Universidad Michoacana de San Nicolás de Hidalgo

Facultad de Ciencias Físico Matemáticas "Mat. Luis Manuel Rivera Gutiérrez"

Tesis

Teoremas de Estructura y Clasificación en Grupos Abelianos

Para obtener el título de:

Licenciada en Ciencias Físico Matemáticas

Estefanía González Arroyo

Asesora:

Dra. María Luisa Pérez Seguí

Morelia, Michoacán, enero 2016

Índice general

Resumen

El trabajo consiste en estudiar los resultados clásicos sobre teoremas de estructura y clasificación de distintas clases de grupos abelianos. Se dan las definiciones generales, así como los resultados importantes de teoría de grupos necesarios para poder establecer los teoremas.

Las distintas clases para los que se establecen los teoremas de estructura y clasificación son los siguientes:

• Los *grupos cíclicos* (aquéllos generados por un solo elemento). Éstos son $\mathbb{Z}$ y $\mathbb{Z}_n$, con $n \in \mathbb{N}$.

•Los *grupos divisibles* (aquéllos en los que la ecuación $nx = a$ siempre tiene solución para $n \in \mathbb{N}$ y a en el grupo A). Éstos resultan ser sumas directas en forma única de copias de $\mathbb{Q}$ (el grupo de los números racionales) y copias de $\mathbb{Z}_{p^\infty}$ para primos p.

•Los *grupos libres* (aquéllos que tienen base). Éstos son suma directa de copias de $\mathbb{Z}$ y están determinados por su rango (o dimensión).

•Los *grupos finitamente generados* (aquéllos que pueden generarse con sólo un número finito de elementos). Aquí el teorema de estructura y clasificación dice que son de la forma con:

$$\mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \cdots \oplus \mathbb{Z}_{d_n} \oplus \mathbb{Z}^r, \ \ con \ \ d_1|d_2|\cdots|d_n.$$

•Los *grupos racionales* (subgrupos de $\mathbb{Q}$). Estos grupos quedan determinados de manera única por su *tipo*, el cual es la clase de equivalencia (según cierta relación) de sucesiones de números en $\mathbb{N} \cup \{0, \infty\}$. En particular se ve que hay una cantidad no numerable de grupos racionales no isomorfos.

abelianos, divisibles, finitamente, generados, racionales.

Abstract

This work consists in studying the classical results of structure and classification theorems of different types of abelian groups. We give the general definitions, as well as the important results of group theory which are necessary for establishing the theorems.

The different types for which the structure and classification theorems are established are the following:

- *Cyclic groups* (those generated for only one element). These are $\mathbb{Z}$ and $\mathbb{Z}_n$ where $n \in \mathbb{N}$.

- *Divisible groups* (those in which the equation $nx = a$ has always solution for $n \in \mathbb{N}$ and a in the group A). These groups are direct sums of $\mathbb{Q}$-copies ($\mathbb{Q}$ the rational group) and $\mathbb{Z}_{p^\infty}$-copies for some p primes.

- *Free groups* (those which have a base). These are direct sum of $\mathbb{Z}$-copies and they are determinate by its rank (dimension).

- Finitely generated groups (those generated by a finite set). We can write them as follow:

  $$\mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \cdots \oplus \mathbb{Z}_{d_n} \oplus \mathbb{Z}^r$$

  where $d_1|d_2|\cdots|d_n$.

- *Rational groups* (subgroups of $\mathbb{Q}$). These groups are determined by its *type* in a unique form, which is a equivalence relation (according to certain relation) of number sequences with elements in $\mathbb{N} \cup \{0, \infty\}$. Particularly, it is shown that there is a uncountable quantity of them.

Agradecimientos

Quiero agradecer en primer lugar a mi madre que me ha dado todo lo que ha podido y más. Me ha apoyado incondicionalmente y sin ella no sería lo que soy ahora. Gracias por tu amor, compresión y regaños.

A mis hermanos por siempre estar ahí, por enseñarme tantas cosas, por quererme y por hacerme reír. Lenin que siempre nos cuida y apoya, por ayudarme en física. Perla que siempre me induce a hacer lo correcto y a esforzarme. A Gil que siempre ha creído en mi, que me apoya, que me ayuda, por ser mi hermano pequeño. A Diana la chica más genial que he conocido, me has enseñado tantas cosas, tú que siempre estás tan alegre. A mi papá por se mi papá.

A mis profesores, en especial a Malú por su paciencia al realizar este trabajo, sé que no he sido la mejor alumna. Por los conocimientos transmitidos, por extenuante trabajo que es revisar lo que escribo.

A Jonathan, que ha estado todo este tiempo. Aún no sé como has podido soportarme, gracias por tu paciencia. Gracias por tu cariño, por todas esas tardes de estudio, por las enseñanzas, por todas las pláticas y por hacerme sonreír tanto. Gracias por la confianza, te quiero tanto.

A Manuel, gracias por quererme tanto. Tú que siempre estás ahí cuando te necesito. Gracias por aguantarme, por mis absurdas peticiones y por soportar mis días de mal humor. Me inspira tu dedicación y tu amor por las matemáticas. Te quiero.

A Asminda, que siempre está ahí,por tu amistad, por la paciencia, por la ayuda, por escuchar mis problemas,por la cofianza y por enseñarme que hay que ganarse las cosas. Te deseo lo mejor, te quiero.

A mis amigos y compañeros de Fismat con los que comencé en especial a Manolo, Memo, Kim, Fanny y Jorch.

A mis queridos Tutuuti, Saraí, Alan y Caty.

Introducción

Los grupos son estructuras importantes dentro del estudio de las matemáticas, en particular tenemos cierto tipo de grupo denominado *abelianos* que son aquéllos en los que la operación de grupo es conmutativa; como son $\mathbb{Z}$, $\mathbb{Q}$, $n\mathbb{Z}$. La notación usual para denotar la operación dentro de lo grupos abelianos es la aditiva; así la operación se denota como $+$, el neutro como 0 y el inverso de un elemento a como $-a$. Por otro lado los grupos abelianos son $\mathbb{Z}$-módulos y los $\mathbb{Z}-$*módulos* son grupos abelianos, es decir, los grupos abelianos coinciden con los $\mathbb{Z}$-módulos.

La estructura de los grupos abelianos como $\mathbb{Z}$-módulos nos permite estudiarlos de una manera muy diferente a la de los grupos no abelianos. Cada una de estas estructuras tiene sus dificultades particulares. Lo que buscaremos es dar teoremas de estructura y clasificación en ciertos tipos de grupos abelianos.

En el primer capítulo vemos algunas nociones básicas y resultados de grupos abelianos y enunciamos algunos resultados que nos serán útiles en el desarrollo posterior de este trabajo, además de probar algunos resultados importantes como lo son el Lema del 5 y el Tercer Teorema de Isomorfismo.

En los siguientes capítulo damos las nociones de grupos cíclicos, cocíclicos, de torsión y divisibles, además de la noción de suma directa en grupos abelianos. Respecto al tema de estructura y clasificación en grupos abelianos veremos que los grupos cíclicos son isomorfos a $\mathbb{Z}$ o a $\mathbb{Z}_n$ con $n \in \mathbb{N}$. Los cocíclicos a $\mathbb{Z}_{p^k}$ con $k \in \mathbb{N} \cup \{\infty\}$. Los grupos de torsión son sumas directas de sus partes $p-$primarias, y los grupos divisibles son sumas directas de $\mathbb{Q}$ y sumas $\mathbb{Z}_p^\infty$ para ciertos p primos de manera

única.

En el capítulo 4 hablamos de grupos libres que son aquéllos que tienen una estructura parecida a la de los espacios vectoriales ya que poseen una base.

Más adelante damos el teorema de estructura y clasificación de grupos abelianos finitamente generado que nos dice que un grupo abeliano finitamente generado se puede ver como $\mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \cdots \oplus \mathbb{Z}_{d_n} \oplus \mathbb{Z}^r$ con $d_1|d_2|\cdots|d_n$.

Por último hablamos de los subgrupos de $\mathbb{Q}$, llamados grupos racionales y veremos que hay una cantidad infinita de grupos racionales no isomorfos, además de que también daremos un teorema de clasificación de éstos.

Capítulo 1

Preliminares

En este capítulo enunciamos algunos conceptos básicos de grupos abelianos necesarios para los siguientes capítulos, así como teoremas de matemáticas en general que nos serán útiles. Además demostramos algunas propiedades importantes de grupos abelianos.

A los grupos donde todos los elementos conmutan se les llama grupos abelianos. Estos son exactamente los $\mathbb{Z} - m\acute{o}dulos$. La notación usual en grupos abelianos es la aditiva. Si B es un subgrupo de A escribimos $B \leq A$.

Definición 1.1. Se denomina *orden* de a, $o(a)$, al menor $n \in \mathbb{N}$ tal que $na = 0$.

De la definición anterior tenemos que si $na = ma$, $o(a)|n - m$.

Definición 1.2. El conjunto de elementos de orden finito de A, $t(A)$, se llama *parte de torsión* de A. Si $t(A) = A$ se dice que A es un *grupo de torsión*. Si $t(A) = 0$ se dice que A es *libre de torsión*; si no ocurre nada de lo anterior se dice que A es *mixto*.

Tenemos que $A/t(A)$ es libre de torsión y $t(A)$ el es menor subgrupo que hace que el cociente sea libre de torsión.

Definición 1.3. Para p primo, el conjunto de elementos de orden potencia de p, $t_p(A)$, es un subgrupo de A llamado *parte p-primaria* de A.

Definición 1.4. Si $A = t_p(A)$ decimos que A es *p-primario* o *p-grupo.*

Definición 1.5. Si A es un p-grupo y $o(a) = p^k$, decimos que k es el *exponente* de a y escribimos $e(a) = k$.

Definición 1.6. Definimos $A[n] = \{a \in A : na = 0\} = \{a \in A : o(a)|n\}$.

Definición 1.7. El *soclo* de A, $S(A)$, es el subgrupo de A de todos lo elementos de orden finito libre de cuadrados.

Podemos ver que $a \in S(A)$ si, y sólo si, $a = 0$ o existen $p_1, p_2, \ldots, p_k$ primos distintos tales que $o(a) = p_1 p_2 \cdots p_k$. Así tenemos que si A es un p-grupo entonces $S(A) = A[p]$.

Definición 1.8. Llamamos *elemental* a un grupo A si $A = S(A)$.

Definición 1.9. Definimos $nA = \{na : a \in A\}$. Éste es un subgrupo de A que consta de los elementos divisibles por n.

Definición 1.10. Un grupo A es *n-divisible* si $A = nA$; es *divisible* si es n-divisible para todo n.

Definición. 1.11. Un *subgrupo invariante* es aquél tal que dado cualquier endomorfismo de A, la imagen del subgrupo cae dentro de él mismo.

Definición 1.12. La *p-altura* de a es k, en símbolos $h_p(a) = k$, si $a \in p^k A \setminus p^{k+1}A$; si $a \in \bigcap_k p^k A$ decimos que a tiene *p-altura infinita* y escribimos $h_p(a) = \infty$.

Dado un homomorfismo $f : A \to B$, tenemos lo siguiente; si A es finitamente generado (o cíclico) entonces también lo es $f(A)$. Además tenemos que $f(nA) \subset nB, f(t(A)) \subset t(B), f(t_p(A)) \subset t_p(B), f(A[n]) \subset B[n]$ y $f(S(A)) \subset S(B)$. Esto nos dice que los subgrupos $nA, t(A), t_p(A), S(A)$ y $A[n]$ son invariantes. Respecto a la altura, vemos que $h_p(a) \leq h_p(f(a))$, y si a es de orden finito, $o(f(a))|o(a)$.

Dado $a \in A$ hay un único homomorfismo $f : \mathbb{Z} \to A$ que manda al 1 en a; éste está dado por $f(z) = za$.

Definición 1.13. Una sucesión

$$A \xrightarrow{f} B \xrightarrow{g} C$$

es exacta si $Im(f) = Ker(g)$. Esto es, $g \circ f = 0$, y si $g(b) = 0$ entonces existe $a \in A$ tal que $f(a) = b$.
Una sucesión $\cdots \to A_{n-1} \to A_n \to A_{n+1} \cdots$ es exacta si lo es en cada A_n.
Las sucesiones exactas de la forma

$$0 \to A \to B \to C \to 0,$$

donde la primera y la última flecha representan los homomorfismo triviales, se llaman *sucesiones exactas cortas*.

Enunciemos algunos resultados que nos servirán mas adelante.

1. $0 \longrightarrow A \xrightarrow{f} B$ es exacta si, y sólo si, f es monomorfismo.

2. $A \xrightarrow{f} B \longrightarrow 0$ es exacta si, y sólo si, f es epimorfismo.

3. Dado un monomorfismo $A \xrightarrow{i} B$ tenemos una sucesión exacta corta

   $$0 \longrightarrow A \xrightarrow{i} B \xrightarrow{\rho} B/i(A) \longrightarrow 0,$$

   donde ρ es la proyección natural.

4. Dado un epimorfismo $B \xrightarrow{\rho} C$ tenemos una sucesión exacta corta

   $$0 \longrightarrow Ker(\rho) \xrightarrow{i} B \xrightarrow{\rho} C \longrightarrow 0,$$

   donde i es la inclusión.

