Universidad de Sonora

Departamento de Matemáticas

Tesis

Clasificación de Grupos Abelianos

Que para obtener el título de

Licenciado en Matemáticas

Presenta

Martín Eduardo Frías Armenta

Hermosillo, Sonora, 15 julio de 1993

Contenido

Introducción

Dentro de las matemáticas hay un tipo de estructuras algebraicas llamadas *grupos* que aparecen en muchos campos,

Howard Eves escribe (ver [1, pag. 130])

"... El programa de Erlangen pareció legítimo y correcto en un tiempo en que la teoría de grupos invadía casi todo el dominio de la matemática, y algunos profesores de ésta empezaron a creer que toda matemática no es sino un aspecto u otro de la teoría de los grupos. ..."

Aunque Eves da entender que los grupos han pasado ha segundo termino, todavía existen muchos campos, de la matemática,en los que el concepto de grupos es fundamental, por ejemplo, la base de la Topología Algebraica es el llamado grupo fundamental.[1]

Hay un resultado (teorema de Cayley) que nos dice que todo grupo es isomorfo a un subgrupo de un grupo de permutaciones. Pero este no es un gran adelanto ya que el grupo de permutaciones es siempre más

[1]El grupo fundamental del círculo es $\mathcal{Z}$, el grupo fundamental del toro hueco es $\mathcal{Z}X\mathcal{Z}$, el grupo fundamental del plano proyectivo es $\mathcal{Z}_2$ el de la botella de Klein $\mathcal{Z}_2$ el de la esfera es el trivial etc. Hay muchas propiedades de los espacios topológicos que se pueden probar apartir de la estructura de su grupo fundamental.(Para más sobre esto se puede ver Tesis de licenciatura de Gloria G. Andablo Reyes).

complicado que el original. Un mejor camino para desentrañar la estructura de los grupos es tratar de ponerlos en terminos de otros grupos más conocidos y más manejables. En este sentido hay un resultado llamado teorema de "Jordan-Hölder" que dice que cualquier grupo finito tiene una única descomposición en grupos finitos simples[2]; este teorema es similar al teorema fundamental de la aritmética en el sentido de que la descomposición siempre existe y es única salvo el orden. Esto no es tan fuerte como parece, ya que puede haber dos grupos distintos con la misma descomposición; por ejemplo: $\mathcal{Z}_2 \times \mathcal{Z}_2$ y $\mathcal{Z}_4$ tienen la misma "descomposición Jordan-Hölder"(a saber $\mathcal{Z}_2$), y sin embargo son grupos distintos.

En presente trabajo se desarrolla un resultado más fuerte[3] para el caso concreto de grupos abelianos. Además de que se desarrolla una teoría similar para grupos abelianos finitamente generados, y grupos abelianos infinitos.

En el capítulo uno, se demuestra que todo grupo abeliano finito tiene una única descomposición como suma directa de grupos $\mathcal{Z}_{p^n}$ para varios primos p, más aun si dos grupos tienen la misma descomposición son isomorfos.

En el capítulo dos se demuestra que todo grupo abeliano arbitrario es suma directa de un grupo "divisible" más un grupo "reducido", y los

[2]Ver [3, 5] de la bibliografía o Tesis de licenciatura de Guillermo Davila donde se hace un desarrollo similar a los libros citados.

[3]De la descomposición de un grupo sólo se puede construir el grupo en cuestión.

divisibles[4] a su vez son sumas directas de copias de $\mathcal{Q}$, y de "$\mathcal{Z}(p^\infty)$" para varios primos p.

En el capítulo tres se hace una mejor caracterización de los grupos divisibles, ya que estos son la parte más "grande" de los grupos abelianos arbitrarios. Para estos dos capítulos aunque el trabajo se apega más a [4] también se puede ver [8].

En el capítulo cuatro se generaliza el resultado anterior a los grupos finitamente generados, es decir, todo grupo finitamente generado tiene una única descomposición como suma directa de grupos $\mathcal{Z}_{p^n}$ y $\mathcal{Z}$. Para este y para el capítulo uno se pueden tomar como referecias [8, 7, 6] y para ver más ejemplos para el material expuesto se puede ver [2]. Aunque en [7] la herramienta usada es de otro tipo (teoría de funtores).

Para terminar el presente trabajo, aparece, en forma de apéndice el enuciado de Lema de Zorn que es usado en muchas de las demostraciones que aquí aparecen.

[4]Tanto el consepto de *divisible* como $\mathcal{Z}(p^\infty)$serán desarrollados en el capítulo tres

Quisiera aprovechar este espacio para agradecer:

A mi familia, que me ayudo tanto durante mi estancia en la Universidad de Sonora.

Al maestro Ramiro Avila Godoy, por sus consejos en los momentos adecuados.

A la Universidad de Sonora gracias a la cual aprendí tantas cosas.

A la m.c. Martha Guzman, al m.c Carlos Robles y al Dr. Marcelo Aguilar, por el tiempo invertido a este trabajo.

A todos los amigos por serlo.

Capítulo 1

Grupos Abelianos Finitos

En este capítulo daremos una caracterización de todos los grupos abelianos finitos en terminos de sus "factores directos"; de hecho demostraremos que todo grupo abeliano finito tiene una descomposición única en productos directos de $\mathcal{Z}_{p^n}$,[1] al cual llamaremos teorema fundamental de grupos abelianos finitos. Este teorema es guarda cierta anlogia con el teorema fundamental de la aritmética.

Para ello en la primera sección revisaremos la definición de producto directo,[2] demostraremos también un resultado (teorema 1.6) que nos será de gran ayuda en la demostración de muchos otros resultados importantes del presente trabajo. En la segunda sección demostraremos que todo grupo finito tiene una descomposición en suma directa de grupos cíclicos "p-primarios". En la tercera sección demostraremos la unicidad de dicha descomposición con lo que llegariamos el teorema

[1] Al contrario de la descomposición "Jordan-Hölder", esta es única en el siguiente sentido: Si dos grupos tienen la misma descomposición, entonces son isomorfos.

[2] En esta sección los resultados son para grupos arbitrarios (aunque los ejemplos son de grupos abelianos).

fundamental.

1.1 Preliminares

Definición 1.1 . *Si H y K son grupos, el* **producto directo (externo)** *de H y K, denotado por $H \times K$, es el conjunto de todos los pares ordenados (h, k), donde la operación binaria es la siguiente*

$$(h, k)(h\prime, k\prime) = (hh\prime, kk\prime).$$

Ejemplo 1.1 .[3] Sea $H = \mathcal{Z}_2 = \{0, 1\}$ y $K = \mathcal{Z}_3 = \{0, 1, 2\}$, entonces:

$$H \times K = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}$$

y la tabla de multiplicación de este grupo es:

$H \times K$	$(0,0)$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$
$(0,0)$	$(0,0)$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$
$(0,1)$	$(0,1)$	$(0,2)$	$(0,0)$	$(1,1)$	$(1,2)$	$(1,0)$
$(0,2)$	$(0,2)$	$(0,0)$	$(0,1)$	$(1,2)$	$(1,0)$	$(1,1)$
$(1,0)$	$(1,0)$	$(1,1)$	$(1,2)$	$(0,0)$	$(0,1)$	$(0,2)$
$(1,1)$	$(1,1)$	$(1,2)$	$(1,0)$	$(0,1)$	$(0,2)$	$(0,0)$
$(1,2)$	$(1,2)$	$(1,0)$	$(1,1)$	$(0,2)$	$(0,0)$	$(0,1)$

Las siguientes observaciones nos serán de gran utilidad para el desarrollo de nuestro tema:

[3]Los ejemplos (**estos tienen el único objetivo de aclarar algunos conceptos**) del presente capítulo todos tienen que ver con $\mathcal{Z}_n$, esto no es de extrañarse ya que son estos presisamente los "factores primos" de los grupos finitos.

1. $H \times K$ es un grupo que contiene copias isomorfas de H y K, a saber, $H \times \{1\}$[4] y $\{1\} \times K$.
   En el ejemplo 1.1 $H \times \{1\} = \mathcal{Z}_2 \times \{0\} = \{(0,0),(1,0)\} \approx \mathcal{Z}_2$ y $\{1\} \times K = \{0\} \times \mathcal{Z}_3 = \{(0,0),(0,1),(0,2)\} \approx \mathcal{Z}_3$

2. $H \times \{1\}$ y $\{1\} \times K$ son subgrupos normales de $H \times K$. Estos dos grupos generan $H \times K$ y su intersección es $\{(1,1)\}$.

3. $H \times K \approx K \times H$.
   Tomando H y K como en el ejemplo 1.1 podemos establecer el siguiente homorfismo $f : H \times K \to K \times H$:

$$
\begin{aligned}
f[(0,0)] &= (0,0) \\
f[(0,1)] &= (1,0) \\
f[(0,2)] &= (2,0) \\
f[(1,0)] &= (0,1) \\
f[(1,1)] &= (1,1) \\
f[(1,2)] &= (2,1)
\end{aligned}
$$

   Claramente f es un isomomorfismo.

Proposición 1.2 . *Sea G un grupo con subgrupos normales H y K tales que $H \bigcap K = \{1\}$ y $HK=G$ entonces:*
a) $hk = kh, \forall\, h \in H$ y $k \in K$.
b) sea $a \in G$, entonces existen únicos $h \in H$ y $k \in K$ tales que $a = hk$.

[4]Como es costumbre para grupos en general se utilizará el 1 como unitario, y cuando se hable de grupos abelianos se utilizará el cero.

Demostración:

a) Sabemos que K y H son normales, así que,
$h^{-1}k^{-1}h \in K$ y $k^{-1}hk \in H \Rightarrow h^{-1}k^{-1}hk \in K$ y $h^{-1}k^{-1}hk \in H$
pero $H \bigcap K = \{1\} \Rightarrow h^{-1}k^{-1}hk = 1 \Rightarrow k^{-1}hk = h \Rightarrow hk = kh.$

b) Si $a \in G = HK$ entonces $a = hk$; supongamos que $a = h\prime k\prime$ con $h, h\prime \in H$ y $k, k\prime \in K$. Luego $h^{-1}h\prime = kk\prime^{-1}$, así este elemento está simultáneamente en H y K, es decir, en $H \bigcap K = \{1\}$, por tanto $h = h\prime$ y $k = k\prime$.

■

La proposición anterior nos servirá para demostrar el siguiente:

Teorema 1.3 . *Sea G un grupo con subgrupos normales H y K tales que $H \bigcap K = \{1\}$ y $HK = G$, entonces $G \approx H \times K$.*

Demostración: Sea $f : G \to H \times K$ definida por: $f(a) = (h, k)$[5], donde a=hk.
$f(aa\prime) = f[(hkh\prime k\prime)] = f[(hh\prime kk\prime)] = (hh\prime, kk\prime) = (h, k)(h\prime, k\prime) = f(a)f(a\prime)$. Claramente f es sobre y además, si $f(hk) = (1, 1)$, entonces $(h, k) = (1, 1)$ luego $h = k = 1$ y $hk = 1$, es decir, f es inyectiva.

[5]Está bien definida por proposición 1.2

■

Ejemplo 1.2 . Sea $G = \mathcal{Z}_{10}$ entonces $H = \{0,5\}$ y $K = \{0,2,4,6,8\}$ en efecto: $H \bigcap K = \{0\}$ y $HK = G$, por tanto, $H \times K \approx \mathcal{Z}_2 \times \mathcal{Z}_5 \approx \mathcal{Z}_{10}$

Teorema 1.4 . *Sea $G = H \times K$ y sean $H_1 \lhd H$ y $K_1 \lhd K$. Entonces $H_1 \times K_1 \lhd G$ y $G/(H_1 \times K_1) \approx (H/H_1) \times (K/K_1)$.*

Demostración: Sean $\alpha : H \to H/H_1$ y $\beta : K \to K/K_1$, los homomorfismos naturales. Sea $F : G \to (H/H_1) \times (K/K_1)$ definida: $F(h,k) = (\alpha(h), \beta(k))$.
F es un homomorfismo cuyo núcleo es $H_1 \times K_1$ y la imagen de F es $(H/H_1) \times (K/K_1)$, por uno de los teoremas de isomorfismos se sigue $G/(H_1 \times K_1) \approx (H/H_1) \times (K/K_1)$.

■

Corolario 1.5 . *Si $G = H \times K$, entonces $G/(H \times \{1\}) \approx K$.*

En el ejemplo 1.2 es claro que $\mathcal{Z}_{10}/\mathcal{Z}_2 \approx \mathcal{Z}_5$.

Los elementos de un producto directo externo son pares ordenados, una condición algo restrictiva. Diremos que un grupo G es el *producto directo interno* de H y K, si H y K son subgrupos normales de G con

$H \bigcap K = \{1\}$ y $HK = G$.

El émfasis aquí es que los propios factores y no copias isomorfas de ellos yasen en G. (Si $G = H \times K$ es un producto directo externo, entonces es también el producto directo interno de $H \times \{1\}$ y $\{1\} \times K$ pero no es el producto directo interno de H y K). Las dos versiones de producto directo por supuesto, producen grupos isomorfos. En lo sucesivo no distinguiremos entre externo e interno y diremos sólo producto directo, de acuerdo con el siguiente

Teorema 1.6 . *Si G es un grupo con subgrupos normales $H_1, H_2, ..., H_m$, entonces $G \approx \prod_{i=1}^{m} H_i$. $\Leftrightarrow$ $G = [\bigcup_{i=1}^{m} H_i]$ y para toda j, $H_j \bigcap [\bigcup_{i \neq j} H_i] = \{1\}$*

Demostración:

($\Leftarrow$) Por inducción:

Para m=2 el teorema es equivalente al teorema 1.3.

Supongamos que el teorema se cumple para m=k-1:

Es decir: $G = [\bigcup_{i=1}^{k-1} H_i]$ y para toda j, $H_j \bigcap [\bigcup_{i \neq j} H_i] = \{1\} \Rightarrow G \approx \prod_{i=1}^{m} H_i$.

Para m=k:

Sea $H = [\bigcup_{i=1}^{k-1} H_i]$ y como se cumplen las hipótesis de inducción para H y los primeros k-1 H_i, se tiene que

$H \approx \prod_{i=1}^{k-1} H_i$

luego $G = [\bigcup_{i=1}^{m} H_i] = [\bigcup_{i=1}^{k-1} H_i \bigcup H_m] = [H \bigcup H_m]$

por lo que $H \bigcap H_m = H_m \bigcap [\bigcup_{i \neq m} H_i] = \{1\}$ y

por el teorema 1.3 $G \approx H \times H_m$, por tanto, $G \approx \prod_{i=1}^{m-1} H_i \times H_m \approx \prod_{i=1}^{m} H_i$

($\Rightarrow$) Por inducción:

Para m=2 trivial por las observaciones hechas anteriormente.

Para m=k-1: si $G \approx \prod_{i=1}^{k-1} H_i$, entonces $G \approx [\bigcup_{i=1}^{k-1} H_i]$ y para toda $j, H_j \bigcap [\bigcup_{i \neq j} H_i] = \{1\}$

Para m=k:

Sea $F_j = \prod_{i=1, i \neq j}^{k} H_i$ por hipótesis de inducción $F_j \approx [\bigcup_{i=1, i \neq j}^{k} H_i]$ así que

$G = \prod_{i=1}^{m} H_i = H_j \times F_j$, luego

entonces: $\{1\} = F_j \bigcap H_j = H_j \bigcap [\bigcup_{i \neq j} H_i] \forall j$

y $G \approx [F_m \bigcup H_m]$, por tanto, $G \approx [\bigcup_{i=1}^{m-1} H_i \bigcup H_m] \approx [\bigcup_{i=1}^{m} H_i]$

■

Este teorema es importante porque se usará como criterio para demostrar validos otros resultados.

1.2 Descomposición en Grupos Cíclicos Primarios

En lo que sigue trabajaremos exclusivamente con grupos abelianos . Como es usual, utilizaremos la notación aditiva en vez de la multiplicativa:

ab	$a+b$
a^{-1}	$-a$
1	0
a^n	na
ab^{-1}	$a-b$
HK	$H+K$
Ha	$H+a$
Producto directo	Suma directa
$H \times K$	$H \bigoplus K$
$\prod_{i=1}^{m}$	$\sum_{i=1}^{m}$
factor directo	sumando directo

Las siguientes observaciones para grupos abelianos simplifican mucho las cosas:

1. Si $a, b \in G$ y $n \in \mathcal{Z}$ entonces $n(a+b) = na + nb$

2. Si H es un subconjunto no vacío de G, entonces $[H]$ es el conjunto de todas las combinaciones lineales finitas de elementos de H con coeficientes en$\mathcal{Z}$.

Definición 1.7 . *Sea p un primo. Un grupo G es* **p-pimario** *(ó es un p-grupo) si todo elemento de G tiene orden una potencia de p.*

Si se trabaja en el contexto de grupos abelianos se usa el término p-primario; si no, se usa p-grupo.

Por ejemplo, $\mathcal{Z}_2$ y $\mathcal{Z}_{16}$ son 2-primarios, $\mathcal{Z}_{27}$ es 3-primario.

