\begin{aligned}
\varphi(x+x') &= [(x+x') - (y+y')] + G[p]_{\alpha+1} \\
&= [(x-y) + (x'-y')] + G[p]_{\alpha+1} \\
&= (x-y) + G[p]_{\alpha+1} + (x'-y') + G[p]_{\alpha+1} \\
&= \varphi(x) + \varphi(x')
\end{aligned}$$

y por lo tanto $\varphi$ es homomorfismo.

Para ver cual es el núcleo de $\varphi$ empecemos notando lo siguiente. En vista que, $G_{\alpha+1} \subseteq G_\alpha$ y claramente $G_{\alpha+1} \subseteq p^{-1}G_{\alpha+2}$ tenemos la siguiente serie de igualdades, $S_{\alpha+1} = S \cap G_{\alpha+1} = S \cap G_\alpha \cap G_{\alpha+1} = S_\alpha \cap G_{\alpha+1} \subseteq S^*_\alpha$, es decir, $S_{\alpha+1} \subseteq S^*_\alpha$. Sea $x \in \ker\varphi$, entonces existe $y \in G_{\alpha+1}$ tal que $x - y \in G[p]_{\alpha+1} \subseteq G_{\alpha+1}$, lo cual implica que $x \in G_{\alpha+1}$, es decir, $x \in S \cap G_{\alpha+1} = S_{\alpha+1}$ y por lo tanto $\ker\varphi \subseteq S_{\alpha+1}$. Por otra parte, si $x \in S_{\alpha+1}$ entonces $px \in G_{\alpha+2}$ y por consiguiente $px = py$ para algún $y \in G_{\alpha+1}$; así que $(x-y) \in G[p]_{\alpha+1}$ y $\varphi(x) = 0$, es decir, $S_{\alpha+1} \subseteq \ker\varphi$ y por lo tanto $\ker\varphi = S_{\alpha+1}$. Por el primer teorema de isomorfismos obtenemos que, existe un isomorfismo

$$\mathcal{U} : S^*_\alpha / S_{\alpha+1} \longrightarrow \varphi(S^*_\alpha) \leq G[p]_\alpha / G[p]_{\alpha+1} \ . \tag{3.23}$$

Con lo anterior, estamos en condiciones de enunciar el lema.

**Lema 3.2.6.** *Para un grupo p-primario $G$ son equivalentes:*

(a) $Im\mathcal{U} \subsetneq G[p]_\alpha/G[p]_{\alpha+1}$

(b) *Existe un elemento en $G[p]_\alpha$ de altura $\alpha$ propio en $S$.*

*Demostración.* $[(a) \Rightarrow (b)]$ Sea $v + G[p]_{\alpha+1} \in G[p]_\alpha/G[p]_{\alpha+1}$ tal que $v + G[p]_{\alpha+1} \notin Im(\mathcal{U})$ entonces $v \in G[p]_\alpha$ y necesariamente $v \notin G[p]_{\alpha+1}$, de lo contrario tendríamos que $v + G[p]_{\alpha+1} = 0 \in Im(\mathcal{U})$; de lo anterior se sigue que $v \in G[p]_\alpha - G[p]_{\alpha+1} = G[p] \cap (G_\alpha - G_{\alpha+1})$ y así $h(v) = \alpha$. Para verificar que $v$ es propio en $S$ supondremos que no lo es y obtendremos un absurdo. Si $v$ no es propio en $S$ existe $s \in S$ tal que $\alpha = h(v) < h(s - v)$ y por la Proposición 3.1.5 $(a)$ $h(s) = h(v + (s - v)) = h(v) = \alpha$; esto implica que $s \in S_\alpha$. Como $(s - v) \in G_{h(s-v)} \subseteq G_{\alpha+1}$, $s - v = py$ para algún $y \in G_\alpha$; así obtenemos que $ps = p^2y \in G_{\alpha+2}$, es decir, $s \in p^{-1}G_{\alpha+2}$ y por lo tanto $s \in S_\alpha \cap p^{-1}G_{\alpha+2} = S^*_\alpha$. Como $v = s - py$ y $ps = p(py)$, de la definición de $\mathcal{U}$ tenemos que $v + G[p]_{\alpha+1} = (s - py) + G[p]_{\alpha+1} \in Im(\mathcal{U})$ lo que es absurdo por la elección de $v + G[p]_{\alpha+1}$. Por lo tanto $v$ es propio en $S$.