   Los siguientes son teoremas conocidos e importantes de álgebra.
   Propiedad universal del núcleo. El núcleo de un homomorfismo $f : A \to B$, junto con la inclusión $i : Ker(f) \to A$, cumplen $f \circ i = 0$ y si $g : C \to A$ es tal que $f \circ g = 0$, entonces existe un único homomorfismo $\overline{g} : C \to Ker(f)$ tal que $i \circ \overline{g} = g$ (g se factoriza a través del $Ker(f)$).

   La *Propiedad universal del grupo cociente* Sea $B \leq A$; entonces A/B y la proyección natural $\pi : A \to A/B$ satisfacen que $\pi(B) = 0$, y además si f :

$A \to C$ es un homomorfismo tal que $f(B) = 0$, entonces existe un único homomorfismo $\overline{f} : A/B \to C$ tal que $\overline{f} \circ \pi = f$. Aquí $\overline{f}$ está definida como $\overline{f}(a + B) = f(a)$.

El *Primer Teorema de Isomorfismo* Sea $f : A \to B$ un homomorfismo; entonces $Im(f) \approx A/Ker(f)$.

El *Teorema de la correspondencia* Establece que los subgrupos de un cociente A/B se corresponden de manera biyectiva a través de la proyección natural π con los subgrupos de A que contienen a B, es decir, $C \leftrightarrow C/B$.

Un lema de conjuntos necesario para algunas demostraciones es el *Lema de Zorn*, lo enunciaremos a continuación.

Lema de Zorn: Sea $\mathcal{X}$ un conjunto no vacío que tiene definido un orden parcial en el que cada subconjunto totalmente ordenado $\mathcal{C}$ llamado *cadena* está acotado superiormente. Entonces $\mathcal{X}$ tiene elementos maximales.

A continuación probaremos dos resultados de grupos divisibles.

Proposición. 1.14. La imagen de un grupo divisible bajo un homomorfismo es también divisible.

Demostración. Sean D un grupo divisible y $\phi : D \to A$ un homomorfismo. Sea $d \in D$, como D es divisible para cualquier $n \in \mathbb{N}$, $d = nd'$, así $\phi(d) = \phi(nd') = n\phi(d')$, de donde vemos que la $Im(D)$ es divisible. ■

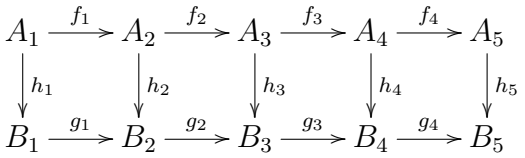
Lo anterior nos dice que en particular el cociente de un divisible es divisible.

Proposición. 1.15. Si A es un p-grupo, entonces es q-divisible para todo primo q diferente de p.

Demostración. Sea $a \in A$ tal que $p^k a = 0$. Como p y q son primos, tenemos que $1 = p^k m + qn$ para algunos n y m enteros, multiplicando por a, $a = (p^k m)a + (qn)a = q(na)$. Así A es q-divisible. ■

Ahora demostraremos algunos resultados menos estándar que nos serán útiles.

Lema. 1.16. *Lema del 5.* Supongamos que el siguiente es un diagrama conmutativo en el que los dos renglones son exactos.



a) Si h_2 y h_4 son monomorfismos y h_1 es epimorfismo, entonces h_3 es monomorfismo.

b) Si h_2 y h_4 son epimorfismos y h_5 es monomorfismo, entonces h_3 es epimorfismo.

Demostración. a) Sea $a_3 \in A$ tal que $h_3(a_3) = 0$. Entonces $g_3(h_3(a_3)) = 0 = h_4(f_3(a_3))$. Pero h_4 es monomorfismo así que $f_3(a_3) = 0$, de donde $a_3 \in ker(f_3) = im(f_2)$. Entonces existe $a_2 \in A_2$ tal que $f_2(a_2) = a_3$ de ahí vemos que $h_3(f_2(a_2)) = g_2(h_2(a_2))$. Así $h_2(a_2) \in Ker(g_2) = Im(g_1)$, luego $h_2(a_2) = g_1(b_1)$ para algún $b_1 \in B$ y existe $a_1 \in A$ tal que $h_1(a_1) = b_1$ y h_1 es epimorfismo. Ahora $h_2(a_2) = g_1(h_1(a_1)) = h_2(f_1(a_1))$ y h_2 es monomorfismo de donde $a_2 = f_1(a_1)$, con lo cual $a_3 = f_2(f_1(a_1)) = 0$ y, por lo tanto, h_3 es monomorfismo. ■

b) Sea $b_3 \in B_3$. Como h_4 es epimorfismo existe $a_4 \in A_4$ tal que $g_3(b_3) = h_4(a_4)$ y $g_4(g_3(b_3)) = 0 = h_5(f_4(a_4))$, de donde $a_4 \in Ker(f_4) = Im(f_3)$. Por lo tanto existe $a_3 \in A_3$ tal que $f(a_3) = a_4$, de donde $h_4(f_3(a_3)) = h_4(a_4) = g_3(b_3)$ y entonces $g_3(h_3(a_3)) = g_3(b_3)$. Esto dice que $b_3 - h_3(a_3) \in Ker(g_3) = Im(g_2)$; luego existe $b_2 \in B_2$ y $a_2 \in A_2$ tal que $h_2(a_2) = b_2$; entonces $b_3 - h_3(a_3) = g_2(b_2)$ de donde $b_3 = h_3(a_3) + g_2(h_2(a_2)) = h_3(a_3) + h_3(f_2(a_2)) = h_3(a_3 + f(a_2))$, es decir, h_3 es epimorfismo. ■

Proposición. 1.17. Un subgrupo B de A es maximal si, y sólo si, $[A : B]$ es primo.

Demostración. Por el teorema de la correspondencia, los subgrupos del cociente A/B se corresponden de manera biyectiva con los subgrupos de A que contienen a B. Como el orden de A/B es primo si, sólo si, no tiene subgrupos propios, se tiene que B es maximal, si, sólo si, $[A : B]$ es primo. ■

Proposición. 1.18. Sea $\{B_i : i \in I\}$ una familia de subgrupos de A. Entonces existe un monomorfismo $f : A/\bigcap_i B_i \to \Pi_i A/B_i$.

Demostración. Definimos el homomorfismo $f : A \to \Pi_i A/B_i$ de manera que $a \to (a + B_i)_i$ con $a \in A$. Hay que ver que f es inyectivo. Si $f(a + \bigcap_i B_i) = (B_i)_i$ es porque $a \in B_i$ para todo $i \in I$, es decir, $a \in \bigcap_i B_i$, por lo tanto el $Ker(f) = \bigcap_i B_i$. ■

Proposición. 1.19. Si $a, b \in A$ entonces $h_p(a+b) \geq min\{h_p(a), h_p(b)\}$. Se da la igualdad si $h_p(a) \neq h_p(b)$.

Demostración. Sean $h_p(a) = k$ y $h_p(b) = l$. Supongamos $k \leq l$; entonces $a = p^k x_1$ y $b = p^l x_2$ para $x_1, x_2 \in A$, y así $a+b = p^k x_1 + p^l x_2 = p^k(x_1 + p^{l-k} x_2)$. De aquí tenemos $h_p(a+b) \geq k = min\{h_p(a), h_p(b)\}$. Si $h_p(b) \neq h_p(a)$; entonces p no divide a $x_1 + p^{l-k} x_2$, por lo tanto $h_p(a + b) = min\{h_p(a), h_p(b)\}$. ■

Proposición. 1.20. Si $B \leq A$, entonces $t(B) = t(A) \bigcap B$ y $S(B) = S(A) \bigcap B$.

Demostración. Sea $a \in t(B)$; entonces $na = 0$ para algún $n \in \mathbb{N}$ y $a \in B$; y de ahí vemos que $a \in t(A) \bigcap B$. Si $a \in t(A) \bigcap B$, tenemos que $a \in t(A)$ y $a \in t(B)$, así que existe un $n \in \mathbb{N}$ tal que $na = 0$ y por esto $a \in t(B)$. Por lo tanto $t(B) = t(A) \bigcap B$.

Sea $b \in S(B)$; entonces $o(b) = p_1 p_2 \cdots p_k$ para algunos primos distintos p_i así que $b \in S(A)$ y, como $b \in B$, tenemos que $b \in S(A) \bigcap B$.
Si $b \in S(A) \bigcap B$, $b \in B$ y $o(b) = p_1 p_2 \cdots p_k$ por lo tanto $b \in S(B)$. ■

De la proposición anterior podemos ver que si $B \leq A$, entonces $t(B) \leq t(A)$.

El siguiente teorema es conocido como el *tercer teorema de isomorfismo.*

Proposición. 1.21. Si B y C son subgrupos de A, entonces, existe un diagrama conmutativo con renglones exactos.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B\cap C & \longrightarrow & B & \longrightarrow & B/B\cap C & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & C & \longrightarrow & B+C & \longrightarrow & (B+C)/C & \longrightarrow & 0 \end{array}$$

Demostración.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B\cap C & \xrightarrow{i_b} & B & \xrightarrow{\rho} & B/B\cap C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle i_c} & & \downarrow{\scriptstyle i_B} & \searrow^{\varphi} & \downarrow{\scriptstyle \phi} & & \\ 0 & \longrightarrow & C & \xrightarrow{i_C} & B+C & \xrightarrow{\pi} & (B+C)/C & \longrightarrow & 0 \end{array}$$

Sean i_b, i_c, i_C, i_B las inclusiones naturales y sean ρ y π la proyecciones naturales. Es claro que con estos homomorfismos las sucesiones son exactas.
Sea $\varphi : B \longrightarrow (B+C)/C$ el homomorfismo dado por $b \to b + C$. Entonces $Ker(\varphi) = B \cap C$ y φ es suprayectivo. Ahora, por el primer teorema de isomorfismo, $B/(B\cap C) \approx (B+C)/C$ y así el diagrama conmuta.

■

Proposición. 1.22. Si $n \in \mathbb{N}$ entonces existe una sucesión exacta corta.

$$0 \to A[n] \to A \to nA \to 0$$

Demostración. Sea i la inclusión de $A[n]$ en A. Definimos $\rho : A \to nA$ para $a \in A$ de manera que $a \to na$. Hay que ver que esto nos hace exacta a la sucesión. Sea $a \in ker(\rho)$; entonces $\rho(a) = na = 0$ y así $Ker(\rho) = A[n] = Im(i)$ por lo tanto la sucesión es exacta corta. ■

Proposición. 1.23. Sea $0 \to A \to B \to C \to 0$ una sucesión exacta. Si A y C son finitamente generados B también lo es.

Demostración. Sean $f_1 : A \to B$ y $f_2 : B \to C$ los homomorfismos de la sucesión exacta. Si $b \in B$, tenemos que $f_2(b) = c = n_1c_1 + n_2c_2 + \cdots + n_kc_k$ con $c \in C$; como f_2 es epimorfismo, existen $b_1, b_2, \ldots, b_k$ tales que $f(b_i) = c_i$ para $i = 1, 2, \ldots, k$, $f_2(b) - (n_1f_2(b_1) + n_2f_2(b_2) + \cdots + n_kf_2(b_k)) = 0$; entonces

$b-(n_1b_1+n_2b_2+\cdots+n_kb_k)\in Ker(f_2)=im(f_1)$. Ahora, existe $a\in A$ tal que $f_1(a)=b-(n_1b_1+n_2b_2+\cdots+n_kb_k)$ y, como A es finitamente generado, $a=m_1a_1+m_2a_2+\cdots+m_la_l$; así $b=(n_1b_1+n_2b_2+\cdots+n_kb_k)+m_1f_1(a_1)+m_2f_1(a_2)+\cdots+m_lf_1(a_l)$. ■

Proposición. 1.24. Si $m,n\in\mathbb{N}$ son primos relativos, entonces la función $\mathbb{Z}\to\mathbb{Z}_m\times\mathbb{Z}_n$ dada por $a\longrightarrow(a+m\mathbb{Z},a+n\mathbb{Z})$ es un homomorfismo con núcleo $mn\mathbb{Z}$.

Demostración. Es claro que es un homomorfismo porque lo es en cada coordenada. Sea $a\in Ker(\varphi)$; entonces $\varphi(a)=(a+m\mathbb{Z},a+n\mathbb{Z})=(m\mathbb{Z},n\mathbb{Z})$. Así $a\in m\mathbb{Z}$ y $a\in n\mathbb{Z}$, por lo tanto a es múltiplo de m y de n, y de aquí que $a=rm=sn$ para $r,s\in\mathbb{Z}$; como m y n son primos relativos, a pertenece a $mn\mathbb{Z}$.

■

Teorema. 1.25. *Teorema chino del residuo.* Sean m y n primos relativos. Dados $a,b\in\mathbb{Z}$ existe $x\in\mathbb{Z}$ tal que $x\equiv a(mod\,m)$ y $x\equiv b(mod\,n)$; además el conjunto de soluciones es una clase módulo mn.

Los espacios vectoriales tienen una buena estructura. Cada espacio tiene asignado un invariante que es la dimensión. Ésta está dada por la cardinalidad de la base, pues todos los espacios vectoriales tienen base y todas las bases de un espacio vectorial tienen la misma cardinalidad. Probemos esto.

Teorema. 1.26. Todo espacio vectorial V tiene una base. Más aún todo conjunto independiente Y se puede completar a una base.

