SOBRE GRUPOS DIVISIBLES E ISOMORFISMOS RELACIONADOS

ANDRÉS SEBASTIÁN CAÑAS PÉREZ

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE MATEMÁTICAS
BUCARAMANGA
2015

SOBRE GRUPOS DIVISIBLES E ISOMORFISMOS RELACIONADOS

Autor

ANDRÉS SEBASTIÁN CAÑAS PÉREZ

Trabajo de grado para optar al título de

Matemático

Director

HÉCTOR EDONIS PINEDO TAPIA

Doctor en Ciencias

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE MATEMÁTICAS
BUCARAMANGA

2015

Agradecimientos

Para mí es muy importante expresar gratitud a todas las personas que a lo largo de estos años de formación me han aportado de alguna manera para que pudiera culminar la carrera universitaria.

Primero a toda mi familia que nunca se dieron por vencidos en mi sueño de estudiar Matemáticas y han sido fuente de inspiración y perseverancia, en especial a mi mamá ya que sin ella no sería quien soy ahora.

A las Olimpiadas Colombianas de Matemáticas porque sin esta bella organización no hubiera podido encontrar el amor a las matemáticas. Y por último a todos los profesores por todo el conocimiento impartido tanto dentro y fuera del aula, en especial al profesor Héctor Pinedo, director de esta tesis, por su paciencia, su orden y dedicación.

Índice general

Resumen

TÍTULO: SOBRE GRUPOS DIVISIBLES E ISOMORFISMOS RELACIONADOS[1]

AUTOR: Andrés Sebastián Cañas Pérez[2]

PALABRAS CLAVE: Grupos abelianos; Grupos divisibles; Isomorfismos entre grupos divisibles.

RESUMEN

Dado un grupo podemos definir la multiplicación por números enteros. Así, la teoría de los grupos divisible surge para darle solución a la duda de si es posible definir una división por números enteros en los grupos, creando la estructura de grupos divisibles.

Este trabajo consiste en estudiar algunos conceptos y resultados de los grupos divisibles. En el primer capítulo se retoman algunas definiciones y resultados clásicos sobre la teoría de conjuntos, álgebra lineal, teoría de grupos y teoría de módulos, que serán importantes para el resto del trabajo.

En el segundo capítulo se estudian resultados de los grupos de torsión y los grupos p-primarios para luego introducir por primera vez la definición de grupos divisibles. Gracias a los grupos de torsión se obtiene una identidad de los grupos divisibles que nos dice que podemos escribirlos como una suma directa de grupos de torsión y libres de torsión, esta es importante para la última sección de este capítulo donde se prueba el teorema que provee las condiciones para que dos grupos divisibles sean isomorfos.

En el tercer capítulo, vamos a utilizar el teorema anteriormente mencionado para mostrar que varios grupos divisibles son isomorfos.

[1]Tesis.

[2]Facultad de Ciencias, Escuela de Matemáticas.
DIRECTOR: Dr. Héctor Edonis Pinedo Tapia.

Abstract

TITLE: ABOUT DIVISIBLE GROUPS AND RELATED ISOMORPHISMS [3]

AUTHOR: Andrés Sebastián Cañas Pérez[4]

KEYWORDS: Abelian groups; Divisible groups; Isomorphism between divisible groups.

ABSTRACT

Given a group, we can define a product by integer numbers. The theory of divisible groups was born to answer the question of whether it is possible to define a division by integer numbers on groups, creating the structure of divisible groups.

In this dissertation we are going to study some concepts and results of divisible groups. In the first chapter we will study some definitions and classical results on Set Theory, Linear Algebra, Group Theory and Module Theory, which will be important for the rest of the dissertation.

In the second chapter we will show some results of torsion groups and p-primary groups, and then we will introduce the definition of divisible groups for the first time in our work. Using torsion groups properties we obtain an identity of the divisible groups that tells us we can write them as a direct sum of torsion-free groups and torsion groups, this is important for the final section of this chapter that provides proof the theorem. This theorem gives us necessary and sufficient conditions for two divisible groups to be isomorphic.

In the third chapter, we will use the theorem we mentioned before to show that several divisible groups are isomorphic.

[3]Thesis.

[4]Faculty of Science, School of Mathematics.
DIRECTED BY: Dr. Héctor Edonis Pinedo Tapia.

Introducción

En el campo de las matemáticas existe una estructura algebraica de gran importancia a la cual llamamos *grupo*. Dados dos grupos distintos, una de las preguntas naturales es la de ver si ellos tienen la misma estructura, lo que lleva a la noción de *isomorfismo*, algunas veces encontrar un isomorfismo explícito entre dos grupos puede llegar a ser un trabajo tedioso.

En este trabajo estaremos principalmente interesados en estudiar una subclase importante de los *grupos abelianos*, los llamados *grupos divisibles*, los cuales son fáciles de reconocer dadas sus características. Una de ellas, que además es muy importante, es que son sumandos directos de cualquier grupo que los contiene. Por esto haremos un recorrido de algunas definiciones y recordaremos algunas de sus propiedades con el motivo de encontrar un mejor camino para demostrar que ciertas clases de grupos son isomorfos.

Para realizar este trabajo debemos regresar a las bases del álgebra abstracta, álgebra lineal y la teoría de conjuntos, tales como los *grupos*, *anillos*, *módulos*, *cardinalidad* entre otros. Se utilizarán nociones que aunque son básicas en el aprendizaje del alumno de pregrado, serán de gran importancia para nosotros para cumplir con nuestro objetivo.

Objetivos

Objetivo General

Usar herramientas teóricas sobre grupos divisibles para obtener isomorfismos entre los siguientes grupos.

$$\mathbb{C}^*, \quad \mathbb{Q}/\mathbb{Z} \oplus \mathbb{R}, \quad \mathbb{R}/\mathbb{Z}, \quad \prod_q \mathbb{Z}(q^\infty) \quad \text{y} \quad S^1,$$

donde q recorre todos los números primos.

Objetivos Específicos

- Profundizar definiciones y resultados de álgebra lineal y teoría de conjuntos que se han estudiado previamente en los cursos de pregrado.
- Adquirir conceptos y propiedades sobre Teoría de módulos y grupos abelianos divisibles.
- Hacer un estudio detallado en teoría elemental de grupos y la teoría de anillos para crear bases teóricas fuertes y alcanzar el objetivo general.

Capítulo 1

Preliminares

En este capítulo se establecen algunos conceptos y resultados conocidos del álgebra abstracta y la teoría de conjuntos que son fundamentales en el desarrollo y comprensión de los capítulos posteriores. Varios de estos conceptos y resultados preliminares, así como algunos ejemplos fueron extraídos de [6] y [9], por tanto para las demostraciones y demás detalles faltantes recomendamos consultar en estas referencias.

1.1. Definiciones básicas de la teoría de conjuntos

Definición 1.1. *Un* **Conjunto parcialmente ordenado** *P es un conjunto equipado con una relación binaria $\leq$ que cumple las siguientes propiedades:*

i. Reflexiva. $a \leq a$.

ii. Antisimétrica. Si $a \leq b$ y $b \leq a$, entonces $a = b$.

iii. Transitiva. Si $a \leq b$ y $b \leq c$, entonces $a \leq c$.

Para todos $a, b, c \in P$.

Definición 1.2. *Un* **Conjunto totalmente ordenado** *P es un conjunto equipado con una relación binaria $\leq$ que lo torna parcialmente ordenado y además para todos $a, b \in P$, $a \leq b$ o*

$b \leq a$.

Nota: *Decimos cadena a todo subconjunto totalmente ordenado de un conjunto parcialmente ordenado.*

Teorema 1.1. ***Lema de Zorn****. Suponga que un conjunto parcialmente ordenado P tiene la propiedad que toda cadena tiene una cota superior en P. Entonces P contiene al menos un elemento maximal.*

Definición 1.3. *Sean A y B dos conjuntos, decimos que A y B son* ***equipotentes*** *si existe $f : A \to B$ biyectiva. En este caso escribimos $A \approx B$.*

La relación $\approx$ es de equivalencia. Es decir, cumple las propiedades reflexiva, transitiva y simétrica.

Definición 1.4. *Si A y B son conjuntos equipotentes, decimos que ellos tienen la misma cardinalidad y escribimos $|A| = |B|$.*

Ejemplo 1.1. *$\mathbb{N}$ y $2\mathbb{N}$ son equipotentes. En efecto, sea $f : \mathbb{N} \to 2\mathbb{N}$ definida por $f(n) = 2n$ para todo $n \in \mathbb{N}$. Dado $m \in 2\mathbb{N}$, existe $n \in \mathbb{N}$ tal que $m = 2n = f(n)$ y si $f(n_1) = f(n_2)$, entonces $2n_1 = 2n_2$ y así $n_1 = n_2$. Por lo tanto f es una biyección, es decir $\mathbb{N}$ y $2\mathbb{N}$ son equipotentes.*

El concepto de equipotencia es útil para definir conjuntos fínitos e infinitos. Para esto, dado $n \in \mathbb{N}$, denotamos $\bar{n} = \{1, 2, \cdots, n\}$. Si $n = 0$, $\bar{0} = \emptyset$.

Definición 1.5. *Sea A un conjunto cualquiera.*

i. Decimos que A es finito si existe $n \in \mathbb{N}$ tal que $|A| = |\bar{n}| = n$. Equivalentemente, existe $f : A \to \bar{n}$ biyectiva.

ii. Decimos que A es infinito si no es finito. Esto es, para todo $n \in \mathbb{N}$, A no es equipotente con $\bar{n}$.

Proposición 1.2. $\mathbb{N}$ *es infinito.*

Sean A y B conjuntos, decimos que $|A| \leq |B|$ si existe $f : A \to B$ inyectiva, equivalentemente existe $g : B \to A$ sobreyectiva. Esta relación establece un orden parcial, gracias al siguiente.

Teorema 1.3. ***Teorema de Cantor-Bernstein****. Sean A y B conjuntos cualesquiera. Si existen $f : A \to B$ y $g : B \to A$ inyectivas, entonces existe $h : A \to B$ biyectiva. O en otras palabras, si $|A| \leq |B|$ y $|B| \leq |A|$, entonces $|A| = |B|$.*

Definición 1.6. *Un conjunto A es enumerable si existe una función inyectiva $f : A \to \mathbb{N}$, equivalentemente si existe una función sobreyectiva $f : \mathbb{N} \to A$*

Probaremos ahora que algunos conjuntos numéricos son también enumerables obteniendo resultados que serán útiles más adelante.

Ejemplo 1.2. $\mathbb{Z}$ *es un conjunto enumerable. Para esto, definimos $f : \mathbb{Z} \to \mathbb{N}$ para todo $x \in \mathbb{Z}$ por*

$$f(x) = \begin{cases} 2x - 1 & \text{if } x > 0 \\ -2x & \text{if } x \leq 0 \end{cases}$$

Primero veamos que f es sobreyectiva. Sea $n \in \mathbb{N}$, si n es par, podemos encontrar $m \in \mathbb{N}$ tal que $m = 2n$, $-m \in \mathbb{Z}$, entonces $f(-m) = n$. De forma análoga podemos ver que si $n \in \mathbb{N}$ es impar, existe $m \in \mathbb{Z}$ tal que $f(m) = n$. Ahora veamos que f es inyectiva, sean $n_1, n_2 \in \mathbb{Z}$, si $f(n_1) = f(n_2)$ debemos considerar tres casos:

i. $f(n_1) = -2n_1$ *y* $f(n_2) = -2n_2$. *De aquí concluimos que* $n_1 = n_2$

ii. $f(n_1) = 2n_1 - 1$ *y* $f(n_2) = 2n - 1$. *De aquí concluimos, nuevamente, que* $n_1 = n_2$

iii. Finalmente $f(n_1) = -2n_1$ *y* $f(n_2) = 2n_2 - 1$. *De aquí concluimos que* $n_1 = -n_2 + \frac{1}{2}$. *Luego* $n_1 \notin \mathbb{Z}$.

Así que $n_1 = n_2$. Por lo tanto $\mathbb{Z}$ es enumerable.

Teorema 1.4. $\mathbb{N} \times \mathbb{N}$ *es enumerable.*

Demostración. Sea $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, definida por $f(m,k) = 2^m(2k+1) - 1$. Veamos que f es inyectiva. Si $f(m_1,k_1) = f(m_2,k_2)$, entonces $2^{m_1}(2k_1+1) - 1 = 2^{m_2}(2k_2+1) - 1$. Es decir $2^{m_1}(2k_1+1) = 2^{m_2}(2k_2+1)$, de aquí podemos afirmar que $m_1 = m_2$ pues $2^{m_1}|2^{m_2}(2k_2+1)$, ya que 2^{m_1} y $2k_2+1$ son primos relativos se sigue que $2^{m_1}|2^{m_2}$ y así $m_1 \leq m_2$, análogamente $m_2 \leq m_1$. Ahora $2k_1+1 = 2k_2+1$, de donde $k_1 = k_2$ y concluimos que f es inyectiva. Luego $|\mathbb{N} \times \mathbb{N}| \leq |\mathbb{N}|$.