Definición 1.8 . *Sea G un grupo y p un primo, G_p es el conjunto de todos los elementos en G cuyo orden es una potencia de p.*

Claramente G_p es subgrupo de G.

Ejemplo 1.3 . Si tomamos $G = \mathcal{Z}_{20}$, entonces $G_2 = \{0, 5, 10, 15\}$ $(\approx \mathcal{Z}_4)$, y $G_5 = \{0, 4, 8, 12, 16\}$ $(\approx \mathcal{Z}_5)$

El siguiente teorema es el primer paso hacia el objetivo de este capítulo ya que reduce el problema de clasificar grupos abelianos finitos al de grupos p-primarios finitos.

Teorema 1.9 (Teorema de Descomposición primaria :) *Todo grupo abeliano finito es una suma directa de grupos p-primarios.*

Demostración: Afirmamos que $G = \sum G_p$, donde los índices varian sobre el conjunto de todos los primos que dividen a $|G|$. Usaremos el criterio del teorema 1.6 , y demostraremos en este orden:.

- i) $x \in G \Rightarrow x$ es una combinacion lineal de elementos en G_p.
- ii) $G_p \bigcap [\bigcup_{q \neq p} G_q] = \{0\}$

(i) Sea $x \in G, x \neq 0$, y sea n el orden de x. Por el teorema fundamental de la aritmética, $n = p_1^{e_1} p_2^{e_2} ... p_k^{e_k}$, donde los p_i son primos distintos y el exponente $e_i \geq 1$. Tomemos al conjunto de $n_i = \frac{n}{p_i^{e_i}}$, y observemos que $(n_1, n_2, ..., n_k) = 1$. Así, existen m_i tales que $\sum_{i=1}^{k} m_i n_i = 1$, por lo que , $\sum_{i=1}^{k} m_i n_i x = x$; nótese ahora que $p_i^{e_i} m_i n_i x = m_i n x = 0$, así, $m_i n_i x \in G_{p_i}$. Conclución $\bigcup G_{p_i}$ genera a G.

(ii) Sea $x \in G_p \bigcap [\bigcup_{q \neq p} G_q]$. Por un lado tenemos, $p^e x = 0$ para algún e; por otro $x = \sum x_q$, donde $q^{e_q} x_q = 0$, para exponentes e_q. Hagamos $t = \prod q^{e_q}$, entonces $tx = 0$. Es claro que $(p^e, t) = 1$, así, exiten $a, b \in \mathcal{Z}$ tales que $ap^e + bt = 1$ por lo que $x = ap^e x + btx = 0$.

■

Los subgrupos G_p de G son llamados componentes primarias de G.

Ejemplo 1.4 . Tomemos $G = \mathcal{Z}_4 \oplus \mathcal{Z}_6$ entonces las dos componentes primarias son $G_2 \approx \mathcal{Z}_4 \oplus \mathcal{Z}_2$ y $G_3 \approx \mathcal{Z}_3$

Proposición 1.10 . *Sea G un grupo abeliano p-primario y sean y_1, y_2, ..., y_t elementos de G tales que*

$$[y_1, y_2, ..., y_t] = [y_1] \bigoplus [y_2] \bigoplus ... \bigoplus [y_t]$$

(a) Si $z_1, z_2, ..., z_t$ son elementos de G tales que $pz_i = y_i \forall$, i entonces $[z_1, z_2, ..., z_t] = [z_1] \bigoplus [z_2] \bigoplus ... \bigoplus [z_t]$

(b) Si $k_1, k_2, ..., k_t$ son enteros entonces
$[k_1 y_1, k_2 y_2, ..., k_t y_t] = [k_1 y_1] \bigoplus [k_2 y_2] \bigoplus ... \bigoplus [k_t y_t]$

Demostración: Usando el criterio del teorema 1.6, la primera parte es obvia para ambos incisos:
(a) Sea $x \in [z_i] \bigcap [\bigcup_{j \neq i} z_j]$, entonces $x = m_i z_i = \sum_{j \neq i} m_i z_j]$ por lo que $px = m_i(pz_i) = m_i y_i = \sum_{j \neq i} m_j y_j \in [y_i] \bigcap [\bigcup_{j \neq i} [y_j]] = \{0\}$ $\Rightarrow px = 0$. Por consiguiente $pm_i z_i = m_i y_i = 0 \Rightarrow p | m_i$[6] también, como $0 = \sum_{j \neq i} p(m_j z_j) = \sum_{j \neq i} m_j (pz_j) = \sum_{j \neq i} m_j y_j \Rightarrow m_j y_j = 0$, luego por (6) $p | m_j \, \forall \, j$. Sea $m_j = pt_j$. Así, $x = pt_i z_i = \sum_{j \neq i} pt_j z_j \Rightarrow$ $x = t_i y_i = \sum_{j \neq i} t_j y_j$

Por tanto $x = 0$

(b)Sea $x \in [k_i y_i] \bigcup [\bigcap_{j \neq i} [k_j y_j]]$. Luego,
$x = m_i k_i y_i = \sum_{j \neq i} m_j k_j y_j \in [y_i] \bigcup [\bigcap_{j \neq i} [y_j]] = \{0\}$

Por tanto $x = 0$.

■

[6]Como el orden de y_i es una potencia de p y $m_i y_i = 0$ entonces $p | m_i$.

Ejemplo 1.5 . $G = \mathcal{Z}_{16} \oplus \mathcal{Z}_8$, $(2,0)$ y $(0,4)$ son tales que $[(2,0),(0,4)] = [(2,0)] \oplus [(0,4)]$
por (a) $[(1,0),(0,2)] = [(1,0)] \oplus [(0,2)]$
y por (b) $[(6,0),(0,4)] = [(6,0)] \oplus [(0,4)]$

Definición 1.11 . *Sea G un grupo abeliano y m un entero positivo. mG es el siguiente conjunto*

$$mG = \{mx : x \in G\}$$

Es inmediato que mG es un subgrupo de G. De hecho mG es la imagen del homomorfismo $f : G \to G$ definido por $f(x) = mx$.

Ejemplo 1.6 . Si $G = \mathcal{Z}_8$ entonces $2G = \{0,2,4,6\} \approx \mathcal{Z}_4$

Lema 1.12 . *Sea p un primo, un grupo abeliano G con $pG = \{0\}$ es un espacio vectorial sobre el campo $\mathcal{Z}_p$ y es una suma directa de grupos cíclicos cuando G es finito .*

Demostración: Denotaremos por $\overline{k}$ la clase de residuos del entero k en $\mathcal{Z}_p$.
Definimos una multiplicación escalar en G por $\overline{k}x \doteq kx$ donde $x \in G$
Esta operación está bien definida ya que si $k \equiv \overline{k} \, mod\,(p)$ entonces $k - \overline{k} = mp$ para algún $m \in \mathcal{Z}$, luego $(k - \overline{k})x = mpx = 0$, luego $kx = \overline{k}x$.

Se puede ver fácilmente que G es un espacio vectorial sobre $\mathcal{Z}_p$, y si G es finito, entonces G tiene una base, digamos, $\{x_1, x_2, ..., x_t\}$. Así $G = [x_1, x_2, ..., x_t]$; veamos que $G = [x_1] \oplus [x_2] \oplus ... \oplus [x_t]$
Si $a \in [x_i] \bigcap [\bigcup_{j \neq i} [x_j]]$, entonces $a = \overline{k_i} x_i = \sum_{j \neq i} \overline{k_j} x_j porloque$

$$x_i = \sum_{j \neq i} \overline{k_j}\, \overline{k_i}^{-1} x_j$$

si $\overline{k_i} \neq 0$ entonces x_i está en el espacio generado por $\{x_j\}_{j \neq i}$ lo cual es imposible ya que son linealmente independientes.
Así, $G = [x_1] \oplus [x_2] \oplus ... \oplus [x_t]$ (por el criterio del teorema 1.6).

■

Ejemplo 1.7 . Sea $G = \{0, x_1, x_2, x_3\}$ con la siguiente tabla de sumar:

$\oplus$	0	x_1	x_2	x_3
0	0	x_1	x_2	x_3
x_1	x_1	0	x_3	x_2
x_2	x_2	x_3	0	x_1
x_3	x_3	x_2	x_1	0

Aquí $2G = \{0\}$ (todos los elementos son de orden 2). G es un espacio vectorial sobre $\mathcal{Z}_2$ y $G = [x_1] \oplus [x_3]$ (o también $G = [x_1] \oplus [x_2]$).

El siguiente teorema es importante ya que es prácticamente la demostración de la **existencia** de una descomposición de G en suma de grupos $\mathcal{Z}_{p^n}$

Notación : $G[p] = \{x \in G \mid px = 0\}$

Teorema 1.13 (*Teorema de la base:) Todo grupo abeliano finito G es una suma directa de grupos cíclicos p − primarios.*

Demostración: por el teorema 1.9 podemos suponer que G es p-primario. Usaremos inducción sobre m, donde m es un entero positivo tal que $p^m G = \{0\}$, (tal entero existe, pues tomese $m = max\{m_i : donde \bigcirc (g_i) = p^{m_i},\ g_i \in G\})$. Si $m = 1$, el teorema es exactamente el lema anterior.

Supongamos el teorema válido para m y demostrémoslo para m+1.

Así, sea $p^{m+1}G = \{0\}$. Sea $H = pG$; entonces $p^m H = \{0\}$, y por hipótesis de inducción H es suma directa de grupos primarios cíclicos *Es decir*

$$H = pG = \sum[y_i] \text{ con } y_i \in pG$$

por lo que existen elementos $z_i \in G$, con $pz_i = y_i$. Si L es el subgrupo de G generado por los z_i, entonces $L = \sum[z_i]$ (proposición 1.10).

Afirmamos que L es un sumando directo de G, para lo cual, debemos producir un subgrupo complementario M de G tal que $L \oplus M = G$.

Como $G[p] = \{x \in G : px = 0\}$, entonces $p(G[p]) = 0$, así es que se cumple que $G[p]$ es un espacio vectorial sobre $\mathcal{Z}_p$ por el lema anterior.

Si cada k_i es el orden de cada y_i, entonces cada $k_i z_i$ tienen orden p:

en efecto $pz_i = y_i \Rightarrow p(k_i z_i) = k_i(pz_i) = k_i y_i = 0$

y así, $k_i z_i \in G[p]$.

Por la proposición 1.10, el conjunto de $k_i z_i$ es subconjunto independiente del espacio vectorial $G[p]$, extenderemos ahora este conjunto a una base de $G[p]$ es decir existen elementos $\{x_1, x_2, ..., x_s\}$ tales que:

$\{k_i z_i\} \cup \{x_1, x_2, ..., x_s\}$ es una base de $G[p]$. Sea $M = [x_1, x_2, ..., x_s]$. Como los x_i son linealmente independientes, entoces $M = \sum[x_j]$ (obs: $M \subseteq G[p]$).

Queda por probar que $G = L \oplus M$. para ello usaremos el criterio del teorema 1.6.

(i) $L \bigcap M = \{0\}$: Si $x \in L \bigcap M$, entonces

$x = \sum b_i z_i = \sum a_j x_j$

pero como $x \in M \subseteq G[p], px = 0$,

así $\sum pb_i z_i = 0$ entonces[7] $0 = pb_i z_i = b_i y_i \, \forall \, i$

$b_i = b\prime_i k_i$ ya que el orden de y_i es k_i; se tiene pues:

$0 = x - x = \sum b_i z_i - \sum a_j x_j = \sum b\prime_i k_i z_i - \sum a_j x_j$

pero $\{k_i z_i\} \cup \{x_j\}$ es una base de $G[p]$ por tanto $b\prime_i = 0$ y $a_j = 0 \, \forall \, i, j$

$\Rightarrow x = 0;$

(ii) $G = L + M$.

Sea $x \in G. \Rightarrow px \in pG = H \Rightarrow px = \sum c_i y_i = \sum pc_i z_i$ entonces

$p(x - \sum c_i z_i) = 0$

$\Rightarrow x - \sum c_i z_i \in G[p]$. Como $\{k_i z_i, x_1, ., x_s\}$ es base de $G[p] \Rightarrow$

$\Rightarrow x - \sum c_i z_i = \sum a_j x_j + \sum b_i k_i z_i$

$\Rightarrow x - \sum a_j x_j + \sum (c_i + b_i k_i) z_i \in L + M$

■

[7] Por ser independientes

Si G un grupo abeliano finito, por el teorema anterior $G = \bigoplus_{i\in I} G_i$ donde G_i es cíclico y p_i-primario (p_i algún primo). Se tiene entonces que $|G_i| = p_i^{\alpha_i}$ con $\alpha_i \geq 0$ ya que si $|G_i| = q_1^{\beta_1} q_2^{\beta_2} ... q_s^{\beta_s}$ con $q_1 = p_i, q_t$ primos distintos y $\beta_t \geq 0$ $(t \in \{1, 2, ..., s\})$ y si algún $\beta_t \geq 1$ $(t \neq 1)$ entonces por el teorema de Cauchy para grupos abelianos $\exists\, y \in G_i$ tal que $O(y) = q_t \neq p_i$ lo cual contradice el hecho de que G_i es p_i-primario. Así, $G = \bigoplus \mathcal{Z}_{p_i^{\alpha_i}}$ donde p_i es primo y $\alpha_i \geq 0$.

Los siguientes dos lemas nos ayudarán a demostrar la unicidad del teorema fundamental.

Lema 1.14 . *Si* $G = \bigoplus_{i=1}^{n} H_i$ *entonces* $mG = \bigoplus_{i=1}^{n} mH_i$ *y* $G[p] = \bigoplus_{i=1}^{n} (H_i[p])$

Demostración: Sea $x \in mG$ entonces $x = mg$ para algún $g \in G$. Por consiguiente existen $h_i \in H_i$ $(i = 1, 2, ..., n)$ tales que

$$g = h_1 + h_2 + ... + h_n \Rightarrow$$

$mg = mh_1 + mh_2 + ... + mh_n \in mH_1 + mH_2 + ... + mH_n$.
Ahora si $z \in mH_i \bigcap [\bigcup_{j\neq i} mH_j]$, entonces $z = mh_i = \sum_{j\neq i} mh_j \in H_i \bigcap [\bigcup_{j\neq i} H_j] = \{0\} \Rightarrow z = 0$
Por tanto, $mG = \bigoplus_{i=1}^{n} mH_i$.

Ahora, sea $x \in G[p]$ (por tanto $px = 0$). Existen $h_i \in H_i$ $(i = 1, 2, ..., n)$ tales que $x = h_1 + h_2 + ... + h_n$, luego $0 = px = ph_1 + ph_2 +$

$... + ph_n \in \bigoplus_{i=1}^{n} H_i. \Rightarrow ph_i = 0 \forall i \Rightarrow x \in H_1[p] + H_2[p] + ... + H_n[p]$. Si $z \in H_i[p] \bigcap [\bigcup_{j \neq i} H_j[p]]$, entonces se tiene que $z \in H_i$ y $pz = 0$ y también $z \in [\bigcup_{j \neq i} H_j]$ y $pz = 0 \Rightarrow z \in H_i \bigcap [\bigcup_{j \neq i} H_j] \Rightarrow z = 0$.

■

Lema 1.15 . *Sea H un grupo abeliano finito con $pH = \{0\}$ (por tanto $|H| = p^{\alpha}$, $\alpha \geq 0$) para algún primo p (H es llamado grupo abeliano fundamental). Cualquiera dos descomposiciones de H en suma directa de grupos cíclicos tiene el mismo número de sumandos $d(H)$.*

Demostración: Supongamos que $H = \bigoplus_{i=1}^{n} [y_i] = \bigoplus_{i=1}^{m} [z_j]$. Como H es un espacio vectorial sobre $\mathcal{Z}_p$ se sigue que $\{y_1, y_2, ..., y_n\}$ y $\{z_1, z_2, ..., z_m\}$ son bases de H, luego $n = m$.

Observemos que $d(H)$ es la dimensión de H considerada como espacio vectorial sobre $\mathcal{Z}_p$

■

1.3 Unicidad de la Descomposición

Notación: Si G es un grupo abeliano finito p-primario y si $n \geq 0$ es entero entonces:

$$U(n,G) = d\left(\frac{p^nG \bigcap G[p]}{p^{n+1}G \bigcap G[p]}\right)$$

donde $d(H)$ es la dimención de H como espacio vectorial sobre $\mathcal{Z}_p$; Podría pensarse que la definición de $U(n,G)$ esta fuera de contexto pero con el teorema 1.17 demostraremos que $U(n,G)$ es precisamente la cantidad de sumandos cíclicos de orden p^{n+1}. Antes de demostrar dicho teorema demostraremos una proposición auxiliar.

Proposición 1.16 . *Si $\sigma(p^{n+1})$ es el grupo cíclico de orden p^{n+1} ($\mathcal{Z}_{p^{n+1}}$), entonces:*

$$\mathcal{Z}_p \approx p^n\sigma(p^{n+1}) \approx \sigma(p^{n+1})[p]$$

Para la demostración de esta proposición utilizaremos la notación de clases residuales, pero sólo para esta proposición.