Demostración. Sea $\mathcal{X}=\{X:Y\subset X\subset V$ y X es independiente$\}$. Este conjunto es diferente del vacío pues $Y\in\mathcal{X}$. Sea $\mathcal{C}=\{X_i:i\in I\}$ una cadena de $\mathcal{X}$. Veamos que $\bigcup_i X_i$ es cota superior. Si escribimos a 0 como combinación lineal de elementos de $\bigcup_i X_i$ como sólo tomamos una cantidad finita de elementos éstos están en un X_j para algún j y como es un conjunto linealmente independiente, los coeficientes de la combinación son cero. Por

lema de Zorn tiene un conjunto independiente maximal X_0. Veamos que X_0 genera. Supongamos que existe $x \in V \setminus < X_0 >$. Entonces x no es combinación lineal de elementos de X_0 y así $\{X_0 \cup \{x\}\}$ sería independiente. ■

Teorema. 1.27. Dos bases de un espacio vectorial tienen la misma cardinalidad.

Demostración. Sean B y C dos bases de un espacio vectorial V. Supongamos que $|C| < |B|$.
Caso infinito: Como cada $c \in C$ se puede escribir como una combinación finita de elementos de B, tomemos un conjunto B' conformado de los elementos que generan a los elementos de C, el cual genera a V; así que B' genera a V. Como tomamos sólo una cantidad finita de elementos de B como combinación lineal de elementos de C, tenemos que $|B'| < |B|$. Entonces sea $b \in B \setminus B'$. Podemos escribir a b como combinación lineal de elementos de C que su vez escribimos como combinación lineal de elementos de B', de donde b se escribe como combinación lineal de elementos de B' y esto nos da una combinación lineal de 0 que no es trivial, con elementos de B.
Caso finito: Tenemos que $B = \{b_1, b_2, \ldots, b_n\}$ y $C\{c_1, c_2 \ldots, c_m\}$ con $m < n$. Entonces si escribimos a cada b_i como combinación lineal de los elementos de C formamos una matriz con un número mayor de renglones que de columnas y por el rango de la matriz vemos que algunos renglones son combinaciones lineales de los otros. ■

Como acabamos de ver, los espacios vectoriales tienen base y están totalmente definidos por el tamaño de la base; de esta manera, dados el campo sobre el que está y la dimensión sabemos cuál es nuestro espacio vectorial. Nuestro propósito es buscar algunos invariantes para nuestros grupos. A cada grupo se le puede asociar de manera natural algunos espacios vectoriales. Las dimensiones de éstos nos proporcionan algunos invariantes. Tenemos por ejemplo que los siguientes subgrupos son espacios vectoriales sobre $\mathbb{Z}_p$.

Proposición. 1.28. Si A es un grupo tal que $pA = 0$, entonces A es un $\mathbb{Z}_p$ espacio vectorial.

Demostración. Definimos la multiplicación por escalares en A como $(\overline{n}, a) \mapsto na$. Veamos que está bien definida la operación. Sea $n \equiv n'$, entonces $p|n - n'$ así $(n - n')a = 0$, de donde $na = n'a$. ■

Corolario. 1.29. $A[p]$ y A/pA tienen estructura natural de $\mathbb{Z}_p$-espacios vectoriales.

Capítulo 2

Clases importantes de grupos

En este capítulo vemos algunas clases importantes de grupos: los cíclicos, cocíclicos, los grupos de torsión y las sumas directas en grupos abelianos.

2.1. Grupos cíclicos

Los grupos cíclicos son aquéllos generados por un solo elemento.

$$A = < a > = \{na : n \in \mathbb{Z}\}$$

Si existe $n \in \mathbb{N}$ tal que $na = 0$, el orden de A es igual a n y $A \approx \mathbb{Z}_n$. Si no hay tal n, entonces $o(a) = \infty$ y $A \approx \mathbb{Z}$. Sólo hay estos dos casos. Así $\mathbb{N} \cup \{\infty\}$ nos proporciona una lista completa de invariantes y cada elemento de $\mathbb{N} \cup \{\infty\}$ corresponde a un único grupo cíclico.

Estos grupos son muy simples porque están generados por un único elemento. Veamos que elementos del grupo pueden generarlo. Ya dijimos que los grupos cíclicos son isomorfos a $\mathbb{Z}$ o a $\mathbb{Z}_n$ así podemos dar de manera más fácil a los generadores.

Proposición. 2.1. a) En $\mathbb{Z}$ los generadores son 1 y -1.
b) En $\mathbb{Z}_n$, a es generador si, y sólo si, es primo relativo con n.

Demostración. a) Sea $n \in \mathbb{Z}$. Podemos escribirlo como $n(1) = -n(-1) = n$, así tanto 1 como -1 genera. Es claro que son los únicos.
b) $\Rightarrow$) Sea $d = mcd(a, n)$; de donde $\frac{n}{d}\overline{a} = 0$ y $<\overline{a}> = \{\overline{a}, 2\overline{a}, 3\overline{a} \ldots, \frac{n}{d}\overline{a}\}$. Si a genera a $\mathbb{Z}_n$, entonces $<a>$ tiene n elementos, así $d = 1$.
$\Leftarrow$) Sea a primo relativo con n; entonces podemos escribir $ar + ns = 1$. Sea $b \in \mathbb{Z}$; vemos que $b = b(ar)+b(ns)$; entonces $\overline{b} = br\overline{a}$ por lo tanto $\overline{b} \in < a >$. ■

Además, los subgrupos de un cíclico son cíclicos y podemos decir cuáles son.

Proposición. 2.2. Sea $B \leq A$. Si A es cíclico, $A =< a >$, entonces B es cíclico.

Demostración. Si $B = 0$ no hay nada que probar. Si no tomemos

$$S = \{n \in \mathbb{N} : na \in B\}.$$

Como S no es vacío podemos tomar $n_0 = min\{S\}$. Queremos ver que $B =< n_0a >$, para esto hay que ver que $n_0|n$. Sea $b \in B$, $b = na$; entonces $n = n_0s+r$, para cierta r tal que $0 \leq r < n_0$; de aquí, $ra = na - n_0as \in B$. De la minimalidad de n_0 deducimos que $r = 0$, y así $B \subset < n_0a >$. La otra contención es obvia. ■

Corolario. 2.3. Los subgrupos de $\mathbb{Z}$ son los $k\mathbb{Z}$ para $k \in \mathbb{N}$. Los subgrupos de $\mathbb{Z}_n$ son los $k\mathbb{Z}_n \approx \mathbb{Z}_m$, con $m = \frac{n}{mcd(n,k)}$.

Proposición. 2.4. Si m divisor de n, entonces existe un único $B \leq \mathbb{Z}_n$ de orden m.

Demostración. Vemos que existe, con $B =< \frac{n}{m} >$. Para ver que es único basta ver que si $(a, n) = d$, entonces $< \overline{a} > =< \overline{d} >$. Tenemos que $< \overline{a} > = \{\overline{a}, 2\overline{a}, 3\overline{a}, \ldots, \frac{n}{d}\overline{a}\}$ y que $< d > = \{\overline{d}, 2\overline{d}, 3\overline{d} \ldots, \frac{n}{d}\overline{d}\}$. Como $< \overline{a} > \subset < \overline{d} >$ y tienen la misma cantidad de elementos entonces son iguales. ■

Podemos dar otra caracterización de un grupo cíclico. Si para cada divisor del orden del grupo existe un único subgrupo de este orden tenemos que nuestro grupo es cíclico. Veamos algunos lemas para poder probar esto.

Nota. 2.5. La función φ de Euler se define como $\varphi = |\{n \in \mathbb{N} : n \leq m \text{ y } (m,n) = 1\}$. Partamos $\mathbb{Z}_n$ en conjuntos $X_d = \{x : x \in \mathbb{Z}_n \ y \mid < x > | = d\}$. Entonces $|X_d| = \varphi(d)$; pues $X_d = \{\frac{n}{d}\overline{a} : mcd(a,d) = 1 \text{ y } a \leq d\}$.

Lema. 2.6. Sea $n \in \mathbb{N}$. Entonces $n = \sum \varphi(d)$, con d divisor de n y d entre 1 y n.

Demostración. Lo generado por cada $a \in \mathbb{Z}_n$ es de tamaño d para algún d divisor de n, es decir, $a \in X_d$. Entonces $\mathbb{Z}_n$ es la unión ajena de los conjuntos X_d. Por la nota anterior $|X_d| = \varphi(d)$; por lo tanto $n = \sum \varphi(d)$. ■

Lema. 2.7. Sea A grupo de orden n. Entonces A es cíclico, si y sólo si, para cada d divisor de n, A tiene a lo más un grupo cíclico de orden d.

Demostración. ($\Rightarrow$) Se sigue de 2.4.
($\Leftarrow$) Para cada C subgrupo cíclico de A, tomamos al conjunto de generadores X_C. Sabemos que A es la unión ajena de los X_C y que $|X_C| = \varphi(d)$ si C es cíclico de orden d. Entonces

$$n = \sum_C |X_C| \leq \sum_d \varphi(d) = n,$$

de donde A tiene exactamente un subgrupo de orden d, para cada d divisor de n. ■

Proposición. 2.8. Un grupo C es cíclico si, y sólo si, existe $c \in C$ tal que si $f : A \to C$ es tal que $c \in Im(f)$, entonces f es epimorfismo.

Demostración. ($\Rightarrow$) Sea C cíclico, es decir, $C = < c >$ para algún $c \in C$; si existe $a \in A$ tal que $f(a) = c$, para $f : A \to B$ homomorfismo, entonces $f(na) = nf(a) = nc$, por lo tanto f es un epimorfismo.
($\Leftarrow$) Tomamos $A = < c >$ y f como la inclusión. Como f es suprayectiva $C = < c >$. ■

2.2. Grupos cocíclicos.

Utilizamos la última proposición que nos da una equivalencia de grupo cíclico, para definir de manera dual a los grupos cocíclicos es dual.

Definición. 2.9. Un grupo C es *cocíclico* si hay un elemento $c \in C$, tal que si $f : C \to A$ es tal que $c \notin Ker(f)$, entonces f es monomorfismo.

Lema. 2.10. Si C es cocíclico con cogenerador c, entonces c pertenece a todo subgrupo no cero.

Demostración. Sea $B \leq C$, $B \neq 0$, y sea $f : C \to C/B$ la proyección natural. Como c es cogenerador y f no es monomorfismo, entonces $c \in Ker(f)$, por lo tanto $c \in B$. ■

Lema. 2.11. C es cocíclico si, y sólo si, C tiene un subgrupo menor A (no cero). En este caso A es cíclico de orden primo generado por c, un cogenerador C.

Demostración. ($\Rightarrow$) Por el lema anterior $c \in \bigcap_{0 \neq B \leq C} B$; además $< c >$ es un subgrupo de C y es el menor que contiene a c, entonces se da la igualdad.
($\Leftarrow$) Sea A el menor subgrupo de C con A cíclico de orden primo. Tomemos un generador a y sea $f : C \to B$ tal que $a \neq Ker(f)$. Vemos que $Ker(f) = 0$; si no tendríamos que $A \subset Ker(f)$ y así a pertenecería a $Ker(f)$. ■

Corolario. 2.12. Si C es cocíclico entonces C es p-grupo para algún primo p.

Demostración. Sea p el orden de c un cogenerador de C. Supongamos que existe $a \in C$ tal que $o(a)$ no es una potencia de p; entonces $c \notin < a >$. ■

Proposición. 2.13. $\mathbb{Z}_{p^n}$ es cocíclico con cogenerador $\overline{p}^{n-1}$

Demostración. Los subgrupos de $\mathbb{Z}_{p^n}$ están encadenados; entonces es claro que es cocíclico, y como el menor subgrupo es el generado por $\overline{p}^{n-1}$, se tiene que éste es el cogenerador. ■

Construiremos otros grupos cocíclicos.

Definimos $\mathbb{Z}_{p^\infty}$ como la parte p-primaria de $\mathbb{Q}/\mathbb{Z}$. Entonces

$$\mathbb{Z}_{p^\infty} = \left\{ \frac{a}{p^k} + \mathbb{Z} : a \in \mathbb{Z}, k \in \mathbb{N} \right\}.$$

También podemos ver a $\mathbb{Z}_{p^\infty}$ como un subgrupo de $S^1 = \{z \in \mathbb{C} : ||z|| = 1\}$.

$$\mathbb{Z}_{p^\infty} = \{e^{2\pi k/p^n} : k, n \in \mathbb{N}\},$$

que corresponde subgrupo de las raíces p^n-ésimas de 1 en $\mathbb{C}$.

Observamos que todos los subgrupos de $\mathbb{Z}_{p^\infty}$ están encadenados, son isomorfos a $\mathbb{Z}_{p^k}$ para $k \in \mathbb{N}$ y la unión de ellos es $\mathbb{Z}_{p^\infty}$.

$$< \frac{1}{p} + \mathbb{Z} > \subset < \frac{1}{p^2} + \mathbb{Z} > \subset < \frac{1}{p^3} + \mathbb{Z} > \subset \cdots$$

También vemos que $\mathbb{Z}_{p^\infty}$ tiene generadores $c_1, c_2, \ldots$ que satisfacen, $pc_1 = 0$ y $pc_{k+1} = c_k$ para $k \in \mathbb{N}$, donde $c_k = \frac{1}{p^k} + \mathbb{Z}$. Entonces $\mathbb{Z}_{p^\infty} = < c_1, c_2, \ldots >$

Proposición. 2.14. $\mathbb{Z}_{p^\infty}$ es un p-grupo, divisible y cocíclico.

