UNA DEMOSTRACIÓN DEL ISOMORFISMO ENTRE LOS COMPLEJOS SIN EL CERO Y EL CÍRCULO DE RADIO UNO

Odri Johanna Cubillos Barragán

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE MATEMÁTICAS
BUCARAMANGA
2007

UNA DEMOSTRACIÓN DEL ISOMORFISMO ENTRE LOS COMPLEJOS SIN EL CERO Y EL CÍRCULO DE RADIO UNO

Odri Johanna Cubillos Barragán

Monografía presentada como requisito para optar al
título de Licenciado en Matemáticas

Director
RAFAEL FERNANDO ISAACS GIRALDO
Magister en Matemáticas

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE MATEMÁTICAS
BUCARAMANGA
2007

Nota de aceptación

(4.2) CUATRO DOS

RAFAEL F. ISAACS GIRALDO
Magister en Matemáticas
Director

SOFIA PINZÓN DURÁN
Doctora en Matemáticas
Calificador

CARLOS WILSON RODRÍGUEZ
Magister en Matemáticas
Calificador

Bucaramanga, junio de 2007

Dedicatoria. “A mis padres, mi hermana y mis amigos por su apoyo y paciencia en alcanzar esta meta ”.

TITULO: UNA DEMOSTRACIÓN DEL ISOMORFISMO DE LOS COMPLEJOS SIN EL CERO Y EL CÍRCULO DE RADIO UNO

PALABRAS CLAVES:

Isomorfismo
Grupos
Grupos divisibles
Espacios vectoriales de dimensión infinita
Lema de Zorn
El campo de los números complejos sin el cero
Grupos Abelianos

Descripción

Es este trabajo esta basado en el artículo de Richard Duffy [1] en el que se presenta la demostración de los grupos multiplicativos $\mathbb{C}^*$ y S^*1 dicha demostración no utiliza el teorema fundamental de grupos divisibles, para la demostración se usarán otras serie de herramientas y conceptos como lo son: el Lema de Zorn, el isomorfismo de espacios vectoriales con dimensión infinita y algunos conceptos de isomorfismo para el producto de grupos abelianos. La demostración utilizará todos estos resultados para presentar una serie de isomorfismos basados en el isomorfismo de espacios vectoriales $\mathbb{R} \times \mathbb{R} \cong \mathbb{R}$ para llegar a l nuestro objetivo final el isomorfismo que existe entre $\mathbb{C}^*$ y S^1.

Durante el desarrollo de este trabajo se muestran ciertos resultados como: ilustrar a partir de sumas directas de grupos de isomorfimo conocidos o estructuras interesantes como lo es el conjunto de las sucesiones; el cual se puede ver como suma directa de funciones en los naturales y mostrar la representación del grupo $\mathbb{C}$ como suma directas de grupos isomorfos a $\mathbb{C}_{p^\infty}$ o $\mathbb{Q}$.

[1] An elementary proof of the isomorfismo $\mathbb{C}^* \cong S^1$, The American mathematical monthly, Vol 90 Number, 1983, p. 201.

TITLE: A DEMONSTRATION OF THE ISOMORPHISM BETWEEN THE COMPLEXES WITHOUT ZERO AND THE CIRCLE OF RADIO ONE

KEY WORDS:

Isomorphism
Groups
Divisible groups
Abelian groups
Vectorial spaces of infinite dimension
Motto of Zorn
The field of the complex numbers without zero

Description:

This work is based on the article of Richard Duffy [2] where the demonstration of the Abelian groups $\mathbb{C}^*$ and S^*1 is presented. Such demonstration does not make use of the fundamental theorem of divisible groups. For this demonstration, other concepts and tools like the Lemm of Zorn's, the isomorphism of vectorial spaces whith infinite dimension and some isomorphism concepts for the product of the Abelian groups will be used. The demonstration will use all these results to present a series of isomorphisms based on the isomorphism of vectorial spaces $\mathbb{R} \times \mathbb{R} \cong \mathbb{R}$ to obtain our final objetive which is the isomorfhism between $\mathbb{C}^*$ y S^1.

During the development of this work certain results are presented like the illustration from direct sums of isomorphisms of well-Kown groups or interesting structures like the set of successions that can be seen as a direct sum of the functions in the naturals. Additionally, the illustration of the isomorph groups $\mathbb{C}_{p^\infty}$ o $\mathbb{Q}$.

[2] An elementary proof of the isomorfismo $\mathbb{C}^* \cong S^1$, The American mathematical monthly, Vol 90 Number, 1983, p. 201.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICAS

INTRODUCCIÓN

Mostrar que dos "cosas" en cualquier contesto son iguales o no, aparenta un ejercicio muy sencillo, pero en la realidad determinar que tan "iguales son", puede convertirse en toda una ardua tarea. Lo que se suele hacer en la mayoría de los casos es comparar e indicar que cualidades o propiedades cumplen ambos objetos y cuales no. Es entonces donde aparecen las diferentes estructuras (sociales, mentales, lógicas, matemáticas, etc.). En particular las estructuras algebraicas se caracterizan por ser un conjunto con una o varias operaciones y matematicamente hablando si dos estructuras son en esencia iguales entonces son isomorfas. Por lo tanto cuando dos estructuras son isomorfas, ambas cumplen las mismas propiedades, y cualquier propiedad estructural es simultáneamente cierta o falsa para ambas. Por eso en matemáticas las estructuras, en la mayoría de los casos, se estudian y clasifican por medio de isomorfismos.

Este importante concepto se pretende recoger y utilizar en este trabajo, el cual nace a partir del análisis del artículo publicado por Richard Duffy [1]. Por lo tanto no solo se estudiarán algunas estructuras abelianas sino que se recoge la mayoría de conceptos y temas que se trabajan en un curso de Álgebra Moderna y algunos conceptos de Teoría de Conjuntos. El isomorfismo de los grupos abelianos $(\mathbb{C}^*, S^1)$ es un claro ejemplo de estructuras que aparentemente no son iguales y cuya demostración necesita de herramientas avanzadas y complejas, las cuales no se encuentran a nuestro alcance.

Entonces se dedicará nuestra atención al estudio de estos dos grupos abelianos y el isomorfismo que existe entre ellos, para lo cual se contará con herramientas que se han obtenido en el transcurso de la Licenciatura. Se inciará con el estudio de los grupos $\mathbb{C}^*, S^1$ y algunas de su propiedades estructurales. Se abordarán también algunos conceptos de la teoría de conjuntos como son las relaciones, sus propiedades y el importante Lema de Zorn, indispensable para muchos resultados importantes en las matemáticas y en particular para este trabajo. Además se revisarán los conceptos y ejemplos interesantes de los isomorfismo de grupos abelianos asi como de espacios vectoriales. Para culminar con el isomorfismo de $\mathbb{C}^* \cong S^1$ el cual depende de los resultados obtenidos en los diferentes capitulos de este trabajo. Además se pretende mostrar que en el grupo multiplicativo de los Complejos se encuentran una variedad muy rica de ejemplos de grupos conmutativos que ilustra las propiedades de los grupos abelianos que se pueden estudiar en un curso básico de Álgebra Moderna.

CAPÍTULO 1

PRELIMINARES

El poder establecer semejanzas e igualdades entre diferentes objetos es un punto fundamental que muchas veces resulta de suma dificultad. Poder establecer o al menos mostrar que dos cosas "*no son lo mismo pero son igual*" es lo que se conoce como isomorfismo. Este es un tema de estudio que siempre ha sido de gran interés en las matemáticas y ha dado resultados interesantes como lo es el isomorfismo que existe entre los grupos multiplicativos de los complejos sin el cero y el circulo de radio uno (el cual se notara como $\mathbb{C}^* \cong S^1$); dado que una estructura es subestructura de la otra y aparentemente la estructura mayor los complejos sin el cero $\mathbb{C}^*$ es más compleja que el subconjunto del circulo de radio uno S^1.

Vale la pena transcribir como el texto de John J. Frailegh [2] presenta el concepto de isomorfismo de grupos:

> "la idea de que dos grupos G y G' son estructuralmente iguales o isomorfos, si son idénticos salvo por el nombre de los elementos y las operaciones. De este modo, se obtiene G' a partir de G cambiando el nombre de un elemento x en G por el nombre de cierto elemento x' en G'. Esto es, a cada $x \in G$ se le asígna una contraparte $x' \in G'$. En realidad, no es más que una ***función*** ϕ con dominio G. Es claro, que dos elementos diferentes x y y en G deben tener contrapartes diferentes $x' = x\phi$ y $y' = y\phi$ en G' es decir, la función ϕ debe ser uno a uno. Además, cada elemento de G' debe ser la contraparte de algún elemento de G o sea que la función ϕ debe ser sobre G'. Esto cambia el nombre de los elementos. por último, si los grupos serán estructuralmente el mismo y si, por el momento, se denota la operación del grupo G por $*$ y la de G' por $*'$, entonces la contraparte de $x*y$ debe ser $x'*'y'$, o $(x*y)\phi$ debería ser $(x\phi)*'(y\phi)$. Por lo común se omiten las notaciones $*$ y $*'$ para las operaciones se usa la notación multiplicativa, esto es,
>
> $$(xy)\phi = (x\phi)(y\phi). \tag{1.0.1}$$
>
> Nótese que la multiplicación xy en el lado izquierdo en $(xy)\phi = (x\phi)(y\phi)$ es la multiplicación en G mientras la multiplicación $(x\phi)(y\phi)$ del lado derecho es la de G'. Estas ideas se conjugan en la siguiente definición.

> *Definición* 1.0.1. Un **isomorfismo** entre los grupos $(G, .)$ y $(G', *)$ es una función ϕ uno a uno, que lleva G sobre G' y tal que para todas las x y y en G,
>
> $$(x.y)\phi = (x\phi) * (y\phi).$$
>
> Los grupos G y G' son isomorfos. La notación usual es $G \cong G'$" [1].

En el artículo de *Duffy* [1] se establece una demostración del isomorfismo entre los grupos multiplicativos de los complejos sin el cero $\mathbb{C}^*$ y el círculo de radio uno S^1, que no se establece de forma natural como si lo es, el isomorfismo entre $\mathbb{Z}$ y $2\mathbb{Z}$, o en general $\mathbb{Z}$ con los multiplos de k siendo $k \in \mathbb{Z}$, es decir $k\mathbb{Z}$; en donde a cada entero n tiene como imagen kn. También es fácil intuir que dos grupos cíclicos con el mismo cardinal son isomorfos así se ve que por ejemplo: ${\mathbb{Z}^*}_7$ y $\mathbb{Z}_6$ con la suma son isomorfos[2]. *Duffy* [1] realiza es su articulo una demostración del isomorfismo empleando uno de los postulados del *Axioma de Elección*, el *Lema de Zorn* y teoremas de isomorfismo para grupos, sin usar el Teorema Fundamental de grupos divisibles.

El *Axioma de Elección* y su colorario el *Lema de Zorn* son herramientas de gran utilidad en la matemática actual que han derivado grandes resultados sorprendentes como la paradoja de *Banach-Tarski* [8].

> "*Existe una descomposición de un numero finito de pedazos de S^2 (la esfera unitaria en $\mathbb{R}^3$) tal que al recomponerse de cierta manera adecuada, terminan siendo isométricas a la unión de dos esferas unitarias* " [3]

Durante la demostración del isomorfismo, *Duffy* usa una de las consecuencias del Lema de Zorn; " *todo conjunto linealmente independiente de un espacio vectorial puede ser extendido a una base*" y que el grupo aditivo de los enteros $(\mathbb{Z})$ es un subgrupo normal de $\mathbb{R}$ se apoyo también en los teoremas fundamentales del isomorfismo para grupos. Estos temas serán expuestos de manera más detallada en el transcurso de este trabajo obteniendo los resultados necesarios para la demostración del isomorfismo de grupos ($\mathbb{C}^* \cong S^1$).

1.1. Notación y resultados previos

Las estructuras algebraicas comprenden un conjunto dotado de una o varias operaciones. Es a veces conveniente especificar el conjunto y todos las operaciones involucradas pero esto también puede volver la notación pesada.
Todo los subgrupos que se trabajarán serán númericos y conmutativos y estará implícita la operación. Cuando se hable de grupos en general se utilizará notación aditiva o multiplicativa y en la siguiente tabla se especifica cómo se nota los módulos, los inversos y las repeticiones de operaciones en cada una de las notaciones.

[1] Frailegh utiliza la notación $(x)\phi$ para la imagen de x por medio de la función ϕ, además decir que ϕ lleva A sobre B implica que la función ϕ es sobreyectiva.

[2] ${\mathbb{Z}^*}_7$: el grupo de los enteros módulo 7 sin el cero con la multiplicaión.

[3] Macho Stalder, Marta, La paradoja de BanachTarski: Cómo construir el sol apartir de un guisante.

	ADICIÓN	MULTIPLICACIÓN
OPERACIÓN	$+$	$.$
MODULO	0	1
INVERSO	$-x$	$x^{-1} = \frac{1}{x}$
OPERAR n VECES A x	nx	x^n

Tabla 1.1: Tabla de notación para grupos

Los grupos que más se usarán en el desarrollo de este trabajo serán los siguientes grupos aditivos: el de los enteros $\mathbb{Z}$, los racionales $\mathbb{Q}$, enteros módulo n notado $\mathbb{Z}_n$, reales $\mathbb{R}$ y los complejos $\mathbb{C}$; los grupos multiplicativos que se utilizarán serán los racionales sin el cero $\mathbb{Q}^*$, los reales sin el cero $\mathbb{R}^*$, los racionales positivos $\mathbb{Q}^+$, los reales positivos $\mathbb{R}^+$ y los complejos sin el cero $\mathbb{C}^*$. No se utilizará la notación clasica de grupos $(G, \oslash)$ puesto que para cada una de la notaciones descritas anteriormente la operación está implicita.
En $\mathbb{Z}$ se trabajará suponiendo conocidos los resultados elementales de divisibilidad, el máximo común divisor de los números n, m se notará $\text{mcd}(n, m)$ y también se tendrá en cuenta que si $\text{mcd}(n, m) = d$ existen entonces α y β enteros tales que $d = \alpha n + \beta m$.
Cuando se hable de funciones, isomorfismo de grupos, isomorfismo de espacios vectoriales y transformaciones lineales, se supondrá la familiaridad con el concepto de función entre dos conjuntos, dominio, recorrido, función uno a uno, función sobreyectiva, funciones biyectivas, etc., cuya notación será la notación clasica, es decir para describir a una función de A en B se notará como $f : A \to B$, la imagen de a por medio de f se notará como $f(a)$, la inversa de la función f, si existe, se notará como $f^{-1} : B \to A$.
Cuando se hable de conjuntos, espacios vectoriales y/o grupos éstos se notarán con letras mayúsculas, mientras que los elementos de los mismos con minúsculas.
Se notará $\mathcal{P}(X)$ la colección de todos los subconjuntos de X. Si $\phi \neq \mathcal{F} \subseteq \mathcal{P}(X)$ se dirá que $\mathcal{F}$ es una ***partición*** del conjunto X si y sólo si:

1. $\phi \notin \mathcal{F}$;
2. $\bigcup \mathcal{F} = X$;
3. Los conjuntos de $\mathcal{F}$ son disyuntos dos a dos, es decir, si $S_1, S_2 \in \mathcal{F}$ y $S_1 \neq S_2$, entonces $S_1 \cap S_2 = \phi$.

También se suponen conocidas las propiedades elementales de los cardinales transfinitos, en especial usaremos que si κ es un cardinal infinito entonces $\kappa\kappa = \kappa$.

