UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE CIENCIAS

ESCUELA PROFESIONAL DE MATEMÁTICA

"GRUPOS ABELIANOS"

INFORME DE SUFICIENCIA

PARA OPTAR EL TITULO PROFESIONAL DE:

LICENCIADO EN MATEMÁTICA

JORGE LUIS CORNEJO HUAMÁN

LIMA-PERÚ
2003

A mi madre Olinda,

quien con su constante apoyo me alienta a seguir adelante.

A mis sobrinos Christian, Johana y Steven.

Resumen

En este informe se trata de describir la estructura de los grupos abelianos libres, los grupos abelianos finitamente generados y los grupos divisibles.

Una clasificación elemental es la siguiente:

> Grupos de Torsión (si todos sus elementos son de orden finito), grupos sin torsión (si el único elemento de orden finito es el cero) y grupos mixtos (si tiene elementos no nulos de orden finito y elementos de orden infinito). Si todos los elementos de un grupo abeliano G son de orden p^k, donde p es un primo fijo y k es un entero no negativo, entonces se dice que G es un grupo p-primario.

El teorema de estructura de los grupos de torsión establece que todo grupo de torsión es una suma directa de grupos primarios. Los grupos abelianos libres son las sumas directas de grupos isomorfos al grupo cíclico $\mathbb{Z}$.

Un resultado importante es el siguiente:

> Todo grupo abeliano es cociente de un grupo abeliano libre.

El teorema fundamental de los grupos abelianos establece que todo grupo abeliano finitamente generado es una suma directa finita de grupos cíclicos infinitos y/o grupos cíclicos primarios.

Dos consecuencias inmediatas de este teorema son las siguientes:

(a) Todo grupo abeliano finito es una suma directa de grupos cíclicos primarios.

(b) Los grupos abelianos finitamente generados sin torsión son los grupos abelianos libres finitamente generados.

El teorema de estructura de los grupos divisibles establece que todo grupo divisible es una suma directa de grupos p-Prüfer y/o grupos isomorfos a $\mathbb{Q}$ (los grupos p-Prüfer son las p-componentes de $\mathbb{Q}/\mathbb{Z}$).
De aquí se deduce que los grupos divisibles de torsión son las suams directas de grupos p-Prüfer; y los grupos divisibles sin torsión (como $\mathbb{R}$ y $\mathbb{C}$, por ejemplo) son sumas directas de grupos isomorfos a $\mathbb{Q}$.

Índice general

Introducción

Este informe académico trata de un tema importante del Algebra Moderna que son los **Grupos Abelianos**. El objetivo de este trabajo es describir la estructura de una amplia clase de grupos abelianos, sin pretender desarrollar el tema de grupos abelianos en toda su generalidad. Las herramientas para construir grupos abelianos de estructura compleja son los grupos abelianos de estructura elemental, como los grupos cíclicos, grupos primarios (p-grupos abelianos), el grupo aditivo de los números racionales y los grupos p-Prüfer utilizando el concepto de **suma directa** (finita ó infinita).

Por otro lado, a travez del concepto de suma directa y realizando un proceso de descomposición, se reduce el estudio de ciertas clases de grupos abelianos (de torsión, finitamente generados, divisibles, etc) al estudio de grupos abelianos de estructura elemental.

Usualmente la operación binaria de un grupo abeliano se denota con el símbolo "$+$". Para trasladar la notación multiplicativa a la notación aditiva utilizaremos el siguiente "diccionario":

ab	....	$a+b$
a^{-1}	....	$-a$
1	....	0
a^n	....	na
ab^{-1}	....	$a-b$
HK	....	$H+K$
Ha	....	$a+H$
producto directo	....	suma directa
$H \times K$	....	$H \oplus K$
$\prod_{i\in I} H_i$	....	$\bigoplus_{i\in I} H_i$

Observamos que una suma directa de grupos abelianos es un grupo abeliano. Las sumas directas (finitas ó infinitas) de grupos cíclicos infinitos son llamados **grupos abelianos libres**. Un resultado fundamental que demostraremos más adelante es el siguiente:

"Todo grupo abeliano es cociente de un grupo abeliano libre".

Dado cualquier grupo abeliano G, el conjunto $T(G)$ de todos los elementos de G de orden finito forma un subgrupo de G, llamado el **subgrupo de torsión** de G. Un grupo abeliano G es llamado un grupo de torsión, si $T(G) = G$, es decir, todos sus elementos son de orden finito (por ejemplo $\mathbb{Q}/\mathbb{Z}$). Un grupo cuyos elementos son todos de orden p^k donde p es un primo fijo y k es un entero no negativo, es llamado un **grupo p-primario (ó p-grupo)** ó simplemente **grupo primario**. Demostraremos que el estudio de los grupos de torsión se reduce al estudio de los grupos primarios en el siguiente sentido:

"Todo grupo de torsión es una suma directa de grupos (abelianos) primarios".

El resultado anterior es conocido como el Teorema de Estructura de los Grupos de Torsión.

Un valioso grupo abeliano p-primario es el **grupo p-Prüfer**. Cada p-componente del grupo de torsión $\mathbb{Q}/\mathbb{Z}$ es llamado **grupo p-Prüfer**. Un grupo abeliano G es llamado un **grupo sin torsión**, si $T(G) = \{0\}$, es decir, el único elemento de orden finito es el cero (por ejemplo: $\mathbb{Q}$). Un grupo abeliano G es llamado un grupo mixto, si $\{0\} \neq T(G) \neq G$ (por ejemplo: $\mathbb{Q} - \{0\}$, $\mathbb{R}/\mathbb{Z}$). Muchos grupos abelianos son sumas directas de grupos ciclicos, el grupo aditivo $\mathbb{Q}$ de los números racionales y grupos p-Prüfer.

El grupo aditivo $\mathbb{Q}$ de los números racionales tiene la siguiente propiedad: Si $t \in \mathbb{Q}$ es arbitrario y n es un entero diferente de cero cualquiera, entonces existe un $r \in \mathbb{Q}$ tal que $nr = t$. Los grupos abelianos con esta propiedad son llamados **grupos divisibles**. Los grupos p-Prüfer también son divisibles. Estos no son los únicos grupos divisibles, el grupo aditivo de los números reales también es divisible. Un grato resultado es el siguiente:

"Todo grupo divisible es una suma directa de grupos p-Prüfer y/o grupos isomorfos al grupo aditivo de los números racionales".

Dicho resultado es conocido como el Teorema de Estructura de los Grupos Divisibles.

Si G es un grupo tal que $G = [X]$, donde X es un subconjunto finito de G, entonces se dice que G es **un grupo finitamente generado**. El siguiente resultado es llamado el **Teorema Fundamental de los Grupos Abelianos**:

"Todo grupo abeliano finitamente generado es una suma directa finita de grupos cíclicos infinitos y/o cíclicos primarios".

A cada grupo abeliano finitamente generado se asocia un conjunto de números enteros no negativos llamado **tipo** del grupo abeliano. El concepto de tipo determina totalmente la estructura de un grupo abeliano finitamente generado. En efecto, se tiene el siguiente resultado:

"Dos grupos abelianos finitamente generados son isomorfos si y solamente si tienen el mismo tipo".

Capítulo 1

Generalidades

1.1. Concepto de Grupo Abeliano

Definición 1.1 *Un grupo* $(G, *)$ *es llamado abeliano, si* $a * b = b * a$ *para cualesquiera* $a, b \in G$.

Observación: Usualmente la operación binaria " $*$ " de un grupo abeliano se denota mediante el simbolo " $+$ ".

Teorema 1.1 *Toda imagen homomorfa de un grupo abeliano es un grupo abeliano.*

Demostración:
Sean $(G, +)$ un grupo abeliano, $(H, *)$ un grupo cualquiera y $f : G \to H$ un homomorfismo de grupos.
Dados $a, b \in G$ cualquiera.

$$\begin{aligned} f(a) * f(b) &= f(a+b) \\ &= f(b+a) \\ &= f(b) * f(a) \end{aligned}$$

Por consiguiente, $f(G)$ es un grupo abeliano. $\square$

Corolario. Todo cociente de un grupo abeliano es un grupo abeliano.

Demostración:

Sea G un grupo abeliano y sea H un subgrupo de G, como G/H es la imagen del homomorfismo natural $\Pi : G \to G/H$

entonces por el teorema 1.1, G/H es un grupo abeliano. $\square$

1.2. Ejemplos de Grupos Abelianos

1. Sean G y H grupos abelianos y sea

$$Hom(G, H) = \{f / \ f \text{ es un homomorfismo de } G \text{ en } H\}$$

Dados $f, g \in Hom(G, H)$ se define $f + g$ por

$$(f + g)(x) = f(x) + g(x), x \in G \tag{1.1}$$

Mostraremos que $Hom(G, H)$ con la operación definida por (1.1) es un grupo abeliano

(a) Veamos que $f + g \in Hom(G, H)$:

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

para cualesquiera $x, y \in G$. Luego $f + g \in Hom(G, H)$.

(b) Asociatividad de la adición:

$$\begin{aligned} [(f+g)+h](x) &= (f+g)(x) + h(x) \\ &= [f(x) + g(x)] + h(x) \\ &= f(x) + [g(x) + h(x)] \\ &= f(x) + (g+h)(x) \\ &= [f + (g+h)](x) \end{aligned}$$

para todo $x \in G$. Esto significa que

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

(c) Existencia de identidad:

sea $w : G \to H$ definida por

$$w(x) = 0, \quad x \in G$$

Se verifica inmediatamente que $w \in Hom(G, H)$.

Ahora, para todo $f \in Hom(G, H)$ y para todo $x \in G$:

$$\begin{aligned}
(f+w)(x) &= f(x)+w(x) \\
&= f(x)+0 \\
&= f(x) \\
&= 0+f(x) \\
&= w(x)+f(x) \\
&= (w+f)(x)
\end{aligned}$$

Luego $\quad f+w = f = w+f.$

Lo cual prueba que w es la identidad (elemento neutro aditivo).

(d) Existencia de inversos:

Dado $f \in Hom(G, H)$, definimos $-f$ por

$$(-f)(x) = -f(x), \quad x \in G$$

Para todo $x \in G$:

$$\begin{aligned}
[f+(-f)](x) &= f(x)+(-f)(x) \\
&= f(x)+[-f(x)] \\
&= 0 \\
&= [-f(x)]+f(x) \\
&= (-f)(x)+f(x) \\
&= [(-f)+f](x)
\end{aligned}$$

Luego $\quad f+(-f) = w = (-f)+f.$

(e) Conmutatividad de la adición:

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

para todo $x \in G$. Esto significa que

$$f+g=g+f$$

Por lo tanto $Hom(G,H)$ con la adición definida por (1.1) es un grupo abeliano.

2. Para cualquier grupo abeliano G:

$$Hom(\mathbb{Z},G) \approx G$$

En efecto, la aplicación $\varphi : Hom(\mathbb{Z},G) \to G$ definida por $\varphi(f) = f(1)$ es un isomorfismo, puesto que:

(a) φ es un homomorfismo:

$$\begin{aligned} \varphi(f+g) &= (f+g)(1) \\ &= f(1)+g(1) \\ &= \varphi(f)+\varphi(g) \end{aligned}$$

para cualesquiera f, $g \in Hom(\mathbb{Z},G)$.

(b) φ es sobreyectivo:

Dado cualquier $x \in G$, definimos $f_x : \mathbb{Z} \to G$ por $f_x(n) = nx$.

Como

$$\begin{aligned} f_x(n+m) &= (n+m)x \\ &= nx+mx \\ &= f_x(n)+f_x(m) \end{aligned}$$

para cualesquiera $n, m \in \mathbb{Z}$, entonces $f_x \in Hom(\mathbb{Z},G)$.

Ademas $\varphi(f_x) = x$, puesto que

$$\begin{aligned}\varphi(f_x) &= f_x(1)\\ &= 1x\\ &= x.\end{aligned}$$

(c) φ es inyectivo:

Sea $f \in Ker\varphi$ arbitrario. Entonces $\varphi(f) = 0$, esto es, $f(1) = 0$. Luego, para todo $n \in \mathbb{Z}$:

$$f(n) = f(n1) = nf(1) = 0 = w(n)$$

Por lo tanto $f = w$, la identidad. Se sigue que

$$Ker\ \varphi = \{w\}.$$

3. $$Hom(\mathbb{Q}, \mathbb{Z}) = 0$$

Sea $f \in Hom(\mathbb{Q}, \mathbb{Z})$ arbitrario. Dado cualquier $q \in \mathbb{Q}$,

$$\forall n \in \mathbb{Z} : f(q) = f(n(q/n)) = nf(q/n)$$

lo cual significa que el entero $f(q)$ es divisible por todo $n \in \mathbb{N}$

Por lo tanto $f(q) = 0$. En consecuencia $f = 0$.

4. $$Hom(\mathbb{Q}, \mathbb{Q}) \approx \mathbb{Q}$$

Para cada $q \in \mathbb{Q}$, definimos $f_q : \mathbb{Q} \to \mathbb{Q}$ por

$$f_q(x) = qx, \quad x \in \mathbb{Q}$$

Se verifica inmediatamente que $f_q \in Hom(\mathbb{Q}, \mathbb{Q})$.

Ahora, definimos $\varphi : \mathbb{Q} \to Hom(\mathbb{Q}, \mathbb{Q})$ por $\varphi(q) = f_q$, $q \in \mathbb{Q}$.

Afirmamos que φ es un isomorfismo. En efecto:

(a) φ es un homomorfismo:

Dados $q, r \in \mathbb{Q}$ cualesquiera.

$$\begin{aligned} f_{q+r}(x) &= (q+r)x \\ &= qx + rx \\ &= f_q(x) + f_r(x) \\ &= (f_q + f_r)(x) \end{aligned}$$

para todo $x \in \mathbb{Q}$. Entonces $f_{q+r} = f_q + f_r$.

Por consiguiente

$$\varphi(q+r) = f_{q+r} = f_q + f_r = \varphi(q) + \varphi(r)$$

para cualesquiera $q, r \in \mathbb{Q}$.

(b) φ es inyectivo:

Sea $q \in Ker\varphi$ arbitrario. Entonces $\varphi(q) = w$, esto es, $f_q = w$.

Luego $q = q1 = f_q(1) = w(1) = 0$. Por lo tanto

$$Ker\varphi = \{0\}.$$

(c) φ es sobreyectivo:

Sea $f \in Hom(\mathbb{Q}, \mathbb{Q})$ arbitrario. Denotemos $f(1) = r$. Para cualquier $m/n \in \mathbb{Q}$:

$$\begin{aligned} f_r(m/n) &= r(m/n) \\ &= (m/n)r \\ &= (m/n)f(1) \\ &= (1/n)mf(n/n) \\ &= (1/n)f(m(n/n)) \\ &= (1/n)f(n(m/n)) \\ &= (1/n)nf(m/n) \\ &= f(m/n) \end{aligned}$$

Luego $\varphi(r) = f_r = f$.