Demostración. Es claro que es un p-grupo. Como es un p-grupo, para ver que es divisible basta ver que es p-divisible y, como cada generador lo es, tenemos que también el grupo. Es cocíclico ya que tiene un subgrupo menor $< c_1 >$. ■

Vamos a ver que los $\mathbb{Z}_{p^k}$ para $k \in \mathbb{N} \cup \{\infty\}$ son los únicos grupos cocíclicos.

Proposición. 2.15. Los grupos cocíclicos son los $\mathbb{Z}_{p^k}$ para $k \in \mathbb{N} \cup \{\infty\}$.

Demostración. Tenemos que estos grupos son cocíclicos; veamos que son todos. Sea C cocíclico. Veamos que para cada $k \in \mathbb{N}$ hay a lo más un subgrupo C_k de orden p^k que, en caso de existir, es cíclico y $C_k \subset C_{k+1}$.

Por inducción sobre el exponente de p. Para $k = 1$ tomamos el subgrupo generado por el cogenerador $< c >$ que es de orden p primo. Supongamos que tenemos un único subgrupo C_k con orden p^k para alguna $k \geq 1$ y sea c_k un generador. Entonces $C_k = < c_k >$. Ahora supongamos que existen A y B subgrupos de orden p^{k+1}. Si no existe ninguno tampoco habría subgrupos

de orden mayor. Sean $a \in A \setminus C_k$ y $b \in B \setminus C_k$. Entonces $pa, pb \in C_k$. Sean $pa = rc_k$ y $pb = sc_k$. Por lo tanto el orden a y b es p^{k+1} y $A =< a >$, $B =< b >$, entonces r y s son primos relativos con p, así existen r' y s' tales que $c_k = r'pa$ y $c_k = s'pb$. Sean $a' = r'a$ y $b' = s'b$; entonces el $o(a') = p^{k+1}$ y $o(b) = p^{k+1}$ y $< a >=< a' >$, $< b >=< b' >$. Probemos que $< a' >=< b' >$. Tenemos que $pa' = pb'$, de donde $p(a' - b') = 0$ así que $a' - b' = tc$ y como $tc \in < b' >$, tenemos que $a' \in < b' >$ y entonces $< a' > \subset < b' >$. De manera similar vemos que $< b' > \subset < a' >$. ■

Corolario. 2.16. Si A es un cociente de $\mathbb{Z}_{p^\infty}$ entonces $A \approx \mathbb{Z}_{p^\infty}$.

Demostración. Por el teorema de la correspondencia los subgrupos del cociente se corresponden con los subgrupos de $\mathbb{Z}_{p^\infty}$ que contienen al subgrupo con el que se hace cociente. Como están encadenados, entonces también los del cociente están encadenados y así vemos que tienen un subgrupo menor. Además, como es cociente de divisible A es divisible. Es claro que es p-grupo. Por lo tanto es cocíclico y, por la proposición anterior, es isomorfo a $\mathbb{Z}_{p^\infty}$. ■

.

Proposición. 2.17. Si C es cocíclico con cogenerador c y $B \leq C$, entonces C/B es cocíclico con cogenerador $c + B$

Demostración. Es claro para $\mathbb{Z}_{p^k}$ con $k \in \mathbb{N} \cup \{\infty\}$. ■

Proposición. 2.18. Si para cada natural k, A contiene un subgrupo isomorfo a $\mathbb{Z}_{p^k}$, entonces $A \approx \mathbb{Z}_{p^\infty}$.

Demostración. Para cada $k \in \mathbb{N}$ sea $A_k \approx \mathbb{Z}_{p^k}$. Entonces vemos que pA_k es isomorfo a $\mathbb{Z}_{p^{k-1}} \approx A_{k-1} \leq A$ así $A = pA$ y como ningún subgrupo propio de $\mathbb{Z}_{p^\infty}$ tiene esta propiedad tenemos que $A \approx \mathbb{Z}_{p^\infty}$. ■

2.3. Sumas directas

Un grupo A es suma directa de subgrupos B y C si todo elemento de $a \in A$ se escribe de manera única como $a = b + c$ con $b \in B$ y $c \in C$. Escribimos $A = B \oplus C$. Así tenemos una forma de construir ciertos grupos mediante otros. Además tenemos que A es el menor subgrupo que contiene a B y a C.

Observación. 2.19. Sean $B, C \leq A$. Entonces las siguientes son equivalentes:

a) A es suma directa de B y C.

b) $A = B + C$ y $B \cap C = 0$.

c) $A = B + C$ y la única forma de escribir 0 como suma $b + c$ con $b \in B$ y $c \in C$, es con $b = 0 = c$.

Proposición. 2.20. Si $A = B \oplus C$, entonces existe una sucesión exacta corta

$$0 \longrightarrow B \xrightarrow{i} A \xrightarrow{\pi} C \longrightarrow 0,$$

donde i es la inclusión y π es la proyección definida de manera que si $a = b + c$ entonces $\pi(a) = c$ y así $i(B) = Ker(\pi)$ y C es isomorfo al cociente de A/B. ■

Decimos que B es *sumando directo* de A si $B \leq A$ y existe C tal que $A = B \oplus C$. Se dice que C es el *complemento* de B. Si esto sucede escribimos $B|A$.

Proposición. 2.21. Sean $C \leq B \leq A$ grupos.

a) Si $C|B$ y $B|A$ entonces $C|A$.

b) Si $C|A$ entonces $C|B$.

Demostración. a) Es claro.

b) Como C es sumando directo de A, existe C' tal que $A = C \oplus C'$. Sea $b \in B$, $b = c + c'$ con $c \in C$ y $c' \in C'$. Vemos que $c' \in B$; por lo tanto $B = C \oplus (C' \cap B)$. ■

Decimos que una sucesión exacta

$$0 \longrightarrow B \xrightarrow{i} A \xrightarrow{\pi} C \longrightarrow 0$$

se *escinde por la derecha* si existe j tal que $\pi \circ j = id_C$. En este caso j se llama *sección* de π. La sucesión se *escinde por la izquierda* si existe ρ tal que $\rho \circ i = id_B$. En este caso decimos que ρ es retracción de i.

Proposición. 2.22. Dada la sucesión exacta

$$(*)\ \ 0 \longrightarrow B \xrightarrow{i} A \xrightarrow{\pi} A/i(B) \longrightarrow 0$$

son equivalentes:

a) $(*)$ se escinde por la izquierda.

b) $(*)$ se escinde por la derecha.

c) $i(B)$ es sumando directo de A.

Demostración. (a) $\Rightarrow$ (b) Sea ρ una retracción de i. Entonces $\rho \circ i = id_B$. Sea $h : A \to A$ definida como $h = id_A - i \circ \rho$. Como $h(i(B)) = 0$, por la propiedad universal del cociente, existe $j : B/i(B) \to A$ de manera que $j \circ \pi = h$. Vemos que $j(c) = h(a)$ para cualquier a tal que $\pi(a) = c$; entonces $\pi(j(c)) = c$ y así $j \circ \pi = id_C$.

(b) $\Rightarrow$ (a) Sea j tal que $\pi \circ j = id_C$. Sea $a \in A$. Tenemos que $\pi(a - j(\pi(a))) = \pi(a) - \pi(j(\pi(a)) = \pi(a) - \pi(a) = 0$; entonces $a - j(\pi(a)) \in Ker(\pi) = Im(i)$. Como i es un monomorfismo, existe un único $b \in B$ tal que $i(b) = a - j(\pi(a))$, entonces definimos $\rho(a) = b$. Ahora, para ver que $\rho \circ i = id_B$, como $Im(i) = Ker(\pi)$, entonces $i(b) = i(b) - j(\pi(a))$ y de ahí se sigue que $\rho \circ i = id_B$.

(a) y (b) $\Rightarrow$ c) Sea $a \in A$. Tenemos que $\pi(a - j \circ \pi(a)) = 0$ ya que $j \circ \pi = id_C$; como $Im(i) = ker(\pi)$, existe $b \in B$ tal que $i(b) = a - j \circ \pi(a)$, de donde $a = i(b) + j(\pi(a))$. Supongamos que existen $b \in B$ y $c \in C$, tales que $i(b) = j(c)$; entonces $0 = \pi \circ i(b) = \pi \circ j(c) = c$, de ahí tenemos que $j(c) = 0$ y, como j es

inyectiva, $c = 0$.

(c) $\Rightarrow$ (a) Sea $A = i(B) \oplus C'$; definimos $\rho(a)$, como el único elemento b de B tal que $a = i(b) + c'$ con $c' \in C'$. ■

Corolario. 2.23. Si la sucesión

$$0 \longrightarrow B \xrightarrow{i} A \xrightarrow{\pi} C \longrightarrow 0$$

se escinde con $j : C \to A$ y $\rho : A \to B$, entonces también la sucesión

$$0 \longrightarrow C \xrightarrow{j} A \xrightarrow{\rho} B \longrightarrow 0$$

es exacta y se escinde. ■

Proposición. 2.24. Si la sucesión exacta $0 \to B \to A \to C \to 0$ se escinde, entonces $A \approx B \times C$.

Demostración.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B & \xrightarrow{i'} & B \times C & \xrightarrow{\pi'} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle id_B} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle id_C} & & \\ 0 & \longrightarrow & B & \xrightarrow{i} & A & \xrightarrow{\pi} & C & \longrightarrow & 0 \end{array}$$

Sean i e i' las inclusiones naturales, π y π' las proyecciones naturales. Como la sucesión de abajo se escinde, existe $j : C \to A$ tal que $j \circ \pi = id_C$. Entonces definimos $\phi((b, c)) = i(b) + j(c)$; esto hace que el diagrama conmute y, por lema del 5, como las identidades son isomorfismos, tenemos que ϕ es isomorfismo. Así $A \approx B \times C$. ■

Proposición. 2.25. Si $A = B \oplus C$ entonces $A \approx B \times C$.

Demostración. Por la proposición anterior, dada una sucesión exacta que se escinde $0 \to B \to A \to C \to 0$, se tiene que $A \approx B \times C$ y, por 2.24, $A \approx B \oplus C$. ■

De esta manera, mediante una sucesión exacta tenemos una forma de decir si un grupo es sumando directo de otro.

Definición. 2.26. Decimos que A es suma directa de una familia (posiblemente infinita) de grupos $\{A_i : i \in I\}$, en símbolos $A = \bigoplus A_i$, si cada elemento de A se escribe de manera única como suma finita de elementos de los A_i. Equivalentemente, $A = \sum_i A_i$, y la única manera de escribir 0 como suma de elementos de los A_i, $\sum_i a_i = 0$, es que cada $a_i = 0$ para todo i.

Definición. 2.27. Dada una familia de grupos $\{A_i : i \in I\}$, el *producto directo* de la familia es el producto cartesiano $A = \prod_i A_i$ con las operaciones coordenada a coordenada. Cada A_i se llama *factor* de A. Para cada $i \in I$, el subgrupo de A formado por los elementos que tienen 0 en todas sus coordenadas distintas de i es un grupo A_i' isomorfo a A_i. Los A_i' forman su suma directa que consta de los elementos de A que tienen un número finito de coordenadas distintas de 0. Llamamos a esta la *suma directa externa* de los A_i. De esta manera es posible pensar a la suma directa dentro del producto directo. Es claro que si el número de grupos es finito la suma y producto directo coinciden.

Proposición. 2.28. Si B es un subgrupo invariante de A y $A = \bigoplus_{i\in I} A_i$, entonces $B = \bigoplus_{i\in I}(B \cap A_i)$.

Demostración. Sea $b \in B$; entonces $b = a_{i_1} + a_{i_2} + \cdots + a_{i_k}$, con $i_j \in I$ y $a_{i_l} \in A_{i_l}$. Sean $\pi_i : \bigoplus A_i \to A_i$ y $\alpha_i : A_i \to \bigoplus A_i$. Como B es invariante y $a_{i_j} = \alpha_i \circ \pi_i(b)$, entonces $a_i \in B$, y la suma es directa claramente. ■

Corolario. 2.29. (a) Si $B = t(A)$ y $A = \bigoplus_{i\in I} A_i$ entonces $B = \bigoplus_{i\in I}(B \cap A_i) = \bigoplus_{i\in I} t(A_i)$.

(b) Si $B = A[n]$ y $A = \bigoplus_{i\in I} A_i$ entonces $B = \bigoplus_{i\in I}(B \cap A_i) = \bigoplus_{i\in I} A_i[n]$.

(c) Si $B = S(A)$ y $A = \bigoplus_{i\in I} A_i$ entonces $B = \bigoplus_{i\in I}(B \cap A_i) = \bigoplus_{i\in I} S(A_i)$.

(d) Si $B = nA$ y $A = \bigoplus_{i\in I} A_i$ entonces $B = \bigoplus_{i\in I}(B \cap A_i) = \bigoplus_{i\in I} nA_i$.

Proposición. 2.30. Si $A = \bigoplus_{i\in I} A_i$ y para alguna $i_0 \leq I$ se tiene que $B \in A_{i_0}$, entonces $A/B = (A_{i_0}/B) \oplus \bigoplus_{i\neq i_0} A_i$.

Demostración. Es claro. ■

Proposición. 2.31. Si $A/B = \bigoplus_{i\in I} A_i/B$ y para toda $i \in I$ existe C_i tal que $A_i = B \oplus C$ entonces $A = B \oplus \bigoplus C_i$.