CAPÍTULO 2

EL CONJUNTO DE LOS NÚMEROS COMPLEJOS

2.1. Números complejos

Definición 2.1.1. [3] Un número complejo z puede ser definido como el par ordenado (x, y) de números reales x y y,

$$z = (x, y)$$

donde x se llamará *la parte real* y y *la parte imaginaria* del complejo z.
Sean z_1 y z_2 dos números complejos cualesquiera, tales que $z_1 = (x_1, y_1)$ y $z_2 = (x_2, y_2)$.
Se define la adición de complejos como:

$$z_1 + z_2 = (x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2).$$

Se define la multiplicación de complejos como:

$$z_1 z_2 = (x_1, y_1)(x_2, y_2) = (x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1).$$

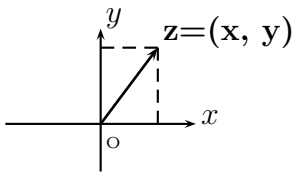
De la definición es natural asociar el par ordenado (x, y) a la representación geométrica de un número complejo z con la coordenada rectangular de un punto en el plano xy. Cada número complejo corresponde a un único punto y recíprocamente. El origen representa el punto $z = 0$ y el plano xy se llamará *plano complejo*.
A partir de la definición (2.1.1) y la representación geométrica anterior podemos afirmar que:

1. El par ordenado $(x, 0)$ se asocia como el número real x;

$$(x, 0) = x.$$

2. El par ordenado $(0, 1)$ se le asocia el símbolo i y será llamado **unidad imaginaria**:

$$(0, 1) = i.$$



Gráfica 2.1: Representación geométrica de $z = (x, y)$.

Así, tenemos que los números reales son subconjunto de los números complejos y el par ordenado $(0, y)$ es un número *imaginario puro* y consecuentemente se denota el número complejo z como $z = (x, y) = x + yi$.

2.1.1. Módulo de un número complejo

El número real no negativo $\sqrt{x^2 + y^2}$ es llamado el *valor absoluto* o *módulo* del número complejo $z = x + yi$, se tiene por definición,

$$|z| = |x + yi| = \sqrt{x^2 + y^2}. \tag{2.1.1}$$

Geométricamente, el valor absoluto o módulo de un número complejo z es la magnitud del vector z, es decir, la distancia desde el punto z al origen. Hay que tener en cuenta que el enunciado $|z_1| > |z_2|$ significa que el punto z_1 está a mayor distancia del origen que el punto z_2.

La relación de orden que se establece en los números reales "mayor que" o "menor que" no tiene sentido en los números complejos, a menos que ambos sean reales. Por lo tanto, la relación de orden enunciada sólo es aplicable a los módulos de números complejos, o sea la afirmación $z_1 < z_2$ o $z_1 > z_2$ ***no tiene sentido a menos que ambos sean reales***.

2.1.2. Conjugado de un número complejo

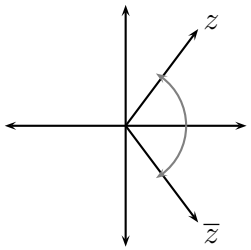
El conjugado de un número complejo $z = x + yi$ o simplemente conjugado, es el número

$$\bar{z} = (x, -y) = x - yi. \tag{2.1.2}$$

Desde el punto de vista geométrico, un punto $\bar{z}$ es la reflexión de un punto z en en eje x puesto que la posición del punto $\bar{z}$ es simétrica al punto z en relación al eje x.
Sean $z_1 = (x_1, y_1)$ y $z_2 = (x_2, y_2)$, entonces:

$$\overline{z_1 + z_2} = (x_1 + x_2) - (y_1 + y_2)i = (x_1 - y_1 i) + (x_2 - y_2 i) = \overline{z_1} + \overline{z_2}$$

$$\overline{z_1 z_2} = (x_1 x_2 - y_1 y_2) - (x_1 y_2 + x_2 y_1)i =$$
$$(x_1 x_2 - y_1 y_2, -x_1 y_2 - x_2 y_1) = (x_1 - y_1)(x_2 - y_2) = \overline{z_1 z_2}.$$



Gráfica 2.2: Representación geométrica del conjugado de z.

En otras palabras, el conjugado de la suma es la suma de los conjugados:

$$\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}. \tag{2.1.3}$$

y el conjugado del producto es el producto de conjugados:

$$\overline{z_1 z_2} = \overline{z_1} \cdot \overline{z_2}. \tag{2.1.4}$$

2.1.3. Forma polar de un número complejo

Las coordenadas polares de un número complejo representado por $z = x+yi$, son los valores (r, θ) donde:

$$x = r\cos\theta \quad y = r\,\mathrm{sen}\,\theta \tag{2.1.5}$$

$$r = \sqrt{x^2 + y^2} \qquad r = |z| \tag{2.1.6}$$

Así el número complejo z se escribe de la forma

$$z = r(\cos\theta + i\,\mathrm{sen}\,\theta). \tag{2.1.7}$$

El ángulo θ es llamado *el argumento* de z denotado por $\arg(z)$. Cuando $z \neq 0$ los valores de θ son determinados por las ecuaciones (2.1.5) y la relación

$$\tan\theta = \frac{y}{x} \tag{2.1.8}$$

donde la ecuación (2.1.5) muestra el cuadrante en el que el punto z se encuentra.

Euler proporcionó un resultado sorprendente que relaciona la forma polar de un número complejo con la exponenciación de su argumento

$$z = r(\cos\theta + i\,\mathrm{sen}\,\theta) = re^{i\theta} \tag{2.1.9}$$

El $\arg(z)$ es multivalente en relación a la ecuación (2.1.5) dado que las funciones cos y sen son funciones periódicas con un periodo de 2π radianes. Si $z \neq 0$, existe un único valor en radianes de θ en el intervalo $\theta_0 \leq \theta < \theta_0 + 2\pi$, donde θ_0 es un número cualquiera. Cuando

$z = 0$, entonces $r = 0$ y θ es arbitrario. Como un ejemplo se puede ver que si $z = 2 - 2i$, entonces $r = 2\sqrt{2}$ y $\arg(z) = \frac{-\pi}{4} \pm 2n\pi$ (donde $n = 0, 1, 2, \ldots$), otro ejemplo es,

$$-i = \cos(\frac{3\pi}{2}) + i\,\mathrm{sen}(\frac{3\pi}{2}) = cos(-\frac{\pi}{2}) + i\,\mathrm{sen}(-\frac{\pi}{2}).$$

Cuando z tiene la forma (2.1.7), la forma polar de su conjugado es

$$\bar{z} = r[\cos(-\theta) + i\,\mathrm{sen}(-\theta)] = re^{-i\theta}. \tag{2.1.10}$$

2.2. El grupo multiplicativo de los complejos sin el cero $\mathbb{C}^*$

Como se mencionó al inicio de este trabajo una estructura algebraica esta conformada por un conjunto y una o varias operaciones para el caso de los complejos el conjunto $\mathbb{C}$ es un grupo con la adición lo mismo que $\mathbb{C}^*$ con la multiplicación.

Definición 2.2.1. [4] Sea G un conjunto con una operación binaria[1]. Se dirá que G es un grupo si y solo si cumple las siguientes propiedades.

1. Clausurativa: si para todo $g_1, g_2 \in G$ se tiene que $g_1 g_2 \in G$.
2. Asociativa: Para todo $g_1, g_2, g_3 \in G$ se tiene que $g_1(g_2 g_3) = (g_1 g_2)g_3$.
3. Modulativa: Existe un unico $e \in g$ tal que para todo $g \in G$ se cumple que $eg = g = ge$; el elemento $e \in G$ se llamara *módulo*.
4. Invertiva: Para todo $g \in G$ exite un $g' \in G$ tal que $g'g = e = gg'$; donde e es el módulo de G y el elemento g' se llamara inverso de g.

Definición 2.2.2. Sea G un grupo, se dirá que es un **grupo abeliano** o **grupo conmutativo** si se cumple la propiedad conmutativa:
Para todo $g_1, g_2 \in G$ se debe cumplir que $g_1 g_2 = g_2 g_1$.

Proposición 2.2.3. *Los complejos sin el cero $\mathbb{C}^*$ forman un grupo abeliano.*

Por lo tanto, sean z_1, z_2 y z_3 complejos cualesquiera no nulos

1. Propiedad asociativa
   Se debe mostrar que $[z_1 z_2]z_3 = z_1[z_2 z_3]$.

$$\begin{aligned}
[z_1 z_2]z_3 &= (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1)(x_3, y_3) \\
&= [(x_1x_2 - y_1y_2)x_3 - (x_1y_2 + x_2y_1)y_3, (x_1x_2 - y_1y_2)y_3 + (x_1y_2 + x_2y_1)x_3)] \\
&= [(x_1x_2x_3 - y_1y_2x_3) - (x_1y_2y_3 + x_2y_1y_3), (x_1x_2y_3 - y_1y_2y_3) + (x_1y_2x_3 + x_2y_1x_3)] \\
&= [(x_2x_3 - y_2y_3)x_1 - (x_2y_3 + x_3y_2)y_1, (x_2x_3 - y_2y_3)y_1 + (x_2y_3 + x_3y_2)x_1)] \\
&= (x_1, y_1)(x_2x_3 - y_2y_3, x_2y_3 + x_3y_2) = z_1[z_2z_3].
\end{aligned}$$

[1] La operación se denota como "·", pero se omitirá entre los elementos para su notación. En algunos textos y para otras operaciones se utilizan otros simbolos.

2. Propiedad conmutativa
   Se debe mostrar que $z_1 z_2 = z_2 z_1$.

$$\begin{aligned} z_1 z_2 &= (x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1) \\ &= (x_2 x_1 - y_1 y_2, y_2 x_1 + y_1 x_2) \\ &= z_2 z_1. \end{aligned}$$

3. Propiedad modulativa
   Debe existir un unico $z_0 \in \mathbb{C}^*$ tal que $z z_0 = z_0 z = z$, donde z_0 se llama módulo de $\mathbb{C}^*$. Existencia: considere $z_0 = (x_0, y_0)$ satisfaciendo la igualdad

$$z_0 z = (x_0 x - y_0 y, x_0 y + x y_0) = z = (x, y)$$

   luego

$$x = x_0 x - y_0 y \tag{2.2.1}$$
$$y = x_0 y + x y_0 \tag{2.2.2}$$

   entonces, de la ecuación (2.2.2) si se supone que $-y_0 y = 0$, se tiene que

$$\begin{aligned} x_0 x &= x \\ x_0 &= 1. \end{aligned} \tag{2.2.3}$$

   Por la ecuación (2.2.2) y (2.2.3) se tiene que

$$\begin{aligned} x y_0 &= 0 \\ y_0 &= 0. \end{aligned} \tag{2.2.4}$$

   Por lo tanto, $z_0 = (1, 0)$. Como ya se mostró que $\mathbb{C}^*$ cumple la ley conmutativa por lo tanto solo es necesario demostrará que existe el módulo para un solo lado.

   Unicidad: Para todo $z = (x, y) \in \mathbb{C}^*$ existe un unico $Z_0 = (1, 0)$ tal que $z_0 z = z z_0 = z$ Se supondra que exite un $z_e = (x_e, y_e)$ donde $z_0 \neq z_e$ tal que $z_0 z = z_e z = z$

$$\begin{aligned} z_0 z &= z_e z \\ (1 + 0i)(x + yi) &= (x_e + y_e i)(x + yi) \\ x + yi &= (x_e x - y_e y) + (x y_e + y x_e) i. \end{aligned} \tag{2.2.5}$$

   donde $x = (x_e x - y_e y)$ y $y = (x y_e + y x_e)$, pero para que las igualdades se cumplan se debe tener que $x_e = 1$ y $y_e = 0$ entonces $z_e = 1 + 0i$ llegando así a una contradicción puesto $z_0 \neq z_e$ por lo tanto $z_0 = z_e$.

4. Propiedad invertiva
   Para cada z no nulo existe un único z', tal que $z z' = z' z = z_0 = (1, 0)$.
   Si $z = a + bi$ es un complejo no nulo se considerará $z' = a' + b'i$ que satisface

$$\begin{aligned} z z' &= (a + bi)(a' + b'i) = (0, 1) \\ &= (a a' - b b') + (a' b + a b') i = (0, 1) \end{aligned} \tag{2.2.6}$$

de donde por la igualdad y una serie de cálculos se obtiene que

$$z' = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i. \tag{2.2.7}$$

así $a' = \frac{a}{a^2+b^2}$ y $b' = -\frac{b}{a^2+b^2}$.

Ahora bien, se ha llegado a ver cómo son los inversos multiplicativos de un complejo cualesquiera. ¿Pero cómo es la forma polar de estos números? Apoyados en (2.1.7) se tiene que si z y z' dos números complejos cualesquiera, expresados en su forma polar por $z = r(\cos\theta + i\,\mathrm{sen}\,\theta)$ y $z' = r'(\cos\theta' + i\,\mathrm{sen}\,\theta')$, entonces

$$\begin{aligned} zz' &= rr'(\cos\theta\cos\theta' - \mathrm{sen}\,\theta\,\mathrm{sen}\,\theta') + i(\mathrm{sen}\,\theta\cos\theta' + \cos\theta\,\mathrm{sen}\,\theta') \\ zz' &= rr'[\cos(\theta+\theta') + i\,\mathrm{sen}(\theta+\theta')] \end{aligned} \tag{2.2.8}$$

De lo anterior, se puede ver que el producto de dos complejos no es más que el complejo cuya argumento es la suma de ángulos o argumentos de los factores y su módulo es el producto de los módulos. Además da sentido a la notación de Euler (2.1.9), la cual no es tan natural como las otras notaciones. Se supondrá que

$$zz' = rr'[\cos(\theta+\theta') + i\,\mathrm{sen}(\theta+\theta')] = (1,0). \tag{2.2.9}$$

De la ecuación anterior se obtiene que:

$$1 = rr'\cos(\theta+\theta') \tag{2.2.10}$$

$$0 = rr'\,\mathrm{sen}(\theta+\theta'). \tag{2.2.11}$$

De las ecuaciones (2.2.10) y (2.2.11) se obtiene que $rr' = 1$ y $\cos(\theta+\theta') = 1$ y $\mathrm{sen}(\theta+\theta') = 0$. Claramente $r \neq 0$ y por lo tanto se concluye que $r' = \frac{1}{r}$ por ser reales, de igual manera para que $\cos(\theta+\theta') = 1$ y $\mathrm{sen}(\theta+\theta') = 0$ se debe cumplir que $\theta + \theta' = (2n)\pi$, para $n = 0, 1, 2, 3, \ldots$.

Gracias a que la función cos y sen son periódicas, cumplen con la condición $\theta' = 2n\pi - \theta$, por lo que

$$\begin{aligned} z' &= r'(\cos\theta' + i\,\mathrm{sen}\,\theta') \\ z' &= \frac{1}{r}[\cos(2n\pi-\theta) + i\,\mathrm{sen}(2n\pi-\theta)]. \end{aligned} \tag{2.2.12}$$

A partir de lo anterior, resulta sencillo establecer la forma del inverso multiplicativo de un número complejo no nulo. En particular

$$z^{-1} = \frac{1}{z} = \frac{1}{r}[\cos(-\theta) + i\,\mathrm{sen}(-\theta)] = \frac{1}{r}(\cos\theta - i\,\mathrm{sen}\,\theta). \tag{2.2.13}$$

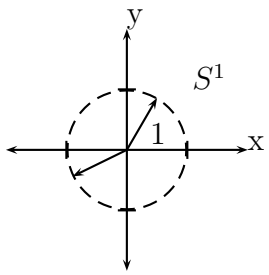
Por todo lo expuesto podemos afirmar que el conjunto de los complejos sin el cero $\mathbb{C}^*$ con la multiplicación tienen estructura de grupo.