Veamos que $|\mathbb{N}| \leq |\mathbb{N}\times\mathbb{N}|$. Para esto definamos $i : \mathbb{N} \to \mathbb{N}\times\mathbb{N}$ por $i(n) = (n,n)$. i es claramente inyectiva y por lo tanto $|\mathbb{N}| \leq |\mathbb{N} \times \mathbb{N}|$. Podemos concluir por el teorema de Cantor-Bernstein que $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$ y entonces $\mathbb{N} \times \mathbb{N}$ es enumerable. □

Teorema 1.5. *Si A y B son enumerables, entonces $A \times B$ es enumerable.*

Demostración. Como A y B son enumerables existen biyecciones $f : A \to \mathbb{N}$ y $g : B \to \mathbb{N}$. Entonces $f \times g : A \times B \to \mathbb{N} \times \mathbb{N}$ dada por

$$f \times g((a,b)) = (f(a), g(b)),$$

es biyectiva. Por lo tanto $|A \times B| = |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$. Concluimos que $A \times B$ es enumerable. □

Usando los dos teoremas anteriores tenemos el siguiente.

Ejemplo 1.3. *i.* $\mathbb{Z} \times \mathbb{N}$ *es enumerable.*

ii. Si $A_1, A_2, \cdots, A_n$ son enumerables entonces $A_1 \times \cdots \times A_n$ es enumerable.

Definición 1.7. *Denotamos el cardinal de $\mathbb{N}$ por $\aleph_0$.*

Definición 1.8. *Un conjunto A no es enumerable cuando $\aleph_0 < |A|$ o equivalentemente no existe una función sobreyectiva $\mathbb{N} \to A$.*

Teorema 1.6. *Sea $f : A \to B$ sobreyectiva. Si A es enumerable, entonces B también es enumerable.*

Demostración. Como $f : A \to B$ es sobreyectiva, $|B| \leq |A|$ y como A es enumerable, existe $g : A \to \mathbb{N}$ inyectiva y por lo tanto $|A| \leq \aleph_0$. A partir de esto concluimos que $|B| \leq \aleph_0$. Entonces existe una función $h : B \to \mathbb{N}$ inyectiva y B es enumerable. □

Teorema 1.7. *La unión enumerable de conjuntos enumerables es un conjunto enumerable.*

Demostración. Sea $A = \bigcup_{i \in I} A_i$, donde I es un conjunto enumerable y A_i es un conjunto enumerable para todo $i \in I$. Como A_i es enumerable existe una función sobreyectiva $f_i : \mathbb{N} \to A_i$ y además existe una función sobreyectiva $\varphi : \mathbb{N} \to I$. Definamos la función $f : \mathbb{N} \times \mathbb{N} \to A$ por $f(m, n) = f_{\phi(n)}(m)$. Sea $x \in A$, luego existe $i \in I$ tal que $x \in A_i$ y existe $n \in \mathbb{N}$ tal que $i = \varphi(n)$. Ahora, $f_i = f_\varphi(n)$ es sobreyectiva y por lo tanto, para x existe $m \in \mathbb{N}$ tal que $f_{\varphi(n)}(m) = x$, es decir, existe $(m, n) \in \mathbb{N} \times \mathbb{N}$ tal que $f(m, n) = f_{\varphi(n)}(m) = x$, entonces f es sobreyectiva. Por el Teorema 1.1.6, A es enumerable. □

Definición 1.9. *Decimos que λ es un número cardinal si existe un conjunto A tal que $|A| = \lambda$.*

Sean λ, μ números cardinales y A y B conjuntos tales que $\lambda = |A|$ y $\mu = |B|$. Definimos el producto de cardinales como $\lambda\mu = |A \times B|$ y la potenciación de cardinales $\lambda^\mu = |A^B|$, donde $A^B = \{f : B \to A : f \text{ es función}\}$.

Para ver que el producto de cardinales está bien definido consideremos A, A', B y B' conjuntos tales que $|A| = |A'|$ y $|B| = |B'|$, entonces es fácil ver que $|A \times B| = |A' \times B'|$. En efecto, si existen funciones biyectivas $f : A \to A'$ y $g : B \to B'$, luego $f \times g : A \times B \to A' \times B'$ definida por $f \times g(a, b) = (f(a), g(b))$ es biyectiva.

De forma parecida se puede probar que $|A^B| = |A'^{B'}|$ y así ver que está bien definida la potenciación de cardinales.

Proposición 1.8. *Dados a, b, c, d números cardinales tales que $a \leq b$ y $c \leq d$, entonces $a^c \leq b^d$.*

Proposición 1.9. *Sea k un cardinal infinito, entonces $k^2 = k$.*

En particular cumple para $\aleph_0^2 = \aleph_0$. El lector interesado en la demostración de la proposición anterior puede consultar en [6, pág 155].

Definición 1.10. *Llamaremos a la cardinalidad de $\mathbb{R}$ como* ***el cardinal del continuo*** *y lo denotaremos por* $\mathfrak{c}$.

Lema 1.10. (a, b) *y* $(0, 1)$ *son equipotentes.*

Demostración. Sea $f : (a, b) \to (0, 1)$, dada por $f(x) = \frac{x-a}{b-a}$ para todo $x \in (a, b)$. Veamos que f es una biyección. Supongamos que $f(x) = f(y)$, luego

$$\tfrac{x-a}{b-a} = \tfrac{y-a}{b-a},$$

que es lo mismo a

$$x - a = y - a,$$

es decir que $x = y$. Ahora, sea $c \in (0, 1)$ y $x = c(b - a) + a$. Como $0 < c < 1$, luego $0 < c(b - a) < (b - a)$ y $a < c(b - a) + a < (b - a) + a$, entonces $a < x < b$. Por lo cual podemos concluir que f es una biyección y, (a, b) y $(0, 1)$ son equipotentes. □

Proposición 1.11. *Los intervalos de la forma*

$$(a, b), [a, b], (a, b], [a, b), [a, \infty), (-\infty, b]$$

tienen cardinalidad $\mathfrak{c}$.

Demostración. Vamos a probar para uno de los intervalos. Veamos que (a, b) es equipotente con $\mathbb{R}$. Ahora, (a, b) y $(0, 1)$ son equipotentes por el Lema 1.1.10 anterior, así que basta sólo mostrar que $(0, 1)$ y $\mathbb{R}$ son equipotentes. Sea $f : (0, 1) \to \mathbb{R}$ definida por

$$f(x) = \begin{cases} 2 - \frac{1}{x} & \text{if } 0 < x < \frac{1}{2} \\ \frac{1}{1-x} - 2 & \text{if } \frac{1}{2} < x < 1 \end{cases}$$

con función inversa

$$f^{-1}(y) = \begin{cases} \frac{1}{2-y} & \text{if } y < 0 \\ 1 - \frac{1}{2+y} & \text{if } 0 \leq y. \end{cases}$$

Luego $(0, 1)$ y $\mathbb{R}$ son equipotentes y por lo tanto (a, b) y $\mathbb{R}$ también. □

Proposición 1.12. $\mathbb{R}$ *tiene el mismo cardinal que* $P(\mathbb{N})$*. Es decir*

$$\mathfrak{c} = 2^{\aleph_0}.$$

A continuación vamos a enunciar la hipótesis del continuo ya que será una herramienta importante al final de esta tesis. Formulada por Georg Cantor en 1978 afirma que no existen conjuntos infinitos cuyo cardinal esté estrictamente entre $\aleph_0$ y el cardinal de los reales. En 1900 fue presentado como uno de los 23 problemas de Hilbert.

Teorema 1.13. ***Hipótesis del continuo***. *No existe ningún conjunto A tal que su cardinal* $|A|$ *cumpla*

$$\aleph_0 < |A| < \mathfrak{c}.$$

1.2. Definiciones básicas de la teoría de grupos

Definición 1.11. *Un grupo es un conjunto G equipado con una operación binaria* $*$*, esto es, una función* $* \colon G \times G \to G$ *tal que:*

i. *La* **ley asociativa** *se cumple: Para todos* $x, y, z \in G$*,*

$$x * (y * z) = (x * y) * z.$$

ii. *Existe un elemento* $1 \in G$*, llamado* **identidad***, que cumple* $1 * x = x * 1$ *para todo* $x \in G$*.*

iii. *Todo* $x \in G$ *tiene un* **inverso***: existe* $x' \in G$ *tal que* $x * x' = x' * x = e$ *para todo* $x \in G$*. Este* x' *será denotado por* x^{-1}*.*

Nota: Para simplificar la notación el producto $a * b$ de dos elementos a y b en un grupo será denotado por ab.

Ejemplo 1.4. *Sea* $G = \{A \in M_n(\mathbb{R}) : \det(A) \neq 0\}$*. Entonces G es un grupo con el producto usual de matrices, además el elemento identidad de G es la matriz* I_n *y el inverso de* $A \in G$ *es la matriz* $A^{-1} \in G$*, pues* $AA^{-1} = A^{-1}A = I$*.*

Consideremos dos matrices $A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right)$ *y* $B = \left(\begin{smallmatrix} 0 & 1 \\ 2 & 0 \end{smallmatrix}\right)$*, veamos que* $AB \neq BA$*:*

$$AB = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 4 & 0 \end{pmatrix}$$

$$BA = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}$$

Y por lo tanto $AB \neq BA$.

Por el ejemplo que acabamos de ver, tenemos que la operación binaria en grupos en general no es conmutativa, los grupos en los que vale la conmutatividad son llamados abelianos. Más precisamente, tenemos la siguiente definifición.

Definición 1.12. *Un grupo* G *es llamado* **abeliano** *si* $xy = yx$, *para todos* $x, y \in G$.

Ejemplo 1.5. *El conjunto* $\mathbb{C}^*$ *de los números complejos no nulos es un grupo abeliano, donde la operación binaria es la multiplicación usual. El elemento identidad es* 1 *y el inverso de* z *es* $1/z$, *para todo* $z \in \mathbb{C}^*$.

Definición 1.13. *Un subconjunto* H *de un grupo* G *es un* **subgrupo** *si:*

i. $1 \in H$.

ii. H *es cerrado bajo el producto; es decir, si* $x, y \in H$ *entonces* $xy \in H$.

iii. *Si* $x \in H$, *entonces* $x^{-1} \in H$.

Escribiremos $H \leq G$ para indicar que H es subgrupo de G.

Ejemplo 1.6. *Tomaremos el grupo aditivo* $\mathbb{C}$, *tenemos la cadena de subgrupos:*

$$\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}.$$

Definición 1.14. *Consideremos* G *un grupo:*

i. *Sea* $a \in G$ *tal que* $a^k = 1$ *para algún* $k \in \mathbb{N}, k \geq 1$, *entonces el menor* k *que cumple esta condición será llamado el* **orden** *de* a *y será denotado por* $ord(a)$*; si* k *no existe, diremos que* a *es de* **orden infinito**.

ii. Dado un grupo G, su cardinalidad, denotada por $|G|$, es llamada de **orden** *de G. Si $|G|$ no es finita, decimos que G tiene orden infinita.*

iii. Si X es un subconjunto de G, entonces existe un subgrupo $\langle X\rangle$ de G tal que es el menor subgrupo que contiene X, es decir $\langle X\rangle \subseteq H$ para todo subgrupo H de G que contiene a X. Tal subgrupo es llamado **subgrupo generado** *por X.*

Ejemplo 1.7. *Tomemos el grupo aditivo $\mathbb{Z}_6$. Tenemos que $\mathbb{Z}_6$ es un grupo finito orden 6. Sabemos también que $\bar{4} \in \mathbb{Z}_6$ y queremos calcular su orden, para esto veamos que $\bar{4}^1 = \bar{4}, \bar{4}^2 = \bar{4} + \bar{4} = \bar{2}, \bar{4}^3 = \bar{2} + \bar{4} = \bar{0}$ y por lo tanto obtenemos que $ord(\bar{4}) = 3$. Además el subgrupo generado por $\bar{4}$ será: $\langle\{\bar{4}\}\rangle = \{\bar{0}, \bar{2}, \bar{4}\}$.*

Queremos ahora recordar la definición de grupo cociente, para esto necesitamos introducir algunos conceptos.

Definición 1.15. *Consideremos G un grupo:*

i. Consideremos $H \leq G$ y $g \in G$. Entonces

$$gH = \{gh : h \in H\} \text{ es llamada } \textbf{clase lateral a izquierda} \text{ de } H \text{ en } G,$$
$$Hg = \{hg : h \in H\} \text{ es llamada } \textbf{clase lateral a derecha} \text{ de } H \text{ en } G.$$

ii. Sea $N \leq G$: N es llamado **subgrupo normal** *si $k \in N$ y $g \in G$ implica $gkg^{-1} \in N$. Si N es un subgrupo normal, escribimos*

$$N \lhd G.$$

Para subgrupos normales $N \lhd G$ vale que toda clase lateral a izquierda es clase lateral a derecha, usando este hecho podemos definir una operación binaria en el conjunto cociente $G/N = \{aN : a \in G\}$ dada por $(aN)(bN) = (ab)N$ donde $a, b \in G$.

Definición 1.16. *Sea N un subgrupo normal de un grupo G. El grupo G/N con la operación definida arriba es llamado el* **grupo cociente** *de G por N.*

Ejemplo 1.8. *Consideremos el grupo aditivo* $\mathbb{Z}_4$ *y el subgrupo* $H = \{\bar{0}, \bar{2}\}$. *Como* $\mathbb{Z}_4$ *es un grupo abeliano,* H *es normal y por lo tanto podemos definir* $\mathbb{Z}_4/H$. *Para esto miremos las clases laterales de* H *en* $\mathbb{Z}_4$*:*

- $0 + H = \{\bar{0}, \bar{2}\}$,
- $1 + H = \{\bar{1}, \bar{3}\}$,
- $2 + H = \{\bar{0}, \bar{2}\}$,
- $3 + H = \{\bar{1}, \bar{3}\}$.