Demostración. Sea $a \in A$. Tenemos que

$$a + B = \sum_{k=0}^{n} a_{i_k} + B = \sum_{k=0}^{n} b_{i_k} + c_{i_k} + B = \sum_{k=0}^{n} c_{i_k} + B,$$

de donde, como $a - \sum_{k=0}^{n} c_{i_k} \in B$, existe $b \in B$ tal que $a = b + \sum_{k=0}^{n} c_{i_k}$.
Si $b + \sum_{k=0}^{n} c_{i_k} = 0$, $(b + \sum_{k=0}^{n} c_{i_k}) + B = B$, $\sum_{k=0}^{n} c_{i_k} + B = B$ y así $c_{i_k} \in B$ para toda k; por lo tanto $c_{i_k} = 0$ para toda k. ■

Proposición. 2.32. Si $\{A_i : i \in I\}$ es una familia de grupos, entonces $A = \bigoplus_{i\in I} A_i$ es libre de torsión si, y sólo si, cada A_i lo es. Lo mismo sucede para el producto directo.

Demostración. ($\Rightarrow$) Sea $a_i \in A_i \subset A$; entonces $na_i \neq 0$ para toda $n \in \mathbb{N}$, de donde los A_i son libres de torsión.
($\Leftarrow$) Si A_i es libre de torsión para toda i, sea $a \in A$. Como $a = a_{i_1} + a_{i_2} + \cdots + a_{i_k}$, $i_j \in I$, entonces $na = na_{i_1} + na_{i_2} + \cdots + na_{i_k} \neq 0$ ya que $na_{i_j} \neq 0$ para todo i_j y todo $n \in N$. ■

Teorema. 2.33. *Propiedad universal del producto directo.* Sea $\{A_i : i \in I\}$ una familia de grupos. Entonces el producto directo A de la familia, junto con las proyecciones naturales $\{\pi_i : A \to A_i\}$, son tales que dado cualquier grupo X y una familia de homomorfismos $\{f_i : X \to A_i : i \in I\}$ existe un único homomorfismo $f : X \to A$ tal que $\pi \circ f = f_i$ para toda i.

Teorema. 2.34. *Propiedad universal de la suma directa.* Sea $\{A_i : i \in I\}$ una familia de grupos. Tenemos que la suma directa A de la familia, junto con las inclusiones naturales $\{\alpha_i : A_i \to A\}$, son tales que dado cualquier grupo X y una familia de homomorfismo $\{f_i : A_i \to X : i \in I\}$ existe un único homomorfismo $f : A \to X$ tal que $f \circ \alpha_i = f_i$ para todo i.

Demostración. Sea $a \in A$; tenemos que a se escribe de manera única como $a = \sum a_i$ para $a_i \in A_i$. Entonces definimos $f(a) = \sum f_i(a_i)$. ■

Definición. 2.35. Si para cada $i \in I$ se tiene que $A_i \approx A$, entonces para $\prod_{i\in I} A_i$ escribimos A^I y para $\bigoplus_{i\in I} A_i$ escribimos $A^{(I)}$.

Proposición. 2.36. Una familia de sucesiones exactas $0 \to B_i \to A_i \to C_i \to 0$ induce una sucesión exacta corta $0 \to \bigoplus B_i \to \bigoplus A_i \to \bigoplus C_i \to 0$. En particular si $B_i \leq A_i$ para toda $i \in I$ entonces

$$(\bigoplus A_i)/(\bigoplus B_i) \approx \bigoplus (A_i/B_i)$$

Demostración. Sea $0 \to B_i \to A_i \to C_i \to 0$ una familia de sucesiones exactas, con homomorfismos $f_i : B_i \to A_i \subset \bigoplus A_i$ y $g_i : A_i \to C_i \subset \bigoplus C_i$; entonces por la propiedad universal de la suma directa existen homomorfismos $f : \bigoplus B_i \to \bigoplus A_i$ y $g : \bigoplus A_i \to \bigoplus C_i$ tales que $f \circ \alpha_i = f_i$ y $g \circ \pi_i = g_i$; donde los α_i y las π_i son las proyecciones naturales. Así tenemos una sucesión $0 \to \bigoplus B_i \to \bigoplus A_i \to \bigoplus C_i \to 0$; que es exacta, ya que en cada sumando lo es.
Por lo anterior vemos que si $B_i \leq A_i$, entonces tenemos la familia de sucesiones exactas $0 \to B_i \to A_i \to A_i/B_i \to 0$ y por lo que acabamos de probar inducen la sucesión exacta $0 \to \bigoplus B_i \to \bigoplus A_i \to \bigoplus A_i/B_i \to 0$. Como $\bigoplus B_i \leq \bigoplus A_i$ sabemos que $\bigoplus A_i/B_i \approx (\bigoplus A_i)/(\bigoplus B_i)$. ■

Proposición. 2.37. Sea $\{A_i : i \in I\}$ una familia de subgrupos de A. Entonces $\sum_{i\in I} A_i$ es cociente de $\bigoplus_{i\in I} A_i$, la suma directa externa de los A_i.

Demostración. Sea $a \in A$; entonces $a = a_{i_1} + a_{i_2} + \cdots + a_{i_k}$ con $a_{i_j} \in A_{i_j}$. Definimos $\varphi(a) = \sum_{i_j} a_{i_j}$. ■

Nota. 2.38. *a*) Un producto directo es divisible si, y sólo si, cada factor lo es.

b) Una suma directa es divisible si, y sólo si, cada sumando lo es.

2.4. Grupos de torsión

Un grupo es de torsión si sus elementos tienen orden finito. Tenemos una manera de escribir a un grupo de torsión como suma de sus partes p-primarias.

Teorema. 2.39. Sea A de torsión, entonces $A = \bigoplus_{p\in\mathcal{P}} t_p(A)$, donde $\mathcal{P}$ es el conjunto de todos lo primos.

Demostración. Sea $a \in A$, $a \neq 0$, tal que $na = 0$ para algún $n \in \mathbb{N}$. Escribimos $n = p_1^{k_1}p_2{}^{k_2}\cdots p_r^{k_r}$. Los $n/p_i^{k_i}$ son primos relativos entre sí, entonces podemos escribir $1 = (n/p_1^{k_1})s_1 + (n/p_2^{k_2})s_2 + \cdots + (n/p_r^{k_r})s_r$; de ahí tenemos que $a = (n/p_1^{k_1})s_1a+(n/p_2^{k_2})s_2a+\cdots+(n/p_r^{k_r})s_ra$ así $(n/p_i^{k_i})s_ia \in t_{p_i}(A)$. Entonces A es suma de sus partes p-primarias. Veamos que es directa. Sea $a_1+a_2+\cdots+a_m = 0$ con $a_i \in t_{p_i}(A)$; entonces para algún k_i, tenemos que $p_i^{k_i}a_i = 0$. De esta manera vemos que $p_1^{k_1}a_1 = 0$, y $p_2^{k_2}p_2^{k_2}\cdots p_m^{k_m}a_1 = 0$. Como $p_1^{k_1}$ y $p_2^{k_2}p_3^{k_3}\cdots p_m^{k_m}$ son primos relativos podemos escribir $1 = (p_1^{k_1})r + (p_2^{k_2}p_3^{k_3}\cdots p_m^{k_m})s$, de donde $a_1 = a_1(p_1^{k_1})r + a_1(p_2^{k_2}p_3^{k_3}\cdots p_m^{k_m})s = 0$. De manera análoga se tiene que $a_i = 0$ para toda i; así vemos que la suma es directa. ■

Observación. 2.40. Si $n = kl$ con k y l primos relativos, entonces $\mathbb{Z}_n \approx \mathbb{Z}_k \oplus \mathbb{Z}_l$. Como ejemplos tenemos $\mathbb{Z}_{91} \approx \mathbb{Z}_7 \oplus \mathbb{Z}_{13}$ y $\mathbb{Z}_{36} \approx \mathbb{Z}_4 \oplus \mathbb{Z}_9$. De esta manera podemos escribir a un grupo cíclico como suma directa de potencias de los primos que lo dividen.

Proposición. 2.41. Si $\{A_i : i \in I\}$ es una familia de grupos, entonces $A = \bigoplus A_i$ es de torsión si, y sólo si, cada A_i es de torsión.

Demostración. Sean $A = \bigoplus A_i$ y $a \in A$. Entonces $a = a_{i_1} + a_{i_2} + \cdots + a_{i_k}$ con $i_j \in I$. Como A es de torsión $na = 0$ para algún n; de esta manera $na = na_{i_1} + na_{i_2} + \cdots + na_{i_k} = 0$. Como la suma es directa cada $na_{i_j} = 0$. Así vemos que los A_i son de torsión.
Sea $a \in A$; entonces $a = a_{i_1} + a_{i_2} + \cdots + a_{i_k}$. Como cada A_i es de torsión existen n_j tales que $n_ja_{i_j} = 0$. Sea $n = n_1n_2\cdots n_k$, entonces $na = 0$.

■

Dando una demostración análoga a la del teorema 2.37, podemos escribir a un grupo elemental como suma directa de grupos cíclicos de orden p; ésta es una buena manera de escribirlos ya que los grupos cíclicos son sencillos. Más adelante buscaremos escribir a los grupos finitos como suma de cíclicos.

Proposición. 2.42. Si A es un grupo elemental, entonces A es suma directa de $\mathbb{Z}_p$ para ciertos primos p.

Demostración. Sean $a \in A$ y $o(a) = n$. Como n es libre de cuadrados, $n = p_1 p_2 \cdots p_k$, vemos que los n/p_i son primos relativos; así $1 = (n/p_1)s_1 + (n/p_2)s_2 + \cdots + (n/p_k)s_k$, de ahí tenemos que $a = (n/p_1)s_1 a + (n/p_2)s_2 a + \cdots + (n/p_k)s_k a$. Cada $s(n/p_i)a \in \mathbb{Z}_p$, así que los elementos de A se escriben como sumas de elementos de $\mathbb{Z}_p$. Supongamos que $a_1 + a_2 + \cdots + a_k = 0$ con $a_1 \in \mathbb{Z}_{p_1}$; si multiplicamos por $p_2 p_3 \cdots p_k$ tenemos que $(p_2 p_3 \cdots p_n)a_1 = 0$. Por otro lado podemos escribir $1 = p_1 r + (p_2 p_3 \cdots p_k)s$, de donde $a_1 = a_1 p_1 r + a_1(p_2 p_3 \cdots p_k)s = 0$. ■

Capítulo 3

Grupos divisibles

En secciones anteriores ya dimos algunas propiedades de divisibilidad en grupos. A continuación daremos más propiedades y probaremos algunos teoremas, entre ellos el teorema de estructura y clasificación de grupos divisibles.

Proposición. 3.1. Si en una sucesión exacta corta $0 \to B \xrightarrow{f} A \xrightarrow{g} C \to 0$ se tiene que B y C son n-divisibles, entonces A también es n-divisible.

Demostración. Sea $a \in A$. Tenemos que $g(a) = c$ para algún $c \in C$; como C es n-divisible existe $c' \in C$ tal que $c = nc'$, de donde $g(a) = nc'$. Como g es epimorfismo existe un $a' \in A$ tal que $g(a') = c'$; así $g(a) = ng(a')$ y $g(a) - ng(a') = 0$. Entonces como $a - na' \in Ker(g)$ existe $b \in B$ de tal forma que $f(b) = a - na'$; como b es divisible $b = nb'$. Por lo tanto $a = na' + nf(b')$. ■

Proposición. 3.2. Sea A un grupo y sea $k \in \mathbb{N}$. Sea $\mu_k : A \to A$ un homomorfismo dado por la multiplicación por k.
a) A es divisible si, y sólo si, μ_k es suprayectiva para toda k.
b) A es libre de torsión si, y sólo si, μ_k es inyectiva para toda k.

Demostración. $\Rightarrow$) a) Sea $a \in A$. Como A es divisible, para cualquier $k \in \mathbb{N}$ existe $a' \in A$ tal que $a = ka'$; entonces $\mu_k(a') = a$. Así que μ_k es suprayectiva.
$\Leftarrow$) Sean $a \in A$ y k natural; como μ_k es suprayectiva, tenemos que existe a' tal que $a = ka'$; entonces A es divisible.

b) $\Rightarrow$) Sea A libre de torsión; entonces dado $a \neq 0$ tenemos que $ka \neq 0$ para todo k y de aquí tenemos que $Ker(\mu_k) = 0$.
$\Leftarrow$) Si $Ker(\mu_k) = 0$, entonces $ka = 0$ sólo si $a = 0$, por lo que A es libre de torsión. ■

Proposición. 3.3. Si A es un grupo, entonces existe D subgrupo divisible de A que contiene a todos los subgrupos divisibles de A.

Demostración. Sean $\{D_i : i \in I\}$ los subgrupos divisibles de A. Sea $D = \sum_i D_i$. Como $\bigoplus D_i$ es divisible y D es cociente de la suma directa, entonces también es divisible. ■

Decimos que un grupo Q es *inyectivo* si dado $f : B \to A$ monomorfismo y dado $h : B \to Q$ homomorfismo existe una extensión $H : A \to Q$ tal que H cumple que $H \circ f = h$.
Las dos proposiciones siguientes nos dicen que A es divisible si, y sólo si, A es inyectivo.

Proposición. 3.4. Si A es inyectivo, entonces A es divisible.