$[(b) \Rightarrow (a)]$ Sea $v \in G[p]_\alpha$ con $h(v) = \alpha$ y propio en $S$. Supongamos además que $v + G[p]_{\alpha+1} \in Im(\mathcal{U})$, entonces existen $x \in S^*_\alpha$ tal que $\mathcal{U}(x + S_{\alpha+1}) = v + G[p]_{\alpha+1}$; sea $y \in G_{\alpha+1}$ tal que $(x - y) + G[p]_{\alpha+1} = \mathcal{U}(x + S_{\alpha+1}) = v + G[p]_{\alpha+1}$. Sea $w \in G[p]_{\alpha+1}$ tal que $(x - y) = (v + w)$, entonces $(x - v) = (y + w) \in G_{\alpha+1}$ y por consiguiente $h(x - v) = h(y + w) \geq \alpha + 1 > \alpha$, es decir, $h(x - v) > \alpha$ lo que es absurdo ya que $v$ es propio en $S$. Por lo tanto $v + G[p]_\alpha \notin Im(\mathcal{U})$. ■

**Nota 3.2.7.** *De la demostración del Lema 3.2.6 podemos deducir que, los elementos en $G$ de altura $\alpha$ que son propios en $S$ son aquellos $x \in G[p]_\alpha$ tales que*

$$x + G[p]_{\alpha+1} \in G[p]_\alpha/G[p]_{\alpha+1} - Im(\mathcal{U}).$$

Finalmente, y considerando la discusión anterior, estamos listos para la demostración del Teorema de Ulm.

**Teorema 3.2.8.** *(**Teorema de Ulm**) Dos grupos p-primarios reducidos numerables son isomorfos si y sólo si tienen los mismos invariantes de Ulm.*

*Demostración.* Considerando lo discutido en esta sección asumiremos las siguientes condiciones: $S$ y $T$ son subgrupos finitos de $G$ y $H$, respectivamente; $\varphi : S \longrightarrow T$ es un isomorfismo que preserva alturas; $x \in G - S$ tal que $px \in S$, con $x$ propio respecto a $S$ y $h_G(x) = \alpha$ es máximo en el conjunto $\{h_G(w) \mid w \in x + S \text{ y } h_G(w) = h_G(x)\}$ (véase la página 80). Sea $z = \varphi(px)$, Para poder "reunir" las hipótesis de la Proposición 3.2.4 debemos encontrar un elemento $y \in H - T$ tal que $py = \varphi(px) \in T$, $h_H(y) = \alpha$ y que $y$ sea propio

respecto a $T$. Una vez encontrado $y$, la Proposición 3.2.4 nos asegura que $\varphi$ se extiende a un isomorfismo que preserva alturas.

En vista de que $h_H(z) = h_G(px) > h_G(x) = \alpha$ tenemos que $h_H(z) \geq \alpha + 1$. Consideraremos dos casos, cuando $h_H(z) = \alpha + 1$ y el caso $h_H(z) > \alpha + 1$.

**Caso 1.** *$h_H(z) = \alpha + 1$. Como $z \in H_{\alpha+1} - H_{\alpha+2}$ existe $y \in H_\alpha$ tal que*

$$z = py, \tag{3.24}$$

*además $h_H(y) \geq \alpha$. Si $h_H(y) > \alpha$ entonces $h_H(z) = h_H(py) > h_H(y) \geq \alpha + 1$ lo cual es absurdo; por lo tanto*

$$h_H(y) = \alpha. \tag{3.25}$$

*Sólo falta verificar que $y$ es propio respecto a $T$. Veamos que $y \notin T$, si $y \in T$, existe $s \in S$ tal que $\varphi(s) = y$, multiplicando por $p$ tenemos que $\varphi(ps) = \varphi(px)$ y por consiguiente $ps = px$; así $p(x - s) = 0$. Como $s \in S$ necesariamente $(x - s) \notin S$. Por otra parte, $h_G(s) = h_H(\varphi(s)) = h_H(y) = \alpha = h_G(x)$; así*

$$h_G(x) \leq h_G(x - s) \leq h_G(x),$$

*por lo tanto $h_G(x - s) = h_G(x)$. Ahora bien, $h_G(p(x - s)) = h_G(0) = \infty > h_G(x)$ que es absurdo pues contradice la elección de que $h_G(x)$ es máximo respecto a los elementos en $x + S$ cuya altura coincide con $h_G(x)$. Por lo tanto*

$$y \notin T. \tag{3.26}$$

*Supongamos que $y$ no es propio respecto a $T$, entonces existe $t \in T$ tal que $h_H(y + t) > h_H(y) = \alpha$ y por consiguiente $h_H(y + t) \geq \alpha + 1$. Sea $t = \varphi(s')$, para alguna $s' \in S$. Necesariamente $y + t \neq 0$, así $h_H(p(y + t)) \geq \alpha + 2$. Si $h_H(t) < h_H(y) = \alpha$ entonces $h_H(t) = h_H(y + t) > \alpha$ que es absurdo, por consiguiente $h_H(t) \geq h_H(y) = \alpha$. Si $h_H(t) > h_H(y) = \alpha$ se tiene que $\alpha = h_H(y + t) > \alpha$ nuevamente un absurdo; por tanto debe ser $h_H(t) = h_H(y)$, y como $\varphi$ preserva alturas obtenemos que $h_G(s') = h_H(t) = \alpha = h_G(x)$. Así $h_G(x) = h_G(x + s) \leq h_G(x)$, es decir $h_G(x + s') = h_G(x)$. Como $\varphi(px) = py$ y $\varphi(ps') = pt$ tenemos que $\varphi(p(x + s')) = p(y + t)$ lo que implica que $h_G(p(x + s')) = h_H(p(y + t)) > \alpha + 1 = h_H(z) = h_H(\varphi(px)) = h_G(px)$ lo cual es absurdo ya que contradice la elección de $h_G(px)$. Así*

$$y \text{ es propio respecto a } T. \tag{3.27}$$

*Finalmente por (3.24), (3.25) y (3.27) tenemos completas las hipótesis de la Proposición 3.2.4.*