Por lo tanto $\mathbb{Z}_4/H = \{\{\bar{0}, \bar{2}\}, \{\bar{1}, \bar{3}\}\} \cong \mathbb{Z}_2$.

Recordamos ahora un resultado clásico sobre grupos finitos.

Teorema 1.14. (***Teorema de Lagrange***)
Si H es un subgrupo de un grupo finito G, entonces $|H|$ es divisor de $|G|$.

Los grupos abelianos serán un papel importante en el desarrollo de este trabajo. Haremos énfasis en los ***grupos divisibles*** y sus propiedades que se de definirán a continuación.

Nota: Cuando estemos trabajando con grupos abelianos denotaremos la identidad por 0, el producto por + y el inverso de a por $-a$.

1.3. Definiciones básicas de la teoría de anillos y módulos

Definición 1.17. *Un anillo es un conjunto* R *equipado con dos operaciones binarias, adición y multiplicación, tales que:*

i. R es un grupo abeliano bajo de adición.

ii. $a\,(bc) = (ab)\,c$, *para todos* $a, b, c \in R$.

iii. Existe un elemento $1 \in R$ *tal que* $1a = a = a1$, *para todo* $a \in R$.

iv. Distributividad: $a(b+c) = ab + ac$ *y* $(b+c)a = ba + ca$, *para todos* $a, b, c \in R$.

Decimos que un anillo es **conmutativo** *cuando la multiplicación es conmutativa.*

Ejemplo 1.9. *Consideremos* $M_2(\mathbb{R})$ *con la adición y multiplicación usual de matrices. Sabemos que* $M_2(\mathbb{R})$ *es un grupo abeliano con la adición y su elemento neutro es la matriz nula. Además este cumple los axiomas de asociatividad y tiene elemento identidad* I_2 *respecto a la multiplicacón, en consecuencia* $M_2(\mathbb{R})$ *es anillo.*
Como vimos anteriormente, la multiplicación matricial en general no es conmutativa y por lo tanto $M_2(\mathbb{R})$ *es un anillo* **no conmutativo**.

Definición 1.18. *Sea a un elemento no nulo de un anillo R. Diremos que a es un* **divisor de cero por la izquierda** *si existe un elemento no nulo b tal que:*

$$ab = 0.$$

Se define de forma análoga a los **divisores de cero por la derecha**.

Definición 1.19. *Un* **ideal** *de un anillo R es un subconjunto* $\mathfrak{I}$ *de R tal que:*

i. $0 \in \mathfrak{I}$.

ii. Si $a, b \in \mathfrak{I}$ *entonces* $a + b \in \mathfrak{I}$.

iii. If $a \in \mathfrak{I}$ *y* $r \in R$ *entonces* $ra, ar \in \mathfrak{I}$.

Dado un anillo conmutativo R, tenemos que R y $\{0\}$ *siempre serán ideales de R. Un ideal* $\mathfrak{I} \subsetneq R$ *es llamado* **ideal propio**.

Definición 1.20. *Sea R un anillo conmutativo*

i. Decimos que un ideal $\mathfrak{I}$ *es* **principal** *si existe* $a \in R$ *tal que*

$$\mathfrak{I} = (a) = \{ra : r \in R\}.$$

ii. Decimos que un anillo conmutativo R no nulo es un **dominio entero** *o* ***dominio*** *si no posee divisores de* 0.

iii. Un **Dominio de ideales principales** *(DIP) es un dominio entero en el que todo ideal es principal.*

Ejemplo 1.10. *El anillo de los enteros es un DIP.*
En efecto, sea $\mathfrak{I} \subseteq \mathbb{Z}$ *un ideal; queremos probar que este es principal. Si* $\mathfrak{I} = (0)$*, entonces* $\mathfrak{I}$ *es principal. Ahora, si* $\mathfrak{I} \neq (0)$*, escojamos n el menor entero positivo en* $\mathfrak{I}$*. Vamos a probar que* $\mathfrak{I} = (n)$*. Sabemos que* $(n) \subseteq \mathfrak{I}$ *por la definición de ideal. Por otro lado si* $m \in \mathfrak{I}$ *por el algoritmo de la división existen* $q, r \in \mathbb{Z}$ *tales que* $m = qn + r$*, donde* $0 \leq r < n$*.*
Por lo tanto $r = m - qn \in \mathfrak{I}$*, y como n es el menor entero positivo en* $\mathfrak{I}$ *se sigue que* $r = 0$*. Luego* $m = qn \in (n)$*, así concluimos que* $\mathfrak{I} = (n)$*.*

Definición 1.21. *(***Cuerpo***)*

i. Un anillo es **unitario** *o* **anillo con unidad** *si existe un elemento en R,* $1 \neq 0$*, tal que* $r1 = 1r = r$ *para todo* $r \in R$*. A este elemento 1 se le denomina* **identidad**.

ii. Un **anillo de división** *es un anillo unitario en el que todo elemento distinto de cero es invertible.*

iii. Un **cuerpo** *es un anillo de división conmutativo.*

Ejemplo 1.11. *El anillo de los números racionales* $\mathbb{Q}$ *con la adición y multiplicación usual es un campo. También sabemos que* $\mathbb{Z}_n$ *es campo exactamente cuando* $n \in \mathbb{Z}^+$ *es primo.*

Definición 1.22. *Sea R un anillo con unidad. Un* R**-módulo a izquierda** *es un grupo abeliano M equipado con una multiplicación por escalar* $\cdot : R \times M \to M$ *definida por*

$$(r, m) \mapsto rm,$$

tal que cumple los siguientes axiomas para todos $m, m' \in M$ *y todos* $r, r' \in R$

i. $r(m + m') = rm + rm'$.

ii. $(r + r')m = rm + r'm$.

iii. $(rr')m = r(r'm)$.

iv. $1m = m$.

Escribiremos ${}_RM$ para indicar que M es un R-módulo a izquierda.
*Análogamente decimos que M es un R-***módulo a derecha** *si existe una multiplicación escalar $\cdot : M \times R \to M$ definida por*

$$(m, r) \mapsto mr$$

tal que cumple los siguientes axiomas para todos $m, m' \in M$ y todos $r, r', 1 \in R$

i. $(m + m')r = mr + m'r$.

ii. $m(r + r') = mr + mr'$.

iii. $m(rr') = (mr)r'$.

iv. $m1 = m$.

Al igual que el R-módulo a izquierda, este puede ser denotado por M_R. Si R es conmutativo, se sigue que todo ${}_RM$ es M_R.

Nota: Cuando digamos R-módulo nos estaremos refiriendo a un R-módulo a izquierda.

Ejemplo 1.12. *Todo anillo R es un R-módulo sobre sí mismo.*

Ejemplo 1.13. *Sea R un anillo. Entonces el grupo aditivo $M_n(R)$ es un R-módulo con la multiplicación por escalar definida por:*

$$kA = \begin{pmatrix} ka_{11} & \cdots & ka_{1n} \\ \vdots & \ddots & \vdots \\ ka_{n1} & \cdots & ka_{nn} \end{pmatrix},$$

donde $k \in R$ y $A \in M_n(R)$.

Definición 1.23. *Supongamos que M es un R-módulo. N es un subgrupo abeliano de M. Entonces N es un* ***submódulo*** *si, para cualquier $n \in N$ y cualquier $r \in R$, $rn \in N$.*

Definición 1.24. *Si R es un anillo y M y N son R-módulos. La función $f : M \to N$ es un homomorfismo de módulos si*

i. $f(m + m') = f(m) + f(m')$.

ii. $f(rm) = rf(m)$.

Para todos $m, m' \in M$ y para todo $r \in R$. Si f es un una biyección, entonces es llamado un isomorfismo de módulos. Decimos que M y N son isomorfos y lo denotamos $M \cong N$ si existe algún isomorfismo entre ellos.

Ejemplo 1.14. *$\mathbb{C}$ y $\mathbb{R}^2$ vistos como $\mathbb{R}$-módulos son isomorfos. Definamos $f : \mathbb{C} \to \mathbb{R}^2$ por $f(x + iy) = (x, y)$, esta función es claramente una biyección. Queremos ver que es un homomorfismo de módulos. Primero observemos que*

$$\begin{aligned} f((x + iy) + (t + iw)) &= f((x + t) + i(y + w)) \\ &= ((x + t), (y + w)) \\ &= (x, y) + (t, w) \\ &= f(x + iy) + f(t + iw), \end{aligned}$$

y además, dado $a \in \mathbb{R}$

$$\begin{aligned} f(a(x + iy)) &= f((ax + iay)) \\ &= (ax, ay) \\ &= a(x, y) \\ &= af(x + iy). \end{aligned}$$

Por lo tanto ellos vistos como $\mathbb{R}$-módulos son isomorfos pero si los vemos como anillos ellos no lo son.

Ejemplo 1.15. *Sean $m, n \in \mathbb{Z}$, miremos a $n\mathbb{Z}$ y $m\mathbb{Z}$ como módulos sobre $\mathbb{Z}$. Sea $f : n\mathbb{Z} \to m\mathbb{Z}$ definida por $f(na) = ma$. Veamos que f es un homomorfismo de módulos. Dados $na, nb \in n\mathbb{Z}$*

$$\begin{aligned} f(na + nb) &= f(n(a + b)) \\ &= m(a + b) \\ &= ma + mb \\ &= f(na) + f(nb), \end{aligned}$$

y además, dado $x \in \mathbb{N}$

$$\begin{aligned} f(x(na)) &= f((nx)a) \\ &= f(n(xa)) \\ &= m(xa) \\ &= x(ma) \\ &= xf(na). \end{aligned}$$

Algunas de las definiciones y teoremas ya vistos en la sección de la teoría grupos se pueden extender al contexto de módulos sobre dominios.

Definición 1.25. *Dados R un anillo y $(M)_{i\in I}$ una familia de R-módulos se define como suma directa externa al conjunto*

$$\bigoplus_{i\in I} M_i = \{(m_i)_{i\in I} \in \prod_{i\in I} M_i : m_i \neq 0 \text{ para un número fínito de } i\},$$

y las operaciones algebraicas se están dadas componente a componente.

Definición 1.26. *Sea M un R-módulo y consideremos una familia $(M)_{i\in I}$ de submódulos de*

M, se dice que el submódulo $\sum_{i\in I} M_i$*, es una suma directa interna si* $M_j \cap \sum_{i\neq j} M_i = \{0\}$ *para cada* $j \in I$ *y también se denota por* $\bigoplus_{i\in I} M_i$*.*

Definición 1.27. *Si M es un R-módulo, donde R es un dominio, entonces el submódulo de torsión es definido como*

$$tM = \{m \in M : existe r \in R, r \neq 0 \text{ tal que } rm = 0\}.$$

Teorema 1.15. *Si R es un dominio M es un R-módulo, entonces tM es un submódulo de M.*

Demostración. Si $m, m' \in tM$, entonces existen $r, r' \in R \setminus \{0\}$ tales que $rm = r'm' = 0$. Es claro que $rr'(m + m') = 0$. Como R es un dominio, $rr' \neq 0$ y por lo tanto $m + m'$ tiene orden finito. Luego $m + m' \in tM$. Por otro lado, sea $m \in tM$ y $r \in R$ tal que $rm = 0$ con $r \neq 0$. Si $s \in R$, entonces $sm \in tM$ ya que $r(sm) = rs(m) = 0$. □

Ejemplo 1.16. *El Teorema 1.3.1 puede no ser cierto si R no es dominio. Por ejemplo* $R = \mathbb{Z}_6$*. Veamos a R como un módulo sobre sí mismo, tanto* $\bar{3}$ *y* $\bar{4}$ *tienen orden finito ya que* $\bar{2}\bar{3} = 0$ *y* $\bar{3}\bar{4} = 0$*. Pero* $\bar{3} + \bar{4} = \bar{1}$ *tiene orden infinito.*

Teorema 1.16. *Sean M y M′ R-módulos y R un dominio. Entonces*

i. M/tM es libre de torsión.

ii. Si $M \cong M'$*, entonces* $tM \cong tM'$ *y* $M/tM \cong M'/tM'$*.*

Demostración. *i.* Procedamos por contradicción, esto es, existe $m \in M$ tal que $m + tM \neq tM$, y $m + tM$ tiene orden fínito. Como $m \notin tM$, m tiene orden infinito. Por otro lado existe $r \in R, r \neq 0$ tal que $r(m + tM) = rm + tM = tM$, entonces $rm \in tM$. Por lo tanto existe $s \in R, s \neq 0$ tal que $s(rm) = (sr)m = 0$. Pero sabemos que $sr \neq 0$ porque R es un dominio, luego m tiene orden finito, contradiciendo la hipótesis. De donde M/tM es libre de torsión.

ii. Sea $\phi : M \to M'$ un isomorfismo. Sea $m \in tM$, luego existe $r \in R, r \neq 0$ tal que $rm = 0$, como $r\phi(m) = \phi(rm) = 0$, es decir $\phi(m) \in tM'$, concluimos que $\phi(tM) \subset tM'$. Veamos que $\phi|_{tM} : tM \to tM'$ es un isomorfismo. Como ϕ es un isomorfismo, se deriva que $\phi|_{tM}$

es un homomorfismo inyectivo, nos falta mostrar que es sobreyectivo. Sea $m' \in tM'$, luego existe $m \in M$ tal que $\phi(m) = m'$, también existe $s \in R, s \neq 0$ tal que $sm' = 0$. Entonces $sm' = s\phi(m) = \phi(sm) = 0$, y como ϕ es un isomorfismo concluimos que $sm = 0$ y por consiguiente $sm \in tM$. Luego $\phi|_{tM}$ es un isomorfismo, es decir $tM \cong tM'$.