5. $$Hom(\mathbb{Z}_n, \mathbb{Z}_m) \approx \mathbb{Z}_d$$

donde $d = MCD(n, m)$.

En efecto, denotemos por k a $MCM(n, m)$ y $H = (k/n)\mathbb{Z}$ el subgrupo de $\mathbb{Z}$ generado por el entero k/n.

Para cada $x \in H$, definimos $\varphi_x : \mathbb{Z}_n \to \mathbb{Z}_m$ por

$$\varphi_x(a) = xb$$

donde a es un generador de $\mathbb{Z}_n$ y b es un generador de $\mathbb{Z}_m$.

φ_x está bien definida.

Es suficiente probar que $\varphi_x(0) = 0$, debido a que $\varphi_x(s+t)$ es igual a $\varphi_x(s) + \varphi_x(t)$, para cualesquiera $s, t \in \mathbb{Z}_n$.

Supongamos que $r \equiv 0 mod(n)$ y que $\varphi_x(ra) = (xr)b$.

Como $x \in H = (k/n)\mathbb{Z}$, entonces $x \equiv 0 mod(k/n)$; luego $xr \equiv 0 mod(k)$ y por lo tanto $xr \equiv 0 mod(m)$. Por consiguiente

$$\varphi_x(0) = \varphi_x(ra) = (xr)b = 0$$

Ahora, definimos $\varphi : H \to Hom(\mathbb{Z}_n, \mathbb{Z}_m)$ por

$$\varphi(x) = \varphi_x, \quad x \in H$$

Afirmamos que φ es un epimorfismo. En efecto:

(a) φ es un homomorfismo:

$$\begin{aligned} \varphi_{x+y}(a) &= (x+y)b \\ &= xb + yb \\ &= \varphi_x(a) + \varphi_y(a) \\ &= (\varphi_x + \varphi_y)(a) \end{aligned}$$

para cualesquiera $x, y \in H$. Entonces $\varphi_{x+y} = \varphi_x + \varphi_y$

Por consiguiente

$$\varphi(x+y) = \varphi_{x+y} = \varphi_x + \varphi_y = \varphi(x) + \varphi(y)$$

para cualesquiera $x, y \in H$.

(b) φ es sobreyectivo:

Sea $g \in Hom(\mathbb{Z}_n, \mathbb{Z}_m)$ arbitrario. El homomorfismo g esta determinado por

$$g(a) = hb$$

donde h es algún entero. Como $0 = na$ (puesto que a es de orden n), entonces

$$g(0) = g(na) = ng(a) = (nh)b$$

y por lo tanto $nh \equiv 0 mod(m)$.

Por otro lado, existen $s, t \in \mathbb{Z}$ tales que $d = MCD(n, m) = sn + tm$

Entonces $\quad hd = shn + thm \quad$ de donde $\quad hd \equiv 0 mod(m)$.

Como $mn = MCM(n, m)MCD(n, m) = kd$, entonces $(hd)k = mnh$

Luego $h = (hd/m)(k/n) \in (k/n)\mathbb{Z} = H$.

Pero $\varphi_h(a) \doteq hb = g(a)$ lo cual significa que

$$\varphi(h) = \varphi_h = g$$

Además, $Ker\varphi = m\mathbb{Z} \subset H$:

Si $x \in m\mathbb{Z}$, entonces $\varphi_x(a) = xb = 0$, puesto que $o(b) = m$.

Luego $\varphi(x) = \varphi_x = w$, el homomorfismo nulo y por lo tanto $x \in Ker\varphi$.

Recíprocamente,

si $x \in Ker\varphi$, entonces $\varphi(x) = \varphi_x = w$. Luego $xb = \varphi_x(a) = 0$ y por lo tanto m divide a x, esto es $x \in m\mathbb{Z}$.

Finalmente, por el primer teorema de isomorfismos,

$$\begin{aligned} Hom(\mathbb{Z}_n, \mathbb{Z}_m) &\approx H/Ker\varphi \\ &= H/m\mathbb{Z} \\ &= (k/n)\mathbb{Z}/m\mathbb{Z} \\ &\approx \mathbb{Z}_{m/(k/n)} \\ &= \mathbb{Z}_{mn/k} \\ &= \mathbb{Z}_d. \end{aligned}$$

1.3. Sumas Directas (Finitas o Infinitas)

En adelante G denotará siempre a un Grupo Abeliano.

Dada una familia de conjuntos $(S_i)_{i\in I}$, cuando sea conveniente escribiremos:

$$S(i) \text{ en lugar de } S_i \text{ para cada } i \in I.$$

Si $(G_i)_{i\in I}$ es una familia de subgrupos de G, entonces el subgrupo $[\bigcup\{G_i/i \in I\}]$ será denotado por $\sum_{i\in I} G_i$ y está formado por los elementos $x \in G$ que son de la forma:

$$x = x_1 + x_2 \ldots + x_n$$

donde $x_j \in \bigcup\{G_i/i \in I\}$,$j = 1, 2, \ldots, n$

Definición 1.2 *Sea $(G_i)_{i\in I}$ una familia de subgrupos de G. Se dice que G es la* **suma directa** *de la familia $(G_i)_{i\in I}$, si $G = \sum_{i\in I} G_i$ y cada $x \in G$, $x \neq 0$ se puede expresar de manera única (excepto en el orden de los sumandos) como un elemento de $\sum_{i\in I} G_i$,con sumandos no nulos pertenecientes a $G(i_1), G(i_2), \ldots, G(i_n)$ donde $i_1, i_2, \ldots, i_n \in I$ son distintos.*

Si G es la **suma directa** de la familia $(G_i)_{i\in I}$, entonces se usa la notación : $G = \bigoplus_{i\in I} G_i$
En particular, si G es la suma directa de los subgrupos $G_1, G_2, \ldots, G_n$, entonces se escribe:

$$G = G_1 \oplus G_2 \oplus \ldots \oplus G_n$$

Teorema 1.2 *Sean $G_1, G_2, \ldots, G_n$ subgrupos de G.*
$G = G_1 \oplus G_2 \oplus \ldots \oplus G_n$ si y solo si cada $x \in G$ se puede expresar de manera única como:

$$x = x_1 + x_2 + \ldots + x_n$$

donde $x_i \in G_i$, $i = 1, 2, \ldots, n$.

Demostración:

Sea $G = G_1 \oplus G_2 \oplus \ldots \oplus G_n$ entonces por la definición 1.2 :

$$x = x_1 + x_2 + \ldots + x_m$$

de manera única, donde $m \leq n, \quad x \neq 0, \quad x_j \neq 0, \quad j = 1, 2, \ldots, m$

Luego $\quad x = y_1 + y_2 + \ldots + y_n$ es única completando con ceros.

Si $x = 0$ entonces x tiene la siguiente representación:

$$x = 0 + 0 + \ldots + 0 \quad (n \text{ sumandos}) \tag{1.2}$$

Supongamos que $\quad 0 = x_1 + x_2 + \ldots + x_n$ y que existe $j/x_j \neq 0$ entonces

$$0 = z_1 + z_2 + \ldots + z_m,\ z_k \neq 0, \quad k = 1, 2, \ldots, m, \quad m \leq n$$

$$\text{luego } -z_1 = z_2 + z_3 + \ldots + z_m$$

Denotemos $y = -z_1$ entonces $y = -z_1$, $y = z_2 + z_3 + \ldots + z_m$, luego $y \neq 0$ tiene 2 representaciones lo cual contradice a la definicion 1.2.

Por lo tanto, no existe otra representación distinta de (1.2) entonces $x_j = 0$, $j = 1, 2, \ldots, n$, luego $\quad 0 = 0 + 0 + \ldots + 0$ es única.

Reciprocamente,

Sea $x = x_1 + x_2 + \ldots + x_n$ de manera única. Si $x \neq 0$ entonces $x = y_1 + y_2 + \ldots + y_m$, $m \leq n$ donde y_i es alguno de los x_j, con $y_i \neq 0$, $i = 1, 2, \ldots, m$, $j = 1, 2, \ldots, n$. Luego por definición 1.2, $G = G_1 \oplus G_2 \oplus \ldots \oplus G_n$. $\square$

Observaciones:

1. Si $G = \bigoplus_{i \in I} G_i$, entonces para cualesquiera $i, j \in I, \quad i \neq j : \quad G_i \cap G_j = \{0\}$.
   En efecto, si $x \in G_i \cap G_j$ y $x \neq 0$, entonces x se puede expresar como $x = x_1$ y $x = x_2$, donde $x_1 \in G_i$ y $x_2 \in G_j$, lo cual contradice la definición de suma directa.

2. Si $G = H \oplus K$ y $K = M \oplus N$, entonces $G = H \oplus M \oplus N$

Los siguientes teoremas nos ofrecen un criterio simple para determinar si un grupo es la suma directa de una familia de subgrupos.

Teorema 1.3 *Sean $G_1, G_2, \ldots, G_n$ subgrupos de G.*
$G = G_1 \oplus G_2 \oplus \ldots \oplus G_n$ si y solo si $G = G_1 + G_2 + \ldots + G_n$ y $\forall x_i \in G_i, \quad i = 1, 2, \ldots, n$: $x_1 + x_2 + \ldots + x_n = 0$ implica $x_i = 0, \quad i = 1, 2, \ldots, n$.

Demostración:

Supongamos que $G = G_1 \oplus G_2 \oplus \ldots \oplus G_n$.

Sean $x_i \in G_i, \quad i = 1, 2, \ldots, n$ arbitrarios. Si $x_1 + x_2 + \ldots + x_n = 0$, como $0 \in G$ luego por el teorema 1.2:

$$0 = \underbrace{0 + 0 + \ldots + 0}_{n \text{ sumandos}} \text{ de manera única}$$

Entonces $x_i = 0, \quad i = 1, 2, \ldots, n$.

Reciprocamente,

Supongamos que $G = G_1 + G_2 + \ldots + G_n$ y $\forall x_i \in G_i, \quad i = 1, 2, \ldots, n$:
$x_1 + x_2 + \ldots + x_n = 0$ implica $x_i = 0, \quad i = 1, 2, \ldots, n$.

Sea $x \in G$ arbitrario, entonces existen $x_i \in G_i, \quad i = 1, 2, \ldots, n$ tales que

$$x = x_1 + x_2 + \ldots + x_n$$

Por el teorema 1.2, es suficiente demostrar que esta expresión esúnica.

Sea $x = y_1 + y_2 + \ldots + y_n$ otra representación de x, donde $y_i \in G_i$, $i = 1, 2, \ldots, n$ entonces $(y_1 - x_1) + (y_2 - x_2) + \ldots + (y_n - x_n) = 0$ luego por hipotesis $y_i - x_i = 0, \quad i = 1, 2, \ldots, n$.
Por lo tanto $y_i = x_i, \quad i = 1, 2, \ldots, n$. $\square$

Aplicando el mismo argumento de la demostración anterior se obtiene el siguiente resultado.

Teorema 1.4 *Sea $(G_i) i \in I$ una familia de subgrupos de G.*
$G = \bigoplus_{i \in I} G_i$ si y solo si $G = \sum_{i \in I} G_i$ y para cualesquiera elementos distintos $i_1, i_2, \ldots, i_m$ de I y $\forall x_j \in G(i_j), \quad j = 1, 2, \ldots, m$:
$x_1 + x_2 + \ldots + x_m = 0$ implica $x_j = 0, \quad j = 1, 2, \ldots, m$. $\square$

Teorema 1.5 *Sean $(G_i)_{i \in I}$ una familia de subgrupos de G.*
Entonces, $G = \bigoplus_{i \in I} G_i$ si y solo si $G = \sum_{i \in I} G_i$ y $G_j \cap \sum_{i \neq j} G_i = \{0\}$ para todo $j \in I$

Demostración:

Supongamos que $G = \bigoplus_{i\in I} G_i$ entonces por definición 1.2 $\quad G = \sum_{i\in I} G_i$.

Sea $j \in I$ arbitrario.

Consideremos $x \in G_j \cap \sum_{i\neq j} G_i$ entonces $x \in G_j$ y $x = x_1 + x_2 + \ldots + x_m$ donde $x_k \in G(i_k)$, $k = 1, 2, \ldots, m$ siendo $i_1, i_2, \ldots, i_m \in I - \{j\}$ distintos. Luego

$$x_1 + x_2 + \ldots + x_m + (-x) = 0$$

entonces de acuerdo con el teorema 1.4, se obtiene en particular que $x = 0$.

En consecuencia $\quad G_j \cap \sum_{i\neq j} G_i = \{0\}$ para todo $j \in I$.

Reciprocamente,

Supongamos que $G = \sum_{i\in I} G_i \quad$ y que $\quad G_j \cap \sum_{i\neq j} G_i = \{0\} \quad$ para todo $j \in I$

Si $x_1 + x_2 + \ldots + x_n = 0$ donde $x_j \in G(i_j)$, $\quad j = 1, 2, \ldots, n$

y $i_1, i_2, \ldots, i_n$ son elementos distintos de I, entonces

$-x_j = x_1 + x_2 + \ldots + x_{j-1} + x_{j+1} + \ldots + x_n$ es un elemento de $G(i_j) \cap \sum_{i\neq i_j} G_i \quad$ y por lo tanto $x_j = 0$, $\quad j = 1, 2, \ldots, n$. Luego por el teorema 1.4 $\quad G = \bigoplus_{i\in I} G_i \quad \square$

Ahora, si $G_1, G_2, \ldots, G_n$ son grupos abelianos. ¿Existe un grupo G que sea la suma directa de imagenes isomorfas de los grupos $G_1, G_2, \ldots, G_n$?.

El siguiente teorema nos responde afirmativamente.

Teorema 1.6 *Si $G_1, G_2, \ldots, G_n$ son grupos abelianos cualesquiera, entonces existe un grupo abeliano G que es una suma directa de imagenes isomorfas de $G_1, G_2, \ldots, G_n$.*

Demostración:

Sea G la suma directa (externa) de los grupos $G_1, G_2, \ldots, G_n$ y sean

$H_1 = \{(x_1, 0, 0 \ldots, 0)/x_1 \in G_1\}$, $\quad H_2 = \{(0, x_2, 0, \ldots, 0)/x_2 \in G_2\}, \ldots,$

$H_n = \{(0, 0, 0, \ldots, 0, x_n)/x_n \in G_n\}$.