**Caso 2.** $h_H(z) > \alpha+1$. *Este caso implica que* $h_G(px) > \alpha+1$ *y por consiguiente* $px \in G_{\alpha+2}$. *Sea* $v \in G_{\alpha+1}$ *tal que* $px = pv$; *así que* $(x-v) \in G[p]_\alpha$, *además* $h_G(v) \geq \alpha+1 > h_G(x)$ *y por lo tanto* $h_G(x-v) = h_G(x)$. *Como* $h_G(x) < h_G(v)$, *entonces para cada* $s \in S$ $h_G((x-v)+s) = h_G((x+s)-v) = h_G(x+s) \leq h_G(x) = h_G(x-v)$, *la segunda igualdad se da ya que* $h_G(x+s) \leq h_G(x) < h_G(v) = h_G(-v)$. *Es decir,* $(x-v)$ *es propio respecto a* $S$ *y así* $(x-v)$ *satisface las hipótesis del Lema 3.2.6. Como* $S$ *es finito, necesariamente* $S^*_\alpha/S_\alpha$ *es finito y por consiguiente,* $S^*_\alpha/S_\alpha$ *es un* $\mathbb{Z}_p$*-espacio vectorial de dimensión finita. Por el Lema 3.2.6 esta dimensión es estrictamente menor que* $\dim_{\mathbb{Z}_p}(G[p]_\alpha/G[p]_{\alpha+1}) = f_{p,G}(\alpha)$, *el* $\alpha$*-ésimo invariante de Ulm de* $G$. *Como* $\varphi$ *preserva alturas, tenemos que*

$$\varphi(S_\alpha) = T_\alpha,\ \varphi(S^*_\alpha) = T^*_\alpha,$$

*y por consiguiente* $\varphi(S^*_\alpha/S_\alpha) = T^*_\alpha/T_\alpha$. *Así que,*

$$\dim_{\mathbb{Z}_p}(T^*_\alpha/T_\alpha) = \dim_{\mathbb{Z}_p}(S^*_\alpha/S_\alpha) < f_{p,G}(\alpha) = f_{p,H}(\alpha).$$

*Nuevamente, por el Lema 3.2.6, existe* $y_1 \in H$ *tal que* $py_1 = 0$, $h_H(y_1) = \alpha$ *y* $y_1$ *es propio respecto a* $T$ *(véase la Nota 3.2.7). Como* $h_H(z) > \alpha+1$, $z \in H_{\alpha+2}$ *y así existe* $y_2 \in H_{\alpha+1}$ *tal que* $py_2 = z$. *Sea* $y = y_1 + y_2$. *Entonces*

$$py = py_1 + py_2 = pz, \tag{3.28}$$

$$h_H(y) = h_H(y_1 + y_2) = h_H(y_1) = \alpha, \tag{3.29}$$

*la segunda igualdad se da porque* $h_H(y_1) = \alpha < \alpha+1 \leq h_H(y_2)$. *Para toda* $t \in T$ *se tiene que*

$$h_H(y+t) = h_H((y_1+t)+y_2) = h_H(y_1+t) \leq h_H(y_1) = h_H(y),$$

*nuevamente, la segunda igualdad es porque* $h_H(y_1+t) \leq h_H(y_1) < h_H(y_2)$. *Es decir,*

$$y \text{ es propio respecto a } T. \tag{3.30}$$

*Además* $y \notin T$ *pues de lo contrario* $y \in T_\alpha$ *y como* $py = pz \in H_{\alpha+2}$ *entonces* $y \in T^*_\alpha$. *Como* $p(y-y_2) = py_1 = 0$ *tenemos que* $(y-y_2) \in H[p]_\alpha$, *recuérdese que* $y_2 \in H_{\alpha+1}$. *Entonces* $y_1 + H[p]_{\alpha+1} = (y-y_2) + H[p]_{\alpha+1} \in Im(\mathcal{U})$ *lo cual es absurdo pues contradice la elección de* $y_1$ *(véase la Nota 3.2.7). Por lo tanto*

$$y \notin T. \tag{3.31}$$

*Finalmente (3.28), (3.29), (3.30) y (3.31) completa las hipótesis de la Lema 3.2.6 lo que termina este caso y por tanto la demostración.*

■

**Ejemplo 3.2.9.** *Sea $G$ el grupo generado por $x$ y $y_i$ $(i = 1, \ldots, n, \ldots)$ y que satisfacen las siguientes relaciones*

$$px = 0,\ x = py_1 = p^2y_2 = \cdots = p^ny_n = \cdots$$

*Los invariantes de Ulm son*

$$f_{p,G}(0) = f_{p,G}(1) = f_{p,G}(2) = \cdots = f_{p,G}(n) = \cdots = f_{p,G}(\omega) = 1 \tag{3.32}$$