Ahora, sea $\bar{\phi} : M/tM \to M'/tM'$ definida por $\bar{\phi}(m + tM) = \phi(m) + tM$. Mostremos que ϕ es un isomorfismo. Primero veamos que es un homomorfismo. Sean $m_1, m_2 \in M$, luego

$$\begin{aligned}\bar{\phi}(m_1 + m_2 + tM) &= \phi(m_1 + m_2) + tM' = \phi(m_1) + \phi(m_2) + tM' \\ &= \phi(m_1) + tM' + \phi(m_2) + tM' = \bar{\phi}(m_1) + \bar{\phi}(m_2),\end{aligned}$$

por lo que acabamos de ver sabemos que $\bar{\phi}(tM) = tM'$ y además para $r \in R$ y $m \in M$ se sigue

$$\bar{\phi}(r(m + tM)) = \bar{\phi}(rm + tM) = \phi(rm) + tM' = r\phi(m) + tM' = r\bar{\phi}(m + tM).$$

Además $\bar{\phi}$ es sobreyectiva pues ϕ lo es. Ahora, sea $m \in M$ tal que $m + tM \in Ker(\bar{\phi})$, entonces $\bar{\phi}(m + tM) = \phi(m) + tM' = tM'$ y $\phi(m) \in tM'$. Por el caso anterior obtenemos que $m \in tM$ y de esta forma podemos concluir que $Ker(\bar{\phi}) = tM$ y por lo tanto $\bar{\phi}$ es inyectiva.

□

Definición 1.28. *Un R-módulo Q sobre el anillo R es inyectivo si satisface una (y por lo tanto todas) de las siguientes condiciones equivalentes*

i. Si Q es un submódulo de otro R-Módulo M, entonces existe a otro submódulo K de M tal que $M = Q \oplus K$.

ii. Si X y Y son R-módulos y $f : X \to Y$ es un homomorfismo inyectivo y $g : X \to Q$ un homomorfismo arbitrario, entonces existe un homomorfismo $h : Y \to Q$ tal que $hf = g$.

Teorema 1.17. ***Criterio de Baer****: Un R-módulo E es inyectivo si y sólo si todo homomorfismo* $f : I \to E$*, donde I es un ideal en R, puede ser extendida a* $h : R \to E$*.*

1.4. Definiciones básicas de espacios vectoriales

Se hará mención de nociones del álgebra lineal que se emplearán en algunas demostraciones.

Definición 1.29. *Si V es un F-módulo, donde F es un campo, decimos que V es un F-espacio vectorial.*

Definición 1.30. *Sea V un espacio vectorial:*

i. $S \subseteq V$ *es* **linealmente independiente** *si y sólo si todo vector* $x \in V$ *puede ser escrito a lo sumo una vez como combinación lineal de una familia de elementos de S (con excepción de suma de ceros y la reindexación de elementos de S).*

ii. Un subconjunto linealmente independiente $\mathcal{B}$ *de V que verifica que todo vector* $v \in V$ *se puede escribir de forma única de combinación lineal de elementos de* $\mathcal{B}$ *es llamado* **base**.

Teorema 1.18. *Si V es un espacio vectorial entonces*

i. V tiene una base.

ii. Todas las bases de V tienen misma la cardinalidad.

Definición 1.31. *Sea* $\mathcal{B}$ *una base de un espacio vectorial V, se dirá que su* **dimensión** *es el cardinal de* $\mathcal{B}$*. Este se denotará por* $dim(V)$*.*

Capítulo 2

Grupos divisibles y de torsión

2.1. Grupos de torsión

Definición 2.1. *Sea G un grupo abeliano. Definimos el* **subgrupo de tosión** *tG de G como*

$$tG = \{a \in G : a \text{ tiene orden finito }\}.$$

Diremos que G es un **grupo de torsión** *si G = tG y que G es* **libre de torsión** *si tG* $= \{0\}$.

Ejemplo 2.1. *Todo grupo abeliano fínito es de torsión. En efecto, sean G un grupo finito y* $a \in G$. *Por definición sabemos que* $tG \subseteq G$, *ahora queremos ver la otra contenencia. Por el Teorema de Lagrange obtenemos que* $ord(a)||G|$ *y podemos concluir que* $ord(a)$ *es finito. Por lo tanto tG = G. Es decir, todo grupo finito es de torsión.*

Ejemplo 2.2. *Consideremos el grupo aditivo* $\mathbb{Z}$. *Sea* $a \in \mathbb{Z}$ *tal que* $a \neq 0$. *Sabemos que para todo* $n \in \mathbb{N}, n \geq 1$, $na \neq 0$, *así a es de orden infinito y por lo tanto* $t\mathbb{Z} = \{0\}$, *es decir* $\mathbb{Z}$ *es libre de torsión.*

Ejemplo 2.3. *Veamos que el grupo multiplicativo* $\mathbb{C}^*$ *no es de torsión ni es libre de torsión. Sabemos que* $2^n > 0$ *para todo* $n \in \mathbb{N}$, *luego* $2 \notin t\mathbb{C}^*$, *entonces* $\mathbb{C}^*$ *no es de torsión. Para ver que no es libre de torsión, sea* $n \in \mathbb{N}, n > 1$ *y consideremos cualquier raíz n-ésima de la unidad diferente de 1, estos números estarán en* $t\mathbb{C}^*$ *y por lo tanto* $t\mathbb{C}^* \neq \{1\}$.

Veamos ahora que el isomorfismo de grupos preserva las partes de torsión y libre de torsión.

Teorema 2.1. *Sean G y H grupos. Tenemos que*

i. G/tG es libre de torsión.

ii. Si $G \cong H$, entonces $tG \cong tH$ y $G/tG \cong H/tH$.

Demostración. Este teorema es corolario del Teorema 1.3.2. □

Teorema 2.2. ***Principio del buen orden***. *Sea A un conjunto tal que $A \subseteq \mathbb{N}$ y $A \neq \emptyset$, entonces A tiene un elemento mínimo; esto es, existe $a \in A$ tal que si $b \in A$, entonces $a \leq b$.*

El principio del buen orden será usado varias veces en las demostraciones de otros teoremas. Recordaremos un resultado de teoría de números, que usaremos más tarde.

Lema 2.3. *Identidad de Bézout: Si $mcd(a_1, a_2, \cdots, a_n) = d$, entonces existen enteros $x_1, x_2, \cdots, x_n$ tales que $d = a_1x_1 + a_2x_2 + \cdots + a_nx_n$, tiene las siguientes propiedades:*

i. d es el entero positivo más pequeño de esta forma.

ii. Todo número de esta forma es múltiplo de d.

iii. d es el máximo común divisor de $a_1, a_2 \cdots, a_n$, es decir que cada máximo común divisor de $a_1, a_2 \cdots, a_n$ divide también a d.

Definición 2.2. *Sea G un grupo abeliano y p un primo.*

*i. Decimos que G es un **grupo p-primario** si todos sus elementos tienen como orden una potencia de p.*

*ii. Definimos el **componente p-primario** G_p de G como el subgrupo de todos los elementos cuyo orden es potencia de p.*

Teorema 2.4. *Todo grupo abeliano de torsión G es suma directa de sus componentes p-primarios:*

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

donde $\mathbb{P}$ es el conjunto de números primos.

Demostración. Sea $x \in G$ un elemento de orden $d \in \mathbb{N}$. Por el teorema fundamental de la aritmética, existen diferentes primos $p_1, \cdots, p_n$ y enteros positivos $\alpha_1, \cdots, \alpha_n$ tal que

$$d = {p_1}^{\alpha_1} \cdots {p_n}^{\alpha_n}.$$

Definamos $r_i = d/{p_i}^{\alpha_i}$, se sigue que $r_i x \in G_{p_i}$ para todo $i \in \{1, \cdots, n\}$. Pero como $mcd(r_1, \cdots, r_n) = 1$ existen enteros $s_1, \cdots, s_n$ con $1 = \sum_{i=1}^{n} s_i r_i$, luego

$$x = \sum_{i=1}^{n} s_i r_i x \in \sum_{p \in \mathbb{P}} G_p.$$

Ahora veamos que para $p, q \in \mathbb{P}$, $G_p \cap \sum_{q \neq p} G_q = \{0\}$. Sea $x \in G_p \cap \sum_{q \neq p} G_q$, luego x puede escribirse como $x = x_p = \sum_{q \neq p} x_q$ donde $x_p \in G_p$ y $x_q \in G_q$ para todo primo $q \neq p$. Existen $n_p \in \mathbb{N}$ tal que ${p^{n_p}} x_p = 0$ y $n_q \in \mathbb{N}$ para todo primo $q \neq p$ tal que ${q^{n_q}} x_q = 0$. Notemos que

$$(\prod_{q \neq p} q^{n_q})x = \prod_{q \neq p} q^{n_q} \sum_{q \neq p} x_q = \sum_{q \neq p} \prod_{q \neq p} q^{n_q} x_q = 0.$$

Sea $d = mcd({p^{n_p}}, \prod_{q \neq p} q^{n_q})$, se verifica que $dx = 0$. Pero como ${p^{n_p}}$ y ${q^{n_q}}$ son primos relativos para todo $q \neq p$, entonces ${p^{n_p}}$ y $\prod_{q \neq p} q^{n_q}$ también son primos relativos, es decir $d = 1$. Entonces $x = 1x = 0$ y concluimos $G_p \cap \sum_{q \neq p} G_q = 0$. Por lo tanto $G = \bigoplus_{p \in \mathbb{P}} G_p$. □

Lema 2.5. *Sean G y H grupos abelianos. Si $G \cong H$ entonces $G_p \cong H_p$ para todo p primo.*

Demostración. Supongamos que $G \cong H$, entonces existe un isomorfismo $f : G \to H$. Sea p un primo cualquiera, veamos que existe un isomorfismo $g : G_p \to H_p$. De hecho $f|_{G_p}$, es el homomorfismo que estamos buscando, para esto mostraremos que $f|_{G_p}(G_P) = H_p$. Sea $x \in G_p$, entonces x tiene orden p^n para algún $n \in \mathbb{N}$, ahora

$$f(p^n x) = p^n f(x) = p^n \ f|_{G_p}(x),$$

pero como f es un isomorfismo

$$f(p^n x) = f(0) = 0,$$

entonces $f|_{G_p}(x) \in H_p$, por lo tanto $f|_{G_p}(G_P) \subset H_p$. Ahora, sea $y \in H_p$, entonces existe $x \in G$ tal que $f(x) = y$. Además, y tiene orden p^m para algún $m \in \mathbb{N}$, entonces $p^m y = 0$ y

$$p^m y = p^m f(x) = f(p^m x),$$

luego $f(p^m x) = 0$ y como f es un isomorfismos $p^m x = 0$, entonces $x \in G_p$. Entonces $f|_{G_p}(G_P) = H_p$, y $G_p \cong H_p$. □

2.2. Grupos divisibles

En un grupo abeliano G, cualquier elemento $g \in G$ puede ser multiplicado por un número entero. Así, ¿qué sucedería si se dividiera por un entero? Para darle sentido a esta duda surge la definición de grupos divisibles.

Definición 2.3. *Sea D un grupo abeliano. Entonces, D es llamado* **divisible** *si para todo $d \in D$ y para todo entero positivo n existe $d' \in D$ tal que $d = nd'$.*

Ejemplo 2.4. *i. $\mathbb{Q}$ es un grupo divisible bajo la adición.*

En efecto, sean $d \in \mathbb{Q}$ y sea n un entero cualquiera. Si $d' = d/n$, tenemos que $d' \in \mathbb{Q}$. De aquí se sigue $d = nd'$ y $\mathbb{Q}$ es un grupo divisible.

ii. Veamos que cualquier grupo abeliano $G \neq \{e\}$ finito, no es divisible. Supongamos que G es divisible, por lo tanto para $x \in G \setminus \{e\}$ y $|G|$ existe $y \in D$ tal que $x = |G|y$. Como G es finito, $|G|y = e$, entonces $x = e$, lo cual nos genera una contradicción. De aquí se sigue que todo G divisible es infinito.

iii. Sea K un cuerpo algebraicamente cerrado. Sean $x \in K$ y $n \in \mathbb{N}$, consideremos el polinomio $a^n = x$, como K un cuerpo algebraicamente cerrado este polinomio tiene

raíces en K. Es decir, existe $y \in K$ tal que $y^n = x$ y por lo tanto el grupo multiplicativo K es divisible.

La definición de divisibilidad se puede extender para grupos no abelianos y a estos se les llama **grupos completos.** El primer grupo divisible finitamente generado fue encontrado por Gubra en [2]

Los siguientes teoremas son propiedades de los grupos divisibles que serán de suma importancia para nosotros y en el trabajo. Presentaremos a su vez las demostraciones correspondientes.

Teorema 2.6. *Sean H y G grupos abelianos.*

i. Si G es divisible y $H \leq G$, entonces G/H es divisible.

ii. Si G es divisible y $\phi : G \to H$ un homomorfismo entonces $\phi(G)$ es un subgrupo divisible de H. Es decir, la imagen de un divisible bajo un homomorfismo es divisible.

iii. La suma directa de grupos es divisible si y sólo si cada sumando es divisible.