2.3. El subgrupo del círculo de radio uno (S^1)

En la sección anterior se afirmó que el conjunto de los complejos sin el cero forman grupo abeliano. En está sección nuestro tema de estudio se centrará en el conjunto correspondiente al círculo de radio uno el cual se notará S^1. Recordemos que

$$S^1 = \{z \in \mathbb{C} \mid |z| = 1\} = \{e^{i\theta} \in \mathbb{C} \mid \theta \in [0, 2\pi]\}. \tag{2.3.1}$$

Lo que geométricamente es equivalente a decir que S^1 está conformado por puntos (x, y) tales que la distancia de ellos al origen es igual a 1, como se observa la gráfica (2.3).



Gráfica 2.3: Representación geométrica de S^1.

Este conjunto es un conjunto no vacío dado que el elemento $z = 1 + 0i = 1$ es un complejo cuya magnitud $|z| = 1$, de igual forma el complejo i es otro elemento de este conjunto. Se aprovechará el siguiente lema para demostrar que el conjuto S^1 es un subgrupo de $\mathbb{C}^*$ sin que sea necesario demostrar todas las propiedades de grupo.

Lema 2.3.1. *Sea G un grupo y H subconjunto de G no vacío, diremos que H es un subgrupo de G si y solo si*

1. *Para todo $g_1, g_2 \in H$ se tiene que $g_1 g_2 \in H$.*
2. *Para todo $g \in H$ exite un $g' \in H$ tal que $g'g = e = gg'$.*

Lo que nos dice el Lema 2.3.1 es que sólo debemos demostrar las propiedades invertiva y clausurativa dado que las demás propiedades se heredan. Para efectos de notación H es subgrupo de G, se notará como $H \leq G$

1. Propiedad clausurativa
   Se tiene que cumplir la premisa que para todo $z_1 = (x_1, y_1), z_2 = (x_2, y_2) \in S^1$.

   $$z_1 \cdot z_2 = z_3 \in S^1.$$

   Para mostrar que efectivamente $z_3 \in S^1$, es más conveniente emplear la forma de *Euler-Moivre* $z = re^{i\theta} = r(\cos\theta + i\,\mathrm{sen}\,\theta)$. De aquí que

   $$(x_1, y_1) \cdot (x_2, y_2) = e^{i\theta_1} \cdot e^{i\theta_2} = e^{i(\theta_1 + \theta_2)} \tag{2.3.2}$$

   donde $\theta_3 = \theta + 2\pi$ como $\theta_2 < 2\pi$ entonces $\theta_1 + \theta_2 = \theta_3$.

2. Propiedad invertiva
   Sea $w = e^{i\theta} \in S^1$ existe un $w^{-1} \in S^1$ tal que $w \cdot w^{-1} = 1$. De la ecuación (2.2.8) podemos establecer que existe w^{-1} de la forma $e^{i(2\pi-\theta)}$ se deberá garantizar que $w^{-1} \in S^1$.

   $$w \cdot w^{-1} = e^{i\theta} \cdot e^{i\theta'} = e^{i(\theta+\theta')} = 1 \tag{2.3.3}$$

   donde $\theta + \theta' \in [0,\, 2\pi]$, por lo tanto

   $$\theta' = -\theta \quad \text{ó} \quad \theta' = 2\pi - \theta, \tag{2.3.4}$$

   es decir, θ será el inverso aditivo del ángulo ó lo que le falte a dicho ángulo para ser igual a 2π y se concluye entonces que $w^{-1} \in S^1$.

2.4. Otros subgrupos de $\mathbb{C}^*$

A continuación se revisarán otros subgrupos $\mathbb{C}^*$, algunos de ellos muy conocidos y utilizados comunmente en diferentes ramas de la matemática.

Son conocidos el grupo de $\mathbb{R}^*$ y el grupo $\mathbb{Q}^*$, estos son subgrupos de $\mathbb{C}^*$. También el grupo los reales positivos $\mathbb{R}^+$ es un subgrupo del grupo multiplicativo de los reales no nulos y por consiguiente de $\mathbb{C}^*$.

Dentro de los subgrupos de $\mathbb{C}^*$, encontramos también subgrupos finitos interesantes, con los cuales se puede construir otros subgrupos infinitos. Por ejemplo, sea $A = \{1, -1, -i, i\}$ este conjunto de elementos de $\mathbb{C}^*$ forma un subgrupo con la multiplicación, que se muestra en la siguiente tabla.

*	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

Tabla 2.1: Tabla del grupo A

En la tabla se puede observar que el subgrupo cumple con ser clausurativo y además todo elemento tiene su inverso. Pero este subgrupo tiene una estructura diferente puesto que al tomar el elemento i de A y multiplicarlo varias veces, se obtienen todos los elementos del grupo $\{i,\ i^2 = -1,\ i^3 = -i,\ i^4 = 1\}$, ésto no sucede con todos los elementos del conjunto, esta nueva estructura nos da cabida a la siguiente definición.

Definición 2.4.1. [2] En un grupo G donde exista un elemento a del grupo G, tal que todo elemento de G puede ser expresado como una potencia de a, será llamado un ***grupo cíclico***. Si la operación del grupo se denota aditivamente, se dirá que todo elemento de G

se puede expresar como na, para n entero. El elemento a se llamará ***generador*** de G y se denotará $G =< a >$.

En el anterior ejemplo i es un generador de A, también $-i$. No son cíclicos los grupos $\mathbb{R}$, $\mathbb{Q}$ ni $\mathbb{Q}^*$, ni $\mathbb{Q}^+$ pues no tienen generador. El grupo $\mathbb{Z}$ los enteros es generado por el 1 y por tanto es cíclico.
El siguiente resultado es muy conocido su demostración aunque sencilla se deja para ser tratada cuando se profundeice en el concepto de isomorfismo (ver Página 29).

Proposición 2.4.2. *Un grupo cíclico infinito es esencialmente igual al grupo aditivo de los enteros. Un grupo cíclico que tiene n elementos es esencialmente igual a un grupo $\mathbb{Z}_n$ que es el grupo de los residuos módulo n con la adición.*

Así, quedan clasificados todos los grupos cíclicos, En el transcurso de este trabajo se verá que todos estos grupos se encuentran inmersos en $\mathbb{C}^*$.

Definición 2.4.3. El número de veces que se debe operar un elemento del grupo para obtener el módulo se conoce como el ***orden*** del elemento. Es decir el orden de x es el menor entero positivo n tal que $x^n = 1$ (o en notación aditiva $nx = 0$). Cuando no existe dicho n, x es de ***orden infinito***.

En el ejemplo anterior el orden de i es 4, pero el orden de -1 es 2. En $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{R}^+$ el orden de cualquier elemento no nulo es infinito. En $\mathbb{R}^*$ todos los elementos son de orden infinito salvo 1 y -1.

Ejemplo 2.4.4. Si tomamos cada elemento de este conjunto $1, -1, i, -i$ y lo multiplicamos por cada $x \in \mathbb{R}^+$ tendremos el siguiente conjunto:

$$E = \{z = (x, y) \in \mathbb{C}^* | x = 0 \quad \vee \quad y = 0\}.$$

este nuevo conjunto, es no vacío pues el conjunto A, definido anteriormente está contenido en él. La representación geométrica de este conjunto son los ejes del plano complejo sin el elemento cero. Se comprobará entonces que este conjunto es un subgrupo de $\mathbb{C}^*$. Como ya se mencionó es un conjunto no vacío por lo tanto solo se debe mostrar la clausura del conjunto y los inversos. Por lo tanto si $z_1 = (x_1, y_1)$, $z_2 = (x_2, y_2) \in E$ se debe cumplir que.

$$z_1 z_2 = (x_1, y_1)(x_2, y_2) = (x_1x_2 - y_1y_2,\ x_1y_2 + x_2y_1) \in E. \tag{2.4.1}$$

Dado que el cero es una de las dos componentes de cada una de las parejas del conjunto E, se observará el caso particular en que $y_2 = 0$ y $x_1 = 0$ por lo tanto

$$(x_1x_2 - y_1y_2,\ x_1y_2 + x_2y_1) = (0,\ x_2y_1) in E. \tag{2.4.2}$$

De forma análoga sucede para las demás posibilidades.
Ahora debemos mostrar que todo elemento de E tiene inverso multiplicativo. Los elementos del conjunto E tiene dos formas posibles $z \in E$ es de la forma $\pm x + 0i$ o $0 \pm yi$ por medio de una serie calculos se obtiene que los inversos multiplicativos serán para la forma $z = \pm x + 0i$ se tiene que $z^{-1} = \pm\frac{1}{x} + 0i$ y para los de la forma $z = 0 \pm yi$ se llega a ver que $z^{-1} = 0 \mp \frac{1}{y}i$.
Otra manera de demostrar esto es expresando los elementos del conjunto E en la notación

de Euler; se tendrá que $E = \{re^{i\theta} \in \mathbb{C}^* | \theta = n\pi/2\}$ con $n \in \mathbb{Z}$, en virtud de (2.3.4) se sabe que la forma de los inversos de un número complejo $z = re^{i\theta}$ será $z^{-1} = \frac{1}{r}e^{i(-\theta)}$ por lo tanto cada elemento que se tome $z \in E$ de la forma $z = re^{i\theta}$ donde $\theta = n\pi/2$ se llega a ver que $z^{-1} = \frac{1}{r}e^{i\theta'}$ donde $\theta' = \frac{(4-n)\pi}{2}$, concluyendo que $z^{-1} \in E$.
Se ha demostrado que E es un subgrupo de $\mathbb{C}^*$ que no es finito y no tiene un elemento generador.

Ejemplo 2.4.5. Sea $\mathbb{Q}[\sqrt{2}] = \{z = a + b\sqrt{2}i \in \mathbb{C}^* | a, b \in \mathbb{Q}\}$, este conjunto también es un subgrupo de $\mathbb{C}^*$ que cumple con la clausura y la propiedad invertiva. Si $z_1 = a + b\sqrt{2}$ y $z_2 = c + d\sqrt{2}$ se define:

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2db) + (ad + bc)\sqrt{2}. \tag{2.4.3}$$

donde $(ac + 2db), (ad + bc) \in \mathbb{Q}$ por ser la suma de racionales clausurativa. Si para todo $a + b\sqrt{2}$ donde $a, b \in \mathbb{Q}$ no nulos, se tiene que sus inversos multiplicativos son de la forma $\frac{-a}{2b^2-a^2} + \frac{b}{2b^2-a^2}\sqrt{2}i$; por lo tanto podemos afirmar que este conjunto es un subgrupo de $\mathbb{C}^*$.

2.4.1. Potencias de números complejos

Como ya se mencionó veremos como el grupo $\mathbb{C}^*$ es un grupo divisible, esto quiere decir que todo elemento tiene raíces de cualquier orden. Como se vio el producto de complejos es la suma de los argumentos y el producto de sus módulos, por lo que, si $z_i = r_i(\cos\theta_i + i\,\mathrm{sen}\,\theta_i)$ entonces,

$$z_1 z_2 \ldots z_n = r_1 r_2 \ldots r_n \left[\cos(\theta_1 + \theta_2 + \ldots + \theta_n) + i\,\mathrm{sen}(\theta_1 + \theta_2 + \ldots + \theta_n)\right].$$

Si, $z = r(\cos\theta + i\,\mathrm{sen}\,\theta)$ y n es un entero positivo, entonces

$$z^n = r^n(\cos n\theta + i\,\mathrm{sen}\,n\theta). \tag{2.4.4}$$

Cuando $r = 1$, esta fórmula se reduce al teorema De Moivre para exponentes enteros positivos.

$$(\cos\theta + i\,\mathrm{sen}\,\theta)^n = \cos n\theta + i\,\mathrm{sen}\,n\theta. \tag{2.4.5}$$

De la ecuación (2.4.5), es natural preguntar por $z^{-n} = \frac{1}{z^n}$ y teniendo en cuenta la ecuación (2.2.8), $\frac{1}{z} = \frac{1}{r}(\cos\theta - i\,\mathrm{sen}\,\theta)$, se obtiene que:

$$z^{-n} = \frac{1}{z^n} = \frac{1}{r^n}\left[\cos(-n\theta) + i\,\mathrm{sen}(-n\theta)\right] = \left(\frac{1}{z}\right)^n. \tag{2.4.6}$$

2.4.2. Extracción de raíces

El problema de extraer la n-esima raíz de un número complejo z se reduce a resolver la ecuación

$$w^n = z, \tag{2.4.7}$$

donde n es un entero positivo. Se considerará a z y w en su forma polar denotados por

$$z = r(cos\theta + i\,\mathrm{sen}\,\theta) \quad w = s(cos\psi + i\,\mathrm{sen}\,\psi),$$

encontrar entonces la raíz de z se reduce a encontrar los valores de s y ψ.

De la ecuación(2.4.4) se sabe que

$$s^n(\cos n\psi + i\,\mathrm{sen}\,n\psi) = r(cos\theta + i\,\mathrm{sen}\,\theta), \tag{2.4.8}$$

se tiene que

$$s^n = r, \qquad n\psi = \theta \pm 2\pi K \tag{2.4.9}$$

donde n es un número entero positivo cualquiera. Como r y s son números positivos, s debe ser la raíz n-enésima real positiva de r. Entonces existen n ángulos ψ tal que:

$$n\psi = \theta \qquad \psi_k = \theta \pm 2\pi k/n \tag{2.4.10}$$

estos valores de ψ dan un mismo valor de w para dos enteros k cualesquiera que no difieran entre sí de un múltiplo de n. Por lo tanto, existen exactamente n soluciones distintas de la Ecuación (2.4.7) cuando $z \neq 0$ a saber

$$w = \sqrt[n]{r}\left(\cos\frac{\theta + 2k\pi}{n} + i\,\mathrm{sen}\,\frac{\theta + 2k\pi}{n}\right), \tag{2.4.11}$$

donde $k = 0, 1, 2, \ldots, n-1$. Son estos los n valores de de $z^{\frac{1}{n}}$.

Geométricamente, la longitud de cada uno de los n vectores $z^{\frac{1}{n}}$ es el número positivo $\sqrt[n]{r}$. El argumento de uno de estos vectores es el ángulo obtenido al dividir a θ por n y los demás argumentos son obtenidos por la adición de múltiplos de $2\pi/n$ a θ/n. Cuando $z = 0$, la Ecuación (2.4.7) tiene una única solución $w = 0$, por lo tanto $w^{1/n} = 0$.

2.4.3. El grupo $\mathbb{C}_n$ las raices n-ésimas de la unidad

Como se estableció en la sección anterior las raíces de la un número complejo son

$$w = \sqrt[n]{r}(\cos\frac{\theta + 2k\pi}{n} + i\,\mathrm{sen}\,\frac{\theta + 2k\pi}{n}), \tag{2.4.12}$$

donde $k = 0, 1, 2, \ldots, n-1$. Son estos los n valores de $z^{\frac{1}{n}}$. Es decir las raices n-ésimas de un número complejo ahora bien en esta sección se estudiará el grupo de las raices n-ésimas de la unidad. Iniciaremos entonces por conocer el conjunto de las raíces de uno.