*y el grupo tiene longitud $\omega + 1$.*

*En efecto, a partir de la definición tenemos que $o(x) = p$ y para toda $n \in \mathbb{Z}^+$ $o(y_n) = p^{n+1}$. Como $G = \langle x \rangle + \sum_{n\in\mathbb{Z}^+} \langle y_n \rangle$ se sigue que*

$$p^nG = p^n \langle y_n \rangle + p^n \langle y_{n+1} \rangle + p^n \langle y_{n+2} \rangle + \cdots + p^n \langle y_{n+k} \rangle + \cdots \tag{3.33}$$

*Además $G[p] = \langle x \rangle + \sum_{n\in\mathbb{Z}^+} \langle p^n y_n \rangle$, y como $\langle p^n y_n \rangle < \langle p y_n \rangle$ para toda $n > 1$ tenemos que para toda $n \in \mathbb{Z}^+$*

$$G[p]_n = p^n \langle y_n \rangle + p^{n+1} \langle y_{n+1} \rangle + p^{n+2} \langle y_{n+2} \rangle + \cdots + p^{n+k} \langle y_{n+k} \rangle + \cdots,$$

*entonces*

$$G[p]_n/G[p]_{n+1} \cong p^n \langle y_m \rangle = \langle x \rangle \cong \mathbb{Z}_p \text{ para cada } n \in \mathbb{Z}^+,$$

*y por lo tanto se cumple (3.32). Por otra parte, a partir de (3.33) se sigue que*

$$G_\omega = \bigcap_{n\in\mathbb{Z}^+} p^nG = \langle x \rangle$$

*y por consiguiente $G_{\omega+1} = pG_\omega = p \langle x \rangle = 0$, es decir, $G$ tiene longitud $\omega + 1$.*

Finalizaremos este capítulo con una serie de resultados acerca de los invariantes de Ulm de ciertos grupos.

**Proposición 3.2.10.** *Sean $\{G_i\}_{i\in I}$ una familia de grupos p-primarios reducidos. Entonces el invariante de Ulm de $\mathcal{G} = \bigoplus_{i\in I} G_i$ se puede obtener sumando los invariante de Ulm de cada $G_i$ con $i \in I$, es decir,*

$$f_{p,\mathcal{G}}(\alpha) = \sum_{i\in I} f_{p,G_i}(\alpha), \tag{3.34}$$

*para cada ordinal $\alpha \leq \lambda$, donde $\lambda$ es la longitud de $\mathcal{G}$.*

*Demostración.* La demostración consistirá en dar un isomorfismo, de $\mathbb{Z}_p$-espacios vectoriales, entre $(\bigoplus_{i\in I} G_i)[p]_\alpha/(\bigoplus_{i\in I} G_i)[p]_{\alpha+1}$ y $\bigoplus_{i\in I}[(G_i[p]_\alpha)/(G_i[p]_{\alpha+1})]$. Por el Lema 3.1.7 tenemos que

$$(\bigoplus_{i\in I} G_i)[p]_\alpha/(\bigoplus_{i\in I} G_i)[p]_{\alpha+1} = [\bigoplus_{i\in I} G_i[p]_\alpha]/[\bigoplus_{i\in I} G_i[p]_{\alpha+1}],$$

y en vista de que $G_i[p]_{\alpha+1}$ es un subgrupo de $G_i[p]_\alpha$ para toda $i \in I$, la Proposición 1.1.9 asegura que la función

$$\varphi : \bigoplus_{i\in I} G_i[p]_\alpha \longrightarrow \bigoplus_{i\in I}[(G_i[p]_\alpha)/(G_i[p]_{\alpha+1})]$$

dada por

$$\varphi((x_i)_{i\in I}) = (x_i + G_i[p]_\alpha)_{i\in I},$$

determina un homomorfismo de grupos bien definido que es suprayectivo y con núcleo $\bigoplus_{i\in I} G_i[p]_{\alpha+1}$. Así que el primer teorema de isomorfismos garantiza que la función

$$\overline{\varphi} : \bigoplus_{i\in I} G_i[p]_\alpha/\bigoplus_{i\in I} G_i[p]_{\alpha+1} \longrightarrow \bigoplus_{i\in I}[(G_i[p]_\alpha)/(G_i[p]_{\alpha+1})],$$

dada como $\overline{\varphi}(\overline{(x_i)}_{i\in I}) = \varphi((x_i)_{i\in I})$, donde $\overline{(x_i)}_{i\in I}$ es la clase lateral de $(x_i)_{i\in I}$ modulo $\bigoplus_{i\in I} G_i[p]_{\alpha+1}$, es un isomorfismo de grupos. Para ver que $\overline{\varphi}$ es un isomorfismo de $\mathbb{Z}_p$-espacios vectoriales sólo falta mostrar que preserva el producto por escalares. Pero esto es claro a partir de la definición de producto por escalares que se dio en la Proposición 1.3.17 y del hecho de que $\varphi$ es homomorfismo de grupos. De esta manera, $\overline{\varphi}$ es un isomorfismo de $\mathbb{Z}_p$-espacios vectoriales y por lo tanto las dimensiones de $\bigoplus_{i\in I} G_i[p]_\alpha/\bigoplus_{i\in I} G_i[p]_{\alpha+1}$ y $\bigoplus_{i\in I}[(G_i[p]_\alpha)/(G_i[p]_{\alpha+1})]$ coinciden. Es decir, (3.34) se cumple. ■

La siguiente proposición dará respuesta a los problemas que enunciamos en la introducción para el caso de grupos de torsión numerables.