Demostración:

$\mathcal{Z}_p \approx \{0, p^n, 2p^n, 3p^n, ..., (p-1)p^n\} \subseteq p^n\sigma(p^{n+1})$

ahora, tomemos $\overline{x} \in \sigma(p^{n+1})$ tal que $p^n\overline{x} \in p^n\sigma(p^{n+1})$ y sea x el entero positivo más pequeño que pertenece a la clase de residuos $\overline{x}$ modulo p^{n+1}. Entonces por el algoritmo de euclides existen k_1 y k_2 tales que:

$x = k_1p + k_2$ con $0 \leq k_2 < p$

$\Rightarrow p^nx = p^{n+1}k_1 + p^nk_2$ con $0 \leq k_2 < p$

$\Rightarrow p^n\overline{x} = p^n\overline{k_2}$ con $0 \leq k_2 < p$

$\Rightarrow p^n\overline{x} \in \{0, p^n, 2p^n, 3p^n, ..., (p-1)p^n\}$

$\therefore \mathcal{Z}_p \approx p^n\sigma(p^{n+1})$

Sabemos que $p^n\sigma(p^{n+1}) \subseteq \sigma(p^{n+1})[p]$,

tomemos ahora, $\overline{x} \in \sigma(p^{n+1})[p] \Rightarrow p\overline{x} = 0$

Sea x el entero positivo más pequeño que pertenece a la clase de residuos $\overline{x}$ modulo p^{n+1}. Entonces por el algoritmo de Euclides existen k_1 y k_2 tales que:

$x = k_1p^n + k_2$ con $0 \leq k_2 < p^n$

$\Rightarrow (\overline{0} =)\ px = p^{n+1}k_1 + pk_2$ con $0 \leq pk_2 < p^{n+1}$

$\Rightarrow 0 \leq pk_2 = rp^{n+1} < p^{n+1}$

$\Rightarrow k_2 = 0$

$\Rightarrow x = k_1p^n \in p^n\sigma(p^{n+1})$.

□

Ahora pasemos al teorema que nos interesa.

Teorema 1.17 . *Sea G un grupo abeliano finito p-primario. Cualquiera dos descomposiciones de G en una suma directa de grupos cíclicos tiene el mismo número de sumandos de cada orden. De hecho, el número de sumandos cíclicos de orden p^{n+1} es $U(n, G)$.*

Demostración: Sea $G = \sum \sigma_i$, donde cada σ_i es un subgrupo cíclico de G. Ahora, adoptaremos la siguiente notación:

$G = \sum \sigma(p) \bigoplus \sum \sigma(p^2) \bigoplus \ldots \bigoplus \sum \sigma(p^t)$,

donde $\sum \sigma(p^i)$ significa la suma de todos los subgrupos cíclicos de orden

p^i y $\sum \sigma(p^i) = \{0\}$ si no hay sumandos de orden p^i. Por el lema 1.14,

$$G[p] = \sum \sigma(p)[p] \bigoplus \sum \sigma(p^2)[p] \bigoplus \ldots \bigoplus \sum \sigma(p^t)[p]$$

$$G[p] = \sum \sigma(p) \bigoplus \sum p\sigma(p^2) \bigoplus \ldots \bigoplus \sum p^{t-1}\sigma(p^t)$$

mientras que

$$p^n G = \sum p^n\sigma(p) \bigoplus \sum p^n\sigma(p^2) \bigoplus \ldots \bigoplus \sum p^n\sigma(p^t)\ (n \leq t)$$

y también por el lema 1.14

$$p^n G = \sum p^n\sigma(p^{n+1}) \bigoplus \sum p^n\sigma(p^{n+2}) \bigoplus \ldots \bigoplus \sum p^n\sigma(p^t)\ (n \leq t)$$

Una obserbación importante que debemos hacer es que tanto $\sum \sigma(p^i)$ como $\sum \sigma(p^i)[p]$ y $\sum p^r\sigma(p^i)$ (con $r < i$) tienen la misma cantidad de sumandos por lema 1.14.

Entonces,

$$p^n G \bigcap G[p] = \sum p^n\sigma(p^{n+1}) \oplus \sum p^n\sigma(p^{n+2}) \oplus \ldots \oplus \sum p^n\sigma(p^t)$$

$$\bigcap \sum \sigma(p) \oplus \sum p\sigma(p^2) \oplus \ldots \oplus \sum p^{t-1}\sigma(p^t)$$

Así $\forall n < t$,

$$p^n G \bigcap G[p] = \sum p^n\sigma(p^{n+1}) \bigoplus \sum p^{n+1}\sigma(p^{n+2}) \bigoplus \ldots \bigoplus \sum p^{t-1}\sigma(p^t)$$

Esta igualdad se tiene porque:

$\{0\} \subseteq p^i\sigma(p^{i+1})$ para $i = 0, 1, 2, ..., n$.

y

$p^i\sigma(p^{i+1}) \subseteq p^n\sigma(p^{i+1})$ para $i = n, n+1, ..., t-1$

Además de usar el hecho de que si $A_1, b_1 \subseteq C_1$; $A_2, B_2 \subseteq C_2$; ...; $A_n, B_n \subseteq C_n$ y $[\bigcup_{i=1}^{n} C_i] = C_1 \bigoplus ... \bigoplus C_n$ entonces $(A_1 \bigoplus ... \bigoplus A_n) \bigcap (B_1 \bigoplus ... \bigoplus B_n) = (A_1 \bigcap B_1 \bigoplus ... \bigoplus A_n \bigcap B_n)$.

Luego,

$$p^{n+1}G \bigcap G[p] = \sum p^{n+1}\sigma(p^{n+2}) \bigoplus \sum p^{n+2}\sigma(p^{n+3}) \bigoplus ... \bigoplus \sum p^{t-1}\sigma(p^t)$$

$$(p^nG \bigcap G[p])/(p^{n+1}G \bigcap G[p]) \approx \sum p^n\sigma(p^{n+1})$$

por tanto:

$$U(n, G) = d(\sum p^n\sigma(p^{n+1}))$$

Se tiene además $p\sum p^n\sigma(p^{n+1}) = 0$ y por lema 1.15, se sigue que $U(n, G)$ es la dimención de $\sum p^n\sigma(p^{n+1})$ como espacio vectorial sobre $\mathcal{Z}_p$, es decir, $U(n, G)$ es la cantidad de sumandos de orden p^{n+1}.
Ahora, $U(n, G)$ depende únicamente de G, no de la descomposición de G, por tanto para cualesquiera dos descomposiciones de G la cantidad de sumandos de orden p^n es la misma.

■

Teorema 1.18 . *Sea G y H grupos abelianos finitos p-primarios Entonces $G \approx H$ si, y sólo si $U(n, G) = U(n, H)$ $\forall n \geq 0$*

($\Rightarrow$) Supongamos que $f : G \to H$ es un isomorfismo. Se tiene que $G = \sum \sigma_i$, donde cada σ_i es cíclico, y por el teorema 1.17, $U(n, G)$ es el número de σ_i de orden p^{n+1}, ahora
$H = f(G) = f(\sum \sigma_i) = \sum f(\sigma_i)$ (por ser isomorfismo)
y $f(\sigma_i) = \sigma_i \, \forall \, i$.
Para cada $n \geq 0$ hay así $U(n, G)$ sumandos $f(\sigma_i)$ de H de orden p^{n+1} pero, por el teorema 1.17, este número es $U(n, H)$. Por tanto $U(n, G) = U(n, H) \; \forall n \geq 0$

($\Leftarrow$) Supongamos $U(n, G) = U(n, H) \forall \, n \geq 0$. Por el teorema 1.17 tenemos que el número de sumandos cíclicos en G de orden p^{n+1} coincide con el número de sumandos cíclicos en H de orden p^{n+1}, $\forall n \geq 0$
Sean

$$G = \sum \sigma(p) \bigoplus \sum \sigma(p^2) \bigoplus \ldots \bigoplus \sum \sigma(p^t)$$

y

$$H = \sum {}'\sigma(p) \bigoplus \sum {}'\sigma(p^2) \bigoplus \ldots \bigoplus \sum {}'\sigma(p^s)$$

luego $\sum \sigma(p^i)$ y $\sum' \sigma(p^i)$ tienen el mismo número de sumandos entonces $t = s$ y $\sum \sigma(p^i) \approx \sum' \sigma(p^i)$ por tanto

$$\begin{aligned} G &= \sum \sigma(p) \oplus \sum \sigma(p^2) \oplus \ldots \oplus \sum \sigma(p^t) \\ &\approx \sum' \sigma(p) \oplus \sum' \sigma(p^2) \oplus \ldots \oplus \sum' \sigma(p^t) = H \end{aligned}$$

Entonces $G \approx H$

Los dos teoremas anteriores casi completan el objetivo de este capítulo, solo falta librarnos del adjetivo p-primarios lo cual lograremos con las siguientes tres proposiciones.

Lema 1.19 . *Sean G y H grupos abelianos finitos y sea $f : G \to H$ un homomorfismo. Para cada p se tiene,*

$$f(G_p) \subseteq H_p$$

Demostración: Sea $y \in f(G_p)$, entonces $y = f(x)$ para algún $x \in G_p$.
$\Rightarrow$ para algún $\alpha \geq 0$ $p^\alpha x = 0$
luego $p^\alpha y = p^\alpha f(x) = f(p^\alpha x) = f(0) = 0$.
$\Rightarrow o(y)|p^\alpha \Rightarrow o(y) = p^\beta$ para algún β
$\Rightarrow y \in H_p$

■

Teorema 1.20 . *Sea G y H grupos abelianos finitos; $G \approx H$ si, y solo si $G_p \approx H_p$ para todo primo p.*

Demostración:
($\Rightarrow$) Observemos primeramente que si $f : G \to H$ es isomorfismo entonces para $x \in G$, $o(x) = o(f(x))$. En efecto sea $m = o(x)$ entonces $mf(x) = f(mx) = f(0) = 0$ y si $0 < r < m$ fuese tal que $rf(x) = 0$
$0 = rf(x) = f(rx) \Rightarrow$ [8] $rx = 0$ ∇ •

[8] por ser 1-1

por tanto, $o(f(x)) = o(x)$.

Ahora, nos gustaría ver que$f(G_p) = H_p$. Ya tenemos $f(G_p) \subseteq H_p$; si $z \in H_p \Rightarrow o(z) = p^\alpha \Rightarrow p^\alpha z = 0$ para algún $\alpha \geq 0$. Como $z \in H$, $\exists\, x \in G$ tal que $f(x) = z$ y puesto $o(x) = o(f(x)) = o(z) \Rightarrow o(x) = p^\alpha$, así, $z = f(x)$ con $x \in G_p$, es decir, $H_p \subseteq f(G_p)$.

Por tanto $f|_{G_p} : G_p \to f(G_p) = H_p$ es isomorfismo, es decir $G_p \approx H_p \; \forall\, p$ primo .

($\Leftarrow$) Sabemos que $G = \bigoplus G_p$ donde p varía sobre el conjunto I de los primos divisores de $|G|$.

Análogamente $H = \bigoplus H_q$ con q variando sobre el conjunto de índices J de los divisores de $|H|$.

Por hipótesis, para cada $p \in I$ primo, $G_p \approx H_p$, por tanto, H contiene un subgrupo H_p y como ésto se verifica $\forall p \in I$

$\Rightarrow G = \bigoplus G_p \approx \bigoplus_{p \in I} H_p < H$. Análogamente $H \approx \bigoplus_{q \in J} G_q < G$.

por tanto $G \approx H$

Teorema 1.21 (Teorema fundamental) *Sea G un grupo abeliano finito. Cualquiera dos descomposiciones de G en suma directa de grupos cíclicos primarios tiene el mismo número de sumandos de cada orden.*

Demostración: Supongamos que $G \approx \bigoplus \sigma_i$; $G \approx \bigoplus \overline{\sigma_j}$ donde en ambas descomposiciones los sumandos son grupos cíclicos primarios.

Sea p un primo tal que $p|o(G)$

y sean (para $n \geq 0$)

$k = \#$ de sumandos de orden p^{n+1} que aparecen en $\bigoplus \sigma_i$ y

$l = \#$ de sumandos de orden p^{n+1} que aparecen en $\bigoplus \overline{\sigma_i}$

$\bigoplus \sigma_i \approx \bigoplus \overline{\sigma_j} \Rightarrow (\bigoplus \sigma_i)_p \approx (\bigoplus \overline{\sigma_j})_p$ por el teorema 1.20

$\Rightarrow U(n, (\bigoplus \sigma_i)_p) = U(n, (\bigoplus \overline{\sigma_j})_p)$ $\forall n \geq 0$ por el teorema 1.17 y por el teorema 1.18

Por lo tanto $k = l$. $(\forall\, p, \forall\, n)$.

■

Capítulo 2

Grupos Abelianos Infinitos

Al contrario de los grupos abelianos finitos, los infinitos no están completamente clasificados, sin embargo los principales resultados los presentaremos aquí. El principal resultado es el siguiente: Si G es un grupo abeliano infinito, entonces $G = \sum \mathcal{Q} \bigoplus \sum \mathcal{Z}(p^\infty) \bigoplus R$ para varios primos p; donde $\sum \mathcal{Q}$ es suma directa de copias de $\mathcal{Q}$, $\mathcal{Z}(p^\infty)$es la componente p-primaria de $\mathcal{Q}/\mathcal{Z}$ y R es un grupo abeliano "reducido". Para llegar a la demostración del resultado anterior empezaremos con algunas definiciones y ejemplos, que veremos en la primera sección, después en la segunda sección revisaremos los conceptos de grupos de torsión y libres de torsión que utilizaremos en el capítulo cuatro. En la última sección demostraremos algunas proposiciones antes de demostrar el resultado del que hablamos arriba.

2.1 Preliminares

Grupos cíclicos

Un grupo G es cíclico si puede ser generado por un sólo elemento. Si tal

elemento tiene orden infinito, entonces G es isomorfo al grupo aditivo de los enteros y es llamado un grupo cíclico infinito; si tiene orden finito n, G es cíclico de orden n y es isomorfo al grupo aditivo de los enteros módulo n.

Usaremos la notación $\mathcal{Z}$ y $\mathcal{Z}_n$ respectivamente para estos dos grupos.

Sumas directas externas

Sea $\{G_i\}_{i\in I}$ una familia de grupos, donde I es cualquier conjunto Definimos la suma directa de los grupos G_i denotada:

$$\bigoplus_{i\in I} G_i := \{(a_i)_{i\in I} \in \prod_{i\in I} G_i / a_i = 0 \text{ para toda } i \in I \text{ salvo un número finito }\}$$

Es decir los elementos de $\bigoplus_{i\in I} G_i$ son "vectores" que tienen todas sus coordenadas 0 (cero) salvo un número finito.

La suma en $\bigoplus_{i\in I} G_i$ se define componente a componente es decir: $(a_i)_{i\in I} + (b_i)_{i\in I} := (a_i + b_i)_{i\in I}$ con esta operación, G resulta ser un grupo abeliano.

Unión e Intersección:

Si S y T son subgrupos de un grupo; Sabemos que $S \bigcap T$ es también un subgrupo.

Más generalmente, si $\{S_i\}_{i\in I}$ es una familia de subgrupos de G, $\bigcap_{i\in I} S_i$ es un subgrupo de G. En la unión, no ocurre lo mismo (la unión de dos subgrupos no es en general un subgrupo; de hecho $S \bigcup T$ es un subgrupo $\Leftrightarrow S \subseteq T$ ó $T \subseteq S$). El subgrupo más pequeño que contiene

a S y T (como ya vimos antes) es presisamente $S+T$ el conjunto de todos los elementos $s+t$ donde $s \in S, t \in T$. Generalicemos la idea:

Definición 2.1 . *Sea $\{S_i\}_{i\in I}$ una familia de subgrupos de G. Su unión, escrita como $\sum_{i\in I} S_i$, es el subgrupo más pequeño que contiene a $S_i \forall i \in I$.*

Proposición 2.2 . $\sum_{i\in I} S_i = \{\sum_{t=1}^{r} s_{i_t} / s_{i_t} \in S_{i_t}, r \in \mathcal{N}\}$ *(el conjunto de todas las sumas* finitas *de elementos de S_i).*

Demostración: Claramente el segundo conjunto es un subgrupo de G y contiene a $S_i \forall i \in I$, por tanto contiene a $\sum_{i\in I} S_i$; recíprocamente, $\sum_{i\in I} S_i$ contiene a todas las sumas que aparecen en el segundo conjunto; así, ambos conjuntos coinciden.

■

Sumas directas internas

Al trabajar con sumas directas se está más frecuentemente afrontado al problema de mostrar que un grupo es isomorfo a la suma directa de ciertos de sus subgrupos. Supongamos primero que el grupo G tiene subgrupos S y T tales que $S \bigcap T = \{0\}$, $S+T = G$. Entonces como ya probamos en el teorema 1.3 (productos directos finitos) G es isomorfo a la *suma directa interna* de S y T. En general, uno dice que G es la suma directa de S y T y se escribe $S \bigoplus T$.