Ahora bien. como $1 = \cos 0 + i\,\mathrm{sen}\,0$, entonces las raíces n-ésimas de 1 se pueden escribir como

$$1^{1/n} = \cos\frac{2\pi k}{n} + i\,\mathrm{sen}\,\frac{2\pi k}{n} \qquad (k = 0, 1, 2, \ldots, n-1). \tag{2.4.13}$$

En particular, cuando $k = 1$, la raíz correspondiente se denota ω

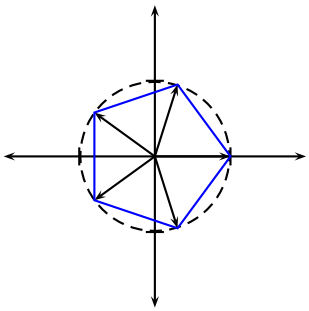
$$\omega = \cos\frac{2\pi}{n} + i\,\mathrm{sen}\,\frac{2\pi}{n} \tag{2.4.14}$$

Teniendo en cuenta el teorema De Moivre (2.4.5), las raíces de (2.4.7) son

$$1, \omega, \omega^2, \ldots, \omega^{n-1}. \tag{2.4.15}$$

En el plano complejo, estas raíces son los vértices del polígono regular de n lados inscrito en el círculo de radio uno.

Ejemplo 2.4.6. La solución de la ecuación $u^5 - 1 = 0$ son el conjunto de puntos en el plano $\{(\cos 0, \mathrm{sen}\, 0),\ (\cos\frac{2\pi}{5}, \mathrm{sen}\,\frac{2\pi}{5}),\ (\cos\frac{4\pi}{5}, \mathrm{sen}\,\frac{4\pi}{5}),\ (\cos\frac{6\pi}{5}, \mathrm{sen}\,\frac{6\pi}{5}),\ (\cos\frac{8\pi}{5}, \mathrm{sen}\,\frac{8\pi}{5})\}$. Como se ve en la figura siguiente:



Gráfica 2.4: Grafica de las soluciones de $u^5 - 1 = 0$

Este conjunto de puntos define un pentágono cuyas aristas tienen longitud uno.

Si z_1 es una raíz n-ésima cualquiera de z, entonces

$$z_1, z_1\omega, z_1\omega^2, \ldots, z_1\omega^k, \ldots z_1\omega^{n-1} \tag{2.4.16}$$

son las n raíces de z, puesto que multiplicar z_1 por ω^k corresponde a aumentar $2k\pi/n$ el argumento de z_1.

Definición 2.4.7. $\mathbb{C}_n = \{z \in \mathbb{C} \mid z^n = 1\}$ con $n \in \mathbb{N}$ el conjunto de las raices n-ésimas de uno.

Este subconjunto de $\mathbb{C}$ es no vacío como se mostró anteriormente, se verá que cumple con las condiciones para ser subgrupo.
Para esto consideraremos $z_1, z_2 \in \mathbb{C}_n$ se debe ver que $z_1.z_2 = z_3 \in \mathbb{C}_n$ pero $z_2 = \cos\frac{2\pi k}{n} + i\,\mathrm{sen}\,\frac{2\pi k}{n}$ con $(k = 0, 1, 2, \ldots, m-1)$ y $z_1 = \cos\frac{2\pi k}{m} + i\,\mathrm{sen}\,\frac{2\pi k}{m}$ con $(k = 0, 1, 2, \ldots, m-1)$. Entonces se tiene que

$$\begin{aligned} z_1.z_2 &= [\cos\frac{2\pi k}{n} + i\,\mathrm{sen}\,\frac{2\pi k}{n}][\cos\frac{2\pi k}{m} + i\,\mathrm{sen}\,\frac{2\pi k}{m}] \\ &= \cos\frac{2\pi k(m+n)}{mn} + i\,\mathrm{sen}\,\frac{2\pi k(m+n)}{mn} \end{aligned} \tag{2.4.17}$$

como $k(m+n), nm \in \mathbb{N}$ se tiene que:

$$z_1.z_2 = \cos\frac{2\pi k'}{s} + i\,\text{sen}\,\frac{2\pi k'}{s} = z_3$$

por lo tanto $z_3 \in \mathbb{C}_n$.
Es claro que el inverso multiplicativo de un elemento de $\mathbb{C}_n$ está en el grupo puesto que si z' es el inverso multiplicativo $z.z' = 1$ entonces $(z.z')^n = (1)^n = 1$ dado que $z^n.(z')^n = 1$ entonces $(z')^n = 1$. Es decir el inverso multiplicativo de un número z tiene el mismo orden de z.

2.5. $\mathbb{C}^*$ como grupo divisible

Cuando dos grupos son isomorfos tiene las mismas propiedades. En este caso los dos grupos ($\mathbb{C}^*$ y S^1) son conmutativos pero esto no es suficiente para poder decir que los grupos son isomorfos; para demostrar que dos grupos son isomorfos a veces es fácil encontrar el isomorfismo entre los grupos (ver la Definición 1.0.1), para demostrar en cambio que dos grupos no son isomorfos resulta muy complicado mostrar que no existe un isomorfismo entre los conjuntos, por esto lo que se suele hacer es establecer una propiedad estructural que no cumpla alguno de los dos conjuntos y el otro sí.
Hasta el momento se han estudiado diferentes propiedades estructurales que ambos grupos han cumplido satisfactoriamente, ahora estudiaremos otra de estas propiedades con la que se desarrolla la demostración clásica del isomorfismo de los complejos sin cero y el círculo de radio uno ($\mathbb{C}^* \cong S^1$).

Definición 2.5.1. Un grupo es divisible o con división si la ecuación $x^n = g$ (en notación aditiva $n.x = g$) tiene solución en el grupo siendo n entero positivo y $g \in G$.

La divisibilidad del grupo multiplicativo de los números complejos puede expresarse como la existencia de las raíces n-ésimas de cualquier elemento, es decir, se puede resolver la ecuación $z^n - u = 0$ para todo $u \in S^1$. Pero antes de analizar al grupo de los complejos sin el cero como grupo divisible, se presentaràn ejemplos de algunos grupos divisibles.
Los grupos $\mathbb{Q}$ y $\mathbb{R}$ son grupos con división, desde bachillerato sabemos que para cualquier g que pertenezca a los grupos mencionados, y $n \in \mathbb{Z}^+$ existe un único x tal que $nx = g$.
$\mathbb{R}^+$ no es un grupo divisible. Dado que la ecuación $x^2 = 2$ no tiene solución en el grupo.

En la sección (2.4) se analizaron algunos subgrupos de $\mathbb{C}^*$. De estos subgrupos podemos decir que $A = \{1, -1, -i, i\}$, no es un grupo con división dado que la ecuación $x^2 = -i$ no tiene solución en el grupo.

Definición 2.5.2. Sea G un grupo aditivo, y sea n un número natural cualquiera, entonces $nG := \{ng \mid g \in G\}$ con $n \in \mathbb{Z}^+$. Si G es un grupo multiplicativo entonces $G^n := \{g^n \mid g \in G\}$ con $n \in \mathbb{Z}^+$.

Proposición 2.5.3. *G es disivible si y solo si $G = pG$ para todo primo p.*

Demostración. (Se utilizará notación aditiva)

1. Supongamos que G es divisible: claramente, pG está contenido siempre en G dado que G es divisible; sea g un elemento cualquiera de G y sea p un primo cualquiera entonces existe un elemento $b \in G$ tal que $g = pb$; como $pb \in pG$, tenemos que g está en pG, por lo tanto $G \subset pG$, entonces $G = pG$.

2. Supongamos ahora que $G = pG$ para todo primo p; sean $g \in G$ y $n \in \mathbb{N}$ si $n = 1$ se cumple puesto $1.x = x = g$. Ahora bien cuando $n \neq 1$ se puede expresar a n como $n = p_1 p_2 \dots p_r$, con $p_1 \dots p_r$ primos (no necesariamente distintos), así que:

$$\begin{gathered} \textit{existe } b_1 \in G \textit{ tal que } g = p_1 b_1, \textit{ pues } G = p_1 G; \\ \textit{existe } b_2 \in G \textit{ tal que } b_1 = p_2 b_2, \textit{ pues } G = p_2 G; \\ \vdots \qquad\qquad \vdots \qquad\qquad \vdots \\ \textit{existe } b_r \in G \textit{ tal que } b_(r-1) = p_r b_r, \textit{ pues } G = p_r G, \end{gathered}$$

   de lo anterior podemos escribir $g = p_1 b_1 = p_1 p_2 b_2 = \dots = p_1 p_2 \dots p_r b_r = n b_r$ entonces $g = n b_r$ pero esta es la definición de grupo divisible.

■

El grupo $\mathbb{C}$ es un grupo divisible puesto que todo elemento posee raíz, como se vio detalladamente en el (2.4.11) y se mostró la solución a la ecuación $w^n = z$ donde $n \in \mathbb{N}$ y $z \in \mathbb{C}$, además en (2.4.16) se mostro que toda raíz compleja puede expresarse en función de la raíz de la unidad por lo tanto $\mathbb{C}^*$ es un grupo con división.

Lema 2.5.4. *Si mcd$(m, n) = 1$, para todo $x \in \mathbb{Z}_n$ existe un $y \in \mathbb{Z}_n$ tal que $my = x$.*

Demostración. Como $\text{mcd}(m, n) = 1$ entonces se tiene que existen $\alpha, \beta \in \mathbb{Z}$ tal que $1 = \alpha m + \beta n$ lo que implica que

$$\alpha m \equiv 1g \pmod{n}$$

entonces haciendo $y \equiv \alpha x \pmod{n}$ se tiene que y cumple que $my \equiv x \pmod{n}$. ■

2.5.1. El Subgrupo $\mathbb{C}_{p^\infty}$

Nótese que $\{1\} \subseteq \mathbb{C}_p \subseteq \mathbb{C}_{p^2} \subseteq \mathbb{C}_{p^3} \subseteq \dots \subseteq S^1$ así se deduce fácilmente que $\mathbb{C}_p \cup \mathbb{C}_{p^2} \cup \mathbb{C}_{p^3} \cup \dots$ es grupo y cuando p es primo se notará $\mathbb{C}_{p^\infty}$ y de ahì se tiene otro subgrupo de $\mathbb{C}^*$ incluido en S^1:

$$\mathbb{C}_{p^\infty} = \{z \in \mathbb{C}^* \mid \exists n \in \mathbb{N}, \quad z^{p^n} = 1\},$$

es decir, $\mathbb{C}_{p^\infty}$ comprende todos aquellos complejos cuyo orden es una potencia de p.
Primero se ilustrará que $\mathbb{C}_{p^\infty}$ es un grupo divisible. Enseguida se demostrará que en efecto es divisible[2].

Ejemplo 2.5.5. Sea $i \in \mathbb{C}_{2^\infty}$. La ecuación $z^3 = i$ tiene tres soluciones en $\mathbb{C}^*$ son ellas $\frac{1}{2}(i + \sqrt{3})$, $\frac{1}{2}(i - \sqrt{3})$ y $-i$. Sólo $-i \in \mathbb{C}_{2^\infty}$, es decir $z = -i$ es la solución en $\mathbb{C}_{2^\infty}$ ya que $(-i)^{2^2} = 1$. También $e^{i\pi/4} \in \mathbb{C}_{2^\infty}$. La ecuación $z^3 = e^{i\pi/4}$ tiene tres soluciones en $\mathbb{C}^*$ las cuales son [3] $-0{,}7071 + 0{,}7071i$, $-0{,}2588 - 0{,}9659i$ y $0{,}9659i + 0{,}2588$ de estas solo $-0{,}7071 + 0{,}7071i \in \mathbb{C}_{2^\infty}$, es decir $z = e^{i3\pi/4}$ es la solución en $\mathbb{C}_{2^\infty}$ dado que $(e^{i3\pi/4})^{2^3} = 1$.

[2] Si p no es primo $\mathbb{C}_{p^\infty}$ es un grupo pero no se puede garantizar que sea un grupo divisible

[3] Estas han sido calculadas con Matlab, naturalmente son aproximadas.

Lema 2.5.6. *Sea p un número primo, se tiene que $(\mathbb{C}_{p^n})^p = \mathbb{C}_{p^{n-1}}$.*

Demostración. Es evidente que $(\mathbb{C}_{p^n})^p \supseteq \mathbb{C}_{p^{n-1}}$ entonces solo se debe ver la otra contenencia $(\mathbb{C}_{p^n})^p \subseteq \mathbb{C}_{p^{n-1}}$. Como $\mathbb{C}_{p^n}$ esta compuesto por todos aquellos complejos con orden $1, p, p^2, p^3, \ldots, p^n$ al tomar $x \in \mathbb{C}_{p^n}$ por definición $x^{p^k} = 1$ para $0 \leq k \leq n$ y por tanto $(x^p)^{p^{k-1}} = 1$ por tanto x^p es un elemento de orden $1, p, p^2, p^3, \ldots, p^{n-1}$ y se tiene $(\mathbb{C}_{p^n})^p = \mathbb{C}_{p^{n-1}}$. ■

Teorema 2.5.7. *El grupo $\mathbb{C}_{p^\infty}$ es divisible.*

Demostración. Por el lema 2.5.4 es fácil ver que la ecuación $x^n = y$ tiene solución para todo $y \in \mathbb{C}_{p^\infty}$ si $\text{mcd}(n, p) = 1$; se tiene entonces que $(\mathbb{C}_{p^\infty})^q = \mathbb{C}_{p^\infty}$ si q es un primo diferente de p. Para aplicar la Proposición 2.5.3 falta demostrar que $(\mathbb{C}_{p^\infty})^p = \mathbb{C}_{p^\infty}$; puesto que: $(\mathbb{C}_{p^\infty})^p = \{1\}^p \cup (\mathbb{C}_p)^p \cup (\mathbb{C}_{p^2})^p \cup (\mathbb{C}_{p^3})^p \cup \ldots$ pero por el lema anterior sabemos que $(\mathbb{C}_{p^n})^p = \mathbb{C}_{p^{n-1}}$ entonces se tiene que $(\mathbb{C}_{p^\infty})^p = \mathbb{C}_{p^\infty}$. Se ha visto que para todo primo q es cierto $(\mathbb{C}_{p^\infty})^q = \mathbb{C}_{p^\infty}$. ■

CAPÍTULO 3

ORDEN Y ELECCIÓN

Como se mencionó en la introducción se utilizarán diferentes elementos de las matemáticas para la demostración del isomorfismo entre $\mathbb{C}^* \cong S^1$. Hasta este momento se ha realizado un recorrido por los dos grupos multiplicativos en estudio y algunos otros temas fundamentales para el desarrollo de este trabajo. En este capítulo se abordará, de forma más detallada las relaciones de orden y de equivalencia; además se conocerá de forma detallada el axioma de elección el cual es de gran utilidad en las diferentes ramas de la matemàtica.

3.1. Relaciones y Propiedades

Para iniciar el estudio de las relaciones de orden se procederà primero a estudiar qué es una relación. Está se entenderá como un subconjunto del producto cartesiano.
Sea $\mathcal{R}$ la relación establecida de un conjunto A en si mismo, se analizarán ciertas propiedades de las relaciones. Si $(x, y) \in \mathcal{R}$ se notará $x\mathcal{R}y$.