Entonces H_i es un subgrupo de G y $H_i \approx G_i$, $\quad i = 1, 2, \ldots, n$. Es claro que todo elemento $(x_1, x_2, \ldots, x_n)$ de G se expresa de manera única como

$$(x_1, 0, 0, \ldots, 0) + (0, x_2, 0, \ldots, 0) + \ldots + (0, 0, 0, \ldots, 0, x_n).$$

Por lo tanto

$$G = H_1 \oplus H_2 \oplus \ldots \oplus H_n. \quad \square$$

Un resultado importante que demostraremos más adelante establece que si G es la suma directa de $G_1, G_2, \ldots, G_n$ y H es la suma directa de $H_1, H_2, \ldots, H_n$, donde $G_i \approx H_i$, $i = 1, 2, \ldots, n$, entonces $G \approx H$.

Teorema 1.7 *Si $(G_i)_{i \in I}$ es una familia de grupos abelianos arbitraria, entonces existe un grupo abeliano G que es la suma directa de una familia de subgrupos $(H_i)_{i \in I}$, donde $H_i \approx G_i$ para todo $i \in I$.*

Demostración:

Sea G la suma directa (externa) de la familia de grupos $(G_i)_{i \in I}$. Un elemento x de G es una función de I en la unión de $(G_i)_{i \in I}$ que satisface la siguiente condición:

$x(i) \in G_i$ para todo $i \in I$ y $\{i \in I \;/\; x(i) \neq 0\}$es finito (posiblemente $\emptyset$).

Definimos la adición en G de la manera usual:

$$(x + y)(i) \;=\; x(i) + y(i), \quad i \in I$$

para cualesquiera $x, y \in G$. Como

$$\{i \in I \;/\; (x + y)(i) \neq 0\} \subset \{i \in I \;/ x(i) \neq 0\} \cup \{i \in I \;/ y(i) \neq 0\}$$

entonces $\{i \in I \;/\; (x + y)(i) \neq 0\}$ es finito y por lo tanto $x + y \in G$,

puesto que$(x + y)(i) = x(i) + y(i) \in G_i$ para todo $i \in I$.

Es claro que esta adición en G es asociativa. El elementoneutro es la función $w \in G$ definida por $w(i) = 0 \in G_i$ para todo $i \in I$. El opuesto de $x \in G$ es la función $-x$ definida por $(-x)(i) = -x(i)$ para cada $i \in I$.

Además $x + y = y + x$ para cualesquiera $x, y \in G$.

Por lo tanto G con la adición antes definida es un grupo abeliano.

Ahora, para cada $i \in I$, sea

$$H_i = \{x \in G \; / \; x(j) = 0 \in G_j \text{ para todo } j \in I, \; j \neq i\}.$$

Es claro que $w \in H_i$ (w es el cero de G) y así $H_i \neq \emptyset$.

Además, si x, y son elementos cualesquiera de H_i, entonces

$$(x - y)(j) = x(j) - y(j) = 0 - 0 = 0 \text{ para todo } j \in I, \quad j \neq i$$

Luego H_i es un subgrupo de G.

Veamos que $H_i \approx G_i$ para todo $i \in I$.

Definamos $f_i : H_i \longrightarrow G_i$ por $f_i(x) = x(i)$, $\quad x \in H_i$. Si $x, y \in H_i$ y $f_i(x) = f_i(y)$, entonces $x(i) = y(i)$. Además $x(j) = 0 = y(j)$ para todo $j \in I$, $\quad j \neq i$.

Luego $x = y$. Por lo tanto f_i es inyectiva. Ahora veamos que f_i es sobreyectiva.

Sea $a \in G_i$ arbitrario.

Definamos la función x de I en $\bigcup\{G_j / j \in I\}$ por $x(i) = a$ y $x(j) = 0 \in G_j$ si $j \neq i$.

Entonces $x \in H_i$ y $f_i(x) = x(i) = a$. Luego f_i es sobreyectiva. Además, f_i es un homomorfismo pues si x, $y \in H_i$, entonces

$$f_i(x + y) = (x + y)(i) = x(i) + y(i) = f_i(x) + f_i(y).$$

Por consiguiente f_i es un isomorfismo.

Finalmente demostraremos que

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

Sea $x \in G$ arbitrario. Si $x = 0$, entonces

$$x = x_1 + x_2 + \ldots + x_m$$

donde cada x_j es el cero de algún $H(i_j)$. Si $x \neq 0$, entonces existen elementos distintos $i_1, i_2, \ldots, i_m$ de I tales que $x(i_j) \neq 0$, $\quad j = 1, 2, \ldots, m$, y $x(i) = 0$ para todo i que no pertenece a $\{i_1, i_2 \ldots, i_m\}$.

Sean $x_1 \in H(i_1)$, $x_2 \in H(i_2)$, $\ldots, x_m \in H(i_m)$ tales que $x_j(i_j) = x(i_j)$, $j = 1, 2, \ldots, m$. Es claro que

$$x = x_1 + x_2 + \ldots + x_m$$

Supongamos que $i_1, i_2, \ldots, i_m$ son elementos distintos de I y que $x_1 \in H(i_1), x_2 \in H(i_2)$, $x_3 \in H(i_3), \ldots, x_m \in H(i_m)$ son tales que $x_1 + x_2 + \ldots + x_m = w$ (el cero de G). Entonces para cada $j \in \{1, 2, \ldots, m\}$:

$$x_j(i_j) = (x_1 + x_2 + \ldots + x_m)(i_j) = w(i_j) = 0.$$

Se sigue que $x_j = w$, $\quad j = 1, 2, \ldots, m$. Por consiguiente G es la suma directa de la familia $(H_i)_{i \in I}$. $\square$

1.4. Propiedad de Extensión Homomórfica

La propiedad de extensión homomórfica de las sumas directas nos conducirá a un concepto muy importante que es el de **Grupo Abeliano Libre.**
Establecemos ésta propiedad de extensión en dos teoremas, en primer lugar para una suma directa finita y en seguida para una suma directa arbitraria.

Teorema 1.8 *Sean $G = G_1 \oplus G_2 \oplus \ldots \oplus G_n$ y H un grupo abeliano cualquiera. Si $f_i : G_i \to H$, $\quad i = 1, 2, \ldots, n$ son homomorfismos, entonces existe un homomorfismo $f : G \to H$ tal que la restricción de f a G_i es f_i, $\quad i = 1, 2, \ldots, n$.*
Es decir $f\,|_{G_i} = f_i$, $\quad i = 1, 2, \ldots, n$.

Demostración:
Como cada $x \in G$ se puede expresar de manera única como $x = x_1 + x_2 + \ldots + x_n$ donde $x_i \in G_i$, $\quad i = 1, 2, \ldots, n$, entonces se puede definir:

$$f(x) = f_1(x_1) + f_2(x_2) + \ldots + f_n(x_n) \tag{1.3}$$

Dada la unicidad de la expresión para x, se concluye que $f\,|_{G_i} = f_i$, $\quad i = 1, 2, \ldots, n$.
Veamos que f es un homomorfismo.

Sean $x, y \in G$ arbitrarios, entonces existen $x_i,\ y_i \in G_i,\quad i = 1, 2, \ldots, n$ únicos tales que:

$$x = x_1 + x_2 + \ldots + x_n$$

$$y = y_1 + y_2 + \ldots + y_n$$

Por lo tanto, la expresión:
$x + y = (x_1 + y_1) + (x_2 + y_2) + \ldots + (x_n + y_n)$ es única y de (1.3) tenemos:

$$\begin{aligned} f(x+y) &= \sum_{i=1}^{n} f_i(x_i + y_i) = \sum_{i=1}^{n}[f_i(x_i) + f_i(y_i)] \\ &= \sum_{i=1}^{n} f_i(x_i) + \sum_{i=1}^{n} f_i(y_i) \\ &= f(x) + f(y) \end{aligned}$$

Luego f es un homomorfismo.

El mismo argumento de la demostración anterior se utiliza para demostrar la forma general de la propiedad de extensión homomórfica que a continuación enunciamos solamente.

Teorema 1.9 *Sea $G = \bigoplus_{i \in I} G_i$ y H un grupo abeliano cualquiera.*
Si para cada $i \in I \quad f_i : G_i \to H$ es un homomorfismo, entonces existe un homomorfismo $f : G \to H$ tal que $f\,|_{G_i} = f_i$ para todo $i \in I$. $\square$

Aplicando ésta propiedad de extensión homomorfica se obtiene un resultado importante, el cual establecemos en el siguiente ejemplo.

Ejemplo:

"H es un sumando directo de G si y solamente si existe un epimorfismo f de G sobre H tal que $f\,|_H = id_H$".

En efecto, si H es sumando directo de G, entonces existe un subgrupo K de G tal que $G = H \oplus K$.

Sea $f_1 = id_H$ y f_2 el homomorfismo nulo de K en H. De acuerdo con la propiedad de extensión homomórfica, existe un homomorfismo $f : G \to H$ tal que

$f\mid_H = f_1 = id_H$ y $f\mid_K = f_2 = 0$.

Como $H = f_1(H) = f(H) \subset f(G) \subset H$ entonces $f(G) = H$. Por lo tanto $f : G \to H$ es un epimorfismo tal que $f\mid_H = id_H$.

Recíprocamente,

Si existe un epimorfismo f de G sobre H tal que $f\mid_H = id_H$, entonces considerando $K = Kerf$, $x \in G$ arbitrario y denotando $h = f(x)$ se tiene que:

$$f(x-h) = f(x) - f(h) = f(x) - id_H(h) = f(x) - h = 0$$

De este modo $x - h \in Kerf = K$ y por lo tanto $x \in H + K$.

Tenemos así, que $G = H + K$. Además, si $x \in H \cap K$ entonces $x \in H$ y $x \in K$ luego $x = id_H(x) = f(x) = 0$. Por lo tanto $H \cap K = \{0\}$ y en consecuencia $G = H \oplus K$ y H es un sumando directo de G. $\square$

Teorema 1.10 *Sean G y H grupos abelianos, $(G_i)_{i\in I}$ y $(H_i)_{i\in I}$ familias de subgrupos de G y de H respectivamente. Si $G = \bigoplus_{i\in I} G_i$, $H = \bigoplus_{i\in I} H_i$ y $G_i \approx H_i$ para todo $i \in I$, entonces $G \approx H$.*

Demostración:

Para cada $i \in I$, existe un isomorfismo $f_i : G_i \to H_i$. Por la propiedad de extensión homomórfica, existe un homomorfismo $f : G \to H$ tal que $f\mid_{G_i} = f_i$ para todo $i \in I$.

Sea $h \in \bigcup_{i\in I} H_i$ cualquiera. Entonces existe $j \in I$ tal que $h \in H_j = f_j(G_j)$, luego $h = f_j(x) = f(x)$ para algún $x \in G_j \subset G$. Se sigue que $\bigcup_{i\in I} H_i \subset f(G)$. Por lo tanto

$$H = \sum_{i\in I} H_i = \left[\bigcup_{i\in I} H_i\right] \subset f(G) \subset H$$

y en consecuencia $f(G) = H$, es decir, f es sobreyectiva.

Solamente falta demostrar que $Kerf = \{0\}$.

Sea $x \in Kerf$ cualquiera. Supongamos que $x \neq 0$, entonces existen $i_1, i_2, \ldots, i_n \in I$ distintos y $x_j \in G(i_j) - \{0\}$, $j = 1, 2, \ldots, n$ tales que $x = x_1 + x_2 + \ldots + x_n$. Luego

$$f_{i(1)}(x_1) + f_{i(2)}(x_2) + \ldots + f_{i(n)}(x_n) = f(x) = 0$$

donde $i(j) = i_j, \quad j = 1, 2, \ldots, n$.

De acuerdo con el teorema 1.4 $f_{i(j)}(x_j) = 0, \quad j = 1, 2, \ldots n$. Como $f_{i(j)}$ es un isomorfismo (en particular, su núcleo es trivial), entonces $x_j = 0, \quad j = 1, 2, \ldots, n$ lo cual es una contradicción.

Por consiguiente $Ker f = \{0\}$. Se concluye así que $G \approx H$. $\square$

Capítulo 2

Grupos Abelianos Libres

En esta sección trataremos acerca de los grupos abelianos libres.
Se caracterizará los grupos abelianos libres como sumas directas de grupos isomorfos a $\mathbb{Z}$. Además se demostrará que todo grupo abeliano es cociente de un grupo abeliano libre.
De la propiedad de extensión homomórfica se obtiene el siguiente teorema, el cual conduce al concepto de una clase importante de grupos, que son los llamados grupos abelianos libres.

Teorema 2.1 *Si $G = \bigoplus_{i\in I} [a_i]$, donde cada $a_i \in G$ es de orden infinito (es decir, $[a_i]$ es un grupo cíclico infinito, y por lo tanto isomorfo a $\mathbb{Z}$, para todo $i \in I$) y $X = \{a_i / i \in I\}$, entonces para cualquier grupo abeliano H y para cualquier aplicación $\varphi : X \to H$, existe un homomorfismo $f : G \to H$, tal que $f\mid_X = \varphi$.*

Demostración:
Para cualquier $i \in I$, definimos $f_i : [a_i] \to H$ de la siguiente manera:

$$f_i(ka_i) = k\varphi(a_i) \qquad (k \in \mathbb{Z})$$

Para cualesquiera $ka_i,\ ma_i \in [a_i]$, $(k, m \in \mathbb{Z})$ se verifica:
$f_i(ka_i + ma_i) = f_i((k+m)a_i) = (k+m)\varphi(a_i) = k\varphi(a_i) + m\varphi(a_i) = f_i(ka_i) + f_i(ma_i)$.
Entonces f_i es un homomorfismo de $[a_i]$ en H. De acuerdo con la propiedad de extensión

homomórfica, existe un homomorfismo $f : G \to H$ tal que $f\mid_{[a_i]} = f_i$ para todo $i \in I$. Luego para cualquier $a_i \in X$:

$$f(a_i) = f_i(a_i) = f_i(1a_i) = 1\varphi(a_i) = \varphi(a_i)$$

Por lo tanto $f\mid_X = \varphi$. $\square$

2.1. Concepto de Grupo Abeliano Libre

Definición 2.1 *Se dice que G es un grupo abeliano libre si existe un subconjunto X de G que satisface las siguientes condiciones:*

(a) $G = [X]$

(b) Para cualquier grupo abeliano H y cualquier aplicación $\varphi : X \to H$, existe un homomorfismo $f : G \to H$ tal que $f\mid_X = \varphi$.

En este caso se dice que G es generado libremente por X y que X es una base de G.
Observación: La condición (b) de la definición anterior es llamada la **Propiedad Universal de los Grupos Abelianos Libres**.
De acuerdo, con el teorema anterior, cualquier suma directa de grupos cíclicos infinitos es un grupo abeliano libre. La recíproca también es valida.