Proposición 2.3 . *Sea* $\{S_i\}_{i\in I}$ *una familia de subgrupos de* G, *entonces* $G \approx \bigoplus_{i\in I} S_i \Leftrightarrow G = \sum_{i\in I} S_i \bigwedge \forall i \in I \ S_i \bigcap \sum_{j\neq i} S_j = \{0\}$ *(o equivalentemente a esta última condición: cada* $g \in G$ *tiene una represntación única como suma finita de elementos de los subgrupos* S_i*)*

Demostración:

($\Leftarrow$) Sea $\Psi : G \to \bigoplus_{i\in I} S_i$ tal que si $g = s_{i_1} + ... + s_{i_n}$ *entonces*

$\Psi(g) = (x_i)_{i\in I}$

donde:

$$x_{i_t} = s_{i_t},\ t = 1, ..., n$$
$$x_i = 0,\ \forall i \neq i_t \bigwedge t = 1, ..., n$$

Ψ está bien definida, pues la representación para g es única, Ψ es homomorfismo, es sobre y su núcleo es 0. $\therefore$ Ψ es isomorfismo.

($\Rightarrow$) Sea $\Phi : G \to \bigoplus_{i\in I} S_i$ un isomofismo y sea $a \in G$. Existen únicos $s_{i_t} \in S_{i_t} (t = 1, ..., n)$ tal que $\Phi(a) = (x_i)_{i\in I}$ donde

$$x_{i_t} = s_{i_t},\ t = 1, ..., n$$
$$x_i = 0,\ \forall i \neq i_t \bigwedge t = 1, ..., n$$

Sea $\overline{S_j} = \{(x_i) \in \bigoplus_{i\in I} S_i \,/\, x_j \in S_j,\ x_i = 0\ \forall i \neq j\}$,

$\overline{S_j}$ es un subgrupo de $\bigoplus_{i\in I} S_i$; $\overline{S_j} \approx S_j \bigwedge S_j \approx \Phi(S_j) < \bigoplus_{i\in I} S_i$. Así podemos pensar $\Phi(S_j)$ como $\overline{S_j}\ \forall j$. Por tanto $\forall t = 1, ..., n\ \Phi(S_{i_t}) = \{(x_i^t)\}$ donde

$$x_i^t = s_{i_t}$$
$$x_j^t = 0, \forall j \neq i_t$$

y por consiguiente

$\Phi(a) = (x_i)_{i\in I} = (x_i^1)_{i\in I} + (x_i^2)_{i\in I} + ... + (x_i^n)_{i\in I} = \Phi(s_{i_1}) + \Phi(s_{i_2}) + ... + \Phi(s_{i_n}) = \Phi(s_{i_1} + s_{i_2} + ... + s_{i_n})$ como Φ es $1-1 \Rightarrow a = s_{i_1} + s_{i_2} + ... + s_{i_n} \in \sum S_i$.

Ahora:

Sea $a \in S_{i_r} \bigcap \sum_{j\neq i_r} S_j$. Entonces: $a = s_{i_r} = s_{j_1} + s_{j_2} + ... + s_{j_m}$ con $j_1, ..., j_m \neq i_r$ $\Phi(a) = (x_i^r)_{i\in I}$ donde

$$x_{i_r}^r = s_{i_r}$$
$$x_j^r = 0 \ \forall j \neq i_r$$

y $\Phi(a) = \Phi(s_{j_1}) + \Phi(s_{j_2}) + ... + \Phi(s_{j_m}) = (x_i^{j_1})_{i\in I} + ... + (x_i^{j_m})_{i\in I} = (x_i)_{i\in I}$ donde

$$x_{j_t} = s_{j_t} \text{ con } t = 1, 2, ..., m$$
$$x_i = 0 \ \forall i \neq j_t \ (t = 1, 2, ..., m)$$

por lo tanto $x_{i_r}^r = 0$, luego $a = 0$.

■

Definición 2.4 .

1. *Sea $\{S_i\}_{i\in I}$ una familia de subgrupos de G. Si $\sum_{i\in I} S_i \cong \bigoplus_{i\in I} S_i$, diremos que los subrupos S_i* son independientes.

2. *Sea* $\{x_i\}_{i\in I} \subseteq G$. *Diremos que los* elementos x_i son independintes *si los subgrupos cíclicos que generan son independientes en el sentido de (1).*

   Escribiremos $\sum_{i\in I}(x_i)$ *para el subgrupo generado por todos los elementos*$\{x_i\}$.

La siguiente proposición nos hace notar la relación (o analogía) de este concepto y el de independencia lineal en espacios vectoriales.

Proposición 2.5 . *Una condición necesaria y suficiente para que los elementos* $x_i \in G(i \in I)$ *sean independientes es que: si una suma finita* $\sum n_i x_i = 0(n_i \in \mathcal{Z})$ *entonces cada* $n_i x_i = 0$

Demostración:

($\Rightarrow$) Por hipótesis $\sum_{i\in I}(x_i) = \bigoplus_{i\in I}(x_i)$. Supongamos que

$$\sum_{suma\, finita} n_i x_i = 0$$

para *cada* i tenemos: $n_i x_i = -\sum_{j\neq i} n_j x_j =$

$$\sum_{j\neq i}(-n_j)x_j \in (x_i)\bigcap \sum_{j\neq i}(x_j) = \{0\}$$

($\Leftarrow$) Si $x \in (x_i)\bigcap \sum_{j\neq i}(x_j)$ entonces

$$x = n_i x_i = \sum_{j\neq i,\, finita} n_j x_j \Rightarrow$$

$(-n_i)x_i + \sum_{j\neq i} n_j x_j = 0 \Rightarrow n_i x_i = 0 = n_j x_j, \forall j \neq i$

Por lo tanto, los x_i son independientes.

$$x_{i_0} = a_{i_0}{}^{1}$$
$$x_i = 0 \forall\, i \neq i_0$$

Caso 1 (a_{i_0}) es infinito.

Tomemos cualquier $n > 1$. Sea $y = (y_i)_{i\in I} \in G$. Si $y_{i_0} \neq 0$ entonces $y_{i_0} = ma_{i_0}$ y así ny es tal que $ny_{i_0} = nma_{i_0} \neq a_{i_0}$, por consiguiente $ny \neq z_0$. Si $y_{i_0} = 0$ entonces $ny_{i_0} = 0 \neq a_{i_0} \Rightarrow ny \neq z_0$.

Caso 2 (a_{i_0}) es finito.

Sea $n = \bigcirc(a_{i_0})$ y sea $y = (y_i)_{i\in I} \in G.$, entonces $ny = (ny_i)_{i\in I}$ es tal que $ny_{i_0} = n(ma_{i_0}) = m(na_{i_0}) = 0 \neq a_{i_0} = x_{i_0}$
$\Rightarrow ny \neq z_0$.

■

Racionales Módulo uno

$\mathcal{Z}$ es un subgrupo de $\mathcal{Q}$. El grupo cociente $\mathcal{Q}/\mathcal{Z}$ se conoce como los racionales módulo 1.

Observemos que todo elemento en $\mathcal{Q}/\mathcal{Z}$ tiene orden finito en efecto: Sea $r + \mathcal{Z} \in \mathcal{Q}/\mathcal{Z}$ donde $r = \frac{p}{q}; p \in \mathcal{Z}, q \in \mathcal{N}$ entonces $q(r + \mathcal{Z}) = qr + \mathcal{Z} = p + \mathcal{Z} = \mathcal{Z}$.

También observemos que $\mathcal{Q}/\mathcal{Z}$ **no** es suma directa de grupos cíclicos, en efecto:

Si $r + \mathcal{Z} \in \mathcal{Q}/\mathcal{Z}$ con $r = \frac{p}{q}; p \in \mathcal{Z}, q \in \mathcal{N}$. Sea $n \in \mathcal{N}$ entonces el

[1] Donde a_{i_0} es el generador del grupo cíclico al que pertenece

elemento $s+\mathcal{Z}$ con $s=\frac{p}{nq}$ satisface $n(s+\mathcal{Z})=n(\frac{p}{qn}+\mathcal{Z})=r+\mathcal{Z}$ y por la propsición 2.7 $\mathcal{Q}/\mathcal{Z}$ *no* puede ser suma directa de grupos cíclicos.

El Grupo $\mathcal{Z}(p^\infty)$

Hay una importante modificación de los dos ejemplos precedentes. Sea p un primo fijo. Denotemos $\mathcal{P}$ al grupo aditivo de aquellos números racionales cuyos denominadores son potencia de p es decir:

$$\mathcal{P}=\{\tfrac{m}{p^n}/n\in\mathcal{Z}^+\bigcup\{0\},m\in\mathcal{Z}\}.$$

formemos el grupo cociente $\mathcal{P}/\mathcal{Z}$ y denotémoslo por $\mathcal{Z}(p^\infty)$.

Observación:

$$\mathcal{Z}(p^\infty)=\{\tfrac{m}{p^n}+\mathcal{Z}/n\in\mathcal{Z}^+\bigcup\{0\},0\leq m<p^n\}$$

En efecto: Sea $y\in\mathcal{Z}(p^\infty)$ entonces $y=\frac{m}{p^n}+\mathcal{Z}$ con $m\in\mathcal{Z},n\geq 0$ por el algoritmo de la división $\exists\, t,r\in\mathcal{Z}$ tales que $m=p^nt+r$ con $0\leq r<p^n$; luego $\frac{m}{p^n}=t+\frac{r}{p^n}$ y así $\frac{m}{p^n}+\mathcal{Z}=(t+\frac{r}{p^n})+\mathcal{Z}=\frac{r}{p^n}+\mathcal{Z}$ donde $0\leq r<p^n$.

■

Cosideremos por ejemplo p=2: podemos escribir los elementos de $\mathcal{Z}(2^\infty)$ como $\overline{0};\overline{\frac{1}{2}};\overline{\frac{1}{4}};\overline{\frac{3}{4}};\overline{\frac{1}{8}};\overline{\frac{3}{8}};\overline{\frac{5}{8}};\overline{\frac{7}{8}};\overline{\frac{1}{16}};\overline{\frac{3}{16}}$; etc. bajo el entendido de que la adición toma lugar módulo 1. Así $\overline{\frac{1}{2}}+\overline{\frac{1}{2}}=\overline{0};\overline{\frac{1}{2}}+\overline{\frac{3}{4}}=\overline{\frac{1}{4}};\overline{\frac{3}{4}}+\overline{\frac{5}{8}}=\overline{\frac{3}{8}}$, etc. ¿cuales son los subgrupos de $\mathcal{Z}(p^\infty)$? Por ejemplo hay un subgrupo de orden p consistente de $\overline{0};\overline{\frac{1}{p}};\ldots;\overline{\frac{p-1}{p}}$; uno de orden p^2 consistente de $\overline{0};\overline{\frac{1}{p^2}};\ldots;\overline{\frac{p^2-1}{p^2}}$; y en general un subgrupo cíclico H_n de orden p^n generado por $\frac{1}{p^n}\{\overline{0};\overline{\frac{1}{p^n}};\ldots;\overline{\frac{p^n-1}{p^n}}\}$.

Afirmamos que los únicos subgrupos propios de $\mathcal{Z}(p^\infty)$ son los H_n.

En efecto: Sea H un subgrupo de $\mathcal{Z}(p^\infty)$, $H\neq\mathcal{Z}(p^\infty)$ observemos que $\mathcal{Z}(p^\infty)=\bigcup_{n=0}^{\infty}H_n$ y $H_n\subseteq H_{n+1}\forall n\in\mathcal{N}$. Como $H\neq\mathcal{Z}(p^\infty)\exists\, y\in$

$\mathcal{Z}(p^\infty)$ tal que $y \notin H$ digamos que $y = \frac{k}{p^N}$ con $(k,p) = 1, 0 < k < p^N$ y $N \geq 1$. y sea $M = min\{n/\frac{k}{p^n} \notin H$ para algún $k \in \{1,...,p^{n-1}\}$ tal que $(k,p) = 1\}$ (1)...Necesariamente $\frac{l}{p^M} \notin H \forall l \in \{1,...,p^M - 1\}$ tal que$(p,l) = 1$ pues como $\bigcirc(\frac{l}{p^M}) = \bigcirc(\frac{1}{p^M}) = p^M$ entonces si ocurriera que $\frac{l}{p^M} \in H$ para algún l como antes se tendrá que $(\frac{l}{p^M}) = (\frac{1}{p^M}) \subseteq H$ lo cual es una contradicción.

De la elección de M y de la observación (1) se sigue que $H_M \bigcap H = H_{M-1}$.

Además *no* puede existir $z \in (H_{M+1} - H_M) \bigcap H$ pues si así ocurriera, digamos $z = \frac{l}{p^{M+1}}$ con $(l,p) = 1$, $l < p^{M+1}$ entonces como $(\frac{l}{p^{M+1}}) = (\frac{1}{p^{M+1}}) = H_{M+1}$ se tendría que $H_{M+1} \subseteq H \Rightarrow H_M \subseteq H$ lo cual es absurdo. Por consiguiente $H_{M+1} \bigcap H = [(H_{M+1} - H_M) \bigcap H] \bigcup [H_M \bigcap H] = H_M \bigcap H = H_{M-1}$

y en general $H_{M+k} \bigcap H = H_{M-1} \forall k \geq 0$

$\therefore H = \bigcup_{n=0}^{\infty} H_n \bigcap H = [\bigcup_{n=0}^{M-1}(H_n \bigcap H)] \bigcup [\bigcup_{n=M}^{\infty}(H_n \bigcap H)] = [\bigcup_{n=0}^{M-1}(H_n \bigcap H)] \bigcup H_{M-1} = H_{M-1} \bigcap H \bigcup H_{M-1} = H_{M-1}$. Así hemos probado que los únicos subgrupos propios de $\mathcal{Z}(p^\infty)$ son los H_n, que son de la forma:

$$H_n = (\frac{1}{p^n}) = \{0, \frac{1}{p^n}, \frac{2}{p^n}, ..., \frac{p^n - 1}{p^n}\} \approx \mathcal{Z}_{p^n}$$

■

Como hemos visto antes, los subgrupos forman una cadena acendente que nunca termina:

$0 \subsetneq H_1 \subsetneq H_2 \subsetneq ... \subsetneq H_n \subsetneq ... \subsetneq \mathcal{Z}(p^\infty)$.

Por el contrario, toda cadena descendente de subgrupos debe ser finita.
Así, $\mathcal{Z}(p^\infty)$tiene la condición de cadena ascendente.
Ahora daremos otra relización de $\mathcal{Z}(p^\infty)$:

Proposición 2.8 . *Sea p un primo y sea $A(p^n) = \{w \in \mathbb{C} : w^{p^n} = 1\}$. Si $A = \bigcup_{n=0}^{\infty} A(p^n)$ entonces A es un grupo bajo la multiplicación ordinaria en $\mathbb{C}$ y es isomorfo a $\mathcal{Z}(p^\infty)$*

Demostración: Sean $w_1, w_2 \in A$. Entonces existen $n_1, n_2 \in \mathcal{N} \bigcup \{0\}$ tales que $w_1^{p^{n_1}} = w_2^{p^{n_2}} = 1$.
Si $n = max\{n_1, n_2\}$ entonces:
$(w_1 w_2)^{p^n} = (w_1)^{p^n}(w_2)^{p^n} = 1 \cdot 1 = 1$.
Claramente, si $w^{p^n} = 1$ entonces $(w^{-1})^{p^n} = (w^{p^n})^{-1} = 1$.
Ahora observemos que para cada $n \in \mathcal{N}$, $A(p^n)$ es un grupo cíclico, de hecho:
$A(p^n) = (cos\frac{2\pi}{p^n} + \imath sen\frac{2\pi}{p^n}) = (e^{\frac{2\pi\imath}{p^n}})$
Definamos $\psi : \bigcup_{n=0}^{\infty} A(p^n) \to \mathcal{Z}(p^\infty)$
como sigue: $e^{\frac{2k\pi\imath}{p^n}} \mapsto \frac{\overline{k}}{p^n}$; ψ está bien definida.
Observemos que $\psi(e^{\frac{2k_1\pi\imath}{p^n}} e^{\frac{2k_2\pi\imath}{p^n}}) = \psi(e^{\frac{2(k_1+k_2)\pi\imath}{p^n}}) = \frac{\overline{k_1+k_2}}{p^n} = \frac{\overline{k_1}}{p^n} + \frac{\overline{k_2}}{p^n}$
Claramente ψ es sobre y es inyectiva ya que $\psi(e^{\frac{2k\pi\imath}{p^n}}) = 0 \Rightarrow \frac{\overline{k}}{p^n} = 0$
$\Rightarrow \frac{k}{p^n} \in \mathcal{Z} \Rightarrow e^{2\frac{k}{p^n}\pi\imath} = 1$

■

2.2 Grupos de Torsión

En esta sección reduciremos el problema del estudio de grupos, al de de grupos torsión y grupos libres de toesión. También demostraremos

que todo grupo de torsión es suma directa de grupos primarios.