**Proposición 3.2.11.** (*a*) *En cualquiera de los problemas dados en la introducción, si $G$ y $H$ son grupos $p$-primarios reducidos. Entonces $G$ y $H$ tiene los mismos invariantes de Ulm.*

(*b*) *Si además de* (*a*) *asumimos que $G$ y $H$ son numerables, entonces $G$ y $H$ son isomorfos.*

(*c*) *Los tres problemas de la introducción tienen respuesta afirmativa para grupos de torsión numerables.*

*Demostración.* [$(a)$]

(1) Sean $G$ y $H$ grupos $p$-primarios reducidos tales que, $G$ es isomorfo a un sumando directo de $H$ y $H$ es isomorfo a un sumando directo de $G$, entonces $G$ y $H$ tienen los mismos invariantes de Ulm.

*Demostración.* Supóngase que $G = K \oplus H'$ y $H = L \oplus G'$, donde $H' \cong H$ y $G' \cong G$. Por la Proposición 3.2.10 sabemos que

$$f_{p,K\oplus H'}(\alpha) = f_{p,K}(\alpha) + f_{p,H'}(\alpha) \text{ y } f_{p,L\oplus G'}(\alpha) = f_{p,L}(\alpha) + f_{p,G'}(\alpha) \tag{3.35}$$

para todo ordinal $\alpha$ menor que $\lambda_G = \lambda_H$, donde $\lambda_G$ y $\lambda_H$ son las longitudes de $G$ y $H$ respectivamente.[1] Como $f_{p,H'}(\alpha) = f_{p,G}(\alpha)$ y $f_{p,G'}(\alpha) = f_{p,H}(\alpha)$, a partir de (3.35) obtenemos que

$$f_{p,H}(\alpha) \leq f_{p,G}(\alpha) \text{ y } f_{p,G}(\alpha) \leq f_{p,H}(\alpha),$$

por lo tanto $f_{p,G}(\alpha) = f_{p,H}(\alpha)$ para todo ordinal $\alpha$ menor que $\lambda_G$. ■

(2) Si $G \oplus G \cong H \oplus H$, entonces $G$ y $H$ tienen los mismos invariantes de Ulm.

*Demostración.* Nuevamente por la Proposición 3.2.10 tenemos que para cada ordinal $\alpha < \text{mín}\{\lambda_G, \lambda_H\}$ $f_{p,G}(\alpha) + f_{p,G}(\alpha) = f_{p,H}(\alpha) + f_{p,H}(\alpha)$; esto implica que ambos cardinales $f_{p,G}(\alpha)$ y $f_{p,G}(\alpha)$ son finitos ó infinitos. En ambos casos obtenemos que $f_{p,G}(\alpha) = f_{p,H}(\alpha)$. ■

(3) Sean $\mathcal{F}$ un grupo $p$-primario finitamente generado, $G$ y $H$ grupos $p$-primarios reducidos tales que $\mathcal{F} \oplus G \cong \mathcal{F} \oplus H$, entonces $G$ y $H$ tienen los mismos invariantes de Ulm.

*Demostración.* Como $\mathcal{F}$ es reducido (véase la Nota 2.1.9 y [Fu], Cap. 3) y $\mathcal{F} \oplus G \cong \mathcal{F} \oplus H$ por la Proposición 3.2.10 tenemos que para cada ordinal $\alpha < \text{mín}\{\lambda_{\mathcal{F}}, \lambda_G, \lambda_H\}$

$$f_{p,\mathcal{F}}(\alpha) + f_{p,G}(\alpha) = f_{p,\mathcal{F}}(\alpha) + f_{p,H}(\alpha).$$

Como $\mathcal{F}$ es finitamente generado, $f_{p,\mathcal{F}}(\alpha)$ es finito. Así que de la igualdad anterior se sigue que $f_{p,G}(\alpha) = f_{p,H}(\alpha)$ para todo ordinal $\alpha < \text{mín}\{\lambda_{\mathcal{F}}, \lambda_G, \lambda_H\}$. ■

[1] Como $G \cong G' \leq H$ se sigue que $\lambda_G \leq \lambda_H$, análogamente se obtiene que $\lambda_H \leq \lambda_G$ y por lo tanto $\lambda_G = \lambda_H$.

[$(b)$] Esto es consecuencia inmediata del Teorema 3.2.8 y del inciso anterior en cada caso.

[$(c)$] Esto es una consecuencia inmediata de los incisos anteriores así como de lo visto en la Nota 1.3.16. ■

**Proposición 3.2.12.** *Sea* $G = \prod_{i\in\mathbb{Z}^+} \mathcal{Z}_{p^i}$. *Entonces*

*a)* $t(G)$ *no es un sumando directo de* $G$.