Teorema 2.2 *Si G es un grupo abeliano libre y $X = \{x_i / i \in I\}$ es una base de G, entonces $G = \bigoplus_{i\in I} [x_i]$, donde $[x_i]$ es cíclico infinito para todo $i \in I$.*

Demostración:
Consideramos la siguiente familia de grupos indizada por $I : (K_i)_{i\in I}$, donde $K_i = \mathbb{Z}$ para todo $i \in I$.
Por el teorema 1.7 existe un grupo abeliano H y una familia $(H_i)_{i\in I}$ de subgrupos de H tales que $H = \bigoplus_{i\in I} H_i$ y $H_i \approx K_i$ para todo $i \in I$. Entonces H_i es cíclico infinito para todo $i \in I$ y por lo tanto para todo $i \in I$ existe $y_i \in H$ tal que $H_i = [y_i]$ y $o(y_i) = \infty$.
Sea $\varphi : X \to H$ definida por $\varphi(x_i) = y_i, \quad i \in I$.

Como G es generado libremente por X, entonces existe un homomorfismo $f : G \to H$ tal que $f\mid_X = \varphi$.

Por otra parte $H = \bigoplus_{i \in I} [y_i]$. De acuerdo con la demostración del teorema 2.1

$Y = \{y_i / i \in I\}$ es una base de H. Entonces la aplicación $\lambda : Y \to G$ definida por $\lambda(y_i) = x_i, \quad i \in I$, puede extenderse a un homomorfismo $g : H \to G$.

Es evidente que:

$$\lambda \circ \varphi = id_X \quad \text{y} \quad \varphi \circ \lambda = id_Y$$

Veamos que $\quad g \circ f = id_G$:

Sea $x \in G$ arbitrario. Entonces $\quad x = n_1 a_1 + n_2 a_2 + \ldots + n_r a_r$ para algunos $a_j \in X$, $n_j \in \mathbb{Z}$, $\quad j = 1, 2, \ldots, r$. luego

$$\begin{aligned} g(f(x)) &= g(\sum_{j=1}^{r} n_j f(a_j)) \\ &= g(\sum_{j=1}^{r} n_j \varphi(a_j)) \\ &= \sum_{j=1}^{r} n_j g(\varphi(a_j)) \\ &= \sum_{j=1}^{r} n_j \lambda(\varphi(a_j)) \\ &= \sum_{j=1}^{r} n_j a_j \\ &= x \end{aligned}$$

Similarmente se verifica que $f \circ g = id_H$. En concecuencia, f y g son isomorfismos, cada uno inverso del otro.

Finalmente, como $H = \bigoplus_{i \in I} [y_i]$, g es un isomorfismo y $[x_i] \approx [y_i]$ (puesto que $[x_i] = [g(y_i)] = g([y_i])$) para todo $i \in I$, entonces por el teorema 1.7 $G = \bigoplus_{i \in I} [x_i]$ donde $[x_i]$ es cíclico infinito para todo $i \in I$. $\square$

2.2. Caracterización de los Grupos Abelianos Libres

Corolario. G es un grupo abeliano libre si y solo si es una suma directa (finita ó infinita) de grupos isomorfos a $\mathbb{Z}$.

Consecuencia de la Propiedad Universal de los Grupos Abelianos Libres

Teorema 2.3 *Todo grupo abeliano es isomorfo a un grupo cociente de algun grupo abeliano libre.*

Demostración:

Sea G un grupo abeliano arbitrario. Indizando los elementos de G, podemos escribir: $G = \{y_i/i \in I\}$. Consideramos la familia de grupos $(G_i)_{i\in I}$, donde $G_i = \mathbb{Z}$ para todo $i \in I$ (el conjunto de indices es el mismo que se ha utilizado para indizar los elementos de G).

Por el teorema 1.7, existe un grupo abeliano F y una familia $(F_i)_{i\in I}$ de subgrupos de F tal que $F_i \approx G_i$ (y por lo tanto F_i es cíclico infinito) para todo $i \in I$ y $F = \bigoplus_{i\in I} F_i$. Para cada $i \in I$, existe $x_i \in F$ tal que $F_i = [x_i]$. Por el teorema 2.1 F es un grupo abeliano libre y $X = \{x_i/i \in I\}$ es una base de F, luego la aplicación $\varphi : X \to G$ definida por $\varphi(x_i) = y_i$ se puede extender a un homomorfismo $f : F \to G$ tal que $f\mid_X = \varphi$. Denotemos $K = Ker f$. Como φ es sobreyectiva, entonces f es un epimorfismo. Luego por el primer teorema de isomorfismos, $G \approx F/K$ (grupo cociente del grupo abeliano libre F). □

2.3. Ejemplos de Grupos Abelianos Libres

1. Sea G un grupo abeliano libre y X una base de G. Si X tiene n elementos, entonces todo elemento de G tiene una representación única de la forma:

$$k_1x_1 + k_2x_2 + \ldots + k_nx_n \tag{2.1}$$

donde $k_i \in \mathbb{Z}$, $\quad x_i \in X$, $\quad i = 1, 2, \ldots, n$.

En efecto, $G = [x_1] \oplus [x_2] \oplus \ldots \oplus [x_n]$ donde $X = \{x_1, x_2, \ldots, x_n\}$, de acuerdo con el teorema 1.2 entonces cada elemento de G tiene una representación única $y_1 + y_2 + \ldots + y_n$ donde $y_i \in [x_i]$, $i = 1, 2, \ldots, n$. Además, $[x_i]$ es cíclico infinito, $i = 1,2,\ldots,n$. Por la teoría de los grupos cíclicos infinitos, $y_i = k_i x_i$, donde $k_i \in \mathbb{Z}$, de manera única. Por consiguiente todo elemento de G tiene una única representación de la forma (2.1).

2. Sea G un grupo abeliano libre y X una base de G con n elementos, entonces

$$G \approx \mathbb{Z}^n = \mathbb{Z} \times \mathbb{Z} \times \ldots \times \mathbb{Z} \text{ (n factores)}$$

En efecto, $G = [x_1] \oplus [x_2] \oplus \ldots \oplus [x_n]$ donde

$$X = \{x_1, x_2, \ldots, x_n\} \text{ y } o(x_i) = \infty, \quad i = 1, 2, \ldots, n$$

entonces $G \approx [x_1] \times [x_2] \times \ldots \times [x_n]$ y cada $[x_i] \approx \mathbb{Z}$, $i = 1, 2, \ldots, n$ pues $\mathbb{Z}$ es el único grupo cíclico infinito, salvo isomorfismo.
Por consiguiente

$$G \approx \mathbb{Z}^n = \mathbb{Z} \times \mathbb{Z} \times \ldots \times \mathbb{Z}(\text{ n factores })$$

3. Sea G un grupo abeliano libre con base

$$X = \{x_1, x_2, \ldots, x_n\}$$

Si $y_1 = x_1 + k_2x_2 + k_3x_3 + \ldots + k_nx_n$ donde $k_2, k_3, \ldots, k_n$ son enteros arbitrarios, entonces $Y = \{y_1, x_2, \ldots, x_n\}$ tambien es una base de G.
En efecto, de la hipotesis $G = [y_1, x_2, x_3, \ldots, x_n] = [y_1] + [x_2] + [x_3] \ldots + [x_n]$
Sean $t_1, t_2, \ldots, t_n$, enteros arbitrarios tales que

$$t_1y_1 + t_2x_2 + t_3x_3 \ldots + t_nx_n = 0 \tag{2.2}$$

Como $y_1 = x_1 + k_2x_2 + k_3x_3 \ldots + k_nx_n$ entonces sustituyendo en (2.2) tenemos:

$$t_1x_1 + (t_1k_2 + t_2)x_2 + (t_1k_3 + t_3)x_3 + \ldots + (t_1k_n + t_n)x_n = 0$$

Además $G = [x_1] \oplus [x_2] \oplus \ldots \oplus [x_n]$ donde x_i es de orden infinito, $i = 1, 2, \ldots, n$ entonces por el teorema 1.3

$$t_1 x_1 = 0, \ (t_1 k_2 + t_2) x_2 = 0, \ (t_1 k_3 + t_3) x_3 = 0, \ldots, (t_1 k_n + t_n) x_n = 0$$

Como cada x_i es de orden infinito, $i = 1, 2, \ldots, n$. Por lo tanto

$$t_1 = 0, \ t_1 k_2 + t_2 = 0, \ t_1 k_3 + t_3 = 0, \ldots, t_1 k_n + t_n = 0$$

Por consiguiente

$$t_1 = t_2 = t_3 = \ldots = t_n = 0$$

Luego $Y = \{y_1, x_2, \ldots, x_n\}$ tambien es una base de G. □

Capítulo 3

Grupos de Torsión, Grupos p-Prüfer y Grupos Divisibles

3.1. El Subgrupo de Torsión de un Grupo Abeliano

Dado cualquier grupo abeliano G, el conjunto

$$T(G) = \{a \in G/o(a) \text{ esfinito}\}$$

es un subgrupo de G. En efecto, si a, $b \in T(G)$, $o(a) = m$ y $o(b) = n$ entonces

$$mn(a - b) = n(ma) - m(nb) = 0 - 0 = 0$$

y por lo tanto $o(a - b)$ es finito. Además, como $e \in T(G)$ entonces $T(G) \neq \emptyset$. Por consiguiente $T(G)$ es un subgrupo de G.

Definición 3.1 *Sea G un grupo abeliano. El subgrupo*

$$T(G) = \{a \in G/o(a) \text{ es finito }\}$$

es llamado el subgrupo de torsión de G.

Ejemplos:

1. El subgrupo de torsión del grupo aditivo $\mathbb{Q}$ es

$$T(\mathbb{Q}) = \{0\}$$

puesto que para cualquier $m \in \mathbb{Z}^+$ y para cualquier $r \in \mathbb{Q}$:

$$mr = 0 \text{ implica } r = 0$$

2. El subgrupo de torsión del grupo aditivo $\mathbb{Q}/\mathbb{Z}$ es

$$T(\mathbb{Q}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$$

En efecto: Si $r = m/n \in \mathbb{Q}$, donde $m, n \in \mathbb{Z}$ y $n > 0$, entonces

$$n(r + \mathbb{Z}) = nr + \mathbb{Z} = m + \mathbb{Z} = \mathbb{Z}$$

y por lo tanto $r + \mathbb{Z}$ es de orden finito.

3. El subgrupo de torsión del grupo aditivo $\mathbb{R}/\mathbb{Z}$ es

$$T(\mathbb{R}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$$

En efecto, si $x + \mathbb{Z} \in T(\mathbb{R}/\mathbb{Z})$ y $o(x + \mathbb{Z}) = n$ entonces

$$nx + \mathbb{Z} = n(x + \mathbb{Z}) = \mathbb{Z}$$

Luego $nx \in \mathbb{Z}$ y por lo tanto $x = (nx)/n \in \mathbb{Q}$, de manera que $x + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$.
Recíprocamente,
Si $r + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$ donde $r = m/n$ $(m, n \in \mathbb{Z}$ y $n > 0)$ entonces

$$n(r + \mathbb{Z}) = nr + \mathbb{Z} = m + \mathbb{Z} = \mathbb{Z}$$

y por lo tanto $r + \mathbb{Z}$ es de orden finito, es decir $r + \mathbb{Z} \in T(\mathbb{R}/\mathbb{Z})$.

Teorema 3.1 *Para cualquier subgrupo H de G:*

$$T(H) = H \cap T(G).$$

Demostración:

Si $a \in T(H)$ entonces $a \in H$ y a es de orden finito, es decir $a \in H \cap T(G)$.

Recíprocamente,

si $a \in H \cap T(G)$ entonces $a \in H$ y a es de orden finito, es decir $a \in T(H)$. $\square$

Teorema 3.2 *Si $G = \bigoplus_{i\in I} G_i$, donde $(G_i)_{i\in I}$ es una familia de subgrupos de G, entonces $T(G) = \bigoplus_{i\in I} T(G_i)$*

Demostración:

Como $T(G_i) = G_i \cap T(G)$ para todo $i \in I$, de acuerdo con el teorema 3.1 entonces $T(G_i)$ es un subgrupo de $T(G)$ para todo $i \in I$.

Sea $x \in T(G)$, $x \neq 0$ arbitrario. Como $x \in G$, $x \neq 0$ y $G = \bigoplus_{i\in I} G_i$, entonces existen $i_1, i_2, \ldots, i_n \in I$ distintos y existen $x_j \in G(i_j)$, $x_j \neq 0$ $j = 1, 2, \ldots, n$ tal que

$$x = x_1 + x_2 + \ldots + x_n \tag{3.1}$$

siendo ésta representación única.

Sea $k = o(x)$. Entonces

$$kx_1 + kx_2 + \ldots + kx_n = kx = 0$$

Luego por el teorema 1.4 $kx_j = 0$, $\quad j = 1, 2, \ldots, n$.

Por lo tanto $x_j \in T(G)$, $j = 1, 2, \ldots, n$ y así $x_j \in T(G(i_j))$ $j = 1, 2, \ldots, n$.

Por consiguiente $T(G) = \bigoplus_{i\in I} T(G_i)$ en virtud de la unicidad de la representación (3.1). $\square$

3.2. Grupos de Torsión, Grupos sin Torsión y Grupos Mixtos

Consideremos los grupos abelianos siguientes:

1. El grupo aditivo de los números racionales $\mathbb{Q}$

2. El grupo cociente aditivo $\mathbb{Q}/\mathbb{Z}$

3. El grupo multiplicativo de los numeros complejos no nulos $\mathbb{C} - \{0\}$

Como $T(\mathbb{Q}) = \{0\}$ y $T(\mathbb{Q}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$ entonces $\mathbb{Q}$ y $\mathbb{Q}/\mathbb{Z}$ no son isomorfos.
Por otro lado, como $T(\mathbb{C} - \{0\}) \neq \{1\}$ (puesto que $o(i) = 4$, por ejemplo)
y $T(\mathbb{C} - \{0\}) \neq \mathbb{C} - \{0\}$ (puesto que $o(2) = \infty$, por ejemplo)
entonces, los grupos abelianos $\mathbb{Q}$, $\mathbb{Q}/\mathbb{Z}$ y $\mathbb{C} - \{0\}$ no son isomorfos.
Una primera clasificación de los grupos abelianos es la siguiente:
Grupos de torsión, Grupos sin torsión y Grupos mixtos de acuerdo a las definiciones que siguen:

Grupos de Torsión

Definición 3.2 *G es llamado un grupo de torsión, si $T(G) = G$. Es decir, si todo elemento de G es de orden finito.*

Ejemplos:

(1) Como $T(\mathbb{Q}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$, entonces $\mathbb{Q}/\mathbb{Z}$ en un grupo de torsión.