Definición 2.9 . *Diremos que un grupo abeliano es un* grupo de torsión *si todos sus elementos tienen orden finito.*

Por ejemplo $\mathcal{Q}/\mathcal{Z}$ y $\mathcal{Z}(p^\infty)$ y todo grupo finito es un grupo de torsión.

Ejemplo 2.1 . Sea $G = \{cos(\frac{2k\pi}{3^n}) + isen(\frac{2k\pi}{3^n}) \ / \ n \in \mathcal{N} - \{0\};\ k \in \mathcal{Z}\}$, donde la operación es la multiplicación usual en $\mathcal{C}$. Así G es infinito; pero todo element de G tiene orden finito pues $(cos(\frac{2k\pi}{3^n}) + isen(\frac{2k\pi}{3^n}))^{3^n} = cos(2k\pi)+isen(2k\pi) = 1$, de hecho $G = \{w \in \mathcal{C} \ / \ w^{3^n}\}$.

Definición 2.10 . *Diremos que un grupo es* libre de torsión *si todos sus elementos (excepto el 0) tienen orden infinito.*

Por ejemplo $\mathcal{Z}$ y $\mathcal{Q}$ son grupos libres de torsión.

Ejemplo 2.2 . Sea $G = \{2^r \ / \ r \in \mathcal{Z}\}$ con la multiplicación usual de $\mathcal{Q}$. Así ningún elemento *no* identidad tiene orden finito ya que:
$(2^r)^n = 1 \Leftrightarrow 2^{rn} \Leftrightarrow r = 0$ ó $n = 0$

Proposición 2.11 . *Sea G un grupo abeliano y sea T el conjunto de todos los elmentos en G que tienen orden finito. Entonces, T es un subgrupo de torsión y G/T es libre de torsión. T es llamado el subgrupo de torsión de G (a veces lo denotaremos por tG).*

Demostración:

• T es un subgrupo de torsión G:

Sean $a, b \in T \Rightarrow \exists\, \mathcal{N}_a, n_b \in \mathcal{Z}$ tales que $n_a a = 1$ y $n_b b = 1$.

Ahora, $(n_a n_b)(ab) = (n_a n_b)ab = 0 \Rightarrow ab \in T$

y $-n_a(-a) = n_a a = 0 \Rightarrow -a \in T$

$\therefore T$ es un subgrupo de torsión de G.

• G/T es libre de torsión:

Si $z \in G/T$ digamos $z = g + T$. Entonces si $n \in \mathcal{N}$, entonces $nz = 0 \Leftrightarrow$ $ng + T = T \Leftrightarrow ng \in T \Leftrightarrow \exists m \in \mathcal{N}$ mínimo tal que $m(ng) = 0 \Leftrightarrow g \in$ $T \Leftrightarrow z = 0$

■

Definición 2.12 . *Diremos que un grupo de torsión es* primario *si existe un primo p tal que todo elemento tiene orden una potencia de p.*

El estudio de los grupos de torsión es reducido al estudio de los grupos primarios por el suiguiente teorema:

Teorema 2.13 . *Todo grupo de torsión G es una suma directa de grupos primarios*

Demostración: Para cada primo p consideremos el conjunto $G_p \subseteq G$ cuyos elementos tienen orden una potencia de p. G_p es un subgrupo de G y además es primario, probaremos que $G = \bigoplus_p G_p$.

1. Sea $x \in G$ tal que $\bigcirc(x) = n = p_1^{r_1}...p_k^{r_k}$ donde los p_i son primos distintos y $r_i \geq 1 \, \forall \, i$.

   Escribamos $n_i = n/p_i^{r_i} \, \forall \, i$; así $(n_1, ..., n_k) = 1$ y por tanto $\exists$ a_1, ..., $a_k \in \mathcal{Z}$ tal que $a_1 n_1 + ... + a_k n_k = 1$

   luego

   $x = a_1 n_1 x + a_2 n_2 x + ... + a_k n_k x$

   y como

   $p_i^{r_i}(a_i n_i x) = a_i(nx) = 0 \Longrightarrow a_i n_i x \in G_{p_i}$

   $\therefore$ G es la unión de los subgrupos G_p.

2. Supongamos que $x = y_1 + ... + y_k = z_1 + ... + z_k$ tal que $y_i, z_i \in G_{p_i} \, \forall \, i = 1, ..., k$. Entonces $y_1 - z_1 = (z_2 + ... + z_k) - (y_2 + ... + y_k)$; pero $y_1 - z_1$ tiene orden una potencia de p_1 y el lado derecho tiene un orden producto de potencia de $p_2, ..., p_k$. Esto sólo es posible si $y_1 - z_1 = 0$. Análogamente se prueba que $y_i - z_i = 0 \, \forall \, i = 2, ..., k$.

■

De hecho : Hay una *única* manera de expresar a un grupo de torsión como una suma directa de subgrupos primarios, uno por cada primo p.
En efecto :
Ya que si $G = \bigoplus H_i$ donde por cada primo p hay un solo H_i p-primario entonces $H_i = G_p$ (pues siempre es cierto $H_i \subseteq G_p$ si $x \in G_p$ forzosamente $x \in H_i$).
Por consiguiente, la descomposición es única no sólo salvo isomorfismos; los subgrupos son subgrupos únicos. Damos ahora dos ilustraciones del

teorema 2.13:

Ejemplo 2.3 . Consideremos el grupo cíclico $\mathcal{Z}_n$ donde $n = p_i^{r_1}...p_k^{r_k}$ donde p_i son primos distintos y $r_i \geq 1 \, \forall i$ se tiene entonces que $\mathcal{Z}_n = \mathcal{Z}_{p_i^{r_i}} \oplus ... \oplus \mathcal{Z}_{p_k^{r_k}}$.

Ejemplo 2.4 . Sea G el grupo aditivo de los racionales módulo 1, es decir, $G = \mathcal{Q}/\mathcal{Z}$. Afirmamos que la componente p primaria para el primo p, G_p, es presisamente $\mathcal{Z}(p^\infty)$.

En efecto:
Claramente $\mathcal{Z}(p^\infty) \subseteq G_p$. Ahora, sea $\xi \in G_p$ tal que $\xi = \frac{m}{n} + \mathcal{Z}$ con $0 \leq m < n$, $(m,n) = 1$.
Existe $k \geq 0$ tal que $\bar{0} = p^k\xi = \frac{mp^k}{n} + \mathcal{Z}$, luego $\frac{mp^k}{n} \in \mathcal{Z}$ y esto implica que $n|p^k$ pues $(m,n) = 1$. Así $n = p^l$ con $l \leq k$ y por tanto $\xi = \frac{m}{p^l} + \mathcal{Z} \in \mathcal{Z}(p^\infty)$. Por consiguiente, $\mathcal{Q}/\mathcal{Z}$ es suma directa de *todos* los subgrupos $\mathcal{Z}(p^\infty)$.

■

2.3 Grupos Divisibles

Definición 2.14 . *Sea $n \in \mathcal{Z}, G$ un grupo abeliano y $x \in G$. Diremos que x es divisible por n, si existe un elemento $y \in G$ tal que $ny = x$.*

Ejemplo 2.5 . El elemento 0 es divisible por cualquier entero.

Ejemplo 2.6 . Si $\bigcirc(x) = m$ entonces x es divisible por cualquier entero primo relativo a m. En efecto: si $(k, m) = 1$, existen enteros λ, μ tal que $k\lambda + m\mu = 1$ por consiguiente $(k\lambda + m\mu)x = x \Rightarrow k\lambda x + m\mu x = x \Rightarrow k\lambda x = x \Rightarrow k\underbrace{(\lambda x)}_{\in G} = x$.

Ejemplo 2.7 . En el grupo aditivo de números racionales, cada elemento es divisble por cada entero no cero ($x = \frac{p}{q}, n \in \mathcal{Z} - \{0\}$. $n(\frac{p}{nq}) = \frac{p}{q}$).

Definición 2.15 . *Un grupo abeliano G es* **divisible** *si para cada $x \in G$ y cada entero (no cero) n existe un elemento $y \in G$ tal que $ny = x$.*
Equivalentemente, G es divisible si $G = nG \ \forall n \in \mathcal{Z} - \{0\}$

Observaciones

1. Un grupo cíclico *no* es divisible.
   Veremos que : $\exists\, x_0 \in G$ y $\exists\, n_0 \in \mathcal{Z}$ tal que $\forall\, y \in G\, n_0 y \neq x_0$
   En efecto:
   si G es finito, entonces $G =< a >$, $n_0 = \bigcirc(a) = |G|$, $x_0 = a$ entonces $\forall y \in G\ n_0 y = n_0 ma = m(n_0 a) = 0 \neq x_0$. Si G es infinito, tomamos n_0 cualquier entero no cero.

2. Una suma directa de grupos cíclicos *no* es divisible (esto ya lo probamos antes corolario 2.6).

3. Una suma directa de grupos es divisible $\Leftrightarrow$ cada sumando es divisible.

Demostración: Supongamos que

$$G = \bigoplus_{i \in I} G_i$$

($\Rightarrow$) Sea $a_i \in G_i$ y $n \in \mathcal{Z}$. si $x = (x_j)_{j \in I}$ tal que $x_j = 0 \forall j \neq i, x_i = a_i$. Entonces $\exists y = (y_j)_{j \in I} \in G$ tal que $ny = x$, luego $ny_i = a_i$.

($\Leftarrow$) Sea $x = (x_i)_{i \in I} \in G$ y $n \in \mathcal{Z}$. Para cada $i \in I$ $\exists y_i \in G_i$ tal que $ny_i = x_i$; así $y = (y_i)_{i \in I}$ es tal que $ny = x$.

4. La imagen homomórfica de un grupo divisible es divisible.

   Demostración Sea G divisible, H un grupo y $\Phi : G \to H$ un homomorfismo sobre. Sea $y \in H, n \in \mathcal{Z}$. Existe $x \in G$ tal que $\Phi(x) = y$. Para este x existe $x_0 \in G$ tal que $nx_0 = x$. Sea $y_0 = \Phi(x_0)$ entonces $ny_0 = n\Phi(x_0) = \Phi(nx_0) = \Phi(x) = y$.

5. El grupo de racionales módulo uno es divisible.

   Demostración Sea $\Pi : \mathcal{Q} \to \mathcal{Q}/\mathcal{Z}$ la proyección canónica. Como $\mathcal{Q}$ es divisible y Π es epimorfismo entonces $\mathcal{Q}/\mathcal{Z}$ es divisible (por 4).

6. El grupo $\mathcal{Z}(p^\infty)$ es divisible:

   Este hecho *no* es aparente a partir de la definición de $\mathcal{Z}(p^\infty)$ como $\mathcal{P}/\mathcal{Z}$ puesto que para p primo

$$\mathcal{P} = \{\frac{m}{p^n} : m \in \mathcal{Z}, n \in \mathcal{Z}^+ \cup \{0\}\}$$

no es divisible. (Esto se tiene por lo siguiente: sea $x = \frac{1}{p}$, $p > 2$, $n = 2$; supongamos que $\exists y = \frac{m}{p^k} \in P$ con $(m,p) = 1$ tal que $2\frac{m}{p^k} = \frac{1}{p}$. Entonces $\frac{2m}{p^{k-1}} = 1$. Si $k \geq 2$ entonces $2m = p^{k-1}$ lo cual es imposible pues $(2,p) = (m,p) = 1$. Si $k = 1$ entonces $2m = 1 \Rightarrow m = \frac{1}{2}$ contradicción pues $m \in \mathcal{Z}$).

Como vimos en el ejemplo 2.4 (de la pagina 47) que $\mathcal{Z}(p^\infty)$ es un sumando directo de los racionales módulo uno entonces por (3) $\mathcal{Z}(p^\infty)$ es divisible.

Demos otro argumento más directo:

Como $\mathcal{Z}(p^\infty)$ es primario, entonces por el ejemplo (2) todos sus elementos son divisibles por cualquier entero primo relativo a p. Sea $x = \frac{m}{p^s}$ con $(m,p) = 1, s \geq 0$ sea $n = p_1^{r_1}...p_k^{r_k}$ con $r_i \geq 1 \; \forall i = 1,2,...,k$. si $p_i \neq p \; \forall i \Rightarrow (n,p) = (n,p^s) = 1$ y así x es divisible por n (por el comentario inicial).

Si $\exists i$ tal que $p_i = p$, digamos $p_1 = p$ entonces el entero $\frac{n}{p_1^{r_1}}$ es primo relativo con p y así $\exists y \in \mathcal{Z}(p^\infty)$ tal que $(\frac{n}{p_1^{r_1}})y = x$ así $n(\frac{y}{p_1^{r_1}}) = x$ con $(\frac{y}{p_1^{r_1}}) \in \mathcal{Z}(p^\infty)$. $\therefore \mathcal{Z}(p^\infty)$ es divisible.

■

Definición 2.16 . *Diremos que un subgrupo H de G es divisible si para cada $h \in H$ y cada $n \in \mathcal{Z} - \{0\}$, $\exists\, h_1 \in H$ tal que $nh_1 = h$.*

Teorema 2.17 . *Un subgrupo divisible de un grupo abeliano es un sumando directo.*

Demostración: Sea H un subgrupo divisible de G. Nuestra tarea es encontrar un subgrupo K de G con $H \bigcap K = \{0\}$ y $H + K = G$. La prueba del teorema utilizará el lema de Zorn.

Sea $\mathcal{F} = \{L \leq G : H \bigcap L = \{0\}\}$.

$\mathcal{F}$ es no vacío pues al menos $\{0\} \in \mathcal{F}$.

Nos gustaría conseguir un L tan grande como sea posible; buscaremos por tanto un elemento máximal en $\mathcal{F}$. Ordenemos parcialmente $\mathcal{F}$ por inclusión. Para usar el lema de Zorn tenemos que verificar que toda cadena en $\mathcal{F}$ tíene una mínima cota superior.

Supongamos que $\{L_i\}_i$ es una cadena en $\mathcal{F}$.

Para conseguir la mínima cota superior simplemente tomamos la unión de los L_i: Sea $M = \bigcup_i L_i$ Necesitamos verificar tres cosas:

- **M es un subgrupo.**

  Sean $x, y \in M$; existen i, j tal que $x \in L_i, y \in L_j$ y como $L_i \subseteq L_j$ ó $L_j \subset L_i$ entonces $x - y \in L_j$ ó $x - y \in L_i \Rightarrow x - y \in M$.

- $H \bigcap M = \{0\}$.

  $H \bigcap M = H \bigcap (\bigcup_i L_i) = \bigcup_i (H \bigcap L_i) = \{0\}$

- **M es la mínima cota superior de $\{L_i\}_i$.**

  Es claro que $L_i \subseteq M \ \forall i$ y si $N \supseteq L_i \ \forall i \in I \Rightarrow N \supseteq M$.

Así por el lema de Zorn $\mathcal{F}$ tiene un elemento maxímal K. Así K es un subgrupo de G tal que $K \bigcap H = \{0\}$. Probemos que $G = H + K$. Supongamos lo contrario. Por consiguiente, existe un elemento $x \in G$ tal que $x \notin H + K$. Necesariamente $x \notin K$ (pues si $x \in K \Rightarrow x = 0 + x \in H + K$). Sea K' el subgrupo generado por K y $\{x\}$. $K' \supsetneq K$ y de hecho

$K\prime = \{k + nx/k \in K, n \in \mathcal{Z}\}$. Por la maximalidad de K tenemos que $H \bigcap K\prime \neq \{0\}$; por tanto, existe un elemento $h \in H \bigcap K\prime, h \neq 0$, digamos

$h = k + nx$ $(*)$

De la ecuación $(*)$ se tiene que $nx \in H+K$. En otras palabras, cada vez que tomemos un $g \notin H + K$ es decir un $\bar{g} = g + (H + K) \neq 0$ podemos encontrar $n \in \mathcal{Z}$ tal que $ng \in H + K$; por consiguiente $n\bar{g} = \bar{0}$ y así $G/(H + K)$ es un grupo de torsión.

Supongamos que n es el más pequeño entero positivo tal que $nx \in H + K$ (por consiguiente $n > 1$). Sea p un primo tal que $p|n$ y sea $y = (\frac{n}{p})x$. Como $\frac{n}{p} < n$ entonces $y \notin H + K$ (por elección de n). Pero :

$$py = nx = h - k$$

Puesto que H es divisible $\exists h_1 \in H$ tal que $h = ph_1$ sea $z = y - h_1$, entonces $z \notin H + K$ (por que si $z \in H + K$ entonces $y \in H + K$ contradicción) pero $pz = py - ph_1 = (h - k) - h = -k \in K$

Como $z \notin H + K$ podemos repetir el argumento de antes y formemos un subgrupo $K\prime\prime$ generado por $K \bigcup \{z\}$ y de nuevo por la maximalidad de $K, K\prime\prime \bigcap H \neq \{0\}$. Así, existe un elemento $h_2 \in K\prime\prime \bigcap H$ tal que $h_2 \neq 0$ es decir,

$$(**)...h_2 = k_2 + mz \ \textit{donde} \ h_2 \neq 0, k_2 \in K, m \in \mathcal{Z}$$

No puede ocurrir que m sea múltiplo de p porque de ser así, el lado derecho de $(**)$ estaría en K y el lado izquierdo en H, luego $h_2 \in (H \bigcap K) - \{0\}$ contradicción.