Demostración. Dado $n \in \mathbb{N}$ tenemos un monomorfismo dado por la inclusión de $n\mathbb{Z}$ en $\mathbb{Z}$. Además como $n\mathbb{Z} \approx \mathbb{Z}$ hay un isomorfismo que manda a n en el 1 y como sabemos siempre podemos definir un homomorfismo de $\mathbb{Z}$ que manda al 1 en a; así podemos definir $h : n\mathbb{Z} \to A$, como $h(n) = a$. Ya que A es inyectivo, entonces existe una extensión $H : \mathbb{Z} \to A$ de h. Así tenemos que $nH(1) = H(n) = h(n) = a$, lo que nos dice que A es n-divisible para cualquier $n \in \mathbb{N}$. ■

Proposición. 3.5. *Criterio de Baer.* Si D es un grupo divisible entonces también es inyectivo.

Demostración. Sean A un grupo y $B \leq A$. Sea $f : B \to D$ un homomorfismo. Definimos un conjunto $\mathcal{X} = \{(B', f') : B \leq B' \text{ y } f'|_B = f\}$ donde los B' son subgrupos de A. Ordenamos a $\mathcal{X}$ de forma que $(B', f') \preceq (B'_i, f'_i)$ si $B' \leq B'_i$ y

$f_i|'_B = f'$. Sea $\mathcal{C}$ una cadena de $\mathcal{X}$. Entonces $\bigcup_\lambda B_\lambda$ es un subgrupo de A que contiene a B y definimos la función f por $f'(b) = f'_{\lambda_0}(b)$ si $b \in B_{\lambda_0}$. De esta manera tenemos una cota $(\bigcup_\lambda B_\lambda, f')$ para cada cadena $\mathcal{C}$, y por lema Zorn, $\mathcal{X}$ tiene máximo B_0. Supongamos que $B_0 \neq A$ y sea $a \in A \setminus B_0$. Tomemos $B_1 = <\{a\} \cup B_0>$. Sea $I = \{n \in \mathbb{N} : na \in B_0\}$. Entonces I es un subgrupo de $\mathbb{Z}$. Sean n_0 un generador de I y $x \in D$ tal que $n_0 x = f_0(n_0 a)$, así podemos definir $f_1 : B_1 \to D$ tal que $f_1(b_0 + ra) = f_0(b_0) + rx$ para $b_0 \in B_0$ y $r \in \mathbb{Z}$. Veamos que f_1 está bien definido. Supongamos que $b_0 + ra = b'_0 + r'a$; entonces $(r - r')a \in B_0$, así que $r - r' \in I$, de donde $r - r' = mn_0$ y por lo tanto $f(b'_0) - f(b_0) = f_0(b'_0 - b_0) = f((r - r')a) = f_0(mn_0) = mn_0 x = (r - r)x = rx - r'x$. ■

Proposición. 3.6. Si $D \leq A$ es divisible, entonces D es sumando directo.

Demostración. Tomemos a id_D el homomorfismo identidad en D. Como D es divisible, es inyectivo; entonces tenemos una extensión $A \to D$, que junto con la inclusión de D en A nos da una escisión. Así tenemos que D es sumando directo de A. ■

Decimos que A es *reducido* si no tiene subgrupos divisibles diferentes de A y de 0.

Lema. 3.7. Si A es divisible y libre de torsión, entonces A tiene estructura natural como $\mathbb{Q}$-espacio vectorial.

Demostración. Sean $a \in A$ y $n \in \mathbb{N}$; entonces existe a' tal que $a = na'$. Como A es libre de torsión, este a' es único, y así podemos definir $\frac{m}{n}a$ como ma'. Es fácil ver que esto nos da una multiplicación por escalares que convierte a A en un espacio vectorial. ■

Con el siguiente teorema vemos cómo son los grupos divisibles.

Teorema. 3.8. Todo grupo D divisible es isomorfo a sumas de $\mathbb{Q}$ y $\mathbb{Z}_{p^\infty}$ para algunos primos p.

Demostración. Como $t(D)$ es divisible entonces es sumando directo de D, así que existe A tal que $t(D) \oplus A = D$. Como A es sumando directo de D, también es divisible y además es libre de torsión, así tenemos que es un $\mathbb{Q}$-espacio vectorial.
Ahora, $t(D)$ es suma directa de sus partes p-primarias. Sabemos que $t(D)[p]$ es un $\mathbb{Z}_p$-espacio vectorial. Tomamos una base X de $t(D)[p]$. Sea $x_i \in X$ con $i \in I$; definimos $x_{i,j}$, de manera que si $j = 1$, $px_{i,1} = x_i$ y si $j \geq 2$ $px_{i,j} = x_{i,j-1}$. Entonces para cada i, tenemos un subgrupo D_i isomorfo a $\mathbb{Z}_{p^\infty}$. Veamos que $\sum_{i\in I} D_i$ es suma directa. Sea $a \in t(D)[p]$. Por inducción sobre el exponente de a. Si $e(a) = 1$, entonces $a \in t(D)[p]$ y así vemos que a está generado por los x_i. Supongamos que es cierto para un exponente k. Ahora si $e(a) = k + 1$, tenemos que $pa \in \sum_{i\in I} D_i$. De esta manera existen a_{k_i}, tales que $pa = pa_{k_1} + pa_{k_2} + \cdots + pa_{k_n}$ con $pa_{k_i} \in D_{k_i}$. Así tenemos que $p(a - a_{k_1} + a_{k_2} + \cdots + a_{k_n}) = 0$, entonces $a - a_{k_1} + a_{k_2} + \cdots + a_{k_n} \in t(D)[p]$ que está generado por los x_i. La suma es directa ya que los x_i son linealmente independientes. ■

El teorema anterior nos permite asociar cardinales invariantes a cada grupo divisible, que son la dimensión r_0 sobre $\mathbb{Q}$ de $D/t(D)$ y la dimensión r_p sobre $\mathbb{Z}_{p^\infty}$.

Algunos ejemplos de grupos divisibles son $\mathbb{R}$, $\mathbb{R}[x]$, $\mathbb{Q}$ y de no divisibles son $\mathbb{Z}$, así que no necesariamente un subgrupo de un divisible es divisible.

Proposición. 3.9. Sea $\mathcal{P}$ el conjunto de todos los primos y consideremos los siguientes grupos: $A = \prod_{p\in\mathcal{P}} \mathbb{Z}_p$ y $T = \bigoplus_{p\in\mathcal{P}} \mathbb{Z}_p$. Entonces $t(A) = T$ y $t(A)$ no es sumando directo de A.

Demostración. Ordenamos $\mathcal{P}$: $p_1 < p_2 < p_3 < \cdots$. Sea $a \in T$, $a = (a_1, a_2, \ldots)$. Si a tiene un número infinito de coordenadas distintas de cero, ningún natural lo anula, pero si eso pasa entonces existe N tal que para $n \geq N$, $a_n = 0$, así $p_1 p_2 \cdots p_N a = 0$
Veamos que A/T es divisible y que A no tiene elementos divisibles distintos de

0 para ver que A/T no es isomorfo a ningún subgrupo de A. Sea $(x_1, x_2, \ldots) \in A/T$ y sea $n \in \mathbb{Z}$, $n = p_1^{r_1} p_2^{r_2} \ldots p_K^{r_K}$. Tenemos que para $k \geq K$, p_k es primo relativo con n; entonces existe $y_k \in \mathbb{Z}_{p_k}$ tal que $x_k = ay_k$. Así vemos que $(x_1, x_2, \ldots) - n(0, 0, \ldots, 0, y_{k+1}, y_{k+2}, \ldots) = (x_1, x_2, \ldots, x_k, 0, 0, \ldots) \in T$.
No hay ningún elemento en $A \backslash \{0\}$ que sea divisible. Supongamos que lo hay. Si $x = (x_1, x_2, \ldots) \in A$ con $x_i \neq 0$. Si p_i dividiera a x, tendríamos que $x_i = p_i y_i$; pero en $\mathbb{Z}_{p_i}$ todos los múltiplos de p_i son cero.

■

Por la proposición anterior vemos que aunque dos grupos tengan partes de torsión isomorfas no quiere decir que los grupos sean isomorfos, pero es claro que si dos grupos son isomorfos sus partes de torsión son isomorfas.
En la siguiente proposición daremos otro ejemplo del cual podemos deducir que hay dos grupos no isomorfos con partes de torsión isomorfas.

Proposición. 3.10. Sea $A = \prod_k \mathbb{Z}_{p^k}$. Entonces $t(A)$ no es sumando directo de A.

Demostración. Sean $a = (\overline{1}, \overline{p}, \overline{p}^2, \overline{p}^3, \ldots)$ y $b = (\overline{0}, \overline{0}, \ldots, \overline{p}, \overline{p}^2, \ldots)$ con $m - 1$ ceros al principio. Entonces $a - \overline{p}^m b \in t(A)$ así $a + t(A)$ es un elemento divisible por cualquier $\overline{p}^m$ y de aquí vemos que a es divisible. Si $t(A)$ fuera sumando directo de A, tendríamos que $A/t(A)$ es un subgrupo de A pero, como acabamos de probar, éste tiene elementos divisibles y A no los tiene. ■

Proposición. 3.11. Sea $A = \prod_{n \in \mathbb{N}} \mathbb{Z}_n / \bigoplus_{n \in \mathbb{N}} \mathbb{Z}_n$; entonces A no es divisible.

Demostración. Sea $a \in A \setminus \{0\}$, con $a = (x_1, x_2, x_3 \ldots)$ y sea $n \in \mathbb{N}$ tal que $x_n \neq 0$; entonces si a fuera divisible por n, $x_n = ny_n$, pero $ny_n = 0$ en $\mathbb{Z}_n$. ■

Veremos en el siguiente capítulo que cualquier grupo es subgrupo de un divisible.

Capítulo 4

Grupo libres

Los grupos libres tienen propiedades semejantes a los espacios vectoriales ya que tienen una base. Además tenemos que todos los grupos son cociente de libres.

Un grupo libre es aquél que tiene una base, es decir, que cada elemento del grupo se puede escribir de manera única como combinación lineal de los elementos de la base. En el caso de $\mathbb{Z}-$módulos los grupos libres serán suma directa de copias de $\mathbb{Z}$.

Teorema. 4.1. *Propiedad universal de los grupos abelianos libres.* Sean L un grupo abeliano libre y B una base de éste. Dada $f : B \to A$ una función podemos extenderla a un homomorfismo $F : L \to A$ de manera única.

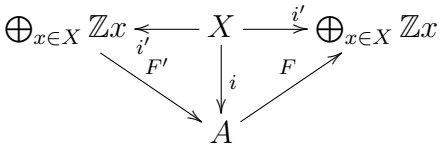
Demostración. Dado que L es libre con base B, tenemos que L es isomorfo a $\bigoplus_{x\in B} \mathbb{Z}x$. De esta manera dado $f : B \to A$, podemos definir $F : L \to A$ de la siguiente manera; sea $a \in L$ entonces existe una única forma de escribir a a como combinación lineal de elementos de B, $a = a_1b_1 + \cdots + a_nb_n$ con $a_i \in \mathbb{Z}$ y $b_i \in B$, de donde definimos $F(a) = a_1f(b_1) + \cdots + a_nf(b_n)$ esto nos da un homomorfismo y a unicidad nos la da el hecho de que hay una única combinación lineal. ■

La propiedad universal caracteriza a los grupos abelianos libres. Veamos esto

a continuación, es decir, si un grupo cumple la propiedad universal, entonces en libre.

Proposición. 4.2. Sean A un grupo y X un subconjunto de elementos tales que para cada asignación de los elementos X en un grupo C existe un único homomorfismo $F : A \to C$ que extiende a la asignación; entonces A es libre y tiene base X.

Demostración. Para el conjunto X consideremos el grupo libre $\bigoplus_{x\in X} \mathbb{Z}x$ que también cumple la propiedad universal y así tenemos el siguiente diagrama



donde $F \circ i = i'$ y $F' \circ i' = i$. Tenemos que $F \circ F' \circ i' = F \circ i = i'$, pero $id \circ i' = i'$, entonces por la unicidad de F y F', $F \circ F'$ es la identidad. De donde $A \approx \bigoplus_{x\in X} \mathbb{Z}x$. ■

Teorema. 4.3. Todo grupo abeliano A es cociente un grupo abeliano libre L.

Demostración. Sea X un conjunto de generadores para A. Definimos $L = \bigoplus_{x\in X} \mathbb{Z}x$, con $\mathbb{Z}x$ el grupo ciclico infinito generado por x; de donde X es una base para L. Ahora tomemos $i : X \to A$ la función inclusión; por la propiedad universal de los grupos abelianos libres existe F un homomorfismo de grupos que extiende a i. Como $X \subset F(L)$, F es un epimorfismo. Por el primer teorema de isomorfismo $A = Im(F) \approx L/Ker(F)$. ■

Necesitábamos saber que todo grupo abeliano es cociente de un libre para poder demostrar la siguiente proposición, enunciada en el capítulo anterior.

Proposición. 4.4. Si A es un grupo abeliano, entonces existe D un grupo divisible del cual A es subgrupo.

Demostración. Sea A un grupo abeliano; entonces es cociente de un grupo libre, así que podemos tomar un homomorfismo $f : \mathbb{Z}^{(I)} \to A$, de donde tenemos

el siguiente diagrama.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Ker(f) & \longrightarrow & \mathbb{Z}^{(I)} & \xrightarrow{f} & A & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle i} & & & & \\ 0 & \longrightarrow & Ker(f) & \longrightarrow & \mathbb{Q}^{(I)} & \longrightarrow & \mathbb{Q}^{(I)}/Ker(f) & \longrightarrow & 0 \end{array}$$

Ahora, por la propiedad universal del grupo cociente existe $\varphi : A \to \mathbb{Q}^{(I)}/ker(f)$ tal que el diagrama conmuta y, por el lema del 5, φ es un monomorfismo. Como $\mathbb{Q}^{(I)}/Ker(f)$ es cociente de un divisible, él mismo es divisible. ■

Teorema. 4.5. Dos bases de un grupo abeliano libre L tienen la misma cardinalidad. Decimos que el *rango* de L es el cardinal de la base y lo denotamos por $r(L)$.