(2) Todo grupo abeliano finito es un grupo de torsión, pues todo elemento de G es de orden finito y con lo cual $T(G) = G$.

Grupos sin Torsión

Definición 3.3 *G es llamado un grupo sin torsión, si $T(G) = \{0\}$. Es decir, si el único elemento de G de orden finito es el* 0.

Ejemplos:

(1) Los grupos aditivos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ son grupos sin torsión.

(2) El grupo multiplicativo $\mathbb{R}^+$ es isomorfo al grupo aditivo $\mathbb{R}$.
(Un isomorfismo de $\mathbb{R}^+$ sobre $\mathbb{R}$ es Ln, la función logaritmo en base e).
Por lo tanto $\mathbb{R}^+$ es un grupo sin torsión.

Grupos Mixtos:

Definición 3.4 *G es llamado un grupo mixto, si $\{0\} \neq T(G) \neq G$.*

Ejemplos:

(1) El grupo multiplicativo $\mathbb{C} - \{0\}$ es mixto, pues $\{1\} \neq T(\mathbb{C} - \{0\}) \neq \mathbb{C} - \{0\}$.

(2) Los grupos multiplicativos $\mathbb{Q} - \{0\}$, $\mathbb{R} - \{0\}$ son mixtos, pues

$T(\mathbb{Q} - \{0\}) = \{1, -1\}, \qquad T(\mathbb{R} - \{0\}) = \{1, -1\}$

(3) El grupo cociente $\mathbb{R}/\mathbb{Z}$ es mixto, pues $\{0\} \neq T(\mathbb{R}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z} \neq \mathbb{R}/\mathbb{Z}$

Teorema 3.3 *(a) $G/T(G)$ es un grupo sin torsión.*

(b) $T(G)$ es el menor subgrupo de G talque $G/T(G)$ es sin torsión.

Demostración:

(a) Sea $x + T(G) \in G/T(G)$ de orden finito n. Entonces

$$nx + T(G) = n(x + T(G)) = 0 + T(G)$$

luego $nx \in T(G)$, es decir nx es de orden finito. Sea $m = o(nx)$ entonces $m(nx) = 0$, pero $m(nx) = (mn)x$ luego $(mn)x = 0$. Esto implica que x es de orden finito, osea $x \in T(G)$. Por lo tanto

$$x + T(G) = 0 + T(G)$$

Por consiguiente el único elemento de $G/T(G)$ que es de orden finito es $0 + T(G)$ (el cero de $G/T(G)$), esto es $G/T(G)$ es un grupo sin torsión.

(b) Supongamos que H es un subgrupo de G tal que G/H es sin torsion.

Demostraremos que $T(G) \subset H$.

En efecto, sea $x \in T(G)$ arbitrario. Entonces x es de orden finito.

Luego $x+H$ es de orden finito, puesto que $x+H$ es la imagen de x bajo el homomorfismo canónico de G sobre G/H. Ahora, como G/H es sin torsión entonces $x + H = 0 + H$ y por lo tanto $x \in H$. Se concluye así que $T(G) \subset H$. $\square$

3.3. Estructura de los Grupos de Torsión

Demostraremos que el estudio de los grupos de torsión se reduce al estudio de los grupos primarios.

Grupos Primarios

Definición 3.5 *G es llamado un grupo primario, si existe un primo p tal que el orden de cualquier elemento de G es una potencia de p.*
Si G es primario y el orden de cualquier elemento de G es una potencia de p, donde p es un primo dado, entonces se dice que G es un grupo p-primario (o un p-grupo).

Ejemplos:
Los grupos $\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$ y $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ son 2-primarios.
El teorema de Cauchy establece que si p es un primo que divide al orden de un grupo (abeliano ó no abeliano) finito, entonces en este grupo existe por lo menos un elemento de orden p. Aplicaremos este hecho para demostrar que un grupo (abeliano) finito G es un grupo p-primario si y solo si $|G|$ es una potencia de p.
(Recordemos que desde el inicio hemos indicado que la letra G siempre denotará a un grupo abeliano)

Teorema 3.4 *Un grupo finito G es p-primario si y solo si $|G|$ es una potencia de p.*

Demostración:
Si $|G|$ es una potencia de p, entonces el orden de cualquier elemento de G también es una potencia de p y por lo tanto G es p-primario.
Ahora, supongamos que G es p-primario. Sea $|G| = n$.
Si $n = 1$ entonces $|G| = p^0$
(el orden de G es una potencia de p).
Si $n > 1$ entonces existe $a \in G$ tal que $a \neq 0$.
Como $o(a) > 1$ y $o(a)$ es una potencia de p, entonces p divide a $o(a)$ y por lo tanto p divide a n. Si n no fuera una potencia de p, entonces existiría un primo q distinto de p tal que q divide a n. Por el teorema de Cauchy se tendría en G por lo menos un

elemento de orden q, lo cual estaría en contradicción con el hecho de ser G p-primario. Se concluye así que $|G|$ es una potenciade p. $\square$

Teorema 3.5 *Cualquier suma directa de grupos p-primarios es un grupo p- primario.*

Demostración:

Supongamos que $G = \bigoplus_{i \in I} G_i$, donde cada G_i es un grupo $p-primario$. Sea $x \in G$ arbitrario. Entonces existen $i_1, i_2, \ldots, i_n \in I$, distintos, y existen $x_j \in G(i_j)$, $j = 1, 2, \ldots n$ tales que

$$x = x_1 + x_2 + \ldots + x_n$$

Por la hipotesis, el orden de cada x_i es una potencia de p.

Sea p^r el mayor orden de los x_i. Entonces $p^r x_i = 0$, $\quad i = 1, 2, \ldots, n$ y por lo tanto $p^r x = 0$. Luego el orden de x es una potencia de p. Por consiguiente G es un grupo p-primario. $\square$

El Teorema de Estructura de los grupos de torsión

Demostraremos que todo grupo de torsión es una suma directa de grupos primarios. De esta manera, el estudio de los grupos de torsión se reduce esencialmente al estudio de los grupos primarios.

Teorema 3.6 *Para cada primo p,* $\quad G_p = \{x \in G/o(x)$ *es una potencia de* $p\}$ *es un subgrupo (p-primario) de G.*

Demostración:

Como el cero de G es de orden $1 = p^0$ entonces $G_p \neq \emptyset$. Sean $x, y \in G_p$ arbitrarios y sea $p^r = max\{o(x), o(y)\}$. Entonces

$$p^r(x - y) = p^r x - p^r y = 0 - 0 = 0$$

Por lo tanto G_p es un subgrupo de G $\square$

Observación: Si p es un primo y no existen en G elementos de orden p^k donde $k \in \mathbb{Z}^+$, entonces $G_p = \{0\}$.

Definición 3.6 *Sea G un grupo de torsión. Para cada primo p, el subgrupo G_p es llamado la p-componente de G.*

Ejemplos:

Sea $G = \mathbb{Z}_{20}$

(1) La 2-componente de G es $G_2 = \{\overline{0}, \overline{5}, \overline{10}, \overline{15}\} = [\ \overline{5}\ ]$

(2) La 5-componente de G es $G_5 = \{\overline{0}, \overline{4}, \overline{8}, \overline{12}, \overline{16}\} = [\ \overline{4}\ ]$

Teorema 3.7 (Teorema de Estructura de los Grupos de Torsión)
Todo grupo de torsión G es la suma directa de sus p-componentes, es decir, $G = \bigoplus_{p\in\Pi} G_p$ donde Π es el conjunto de todos los primos.

Demostración:
Sea $x \in G - \{0\}$ arbitrario. Supongamos que $o(x) = q_1 q_2 \ldots q_n$,
donde $q_i = p_i^{r_i}$, $\quad i = 1, 2, \ldots, n$, $\quad p_1, p_2, \ldots, p_n$ son primos distintos y $r_1, r_2, \ldots, r_n$ son enteros positivos. Sea $q = q_1 q_2 \ldots q_{n-1}$. Entonces q y q_n son coprimos y por lo tanto existen enteros s y t tales que $sq_n + tq = 1$. Luego

$$x = sq_n x + tqx$$

Como $q(sq_n x) = s(qq_n x) = s(0) = 0$ y $q_n(tqx) = t(qq_n x) = t(0) = 0$, entonces

$$o(sq_n x) = q < o(x) \quad \text{y} \quad tqx \in G(p_n)$$

Procediendo inductivanente, podemos suponer que $sq_n x$ es una suma de elementos que pertenecen a $G(p_1), G(p_2), \ldots G(p_{n-1})$. Por consiguiente x se puede expresar en la forma

$$x = x_1 + x_2 + \ldots + x_n$$

donde $x_j \in G(p_j)$, $\quad x_j \neq 0$, $\quad j = 1, 2, \ldots, n$.
Ahora demostraremos que si

$$x_1 + x_2 + \ldots + x_n = 0$$

(donde $x_j \in G(p_j)$, $\quad j = 1, 2, \ldots, n$ y $p_1, p_2, \ldots, p_n$ son primos distintos)

entonces $\quad x_1 = x_2 = \ldots = x_n = 0$.

Procederemos por inducción matemática. Para $n = 1$ se verifica obviamente.Supongam

que se verifica para $n = k$. Consideremos

$$x_1 + x_2 + \ldots + x_k + x_{k+1} = 0$$

Si $o(x_{k+1}) = p_{k+1}^r = q$, entonces $qx_{k+1} = 0$ y

$$\sum_{i=1}^{k} qx_i = \sum_{i=1}^{k+1} qx_i = q\sum_{i=1}^{k+1} x_i = 0$$

Por la hipótesis inductiva,

$$qx_1 = qx_2 = \ldots = qx_k = 0$$

Luego $x_j \in G(p_j) \cap G(p_{k+1}) = \{0\}$, $\quad j = 1, 2, \ldots, k$, es decir $x_1 = x_2 = \ldots = x_k = 0$

por lo tanto también $x_{k+1} = 0$.

Concluinos así que $G = \bigoplus_{p \in \Pi} G_p$ por el teorema 1.4. $\square$

Consecuencias del Teorema de Estructura de los Grupos de Torsión

Teorema 3.8 *Si* $|G| = p^m k$, *donde* p *es un primo que no divide a* $k \in \mathbb{Z}^+$, $m \in$

entonces $|G_p| = p^m$.

Demostración:

Expresemos $|G| = p_1^{r_1} p_2^{r_2} \ldots p_n^{r_n}$ donde $p_1, p_2, \ldots, p_n$ son primos distintos $(p_1 = p$

$r_1, r_2, \ldots, r_n$ son enteros no negativos $(r_1 = m)$. De acuerdo al teorema de estructura

los grupos de torsión, G tiene la siguiente descomposición:

$$G = G^{(1)} \oplus G^{(2)} \oplus \ldots \oplus G^{(n)} \qquad (3$$

donde $G^{(i)}$ es la p_i-componente de G, $i = 1, 2, \ldots, n$. Luego por definición $G^{(i)}$ es

grupo p_i-primario, $i = 1, 2, \ldots, n$ y por el teorema 3.4 existen enteros no negati

$t_1, t_2, \ldots, t_n$ tales que $|G^{(i)}| = p_i^{t_i}$, $\quad i = 1, 2, \ldots, n$, con lo cual de (3.2) se obtiene:

$$p_1^{r_1} p_2^{r_2} \ldots p_n^{r_n} = |G| = |G^{(1)}||G^{(2)}| \ldots |G^{(n)}| = p_1^{t_1} p_2^{t_2} \ldots p_n^{t_n}$$

Finalmente, de la unicidad de la descomposición de un primo se obtiene en particular que:

$$|G_p| = |G^{(1)}| = p_1^{r_1} = p^m. \quad \square$$

Observacion: Si q es un primo distinto de $p_1, p_2, \ldots, p_n$, entonces no existen elementos en G cuyo orden sea una potencia de q y por lo tanto $G_q = \{0\}$.

Teorema 3.9 *Sea $|G| = pq$, p y q son primos distintos entonces $G \approx \mathbb{Z}_p \times \mathbb{Z}_q$.*

Demostración:

De acuerdo con el teorema 3.8 $|G_p| = p$ y $|G_q| = q$, por lo tanto G_p y G_q son cíclicos isomorfos a $\mathbb{Z}_p$ y $\mathbb{Z}_q$ respectivamente. Luego, por el teorema de estructura de los grupos de torsión

$$G = G_p \oplus G_q$$

Por lo tanto $\quad G \approx \mathbb{Z}_p \times \mathbb{Z}_q. \quad \square$

Teorema 3.10 *Sea G es ciclico y $|G| = p_1^{r_1}\ p_2^{r_2} \ldots p_m^{r_m}$, donde $p_1, p_2, \ldots, p_m$ son primos distintos y $r_1, r_2, \ldots, r_m$ son enteros positivos, entonces*

$$G \approx \mathbb{Z}_{p_1{}^{r_1}} \times \mathbb{Z}_{p_2{}^{r_2}} \times \ldots \times \mathbb{Z}_{p_m{}^{r_m}}.$$

Demostración:

De acuerdo al teorema 3.8 la p_i-componente de G es de orden $p_i{}^{r_i} \quad i = 1, 2, \ldots, m$.
Como G es ciclico, entonces cada p_i-componente G_{p_i} es un grupo ciclico y por lo tanto isomorfo a $\mathbb{Z}_{p_i{}^{r_i}}, \quad i = 1, 2, \ldots, m$.
Luego, por el teorema de estructura de los grupos de torsión

$$G = G_{p_1} \oplus G_{p_2} \oplus \ldots \oplus G_{p_n}$$

Por lo tanto

$$G \approx \mathbb{Z}_{p_1{}^{r_1}} \times \mathbb{Z}_{p_2{}^{r_2}} \times \ldots \times \mathbb{Z}_{p_m{}^{r_m}}. \quad \square$$

3.4. Grupos p-Prüfer y Grupos Divisibles

Grupos p-Prüfer

Como ya se ha visto $\mathbb{Q}/\mathbb{Z}$ es un grupo de torsión y por lo tanto $\mathbb{Q}/\mathbb{Z} = \bigoplus_{p\in\Pi} (\mathbb{Q}/\mathbb{Z})_p$

Definición 3.7 *Se denomina grupo p-Prüfer a cualquier grupo isomorfo a la p-componente de* $\mathbb{Q}/\mathbb{Z}$.