*b)* $t(G)$ *es un grupo p-primario sin elementos de altura infinita, pero no es una suma directa de grupos cíclicos.*

*Demostración.* [$(a)$] Comencemos notando que $G$ no tiene elementos de altura infinita, salvo 0. En efecto, sea $y = (\overline{y}_i)_{i\in\mathbb{Z}^+} \in G$ con la propiedad de que $h_G(y)$ es infinita, entonces para cada $n \in \mathbb{Z}^+$ existe $x_n = (\overline{x}_{n,i})_{i\in I} \in G$ tal que $p^k x_n = y$, es decir, para toda $i \in \mathbb{Z}^+$ $p^k\overline{x}_{n,i} = \overline{y}_i \in \mathcal{Z}_{p^i}$ lo que implica que, para toda $i \in \mathbb{Z}^+$ $\overline{y}_i$ es divisible por $p^k$ para toda $k \in \mathbb{Z}^+$, lo cual sólo es posible si $\overline{y}_i = \overline{0}$, para cada $i \in \mathbb{Z}^+$, pues cada $\mathcal{Z}_{p^i}$ es cíclico. Por lo tanto $y = 0$.

Para demostrar que $t(G)$ no es sumando directo de $G$ supondremos lo contrario y obtendremos que es posible encontrar un elemento en $G$ distinto de cero que es de altura infinita en $G$ lo que contradice lo demostrado en el párrafo anterior. Sea

$$y = (1, 1, p, p, p^2, p^2, p^3, p^3, \ldots, p^n, p^n, p^{n+1}, p^{n+1} \ldots) \in G.$$

Veamos que $y$ no puede ser anulado por ninguna potencia de $p$. Para ello notamos primero que, las entradas $2n$ y $2n + 1$ de $y$ son de orden $p^{(n-1)+2}$ para toda $n \geq 1$ ya que en la coordenada $2n$ está el elemento $p^{n-1}$ en el grupo $\mathcal{Z}_{p^{2n}}$ que es de orden $o(p^{n-1}) = p^{n+1}$ . Por otra parte, el elemento en la entrada $2n + 1$ es $p^n$ que pertenece al grupo $\mathcal{Z}_{p^{2n+1}}$ y por consiguiente $o(p^n) = p^{n+1}$.

Sea $k \in \mathbb{Z}^+$, con $k > 2$.[2] Multiplicando $y$ por $p^k$, de lo anterior tenemos que, las primeras $2k - 1$ coordenadas de $p^k y$ son 0;[3] en la siguiente coordenada $2k$, por construcción, está el elemento $p^{k-1} \in \mathcal{Z}_{p^{2k}}$ que es de orden $o(p^{k-1}) = p^{k+1}$ y por consiguiente $p^k(p^{k-1}) \neq 0$ en $\mathcal{Z}_{p^{2k}}$. De la misma manera, las demás coordenadas de $p^k y$ también son distintas de 0 y por lo tanto $p^k y \neq 0$. Dado que la elección de $k$ es arbitraria, concluimos que $y \notin t(G)$. En virtud que

[2] Claramente para los caso $k = 1, 2$ $p^k y \neq 0$.

[3] En la entrada $2(k-1)$ está el elemento $p^{k-2} \in \mathcal{Z}_{p^{2(k-1)}}$ cuyo orden es $p^k$ y en la entrada $2k-1$ está el elemento $p^{k-1} \in \mathcal{Z}_{p^{2k-1}}$ y claramente su orden es $p^k$.

$$\begin{aligned} y &= (1,1,p,p,p^2,p^2,\ldots,p^{k-1},p^{k-1},p^k,p^k,p^{k+1},p^{k+1},\ldots) \\ &= (1,1,p,p,p^2,p^2,\ldots,p^{k-1},p^{k-1},0,0,\ldots)+p^k(0,0.\ldots,1,1,p,p,\ldots), \end{aligned} \tag{3.36}$$

y como $p^{k+1}(1,1,p,p,p^2,p^2,\ldots,p^{k-1},\underset{\substack{\uparrow\\ (2k+1)\text{-ésimo lugar}}}{p^{k-1}},0,0,\ldots)=0$, tenemos que

$$(1,1,p,p,p^2,p^2,\ldots,p^{k-1},p^{k-1},0,0,\ldots)\in t(G).$$

Escribiendo $x=(0,0.\ldots,1,1,p,p,\ldots)\in G$, al tomando la clase lateral de $y$ módulo $t(G)$, a partir de (3.36) obtenemos que $p^k\overline{x}=\overline{y}$, lo cual muestra que $\overline{y}$ es un elemento, distinto de cero, de altura infinita en $G/t(G)$.

Si $t(G)$ es un sumando directo de $G$, ya que $G\cong t(G)\oplus(G/t(G))$, tendríamos que la imagen de $y$ (considerado como un elemento en $t(G)\oplus(G/t(G))$) bajo este isomorfismo determina un elemento en $G$ distinto de cero y con altura infinita lo cual es absurdo. Por lo tanto $t(G)$ no es un sumando directo de $G$.