Demostración.

i. Supongamos que G es divisible y $H \leq G$. Sean $g \in G$ y $n \in \mathbb{N}$, luego existe $g_0 \in G$ tal que $g = ng_0$ y sabemos que $g + H, g_0 + H \in G/H$. Ahora $g + H = ng_0 + H = n(g_0 + H)$. Por lo tanto G/H es divisible.

ii. Supongamos que G es divisible y $\phi : G \to H$ es un homomorfismo. Sea $h \in \phi(G)$, luego existe $g \in G$ tal que $\phi(g) = h$. Sea $n \in \mathbb{N}$, como G divisible existe $g_0 \in G$ tal que $g = ng_0$, por lo tanto $h = \phi(g) = \phi(ng_0) = n\phi(g_0)$. Se sigue que $\phi(G)$ es divisible.

iii. ($\Rightarrow$)Supongamos que $G = \bigoplus_{i \in I} G_i$ es divisible. Sea $a_i \in G_i$ y $n \in \mathbb{N}$. Tomemos $x = (x_j)_{j \in I}$ tal que $x_j = 0$ para todo $j \neq i$ y $x_i = a_i$. Como G es divisible existe $y = (y_j)_{j \in I}$ tal que $ny = x$. Se sigue que existe $y_i \in G_i$ tal que $ny_i = x_i = a_i$. Por lo tanto G_i es divisible para todo $i \in I$.

($\Leftarrow$) Sean $x = (x_i)_{i \in I} \in G$ y $n \in \mathbb{N}$. Para cada i tenemos que G_i es divisible, entonces

existe $y_i \in G_i$ tal que $ny_i = x_i$. Luego existe $y = (y_i)_{i\in I} \in G$ tal que $ny = x$ y por lo tanto G es divisible.

□

Teorema 2.7. *Todo subgrupo divisible de un grupo abeliano es un sumando directo.*

Demostración. Sea G un grupo abeliano y $H \leq G$ divisible. Debemos encontrar un subgrupo K de G tal que $H \cap K = \{0\}$ y $H + K = G$. Sea $\mathcal{F} = \{L \leq G : H \cap L = \{0\}\}$. Sabemos que $\mathcal{F}$ es no vacío ya que $\{0\} \in \mathcal{F}$. Ordenemos parcialmente a $\mathcal{F}$ por la inclusión. Para concluir la prueba queremos usar el lema de Zorn, por lo tanto tenemos que verificar que toda cadena de $\mathcal{F}$ tiene una mínima cota superior. Sea $\{L_i\}_{i\in I}$ una cadena de $\mathcal{F}$. Mostremos que la unión de los L_i es la mínima cota superior. Llamemos $L = \bigcup_{i\in I} L_i$. Veamos que L es un subgrupo de G, sean $x, y \in L$, luego existen $i, j \in I$ tales que $x \in L_i$ y $y \in L_j$. Por definición de cadena podemos suponer sin pérdida de generalidad que $L_i \subseteq L_j$, por lo tanto $x - y \in L_j$ y entonces $x - y \in L$. Concluimos que $L \leq G$. Ahora

$$H \cap L = H \cap (\bigcup_i L_i) = \bigcup_i (H \cap L_i) = \{0\}.$$

Sea $M \in F$ tal que $L_i \subset M$ para todo $i \in I$, entonces $L \subset M$. Por lo tanto, L es la mínima cota superior de tal cadena. Por el lema de Zorn $\mathcal{F}$ tiene un elemento maximal K. Procederemos por contradicción para probar que $G = H + K$, esto es si $G \neq H + K$, luego existe $x \in G$ tal que $x \notin H + K$. Podemos concluir que $x \notin K$. Sea K' el subgrupo generado por $K \cup \{x\}$, luego $K \subset K'$. Por la maximalidad de K se sigue que $H \cap K' \neq \{0\}$. Sea $h \in H \cap K'$, entonces $h = k + nx$, con $k \in K$ y algún $n \in \mathbb{Z}$. Obtenemos que $nx = h - k$, pero $h - k \in H + K$, luego $nx \in H + K$. Supongamos que n es el menor entero positivo tal que $nx \in H + K$.
Sea p primo tal que $p \mid n$ y $y = \frac{n}{p}x$, se sigue que $y \notin H + K$. Pero $py = nx = h - k$ y como H es divisible existe $h_1 \in H$ tal que $h = ph_1$. Definimos $z = y - h_1$. Luego $z \notin H + K$ ya que si estuviera, $y = z + h_1$ y $y \in H + K$ lo cual contradice que $y \notin H + K$. Ahora

$$pz = py - ph_1 = (h - k) - h = -k,$$

por lo tanto $pz \in K$. Como $z \notin H + K$ podemos repetir el argumento anterior y formar el subgrupo K'' generado por $K \cup \{z\}$, de nuevo por la maximalidad de K, $H \cap K'' \neq \{0\}$ y existe $h_2 \neq 0$ tal que $h_2 \in H \cap K''$. Podemos escribir $h_2 = k_2 + mz$, con $k_2 \in K$ y $m \in \mathbb{Z}$. Pero m no puede ser múltiplo de p porque si lo fuera tendríamos que $k_2 + mz \in K$, es decir que $h_2 \in K$ pero esto contradice que $H \cap K = \{0\}$. Por lo tanto $mcd(m, p) = 1$, luego existen $a, b \in \mathbb{Z}$ tales que $am + bp = 1$, es decir $z = amz + bpz$. Pero $amz + bpz = a(h_2 - k_2) + b(-k) \in H + K$, luego $z \in H + K$, lo cual es una contradicción. Podemos concluir que $G = H + K$. □

Teorema 2.8. *Un grupo abeliano D libre de torsión es divisible si y sólo si es un espacio vectorial sobre $\mathbb{Q}$.*

Demostración. ($\Rightarrow$) Sea D un grupo divisible y libre de torsión. Debemos mostrar que D es un espacio vectorial sobre $\mathbb{Q}$. Sean $d \in D$ y $n \in \mathbb{N}$, luego existe $d' \in D$ tal que $nd' = d$ y además, como D es libre de torsión, d' es el único elemento que cumple lo anterior.
Para esto, supongamos que para d" $\in D$ se tiene nd" $= d$. Entonces $nd' = nd$", y por lo tanto $n(d' - d") = 0$. Como D es libre de torsión, $d' - d$" tiene orden finito y por lo tanto es igual 0, es decir, $d' = d$". Definamos ahora la acción de $\mathbb{Q}$ en D. Si $m/n \in \mathbb{Q}$, definimos $(m/n)d = md'$, donde $nd' = d$. Veamos que esta multiplicación está bien definida. Sean $m, n, a, b \in \mathbb{Z}$ tales que $m/n = a/b$, es decir, $a = mb/n$ queremos ver que $(m/n)d = (a/b)d$. Sean $d', d'' \in D$ tales que $nd' = d$ y $bd'' = d$, por lo tanto $nd' = bd''$ y $(m/n)d = md'$ y $(a/b)d = ad''$.
Demostraremos que $ad'' = md'$ y de esa forma podemos concluir que la multiplicación está bien definida. Para n y $bd'' \in D$, d' es el único elemento tal que

$$nd' = bd''.$$

Además $m(nd') = n(md')$ y $m(nd') = m(bd'') = (mb)d''$. Por lo anterior podemos considerar

$$(mb/n)d'' = md'$$

y como $a = mb/n$, entonces $ad'' = md'$ y obtenemos $(m/n)d = (a/b)d$. Por último, debemos probar que D cumple las propiedades de espacio vectorial. Como D es un grupo abeliano sólo

es necesario verificar los axiomas de la multiplicación. Sean $m, n, a, b \in Z$.

i. Sean $d, d' \in D$, queremos ver que $(m/n)(d + d') = (m/n)d + (m/n)d'$. Como D es divisible y libre de torsión existe un único $x \in D$ tal que $d + d' = nx$ y por definición $(m/n)(d + d') = mx$. Por otro lado existen $y, z \in D$ tales que $d = ny$ y $d' = nz$, además $(m/n)d = my$ y $(m/n)d' = mz$. Entonces $d + d' = nx = ny + nz = n(y + z)$ obteniendo que $x = y + z$. Luego $mx = m(y + z) = my + mz = (m/n)d + (m/n)d'$. Concluimos que $(m/n)(d + d') = (m/n)d + (m/n)d'$.

ii. Queremos ver que $(m/n+a/b)d = (m/n)d+(a/b)d$ para todo $d \in D$. Sabemos que existe $d' \in D$ tal que $d = bnd'$ luego $(m/n+a/b)d = (mb+an)d' = mbd'+and'$. Por otro lado, existen $x, y \in D$ tales que $nx = d$ y $by = d$, por definición obtenemos $(m/n)d = mx$ y $(a/b)d = ay$. Pero a su vez tenemos que $nx = bnd'$, luego $x = bd'$ ya que D es libre de torsión. Análogamente obtenemos que $y = nd'$ y por lo tanto $mbd' + and' = mx + ay$. Concluimos así que $(m/n + a/b)d = (m/n)d + (a/b)d$.

iii. Queremos ver que $(m/n)[(a/b)d] = [(ma)/(nb)]d$ para todo $d \in D$. Primero veamos que existe $d' \in D$ tal que $d = bnd'$ y entonces $[(ma)/(nb)]d = mad'$. Por otro lado existe $d'' \in D$ tal que $d = bd''$, por defición obtenemos que

$$(m/n)[(a/b)d] = (m/n)ad''.$$

Ahora, existe $d''' \in D$ tal que $d'' = nd'''$, se sigue que

$$d = bd'' = bnd'''$$

y

$$ad'' = n(ad''').$$

Así llegamos a que $(m/n)ad' = mad'''$. Pero $d = bnd' = bnd'''$, luego $d' = d'''$ y podemos concluir que $(m/n)[(a/b)d] = [(ma)/(nb)]d$.

iv. La propiedad que nos dice $1d = d$ para todo $d \in D$ se sigue porque D es un grupo.

($\Leftarrow$) Si D es un espacio vectorial sobre $\mathbb{Q}$, tiene una base $(d_i)_{i\in I}$ y luego podemos escribir D de la siguiente manera:

$$D = \bigoplus_{i\in I} D_i,$$

donde D_i es el subespacio generado por d_i. Cada uno de estos es una copia de $\mathbb{Q}$ y por lo tanto divisible. Ahora, como suma directa de grupos divisibles es divisible, D es divisible. □

Definición 2.4. *Sea D un grupo abeliano. Denotamos por dD el subgrupo generado por todos los subgrupos divisibles de D.*

Definición 2.5. *Un grupo abeliano G es* **reducido** *si $dG = 0$; es decir, no tiene subgrupos divisibles no nulos.*

Ejemplo 2.5. *Si G es un grupo abeliano finito, $dG = 0$. Por el Ejemplo 2.7 sabemos que todo grupo abeliano finito no es divisible, por lo tanto todo $H \leq G$, al ser finito, tampoco es divisible, concluyendo que $dG = 0$.*

Definición 2.6. *Si G es un grupo abeliano y n es un entero positivo, entonces*

$$G[n] = \{g \in G : ng = 0\}.$$

Ejemplo 2.6. *Consideremos $\mathbb{Z}_4$. Luego $\mathbb{Z}_4[3] = \{g \in G : 3g = 0\} = \{0\}$. En general, si m y n son primos relativos, entonces $\mathbb{Z}_m[n] = \{0\}$.*

Teorema 2.9. *Sea G un grupo, $H \leq G$ y D un grupo divisible. Sea $f : H \to D$ un homomorfismo. Entonces f puede ser extendido a un homomorfismo G en D.*

Demostración. Consideremos el conjunto

$$\mathcal{S} = \{(S, h) : S \leq G \text{ tal que } H \subseteq S \text{ y } h : S \to D \text{ es una extensión de } f\}.$$

$\mathcal{S} \neq \emptyset$ ya que $(H, f) \in \mathcal{S}$. Definimos el orden $\leq$ en $\mathcal{S}$: $(S_i, h_i) \leq (S_j, h_j) \Leftrightarrow S_i \subseteq S_j$ y h_j es una extensión de h_i. Veamos que este es un orden parcial en $\mathcal{S}$. Es clara la propiedad reflexiva. Probaremos la propiedad antisimétrica, sean $(S_i, h_i), (S_j, h_j) \in \mathcal{S}$ tales que $(S_i, h_i) \leq (S_j, h_j)$ y

$(S_j, h_j) \leq (S_i, h_i)$, por definición tenemos $S_i \subseteq S_j$ y $S_j \subseteq S_i$ y por lo tanto $S_i = S_j$, luego $h_i = h_j\big|_{S_i} = h_j\big|_{S_j} = h_j$. Ahora, probemos la propiedad transitiva, sean $(S_i, h_i), (S_j, h_j), (S_k, h_k) \in \mathcal{S}$ tales que $(S_i, h_i) \leq (S_j, h_j)$ y $(S_j, h_j) \leq (S_k, h_k)$, como $S_i \subseteq S_j$ y $S_j \subseteq S_k$ entonces $S_i \subseteq S_k$, también tenemos que $h_k|_{S_j} = h_j$ y $h_j\big|_{S_i} = h_i$, luego $h_k|_{S_j}\big|_{S_i} = h_j\big|_{S_i} = h_i$, pero como $S_i \subseteq S_j$ se sigue que $h_k|_{S_j}\big|_{S_i} = h_k|_{S_i}$, por lo tanto $h_k|_{S_i} = h_i$ y $(S_i, h_i) \leq (S_k, h_k)$, por consiguiente $\leq$ es una relación de orden parcial.