Observaciones:

1. $$\begin{aligned}(\mathbb{Q}/\mathbb{Z})_p &= \{x+\mathbb{Z} \ / \ o(x+\mathbb{Z}) \text{ es una potencia de } p\}\\ &= \{x+\mathbb{Z} \ / \ p^r(x+\mathbb{Z}) = 0+\mathbb{Z}, \text{ para algún } r\in\mathbb{N}\}\\ &= \{x+\mathbb{Z} \ / \ p^r x+\mathbb{Z} = 0+\mathbb{Z}, \text{ para algún } r\in\mathbb{N}\}\\ &= \{x+\mathbb{Z} \ / \ p^r x \in \mathbb{Z}, \text{ para algún } r\in\mathbb{N}\}\\ &= \{(m/p^r)+\mathbb{Z} \ / \ 0\le m < p^{r-1}, \text{ para algún } r\in\mathbb{N}\}\end{aligned}$$

2. Como $(\mathbb{Q}/\mathbb{Z})_p = \{(m/p^r)+\mathbb{Z}/0\le m < p^{r-1}, \text{ para algún } r\in\mathbb{N}\}$, entonces

$$(\mathbb{Q}/\mathbb{Z})_p = \bigcup_{r=1}^{\infty} C_r \text{ donde } C_r = [(1/p^r)+\mathbb{Z}], \quad r = 1,2,3,\ldots$$

Grupos Divisibles

Definición 3.8 *se dice que G es divisible, si para todo entero $n \neq 0$ y para todo $x \in G$, existe $y \in G$ tal que $ny = x$.*

Ejemplo:

El grupo aditivo $\mathbb{Q}$ es divisible, puesto que para todo entero $n \neq 0$ y para todo $x \in \mathbb{Q}$, se tiene:

$$ny = x, \quad \text{donde} \quad y = \frac{x}{n}.$$

Teorema 3.11 *Todo cociente de un grupo divisible es un grupo divisible.*

Demostración:

Supongamos que G es un grupo divisible y que H es un subgrupo de G.

Sean $x + H \in G/H$ y $n \in \mathbb{Z} - \{0\}$ arbitrarios.

Como G es divisible, existe $y \in G$ tal que $ny = x$. Luego $n(y + H) = ny + H = x + H$

Por lo tanto G/H es divisible. $\square$

Teorema 3.12 *Todo sumando directo de un grupo divisible es un grupo divisible.*

Demostración:

Sea G un grupo divisible y sea S un sumando directo de G. Entonces existe un subgrupo H de G tal que

$$G = S \oplus H$$

Como $S \approx G/H$, entonces por el teorema 3.11, S es un grupo divisible. $\square$

Teorema 3.13 *Todo grupo p-Prüfer es divisible.*

Demostración:

Como $\mathbb{Q}$ es divisible, entonces por el teorema 3.11 $\mathbb{Q}/\mathbb{Z}$ es divisible.

Pero como $\mathbb{Q}/\mathbb{Z} = \bigoplus_{p \in \Pi} (\mathbb{Q}/\mathbb{Z})_p$ resulta que cada $(\mathbb{Q}/\mathbb{Z})_p$ es divisible, puesto que todo sumando directo de un grupo divisible es un grupo divisible. $\square$

Teorema de Estructura de los Grupos Divisibles

Mostraremos que todo grupo divisible es una suma directa de grupos p-Prüfer y/o grupos isomorfos al grupo aditivo de los números racionales, resultado que solamente enunciaremos en el siguiente teorema.

Teorema 3.14 (Teorema de estructura de los Grupos divisibles)
Todo grupo divisible es una suma directa arbitraria de grupos p-Prüfer y/o grupos isomorfos a $\mathbb{Q}$.

Consecuencias del teorema de estructura de los grupos divisibles

1. Todo grupo divisible es infinito.

2. Todo grupo divisible de torsión es una suma directa de grupos p-Prüfer.

3. Todo grupo divisible sin torsión es una suma dirtecta de grupos isomorfos a $\mathbb{Q}$.

Capítulo 4

Grupos Abelianos Finitamente Generados

En este capítulo se determinará la estructura de los grupos abelianos finitamente generados. Se demostrará el teorema fundamental de los grupos abelianos, el cual establece que todo grupo abeliano finitamente generado es una suma directa de un número finito de grupos cíclicos primarios y/o grupos cíclicos infinitos. El tipo de un grupo abeliano finitamente generado determina completamente la estructura, de manera que dos grupos abelianos finitamente generados son isomorfos si y solamente si ambos tienen el mismo tipo.

4.1. Concepto de Grupo Abeliano Finitamente Generado

Definición 4.1 *Un grupo abeliano G se dice que es* **finitamente generado**, *si posee un sistema finito de generadores, esto es, si existen $x_1, x_2, \ldots, x_n \in G$ tales que $G = [x_1, x_2, \ldots, x_n]$.*

En este caso, todo elemento x de G es de la forma:

$$x = k_1x_1 + k_2x_2 + \ldots + k_nx_n$$

donde $k_1, k_2, \ldots, k_n \in \mathbb{Z}$.

El subconjunto $\{y_1, y_2, \ldots, y_m\}$ de G también genera a $G = [x_1, x_2, \ldots, x_n]$ si

$$y_j \in [x_1, x_2, \ldots, x_n], \quad j = 1, 2, \ldots, m$$

$$\text{y } x_i \in [y_1, y_2, \ldots, y_m], \quad i = 1, 2, \ldots, n$$

Recordemos que para cualquier subconjunto S de G:

$$[S] = S \text{ si y solo si } S \text{ es un subgrupo de } G.$$

Aplicando ésta propiedad, se deduce facilmente que todo grupo abeliano finito es finitamente generado.

En efecto, si G es finito entonces G es finitamente generado, puesto que un sistema de generadores finito de G es $G = [G]$.

4.2. Ejemplos de Grupos Abelianos Finitamente Generados

1. Todo grupo cíclico es un grupo abeliano finitamente generado. Por ejemplo $\mathbb{Z}$ y $\mathbb{Z}_n$, para cualquier $n \in \mathbb{N}$.

2. Todo subgrupo finitamente generado $\neq 0$ de $\mathbb{Q}$ es cíclico e isomorfo a $\mathbb{Z}$.

   En efecto, sea $H \neq 0$ un subgrupo de $\mathbb{Q}$ y sea $\{x_1, x_2, \ldots, x_n\}$ un sistema de generadores de H. Entonces existen enteros $k_i, m_i, \quad m_i \neq 0$, $i = 1, 2, \ldots, n$ tales que $x_i = k_i/m_i, \quad i = i = 1, 2, \ldots, n$. Sea $m = m_1m_2\ldots m_n$.

   Definimos $\quad f_m : H \to \mathbb{Z}$ por $f_m(x) = mx, \quad x \in H$

   Para todo $x \in H : \; mx \in \mathbb{Z}$

   Dado $x = r_1x_1 + r_2x_2 + \ldots + r_nx_n$ donde $r_i \in \mathbb{Z}$, como $mx_i = mk_i/mi \in \mathbb{Z}$, $i = 1, 2, \ldots, n$ entonces $mx = r_1mx_1 + r_2mx_2 + \ldots + r_nmx_n \in \mathbb{Z}$.

f_m es un homomorfismo:

$$f_m(x+y) = m(x+y) = mx + my = f_m(x) + f_m(y)$$

para cualesquiera $x, y \in H$.

f_m es inyectivo:

Si $x \in Ker(f_m)$ entonces $mx = f_m(x) = 0$, luego $x = 0$ puesto que $m \neq 0$. Por lo tanto $ker(f_m) = \{0\}$. Se concluye así que H es isomorfo a un subgrupo no nulo de $\mathbb{Z}$. Por consiguiente, H es isomorfo a un grupo cíclico infinito, esto es, $H \approx \mathbb{Z}$.

3. Todo cociente de un grupo abeliano finitamente generado es un grupo abeliano finitamente generado

Si $G = [x_1, x_2, \ldots, x_n]$, entonces para cualquier subgrupo H de G:

$$G/H = [x_1 + H, x_2 + H, \ldots, x_n + H]$$

En efecto, sea $x + H \in G/H$ arbitrario. Entonces

$$x = r_1x_1 + r_2x_2 + \ldots + r_nx_n$$

donde $r_i \in \mathbb{Z}, \quad i = 1, 2, \ldots, n$. Luego

$$\begin{aligned} x + H &= r_1x_1 + r_2x_2 + \ldots + r_nx_n + H \\ &= r_1x_1 + H + r_2x_2 + H + \ldots + r_nx_n + H \\ &= r_1(x_1 + H) + r_2(x_2 + H) + \ldots + r_n(x_n + H) \end{aligned}$$

y por lo tanto $x_1 + H, x_2 + H, \ldots, x_n + H$ generan a G/H.

4. Sean G un grupo abeliano y H un subgrupo de G.

Si H y G/H son finitamente generados, entonces G es finitamente generado

En efecto, supongamos que $H = [y_1, y_2, \ldots, y_m]$ y que

$$G/H = [x_1 + H, x_2 + H, \ldots, x_n + H]$$

Sea $x \in G$ arbitrario. Entonces existen $s_i \in \mathbb{Z}, \quad i = 1, 2, \ldots, n$ tales que

$$\begin{aligned} x + H &= s_1(x_1 + H) + s_2(x_2 + H) + \ldots + s_n(x_n + H) \\ &= s_1x_1 + H + s_2x_2 + H + \ldots + s_nx_n + H \\ &= (s_1x_1 + s_2x_2 + \ldots + s_nx_n) + H \end{aligned}$$

Luego $\quad x - (s_1x_1 + s_2x_2 + \ldots + s_nx_n) \in H \quad$ y por lo tanto

$$x - (s_1x_1 + s_2x_2 + \ldots + s_nx_n) = t_1y_1 + t_2y_2 + \ldots + t_my_m$$

donde $t_j \in \mathbb{Z}, \quad j = 1, 2, \ldots, m$. En consecuencia

$$x = s_1x_1 + s_2x_2 + \ldots + s_nx_n + t_1y_1 + t_2y_2 + \ldots + t_my_m$$

Por consiguiente

$$G = [x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m]$$

5. Todo subgrupo de un grupo abeliano finitamente generado es finitamente generado

En efecto, procediendo por inducción sobre el número de elementos de un sistema de generadores, tenemos:

Si G tiene un sistema de generadores con un único elemento, entonces G es cíclico y por lo tanto nuestra afirmación queda probada.

Ahora supongamos que nuestra afirmación se cumple para todos los grupos abelianos que admiten un sistema de k generadores, donde $k \leq n$.

Sea $G = [x_1, x_2, \ldots, x_n, x_{n+1}]$ y sea $H = [x_1, x_2, \ldots, x_n]$. Entonces el grupo cociente $G/H = [x_{n+1} + H]$ es cíclico.

Consideremos el homomorfismo natural

$$\Pi : G \to G/H$$

Por la hipotesis inductiva, todo subgrupo de H es finitamente generado. Sea L un subgrupo cualquiera de G. Entonces $H \cap L$ y $\Pi(L)$ son subgrupos finitamente generados de H y G/H, respectivamente.

Sea Π^* la restricción de Π a L:

$$\Pi^* : L \to \Pi(L)$$

El núcleo de Π^* es $H \cap L$ y $\Pi(L)$ es isomorfo a $L/(H \cap L)$ por el primer teorema de isomorfismos.

Como $\Pi(L)$ es finitamente generado, entonces $L/(H \cap L)$ es finitamente generado. De acuerdo con el ejemplo 4., L es finitamente generado.

6. Un grupo abeliano G es finitamente generado si sólo si toda cadena ascendente de subgrupos

$$G_1 \subset G_2 \subset \ldots \subset G_n \subset G_{n+1} \subset \ldots \tag{4.1}$$

es estacionaria, es decir, existe un indice k tal que $G_k = G_{k+n}$ para todo $n \in \mathbb{N}$
En efecto, supongamos que G es finitamente generado y consideremos la cadena ascendente de subgrupos (4.1). Entonces

$$H = \bigcup_{n \in \mathbb{N}} G_n$$

es un subgrupo de G, ya que es no vacío y dados $x, y \in H$, existen índices i y j, $i \leq j$, tales que $x \in G_i$ e $y \in G_j$ de manera que $G_i \subset G_j$ y $x, y \in G_j$ y por lo tanto $x - y \in G_j \subset H$.

De acuerdo con el ejemplo anterior, H es finitamente generado, digamos por $\{x_1, x_2, \ldots, x_n\}$. Entonces existen índices $n_1, n_2, \ldots, n_r$ tales que $x_j \in G(n_j)$, $j = 1, 2, \ldots, r$.

Si $k = max\{n_1, n_2, \ldots, n_r\}$, entonces $x_j \in G(n_j) \subset G_k$, $j = 1, 2, \ldots, r$; luego $H = [x_1, x_2, \ldots, x_n] \subset G_k \subset H$ y por lo tanto $H = G_k$. Como $H = G_k \subset G_{k+n} \subset H$ para todo $n \in \mathbb{N}$, entonces

$$G_k = G_{k+n} \text{ para todo } n \in \mathbb{N}.$$

esto es (4.1) es estacionaria.

Ahora supongamos que toda cadena ascendente de subgrupos de G es estacionaria. Procediendo por reducción al absurdo, supongamos que G no es finitamente generado. En este caso, todo subgrupo finitamente generado de G es distinto de G. Para cada $n \in \mathbb{N}$ definimos un subgrupo (de G) finitamente generado G_n de la siguiente manera:

$G_1 = 0$; si G_n ha sido definido, entonces $G_n \neq G$ y por lo tanto existe un subgrupo G_{n+1} de G finitamente generado que contiene a G_n. Por consiguiente, se ha obtenido una sucesiónde subgrupos de G estrictamente creciente, no estacionaria, lo cual es una contradicción. Se concluye así que G es finitamente generado.

7. $\mathbb{Q}$ (el grupo aditivo de los números racionales) no es finitamente generado, puesto que la sucesión de subgrupos

$$[1/1!], [1/2!], \ldots, [1/n!], \ldots$$

es estrictamente creciente no estacionaria.

En efecto, si existiera $k \in \mathbb{N}$ tal que

$$[1/k!] = [1/(k+n)!]$$

para todo $n \in \mathbb{N}$, entonces se tendría en particular que:

$$[1/k!] = [1/(k+1)!].$$

Luego $1/(k+1)! = m(1/k!)$ para algún $m \in \mathbb{Z}$ y por lo tanto $1/(k+1) = m$, lo cual es absurdo.

8. $\mathbb{Q}$ no es subgrupo de ningún grupo finitamente generado, puesto que $\mathbb{Q}$ no es finitamente generado.

9. Todo subgrupo finitamente generado de $\mathbb{Q}/\mathbb{Z}$ es cíclico.

En efecto, sea S un subgrupo finitamente generado de $\mathbb{Q}/\mathbb{Z}$. Si S es el subgrupo cero, entonces S es cíclico.