[$(b)$] Claramente $t(G)$ es un grupo $p$-primario y no tiene elementos de altura infinita (recuérdese que, $h_H(x)\leq h_G(x)$ para todo $H\leq G$). Veamos ahora que $t(G)$ no es suma directa de grupos cíclicos y para ello calcularemos sus invariantes de Ulm.

Sea $T=t(G)$ y $\mathcal{A}=\{(a_0,a_1p,a_2p^2,a_3p^3,\ldots)\in G\mid 0\leq a_i<p,\ a_i\in\mathbb{Z}\}$. Claramente $\mathcal{A}\subseteq T$. Sea $(x_i)_{i\in\mathbb{Z}^+}\in T[p]$; $p(x_i)_{i\in\mathbb{Z}^+}=0$ implica que para toda $i\in\mathbb{Z}^+$ se satisface $px_i=0$ y por consiguiente $x_i\in\mathcal{Z}_{p^i}[p]=\langle p^{i-1}\rangle$; así $x_i=m_{i-1}p^{i-1}$ con $0\leq m_{i-1}<p$ para toda $i\in\mathbb{Z}^+$, mostrando que $(x_i)_{i\in\mathbb{Z}^+}\in\mathcal{A}$, es decir, $T[p]\subseteq\mathcal{A}$ y por lo tanto $T[p]=\mathcal{A}$.

Sea $x+G[p]_{n+1}\in G[p]_n/G[p]_{n+1}$, considerando $x\in G[p]_n$, necesariamente tenemos que $x=(0,0,\ldots,0,x_{n+1},x_{n+2},x_{n+3},\ldots)$, donde las primeras $n$ coordenadas son cero. Como $px=0$ tenemos además que $x_{n+j}\in\mathcal{Z}_{p^{n+j}}[p]=\langle p^{n+j-1}\rangle$ y por lo tanto $x_{n+j}=m_{n+j}p^{n+j-1}$ para toda $j\in\mathbb{Z}^+$; así

$$\begin{aligned} x &= (0,0,\ldots,0,m_{n+1}p^n,m_{n+2}p^{n+1},m_{n+3}p^{n+2},\ldots) \\ &= (0,0,\ldots,0,m_{n+1}p^n,0,\ldots)+(0,0,\ldots,0,0,m_{n+2}p^{n+1},m_{n+3}p^{n+2},\ldots) \\ &= (0,0,\ldots,0,m_{n+1}p^n,0,\ldots)+p^{n+1}(0,0,\ldots,0,0,m_{n+2},m_{n+3}p,\ldots), \end{aligned}$$

como

$$p^{n+2}(0,0,\ldots,0,0,m_{n+2},m_{n+3}p,\ldots)=0$$

tenemos que

$$p^{n+1}(0,0,\ldots,0,0,m_{n+2},m_{n+3}p,\ldots)\in G[p]_{n+1}.$$

Sea $y=(0,0,\ldots,0,m_{n+1}p^n,0,\ldots)$; pasando al cociente tenemos que $x+G[p]_{n+1}=y+G[p]_{n+1}$ y como $m_{n+1}p^n\in\mathcal{Z}_{p^{n+1}}[p]$ tenemos que $\dim_{\mathbb{Z}_p}(G[p]_n/G[p]_{n+1})=1$, es decir,

$$f_{p,T}(n) = 1 \text{ para toda } n \in \mathbb{N}. \tag{3.37}$$

Por otra parte, $G_\omega = \bigcap_{n\in\mathbb{Z}^+} p^n T = 0$, es decir, la longitud de $T$ es $\omega$ y por lo tanto $G[p]_\omega = 0$; así $f_{p,T}(\omega) = 0$. Si $T$ es una suma directa de grupos cíclicos, necesariamente $T = \bigoplus_{n\in\mathbb{Z}^+} \mathcal{Z}_{p^n}$ (véase (3.17)) y por lo tanto $T[p] \cong \bigoplus_{n\in\mathbb{Z}^+} \mathbb{Z}_p$; de aquí obtenemos que

$$o(T[p]) = p^{o(\mathbb{Z}^+)} = p^{\aleph_0} = 2^{\aleph_0} > \aleph_0 = o(\bigoplus_{n\in\mathbb{Z}^+} \mathcal{Z}_{p^n}) = o(T),$$

lo cual es absurdo. Por lo tanto $T$ no es una suma directa de grupos cíclicos. ■

# Conclusiones

En cualquier disciplina en la que nos desarrollemos, es necesaria la comprensión clara de nuestros objetos de estudio, y en matemáticas esto no es la excepción. En este sentido, poder describir un objeto lo mejor posible resulta ser una actividad muy interesante y en la mayor parte de los casos complicada. En la teoría de grupos, la primera división que se hace para investigar estos objetos es, por una parte, estudiar a los grupos abelianos (conmutativos) y por otra a los grupos no abelianos.