Demostración. Sean B y C dos bases para L, con $|B| = \kappa$ y $|C| = \lambda$. Tenemos que $L \approx \mathbb{Z}^{(\kappa)} \approx \mathbb{Z}^{(\lambda)}$. Consideremos $L/2L$. Así $(\mathbb{Z}/2\mathbb{Z})^{(\kappa)} \approx \mathbb{Z}^{(\kappa)}/2\mathbb{Z}^{(\kappa)} \approx \mathbb{Z}^{(\lambda)}/2\mathbb{Z}^{(\lambda)} \approx (\mathbb{Z}/2\mathbb{Z})^{(\lambda)}$; tenemos que $|(\mathbb{Z}/2\mathbb{Z})^{(\kappa)}| = 2^\kappa$ y $|(\mathbb{Z}/2\mathbb{Z})^{(\lambda)}| = 2^\lambda$; de donde $\kappa = \lambda$. ■

Proposición. 4.6. Un subgrupo N de un grupo abeliano libre L también es libre. Además $r(N) \leq r(L)$.

Demostración. Sea β una base de L. Damos un buen orden en $\beta = \{x_\sigma : \sigma \leq \tau\}$. Definimos

$$L_\sigma = \bigoplus_{\sigma' \leq \sigma} < x_{\sigma'} > \approx \bigoplus_{\sigma' \leq \sigma} \mathbb{Z}x_\sigma,$$

para cada ordinal $\sigma \leq \tau$. También definimos $N_\sigma = N \cap L_\sigma$. Vemos que $N_\sigma = N_{\sigma+1} \cap L_\sigma$. Así tenemos, por el tercer teorema de isomorfismo $N_{\sigma+1}/N_\sigma \approx N_{\sigma+1}/(N_{\sigma+1} \cap L_\sigma) \approx (N_{\sigma+1} + L_\sigma)/L_\sigma$. Vemos que $(N_{\sigma+1} + L_\sigma)/L_\sigma \leq L_{\sigma+1}/L_\sigma \approx \mathbb{Z}$; de donde $N_{\sigma+1}/N_\sigma$ es un subgrupo de $\mathbb{Z}$ y es isomorfo a $\mathbb{Z}$ o a 0. Tenemos que la sucesión exacta $0 \to N_\sigma \to N_{\sigma+1} \to N_{\sigma+1}/N_\sigma \to 0$ se escinde; entonces N_σ es sumando directo de $N_{\sigma+1}$, de donde $N_{\sigma+1} = N_\sigma \oplus < y_0 >$ para algún $y_0 \in N_{\sigma+1}$, de manera que $< y_\sigma >$ es isomorfo a 0 o a $\mathbb{Z}$. Entonces $N = < y_\sigma : \sigma \leq \tau >$, por lo que N es la suma directa de los $< y_\sigma >$.

Vemos que usamos a lo más el mismo número de sumandos no cero para escribir a N, por lo tanto el rango de un sugrupo es menor o igual al del grupo. ■

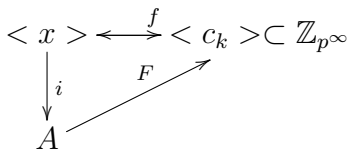
Capítulo 5

Teorema de Estructura y Clasificación de Grupos Abelianos Finitamente Generados

Los grupos abelianos que están finitamente generados están dados por sumas directas de grupos cíclicos y un grupo libre, a continuación probaremos algunos resultados que nos permitirán probar el teorema de estructura y clasificación.

Lema. 5.1. Si un grupo abeliano A es p-primario con p primo y contiene un elemento x de orden maximal, entonces $< x >$ es sumando directo de A.

Demostración. Sea p^k el orden de x. Definimos un homomorfismo $f :< x >\to \mathbb{Z}_{p^\infty}$ tal que $f(x) = c_k$, donde c_k es un generador de $\mathbb{Z}_{p^\infty}$ de orden p^k; esto define un isomorfismo entre $< x >$ y $< c_k >$. Como $\mathbb{Z}_{p^\infty}$ es inyectivo, podemos extender f con $F : A \to \mathbb{Z}_{p^\infty}$. De donde $F(A) \subset < c_k >$ ya que x es maximal.



Así tenemos una escisión de la inclusión de $< x >$ en A con el isomorfismo que hay entre $< x >$ y $< c_k >$, por lo tanto $< x >$ es sumando directo. ■

Corolario. 5.2. Todo grupo abeliano finito es suma de grupos cíclicos.

Demostración. Como es un grupo finito es suma directa de sus partes p-primarias. Además cada parte p-primaria es suma directa de cíclicos, ya que por el lema anterior, tenemos que $t_{p_i}(A)$ se puede escribir como $t_{p_i}(A) =< x > \oplus N$. N también es un p-grupo; haciendo inducción llegamos a que $t_{p_i}(A)$ es suma directa de cíclicos. ■

Observación. 5.3. Dados dos grupos libres L y N y $f : N \to L$ un homomorfismo, sean $h = \{d_1, d_2, \ldots, d_m\}$ y $l = \{e_1, e_2, \ldots, e_n\}$ bases para N y para L, respectivamente. Tenemos que $f(d_i) = \sum a_{ji} e_j$, con lo cual podemos formar una matriz M de tamaño $n \times m$ que representa al homomorfismo f. Ahora, si tenemos dos matrices invertibles P de tamaño $n \times n$ y Q de tamaño $m \times m$, entonces PMQ representa a f, pero para las bases $P(h) = \{P(d_1), P(d_2), \ldots, P(d_n)\}$ y $Q(l) = \{Q(e_1), P(e_2), \ldots, P(e_m)\}$

A continuación vemos que dada una matriz M podemos obtener una matriz diagonal $(d_{i,j})_{i,j}$ de manera que los elementos de la diagonal se vayan dividiendo, es decir $d_{ii}|d_{jj}$ para $j > i$. Esto lo podemos hacer mediante operaciones elementales y es esto es posible gracias a que realizar una operación elemental no es otra cosa que multiplicar por una matriz elemental, y así obtendremos el mismo homomorfismo representado en otra base.

Las operaciones en filas, representan multiplicar a M por una matriz elemental por la izquierda; las operaciones en columnas representan multiplicar M por la derecha por matrices elementales. Describamos las operaciones elementales y sus correspondientes matrices elementales.

a) Multiplicar por una unidad, es decir, 1 o -1 (llamémosla λ), en la fila i es multiplicar por una matriz E_λ que tiene unos en la diagonal excepto

en la fila i donde la entrada es λ y 0 en todas las demás entradas.

$$E_\lambda = \begin{bmatrix} 1 & 0 & \cdots & & & 0 \\ 0 & \ddots & & & & 0 \\ & & & & & \\ 0 & & & \lambda & & 0 \\ & & & & & \\ \vdots & & & & \ddots & \vdots \\ 0 & & \cdots & & & 1 \end{bmatrix}$$

b) Cambiar los renglones i y j es multiplicar por una matriz elemental que se consigue de cambiar los renglones i y j de la matriz identidad.

$$E_{i,j} = \begin{bmatrix} 1 & 0 & \cdots & & & & 0 \\ 0 & \ddots & & & & & \\ 0 & & 0 & & 1 & & \\ \vdots & & & \ddots & & & \vdots \\ 0 & & 1 & & 0 & & \\ & & & & & \ddots & \\ 0 & & \cdots & & & & 1 \end{bmatrix}$$

c) Sumar un reglón j multiplicado por un escalar m a un reglón i es multiplicar por la matriz que es como la identidad pero con la m en la entrada (i, j).

$$E_{i+mj} = \begin{bmatrix} 1 & 0 & \cdots & & & 0 \\ 0 & \ddots & & & & \\ 0 & & 1 & & & \\ \vdots & & & \ddots & & \vdots \\ 0 & & m & & 1 & \\ & & & & & \ddots \\ 0 & & \cdots & & & 1 \end{bmatrix}$$

Operaciones en columnas: Son las matrices de la misma forma que las de filas; multiplicando por la derecha por ellas nos dan las operaciones elementales en

columnas: multiplicar una columna por una unidad, cambiar columnas y sumar una columna multiplicada por un escalar a otra columna.

Proposición. 5.4. *Teorema de la bases simultáneas.* Sea $N \leq L$, con L libre y finitamente generado. Entonces dada una base $\{x_1, x_2, \ldots, x_n\}$, existen $d_1|d_2|\ldots|d_n$ elementos de $\mathbb{Z}$ tales que $\{d_1x_1, d_2x_2, \ldots, d_kx_k\}$ forman una base para N y $d_j = 0$ para $j > k$.

Demostración. Sabemos que N es libre así que escojamos una matriz que represente a la inclusión de N en L y tal que tenga un elemento mínimo $a \neq 0$. Sin perdida de generalidad digamos que a está en la coordenada (1,1). Vamos a ver que a es divisor de todos los elementos de la matriz. Sea b un elemento en la misma columna o renglón que a. Digamos que está en la misma columna. Supongamos que a no divide a b; entonces $b = aq + r$ con $0 < r < a$. Ahora, si restamos q veces el reglón de a, del de b tenemos que $b - qa = aq - r - qa = r$ lo que nos da un elemento más chico que a lo cual es una contradicción. De manera análoga ocurre por renglones. Ahora para cualquier otra posición (i, j), tenemos que hay un múltiplo de a en $(i, 1)$, digamos ma; así, restando $(m-1)$ el reglón 1 al i nos queda $ma - (m-1)a = a$ en $(i, 1)$ y tenemos que todos los de reglón son múltiplos de a, de igual forma para cualquier columna. Así vemos que en todas las entradas hay múltiplos de a. Para hacerla diagonal volvemos 0 a todos los elementos de la primera columna y del primer renglón que no están en la posición $(1, 1)$ y esto es posible ya que todos son múltiplos de a. Ahora en la submatriz que nos queda sin el primer renglón y sin la primera columna; observamos que podemos mover el elemento más chico a la posición $(2, 2)$ y aplicamos hipótesis de inducción observando que las operaciones elementales no alteran el primer renglón y la primera columna. ■

Los $d_1, d_2, \ldots d_n$ son los *factores invariantes* o *divisores elementales* del cociente de L/N; el rango de la parte libre de torsión es $r = n - k$.

La matriz que representa la inclusión

$$\begin{pmatrix} d_1 & & & \\ & d_2 & & \\ & & \ddots & \\ & & & d_k \end{pmatrix}$$

se denomina *forma normal de Smith* del cociente L/N.

Ejemplos. 5.5. : Sea $L = \mathbb{Z}^2$ y $N =< (4,0),(0,7) >$; tomemos la matriz que representa a la inclusión de N en L en la base $B =< (1,0),(0,1) >$ y llevémosla a su forma normal de Smith.

$$\begin{pmatrix} 4 & 0 \\ 0 & 7 \end{pmatrix}$$

Mediante operaciones elementales llegamos a

$$\begin{pmatrix} 1 & 0 \\ 0 & 28 \end{pmatrix}$$

De ahí vemos que $L/N \approx \mathbb{Z}_4 \oplus \mathbb{Z}_7$ y también $L/N \approx \mathbb{Z}_{28}$.

Sean $L = \mathbb{Z}^2$ y $N =< p, -p >$. Veamos a qué es isomorfo el cociente L/N. La matriz que representa la inclusión de N en L con la misma base del ejemplo anterior es

$$\begin{pmatrix} p & -p \\ 0 & 0 \end{pmatrix}$$

Llevándola a su forma normal de Smith nos queda

$$\begin{pmatrix} p & 0 \\ 0 & 0 \end{pmatrix},$$

así $L/N \approx \mathbb{Z}_p \oplus \mathbb{Z}$.

Como corolario del teorema de las bases simultáneas obtenemos una manera de descomponer a los grupos abelianos finitamente generados como suma directa de cíclicos.

Corolario. 5.6. Todo grupo finitamente generado es isomorfo a un grupo de la forma

$$\mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \cdots \oplus \mathbb{Z}_{d_k} \oplus \mathbb{Z}^r,$$

donde $d_1|d_2|\cdots|d_k$ y r son números naturales.

Ya tenemos una forma de representar la descomposición de un grupo A finitamente generado. Veamos que esta representación es única.

Teorema. 5.7. Si $A = \mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \cdots \oplus \mathbb{Z}_{d_n} \oplus \mathbb{Z}^r$ y $B = \mathbb{Z}_{e_1} \oplus \mathbb{Z}_{e_2} \oplus \cdots \oplus \mathbb{Z}_{e_m} \oplus \mathbb{Z}^s$ con $d_1|d_2|\cdots|d_n$, $e_1|e_2|\cdots|e_m$ y $A \approx B$, entonces $m = n$, $r = s$ y para cada i, $d_i = e_i$.