Definición 3.1.1. Una relación $\mathcal{R}$ definida en un conjunto A, se llamará ***reflexiva*** en A, si todo elemento de A está relacionado mediante ella consigo mismo. Es decir:

$$\forall a \in A \; a\mathcal{R}a.$$

Definición 3.1.2. Una relación $\mathcal{R}$ definida en un conjunto A, se llama ***simétrica*** si cada vez que un elemento está relacionado con otro, también el segundo lo está con el primero. Es decir:

$$(\forall a,\, b \in A)(a\mathcal{R}b \;\Rightarrow\; b\mathcal{R}a).$$

Definición 3.1.3. Una relación $\mathcal{R}$ en un conjunto A, se llamará antisimétrica si y solo si cuando $x \neq y$, no se puede tener simultáneamente $x\mathcal{R}y$ y $y\mathcal{R}x$, o sea, si

$$x\mathcal{R}y \text{ y } y\mathcal{R}x \text{ entonces } x = y.$$

Definición 3.1.4. Una relación $\mathcal{R}$ sobre un conjunto A se llama transitiva, si cada vez que un elemento esté relacionado mediante ella con un segundo y éste a su vez lo esté con un

tercero, entonces también el primero está relacionado con el tercero, es decir,

$$(\forall x,\, y,\, z \in A)(x\mathcal{R}y \text{ y } y\mathcal{R}z) \rightarrow x\mathcal{R}z.$$

Algunas operaciones binarias establecen relaciones conocidas como lo son la contenencia de conjuntos, el paralelismo de rectas de un mismo plano, entre otras. Algunas de estas relaciones cumplen con propiedades que otras no, por ejemplo, la relación de paralelismo de rectas de un mismo plano es reflexiva, simétrica y transitiva; mientras que la contenencia de conjuntos es reflexiva, antisimétrica y transitiva; se distinguen dos tipos de relaciones importantes *las relaciones de equivalencia* y *las relaciones de orden.*

Definición 3.1.5. Una relación se llama de equivalencia en un conjunto A si es reflexiva, simétrica y transitiva.

Este tipo de relaciones son muy importantes dado que estas establecen las clases de equivalencia de un conjunto con respecto a la relación, las cuales son de gran importancia y serán tema de estudio en forma particular en los grupos en este trabajo en la Sección 4.2.

Ejemplo 3.1.6. La relación "ser paralelo a"en el conjunto de rectas de un mismo plano, es una relación de equivalencia puesto que es simétrica, reflexiva y transitiva.

Ejemplo 3.1.7. La relación $a \equiv b \pmod{m}$ la cual se define como:

$$a \equiv b \pmod{m} \text{ si } a \text{ y } b \text{ tiene el mismo residuo al dividirse por } m.$$

Se mostrará que esta relación es de equivalencia. Dado cualquier a se tiene que $a \equiv a \pmod{m}$ puesto que a deja el mismo residuo al dividirse por m. Si $a \equiv b \pmod{m}$ implica por definición de congruencia que a y b dejan el mismo residuo al dividirse m pero $b \equiv a \pmod{m}$ puesto que dejan el mismo residuo al dividirse por m. Sea $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m}$ entonces por la propiedad anterior se tiene que $c \equiv b \pmod{m}$ por lo tanton por transistividad se puede asegurar que $a \equiv c \pmod{m}$ y esto se obtine porque tanto a y c dejan el mismo residuo al dividirse por m. Esta relación es llamada también ***relación de congruencia***.

Proposición 3.1.8. *Toda relación de equivalencia $\mathcal{R}$ sobre un conjunto X no vacío, genera una partición sobre el conjunto X que se nota, $X/\mathcal{R}$ y está formada por todas las clases de equivalencia es decir:*

$$X/\mathcal{R} = \{[a]\}_{a \in X}$$

*en donde $[a] = \{x \in X \mid x\mathcal{R}a\}$ es la **clase de equivalencia** de a para cada $a \in X$.*

Demostración. Se probará que $X/\mathcal{R}$ es una partición. Como cada elemento de $X/\mathcal{R}$ es subconjunto de X entonces la $\bigcup X/\mathcal{R} \subset X$, ahora bien, $a \in [a]$ porque $a\mathcal{R}a$ entonces $a \in \bigcup X/\mathcal{R}$ concluyendo que $\bigcup X/\mathcal{R} = X$.
Sean $[a], [b] \in X/\mathcal{R}$ con $[a] \neq [b]$. Si exite un c tal que $c \in [a] \cap [b]$, se tendría que $c\mathcal{R}a$ y $c\mathcal{R}b$ pero por simetría y transitividad de $\mathcal{R}$ se tiene que $a\mathcal{R}b$. Luego si $x \in [a]$ entonces por transitividad de $\mathcal{R}$ se tiene que $x\mathcal{R}b$ por lo tanto $x \in [b]$, de forma análoga sucede con los elementos que se encuentran en la clase de equivalencia de b; entonces $[a] = [b]$. Se ha llegado a una contradicción puesto que $[a] \neq [b]$ entonces podemos concluir que si $[a] \neq [b]$ entonces $[a]$ y $[b]$ son disyuntos. Se concluye que $X/\mathcal{R}$ es una partición de X. ■

Definición 3.1.9. Una relación $\mathcal{R}$ se llama de orden en un conjunto A si ella es reflexiva, antisimétrica y transitiva. Se acostumbra a decir que A es un conjunto ordenado por $\mathcal{R}$.

Para las relaciones de orden usaremos $(\preccurlyeq)$ en vez de $\mathcal{R}$. Los conjuntos que cumplen con todas las propiedades de relación de orden también se les conoce como ***conjuntos parcialmente ordenados*** o ***POSET*** [1].

Ejemplo 3.1.10. Sea $\mathbb{N}$ el conjunto de los naturales, con la relación "menor o igual" $\leq$, esta relación es de orden en $\mathbb{N}$.

Definición 3.1.11. Es $x, y \in A$ y $y \preccurlyeq x$ ó $x \preccurlyeq y$ se dice que x e y son ***comparables***.

Ahora bien si cada par de elementos de A son comparables, se dice que $\leq$ es un ***orden total***; o sea, si $(\forall x, y \in A)(y \preccurlyeq x \ o \ x \preccurlyeq y)$. Se ve inmediatamente que los órdenes en los conjuntos de los naturales, enteros, racionales y reales son todos órdenes en el anterior sentido, pero no son sólo conjuntos parcialmente ordenados sino también órdenes totales. A este orden se le llama ***orden lineal*** o ***cadena***. Mientras que muchos órdenes clásicos son lineales, el determinado por la contenencia de conjuntos proporciona un ejemplo donde éste no es el caso. Dehecho, muchas propiedades avanzadas de los conjuntos ordenados son interesantes principalmente para un orden no lineal.

Definición 3.1.12. Sea $\preccurlyeq$ una relación de orden en A y sea B un subconjunto no vacío de A. Un elemento a de A (único) se llama *el primero, ó mínimo* de B si

1. $a \in B$,
2. $\forall b \in B \quad a \preccurlyeq b$ (a es menor que b) y si $b \preccurlyeq a$ (b es menor que a) se tiene que cumplir que $a = b$.

Definición 3.1.13. Sea A ordenado por $\preccurlyeq$ y sea B un subconjunto no vacío de A. Se dice que un elemento u de A (único) es el *último, el mayor o el máximo* de B si

1. $u \in B$,
2. $\forall x \in B \quad x \preccurlyeq u$ y si $u \preccurlyeq x$ se debe cumplir que $x = u$.

Ejemplo 3.1.14. Un ejemplo muy familiar son las letras del alfabeto en el cual el primer elemento es la letra a y el máximo es la z. Otro ejemplo familiar es el conjunto de los números naturales el cual posee un primer elemento, el número 1 pero no posee un elemento máximo.

Definición 3.1.15. Sea $\preccurlyeq$ una relación de orden en A, y B un subconjunto de A. Una ***cota inferior*** de B es cualquier elemento m de A tal que $(\forall x \in B)(m \preccurlyeq x)$. Una ***cota superior*** de B es cualquier elemento s de A tal que $(\forall x \in B)(x \preccurlyeq s)$.

Definición 3.1.16. Sea A un conjunto ordenado por $\preccurlyeq$ y B un subconjunto no vacío de A. Se dice que M es un elemento **maximal** de B si

1. $M \in B$.
2. $\forall x \in B \quad (M \preccurlyeq x \Rightarrow M = x)$.

Ejemplo 3.1.17. Por ejemplo el subconjunto $(0, 1]$ de $\mathbb{R}$ y la relación "menor o igual" $\leq$ el elemento 1 es el elemento maximal del conjunto.

[1] Abreviatura inglesa de Conjunto Parcialmente Ordenado (partially ordered set).

De forma análoga se define minimal de B: si $m \in B$ y $\forall x \in B \quad x \preccurlyeq m \Rightarrow x = m$.

Ejemplo 3.1.18. Para el ejemplo anterior el conjunto tenía elemento maximal pero no tiene elemento minimal.

Ejemplo 3.1.19. Si se toma $(0, 1)$ este conjunto con la relación $\leq$ no tiene elementos maximal ni minimal.

Ejemplo 3.1.20. Sea $\mathcal{P}(A)$ el conjunto de todos los subconjuntos de A (A un conjunto finito) entonces si se toma $\mathcal{P}(A) - A$ con la inclución de conjuntos como relación este conjunto tiene elemento minimal ϕ, el conjunto vacío, pero tiene muchos elementos maximales. Supongamos que $|A| = n$ donde $n \in \mathbb{N}$, entonces $\mathcal{P}(A) - A$ esta conformado por todos aquellos subconjuntos de A con cardinal menor o igual a $n - 1$, por lo tanto todo subconjunto que posea cardinal igual a $n - 1$ es un conjunto maximal.

Ejemplo 3.1.21. Sea X un conjunto y sea $\mathcal{P}_q(X) = \{Y \subseteq X \,|\, |Y| = q\}$ con $q \in \mathbb{N}$, es decir Y es finito; con la relación de contenencia; este conjunto no tiene maximales pero sí tiene minimal el conjunto vacío ϕ.

Se puede concluir entonces que si a es el elemento mínimo o primer elemento de A, entonces a es un elemento minimal de A y es único. Asimismo, un último elemento de A es un elemento maximal de A y es único.

Definición 3.1.22. Sea $\preccurlyeq$ una relación de orden en A; se dice que A está bien ordenado por $\preccurlyeq$ si la relaciòn es un buen orden sobre A, es decir, si todo subconjunto no vacío de A tiene primer elemento con respecto al orden $\preccurlyeq$.

Proposición 3.1.23. *Todo conjunto bien ordenado es totalmente ordenado, o con más precisión: toda relación de orden que es un buen orden, es un orden total.*

Demostración. Sea X un conjunto bien ordenado, sean $a, b \in X$ se verá que estos elementos se pueden comparar. En efecto el primer elemento de $\{a, b\}$ (por ser X bien ordenado todo subconjunto debe tener primer elemento) o es a o es b. Si es a se tiene $a \leq b$ y si es b se tiene $b \leq a$. ■

Ejemplo 3.1.24. Los naturales con la relacion $\leq$ es un conjunto bien ordenado, pero $\mathbb{R}^+$ y $\mathbb{Z}$ no aunque son ordenes totales.

Si A es totalmente ordenado, puede tener a lo más un elemento minimal que sera el elemento minimo. De igual modo, puede contener a lo más un elemento maximal, que será entonces el mayor o último elemento. Todo conjunto paricalmente ordenado tiene por lo menos un elemento maximal y un elemento minimal.

3.2. Axioma de elección

Hasta el momento se han recopilado una serie de conceptos que se han venido analizando en el transcurso de este trabajo, ahora estudiaremos una herramienta de gran importancia no solo en este trabajo si no en gran parte de la matemática: el Axioma de Elección y su equivalente el Lema de Zorn, este último será una de los elementos más fuertes que usaremos para el desarrollo de la demostración del isomorfismo entre los complejos sin el cero y el círculo de radio uno.

Axioma 3.2.1. ***Axioma de Elección.*** *A toda colección $\mathfrak{C}$ no vacía de conjuntos no vacíos, corresponde al menos una función e de dominio $\mathfrak{C}$ tal que para todo A de $\mathfrak{C}$, $e(A) \in A$. (La función e se le llama función de elección).*

Esta es una de las presentaciones clásicas de este axioma dado que por su uso, en diferentes ramas de la ciencia se presenta de diversas maneras. El lema que sigue fué demostrada por K. Kuratowski[2] en 1912, usando el axioma de elección, unos diez años más tarde M. Zorn [3] probó que este a su vez implica el axioma de elección; debido a que fué la primera vez que alguien demostró la equivalencia de un principio maximal con el axioma de elección, hoy en día por iniciativa de N. Bourbaki[4] se le llama "Lemma de Zorn" [5].

Lema 3.2.2. ***Lema de Zorn****. Si X es un conjunto parcialmente ordenado por la relación $\preccurlyeq$, tal que toda cadena de X es acotada superiormente en X, entonces X posee al menos un elemento maximal.*

Los principios maximales como el lema de Zorn, han reemplazado al mismo axioma de elección en muchas de sus aplicaciones en Álgebra y Topología.
Para ilustrar cómo se usa el lema de Zorn, probaremos que éste implica el axioma de elección (AE).

Proposición 3.2.3. *El lema de Zorn implica el axioma de elección.*

Demostración. Sea X un conjunto no vacío; una función de elección para X debe ser tal que $f(A) \in A$ para todo subconjunto A no vacío de X; la idea de la construcción de la función, está en tomar una f_1 tal que su dominio sea un subconjunto de $\mathcal{P}(X) - \phi$ y que $f_1(A) \in A$ para todo A de su dominio, e ir extendiéndola poco a poco hasta que su dominio sea $\mathcal{P}(X) - \phi$. La función f_1 podría ser por ejemplo $\{(\{a\}, a), (\{a, b\}, b), (X, a)\}$, donde $a, b \in X$. Como para un conjunto X infinito el proceso sugerido no termina nunca, se procede en la forma siguiente: Sea $\Im$ el conjunto de todas la funciones f tales que $Dom(f) \subseteq (\mathcal{P}(X) - \phi)$, $\mathcal{R}(f) \subseteq X$ y $\forall A \in Dom(f)\ f(A) \in A$. Por el ejemplo dado anteriormente se ve que $\Im \neq \phi$; ordenemos $\Im$ por contenencias, es decir $f \leqslant g$ significa que $f \subseteq g$ o lo que es lo mismo, g es una extensión de f.
Sea $\mathfrak{C}$ cadena de $\Im$; como lo deseamos aplicar el lema de Zorn , debemos ver que $\mathfrak{C}$ es acotada superiormente, para lo cual una forma usual de hacerlo cuando el orden es la inclusión, consiste simplemente que $\bigcup \mathfrak{C} \in \Im$. En efecto:

[2]Kazimierz Kuratowski, 2 de febrero de 1896-18 de junio de 1980.

[3]Max August Zorn; 6 de junio de 1906 en Krefeld, Alemania -9 marzo de 1993 Bloomington, Indiana, EEUU.

[4]Nicolás Bourbaki es el nombre colectivo de un grupo de matemáticos franceses que en los años 30 se propusieron revisar los fundamentos de las matemáticas con una exigencia de rigor mucho mayor que la que entonces era moneda corriente en esta ciencia. Fundado en 1935, inició la publicación de sus monumentales Elementos de matemáticas de acuerdo con el nuevo canon de rigor y el método axiomático, pretendiendo cubrir las bases de todas las matemáticas. Hasta el presente (2006) ha redactado los volúmenes de Teoría de conjuntos, Álgebra, Topología general, Funciones de una variable real, Espacios vectoriales topológicos, Integración, Álgebra conmutativa, Variedades diferenciables y analíticas, Grupos y álgebras de Lie y Teorías espectrales. Fue fundado inicialmente por Henri Cartan, Claude Chevalley, Jean Coulomb, Jean Delsarte, Jean Dieudonné, Charles Ehresmann, René de Possel, Szolem Mandelbrojt y André Weil.

[5]Opc. Muñoz Quevedo J., Introducción a la teoría de conjuntos Pág. 306-307.