Si $S = [x_1 + \mathbb{Z}, x_2 + \mathbb{Z}, \ldots, x_n + \mathbb{Z}]$ para algunos $x_1, x_2, \ldots, x_n \in \mathbb{Q}$ y S no es el subgrupo cero, entonces alguno de los x_i no es entero. Luego el subgrupo $[x_1, x_2, \ldots, x_n]$ de $\mathbb{Q}$ no es el subgrupo cero, y por lo tanto es cíclico, conforme el ejemplo 2. Esto significa que existe $x \in \mathbb{Q}$ tal que

$$[x_1, x_2, \ldots, x_n] = [x]$$

De esta identidad se obtiene:

$$S = [x_1 + \mathbb{Z}, x_2 + \mathbb{Z}, \ldots, x_n + \mathbb{Z}] = [x + \mathbb{Z}]$$

de manera que S es cíclico.

10. Un grupo abeliano G es cíclico si y solo si existe un homomorfismo sobreyectivo de $\mathbb{Z}$ sobre G.

En efecto, si existe un homomorfismo sobreyectivo

$$f : \mathbb{Z} \to G$$

entonces $G \approx \mathbb{Z}/Kerf$ por el primer teorema de isomorfismos. Como $\mathbb{Z}$ es cíclico y $Kerf$ es un subgrupo de $\mathbb{Z}$, entonces existe $n \in \mathbb{Z}$, $n \geq 0$ tal que $kerf = n\mathbb{Z}$.
Si $n = 0$, entonces f es un isomorfismo y $G \approx \mathbb{Z}$.
Si $n > 0$, entonces $G \approx \mathbb{Z}_n$.
En cualquier caso, G es cíclico.
Recíprocamente,
Si G es cíclico, entonces existe $a \in G$ tal que $G = [a] = \{na/n \in \mathbb{Z}\}$ (notación aditiva). La aplicación

$$f : \mathbb{Z} \to G$$

definida por $f(n) = na$, es un homomorfismo sobreyectivo.

11. Subgrupos de $\mathbb{Z}_n$ (el grupo de restos módulo n).

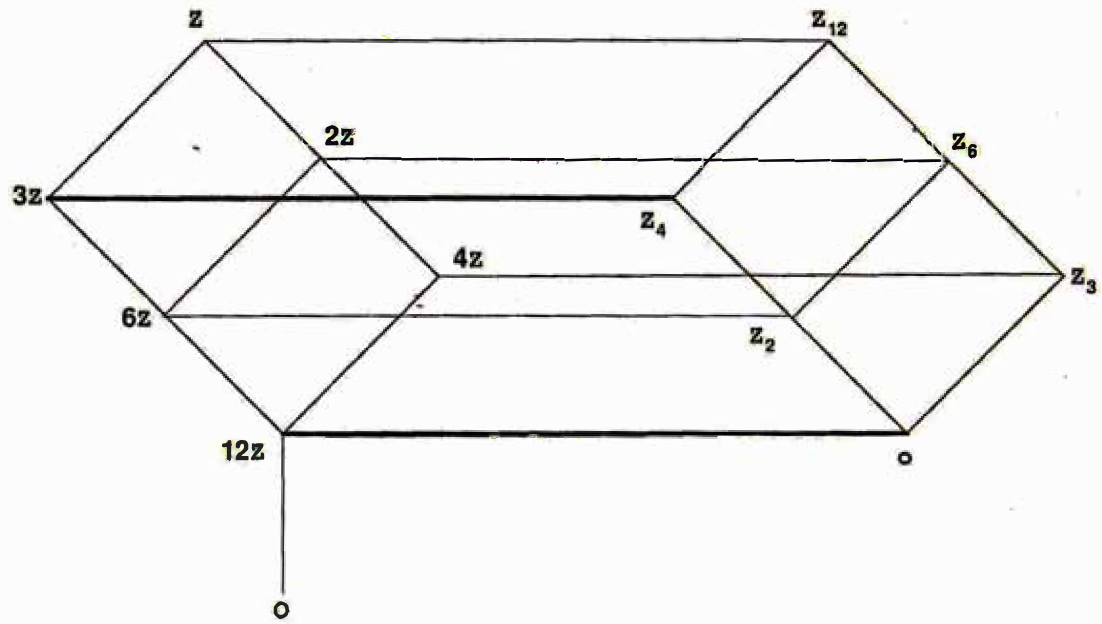
Los subgrupos de $\mathbb{Z}_n$ están en correspondencia biunívoca con los subgrupos de $\mathbb{Z}$ que contienen a $n\mathbb{Z}$. Esta correspondencia está dada de la siguiente manera:
Sea

$$\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$

el homomorfismo canónico.

Si H es un subgrupo de $\mathbb{Z}$ que contiene a $n\mathbb{Z}$, entonces $\varphi(H)$ es un subgrupo de $\mathbb{Z}_n$. Si U es un subgrupo de $\mathbb{Z}_n$, entonces $\varphi^{-1}(U)$ es un subgrupo de $\mathbb{Z}$ que contiene a $n\mathbb{Z}$. Así pues, φ induce una biyección del conjunto de todos los subgrupos de $\mathbb{Z}_n$ sobre el conjunto de los subgrupos de $\mathbb{Z}$ que contienen a $n\mathbb{Z}$.

Por ejemplo, los subgrupos de $\mathbb{Z}_{12}$ vistos a través de un diagrama de Hasse son los siguientes:



$$\varphi : \mathbb{Z} \to \mathbb{Z}/_{12\mathbb{Z}} = \mathbb{Z}_{12}$$

4.3. Lemas sobre Grupos Abelianos Libres Finitamente Generados

Demostraremos que todos los grupos abelianos finitamente generados son sumas directas de grupos cíclicos.

Lema 4.1 *Sea $G = [x_1] \oplus [x_2] \oplus \ldots \oplus [x_n]$ la suma directa de grupos cíclicos infinitos. Si $y_1 = x_1 + k_2x_2 + k_3x_3 + \ldots + k_nx_n$ donde $k_2, k_3, \ldots, k_n$ son enteros arbitrarios, entonces $G = [y_1] \oplus [x_2] \oplus \ldots \oplus [x_n]$.*

Demostración:

De la hipotesis, tenemos que

$G = [y_1, x_2, x_3, \ldots, x_n] = [y_1] + [x_2] + [x_3] + \ldots + [x_n]$

Ahora demostraremos que si $t_1, t_2, \ldots, t_n$ son enteros arbitrarios y

$$t_1y_1 + t_2x_2 + \ldots + t_nx_n = 0 \tag{4.2}$$

entonces $t_1 = t_2 = \ldots = t_n = 0$.

En efecto, como $y_1 = x_1 + k_2x_2 + k_3x_3 + \ldots + k_nx_n$ entonces sustituyendo en (4.2) se obtiene:

$$t_1x_1 + (t_1k_2 + t_2)x_2 + (t_1k_3 + t_3)x_3 + \ldots (t_1k_n + t_n)x_n = 0$$

pero $G = [x_1] \oplus [x_2] \oplus \ldots + [x_n]$ donde x_i es de orden infinito, $i = 1, 2, \ldots, n$.

Luego, por el teorema 1.3

$$t_1x_1 = 0, (t_1k_2 + t_2)x_2 = 0, (t_1k_3 + t_3)x_3 = 0, \ldots, (t_1k_n + t_n)x_n = 0$$

como x_i es de orden infinito, $i = 1, 2, \ldots, n$, entonces

$$t_1 = 0, t_1k_2 + t_2 = 0, t_1k_3 + t_3 = 0, \ldots, t_1k_n + t_n = 0.$$

Por consiguiente $t_1 = t_2 = \ldots = t_n = 0$ □

Recordemos que $X = \{x_1, x_2, \ldots, x_n\}$ es una base de un grupo abeliano libre finitamente generado G, si $G = [x_1] \oplus [x_2] \oplus \ldots \oplus [x_n]$.

El siguiente lema es el más importante resultado acerca de los grupos abelianos libres finitamente generados. La demostración de este lema va más allá de los limites del presente trabajo, por lo cual sólamente lo enunciaremos.

Lema 4.2 *Sea G un grupo abeliano libre. Si G posee una base con n elementos y H es un subgrupo de G, entonces existe una base $Y = \{y_1, y_2, \ldots, y_n\}$ de G y enteros $k_1, k_2, \ldots, k_n$ tales que $H = [k_1y_1, k_2y_2, \ldots, k_ny_n]$.*

Lema 4.3 *Sea $G = H \oplus K$. Si H_1, K_1 son subgrupos de G tales que $H_1 \subset H$ y $K_1 \subset K$, entonces*

$$\frac{G}{H_1 + K_1} \approx \frac{H}{H_1} \oplus \frac{K}{K_1}$$

Demostración:

Sea $S = \dfrac{H}{H_1} \oplus \dfrac{K}{K_1}$ y sean $\Pi_1 : H \to \dfrac{H}{H_1}$, $\Pi_2 : K \to \dfrac{K}{K_1}$ los homomorfismos naturales. Como $\dfrac{H}{H_1} \subset S$ y $\dfrac{K}{K_1} \subset S$, entonces por la propiedad de extensión homomórfica de las sumas directas, existe un homomorfismo

$$f : G \to S$$

tal que las restricciones de f a H y K respectivamente son Π_1 y Π_2. Luego

$$H_1 = Ker(\Pi_1) \subset Kerf \text{ y}$$

$$K_1 = Ker(\Pi_2) \subset Kerf$$

y por lo tanto $H_1 + K_1 \subset Kerf$.

Veamos que $Kerf = H_1 + K_1$. En efecto, si $x \in Kerf$ entonces $x = h + k$ donde $h \in H$ y $k \in K$ y

$(h+H_1)+(k+K_1) = \Pi_1(h)+\Pi_2(k) = f(h)+f(k) = f(h+k) = f(x) = (0+H_1)+(0+K_1)$

Por la unicidad de la representación en S (teorema 1.2) se obtiene que $h + H_1 = 0 + H_1$ y $k + K_1 = 0 + K_1$ de manera que $h \in H_1$ y $k_1 \in K_1$ y por lo tanto

$$x = h + k \in H_1 + K_1$$

con lo cual queda probado que

$$Kerf \subset H_1 + K_1 \subset Kerf$$

es decir, $Kerf = H_1 + K_1$. □

Además, f es sobreyectiva, puesto que dado $(h + H_1) + (k + K_1) \in S$ $(h \in H$ y $k \in K)$:

$$f(h + k) = f(h) + f(k) = \Pi_1(h) + \Pi_2(k) = (h + H_1) + (k + K_1)$$

Finalmente, aplicando el primer teorema de isomorfismos

$$\frac{G}{H_1 + K_1} = \frac{G}{Kerf} \approx S = \frac{H}{H_1} \oplus \frac{K}{K_1} \quad \square$$

Aplicando reiteradamente éste lema se obtiene el siguiente resultado.

Lema 4.4 *Sea G un grupo abeliano libre y sea $X = \{x_1, x_2, \ldots, x_n\}$ una base de G. Si $H = [k_1x_1, k_2x_2, \ldots, k_nx_n]$ donde $k_1, k_2, \ldots, k_n$ son enteros no negativos arbitrarios, entonces*

$$\frac{G}{H} = S_1 \oplus S_2 \ldots \oplus S_n$$

donde S_i es cíclico y

$$o(S_i) = \begin{cases} k_i & ,si\ k_i \neq 0 \\ \infty & ,si\ k_i = 0 \end{cases}$$

$i = 1, 2, \ldots, n$. □

4.4. El Teorema Fundamental de los Grupos Abelianos

En primer lugar mostraremos un teorema que es llamado el teorema básico de los grupos abelianos, refiriéndose básicamente a los grupos abelianos finitamente generados.

Teorema 4.1 *(Teorema Básico)*

Todo grupo abeliano finitamente generado es una suma directa de un número finito de grupos cíclicos.

Demostración:

Sea G un grupo abeliano finitamente generado.

De acuerdo con el teorema 2.3 existe un grupo abeliano libre finitamente generado F y existe un subgrupo H de F tal que $G \approx F/H$. Luego por el lema 4.2, F tiene una base $\{x_1, x_2, \ldots, x_n\}$ tal que $H = [k_1x_1, k_2x_2, \ldots, k_nx_n]$ para algunos enteros no negativos $k_1, k_2, \ldots, k_n$.

Aplicando el lema 4.4 concluimos que F/H es suma directa de un número finito de grupos cíclicos infinitos y/o cíclicos finitos. $\square$

El siguiente teorema que mostraremos es llamado el teorema fundamental de los grupos abelianos, aunque realmente se refiere a los grupos abelianos finitamente generados. Este teorema determina parcialmente la estructura de los grupos abelianos finitamente generados. Basándose en este teorema se define más adelante la noción de tipo de un grupo abeliano finitamente generado con la cual se determina completamente su estructura.

Teorema 4.2 (Teorema fundamental de los Grupos Abelianos)
Todo grupo abeliano finitamente generado es suma directa de un número finito de grupos cíclicos infinitos y/o cíclicos primarios.

Demostración:

Sea G un grupo abeliano finitamente generado. De acuerdo con el teorema básico 4.1, G es suma directa de un número finito de grupos cíclicos infinitos y/o cíclicos finitos, pero por el teorema 3.10 todo grupo cíclico finito es una suma directa de un número finito de grupos ciclicos primarios.

Además como $G \approx F/H$, entonces concluimos que G es una suma directa de un número finito de grupos cíclicos infinitos y/o cíclicos primarios. $\square$.

Corolario: Si G es un grupo sin torsion y finitamente generado, entonces G es un grupo abeliano libre.

Demostración:

Como G es sin torsión, entonces no posee subgrupos cíclicos primarios. Por el teorema fundamental de los grupos abelianos, G es una suma directa finita de grupos cíclicos, todos necesariamente infinitos. Por Consiguiente G es un grupo abeliano libre.

Ejemplo:

Sea $G = \bigoplus_{i=1}^{\infty} G_i$ donde G_i es cíclico de orden 2, $i = 1, 2, 3, \ldots$.

Demostraremos que G no es finitamente generado. En efecto, como

$$\begin{aligned} T(G) &= \bigoplus_{i=1}^{\infty} T(G_i) \qquad \text{(por el teorema 3.2)} \\ &= \bigoplus_{i=1}^{\infty} G_i \\ &= G \end{aligned}$$

entonces G es de torsión, es decir, todos los elementos de G son de orden finito. Por lo tanto G no tiene subgrupos cíclicos infinitos. Supongamos que G es finitamente generado. Entonces G es una suma directa finita de grupos cíclicos primarios, por el teorema fundamental de los grupos abelianos y debido a que G no tiene subgrupos cíclicos infinitos. Por lo tanto G es finito.