Sea $\{(S_\alpha, h_\alpha)\}_\alpha$ una cadena en $\mathcal{S}$ y definamos $S_0 = \bigcup_\alpha S_\alpha$ y si $s \in S_0$ entonces existe α tal que $s \in S_\alpha$, podemos definir $h_0(s) = h_\alpha(s)$. Esta función está bien definida ya que si $s \in S_{\alpha_1}$ y $s \in S_{\alpha_2}$, podemos suponer sin pérdida de generalidad que $S_{\alpha_1} \subseteq S_{\alpha_2}$, luego $h_{\alpha_1}(s) = h_{\alpha_2}(s)$ ya que h_{α_2} es extensión de h_{α_1}.

El elemento $(S_0, h_0) \in S$ ya que por un lado $S_0 \leq G$ y $H \subseteq S_0$ y además si $x \in H$ entonces $h_0(x) = h_\alpha(x)$ para todo α y por lo tanto es una extensión de f. Por su definición sabemos que este elemento es una cota superior pero ahora queremos verificar que es la mínima cota superior: Si $(S_\alpha, h_\alpha) \leq (S', h')$ para todo α, entonces $S_\alpha \subseteq S'$ y como $h'|_{S_\alpha} = h_\alpha$ para todo α, entonces $h'|_{S_0} = h_0$. Por lo tanto $(S_0, h_0) \leq (S', h')$. Luego por el lema de Zorn, existe un elemento maximal $(M, g) \in \mathcal{S}$.

Queremos mostrar que $M = G$. Supongamos lo contrario, entonces existe $x \in G$ tal que $x \notin M$. Sea $M_1 = M + \langle x \rangle$. Queremos extender g para M_1, contradiciendo la maximalidad de M. Consideremos dos casos:

i. Supongamos que $M \cap \langle x \rangle \neq 0$. Por el principio del buen orden, existe el entero positivo k tal que es el más pequeño que cumple $kx \in M$. Entonces, si $y \in M_1$ podemos escribirlo como $y = m + sx$ con $m \in M$ y $0 \leq s < k$. Esta expresión es única ya que si $m + sx = m' + s'x$ con $0 \leq s < s' < k$, entonces $(s' - s)x = m - m' \in M$, pero $0 \leq s' - s < k$, lo cual contradice la elección de k. Ahora, sea $z = kx$, como $z \in M$ entonces $g(z)$ está definido, además como $g(z) \in D$ y D es divisible, existe $\xi \in D$ tal que $k\xi = g(z)$. Ahora, definimos $F : M_1 \to D$ por $F(m + sx) = g(m) + s\xi$ que claramente extiende a g, nos resta ver que es un homomorfismo. Sean $m_1 + s_1 x, m_2 + s_2 x \in M_1$ y supongamos que

$s_1 + s_2 < k$

$$\begin{aligned} F((m_1 + s_1x) + (m_2 + s_2x)) &= F((m_1 + m_2) + (s_1x + s_2x)) \\ &= g(m_1 + m_2) + (s_1 + s_2)\xi \\ &= g(m_1) + g(m_2) + s_1\xi + s_2\xi \\ &= (g(m_1) + s_1\xi) + (g(m_2) + s_2\xi) \\ &= F(m_1 + s_1\xi) + F(m_2 + s_2\xi). \end{aligned}$$

Ahora supongamos que $s_1 + s_2 > k$, luego $s_1 + s_2 = k + s$ con $0 \leq s < k$, entonces

$$\begin{aligned} F((m_1 + s_1x) + (m_2 + s_2x)) &= F((m_1 + m_2) + (s_1x + s_2x)) \\ &= F(m_1 + m_2 + kx + sx)) \\ &= g(m_1 + m_2 + kx) + s\xi \\ &= g(m_1) + g(m_2) + g(kx) + s\xi \\ &= g(m_1) + g(m_2) + g(z) + s\xi \\ &= g(m_1) + g(m_2) + k\xi + s\xi \\ &= g(m_1) + g(m_2) + s_1\xi + s_2\xi \\ &= (g(m_1) + s_1\xi) + (g(m_2) + s_2\xi) \\ &= F(m_1 + s_1\xi) + F(m_2 + s_2\xi). \end{aligned}$$

Luego, F es un homomorfismo tal que $F|_M = g$, lo cual nos genera una contradicción.

ii. Si $M \cap \langle x \rangle = 0$ entonces $M_1 = M \oplus \langle x \rangle$. En este caso definimos $F : M_1 \to D$ por $F(m + ax) = g(m)$. F está bien definida porque la expresión para $m + ax$ es única. F es un homomorfismo porque g lo es y además $F|_M = g$. De nuevo, nos genera contradicción.

En ambos casos obtenemos que $(M, g) \leq (M_1, F)$, que contradice la maximalidad de M, entonces $M = G$. □

Teorema 2.10. *Sean G y H grupos abelianos divisibles p-primarios, entonces $G \cong H$ si y sólo si $G[p] \cong H[p]$.*

Demostración. ($\Rightarrow$) Si existe un isomorfismo $f : G \to H$, veamos que $f|_{G[p]}$ es un isomorfismo de $G[p]$ en $H[p]$. Ya sabemos que $f|_{G[p]}$ es un homomorfismo inyectivo pues f lo es. Queremos ver que $f|_{G[p]}(G[p]) = H[p]$. Sea $x \in G[p]$. Mostremos que $f|_{G[p]}(x) \in H[p]$. Ahora, como f es un homomorfismo vemos que

$$p\, f|_{G[p]}(x) = f|_{G[p]}(px) = f|_{G[p]}(0) = 0$$

y se sigue que $f|_{G[p]}(G[p]) \subseteq H[p]$. Sea $h \in H[p]$, luego existe $g \in G$ tal que $f(g) = h$ y $f(pg) = pf(g) = ph = 0$. Pero como f es un isomorfismo $Ker(f) = \{0\}$, por lo tanto $pg = 0$, es decir, $g \in G[p]$. Concluimos que $f|_{G[p]} : (G[p]) \to H[p]$ es un isomorfismo.
($\Leftarrow$) Sea $f : G[p] \to H[p]$ un isomorfismo. Sea $i_H : H[p] \to H$ el homomorfismo inclusión y $\bar{f} = i_H \circ f : G[p] \to H$, por el teorema anterior podemos extender $\bar{f}$ a un homomorfismo $F : G \to H$. Vamos a probar que F es un isomorfismo.

Primero, veamos que es inyectivo. Como G es un grupo p-primario todo $g \in G$ tiene orden p^n para algún $n \in \mathbb{N}$. Sea $g \in G$ con orden p, como f es un isomorfismo, $g \notin Ker(f)$ y $F(g) = f(g) \neq 0$.
Ahora, sea $g \in G$ con orden p^n con $2 \leq p$, como p es primo, el elemento $p^{n-1}g$ tiene orden p. Supongamos que $F(g) = 0$ y dado que F es un homomorfismo, $p^{n-1}F(g) = F(p^{n-1}g) = 0$ lo cual contradice el caso anterior. Entonces F es inyectiva. Ahora veamos a probar que F es sobreyectiva. Si $h \in H$ este elemento tiene orden p^n, así vamos a proceder por inducción sobre n. Si $n = 1$, entonces $h \in H[p] = imf \subseteq imF$. Supongamos que para algún $n > 1$ todo elemento en H con orden p^n está en imF. Sea ahora $h \in H$ de orden p^{n+1}, luego $p^n h \in H[p]$, y existe $g \in G$ tal que $F(p) = f(g) = p^n h$. Como G es divisible, entonces existe $g' \in G$ tal que $p^n g' = g$, luego $p^n(h - F(g')) = 0$ y por inducción existe $x \in G$ tal que $F(x) = h - F(g')$, luego $F(x + g') = h$, por lo tanto F es sobreyectiva. □

Cuando hablamos de grupos abelianos divisibles una de las propiedades que no podemos obviar es que ellos son un $\mathbb{Z}$-módulo inyectivo. Es decir, los grupos abelianos divisibles describen todos los grupos abelianos inyectivos. Para esto vamos a extender la definición de divisibilidad a la teoría de anillos

Definición 2.7. *Sea R un dominio. Entonces un R-módulo D es **divisible** si, para todo $d \in D$ y $r \in R$ diferente de cero, existe $d' \in D$ tal que $d = rd'$.*

Teorema 2.11. *Si R es un dominio, entonces todo R-módulo inyectivo es divisible.*

Demostración. Supongamos que E es un R-módulo inyectivo. Sean $e \in E$ y $r_0 \in R$ diferente de cero; debemos encontrar $x \in R$ con $e = r_0 x$. Definamos $f : (r_0) \to E$ por $f(rr_0) = re$. Notemos que f está bien definida ya que R es un dominio, si $rr_0 = r'r_0$ implica que $r = r'$. Como E es inyectivo, existe $g : R \to E$ que extiende a f. En particular

$$e = f(r_0) = h(r_0) = r_0 h(1),$$

luego $x = h(1)$ es el elemento en E que necesitábamos. Concluimos que E es divisible. □

Teorema 2.12. *Si R es un DIP, entonces todo R-módulo E es inyectivo si y sólo si es divisible.*

Demostración.
($\Rightarrow$) Se obtiene del teorema anterior.
($\Leftarrow$) Supongamos que E es divisible. Por el criterio de Baer, es suficiente extender una función cualquiera $f : I \to E$ a una función de $h : R \to E$. Como R es un DIP, I es ideal principal, es decir, $I = (r_0)$ para algún $r_0 \in I$. Como E es divisible y $f(r_0) \in E$, existe $e \in E$ tal que $r_0 e = f(r_0)$. Definamos $h : R \to E$ por $h(r) = re$. Sea $x \in I$, luego existe $r \in R$ tal que $x = rr_0$, entonces $f(x) = rf(r_0) = rr_0 e = xe = h(x)$ y por lo tanto h es una extensión de f.

□

En particular como $\mathbb{Z}$ es un DIP, todo $\mathbb{Z}$-módulo inyectivo si y sólo si es divisible.

2.3. Grupo de Prüfer

Vamos a definir un grupo importante para nuestro trabajo. Llamamos grupo de Prüfer en honor al matemático alemán Heinz Prüfer reconocido por sus contribuciones a la teoría de grupos abelianos y números algebraicos, entre otros. La relevancia del grupo de Prüfer en este trabajo es porque ayuda a clasificar los grupos abelianos divisibles.

Definición 2.8. *Sea $p \in \mathbb{Z}$ primo. El* **grupo de Prüfer** *de tipo p^∞ es el subgrupo del grupo multiplicativo $\mathbb{C}^*$ dado por:*

$$\mathbb{Z}(p^\infty) = \langle e^{2\pi i/p^n} : n \geq 1 \rangle = \{e^{2\pi im/p^n} : m \in \mathbb{Z}, n \in \mathbb{N}\}$$

Teorema 2.13. *Sea p un primo cualquiera. El grupo de Prüfer $\mathbb{Z}(p^\infty)$ es enumerable.*

Demostración. Sea $f : \mathbb{Z} \times \mathbb{N} \to \mathbb{Z}(p^\infty)$ definida por

$$f(m, n) = e^{2\pi m/p^n}.$$

Por su misma definición, f es una función sobreyectiva, entonces tenemos $|\mathbb{Z}(p^\infty)| \leq \aleph_0$. Como el grupo de Prüfer es un conjunto infinito concluimos que este es enumerable. □

Teorema 2.14. *Sea p primo. $\mathbb{Z}(p^\infty)$ es un grupo abeliano divisible p-primario.*

Demostración. Dado que $\mathbb{C}^*$ es un grupo abeliano, $\mathbb{Z}(p^\infty)$ también es abeliano. Entonces consideremos $A = \bigoplus_p \mathbb{Z}(p^\infty)$. Vamos a probar que $A \cong \mathbb{Q}/\mathbb{Z}$ y de esta forma podemos concluir que $\mathbb{Z}(p^\infty)$ es un grupo divisible para todo p primo. Un elemento $(x_p)_p \in A$ es de la forma $((e^{2\pi i c_p/p^{n_p}})_p)$, donde $c_p \in \mathbb{Z}$ para todo p primo, para el cual existe solamente un conjunto fínito de índices J,tal que los términos $e^{2\pi i c_{p_j}/{p_j}^{n_{p_j}}} \neq 1$. Definamos $\phi : A \to \mathbb{Q}/\mathbb{Z}$ por $\phi((e^{2\pi i c_p/p^{n_p}})_p) = \sum_{j \in J} {c_{p_j}}/{{p_j}^{n_{p_j}}} + \mathbb{Z}$. Veamos que ϕ es un isomorfismo.