1. $\bigcup \mathfrak{C}$ es una función, ya que si $(\{a\}, b) \in \bigcup \mathfrak{C}$ y $(\{a\}, c) \in \bigcup \mathfrak{C}$, existen $f, g \in \mathfrak{C}$ tales que $(\{a\}, b) \in f$ y $(\{a\}, c) \in g$, pero siendo $\mathfrak{C}$ una cadena $f \subseteq g$ ó $g \subseteq f$; en cualquier caso $(\{a\}, b)$ y $(\{a\}, c)$ están en la misma función lo que implica que $b = c$.

2. El dominio de $\bigcup \mathfrak{C}$ notado como $\mathcal{D}(\bigcup \mathfrak{C}) = \mathcal{D}\left(\bigcup_{f \in \Im} f\right) = \bigcup_{f \in \Im} \mathcal{D}(f) \subseteq \mathcal{P}(X) - \phi$ y por la propiedad análoga del recorrido el cual se notarà como $\mathcal{R}$ se concluye $\mathcal{R}(\bigcup \mathfrak{C}) \subseteq X$.

3. Si $A \in \mathcal{D}(\bigcup \mathfrak{C}) = \bigcup_{f \in \Im} \mathcal{D}(f)$, existe $f \in \mathfrak{C}$ tal que $A \in \mathcal{D}(f)$ y en consecuencia $f(A) \in A$, con lo cual termina la verificación ya que siendo $\bigcup \mathfrak{C}$ una extensión de f, también la imagen de A por $\bigcup \mathfrak{C}$ es $f(A)$.

Concluimos que $\bigcup \mathfrak{C} \in \ Im(f)$ y por consiguiente es una cota superior de $\mathfrak{C}$. Por el Lema de Zorn existe entonces al menos una función g maximal en $\Im$; resta por demostrar que $\mathcal{D}(g) = \mathcal{P}(X) - \{\phi\}$. Si existiese $B \in \mathcal{P}(X) - \{\phi\}$ tal que B no estuviese en $\mathcal{D}(g)$, como $B \neq \phi$, tomando $b \in B$ podríamos formar $h = g \cup \{(B, b)\}$, la cual estaría en $\Im$ y sería una extensión estricta de g, en contradicción con el hecho de ser g maximal. [6] ■

Como se mencionó al inicio de este trabajo el Axioma de elección o su equivalente el Lema de Zorn son necesarios para la demostración de algunos resultados como:

1. La paradoja de Banach-Taski[7].

2. La unión numerable de conjuntos numerables es numerable.

3. Todo espacio vectorial admite una base.

4. Teorema Tychonoff: el producto de espacios compactos es compacto.

5. Para ilustrar el teorema de Hahn-Banach[8].

6. Mostrar que existen conjuntos de números reales que no son medibles en el sentido de Lebesgue.

Este Lema es de gran utilidad en diferentes ramas de la matemática; será pieza fundamental para responder uno de los cuestionamientos planteados al inicio de este trabajo, " todo conjunto linealmente independiente puede extenderse a una base"; este resultado es uno de los principales factores con los que se desarrolla la demostración del isomorfismo de los complejos sin el cero y el círculo de radio uno.

[6] Tomado de Muñoz Quevedo J., Introducción a la teoría de conjuntos Pág. 308.

[7] Pág. 3, [8]

[8] Teorema de Hahn-Banach: Todo funcional lineal f definido en un subespacio E de un espacio vectorial real V y tal que $f(x) \leq p(x)$, donde p es un funcional sublineal definido en V, puede extenderse linealmente $\widehat{f}$ de V que sigue siendo acotado por p. Caicedo Xavier; hppt:\\ users.mbi.ohio-state.edu/genciso/Papers/HahnBanach.pdf

CAPÍTULO 4

HOMOMORFISMO, ISOMORFISMO DE GRUPOS Y GRUPOS COCIENTES

En el inicio de este trabajo se dio una introducción al concepto de isomorfismo, el cual matemáticamente hablando, pretende captar la idea de tener la misma estructura, es decir establecer un isomorfismo es mostrar que dos conjuntos dotados de ciertas operaciones y/o relaciones son estructuralmente iguales. En este capítulo se trabajará formalmente el concepto de isomorfismo entre grupos abelianos.

4.1. Isomorfismos

Definición 4.1.1. Sea $\langle G, * \rangle$ y $\langle H, \oplus \rangle$ grupos, una función $f : G \to H$ es un isomorfismo si es biyectiva y además cumple que

$$\forall g_1, g_2 \in G \; f(g_1 * g_2) = f(g_1) \oplus f(g_2) \tag{4.1.1}$$

Se dice entonces que los dos grupos son isomorfos.

Revisemos entonces algunos ejemplos de isomorfismo

Ejemplo 4.1.2. Sea X el grupo mutiplicativo de los reales positivos y Y el grupo aditivo de los reales; se define $f : X \to Y$ como $f(x) = \ln(x)$. Tenemos que esta función es uno a uno y sobre. Como $\ln(x * y) = \ln(x) + \ln(y)$ entonces f es un ismorfismo.

Definición 4.1.3. Sean A y B grupos, el producto directo entre ellos es el grupo C donde

$$C = A \times B = \{(a, b) \in C \mid a \in A \; y \; b \in B\} \tag{4.1.2}$$

y $\cdot$ se define así:

$$(a, b) \cdot (c, d) = (ac, bd) \tag{4.1.3}$$

C es un nuevo grupo,que se llama el **producto directo** $A \times B$.

Ejemplo 4.1.4. Siempre $A \times B$ es isomorfo a $B \times A$, construir el isomorfismo es inmediato. Una clara ilustración de esto es el $\mathbb{C} \cong \mathbb{R} \times \mathbb{R}$ este es un isomorfismo que a envia a cada $z = a + bi \in C$ en $(a, b) \in \mathbb{R} \times \mathbb{R}$.

Ejemplo 4.1.5. El conocido grupo aditivo $\mathbb{R}^3$ el cual es el producto directo $\mathbb{R} \times (\mathbb{R} \times \mathbb{R})$ que no es lo mismo que el grupo $(\mathbb{R} \times \mathbb{R}) \times \mathbb{R}$ pero por ser isomorfos se entienden como iguales.

Para dos subgrupos de un grupo G se define el producto interno como:

Definición 4.1.6. Sean A y B subgrupos de un grupo G (abeliano) el conjunto:

$$A.B = \{ab \mid a \in A \text{ y } b \in B\}. \tag{4.1.4}$$

$A.B$ es un subgrupo de G llamado el producto interno de A con B.

Se hace énfasis de que este producto interno forma un subgrupo sólo si el grupo donde están contenidos es abeliano. Algunas veces este producto coincide con el producto directo, este caso se caracteriza a continuación.

Teorema 4.1.7. *Sea G un grupo abeliano, A y B subgrupos de G si $A \cap B = \{1\}$ y $A.B = G$ entonces $A \times B \cong G$.*

Demostración. Se define:

$$\begin{aligned} f: \quad A \times B &\to A.B \\ (a, b) &\to a.b \end{aligned}$$

Se debe ver que f es una biyección. Sea $f(a_1, b_1) = f(a_2, b_2)$ entonces $a_1.b_1 = a_2.b_2$ entonces multiplicando por a_1^{-1} y b_2^{-1} se tiene que $a_1^{-1}.a_2 = b_2^{-1}b_1$ como $A \cup B = \{1\}$ entonces como $a_1^{-1}.a_2 \in A$ y como $b_2^{-1}b_1 \in B$ se tiene que $a_1^{-1}.a_2 = b_2^{-1}b_1 = 1$ de ahi se tiene que $a_1 = a_2$ y $b_1 = b_2$, concluyendo que f es inyectiva. Que f es sobre se deduce de que $A.B = G$ y es inmediato ver que f respeta las operaciones. Se tiene entonces que f es un isomorfismo. ■

A continuación se expone una versión reciproca del resultado anterior.

Teorema 4.1.8. *Sea G, A y B grupos abelianos. Si $A \times B \cong G$ entonces existen subgrupos A' y B' de G isomorfos a A y B respecitvamente, tales que $A' \cap B' = \{1\}$ y $A'.B' = G$.*

Ejemplo 4.1.9. $\mathbb{C}^*$ es isomorfo a $\mathbb{R}^+ \times S^1$ pero no es isomorfo a $\mathbb{R}^* \times S^1$. Dado que $\mathbb{R}^+ \cap S^1 = 1$ y $\mathbb{R}^+.S^1 = \{r(x, y) \mid r \in \mathbb{R}^+ \text{ y } (x, y) \in S^1\}$, el producto directo de estos conjuntos son los circulos con centro en el origen y radio $r \in \mathbb{R}^+$, dado que si $r(x, y) \in \mathbb{R}^+.S^1$ entonces se tiene que: $r(x, y) = (rx, ry)$, la magnitud de estos elementos es

$$\sqrt{(rx)^2 + (ry)^2} = \sqrt{r^2x^2 + r^2y^2} = \sqrt{r^2(x^2 + y^2)} = r\sqrt{(x^2 + y^2)}$$

Como $r > 0$ entonces $\sqrt{(x^2 + y^2)} = r$ este grupo constituye al grupo $\mathbb{C}^*$. Por el Teorema 4.1.7 $\mathbb{C}^*$ es isomorfo a $\mathbb{R}^+ \times S^1$.
Ahora bien, como $\mathbb{R}^* \cap S^1 = \{1, -1\}$ podemos asegurar por el Teorema 4.1.7 que $\mathbb{R}^* \times S^1$ no es isomorfo a $\mathbb{C}^*$.

Los isomorfismo que se han presentado son entre grupos infinitos, se presentarán entonces algunos isomorfismos entre grupos finitos.

Sea $\mathbb{Z}_n$ el grupo de los enteros módulo n con la adiciòn. Este es un grupo finito que tiene exactamente n elementos; $\mathbb{Z}_n$ forma un grupo con la multiplicaciòn cuando n es primo y no se tiene encuenta el 0.

Ejemplo 4.1.10. El grupo $\mathbb{Z}_4$ de los enteros módulo 4 con la suma y $\mathbb{Z}_5^*$ los enteros módulo 5 sin el cero con el producto, son isomorfos. Por las tablas de la suma y del producto respectivamente, se puede ver como se insinúa el isomorfismo.
El isomorfismo $f : \mathbb{Z}_4 \to \mathbb{Z}_5^*$ está dado por:

$$f(0) = 1 \qquad f(1) = 2 \qquad f(2) = 4 \qquad f(3) = 3.$$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

*	1	2	3	4
1	1	2	3	4
2	2	4	3	1
3	3	1	4	2
4	4	3	2	1

Tabla 4.1: Grupo aditivo $\mathbb{Z}_4$ y grupo multiplicativo Z_5^*.

*	1	2	4	3
1	1	2	4	3
2	2	4	3	1
4	4	3	1	2
3	3	1	2	4

Tabla 4.2: Grupo multiplicativo $\mathbb{Z}_5$

Al hacer esta alteración en la posición de los elementos en la tabla anterior del grupo $\mathbb{Z}_5^*$ se hace mucho más evidente el isomorfismo entre $\mathbb{Z}_5^*$ y $\mathbb{Z}_4$, dado que las tablas respectivas son iguales salvo el nombre que toman los elementos en cada grupo.

Gracias a este ejemplo se puede apreciar más claramente como el isomorfismo respeta y conserva la estructura, dado que envía módulos en módulos y como ya se vio en la Definición 2.4.1 estos grupos son grupos cìclicos donde $< 1 >$ es el generador de $\mathbb{Z}_4$ y $< 2 >$ de $\mathbb{Z}_5$.
Todo grupo, aún los no abelianos, contiene subgrupos cìclicos. Las potencias de cada elemento de un grupo genera un subgrupo cìclico. Un ejemplo de esto es un grupo cíclico infinito isomorfo a $\mathbb{Z}$. Para nuestro caso cada elemento de $\mathbb{C}^*$ genera un subgrupo ciclíco algunos finitos como es es caso de $< i >= \{i, -1, -i, 1\}$ y otros como $< 3i >= \{3^n i^n \mid n \in \mathbb{Z}\}$ que son infinitos e isomorfos a $\mathbb{Z}$ como se afirmó anteriormente. Para este ejemplo dicho isomorfismo esta dado por:

$$\begin{aligned} f : \ & < 3i > \to \mathbb{Z} \\ & (3i)^n \to n \end{aligned}$$

de tal manera que $(3i)^n(3i)^m = (3i)^{nm}$ con $m, n \in \mathbb{Z}$.
Así queda ejemplarizada la Proposición 2.4.2. Donde los isomorfismo estan definido por la potencia del generador, como lo muestra el ejemplo anterior. Por lo tanto para cualquier grupo cíclico finito con generador $< a >$ se tiene que:

$$\begin{aligned} f: \ & < a > \to \mathbb{Z}_n \\ & (a)^m \to m \qquad (\text{mód } n) \end{aligned}$$

donde $n, m \in \mathbb{N}$. Para el caso infinito el isomorfismo estará dado por:

$$\begin{aligned} f: \ & < a > \to \mathbb{Z} \\ & (a)^n \to n \end{aligned}$$

donde $n \in \mathbb{N}$.

Contrariamente a lo que sugiere la palabra "cíclico", es posible generar infinitos elementos y no formar nunca un ciclo real: es decir, que cada $g^n \in G$ sea distinto. Un grupo con esta condición sería un grupo cíclico infinito, isomorfo al grupo de los enteros con la adición.

Por esto, los grupos cíclicos normalmente se denotan simplemente por el grupo "canónico" al que son isomorfos: si el grupo es de orden n, para n entero, dicho grupo es el grupo $\mathbb{Z}_n$ de enteros $\{0, \ldots, n-1\}$ con la adición módulo n. Si es infinito, éste es, como intuitivamente se piensa isomorfo a $\mathbb{Z}$.

La notación $\mathbb{Z}_n$ comúnmente es evitada, puesto que puede ser confundida con la notación usual para los números p-aditivos. Una alternativa es usar la notación de grupo cociente, $\mathbb{Z}/n\mathbb{Z}$, este concepto se revisará más adelante, dichos grupos serán estudiados en detalle; otra posible solución es denotar la operación como multiplicación y representar el grupo $\mathbb{C}_n = \{1, \xi^1, \xi^2, \ldots, \xi^{n-1}\}$ el cual es el grupo de las raíces de la unidad en $\mathbb{C}$ por lo tanto $\mathbb{C}_n \subset \mathbb{C}^*$, este grupo también sera de nuestro interes y se estudiara en la Sección 6.1 en donde se mostrara que $\mathbb{C}_n \cong \mathbb{Z}_n$.
Por lo dicho anteriormente, todo grupo cíclico es isomorfo a algun $\mathbb{Z}_n$, o $\mathbb{Z}$. Basta entonces con examinar dichos grupos para entender los grupos cíclicos en general.
Dado un grupo cíclico G de orden n (donde n puede ser infinito), y dado $g \in G$, se tiene:

1. Si G es un grupo infinito, entonces el grupo tiene exactamente dos generadores: los elementos que mediante el isomorfismo sean 1 y -1 en $\mathbb{Z}$.