Por consiguiente, $(m,p) = 1$, luego existen enteros a, b tal que $am + bp = 1$. Entonces, como $amz = ah_2 - ak_2 \in H + K$, se tiene que $z = amz + bpz \in H + K$ lo cual es una contradicción.
Por tanto, $G = H + K$.

■

Teorema 2.18 . *Cualquier grupo abeliano G tiene una única representación como suma directa de M y N donde M es un grupo divisible que contiene a cualquier otro subgrupo divisible de G, y N no contiene a ningún subgrupo divisible.*

Demostración: Sea $\mathcal{C} = \{H_\alpha \,|\, H_\alpha$ es un subgrupo divisible de $G\}$ y sea $M = [\bigcup \mathcal{C}] = \{x_{\alpha_1} + ... + x_{\alpha_k} / x_{\alpha_i} \in H_{\alpha_i} \; \forall i \in \mathcal{N}\}$, ahora, dado $n \in \mathcal{N}$, $\exists y_{\alpha_i} \in H_{\alpha_i}$ tal que $ny_{\alpha_i} = x_{\alpha_i}$, por tanto $x_{\alpha_1} + ... + x_{\alpha_k} = n\underbrace{(y_{\alpha_1} + ... + y_{\alpha_k})}_{\in M}$ es decir M es divisible.
Claramente M es máximo (por construcción) y es el único con tal propiedad.
Por el teorema 2.17, M es un sumando directo de G Así $G = M \bigoplus N$. Ahora, el sumando N no puede tener subgrupos divisibles distintos de 0 pues de ser así, éstos estarían contenidos en M y así $N \bigcap M \neq 0$ lo cual es imposible.

■

Definición 2.19 . *Un grupo abeliano es* REDUCIDO *si no contiene ningún subgrupo divisible no cero.*

Así, el teorema 2.18 establece que todo grupo abeliano G es la suma directa de un subgrupo divisible maximal de G y un grupo reducido.

Teorema 2.20 . *Un grupo abeliano divisible es suma directa de grupos, cada uno de ellos isomorfo o bien, al grupo aditivo de los números racionales, o bien a $\mathcal{Z}(p^\infty)$ (para varios primos p).*

Demostración: Sea G el grupo y sea T su subgrupo de torsión. T es un subgrupo divisible de G ya que si $n \in \mathcal{Z}, x \in T$ entonces existe $y \in G$ tal que $ny = x$. Como $x \in T$, $\exists m \in \mathcal{N}$ tal que $mx = 0$ y así $mny = 0 \Rightarrow y \in T$.

Por el teorema 2.17, $G = T \bigoplus F$ donde $F \approx G/T$ y por tanto, F es libre de torsión y también divisible (por ser imagen homomórfica de un grupo divisible).

Ahora estudiaremos T y F separadamente. Relacionaremos la discución acerca de F con la teoría de espacios vectoriales.

Sea $x \in F$ y $n \in \mathcal{Z} - \{0\}$: Como F es divisible y libre de torsión **existe un único $y \in F$ tal que** $ny = x$ (este y es único pues si $ny\prime = ny = x$ con $y\prime \in F$ entonces $n(y\prime - y) = 0 \Rightarrow (y\prime - y)$ tiene orden finito $\Rightarrow y\prime - y = 0$ pues F es libre de torsión, así $y\prime = y$.)

Por tanto podemos dar un significado único a la expresión $(\frac{1}{n})x$ y por consiguiente, también podemos dar un significado único a rx donde $r \in \mathcal{Q}$. Así podemos definir:

$\mathcal{Q} \times F \longrightarrow F$ tal que $(r, x) = r \cdot x$

Es fácil verificar que ésta función verifica las propiedades definitorias de un producto por un escalar, por ejemplo veamos que:

$\frac{m}{n}(x_1+x_2) = \frac{m}{n}x_1+\frac{m}{n}x_2$: existe un **único** $y \in F$ tal que $y = \frac{m}{n}(x_1+x_2)$.

Por otro lado, existen **únicos** $y_1, y_2 \in F$ tal que $y_1 = \frac{m}{n}x_1$, $y_2 = \frac{m}{n}x_2$, así $ny_1 = mx_1$, $ny_2 = mx_2$, luego $ny_1 + ny_2 = m(x_2 + x_1)$, es decir $n(y_1 + y_2) = m(x_2 + x_1) \Rightarrow y = y_1 + y_2 \Rightarrow$

$$\frac{m}{n}(x_1 + x_2) = \frac{m}{n}x_1 + \frac{m}{n}x_2$$

Por consiguiente, F es un espacio vectorial sobre el campo $\mathcal{Q}$. Pero cualquier espacio vectorial tiene una base, digamos que $\{x_\alpha\}_{\alpha \in I}$ es base de F. Así

$$F = \bigoplus_{\alpha \in I} < x_\alpha >$$

donde $< x_\alpha >= \{qx_\alpha / q \in \mathcal{Q}\}$. Traducido esto en terminos de grupos, tenemos que F es una suma directa de grupos abelianos cada uno de los cuales es isomorfo a $\mathcal{Q}$.

Pongamos ahora nuestra atención en el grupo de torsión divisible T. Como T es de torsión, por el teorema 2.13 resulta que T es suma directa de grupos primarios y puesto que T es divisible entonces cada uno de los sumandos será divisible. Por tanto, no hay pérdida de generalidad en suponer que el propio T es primario, digamos que es p-primario. **Probaremos que T es una suma directa de grupos isomorfos a $\mathcal{Z}(p^\infty)$.**

Para ello, consideremos **los subgrupos de T que son isomorfos a $\mathcal{Z}(p^\infty)$.** Veamos que esta familia es realmente no vacía: (*)

Puesto que T es p-primario y $T \neq 0$[2], podemos encontrar un elemento $x_1 \in T$ tal que $\bigcirc(x_1) = p$. Como T es divisible existe una sucesión de elementos $x_2, x_3, \ldots \in T$ tales que $px_2 = x_1, px_3 = x_2, \ldots$ y en

[2]Si $T = 0$ la prueba del teorema ya terminó.

general, $px_{i+1} = x_i \; \forall i \geq 1$ (observemos que x_i tiene orden p^i). Sea $N = [\bigcup_{i \in \mathcal{N}} x_i]$. Ahora, definimos:

$\Psi : N \longrightarrow \mathcal{Z}(p^\infty)$ tal que $x_i \rightsquigarrow \frac{1}{p^i}$

Entonces Ψ es un isomorfismo y así T contiene un subgrupo N que es isomorfo a $\mathcal{Z}(p^\infty)$. Por lo tanto la familia de subgrupos de T isomorfos a $\mathcal{Z}(p^\infty)$ es no vacía.

Nuestro objetivo es expresar a T como suma directa de tales subgrupos, por tanto consideremos

$\mathcal{B} =$ familia cuyos elementos son todos los conjuntos indepedientes[3] de subgrupos isomorfos a $\mathcal{Z}(p^\infty)$

Así, cada elemento de $\mathcal{B}$ es un conjunto independiente de subgrupos, es decir, es un conjunto de conjuntos y por tanto ¡ $\mathcal{B}$ es un conjunto de conjuntos de conjuntos! Ahora, ordenemos $\mathcal{B}$ parcialmente por inclución. Sea $\{C_j\}_{j \in J}$ una cadena en $\mathcal{B}$, digamos que $C_j = \{A_{ji}\}_i$ con C_j independiente y $A_{ji} \approx \mathcal{Z}(p^\infty)$. Sea $\mathcal{C} = \bigcup_{j \in J} C_j$; veamos que $\mathcal{C} \in \mathcal{B}$, para éllo, hay que ver que

$$[\bigcup_{A_{ij} \in \mathcal{C}} A_{ij}] = \bigoplus_{A_{ij} \in \mathcal{C}} A_{ij}$$

[3]Recordemos que:

1. Si $\{S_i\}_{i \in I}$ es una familia de subgrupos de G.Y si $\sum_{i \in I} S_i \cong \bigoplus_{i \in I} S_i$, entonces los subrupos S_i **son independientes**.

2. Si $\{x_i\}_{i \in I} \subseteq G$. Los **elementos** x_i **son independintes** si los subgrupos cíclicos que generan son independientes en el sentido de (1).

Sea $x \in [\bigcup_{A_{ij} \in \mathcal{C}} A_{ij}]$ tal que $x = x_{i_1,j_1} + \ldots + x_{i_k,j_k} = 0$ con $x_{i_1,j_1} \in A_{i_1,j_1}; \cdots; x_{i_k,j_k} \in A_{i_k,j_k}$. Pero $A_{i_1,j_1} \in C_{j_1}; \cdots; A_{i_k,j_k} \in C_{j_k}$ Luego $\exists j \in \{j_1, \cdots, j_k\}$ tal que $C_{j_s} \subseteq C_j \forall s = 1, \cdots, k \therefore \{A_{i_1,j_1}, \cdots, A_{i_k,j_k}\} \subseteq C_j$ y como C_j es independiente entonces $x_{i_1 j_1} = \ldots = x_{i_k j_k} = 0$ Por tanto, $\mathcal{C}$ es un conjunto independiente de subgrupos isomorfos a $\mathcal{Z}(p^\infty)$. Además, es claro que $\mathcal{C}$ es la minima cota superior de la cadena $\{C_j\}_{j \in J}$. Ahora por el lema de Zorn, existe un conjunto **independiente maximal** de subgrupos isomorfos a $\mathcal{Z}(p^\infty)$, digamos $\{S_i\}_{i \in I}$. Sea

$$S = [\bigcup_{i \in I} S_i] = \bigoplus_{i \in I} S_i$$

La prueba estara concluida si probamos que $S = T$ veamos: por un lado, se tiene que S es divisible ya que $S_i \approx \mathcal{Z}(p^\infty)$ y $\mathcal{Z}(p^\infty)$ es divisible. Por el teorema 2.17 se tiene que $T = S \bigoplus R$. Queremos probar que $R = 0$. Si fuese $R \neq 0$, escojamos en R un elemento x_1 de orden p (ésto podemos hacerlo pues T es p-primario).

Como T es divisible, entonces R es divisible y por consiguiente, razonando como (*) podemos encontrar un subgrupo L de R con $L \approx \mathcal{Z}(p^\infty)$. Ahora consideremos $\mathcal{F} = \{S_i\}_i \bigcup \{L\}$. Entonces $\mathcal{F}$ es un conjunto independiente de subgrupos isomorfos a $\mathcal{Z}(p^\infty)$ tal que $\mathcal{F} \supsetneq \{S_i\}_i$, lo cual contradice la maximalidad de $\{S_i\}_i$. Por tanto $R = 0$ y así $S = T$.

■

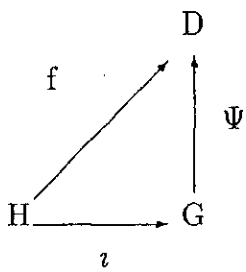
Capítulo 3

Grupos Divisibles

Después de ver la importancia que tienen los grupos divisibles, en este capítulo demostraremos seis proposiciones que nos darán una mejor idea de como son estos, los resultados de mayor importancia de este capítulo están en la segunda sección.

3.1 Tres Proposiciones Preliminares

Proposición 3.1 . *Sea G un grupo, H un subgrupo, D un grupo divisible. Sea $f : H \longrightarrow D$ un homomorfismo. Entonces f puede ser extendido a un homorfismo G en D. Es decir que existe un homomorfismo Ψ de G sobre D tal que el siguiente diagrama conmuta:*



(Es decir $f = \Psi \circ i$, i es la inclusión)

Demostración: Consideremos el conjunto:

$\mathcal{S} = \{(s,h) : S$ es subgrupo de G tal que $H \subseteq S$ y $h : S \longrightarrow D$ es una extensión de $f\}$

$\mathcal{S} \neq \emptyset$ ya que $(H,f) \in \mathcal{S}$. Definimos el siguiente orden "$<$" en $\mathcal{S}$:

$(S_i,h_i) < (S_j,h_j) \Leftrightarrow S_i \subseteq S_j$ y h_j es una extensión de h_i. Entonces $<$ resulta ser un orden parcial en $\mathcal{S}$. Ahora, sea $\{(S_\alpha,h_\alpha)\}_\alpha$ una cadena en $\mathcal{S}$ y definamos $S_0 = \bigcup_\alpha S_\alpha$ y si $s \in S_0$ entonces $\exists\, \alpha$ tal que $s \in S_\alpha$, así, también podemos definir $h_0(s) = h_\alpha(s)$. h_0 está bien definida pues si $s \in S_{\alpha_1}, s \in S_{\alpha_2}$ entonces $S_{\alpha_1} \subseteq S_{\alpha_2}$ o bien $S_{\alpha_2} \subseteq S_{\alpha_1}$, digamos $S_{\alpha_1} \subseteq S_{\alpha_2}$, luego $h_{\alpha_2}(s) = h_{\alpha_1}(s)$ pues $h_{\alpha_2}|_{S_{\alpha_1}} = h_{\alpha_1}$.

El elemento $(S_0,h_0) \in \mathcal{S}$ ya que por una parte S_0 es un subgrupo de G que contiene a H y por otro lado, si $x \in H$ entonces como $H \subseteq S_\alpha$ $\forall\ \alpha$ tendremos que $h_0(x) = h_\alpha(x)\,\forall\,\alpha$ (recordemos que todos los $h_\alpha(x)$ coinciden), y por tanto, h_0 es una extensión de h_α $\forall\alpha$, y por tanto una extensión de f.

Además (S_0,h_0) es la mínima cota superior de la cadena $\{(S_\alpha,h_\alpha)\}_\alpha$ ya que por un lado, S_0 contiene a S_α $\forall\alpha$ y si $x \in S_\alpha$ entonces por definición $h_0(x) = h_\alpha(x)$, es decir, $h_0/S_\alpha = h_\alpha$; por tanto

$(S_0,h_0) > (S_\alpha,h_\alpha)$ $\forall\alpha$.

Por otro lado si $(S\prime,h\prime) > (S_\alpha,h_\alpha)$ $\forall\alpha$ $S\prime \supseteq S_0$ y como $h\prime/S_\alpha = h_\alpha$ $\forall\alpha$ entonces $h\prime/S_0 = h_0$ es decir:

$(S\prime,h\prime) > (S_0,h_0)$. Por el Lema de Zorn, existe un elemento maximal $(M,\Psi) \in \mathcal{S}$.

Mostraremos que $M = G$

En efecto, supongamos que existe un elemento $x \in G$ tal que $x \notin M$.

Sea $M_1 = M + [x]$, claramente, $M \neq M_1$, así, que será suficiente extender Ψ a M_1 para tener una contradicción.

Caso I: $M \bigcap [x] \neq 0$

Sea k el entero positivo más pequeño tal que $kx \in M$. Por consiguiente, si $y \in M_1$ entonces $y = m + sx$ con $0 \leq s < k$ y esta expresión es única (ya que si $m + sx = m\prime + s\prime x$ con $0 \leq s < s\prime < k$ entonces $(s\prime - s)x = m - m\prime \in M$ y $0 < s\prime - s < k$ lo cual es una contradicción, por la elección de k). Sea $z = kx$. Puesto que $z \in M$ entonces $\Psi(z)$ está definido. Como $\Psi(z) \in D$ y D es divisible, existe $\xi \in D$ tal que $k\xi = \Psi(z)$ $(= \Psi(kx))$. Definamos $F : M_1 \rightarrow D$ por $F(m + sx) = \Psi(m) + s\xi$,

$$\begin{aligned} \text{Entoces } F((m_1 + m_2) + (s_1 + s_2)x) &= \Psi(m_1 + m_2) + (s_1 + s_2)\xi \\ (\text{si } s_1 + s_2 < k) \qquad &= [\Psi(m_1) + s_1\xi] + [\Psi(m_2) + s_2\xi] \\ &= F(m_1 + s_1x) + F(m_2 + s_2x). \end{aligned}$$

Si $s_1 + s_2 \geq k$ entonces $s_1 + s_2 = k + s$ con $0 \leq s < k \Rightarrow$

$$\begin{aligned} F((m_1 + m_2) + (s_1 + s_2)x) &= F((m_1 + m_2 + kx) + sx) \\ &= \Psi(m_1 + m_2 + kx) + s\xi \\ &= \Psi(m_1) + \Psi(m_2) + \Psi(kx) + s\xi \\ &= \Psi(m_1) + \Psi(m_2) + k\xi + s\xi \\ &= \Psi(m_1) + \Psi(m_2) + (k + s)\xi \\ &= \Psi(m_1) + \Psi(m_2) + (s_1 + s_2)\xi \end{aligned}$$

$$= (\Psi(m_1) + s_1\xi) + (\Psi(m_2) + s_2\xi)$$
$$= F(m_1 + s_1x) + F(m_2 + s_2x)$$

Así F es un homomorfismo y claramente extiende a Ψ. Contradicción.