Es fácil ver que ϕ es un homomorfismo. Sean $(e^{2\pi i c_p/p^{n_p})_p}, (e^{2\pi i c'_p/p^{n'_p}})_p \in A$.

$$\begin{aligned}
\phi((e^{2\pi i c_p/p^{n_p}})_p * (e^{2\pi i c'_p/p^{n'_p}}) &= \phi((e^{2\pi i c_p/p^{n_p}} * e^{2\pi i c'_p/p^{n'_p}})_p) \\
&= \phi((e^{2\pi i (c_p/p^{n_p} + c'_p/p^{n'_p})})_p) \\
&= \phi((e^{2\pi i (p^{n'_p} c_p + p^{n_p} c'_p)/p^{n_p+n'_p}})_p) \\
&= \sum_p (p^{n'_p} c_p + p^{n_p} c'_p)/p^{n_p+n'_p} + \mathbb{Z} \\
&= \sum_p (c_p/p^{n_p} + c'_p/p^{n'_p}) + \mathbb{Z} \\
&= \sum_p c_p/p^{n_p} + \sum_p c'_p/p^{n'_p} + \mathbb{Z} \\
&= \phi((e^{2\pi i c_p/p^{n_p}})_p) * \phi((e^{2\pi i c'_p/p^{n'_p}})_p).
\end{aligned}$$

Ahora, para probar que ϕ es inyectiva veamos que $Ker(\phi) = \{(1)_p\}$. Por definición de ϕ sabemos que $(1)_p \in Ker(\phi)$. Sea $(e^{2\pi i c_p/p_p^n})_p \in Ker(\phi)$, tal que $(e^{2\pi i c_p/p^{n_p}})_p \neq (1)_p$, entonces $\phi((e^{2\pi i c_p/p^{n_p}})_p) = \mathbb{Z}$, es decir $\sum_p c_p/p^{n_p} \in \mathbb{Z}$. Veamos que ${p_j}^{n_{p_j}} | c_{p_j}$ para todo $j \in J$. Reescribimos

$$\sum_{j\in J} c_{p_j}/{p_j}^{n_{p_j}} + \mathbb{Z} = \frac{\sum_{j\in J} c_{p_j} \prod_{k\neq j} p_k}{\prod_{j\in J} p_j} + \mathbb{Z},$$

por lo tanto

$$\frac{\sum_{j\in J} c_{p_j} \prod_{k\neq j} {p_k}^{n_{p_k}}}{\prod_{j\in J} {p_j}^{n_{p_j}}} \in \mathbb{Z},$$

es decir, para todo $j \in J$,

$${p_j}^{n_{p_j}} | \sum_{j\in J} c_{p_j} \prod_{k\neq j} {p_k}^{n_{p_k}},$$

pero

$${p_j}^{n_{p_j}} | c_{p_l} \prod_{k\neq l} {p_k}^{n_{p_k}}$$

para todo $l \neq j$ y entonces

$$p_j{}^{n_{p_j}} | c_{p_j} \prod_{k \neq j} p_k{}^{n_{p_k}}.$$

Sea $k \in J$ tal que $k \neq j$, tenemos que $(p_j, p_k) = 1$ y por lo tanto

$$p_j{}^{n_{p_j}} | c_{p_j},$$

luego $e^{2\pi i c_{p_j}/p_j{}^{n}_{p_j}} = 1$ para todo $j \in J$ lo cual es una contradicción y por lo tanto $Ker(\phi) = \{(1)_p\}$. Así que ϕ es inyectiva.

Veamos que ϕ es sobreyectiva. Sean $a \in \mathbb{Z}$ y $b \in \mathbb{N}$, luego $a/b + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$. Por el teorema fundamental de la aritmética podemos escribir $b = \prod_{j \in J} p_k{}^{n_{p_k}}$. Como los números $b/p_j{}^{n_j}$ son primos relativos dos a dos, de existen $m_{p_j} \in \mathbb{Z}$ tales que $1 = \sum_{j \in J} m_{p_j}(b/p_k{}^{n_{p_k}})$. Luego $a/b = \sum_{j \in J} a m_{p_j}/p_k{}^{n_{p_k}}$. Ahora, sea $(x_p)_p$ tal que $(x_{p_k}) = 1$ si $k \notin J$ y $(x_{p_k}) = e^{2\pi i (a m_{p_k}/p_k{}^{n_{p_k}})}$. Como J es finito concluimos que $(x_p)_p \in A$ y $\phi((x_p)_p) = a/b + \mathbb{Z}$. Por lo tanto ϕ es biyectiva. □

El siguiente teorema clasifica todos los grupos abelianos divisibles.

Teorema 2.15. *Todo grupo abeliano divisible es isomorfo a la suma directa de copias de* $\mathbb{Q}$ *y copias de* $\mathbb{Z}(p^\infty)$ *para varios primos p.*

Demostración. Sea D un grupo divisible, veamos primero que tD es divisible. Si $x \in D$ tiene orden finito, $n \in \mathbb{N}$ y $x = ny$, entonces y tiene orden finito. Se sigue que si D es divisible, tD es divisible también y entonces existe un grupo abeliano V tal que

$$D = tD \oplus V,$$

donde V es libre de torsión. Ya que tD es un subgrupo divisible de D y entonces es un sumando directo. Como $D/tD \cong V$ y V es libre de torsión, V es un espacio vectorial sobre $\mathbb{Q}$ y por lo tanto es isomorfo a la suma de copias de $\mathbb{Q}$.

Ahora, como tD es un grupo de torsión por el Teorema 2.1.4 concluimos que $tD = \bigoplus_p T_p$, donde T_p es su componente p-primario, además, todos sus componentes p-primarios son divisibles. Por lo tanto es suficiente mostrar que para cada p, T_p es suma directa de copias de $\mathbb{Z}(p^\infty)$. Sea $x_1 \in tD$ de orden p. Escogemos x_2 tal que $x_1 = px_2$. Siguiendo este proceso

construimos la secuencia $x_1, x_2, \cdots$ tal que para cada $1 \leq j$, $px_{j+1} = x_j$. Veamos que el subgrupo generado por esta secuencia E es isomorfo a $\mathbb{Z}(p^\infty)$. Sea $x \in E$, luego existe I una colección finita de índices tal que $x = \sum_{j \in I} a_j x_j$ y sea $f : E \to \mathbb{Z}(p^\infty)$, dada por

$$f(x) = f(\sum_{j \in I} a_j x_j) = \prod_{j \in I} e^{(2\pi i a_j / p^j)}.$$

Es fácil ver que f es un isomorfismo. Denotemos S el conjunto de todos los subgrupos isomorfos a $\mathbb{Z}(p^\infty)$ y sea T el conjunto de $X \subset S$ para el cual la suma de los subgrupos de X es una suma directa. Entonces T es parcialmente ordenado por la inclusión y toda cadena tiene una cota superior que es la unión. Por el Lema de Zorn T tiene un elemento maximal. Sea H la suma directa de los subgrupos en X. Como H es suma directa de grupos isomorfos al grupo de Prüfer, es divisible y además, $H \subset T_p$, entonces $T_p = H \bigoplus K$ para algún K. Si K es no trivial, contiene un subgrupo L isomorfo a $\mathbb{Z}(p^\infty)$, y entonces $X \cup L \in T$ y contiene propiamente a X, contradiciendo la maximalidad de X. Por lo tanto $T_p = H$ y es una suma directa de copias de $\mathbb{Z}(p^\infty)$. □

2.4. Isomorfismos entre grupos divisibles

En esta sección vamos a dar una definición que será la clave para nuestro trabajo y nos dará las bases para demostrar cuando grupos divisibles son isomorfos. Dado un espacio divisible D, sabemos que D/tD es un grupo libre de torsión y además es divisible. Entonces por el Teorema 2.2.3 D/tD es un espacio vectorial sobre $\mathbb{Q}$. La acción de $\mathbb{Q}$ sobre D/tD está dada por $\frac{x}{y}a = b$, donde b es el único elemento tal que $yb = xa$.

Veamos que para cualquier grupo divisible D y p primo, $D[p]$ es un espacio vectorial sobre $\mathbb{Z}_p$. Sean $d \in D[p]$ y $\bar{x} \in \mathbb{Z}_p$, entonces existe $n \in \mathbb{N}$ tal que $0 \leq n \leq p-1$ y $x \equiv n \pmod{p}$, definamos

$$\bar{x}d = nd.$$

Para ver que está bien definida tomemos $\bar{x}, \bar{y} \in \mathbb{Z}_p$ tal que $\bar{x} = \bar{y}$. Existe $n \in \mathbb{N}$ tal que $0 \leq n \leq p-1$ y además $x \equiv y \equiv n \pmod{p}$. Por definición $\bar{x}d = nd$ y $\bar{y}d = nd$, entonces

$\bar{x}d = \bar{y}d$. Ahora,

$$p(\bar{x}d) = p(nd) = (pn)d = (np)d = n(pd) = 0,$$

es decir que $\bar{x}d \in D[p]$. Luego, $D[p]$ puede ser visto como un espacio vectorial sobre $\mathbb{Z}_p$. Gracias a esto podemos dar la siguiente definición.

Definición 2.9. *Si D es un grupo abeliano divisible se define*

$$\delta_\infty(D) = dim_{\mathbb{Q}}\,(D/tD)$$

y para todo $p \in \mathbb{Z}$ primo, se define

$$\delta_p(D) = dim_{\mathbb{Z}_p}\,(D[p])$$

Teorema 2.16. *Sean D y D' grupos abelianos divisibles. Entonces $D \cong D'$ si y sólo si $\delta_\infty(D) = \delta_\infty(D')$ y $\delta_p(D) = \delta_p(D')$ para todo p primo.*

Demostración. ($\Rightarrow$) Por Teorema 2.1.1 sabemos que si $D \cong D'$, entonces $tD \cong tD'$ y $D/tD \cong D'/tD'$ como grupos. Ahora D/tD y D'/tD' son grupos divisibles libres de torsión, por lo tanto son espacios sobre $\mathbb{Q}$. Queremos ver que ellos son isomorfos como espacios vectoriales sobre $\mathbb{Q}$ y así $\delta_\infty(D) = \delta_\infty(D')$. Existe $f : D/tD \to D'/tD'$ un isomorfismo de grupos, vamos a probar que f puede ser visto como una transformación lineal biyectiva entre espacios vectoriales, para esto basta mostrar la linealidad de f sobre $\mathbb{Q}$. Como f es homomorfismo, dados $x, y \in D$, $f(x + y) = f(x) + f(y)$. Sea $d \in D$ y $m/n \in \mathbb{Q}$, como D/tD es divisible y además es libre de torsión, existe un único $d' \in D$ tal que $d = nd'$, se sigue que $f(d) = f(nd')$ pero como f es un homomorfismo de grupos $f(nd') = nf(d')$, es decir que $f(d) = nf(d')$, así podemos concluir que $f(d')$ es el único elemento en D'/tD' tal que $f(d) = nf(d')$. Ahora, por la multiplicación definida en el Teorema 2.2.3 sabemos que $(m/n)d = md'$ y $(m/n)f(d) = mf(d') = f(md')$, por estas igualdades tenemos que $f((m/n)d) = f(md')$ y entonces $(m/n)f(d) = f((m/n)d)$, y por lo tanto D/tD y D'/tD' son isomorfos como espacios vectoriales sobre $\mathbb{Q}$.

Por Lema 2.1.5 tenemos también que las componentes p-primarias $(tD)_p \cong (tD')_p$ para todo p, por Teorema 2.2.5, $(tD)_p[p] \cong (tD')_p[p]$ y como $D[p] = (tD)_p[p]$ obtenemos que $D[p] \cong$

$D'[p]$ como grupos abelianos. Sabemos que $D[p]$ y $D'[p]$ pueden ser vistos como espacios vectoriales sobre $\mathbb{Z}_p$ y de forma análoga al caso anterior se demuestra que $D[p] \cong D'[p]$ como espacios vectoriales sobre $\mathbb{Z}_p$, es decir, $\delta_p(D) = \delta_p(D')$.

($\Leftarrow$) Reescribimos $D = V \oplus \bigoplus_p T_p$ y $D' = V' \oplus \bigoplus_p T'_p$, donde V y V' son subgrupos divisibles libres de torsión, además T_p y T'_p son los componentes p-primarios. Luego $\delta_p(D) = \delta_p(D')$ implica que $T_p \cong T'_p$, eso quiere decir que existe un isomorfismo $f_p : T_p \to T'_p$ para todo p. Mientras que $\delta_\infty(D) = \delta_\infty(D')$ implica que $V \cong V'$, es decir existe el isomorfismo $f_V : V \to V'$. Sea $d \in D$, luego $d = d_v + \sum_p d_p$ donde, $d_v \in V$ y $d_p \in T_p$. Definimos $f : D \to D'$ por $f(d) = f_v(d_v) + \sum_p f_p(d_p)$, las propiedades de isomorfismo se heredan de que cada una de las f_p. Por lo tanto $D \cong D'$. □

Capítulo 3

Un problema

En el inicio del trabajo nos propusimos encontrar una herramienta nueva para demostrar isomorfismos entre grupos divisibles. Para esto consideremos los grupos

$$\mathbb{C}^*, \quad \mathbb{Q}/\mathbb{Z} \oplus \mathbb{R}, \quad \mathbb{R}/\mathbb{Z}, \quad \prod_q \mathbb{Z}(q^\infty) \quad \text{y} \quad S^1,$$

donde $S^1 = \{z \in \mathbb{C} : |z| = 1\}$. Primero queremos ver que estos grupos son divisibles para poder aplicar el Teorema 2.4.1.

Veamos que $\mathbb{R}$ es divisible. Sea $x \in \mathbb{R}$ y $n \in \mathbb{N}$, entonces $y = x/n \in \mathbb{R}$ y $nx = y$. Ahora, $\mathbb{Q}$ es divisible, entonces $\mathbb{Q}/\mathbb{Z}$ es divisible y como $\mathbb{R}$ es divisible $\mathbb{Q}/\mathbb{Z} \oplus \mathbb{R}$ también lo será.

Para $\mathbb{C}^*$ ya sabemos que dados $x \in \mathbb{C}^*$ y $n \in \mathbb{N}$ existe $y \in \mathbb{C}^*$ tal que $x = y^n$. De manera análoga S^1 es divisible pues dados $x \in S^1$ y $n \in \mathbb{N}$, el $y \in \mathbb{C}^*$ que cumple la condición $x = y^n$ tiene norma 1 y entonces $y \in S^1$. Por otro lado ya vimos que el grupo de Prüfer es divisible, luego $\prod_q \mathbb{Z}(q^\infty)$ es divisible.