Demostración. Si $A \approx B$, entonces sus partes de torsión y sus partes libres de torsión son isomorfas. Tenemos que $t(A) = \mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \cdots \oplus \mathbb{Z}_{d_n} \approx t(B) = \mathbb{Z}_{e_1} \oplus \mathbb{Z}_{e_2} \oplus \cdots \oplus \mathbb{Z}_{e_m}$. Podemos escribir de manera única $d_i = p_1^{\alpha_{1_i}} p_2^{\alpha_{2_i}} \cdots p_l^{\alpha_{l_i}}$ y $e_i = p_1^{\beta_{1_i}} p_2^{\beta_{2_i}} \cdots p_l^{\beta_{l_i}}$ para ciertos primos, de donde $\alpha_{k_i} \leq \alpha_{k_j}$ y $\beta_{k_i} \leq \beta_{k_j}$ para $i < j$. Así, para p un primo, como $t_p(A) \approx t_p(B)$, entonces $\mathbb{Z}_{p^{\alpha_1}} \oplus \mathbb{Z}_{p^{\alpha_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_m}} \approx \mathbb{Z}_{p^{\beta_1}} \oplus \mathbb{Z}_{p^{\beta_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{\beta_m}}$. Además $t_p(A)[p] \approx t_p(B)[p]$ son espacios vectoriales con dimensión m y n ya que $\mathbb{Z}_{p^\alpha}[p] \approx \mathbb{Z}_p$, entonces $m = n$. Supongamos que la potencias no son iguales; tomemos la primera tal que $\alpha_j \neq \beta_j$; sin pérdida de generalidad, $\alpha_j < \beta_j$.

$$p^{\alpha_j}\mathbb{Z}_{p^{\alpha_1}} \oplus p^{\alpha_j}\mathbb{Z}_{p^{\alpha_2}} \oplus \cdots \oplus p^{\alpha_j}\mathbb{Z}_{p^{\alpha_n}} \approx p^{\alpha_j}\mathbb{Z}_{p^{\beta_1}} \oplus p^{\alpha_j}\mathbb{Z}_{p^{\beta_2}} \oplus \cdots \oplus p^{\alpha_j}\mathbb{Z}_{p^{\beta_m}}.$$

De esta manera uno tendría menos sumandos que otro lo cual es una contradicción. Ahora vemos que, como $A/t(A) \approx B/t(B)$, entonces $\mathbb{Z}^r \approx \mathbb{Z}^s$ y así $r = s$. ■

La proposición siguiente nos dice cómo son todos los subgrupos de un grupo finitamente generado.

Proposición. 5.8. Sean A un grupo abeliano finitamente generado y $B \leq A$. La parte libre de B es de rango menor o igual a la parte libre de A. Además si p es un primo y $p^{r_1} \geq p^{r_2} \geq \cdots \geq p^{r_k}$ son los divisores elementales de $t_p(A)$,

entonces los divisores elementales de $t_p(B)$ son $p^{s_1} \geq \cdots \geq p^{s_2} \geq p^{s_l}$ con $l \leq k$ y, agregando 1's para completar en mismo número de divisores elementales, $s_i \leq r_i$ para $i = 1, 2, \cdots, k$.

Demostración. La parte libre de A es isomorfa a $\mathbb{Z}^m$; como la parte libre de B es subgrupo de la parte libre de A, y como subgrupo de libre es libre y de rango menor, se tiene que la parte libre de B es isomorfa a $\mathbb{Z}^n$ con $n \leq m$. Como $t_p(B) \leq t_p(A)$, entonces $l \leq s$ y $s_i \leq r_i$ ya que el orden de B divide al orden de A. ■

Proposición. 5.9. Sea A un grupo abeliano de orden n. Para cualquier d divisor de n existe un subgrupo de orden d.

Demostración. Como A es finito, es de la forma $\mathbb{Z}_{k_1} \oplus \mathbb{Z}_{k_2} \oplus \cdots \oplus \mathbb{Z}_{k_n}$. Así para cada $\mathbb{Z}_{k_i}$ por 2.4 sabemos que para los divisores d_{i_j} de k_i hay un único subgrupo de orden d_{i_j} ■

Proposición. 5.10. Sea A un grupo abeliano. Si A es el cociente L/N, para L un grupo libre con B una matriz que representa la inclusión de N en L, entonces $|det(B)|$ es igual al orden de A.

Demostración. Como A es el cociente L/N es la suma directa de los grupos cíclicos de orden de los divisores elementales. Dada una matriz que representa la inclusión de N en L sabemos por el teorema de las bases simultáneas que podemos llevarla a un matriz diagonal en la que las entradas de la diagonal son los divisores elementales posiblemente cambiados de signo. Las operaciones elementales en una matriz no alteran su valor absoluto; así el $|det(B)|$ es igual al orden del grupo. ■

Ya que tenemos una caracterización de los grupos finitamente generados, en particular para los grupos de orden finito, podemos escribirlos de una forma canónica mediante sus divisores elementales y además sabemos como son todos los grupos de cierto orden.

Por ejemplo tenemos que todos los grupos de orden 720 son:

$$\mathbb{Z}_{16} \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5 \approx \mathbb{Z}_{720}$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5 \approx \mathbb{Z}_2 \oplus \mathbb{Z}_{360}$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5 \approx \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{180}$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5 \approx \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{90}$$

$$\mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5 \approx \mathbb{Z}_4 \oplus \mathbb{Z}_{180}$$

$$\mathbb{Z}_{16} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \approx \mathbb{Z}_3 \oplus \mathbb{Z}_{240}$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \approx \mathbb{Z}_3 \oplus \mathbb{Z}_{240}$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \approx \mathbb{Z}_6 \oplus \mathbb{Z}_{120}$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \approx \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_{60}$$

$$\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \approx \mathbb{Z}_{12} \oplus \mathbb{Z}_{60}$$

Capítulo 6

Grupos Racionales.

Los subgrupos de $\mathbb{Q}$ son llamados *grupos racionales*. Estos grupos son libres de torsión ya que $\mathbb{Q}$ es libre de torsión.

Proposición. 6.1. Si un subgrupo de $\mathbb{Q}$ está generado por una cantidad finita de elementos, entonces es cíclico.

Demostración. Sea $\{\frac{a_1}{b_1}, \frac{a_2}{b_2}, \ldots, \frac{a_n}{b_n}\}$ un conjunto de generadores para el subgrupo A. Entonces $A \leq < \frac{1}{b_1 b_2 \cdots b_n} >$, ya que

$$\frac{a_i}{b_i} = (a_1 b_1 b_2 \cdots b_{i-1} b_{i+1} \cdots b_n) \frac{1}{b_1 b_2 \cdots b_n}.$$

Como A es subgrupo de un grupo cíclico es cíclico. ■

Como acabamos de ver los subgrupos de $\mathbb{Q}$, finitamente generados son cíclicos, y como son libres de torsión, son isomorfos a $\mathbb{Z}$.

Corolario. 6.2. $\mathbb{Q}$ está generado por una cantidad infinita de elementos.

Proposición. 6.3. Cualesquiera dos elementos de $\mathbb{Q}$ son dependientes, es decir, para $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$ existen $r, s \in \mathbb{Z}$ tales que $r(\frac{a}{b}) = s(\frac{c}{d})$.

Demostración. Vemos que $(bc)\frac{a}{b} = ca = (ad)\frac{c}{d}$. ■

Corolario. 6.4. Cualesquiera dos subgrupos no cero tienen intersección no cero. ■

Por el corolario anterior podemos ver que los subgrupos de $\mathbb{Q}$ son inescindibles.

Proposición. 6.5. Los subgrupos propios de $\mathbb{Q}$ son inescindibles.

Demostración. Todos los subgrupos de $\mathbb{Q}$ diferentes de cero se intersectan en algo diferente de 0; entonces un subgrupo de $\mathbb{Q}$ no tiene sumandos directos no triviales. ■

Recordemos la definición de p-altura para p primo, la altura de a es $h_p(a) = n$ si $a \in p^n A \setminus p^{n+1}A$ para algún $n \in \mathbb{N}$, o ∞ si $a \in p^n A$ para todo $n \in \mathbb{N}$.

Sean A un grupo y $a \in A$, definimos la *característica* de a como la sucesión de alturas de a.

$$\chi(a) = (h_2(a), h_3(a), h_5(a), h_7(a), \dots).$$

Una sucesión $(k_1, k_2, k_3, \dots)$ de elementos de $\mathbb{N} \cup \{\infty\}$ se llama *característica*. Dos características son equivalentes si son iguales en todas sus p-alturas salvo en un número finito de ellas, y si en las que son diferentes son diferentes de ∞. Esto nos una clase de equivalencia a la que llamamos *tipo*.

Al subgrupo generado por $\{\frac{1}{p}, \frac{1}{p^2}, \frac{1}{p^3}, \dots\}$ lo denotamos $\mathbb{Q}^p$ y $\mathbb{Q}_p$ al subgrupo generado por $\{\frac{1}{p} : p \text{ primo}\}$.

Tenemos por ejemplo que en $\mathbb{Q}$ todos los elementos tienen p-altura infinita para cualquier p primo, así que la característica de cualquier elemento en $\mathbb{Q}$ es $\{\infty, \infty, \infty, \dots\}$.
En $\mathbb{Z}$ $\chi(120) = \{3, 1, 1, 0, 0, 0, \dots\}$ y en $3\mathbb{Z}$ $\chi(3) = \{0, 0, 0, 0, \dots\}$
Veamos algunos ejemplos en $\mathbb{Q}^{(3)}$, para 1 tenemos que la característica es $\{0, 0, \infty, 0, 0, 0, \dots\}$, para $\frac{1}{25}$ su característica es $\{0, 0, \infty, 0, 0, \dots\}$ y para 120 la característica es $\{3, 1, 1, 0, 0, 0, \dots\}$.
En $\mathbb{Q}_p$ $\chi(1) = \{1, 1, 1, \dots\}$ y $\chi(120) = \{4, 2, 2, 1, 1, 1, \dots\}$.
En realidad las características de dos elementos de un mismo subgrupo son equivalentes.

Proposición. 6.6. Sean a y b dos elementos no cero en un subgrupo de $\mathbb{Q}$; entonces a y b tienen características equivalentes.

Demostración. Existen $r, s \in \mathbb{Z}$ tales que $ar = bs$; entonces a sólo puede ser más divisible que b por las potencias de primos que dividan a s y b en las potencias que dividan a r. ■

Como todos los elementos de un subgrupo tienen la misma característica, podemos asociar a cada subgrupo A un tipo denotado $\tau(A)$.

Proposición. 6.7. Dado un tipo $(k_1, k_2, \ldots)$ existe A subgrupo de $\mathbb{Q}$ que tiene este tipo.

Demostración. Numeramos a los primos como $p_1 < p_2 < \ldots$. Así para los $k_i \in \mathbb{N}$ tomamos $x_i = \frac{1}{p_i^{\lceil} k_i}$, y para los $k_i = \infty$ tomamos $y_{i,j} = \frac{1}{p^n}$ para todo $n \in \mathbb{N}$. El subgrupo generado por $\{x_i\} \cup \{y_{i,j}\}$ tiene tipo $(k_1, k_2, \cdots)$. ■

Proposición. 6.8. Si A tiene tipo t y k es la característica representante de t, entonces existe $a \in A$ con característica k.

Demostración. Tomemos $a \in A$ con característica $l = (l_1, l_2, l_3, \ldots)$ y $k = (k_1, k_2, k_3, \ldots)$; sabemos que l difiere de k sólo en un número finito de p-alturas y éstas son diferentes de ∞; de esta manera si $l_i \neq k_i$ multiplicamos o dividimos por potencias de p_i a a para obtener un elemento con la característica deseada. ■

Proposición. 6.9. Si A y B son tales que $\tau(A) = \tau(B)$, entonces $A \approx B$.

Demostración. Tomamos $a \in A$ y por el teorema anterior tenemos que existe $b \in B$ con la misma característica de a, entonces definimos un homomorfismo de $< a >$ a $\mathbb{Q}$ que manda a a en b. Como $\mathbb{Q}$ es inyectivo, podemos extender el homomorfismo φ de A a $\mathbb{Q}$. Sea $a' \in A$ entonces $\varphi(a') = b$ y existen enteros r y s tales que $ra = sa'$, así $\varphi(ra) = \varphi(sa') = rb = sb'$ como a y b tienen la misma característica tenemos que $b' \in B$, por lo tanto la imagen de φ es B. ■

Corolario. 6.10. Dos grupos son isomorfos si, y sólo si, tienen el mismo tipo.

Ahora sabemos que hay una cantidad infinita de subgrupos no isomorfos de $\mathbb{Q}$ ya que hay tantos como características.

Proposición. 6.11. Los cocientes no triviales de $\mathbb{Q}$ son sumas de $\mathbb{Z}_{p^\infty}$ para ciertos p primos.

Demostración. Como $\mathbb{Q}$ es divisible, entonces también lo será el cociente. Por 3.8 y por ser de torsión sabemos que isomorfo a copias de $\mathbb{Z}_{p^\infty}$ para ciertos primos p. ■

Bibliografía

[1] Fuchs L., *Infinite Abelian Groups I,* Academicb Press, 1970.

[2] Kaplansky I., *Infinite Abelian Groups* University of Michigan Press, Ann Arbor, Michigan, 1954.

[3] Rotman J., *An Introduction to the Theory of Groups,* (tercera edición), Allyn and Bacon, 1984.

[4] Jacobson N., *Basic algebra I.* W.H. Freeman and Company, New York, 1985.

[5] Lang Serge: *Algebra* Addison-Wesley Publishing Company, 1984.