El objetivo de este trabajo consistió en presentar el Teorema de Ulm, el cual da una clasificación de los grupos abelianos numerables primarios reducidos mediante invariantes conocidos como **invariantes de Ulm**. Para llegar a este importante resultado hicimos uso de varios conceptos y resultados de la Teoría de Grupos, así como del Lema de Zorn y conocimientos básicos sobre cardinales y ordinales.

Hay ciertos tipos de grupos que están completamente clasificados, ya sea a través de representantes típicos (lo que significa que cada grupo del tipo en cuestión es isomorfo a alguno de estos representantes) o a través de invariantes. Como ejemplo se puede mencionar a la clase de grupos abelianos finitamente generados o también la de grupos divisibles.

Se sabe que cada grupo de torsión es suma directa de grupos primarios y también que cada grupo abeliano es suma directa de un grupo divisible y un grupo reducido (aquel que no tiene subgrupos divisibles salvo 0). También se sabe, como hemos dicho, que los grupos divisibles están completamente caracterizados, así que nuestro trabajo se redujo al estudio de los grupos abelianos numerables primarios reducidos.

Cabe aquí puntualizar que el zoclo de un grupo así como el concepto de altura de los elementos de un grupo jugaron un papel fundamental para llegar al Teorema de Ulm.

> ***Teorema de Ulm*** *Dos grupos p-primarios reducidos numerables son isomorfos si y sólo si tienen los mismos invariantes de Ulm.*

El material que se ha cubierto establece una buena base para posteriores estudios de $p$-grupos y grupos abelianos infinitos, en este sentido la bibliografía que sugerimos es [Fu II] y [Gr].

# Glosario de Símbolos

| | | |
|---|---|---|
| $o(G)$ | orden del grupo $G$ | 1 |
| $H \leq G$ | $H$ es subgrupo de $G$ | 1 |
| $H < G$ | subgrupo $H \neq G$ | 1 |
| $\langle X \rangle$ | grupo generado por el conjunto $X$ | 2 |
| $\langle \mathscr{F} \rangle$ | grupo generado por la familia $\mathscr{F}$ | 2 |
| $\sum_{i \in I} S_i$ | suma de la familia de grupos $\{S_i\}_{i \in I}$ | 2 |
| $\langle a \rangle$ | grupo cíclico generado por $a$ | 3 |
| $S(G)$ | zoclo del grupo $G$ | 3 |
| $\prod_{i \in I} G_i$ | producto directo de la familia $\{G_i\}_{i \in I}$ | 3 |
| $\bigoplus_{i \in I} G_i$ | suma directa de la familia $\{G_i\}_{i \in I}$ | 3 y 4 |
| $\mathcal{Z}$ | el grupo aditivo de los número enteros | 10 |
| $\mathcal{Z}_n$ | el grupo aditivo de las clases de residuos módulo $n$ | 10 |
| $t(G)$ | parte de torsión de un grupo $G$ | 11 |

| | | |
|---|---|---|
| $\mathcal{Q}$ | el grupo aditivo de los números racionales | 12 |
| $G_p$ | parte $p$-primario del grupo $G$ | 13 |
| $G[p]$ | elementos del grupo $G$ que son anulados por el número primo $p$ | 17 |
| $\mathcal{Q}_p$ | $\{\frac{m}{p^r} \mid m \in \mathcal{Z},\ r \in \mathbb{N}\}$ | 20 |
| $\mathcal{Z}_{p\infty}$ | el grupo $\mathcal{Q}_p/\mathcal{Z}$ | 20 |
| $F(G)$ | parte libre de torsión del grupo $G$ | 41 |
| $h_G(x)$ | altura de $x \in G$ en el grupo $G$ | 53 |
| $G_\alpha$ | elementos de $G$ cuya altura es mayor o igual que $\alpha$ | 68 |
| $S_\alpha$ | $S \cap G_\alpha$, con $S \leq G$ | 70 |
| $f_{p,G}(\alpha)$ | $\alpha$-ésimo invariante de Ulm | 71 |
| $p^{-1}G_\beta$ | $p^{-1}G_\beta = \{x \in G \mid px \in G_\beta\}$ | 81 |
| $S^*_\alpha$ | $S_\alpha \cap p^{-1}G_{\alpha+2}$ | 82 |

# Bibliografía

[Gr] Griffith, Phillip A, *Infinite Abelian Groups Theory*, University of Chicago Press, Chicago, 1970.

[Fu] Fuchs, Lásló, *Infinite Abelian Groups*, volumen I, Academic Press, Inc, London, 1970.

[Fu II] Fuchs, Lásló, *Infinite Abelian Groups*, volumen II, Academic Press, Inc, London, 1973.

[Gom] Gómez, Carmen, *Intruducción a la Teoría Intuitiva de Conjuntos (Cardinales y Ordinales)*, (Por aparecer en: Las Prensas de Ciencias, Facultad de Ciencias UNAM, México).

[Rot] Rotman, Joseph J, *The Theory of Groups: An Introduction*, Ally and Bcaon, Inc, Boston, 1971.

[Kap] Kaplansky, Irving, *Infinite Abelian Groups*, Cushing-Malloy, Inc, Michigan, 1954.