Lema 3.1. $\aleph_0^{\aleph_0} = \mathfrak{c}$

Demostración. Ya sabemos que $2 \leq \aleph_0$, luego $2^{\aleph_0} \leq \aleph_0^{\aleph_0}$ pero como $\aleph_0 \leq 2^{\aleph_0}$ obtenemos que $\aleph_0^{\aleph_0} \leq (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \aleph_0}$ y por proposición 1.1.9 se sigue que $2^{\aleph_0 \aleph_0} = 2^{\aleph_0}$. A partir de estas desigualdades tenemos que $2^{\aleph_0} \leq \aleph_0^{\aleph_0} \leq 2^{\aleph_0}$ y concluimos que $\aleph_0^{\aleph_0} = \mathfrak{c}$. □

Este lema será importante para la conclusión del siguiente teorema.

Teorema 3.2. *Los siguientes grupos abelianos son isomorfos:*

$$\mathbb{C}^*, \quad \mathbb{Q}/\mathbb{Z} \oplus \mathbb{R}, \quad \mathbb{R}/\mathbb{Z}, \quad \prod_q \mathbb{Z}(q^\infty) \quad \text{y} \quad S^1,$$

donde q recorre el conjunto de los números primos.

Demostración. Ya sabemos que todos los grupos listados anteriormente son divisibles así que por Teorema 2.4.1 debemos mirar que para cualesquiera dos grupos de estos, D y D' se tiene $\delta_\infty(D) = \delta_\infty(D')$ y $\delta_p(D) = \delta_p(D')$ para todo p primo.
Veamos que $\delta_p(D) = 1$, donde p es un primo cualquiera.

i. Para $\mathbb{C}^*$ los elementos en $\mathbb{C}^*[p]$ serán las raíces p-ésimas de la unidad, es decir

$$\mathbb{C}^*[p] = \{e^{2\pi i \frac{k}{p}} : k \in \mathbb{N}, 0 \leq k < p\}.$$

Ya sabemos que este conjunto tiene p elementos y como espacio vectorial sobre $\mathbb{Z}_p$ su dimensión es 1. Por lo tanto $\delta_p(\mathbb{C}^*) = 1$.

ii. El caso S^1 es igual al anterior, pues las raíces de la unidad tienen norma 1, así $\mathbb{C}^*[p] = S^1[p]$.

iii. Para $\prod_q \mathbb{Z}(q^\infty)[p]$ notemos primero que para $q \neq p$ primo, ningún elemento en $\mathbb{Z}(q^\infty)$ va a tener orden p. Así que los elementos $(x_q)_q \in \prod_q \mathbb{Z}(q^\infty)[p]$ son tales que $x_q = 1$ para todo primo $q \neq p$. Entonces sólo debemos mirar qué sucede en el término x_p. Si $x_p^p = 1$, tenemos que x_p es raíz de la unidad y él está en $\mathbb{C}^*[p]$, luego $\delta_p\left(\prod_q \mathbb{Z}(q^\infty)\right) = 1$

iv. Sea $(a/b + \mathbb{Z}, c) \in \mathbb{Q}/\mathbb{Z} \oplus \mathbb{R}$ tal que $mcd(a, b) = 1$ y $p(a/b + \mathbb{Z}, r) = (\mathbb{Z}, 0)$. Es decir, $pr = 0$ y $pa/b \in \mathbb{Z}$, lo que implica $r = 0$ y tenemos que $b = p$, luego $(1/p + \mathbb{Z}, 1/p)$ genera

$$\mathbb{Q}/\mathbb{Z} \oplus \mathbb{R}[p] = \{(1/p + \mathbb{Z}, 0), (2/p + \mathbb{Z}, 0), \cdots ((p-1)/p + \mathbb{Z}, 0), (0 + \mathbb{Z}, 0)\},$$

que tiene p elementos, de donde $\delta_p(\mathbb{Q}/\mathbb{Z} \oplus \mathbb{R}) = 1$.

v. De forma análoga sucede en $\mathbb{R}/\mathbb{Z}[p]$, sea $r + \mathbb{Z} \in \mathbb{R}/\mathbb{Z}[p]$, luego $pr = 1$, es decir $r = 1/p$ y de nuevo, $\mathbb{R}/\mathbb{Z}[p]$ es un espacio generado por un elemento sobre $\mathbb{Z}_p$. Es decir $\delta_p(\mathbb{R}/\mathbb{Z}) = 1$.

Ahora, miremos qué sucede con $\delta_\infty(D)$.

i. Sea $D = \mathbb{Q}/\mathbb{Z} \oplus \mathbb{R}$. Luego $tD = \mathbb{Q}/\mathbb{Z}$ y $D/tD \cong \mathbb{R}$ como espacios sobre $\mathbb{Q}$, es decir $\delta_\infty(D) = dim_{\mathbb{Q}}(\mathbb{R})$. Veamos que este es igual al cardinal del continuo. Sea $\mathcal{B}$ una base de $\mathbb{R}$ sobre $\mathbb{Q}$.

$\mathcal{B}$ no es finita pues como π no es algebraico sobre $\mathbb{Q}$ el conjunto $\{\pi^n\}_{n\geq 1}$ es linealmente independiente sobre $\mathbb{Q}$, por lo tanto $|\mathcal{B}| \geq \aleph_0$.

Veamos que $|\mathcal{B}| > \aleph_0$. Si $|\mathcal{B}| = \aleph_0$, existe una enumeración para $\mathcal{B}$, sea esta $\mathcal{B} = \{x_i\}_{j=1}^{\infty}$. Si $A = \bigcup_{r\geq 1} \mathbb{Q}^n$, entonces A es enumerable y para $x \in R$, existen $m \in \mathbb{N}$, $r_1, \cdots, r_m \in \mathbb{Q}$ y $x_{i_1}, \cdots, x_{i_m} \in \mathcal{B}$ tales que $x = \sum_{j=1}^{m} r_j x_{i_j}$ y así la función $\varphi : A \to \mathbb{R}$ definida por $\varphi(r_1, \cdots, r_n) = \sum_{i=1}^{n} r_i x_i$ es sobreyectiva. Se sigue que $\mathfrak{c} = |\mathbb{R}| \leq |A| = \aleph_0$ lo cual es una contradicción y concluimos que $|\mathcal{B}| > \aleph_0$. Entonces $\delta_\infty(D) = \mathfrak{c}$.

Ahora veamos que $|\mathcal{B}| = \mathfrak{c}$. Tenemos que $\aleph_0 < |\mathcal{B}| \leq |\mathbb{R}| = \mathfrak{c}$ y la hipótesis del continuo implica que $|\mathcal{B}| = \mathfrak{c}$.

ii. Sea $D = \mathbb{R}/\mathbb{Z}$ y si $r+\mathbb{Z} \in D$ tal que $r+\mathbb{Z} \in tD$, existe $n \in \mathbb{N}$ tal que $n(r+\mathbb{Z}) = \mathbb{Z}$ pero esto es lo mismo a decir que $nr \in \mathbb{Z}$, luego $r \in \mathbb{Q}$. Podemos concluir que $tD = \mathbb{Q}/\mathbb{Z}$. Por lo tanto $D/tD \cong \mathbb{R}/\mathbb{Q}$ como espacios vectoriales sobre $\mathbb{Q}$. Es decir $\delta_\infty(D) = dim_{\mathbb{Q}}(\mathbb{R}/\mathbb{Q})$. Como $dim_{\mathbb{Q}}(\mathbb{R}) = \mathfrak{c}$, entonces $\mathbb{R} \cong \bigoplus_{i\in I} \mathbb{Q}$, donde $|I| = \mathfrak{c}$. Luego $\mathbb{R} \cong \mathbb{Q} \oplus \bigoplus_{i\in I'} \mathbb{Q}$ donde $|I'| = \mathfrak{c}$ y $\mathbb{R}/\mathbb{Q} \cong \bigoplus_{i\in I'} \mathbb{Q}$, y se sigue que $\delta_\infty(D) = \mathfrak{c}$.

iii. Sea $D = \mathbb{C}^*$. Definimos una función $f : \mathbb{R} \times \mathbb{R} \to \mathbb{C}$ por $f(a, b) = a + bi$. Luego

$$|\mathbb{C}| = |\mathbb{R} \times \mathbb{R}| = |\mathbb{R}||\mathbb{R}| = \mathfrak{c}\mathfrak{c} = \mathfrak{c}$$

y como $\mathbb{C}^* = \mathbb{C}\setminus\{0\}$, entonces $|\mathbb{C}^*| = \mathfrak{c}$. Ahora escribimos $\mathbb{C}^* = V \oplus t\mathbb{C}^*$ donde V es libre de torsión, además $t\mathbb{C}^* = \bigoplus_{p\in\mathbb{P}'} T_p$, con $\mathbb{P}' \subset \mathbb{P}$ y $|T_p| = p$, $t\mathbb{C}^*$ es enumerable. Pero como $\mathbb{C}^*$ no es enumerable, V no es enumerable. Ahora, $V \cong \bigoplus_{i\in I} \mathbb{Q}$, donde $dim_{\mathbb{Q}}(V) = |I|$. Si I es enumerable V también lo sería, por lo tanto I no es enumerable y como $V \subset \mathbb{C}^*$, entonces $|I| = \mathfrak{c}$, luego $dim_{\mathbb{Q}}(V) = \mathfrak{c}$. Pero como $D/tD \cong V$ como espacios sobre $\mathbb{Q}$, obtenemos que $\delta_\infty(D) = \mathfrak{c}$.

iv. Sean $D = S^1$ y $f : [0, 2\pi) \to S^1$ definida por $f(\theta) = e^{i\theta}$. Ya sabemos que esta función es biyectiva, por lo tanto $|S^1| = |f[0, 2\pi)| = \mathfrak{c}$. Haciendo el proceso análogo del caso anterior obtenemos que $\delta_\infty(D) = \mathfrak{c}$.

v. Para $D = \prod_q \mathbb{Z}(q^\infty)$ sabemos que $|\mathbb{P}| = \aleph_0$. Veamos que $|\mathbb{Z}(q^\infty)| = \aleph_0$ para todo $q \in \mathbb{P}$. Recordemos que el Lema 3.0.2 nos dice que $\aleph_0{}^{\aleph_0} = \mathfrak{c}$, entonces

$$\begin{aligned} |\prod_q \mathbb{Z}(q^\infty)| = \prod_q |\mathbb{Z}(q^\infty)| &= \prod_q \aleph_0 \\ &= \aleph_0{}^{\aleph_0} \\ &= \mathfrak{c}. \end{aligned}$$

De forma análoga a los casos anteriores, $\delta_\infty(D) = \mathfrak{c}$.

Para cada uno de los grupos obtenemos que $\delta_\infty(D) = \mathfrak{c}$ y $\delta_p(D) = 1$ para todo p primo. Por Teorema 2.4.1 se verifica que los grupos son isomorfos dos a dos. □

Conclusiones

Al principio del trabajo nos propusimos mostrar que ciertos grupos abelianos son isomorfos y para esto hicimos un corto pero conciso estudio de algunas definiciones y teoremas básicos en la teoría de conjuntos, álgebra lineal, álgebra moderna y además de esto, revisamos varios conceptos de la teoría de números que tendrían un gran papel para poder cumplir nuestro objetivo. Estudiamos a su vez, nuevos conceptos como el de grupo divisible y sus propiedades que son los protagonistas de este trabajo y que a simple vista es una estructura sencilla pero nos ofrece propiedades bastante útiles.

Al final pudimos cumplir el objetivo de mostrar que los grupos $\mathbb{C}^*$, $\mathbb{Q}/\mathbb{Z} \oplus \mathbb{R}$, $\mathbb{R}/\mathbb{Z}$, $\prod_q \mathbb{Z}(q^\infty)$, y el grupo S^1 son isomorfos usando la propiedad de divisibilidad. Más allá de este resultado específico, nos encontramos con una herramienta general muy fuerte que involucra los conceptos de las teorías ya mencionadas para determinar si dos grupos divisibles son isomorfos sin necesidad de construir explicitamente el isomorfismo entre ellos.

Bibliografía

[1] Fusch, Lasló. *Infinite abelian groups*. Volume 36-1, Academic Press. 1970.

[2] Guba, V. S. *A finitely generated complete group*. Mathematics of the USSR-Izvestiya. 1986.

[3] Lam, T.Y. *Lectures on Modules and Rings*. Springer-Verlag. 1999.

[4] Chapman, E. y Hall, E. *Abstract Algebra with Applications*. Volume I, Springer-Verlag. 1993.

[5] Lezama, Oswaldo. *Anillos, módulos y categorías*. Universidad Nacional de Colombia, Santafé de Bogotá, 1994.

[6] Pinter, Charles C. *A book of Set Theory*. Dover Publications Inc., 2014.

[7] Robinson, Derrick. *A Course in the Theory of Groups*. Second Edition, Springer-Verlag. 1995.

[8] Roman, Steven. *Advanced Linear Algebra*. Fourth Edition, Springer-Verlag. 2005.

[9] Rotman, Joseph J. *Advanced Modern Algebra*. Segunda Edición, American Mathematical Society. 2003.

[10] Rotman, Joseph J. *An Introduction to the Theory of Groups*. Fourth Edition,Springer-Verlag. 1995.