Caso II: $M \bigcap [x] = 0$

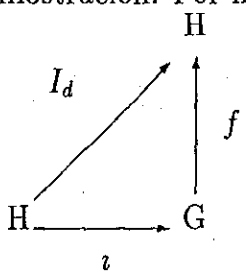
Entonces $M_1 = M \bigoplus [x]$. Definamos en este caso $F : M_1 \to D$ tal que $F(m+\lambda x) = \Psi(m)$. F está bien definida pues la expresión para $m+\lambda x$ es única, F es homomorfismo y claramente $F|_M = \Psi$, es decir, F es extensión de Ψ. Por lo tanto, $(M_1, F) > (M, \Psi)$ y $(M_1, F) \neq (M, \Psi)$ lo cual es una contradicción.

Así, $M = G$

■

Proposición 3.2 . *Sea G un grupo, H un subgrupo y supongamos que el homomorfismo identidad de H sobre si mismo puede ser extendido a un homomorfismo de G sobre H. Entonces H es un sumando directo de G.*

Demostración: Por hipótesis, el siguiente diagrama conmuta:



donde i es la inclusión y
f la extensión de $I_d : H \longrightarrow H$.
Sea $K = Ker(f)$.
Mostraremos que: $G = H \bigoplus K$.

1. Sea $x \in G$, entonces $x = (x - f(x)) + f(x)$, $f(x) \in H$
   y $f(x - f(x)) = f(x) - f(f(x)) =^1 f(x) - f(x) = 0$, es decir,
   $x - f(x) \in K \Rightarrow G = H + K$

2. Sea $x \in H \bigcap K$. Entonces $f(x) = x$ ya que $x \in H$ y $f|_H = I_{d_H}$;
   por otro lado $f(x) = 0$ pues $x \in K$ por tanto $x = 0$.

■

Combinando las proposiciones 3.1 y 3.2 se puede dar una sencilla demostración del teorema 2.17 del capítulo tres en la pagina 50, esto es: Un grupo divisible de un grupo abeliano es un sumando directo.
En efecto:
Sea H un subgrupo divisible del grupo abeliano G sea $I_H : H \to H$ el homomorfismo identidad por la proposición 3.1 existe un homorfismo $f : G \to H$ tal que $f|_H = 1_H$.
Por la proposición 3.2, H es un sumando directo de G.

■

La suiguiente definición y el lema que le sigue son conceptos que se usan para demostrar la proposición 3.3, pero se desarrollarán en el capítulo cuatro, nos permitimos hacer esto para seguir un orden estético de las cosas.

Definición (Def. 4.1): F es un grupo abeliano libre sobre $\{x_k\}_k$ si F es una suma directa de grupos cíclicos infinitos $\mathcal{Z}_k$ donde $\mathcal{Z}_k = [x_k]$

[1] $f \circ i = I_{d_H}$

Lema(lema 4.3): Cualquier grupo abeliano G es un cociente de un grupo abeliano libre.

Proposición 3.3 . *Cualquier grupo abeliano puede ser encajado en un grupo divisible*

Sea G un grupo abeliano. Por el lema 4.3 $G \cong F/K$ con F libre. Sea $\{X_\alpha\}_{\alpha\in\Lambda}$ base de F y sea F' el espacio vectorial sobre $\mathcal{Q}$ con base $\{X_\alpha\}_{\alpha\in\Lambda}$. Entonces F puede ser encajado en F' y por consiguiente F'/K puede ser encajado en F'/K. F'/K es divisible ya que F' es divisible (por ser suma directa de grupos abelianos divisibles: copias de $\mathcal{Q}$) y la imagen homomorfa de un grupo divisible es divisible. Por lo tanto G puede ser encajado en el grupo divisible F'/K.

■

3.2 Dos Proposiciones que Caracterizan

Proposición 3.4 . *Si un grupo G es un sumando directo de cada grupo que lo contiene, entonces es divisible.*

Demostración:
Por la proposición 3.3, G puede ser encajado en un grupo divisible D. Por consiguiente, $D \cong G \bigoplus K$; como D es divisible entonces cada sumando lo es, así G es divisible (observación 3 pag.44).

Proposición 3.5 . *Las siguientes propiedades de un grupo son equivalentes:*

1. *G es divisible.*

2. *G es un sumando directo de cada grupo que lo contiene.*

3. *Si K es un grupo y f un homomorfismo de un subgrupo de K en G, entonces f puede ser extendido a un homomorfismo de K en G.*

Dem:

(1) $\Rightarrow$ (2) Sea L un grupo y G un subgrupo divisible de L. Entonces por el teorema 2.17 G es sumando directo de L.

(2) $\Rightarrow$ (3) Por la proposición 3.4, G es divisible y por la proposición 3.1 f puede ser extendido a un homomorfismo de K en G.

(3) $\Rightarrow$ (1) Sea $n \in \mathcal{Z}$ y $x \in G$. Definimos $\varphi_n : n\mathcal{Z} \longrightarrow G$ tal que $n \rightsquigarrow x$ φ_n es un homomorfismo y por hipótesis φ_n puede extenderse a un homomorfismo $\varphi : \mathcal{Z} \longrightarrow G$. Por consiguiente $n\varphi(1) = \varphi(n \cdot 1) = \varphi(n) = x$ con $\varphi(1) \in G$. Así G es divisible.

■

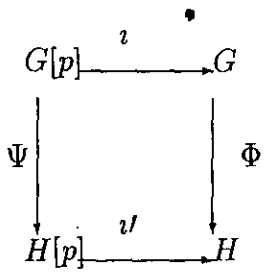
3.3 Una Proposición Adicional

Proposición 3.6 . *Sean G y H dos grupos divisibles p-primarios entonces $G \cong H \Leftrightarrow \{g \in G/pg = 0\} \cong \{h \in H : ph = 0\}$.*

Dem:

($\Rightarrow$) Es clara.

($\Leftarrow$) Sean $G[p] = \{g \in G : pg = 0\}$ $H[p] = \{h \in H : ph = 0\}$ Sea $\Psi : G[p] \longrightarrow H[p]$ un isomorfismo.



por tanto $i\prime \circ \Psi : G[p] \longrightarrow H$ es un homomorfismo y lo podemos extender a un homomorfismo $\Phi : G \longrightarrow H$ ya que H es divisible.

Veremos que Φ es un isomorfismo:

- Sea $x \in Ker(\Phi) \Rightarrow \Phi(x) = 0$. Si fuese $x \neq 0$ sea $p^n =$ orden de x con $n \geq 1$. Entonces $p^{n-1}x$ tiene orden p y, así, $p^{n-1}x \in G[p]$. Entonces $\Psi(p^{n-1}x) = \Phi(p^{n-1}x) = p^{n-1}\Phi(x) = 0$. Como Ψ es isomorfismo $\Rightarrow p^{n-1}x = 0$ lo cual contradice el hecho de que $\bigcirc(x) = p^n$. Por tanto Φ es 1 a 1.

- $Im(\Phi)$ es un subgrupo divisible de H por que $Im(\Phi) \cong G$ y G es divisible. Por tanto $H = Im(\Phi) \bigoplus K$

  Afirmamos que $K = 0$. Si existiera $y \in K - \{0\}$, sea $p^n = \bigcirc(y)$ con $n \geq 1$. Entonces $p^{n-1}y \in H[p]$, y así, $\exists x \in G[p]$ tal que $\Phi(x) = p^{n-1}y$; luego $p^{n-1}y \in Im\Phi$ y como, $y \in K$ y la suma es directa entonces $p^{n-1}y = 0$ lo cual contradice el hecho de que $\bigcirc(y) = p^n$. Por tanto $H = Im\Phi$.

■

Capítulo 4

Grupos Finitamente Generados

En un trabajo sobre clasificación de grupos abelianos no podría faltar el teorema fundamental de grupos ablianos finitamente generados, que es una simple generalización de su homólogo para grupos abelianos finitos. Para llegar a tal resultado dividimos este capítulo en dos secciones. En la primera demostramos algunos resultados (importantes dentro de la teoría de grupos abelianos libres) preliminares que nos ayudarán en nuestro objetivo. En la segunda sección se demuestran las proposiciones restantes para llegar al teorema fundamental.

4.1 Grupos Abelianos Libres

Recordemos que si S es un subconjunto de un grupo G, se dice que S genera a G si todo elemento de G puede escribirse como producto de potencias positivas y negativas de S. (La siguiente condición es equivalente: S no está contenido en ningun subgrupo propio de G).

Definición 4.1 . *F es un grupo abeliano libre sobre $\{x_k\}_k$ si F es una suma directa de grupos cíclicos infinitos $\mathcal{Z}_k$ donde $\mathcal{Z}_k = [x_k]$*

Es inmediato que si $|X| = |Y| < \infty$, entonces, los grupos abelianos libres sobre X y Y son isomorfos.

Ejemplo 4.1 . El grupo libre sobre $\{x_1, x_2\}$ es $\mathcal{Z} \oplus \mathcal{Z}$

Lema 4.2 . *Si F es un grupo abeliano libre con base $\{x_i\}_i$, G un grupo abeliano arbitrario, y $f : \{x_i\}_i \longrightarrow G$ cualquier función, entonces hay un único homomorfismo $g : F \longrightarrow G$ tal que $g(x_i) = f(x_i)$ para todo i.*

Demostración: Si $x \in F$ y $x = \sum_{i=1}^{n} k_i x_i$, con $x_i \in X$ y $k_i \in \mathcal{Z}$.
Entonces:

$$g(x) = \sum_{i=1}^{n} k_i f(x_i)$$

Es claro que g es un homomorfismo y que $g(x_i) = f(x_i) \, \forall \, x_i \in X$.
Ahora sea $h : F \to G$ un homomorfismo tal que $h(x_i) = f(x_i) \forall \, x_i \in X$.
Sea $x \in F$ y $x = \sum_{i=1}^{n} k_i x_i$, con $x_i \in X$ y $k_i \in \mathcal{Z}$.
Entonces:
$h(x) = h(\sum_{i=1}^{n} k_i x_i) = \sum_{i=1}^{n} k_i h(x_i) = \sum_{i=1}^{n} k_i f(x_i) = g(x) \therefore h = g$

■

Ejemplo 4.2 . Sea F el grupo libre sobre x_1 ($F \approx \mathcal{Z}$). $f : \{x_1\} \to \mathcal{Z}_2 \oplus \mathcal{Z}$ tal $f(x_1) = (1, 0)$ entonces $g(x) = x(\overline{1})$

Lema 4.3 . *Cualquier grupo abeliano G es un cociente de un grupo abeliano libre.*

En efecto: observemos antes que si X es cualquier conjunto, entonces existe un grupo abeliano libre F que tiene a X como base: Si $X = \{x\}$ entonces sea F el grupo cíclico infinito $\mathcal{Z}_x$, es decir, el grupo que tiene a x como generador; en el caso general sea $F = \bigoplus_{x \in X} \mathcal{Z}_x$, es decir, F es el conjunto de combinaciones lineales finitas de elementos de X:

$n_1 x_1 + ... + n_k x_k, \quad n_i \in \mathcal{Z}, x_i \in X$

Ahora pasemos a probar el lema:

Sea $S \subset G$ un cojunto de generadores de G (por ejemplo, podemos tomar $S = G$) en virtud de la observación anterior sea F el grupo abeliano libre con base S.

Por el lema 4.2 $i : S \longrightarrow G$ se extiende a un homomorfismo

$g : F \longrightarrow G$.

Solo falta probar que g es sobre: Si $x \in G$, entonces $x = \sum_{i=1}^{n} k_i x_i$, con $x_i \in S$ y $k_i \in \mathcal{Z}$.

Sea $y \in F$ tal que $y = \sum_{i=1}^{n} k_i x_i$, con $x_i \in S$ y $k_i \in \mathcal{Z}$.

Entonces: $g(y) = g(\sum_{i=1}^{n} k_i x_i)$

$= \sum_{i=1}^{n} k_i g(x_i)$

$= \sum_{i=1}^{n} k_i x_i$

$= x.$

$\therefore g$ es sobre.

Como $g : F \longrightarrow G$ es un homomorfismo sobre por los teoremas de

isomorfismos se tiene que $G \cong F/K$ donde $K = Ker(g)$

■

Ejemplo 4.3 . Si $G = \mathcal{Z}_2 \oplus \mathcal{Z} \oplus \mathcal{Z}_3$ entonces $F = \mathcal{Z} \oplus \mathcal{Z} \oplus \mathcal{Z}$ y $K = 2\mathcal{Z} \oplus \{0\} \oplus 3\mathcal{Z}$

Lema 4.4 . *Sea F un grupo abeliano libre sobre un conjunto de k elementos. Entonces el grupo cociente F/nF es un grupo finito de orden n^k.*

Demostración: Sea $S = \{x_1, x_2, ..., x_k\}$ una base de F y sea $H = \{\sum_{i=1}^{k} a_i x_i \ / \ con\ a_i \in \mathcal{Z}_n \text{ y } x_i \in S\}$.
H es un módulo libre sobre $\mathcal{Z}_n$ de dimención k, por tanto, tiene n^k elementos.

$$Veremosque: \ H \cong F/nF$$

Definamos $g : F \to H$, (si $F \ni x = \sum_{i=1}^{k} b_i x_i$, con $b_i \in \mathcal{Z}$ y $x_i \in S$), como sigue
$g(x) = g(\sum_{i=1}^{k} b_i x_i) = \sum_{i=1}^{k} b_i x_i \in H$
es claro que g es un homomorfismo sobre H.
• $Ker(g) \subseteq nF$.
Tomemos $x \in Ker(g) \Rightarrow 0 = g(x) = \sum_{i=1}^{k} b_i x_i \Rightarrow n | b_i \ \forall i \Rightarrow x \in nF$.
• $nF \subset Ker(g)$.
Sea $x \in nF \Rightarrow x = n \sum_{i=1}^{k} b_i x_i \Rightarrow g(x) = \sum_{i=1}^{k} b_i n x_i = 0 \Rightarrow x \in Ker(g)$

$\Rightarrow nF = Ker(g)$.

Por tanto y utilizando los teoremas de isomorfismos:

$F/nF \cong H$

■

Corolario 4.5 . *Sean S y $S\prime$ conjuntos finitos de distinto cardinal, y F y $F\prime$ grupos abelianos libres sobre S y $S\prime$ respectivamente. Entonces F y $F\prime$ no son isomorfos.*

Demostración: La prueba es por contradicción. Todo isomorfismo entre F y $F\prime$ inducirá un isomorfismo entre los grupos cocientes F/F^n y $F\prime/F\prime^n$, en contradicción con el lema.

■

Con esto se completa la demostración de que un grupo abelino libre generado por una conjunto finito queda completamente determinado por la cardinalidad del conjunto sobre el cual es libre.

Definición 4.6 . *Se dice que un grupo es finitamente generado si tiene un conjunto finito de generadores.*

Enunciemos formalmente el último resultado.

Corolario 4.7 . *Un grupo abeliano libre F finitamente generado tiene una única representación como suma directa de copias de $\mathcal{Z}$*

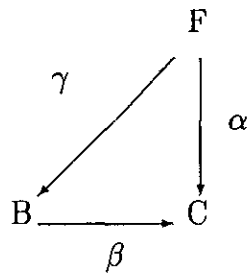
Demostración: Como F está completamente determinado por la cardinalidad del conjunto sobre el cual es libre (digamos n), sea $X = \{x_1, x_2, ..., x_n\}$ un conjunto que tiene dicha cardinalidad entonces $F = \sum_{i=1}^{n} \mathcal{Z}_{x_i}$ donde cada $\mathcal{Z}_{x_i}$ es una copia de $\mathcal{Z}$

$\therefore F$ es suma directa de n copias de $\mathcal{Z}$ y n es único.

■

El suiguiente teorema muestra la importancia de trabajar con generadores.

Teorema 4.8 (La Propiedad Proyectiva) *Sea $\beta : B \to C$ un homorfismo sobre de B en C. Si F es libre y $\alpha : F \to C$ es un homorfismo, entonces existe un homomorfismo $\gamma : F \to B$ con $\beta\gamma = \alpha$, es decir, existe un γ tal que el siguiente diagrama conmuta.*



Demostración:

Sea $\{x_k\}$ una base de F. Para cada k, existe un elemento $b_k \in B$ con $\beta(b_k) = \alpha(x_k)$; esto se sigue por el hecho de que β es sobre. Sea $f : \{x_k\} \to B$ definida por $f(x_k) = b_k$. Por el lema 4.2 existe un homomorfismo $\gamma : F \to B$ tal que $\gamma(x_k) = b_k$. Para revisar que $\beta\gamma = \alpha$,

es suficiente evaluar cada uno de los generadores de F, pero $\beta\gamma(x_k) = \beta(b_k) = \alpha(x_k)$.