2. Todo subgrupo de G es cíclico. De hecho, para n finito, todo subgrupo de G es isomorfo a un $\mathbb{Z}_m$, donde m es divisor de n; y si el grupo es infinito, todo subgrupo de G corresponderá a un subgrupo $m\mathbb{Z}$ de $\mathbb{Z}$ (el cual es también isomorfo a $\mathbb{Z}$), bajo el isomorfismo entre G y $\mathbb{Z}$. Los generadores de $\mathbb{Z}_n$ son los enteros que son primos relativos con n. El número de tales generadores se designa por $\varphi(n)$, donde φ designa la función φ de Euler[1]. En general, si d es un divisor de n, el número de elementos

[1]La función φ de Euler indica, para su parámetro m, el número de elementos invertibles en un cuerpo o anillo finito de dimensión m. Su valor se corresponde igualmente con la cantidad de números primos relativos con m menores que m.

de $\mathbb{Z}_n$ de orden d es $\varphi(d)$. El orden del elemento m es $n/\text{mcd}(m,n)$. Si p es primo, el único grupo con p elementos (salvo isomorfismos) es $\mathbb{Z}_p$.

3. El producto directo de dos grupos cíclicos $\mathbb{Z}_n \times \mathbb{Z}_m$ es cíclico si y sólo si m y n son primos entre sí; en tal caso, el grupo obtenido será isomorfo a $\mathbb{Z}_{nm}$ (Por ejemplo, $\mathbb{Z}_{12}$ es isomorfo a $\mathbb{Z}_3 \times \mathbb{Z}_4$, pero no a $\mathbb{Z}_6 \times \mathbb{Z}_2$.).

De hecho supongiendo que $\text{mcd}(n,m) = 1$. El generado $< n >$ en $\mathbb{Z}_{nm}$ tiene m elementos y el generado $< m >$ en $\mathbb{Z}_{nm}$ tiene n elementos. Además $< n > \cap < m >= \{0\}$ si $n|k$ y $m|k \quad 0 < k < nm$ donde k es múltiplo común. Como el mínimo común multiplo entre los dos números es $\frac{nm}{\text{mcd}(n,m)} = \frac{nm}{1} = nm$. Se tendría que $< n > + < m >= \mathbb{Z}_{nm}$ pero dicho múltiplo común k que cumpla con la condiciòn $n|k$ y $m|k \quad 0 < k < nm$ no existe.

4.2. Clases Laterales y grupos cocientes

Cómo organizar o repartir los elementos de un conjunto y cómo se establecen caracterizaciones entre ellos, es uno de los quehaceres en las matemáticas y otras ciencias. Ciertas relaciones de equivalencia permiten construir a partir de oepraciones entre ellas una nueva estrucatura interesante el ***grupo cociente***.

Definición 4.2.1. Sea G grupo, dado $H \subseteq G$ definimos la siguiente relación binaria en G

$$a \equiv b \pmod{H} \Leftrightarrow a^{-1}b \in H. \tag{4.2.1}$$

a la que llamaremos relación de congruencia módulo H.

Proposición 4.2.2. *Si H es subgrupo de G entonces la relación de congruencia módulo H es una relación de equivalencia (3.1.5) en G.*

A la clase de equivalencia de a $a \in G$ según la relación de congruencia módulo H la llamaremos *Clase lateral de a* y será notado aH, donde

$$aH = \{x \in G \mid a^{-1}x \in H\} = \{ah \mid h \in H\}. \tag{4.2.2}$$

Ejemplo 4.2.3. Si $G = \mathbb{Z}$ y $H = 3\mathbb{Z}$, entonces las clases laterales a izquierda son:

$$\begin{aligned} 0 + 3\mathbb{Z} &= 3\mathbb{Z} \\ 1 + 3\mathbb{Z} &= \{\ldots, -5, -2, 1, 4, 7, \ldots\} \\ 2 + 3\mathbb{Z} &= \{\ldots, -4, -1, 2, 5, 8, \ldots\}. \end{aligned}$$

Como nuestros grupos de estudio $(\mathbb{C}^*, S^1)$ son grupos abelianos no se hará distinción entre las clases laterales a izquierda y las clases laterales a derecha, puesto que son las mismas, pero para grupos no abelianos no se obtiene el mismo resultado. Los resultados que se tienen en este capitulo son todos sobre grupos abelianos, para grupos no abelianos algunos de estos no son ciertos.

Proposición 4.2.4. *Sea H un subgrupo de G (abeliano). El producto de dos clases laterales de H en G es la clase del producto de sus representantes, es decir*

$$(Ha)(Hb) = Hab$$

para cualesquier $a, b \in G$.

Demostración. Sea H un subgrupo de G, $a, b \in G$ y $h_1, h_2 \in H$ entonces $(h_1a) \in Ha$ y $(h_2b) \in Hb$ por lo tanto $(h_1a)(h_2b) = h_1h_2ab$ por conmutatividad de G pero, $h_1h_2ab = h_3ab$ por propiedad clausurativa de G, tenemos que $h_3ab \in Hab$ y hemos demostrado que $HaHb \subseteq Hab$.
Por otra parte si $hab \in Hab$ entonces $hab = ha1b$ donde $1 \in H$ por ser 1 módulo de H.
Como $ha \in Ha$ y $1b \in Hb$ entonces $hab \in HaHb$ y hemos probado que $Hab \subseteq HaHb$ completando la demostración. ■

Son muy importantes los subgrupos en los que las clases laterales tanto a izquierda como a derecha son las mismas, estos se conocen como subgrupos normales y son indispensables para desarrollar la teoría en general de grupos cocientes. En un grupo abeliano todo subgrupo es un subgrupo normal.

Ejemplo 4.2.5. La familia de los conjuntos $\mathcal{U} = \{U_r\}_{r\in\mathbb{R}^+}$ donde

$$U_r = \{z \in \mathbb{C}^* \mid |z| = r\}$$

con $r \in \mathbb{R}^+$ describe todos los círculos de radio r y centro en el origen. Cada U_r es una clase lateral de S^1 en $\mathbb{C}^*$ y la unión de estas clases laterales conforman a $\mathbb{C}^*$ por lo tanto la familia $\mathcal{U}$ es una partición de $\mathbb{C}^*$. Si tomamos a cada elemento de S^1 y se opera con un elemento de $\mathbb{C}^*$ obtendremos un círculo con centro en origen y cuyo radio será la magnitud del elemento de $\mathbb{C}^*$. Por ejemplo, si tomamos a $2i$ y lo multiplicamos por cada uno de los elementos de S^1 obtendremos el círculo centrado en el origen de radio 2; que es U_2. Si se toman dos de estas clases laterales y se operan, se obtendra otra clase lateral la cual describe un círculo centrado en el origen cuyo radio es el producto de los representantes de las clases que se operaron

$$U_{r_1}U_{r_2} = U_{r_1r_2}. \tag{4.2.3}$$

Podemos concluir entonces que el operar estas clases laterales es equivalente a la multiplicación de reales positivos.

El anterior ejemplo suguiere que el conjunto de clases laterales le podemos dar estructura de grupo, esto es cierto y se generá así una estructura; esta forma de crear (o develar) nuevos objetos es general y muy importante en las matemáticas.

Definición 4.2.6. Sea G un grupo y $N \leq G$, G/N es el grupo cuyos elementos son clases laterales de N en G y la operación es el producto de clases de N en G.

Respecto al producto definido se tiene lo siguiente:

1. X, $Y \in G/N$ implica $XY \in G/N$; pues si $X = Na$, $Y = Nb$ para algunos $a, b \in G$, entonces $XY = NaNb = Nab \in G/N$.

2. $X, Y, Z \in G/N$ implica $X = Na$, $Y = Nb$, $Z = Nc$ con $a, b, c \in G$, y, por tanto, $(XY)Z = (NaNb)Nc = Na(NbNc) = X(YZ)$. Por tanto, el producto en G/N satisface la ley asociativa.

3. Considérese el elemento $N = Ne \in G/N$. Si $X \in G/N$, $X = Na$, $a \in G$, entonces $XN = NaNe = Nae = Na = X$, y análogamente también $NX = X$. Por tanto Ne es un elemento identidad para G/N.

4. Supongamos $X = Na \in G/N$ (donde $a \in G$); es claro que $Na^{-1} \in G/N$, y $NaNa^{-1} = Naa^{-1} = Ne$. Análogamente $Na^{-1}Na = Ne$. De donde Na^{-1} es el inverso de Na en G/N.

Teorema 4.2.7. *[4] Si G es un grupo y N un subgrupo de G, entones G/N es también un grupo. Se le llama grupo cociente o grupo factor de G sobre N.*

En el Ejemplo 4.2.3 se mostraron las clases laterales de $3\mathbb{Z}$; al realizar el grupo cociente $\mathbb{Z}/3\mathbb{Z}$ se evidencia que este grupo es isomorfo a $\mathbb{Z}_3$. A cada clase lateral le corresponde un elemento de $\mathbb{Z}_3$, es decir $3\mathbb{Z}$ le corresponde 0; $3\mathbb{Z}+1$ le corresponde 1 y $3\mathbb{Z}+2$ le corresponde 2. Generalizando el grupo cociente $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ con $n \in \mathbb{N}$.
El el Ejemplo 4.2.5 se concluyó que el operar la clases laterales de S^1 es como multiplicar reales positivos, por lo tanto el grupo cociente $\mathbb{C}^*/S^1 \cong \mathbb{R}^+$.

Ejemplo 4.2.8. Se estudiará el grupo cociente $\mathbb{R}/\mathbb{Z}$. Observemos las clases laterales de $\mathbb{Z}$ en $\mathbb{R}$: una clase lateral $\mathbb{Z} + r$ con $r \in R$ es tomar a todos los enteros y "desplazarlos´´ una distancia r a la derecha o izquierda según sea r positivo o negativo. Es claro además que da lo mismo, desplazar $\mathbb{Z}$ un distancia r o una distancia $r + z$ donde $z \in \mathbb{Z}$, por tanto será suficiente, para obtener todas las clase considerar $r \in [0, 1)$. Así podemos decir que el grupo $\mathbb{R}/\mathbb{Z} \cong [0, 1)$ dónde la operación en $[0, 1)$ es la suma "circular" que notamos $\oplus$; si $r, s \in [0, 1)$ definimos:

$$r \oplus s = \begin{cases} r + s & \text{si } r + s < 1 \\ r + s - 1 & \text{si } r + s \geq 1. \end{cases}$$

Nótese que ésta es la suma que se efectúa cuando se suman ángulos. Este es el grupo cociente $\mathbb{R}/\mathbb{Z}$.

Ejemplo 4.2.9. Si tomamos el grupo $\mathbb{R}^*$ y tomamos el subgrupo $A = \{1, -1\}$; entonces cada clase lateral de A en $\mathbb{R}^*$ es un conjunto con exactamente dos elementos: un real y su inverso aditivo. Al operar clases laterales entre sí se obtiene la clase correspondiente al producto de los representantes positivos. Así: $\{2, -2\}\{3, -3\} = \{6, -6\}$. Por lo tanto operar estas clases es tomar únicamente el valor positivo del cada clase, puesto que los valores negativos son representados por su inverso aditivo. Al operar estás clases es como sí se multiplicarán reales positivos. En conclución el grupo $\mathbb{R}^*/A \cong \mathbb{R}^+$.

Ejemplo 4.2.10. Una clase lateral de $\mathbb{Q}^+$ en $\mathbb{Q}^*$ es tomar un elemento de $\mathbb{Q}^*$ y multiplicar por cada uno de los elementos de $\mathbb{Q}^+$, pero los elementos de $\mathbb{Q}^*$ o son negativos, o son positivos; por lo tanto, existiran solo dos clases laterales, una que contiene a todos los positivos y la otra con todos los negativos. Al operar dos de estas clases se obtendrá una nueva clase que

pertenece a alguna de las dos anteriormente señaladas. Al tener solo dos clases laterales el grupo cociente $Q^*/Q^+ \cong \mathbb{Z}_2$, en donde $\mathbb{Q}^+$ es representada por el $0 \in \mathbb{Z}_2$ y la otra $\mathbb{Q}^-$ por $1 \in \mathbb{Z}_2$.

Ejemplo 4.2.11. Si se considera $\mathbb{Q}^*$ y $A = \{1, -1\}$; entonces las clases laterales de A en $\mathbb{Q}^*$ son conjuntos con dos elementos; un racional y su inverso aditivo. De manera similar al Ejemplo 4.2.9 se observa que $\mathbb{Q}^*/A \cong \mathbb{Q}^+$.

4.3. Teoremas fundamentales sobre homomorfismo

Durante el transcurso de este trabajo se han analizado algunos conceptos sobre grupos e isomorfismos; ahora se analizará tres grandes resultados que nos serán de gran utilidad. pero antes recordaremos el concepto de homomorfismo.

Definición 4.3.1. Un homomorfismo es una función entre dos grupos que preserva la estructura. Es decir si $\langle G, . \rangle$ y $\langle H, . \rangle$ grupos y $\psi : G \to H$

$$\forall a, b \in G \quad \psi(a).\psi(b) = \psi(a.b). \tag{4.3.1}$$

Se define ***imagen de*** ψ:

$$Img(\psi) = \{\psi(g) \mid g \in G\}. \tag{4.3.2}$$

Puede ver que $Img(\psi)$ es subgrupo de H.
También se define el núcleo de ψ como el conjunto conformado por todos aquellos elementos cuya imagen es el módulo o identidad del grupo de llegada. Es decir,

$$\ker(\psi) : \{x \in A | \psi(x) = 0\} \tag{4.3.3}$$

donde 0 es el módulo de H.

Es facil ver que el núcleo de cualquier homomorfismo es un subgrupo de G (abeliano).

Teorema 4.3.2. *En el homomorfismo $f : G \to H$ el núcleo de f es el subgrupo K de G. Dos elementos de G tienen la misma imagen en H, si y sólo si pertenecen a una misma clase lateral de K.*

Demostración. Es fácil ver que K es un subgrupo de G. Supongase $x, y \in G$, con $f(x) = u$, $f(y) = u$; $u \in H$. Entonces $f(xy^{-1}) = f(x)f(y)^{-1} = uu^{-1} = 1$, luego $xy^{-1} \in K$, y así $x \in Ky$ y x y y estan en la misma clase lateral de K. Recíprocamente, si $x \in Ky$, entonces $x = ky$, con $k \in K$ y si $f(y) = u$, entonces (como $f(k) = 1$) tenemos que $f(x) = u$. Por lo tanto x y y tienen la misma imagen en H. ■

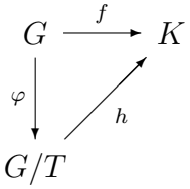
El recíproco de este teorema, es cierto es decir, todo subgrupo K de un grupo G es el núcleo de un homomorfismo $f : G \to H$ para algún grupo H. Específicamente podemos hacer H el grupo factor o cociente G/K como se verá en el siguiente teorema.

Teorema 4.3.3. *Dado un grupo G y un subgrupo K, entonces si $H = G/K$ hay un homomorfismo $G \to H$ cuyo núcleo es K. Este homomorfismo esta dado por $g \to Kg$ y se llama homomorfismo canónico.*

Demostración. Consideremos la función que envia $g \to Kg$ de G sobre H. Si $g_1 \in Kg_1$, $g_2 \in Kg_2$, entonces (como ya se vio) $g_1g_2 \in Kg_3$. Luego $g_1g_2 \to Kg_3 = Kg_1Kg_2$. Así pues la función de G en H preserva el producto y es por tanto un homomorfismo. Como K es la identidad de G/K, entonces $g \to 1$ si y sólo si $g \in K$ en G; luego K es el núcleo del homomorfismo. ■

Teorema 4.3.4. *Si $f : G \to K$ es un homomorfismo sobreyectivo y T el núcleo de f, entonces K es isomorfo a $G/T = H$. Si $f(x) = x'$ entonces el isomorfismo entre H y K envía a Tx en x'.*

El siguiente diagrama muestra cual es la situación que tenemos



Demostración. Como los elementos de G están en la misma clase lateral de T tienen la misma imagen en K, la correspondencia $x' \to T_x$ es uno a uno. Pero si $x \to x'$, $y \to y'$, entonces $xy \to x'y'$. Pero $xy \in T_{xy}$ de donde $x'y' \to T_{xy} = T_xT_y$. Luego la correspondencia $x' \to T_x$ preserva el producto y es un isomorfismo de K sobre $H = G/T$. ■

Resumiendo el contenido de estos teoremas fundamentales sobre homomorfismo se tiene que el núcleo de cualquier homomorfismo es un subgrupo, que cualquier subgrupo es el núcleo de un homomorfismo cuya imagen es única (salvo isomorfismo), y que esta imagen es el grupo factor del grupo dado con respecto al subgrupo.
En la sección anterior se mostraron algunos ejemplos de isomorfismo de grupos cocientes y apartir de las clases laterales y las operaciones entre ellas se mostró de forma intutiva cómo es el grupo cociente y se bosquejó el isomorfo. A partir de estos teoremas se podrá mostrar de manera más formal tales isomorfismos.