Pero $G_i = [a_i]$, donde $a_i \in G$ es de orden 2, $i = 1, 2, 3, \ldots$ y los elementos $a_1,\ a_1 + a_2,\ a_1 + a_2 + a_3, \ldots$ son todos distintos, de manera que G es infinito.

La contradicción anterior nos conduce a concluir que G no es finitamente generado. $\square$

Aplicación del Teorema Fundamental de los Grupos abelianos:

Sea A una rotación de $2\pi/n$ radianes alrededor del centro de un poligono regular de n lados y sea B una reflexión con respecto a una recta que pasa por el centro y por uno de los vértices del poligono.

Entonces, la composición de las simetrías A y B forman el grupo de las simetrías de un polígono regular de n lados llamado el grupo Diedrico de orden $2n$, denotado por D_{2n}, generado por los movimientos A y B que satisface las siguientes relaciones:

$$A^n = e, \quad B^2 = e, \quad BA = A^{-1}B$$

El grupo esta formado por:

$$D_{2n} = \{I, A, A^2, \ldots, A^{n-1}, B, AB, A^2B, \ldots, A^{n-1}B\}$$

Características:

a) D_{2n} es un grupo no abeliano, pero posee algunos subgrupos que son cíclicos y otros que son abelianos no cíclicos.

b) $D_{2n} = [A, B]$

c) $|D_{2n}| = 2n, \quad n \geq 3$

Si $n = 6$ tenemos:

$$D_{12} = \{I, A, A^2, A^3, A^4, A^5, B, AB, A^2B, A^3B, A^4B, A^5B\}$$

llamado el grupo de las simetrías del exagono regular, donde $A^6 = I$ y $B^2 = I$.

El orden de cada uno de los elementos del grupo D_{12} esta dado en el siguiente cuadro

D_{12}	I	A	A^2	A^3	A^4	A^5	B	AB	A^2B	A^3B	A^4B	A^5B
orden	1	6	3	2	3	6	2	2	2	2	2	2

Los subgrupos cíclicos de D_{12} son:

$[I] = \{I\} \approx \mathbb{Z}_1$
$[A] = \{I, A, A^2, A^3, A^4, A^5\} \approx \mathbb{Z}_2 \times \mathbb{Z}_3 \approx \mathbb{Z}_6$
$[A^2] = \{I, A^2, A^4\} \approx \mathbb{Z}_3$
$[A^3] = \{I, A^3\} \approx \mathbb{Z}_2$
$[A^4] = \{I, A^2, A^4\} \approx \mathbb{Z}_3$
$[A^5] = \{I, A^5\} \approx \mathbb{Z}_2$
$[B] = \{I, B\} \approx \mathbb{Z}_2$
$[AB] = \{I, AB\} \approx \mathbb{Z}_2$
$[A^2B] = \{I, A^2B\} \approx \mathbb{Z}_2$
$[A^3B] = \{I, A^3B\} \approx \mathbb{Z}_2$
$[A^4B = \{I, A^4B\} \approx \mathbb{Z}_2$
$[A^5B] = \{I, A^5B\} \approx \mathbb{Z}_2$

Los subgrupos abelianos no cíclicos de D_{12}, de orden 4 son:

$[A^3, B] = \{I, A^3, B, A^3B\} \approx \mathbb{Z}_2 \times \mathbb{Z}_2$
$[AB, A^4B] = \{I, A^3, AB, A^4B\} \approx \mathbb{Z}_2 \times \mathbb{Z}_2$
$[A^2B, A^5B] = \{I, A^3, A^2B, A^5B\} \approx \mathbb{Z}_2 \times \mathbb{Z}_2$

Un subgrupo no abeliano de D_{12}, de orden 6 es:

$$\boxed{[A^2, B] = \{I, A^2, A^4, B, A^2B, A^4B\} \approx S_3 \approx D_6}$$

4.5. El Tipo de un Grupo Abeliano Finitamente Generado

De acuerdo con el teorema fundamental de los grupos abelianos, todo grupo abeliano finitamente generado es suma directa de grupos cíclicos infinitos y/o cíclicos primarios. Veremos que el número de sumandos directos de cada clase (cíclicos infinitos y cíclicos primarios) determinan completamente la estructura de un grupo abeliano finitamente generado.

Definición 4.2 *Dos descomposiciones de un grupo abeliano en sumas directas finitas de grupos cíclicos son de la misma clase, si tienen el mismo número de sumandos de cada orden (finito ó infinito).*

El siguiente teorema es un complemento del teorema fundamental de los grupos abelianos y sirve de base para dar la noción de tipo de un grupo abeliano finitamente generado.

Teorema 4.3 (Teorema de Unicidad de una Descomposición)
Dos descomposiciones cualesquiera de un grupo abeliano en sumas directas finitas de grupos cíclicos infinitos y/o cíclicos primarios son de la misma clase.

Definición 4.3 *Sea G un grupo abeliano finitamente generado.*

(1) Si G es libre y es la suma directa de m grupos cíclicos infinitos, entonces el tipo de G es (m).

(2) Si G es la suma directa de grupos cíclicos primarios de ordenes

$$p_1^{r_1}, p_2^{r_2}, \ldots, p_k^{r_k}$$

y m grupos cíclicos infinitos, $m \geq 0$ donde $p_1 \leq p_2 \leq \ldots \leq p_k$ son primos, $r_i \in \mathbb{Z}^+$, $i = 1, 2, \ldots, k$ tales que $r_j \geq r_{j+1}$ en el caso que $p_j = p_{j+1}$, $j = 1, 2, \ldots, k-1$, entonces el tipo de G es la

$$(k+1)\text{-upla} \quad (p_1^{r_1}, p_2^{r_2}, \ldots, p_k^{r_k}; m)$$

Ejemplos:

1. $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ es de tipo (3), pues es libre y es la suma directa de 3 grupos cíclicos infinitos.
2. $\mathbb{Z} \times \mathbb{Z}_{64} \times \mathbb{Z}_{125} \times \mathbb{Z}_8 \times \mathbb{Z}$ es de tipo $(2^6, 2^3, 5^3; 2)$
3. $\mathbb{Z}_4 \times \mathbb{Z}_{25} \times \mathbb{Z}_{81} \times \mathbb{Z}_9 \times \mathbb{Z}_5$ es de tipo $(2^2, 3^4, 3^2, 5^2, 5; 0)$

Finalmente concluimos éste informe sobre grupos abelianos con un teorema que determina totalmente la estructura de un grupo abeliano finitamente generado.

Teorema 4.4 *Dos grupos abelianos finitamente generados son isomorfos si y solamente si tienen el mismo tipo.*

Demostración:

Sean G y H grupos abelianos finitamente generados.

Supongamos que existe un isomorfismo $f : G \to H$ y que

$$G = G_1 \oplus G_2 \oplus \ldots \oplus G_n$$

donde G_i es cíclico, $i = 1, 2, \ldots, n$.

Demostraremos en primer lugar que:

$$H = f(G_1) \oplus f(G_2) \oplus \ldots \oplus f(G_n)$$

Sea $y \in H$ arbitrario. Como f es sobreyectiva $(f(G) = H)$, entonces existe $x \in G$ tal que $y = f(x)$. Por el teorema 1.2, $x = x_1 + x_2 + \ldots + x_n$ de manera única, luego

$$f(x) = f(x_1 + x_2 + \ldots + x_n)$$

$$y = f(x_1) + f(x_2) + \ldots + f(x_n)$$

entonces $y \in f(G_1) + f(G_2) + \ldots + f(G_n)$.

Ahora, supongamos que $y = y_1 + y_2 + \ldots + y_n$, $y_i \in f(G_i)$, entonces $y_i = f(t_i)$ para algún $t_i \in G_i$, $i = 1, 2, \ldots, n$ así

$$y_1 + y_2 + \ldots + y_n = f(x_1) + f(x_2) + \ldots + f(x_n)$$

$$y_1 - f(x_1) + y_2 - f(x_2) + \ldots + y_n - f(x_n) = 0$$

$$f(t_1) - f(x_1) + f(t_2) - f(x_2) + \ldots + f(t_n) - f(x_n) = 0$$

$$f((t_1 - x_1) + (t_2 - x_2) + \ldots + (t_n - x_n)) = 0$$

Como f es inyectiva, entonces

$$(t_1 - x_1) + (t_2 - x_2) + \ldots + (t_n - x_n) = 0$$

Por el teorema 1.3, $t_i - x_i = 0$, $i = 1, 2, \ldots, n$

$$t_i = x_i, \; i = 1, 2, \ldots, n$$

Luego $y_i = f(t_i) = f(x_i)$, $i = 1, 2, \ldots, n$

$$y = f(x_1) + f(x_2) + \ldots + f(x_n) \text{ de manera única}$$

En consecuencia $H = f(G_1) \oplus f(G_2) \oplus \ldots \oplus f(G_n)$.

Además, como f es un isomorfismo, entonces $f(G_i) \approx G_i$, $\quad i = 1, 2, \ldots, n$.

Por lo tanto G y H tienen el mismo tipo.

Reciprocamente,

Si G y H tienen el mismo tipo, entonces por el teorema 1.10 G y H son isomorfos.

Ejemplos:

(1) Un grupo cíclico de orden p^n, donde p es primo, $n \in \mathbb{Z}^+$, no se puede expresar como la suma directa de subgrupos no triviales.

En efecto, si $|G| = p^n$, entonces G es primario y su tipo es $(p^n; 0)$.

Luego, por el teorema 4,3 G no se puede expresar como la suma directa de más de un grupo.

(2) Sean G, H, K grupos abelianos finitamente generados.

Si $G \oplus H \approx G \oplus K$ entonces $H \approx K$

En efecto, si los tipos de G, H y K son $(g_1, g_2, \ldots, g_n; g)$ $(h_1, h_2, \ldots, h_n; h)$ $(k_1, k_2, \ldots, k_p; k)$ respectivamente, entonces el tipo de $G \oplus H$ es:

$$(a_1, a_2, \ldots, a_{m+n}; g + h)$$

y el tipo de $G \oplus K$ es:

$$(b_1, b_2, \ldots, b_{m+p}; g + k)$$

donde $a_1, a_2, \ldots, a_{m+n}$ son

$$g_1, g_2, \ldots, g_m, h_1, h_2, \ldots, h_n \text{ en algún orden}$$

y $b_1, b_2, \ldots, b_{m+p}$ son

$$g_1, g_2, \ldots, g_m, k_1, k_2, \ldots, k_p \text{ en algún orden.}$$

Además, como $G \oplus H \approx G \oplus K$, entonces por el teorema 4.4 sus tipos son iguales.

Luego, los tipos de H y K son iguales.

Por lo tanto, aplicando nuevamente el teorema 4.4 $H \approx K$

(3) El número de grupos abelianos de orden p^m donde p es primo, $m \in \mathbb{Z}^+$, es igual al número de maneras en que se puede escribir

$$m = r_1 + r_2 + \ldots + r_k$$

donde $r_i \in \mathbb{Z}^+$, $\quad i = 1, 2, \ldots, k \quad$ y $r_j \geq r_{j+1}$, $\quad j = 1, 2, \ldots, k-1$

En efecto, si $|G| = p^m$

(es decir, G es p-primario pero no necesariamente cíclico), entonces su tipo es de la forma:

$$(p^{r_1}, p^{r_2}, \ldots, p^{r_k}; 0)$$

donde $r_i \in \mathbb{Z}^+$, $\quad i = 1, 2, \ldots, k$ y $r_j \geq r_{j+1}$, $\quad j = 1, 2, \ldots, k-1$, luego:

$$\begin{aligned} p^m &= |G| \\ &= p^{r_1} p^{r_2} \ldots p^{r_k} \\ &= p^{r_1 + r_2 + \ldots + r_k} \end{aligned}$$

Por lo tanto $\quad m = r_1 + r_2 + \ldots + r_k$.

Como el tipo determina la estructura de G, entonces el número de grupos abelianos de orden p^m es igual al número de maneras en que se puede escribir

$$m = r_1 + r_2 + \ldots + r_k$$

Asi para $m = 2$, existen exactamente 2 grupos abelianos de orden p^2 (salvo isomorfismo) puesto que:

$$2 = 2, \quad 2 = 1 + 1$$

Para $m = 3$, existen exactamente 3 grupos abelianos de orden p^3 (salvo isomorfismo) puesto que:

$$3 = 3, \quad 3 = 2 + 1, \quad 3 = 1 + 1 + 1$$

Para $m = 4$, existen exactamente 5 grupos abelianos de orden p^4 (salvo isomorfismo) puesto que:

$$4 = 4, \quad 4 = 3 + 1, \quad 4 = 2 + 2, \quad 4 = 2 + 1 + 1, \quad 4 = 1 + 1 + 1 + 1$$

(4) Existen exactamente 12 grupos abelianos de orden 2700 salvo isomorfismo.

En efecto, como $2700 = 2^2 \times 3^3 \times 5^2$, entonces un grupo abeliano de orden 2700 es la suma directa de un grupo de orden 2^2, un grupo de orden 3^3 y un grupo de orden 5^2.

De acuerdo con el ejemplo anterior, existen exactamente 2 grupos abelianos de orden 2^2 (salvo isomorfismo), 3 grupos abelianos de orden 3^3 (salvo isomorfismos) y 2 grupos abelianos de orden 5^2 (salvo isomorfismo).

Por consiguiente, existen exactamente $2 \times 3 \times 2 = 12$ grupos abelianos de orden 2700 (salvo isomorfismo).

Bibliografía

[1] Dorronsoro J.; Hernández E. *Números, Grupos y Anillos*, Addison-Wesley Iberoamericana, España 1996

[2] Fraleigh, J.B. *Algebra Abstracta*, Addison-Wesley Iberoamericana, 1987

[3] Fuchs, L. *Abelian Groups*, Pergamon Press, Londres 1960.

[4] Fuchs, L. *Infinite Abelian Groups*, Vol I, Academia, Nueva York 1970.

[5] Gentile, Enzo R. *Estructuras Algebraicas II (Algebra Lineal)*, OEA, Washington D.C., 1967.

[6] Gentile, Enzo R. *Notas de Algebra*, Universidad de Buenos Aires, Argentina, 1965.

[7] Hall, Jr. Marshall. *The Theory of Groups*, MacMillan 1959.

[8] Herstein, I.N. *Algebra Abstracta*, Grupo Editorial Iberoamericana, México 1988.

[9] Kaplansky, Irving. *Infinite Abelian Groups*, University of Michigan Press, Ann Arbor, Michigan 1956.

[10] Ledermann, Walter. *Introducción a la Teoría de Grupos Finitos*, Dossat, Madrid 1948

[11] Rotman, Joseph J. *The Theory of Groups, An Introduction.* Allyn and Bacon, Boston 1966.

[12] Zassenhaus, Hans J. *The Theory of Groups*, Chelsea, New York 1958.