■

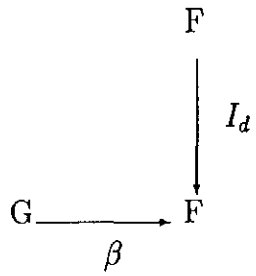
El primer teorema de isomorfismos nos dice que si G es un grupo y β un homomorfismo sobre de G en F, entonces $G/Ker(\beta) \approx F$; el corolario 4.9 nos muestra un resultado más fuerte que tal teorema en caso de que F sea abeliano libre: $G = Ker(\beta) \bigoplus F$.

Corolario 4.9 . *Sea G un grupo y β un homomorfismo sobre de G en F, donde F es libre. Entonces*

$$G = Ker(\beta) \bigoplus S,$$

donde $S \approx F$.

Demostración:
Considerando el siguiente diagrama:



Donde I_d es la identidad. Como se satisfacen las condiciones del teorema 4.8, existe un homomorfismo $\gamma : F \to G$ tal que $\beta\gamma = I_d$.
Ahora, necesitamos demostrar que γ es inyectiva, para poder tomar $S = imagen(\gamma) \approx F$:

•γ es inyectiva:

Sea $y \in Ker(\gamma)$

$\Rightarrow \gamma(y) = 0$

$\Rightarrow y = I_d(y) = \beta(\gamma(y)) = \beta(0) = 0$

$\therefore y = 0.$

Si hacemos $S = imagen(\gamma) \approx F$, entonces $G \approx Ker(\gamma) \bigoplus S$ para probar esto usaremos el criterio del teorema 1.6.

•G esta generado por $Ker(\beta) + S$

sea $x \in G$ es claro que:

$x = \gamma(\beta(x)) + (x - \gamma(\beta(x)))$

Falta ver que, $x - \gamma(\beta(x)) \in Ker(\beta)$, ya que obviamente $\gamma(\beta(x)) \in S$

$$\begin{aligned} \beta(x - \gamma(\beta(x))) &= \beta(x) - \beta(\gamma(\beta(x))) \\ &= \beta(x) - \beta(x) \qquad (\beta \circ \gamma = I_d) \\ &= 0 \end{aligned}$$

$(\Rightarrow x - \gamma(\beta(x)) \in Ker(\beta)).$

•$Ker(\beta) \bigcap S = \{0\}$

Sea $x \in Ker(\beta) \bigcap S$

$\Rightarrow \beta(x) = 0 \bigwedge \exists\, y \in F$ con $\gamma(y) = x$

$\Rightarrow \beta(\gamma(y)) = 0$

y como $\beta \circ \gamma = I_d$

$\Rightarrow y = 0$

$\Rightarrow x = \gamma(y) = \gamma(0) = 0.$

Por el teorema 1.6 $G \approx Ker(\beta) \bigoplus S$ donde $S \approx F$.

■

El corolario anterior es muy usado para demostrar el teorema fundamental.

4.2 Teorema Fundamental

En esta sección utilizaremos que el grupo cociente de un grupo G con su subgrupo de torsión es libre de torsión, resultado que se probó en la pagina 44 (proposición 2.11). En todo lo que sigue se supondrá que se trabaja con grupos abelianos finitamente generados, salvo que se indique lo contrario.

Lema 4.10 . *Si G es un grupo abeliano finitamente generado y H es sumando directo de G, entonces H también es finitamente generado*

Demostración:
Sea S tal que $[S] = G$ y $|S| = n$. (S existe porque G es finitamente generado.)
Sea $f : G \to H$ el homomorfismo natural (existe y es sobre por ser sumando directo). $f(S)$ es finito y $|f(S)| \leq n = |S|$.

Mostraremos que: $[f(S)] = H$

- $f[S] \subseteq H$
  Sea $y \in [f(S)] \Rightarrow y = \sum_{y_i \in f(S)} n_i y_i \Rightarrow$ para cada $y_i \in f(S)$ $\exists$ $x_i \in S$ tal que $f(x_i) = y_i \Rightarrow y = \sum_{x_i \in S} n_i f(x_i) = f(\sum_{x_i \in S} n_i x_i)$ y como $\sum_{x_i \in S} n_i x_i \in [S] = G \Rightarrow y \in H$.

- $H \subseteq f[S]$
  $y \in H \Rightarrow \exists\ x \in G$ tal que $f(x) = y$ pero como $G = [S] \Rightarrow$ $x = \sum_{x_i \in S} n_i x_i \Rightarrow y = f(x) = f(\sum_{x_i \in S} n_i x_i) = \sum_{x_i \in S} n_i f(x_i)$ $\in [f(S)]$

■

Tanto el lema anterior como todos los que siguen son preparatorios para la demostración del teorema 4.15. En el capítulo dos demostramos que $\mathcal{Q}$ no es suma de grupos cíclicos, muy al contrario el lema 4.11 nos dice que:

Lema 4.11 . *Todo subgrupo H de $\mathcal{Q}$, finitamente generado, es cíclico.*

Demostración:
Sea $S = [\frac{a_1}{b_1}, \frac{a_2}{b_2}, ..., \frac{a_n}{b_n}]$ un conjunto de generadores de H con $a_i, b_i \in \mathcal{Z}$ y $b_i \neq 0$ para $i = 1, 2, ..., n$ sea $b = \prod_{i=1}^{n} b_i$, y sea $f : H \to \mathcal{Z}$ definido así: $f(x) = bx$.
f está bien definido (en el siguiente sentido: $f(x) \in \mathcal{Z}\ \forall\ x \in H$).
Ya que si, $x \in H \Rightarrow x = \sum_{i=1}^{n} m_i \frac{a_i}{b_i} \Rightarrow f(x) = b \sum_{i=1}^{n} m_i \frac{a_i}{b_i} = \sum_{i=1}^{n} m_i \frac{a_i b}{b_i}$

$\in \mathcal{Z}$ (pues $b_i | b \; \forall \; i$.)

Como f es inyectiva, ya que $0 = f(x) = bx \Rightarrow x = 0$, entonces $H \approx f(H)$.

Sea

$$d = (\frac{a_1 b}{b_1}, \frac{a_2 b}{b_2}, ..., \frac{a_n b}{b_n}) \in \mathcal{Z} \tag{4.1}$$

Veremos que $f(H) = [d]$

como $H \approx f(H) \Rightarrow f(H) = [f(S)] = [\frac{a_1 b}{b_1}, \frac{a_2 b}{b_2}, ..., \frac{a_n b}{b_n}]$

por la ecuación 4.1 tenemos $d = m_1 \frac{a_1 b}{b_1} + m_2 \frac{a_2 b}{b_2} +, ..., + m_n \frac{a_n b}{b_n}$ así, $d \in [f(S)]$.

Y para cada $\frac{a_i}{b_i} b$ por la ecuación 4.1 se tiene que $d | b \frac{a_i}{b_i} \Rightarrow \exists \; m_i$ tal que $dm_i = b \frac{a_i}{b_i} \Rightarrow b \frac{a_i}{b_i} \in [d]$

$\therefore H \approx f(H) \approx [d]$.

(Aun más $H \approx d\mathcal{Z} \approx \mathcal{Z}$).

■

Lema 4.12 . *Si G es libre de torsión y $x \in G$, definamos*

$$< x >= \{y \in G \; : \; my \in [x] \; para \; algun \; m \in \mathcal{Z}, m \neq 0\}$$

$< x >$ *es isomorfo a un subgrupo de* $\mathcal{Q}$.

Si hacemos $G = \mathcal{Q}$, $x = 1$ entonces $[x] = \mathcal{Z}$ y $< x > \approx \mathcal{Q}$ (ya que ésta es una manera de construir los racionales), sabiendo esto podemos imaginar por donde va la demostración. Ahora pasemos a la demostración:

• Probemos primero que $< x >$ es un grupo.

Sean $x_1, x_2 \in < x > \Rightarrow \exists\ m_1, m_2, n_1, n_2$ tales que $m_1 x_1 = n_1 x$ y $m_2 x_2 = n_2 x$

$$\begin{aligned} m_1 m_2(x_1 + x_2) &= m_1 m_2 x_1 + m_1 m_2 x_2 \\ &= m_2 n_1 x + m_1 n_2 x \\ &= (m_2 n_1 + m_1 n_2) x \in [x] \end{aligned}$$

$$\therefore x_1 + x_2 \in < x > .$$

Sea $x_1 \in < x > \Rightarrow \exists\ m, n$ tal que $m x_1 = n x \Rightarrow m(-x_1) = (-n)x \Rightarrow -x_1 \in < x >$.

Sea $f :< x > \rightarrow Q$ tal que $f(y) = \frac{n}{m}$ cuando $my = nx$.

• f esta bien definida.

Sean m, n y $m\prime$, $n\prime$ tales que $my = nx$ y $m\prime y = n\prime x$

Veremos que: $\frac{n\prime}{m\prime} = \frac{n}{m}$.

$$\begin{aligned} nx = my \Rightarrow \\ m\prime nx &= mm\prime y \\ &= mn\prime x \end{aligned}$$

$\Rightarrow m\prime n = mn\prime$(ya que $[x]$ es libre de torsión y en un grupo cíclico libre de torsión la representación para un elemento, como múltiplo de x, es única.) $\therefore \frac{n\prime}{m\prime} = \frac{n}{m}$.

• f es homomorfismo.

Sean y_1 y $y_2 \in < x >$ entonces existen m_1, m_2, n_1 y n_2 tales que $m_1y_1 = n_1x$ y $m_2y_2 = n_2x$. Ahora, sabemos que

$$\begin{aligned} m_1m_2(y_1 + y_2) &= m_1m_2y_1 + m_1m_2y_2 \\ &= m_2n_1x + m_1n_2x \\ &= (m_2n_1 + m_1n_2)x \end{aligned}$$

Entonces:

$$\begin{aligned} f(y_1 + y_2) &= \tfrac{m_2n_1+m_1n_2}{m_1m_2} \\ &= \tfrac{m_2n_1}{m_1m_2} + \tfrac{m_1n_2}{m_1m_2} \\ &= \tfrac{n_1}{m_1} + \tfrac{n_2}{m_2} \\ &= f(y_1) + f(y_2) \end{aligned}$$

Como f es un homonorfismo sólo falta ver que:

- f es inyectiva.

$0 = f(y) = \frac{n}{m} \Rightarrow n = 0$.

$0 = nx = my$ y como $m \neq 0 \Rightarrow y = 0$.

$\therefore < x > \approx f(< x >) < \mathcal{Q}$.

■

Lema 4.13 . *Si G es libre de torsión y $x \in G$, entonces $G/ < x >$ es también libre de torsión.*

Supongamos que $\exists\, y \in G/ < x >$ tal que $ny = 0$, para algún $n \in \mathcal{Z}$.

como $y = y' + < x >$, con $y' \in G$

entonces $0 = ny = ny\prime + < x >$

$\Rightarrow ny\prime \in < x >$

$\Rightarrow \exists\ m, k$ tal que $mny\prime = kx$

$\Rightarrow y\prime \in < x >$

$\Rightarrow y = 0 + < x >$

$\Rightarrow y = 0 \in G/ < x >$

$\therefore G/ < x >$ es libre de torsión.

■

Proposición 4.14 . *Sea G un grupo de torsión finitamente generado, entonces G es finito.*

Sea $S = \{x_1, x_2, ..., x_n\}$ un conjunto de generadores de G. Como es de torsión $\exists\ r_i \in \mathcal{Z}$ tales que $r_i = \bigcirc(x_i)$ para cada $i \in \{1, 2, ..., n\}$.

Sea $H = \{k_1x_1 + k_2x_2 + ... + k_nx_n\ :\ con\ cada\ k_i \in \{1, 2, ..., r_i\}\}$. Es claro que $H \subseteq G$ y $\#|H| = \prod_{i=1}^{n} r_i < \infty$

Mostraremos que: $G \subseteq H$.

Sea $x \in G \Rightarrow x = l_1x_1 + l_2x_2 + ... + l_nx_n$ donde los $l_i \in \mathcal{Z}$

por el algoritmo de Euclides , para cada i, $\exists\ a_i,\ b_i$, tales que $l_i = r_ia_i + b_i$ y $1 \leq b_i \leq r_i$

$\Rightarrow l_ix_i = (r_ia_i + b_i)x_i = a_ir_ix_i + b_ix_i = b_ix_i$

$\Rightarrow x = b_1x_1 + b_2x_2 + ... + b_nx_n$.

$\Rightarrow x \in H$

$\therefore G \subseteq H$

$G = H$.

Teorema 4.15 (Teorema de la Base) *Todo grupo abeliano finitamente generado G es suma directa de grupos cíclicos. (Primarios o infinitos).*

Demostración:

Sea $G = [x_1, x_2, ..., x_n]$;

Caso (i) G es libre de torsión: Probaremos este caso por inducción: Si n=1, entonces G es cíclico de orden infinito ($\mathcal{Z}$), y ya estaría. Si $n > 1$, sea β el homorfismo natural de G sobre $G/ < x_n >$ como β manda a x_n al 0 entonces $G/ < x_n >$ es generado por $n-1$ elementos (o menos), y por el lema 4.13 es libre de torsión. Por inducción $G/ < x_n >$ es abeliano libre (acordémonos que un grupo abeliano libre es suma directa de grupos cíclicos infinitos). Y así, por el corolario 4.9 (haciendo $F = G/ < x >$), $G =< x_n > \bigoplus(grupo\ abeliano\ libre)$. Ahora $< x_n >$ es finitamente generado (lema 4.10) y un subgrupo de $\mathcal{Q}$ (lema 4.12), por tanto cíclico (lema 4.11).

Tenemos así que G es libre, por tanto suma de grupos cíclicos.

Caso (ii) Caso general: G/tG[1] es finitamente generado y libre de torsión, así, es abeliano libre, por el caso (i). Por el corolario 4.9, (haciendo $F = G/tG$) $G = tG \bigoplus(abeliano\ libre)$. Por el lema 4.10, tG es finitamente generado y de torsión, por ello finito (proposición 4.14). Por el teorema de la base para grupos finitos (teorema 1.13, pagina 20), tG es suma directa de grupos cíclicos.

[1] tG es el grupo de torsión de G

■

Teorema 4.16 (Teorema fundamental) *Todo grupo abeliano finitamente generado G tiene una única representación como suma directa de grupos cíclicos primarios e infinitos.*

Demostración:
Sabemos que $G \approx tG \bigoplus G/tG$. La unicidad para tG es precisamente el teorema fundamental de grupos abelianos finitos. La unicidad para la cantidad de sumandos cíclicos infinitos es el corolario 4.7.

■

Apéndice A

Lema de Zorn

En el desarrollo del presente trabajo se hace uso de una versión del lema de Zorn que se refiere al concepto de un conjunto parcilamente ordenado. Un conjunto parcialmente ordenado es un conjunto con una relación binaria $\geq$ que verifica:

1. $x \geq x$ (reflexivilidad)

2. $x \geq y, y \geq x$ implica $x = y$ (antisimetría)

3. $x \geq y, y \geq z$ implica $x \geq z$ (transitividad).

Sea S un conjunto parcialmente ordenado y T un subconjunto. El elemento $x \in S$ se dice que es la **MINIMA COTA SUPERIOR** de T si $x \geq y$ para toda $y \in T$ y si $z \geq y$, $\forall y \in T \Rightarrow z \geq x$. Observemos que el elemento x puede o no estar en T. Una mínima cota superior no necesariamente existe, **pero en caso de existir es única** (Si x_1, x_2 son dos M.C.S. para T entonces $x_i \geq t \; \forall t \in T (i = 1, 2)$, luego $x_1 \geq x_2$ y $x_2 \geq x_1$, por tanto $x_1 = x_2$)

Diremos que un elemento x de un conjunto parcialmente ordenado S

es **MAXIMAL** si S no contiene un elemento "más grande" (es decir, si $y \in S$ y $y \geq x \Rightarrow x = y$).

Notemos que S podría contener muchos elementos máximales.

Diremos que un conjunto parcialmente ordenado es una **cadena** (o conjunto linealmente ordenado) si cualquiera dos elemento son comparables, es decir, $x \geq y$ ó $y \geq x$.

Lema de Zorn: *Sea S un conjunto parcialmente ordenado en el cual toda cadena tiene una mínima cota superior. Entonces S tiene un elemento maximal.*

Bibliografía

[1] Eves, Howard.
Estudio de las Geometrias, Tomo II.
Editorial UTHEA.

[2] Fraleigh, John B.
A First Course In Abstract Algebra.
University of Rhode Island.
Editorial Addison-Wesley .

[3] Jacobson, Nathan.
Lectures in abstract algebra.
Editorial D. Van Nostrand Company Inc.

[4] Kaplansky, Irving .
Infinite Abelian Groups.
University of Michigan 1954.
Editorial Allyn and Bacon, Inc.

[5] Mac Duffee, Cyrus Colton.
An Introduction To Abstract Algebra.
Editorial John Wiley & Sons, Inc.

[6] Massey, William .
Introducción a la Topología Algebraica.
Editorial Reverté S.A. .

[7] Lang, Serg
Algebra.
Editorial Addison-Wesley.

[8] Rotman, Joseph J. .
The Theory of Groups.
University of Illinois 1965.

[9] Vargas Mendoza José A.
Algebra abstracta.
Editorial Limusa.

Indice Alfabético