Ejemplo 4.3.5. Se considerará el homomorfismo

$$\begin{aligned} f : \mathbb{R}^* &\longrightarrow \mathbb{R}^+ \\ f(r) &= r^2. \end{aligned} \tag{4.3.4}$$

Esta función respeta las operaciones para los grupos dado que, para cualesquiera $r, s \in \mathbb{R}^*$ se cumple que:

$$f(rs) = (rs)^2 = r^2s^2 = f(r)f(s).$$

El núcleo de este homorfismo es el conjunto $A = \{1, -1\}$, dado que $f(A) = f(1) = 1^2 = (-1)^2 = f(-1) = 1$; en virtud del Teorema 4.3.3 el grupo cociente $\mathbb{R}^*/A \cong \mathbb{R}^+$. De manera curiosa otro isomorfismo que respeta la operación y tiene el mismo núcleo es:

$$\begin{aligned} f : \mathbb{R}^* &\longrightarrow \mathbb{R}^+ \\ f(r) &= |r|. \end{aligned}$$

En donde para cualesquiera $r, s \in \mathbb{R}^*$ se cumple que

$$f(rs) = |rs| = |r||s| = f(r)f(s)$$

y $f(A) = f(1) = |1| = |-1| = f(-1)$. Se ha mostrado entonces, dos isomorfismo diferentes con el mismo núcleo.

Ejemplo 4.3.6. Sea el grupo $\mathbb{R}^+ \times \mathbb{R}$ se mostrará que este grupo es isomorfo a el grupo $\mathbb{C}$ con la adiciòn definimos:

$$\begin{aligned} f : \mathbb{R}^+ \times \mathbb{R} &\to \mathbb{C} \\ f(a,b) &= a + bi \end{aligned}$$

Cómo

$$\begin{aligned} f((a,b)+(c,d)) = f((a+c),(b+d)) &= (a+c)+(b+d)i \\ &= (a+bi)+(c+di) = f(a,b)+f(c,d). \end{aligned}$$

Ejemplo 4.3.7. Sea $\mathbb{C}^*$ y $\mathbb{R}^+$ se define f como:

$$\begin{aligned} f : \mathbb{C}^* &\to \mathbb{R}^+ \\ f(z) = f(a+bi) &= |z| = \sqrt{a^2+b^2}. \end{aligned}$$

En donde se tiene que:

$$f(zz') = |zz'| = |z||z'| = f(z)f(z').$$

En este ejemplo f no es una biyección, puesto que no es uno a uno, pero el nucleo de este morfismo es el conjunto de complejos con magnitud uno, esto es, S^1. Por lo tanto el grupo cociente $\mathbb{C}^*/S^1 \cong \mathbb{R}^+$

Ejemplo 4.3.8. Sea $\mathbb{C}^*$ y $\mathbb{C}^*$ se define:

$$\begin{aligned} f : \mathbb{C}^* &\to \mathbb{C}^* \\ f(z) = f(a+bi) &= \overline{z} = a - bi \end{aligned}$$

y se tiene que:

$$\begin{aligned} f(zz') = f((a+bi)+(c+di)) &= f((a+c)+(b+d)i) \\ &= (a+c)-(b+d)i = a+c-bi-di \\ &= (a-bi)+(c-di) = f(a+bi)+f(c+di) \end{aligned}$$

Este es un automorfismo puesto que la función va de $\mathbb{C}^*$ en $\mathbb{C}^*$.

CAPÍTULO 5

BREVE VIAJE HACIA LOS ESPACIOS VECTORIALES

En uno de los capítulos anteriores se dio un vistazo a los conceptos de relaciones de orden, congruencia y lema de Zorn. Estos importantes conceptos nos serán útiles ahora para mostrar, como se dijo al incio de este trabajo, que " todo conjunto linealmente independiente de un espacio vectorial puede ser extendido a una base". Este resultado es necesario para alcanzar el objetivo principal de este trabajo el desarrollo de la demostración del $\mathbb{C}^* \cong S^1$. Además los espacios vectoriales son los cimientos del álgebra lineal de la cual se utilizarán algunos resultados en el desarrollo de la demostración.

5.1. Introducción a campos

Definición 5.1.1. Un anillo con unidad $\langle R, + . \rangle$ es un conjunto R con dos operaciones binarias $+$ y $.$ que llamamos adición y multiplicación, definidas en R satisfaciendo

1. $\langle R, + \rangle$ es un grupo abeliano ó grupo conmutativo (ver Definición 2.2.2).
2. La multiplicacion es asociativa.
3. Para todas las $a, b, c, \in R$ se cumple la **ley distributiva a derecha** $a.(b + c) = (a.b) + (a.c)$ y la **ley distributiva a izquierda** $(a + b).c = (a.c) + (b.c)$.
4. Existe $1 \in R$ (que llamaremos elemento unitario) tal que $1x = x1 = x$ para todo $x \in R$.

Un anillo donde la multiplicación es conmutativa es un **anillo conmutativo**.

Definición 5.1.2. Un anillo conmutativo con unidad donde todos los elementos diferentes de cero tienen inverso multiplicativo es un **campo**.

Los campos son conjuntos con dos operaciones binarias definidas en él, donde cada una de estas operaciones forman un grupo abeliano y estas operaciones se relacionan entre sí por medio de la *propiedad distributiva*.

El campo más familiar que se ha utilizado sobre todo para aquellos estudiantes de niveles básicos es el de los reales ($\mathbb{R}$), se mostrará entonces algunos ejemplos de otros campos.

Ejemplo 5.1.3. $\mathbb{Z}$ no es un campo puesto que cualquier elemento de $\mathbb{Z}$ diferente de 1 o -1 que se tome no tendrá inverso multiplicativo por lo tanto no es una unidad. Las únicas unidades de $\mathbb{Z}$ son 1 y -1.

Ejemplo 5.1.4. $\mathbb{Q}$ es un campo puesto que para todo $q \in \mathbb{Q}$, no nulo, siempre existe un $q' \in \mathbb{Q}$ tal que $qq' = 1$.

Ejemplo 5.1.5. Al contrario del Ejemplo 5.1.3 el conjunto $\mathbb{Z}_p$ es un campo cuando p es primo. Es claro que $\mathbb{Z}_p$ es un anillo puesto que con la suma forma un grupo abeliano; el 1 es el elemento unidad para la multiplicación y esta operación es conmutativa; es fácil mostrar las propiedades distributivas la cuales también se cumplen en $\mathbb{Z}$, por lo tanto $\mathbb{Z}_p$ es un anillo con unidad. Para que $\mathbb{Z}_p$ sea un campo todo elemento diferente de cero debe tener inverso multiplicativo, o sea, $aa^{-1} = 1$; en $\mathbb{Z}$ la ecuación

$$\alpha p + \beta a = 1$$

tiene solución, si y sólo si, a y p son primos relativos, en términos de congruencias que dicha ecuación tenga solución equivale a decir que existe un $b \in \mathbb{Z}_p$ tal que $ba \equiv 1 \pmod{p}$. Por tanto los elementos no nulos de $\mathbb{Z}_p$ es decir $1, 2, \ldots p-1$ tienen cada uno inverso multiplicativo, si y sólo si p es primo.
Por ejemplo para $\mathbb{Z}_7$ se tiene que:

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Tabla 5.1: Grupo Z_7 con la suma

*	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Tabla 5.2: Grupo Z_7 con el producto.

En las Tablas 5.1 y 5.2 se evidencia como $\mathbb{Z}_p$ es un grupo abeliano con la suma, la unidad para el producto es 1 y donde cada elemento tiene inverso, puesto que $1 \cdot 1 = 1 \equiv 1 \pmod{p}$; $2 \cdot 4 = 8 \equiv 1 \pmod{p}$; $5 \cdot 3 = 15 \equiv 1 \pmod{p}$ y $6 \cdot 6 = 36 \equiv 1 \pmod{p}$.

Elemento	Inverso
1	1
2	4
3	5
4	2
5	3
6	6

Tabla 5.3: Inversos multiplicativos de Z_7.

Ejemplo 5.1.6. Sea $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ con la suma y el producto usual forma un campo. La clausura para el campo se cumple tanto para la suma como para el producto dado que:

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (c + d)\sqrt{2}.$$

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2db) + (ad + bc)\sqrt{2}.$$

con $(ac + 2db), (ad + bc) \in \mathbb{Q}$ por ser la suma de racionales clausurativa. El módulo de este campo para la suma es:

$$0 + 0\sqrt{2} = 0.$$

Ahora bien el módulo del producto es

$$1 + 0\sqrt{2} = 1.$$

y para todo $a + b\sqrt{2}$ donde $a, b \in \mathbb{Q}$ no nulos, se tiene que sus inversos multiplicativos son de la forma $\frac{-a}{2b^2-a^2} + \frac{b}{2b^2-a^2}\sqrt{2}$.

5.2. Espacios vectoriales

Definición 5.2.1. Un *espacio vectorial* V sobre un campo F es un grupo abeliano respecto a la adición "+" tal que para todo $\alpha \in F$ y todo $v \in V$ existe un elemento $\alpha v \in V$ de tal modo que, si $v_1, v_2 \in V$:

1. $\alpha(v_1 + v_2) = \alpha v_1 + \alpha v_2$, para $\alpha \in F$, $v_1, v_2 \in V$.
2. $(\alpha + \beta)v = \alpha v + \beta v$, para α, $\beta \in F$, $v \in V$.
3. $\alpha(\beta v) = (\alpha\beta)v$, para α, $\beta \in F$, $v \in V$.
4. $1v = v$, para $v \in V$ donde 1 es el elemento unidad de F.

Antes de conocer algunos resultados, se examinarán varios ejemplos:

Ejemplo 5.2.2. Sean F cualquier campo y $V = F[x]$ el anillo de polinomios en x sobre F. Utilizando solamente el producto de un polinomio por una constante, por ejemplo,

$$\beta(\alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n) = \beta\alpha_0 + \beta\alpha_1 x + \ldots + \beta\alpha_n x^n$$

se encuentra que V se convierte en un espacio vectorial sobre F.

Ejemplo 5.2.3. Sea F cualquier campo y $V = \{(\alpha_1, \alpha_2, \ldots, \alpha_n) | \ \ los\ \alpha_i \in F\}$ el conjunto de n-uplas sobre F, con igualdad y adición definidas por componentes. Para $v = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ y $\beta \in F$, defínase $\beta v = (\beta\alpha_1, \beta\alpha_2, \ldots, \beta\alpha_n)$. V es el espacio vectorial sobre F.

Ejemplo 5.2.4. Sea F un campo y A un conjunto cualquiera y sea $V = \{f \mid f : A \to F\}$ tal espacio vectorial sobre F se notará como F^A y sus operaciones se definen de manera natural: $(f + g)(a) = f(a) + g(a)$ y $(\alpha f)(a) = \alpha(f(a))$ donde $a \in A$, $f, g \in F^A$, $\alpha \in F$.

Ejemplo 5.2.5. El conjunto de las matrices $n \times n$ con componentes en $\mathbb{R}$ son un espacio vectorial; con la suma de matrices y el producto por un escalar.

Trataremos ahora algunas nociones más particulares de los espacios vectoriales.

Lema 5.2.6. *Si V es un espacio vectorial sobre un campo F, entonces, para todo $\alpha \in F$ y todo $v \in V$:*

1. $\alpha 0 = 0$, *donde* 0 *es el elemento neutro de* V;
2. $0v = 0$, *donde* 0 *es el elemento neuatro de* F;
3. $\alpha v = 0$ *implica que* $\alpha = 0$ *o bien;* $v = 0$.
4. $(-\alpha)v = -(\alpha v)$.

Se utilizará el mismo símbolo 0 para le cero de F como el de V. Además en los espacios vectoriales como en los grupos abelianos este elemento 0 es único. Esto deduce del siquiente resultado válido para grupos en general.

Proposición 5.2.7. *En un espacio vectorial la ecuación $a + x = b$ tiene solución única en el espacio.*

Demostración. Como V es un grupo con respecto a $+$ entonces cada elemento tiene su inverso por lo tanto

$$\begin{aligned} a + x &= b \\ a + (-a) + x &= b - a \\ x &= b - a \end{aligned}$$

Donde $b - a = c$ y c es un elemento de V. ■

Ahora estudiaremos algunos subconjuntos muy importantes dentro de los espacios vectoriales.

5.3. Combinaciones Lineales y Subespacios

Definición 5.3.1. Sean V un espacio vectorial sobre F y $v_1, v_2, \ldots, v_n$ elementos de V. Se dice que un elemento $v \in V$ es una *combinación lineal* de $v_1, v_2, \ldots, v_n$ si $v = \alpha_1 v_1 + \ldots + \alpha_n v_n$ para algunos $\alpha_1, \ldots, \alpha_n$ en F.

Ejemplo 5.3.2. Sea $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ un elemento del espacio vectorial de matrices 2×2 con coeficientes reales (ver Ejemplo 5.2.5) entonces, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \alpha_2 \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \alpha_2 \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \alpha_3 \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \alpha_4 \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ donde $\alpha_1 = a, \alpha_2 = b, \alpha_3 = c$ y $\alpha_4 = d$ por lo tanto podemos notar este elemento como combinación lineal de $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ y $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.

Definición 5.3.3. Sea V un espacio vectorial se dice que los elementos $\upsilon_1, \upsilon_2, \ldots, \upsilon_n$ en V son *linealmente independientes* si $\alpha_1\upsilon_1 + \ldots + \alpha_n\upsilon_n = 0$, donde $\alpha_1, \ldots, \alpha_n$ están en F, implica que $\alpha_1 = \alpha_2 = \ldots = \alpha_n = 0$.

Si los elementos $\upsilon_1, \upsilon_2, \ldots, \upsilon_n$ en V no son *linealmente independientes* sobre F, entonces se dice que son *linealmente dependientes* sobre F. La independencia lineal depende del campo, por ejemplo; Si $\mathbb{C} \supset \mathbb{R}$, entonces $\mathbb{C}$ es un espacio vectorial sobre $\mathbb{R}$, pero también es un espacio vectorial sobre $\mathbb{C}$ mismo. Los elementos $1, i$ en $\mathbb{C}$ son linealmente independientes sobre $\mathbb{R}$ pero no lo son sobre $\mathbb{C}$, ya que $i1 + (-1)i = 0$ es una combinación lineal no trivial de $1, i$ sobre $\mathbb{C}$.

Ejemplo 5.3.4. En el ejemplo se observó como se expresó a a la matriz $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ como combiación lineal de las matrices $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} y \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$. Estas matrices son linealmente independientes puesto que la única manera de que al combinarlos linealmente obtengamos la matriz nula es cuando los $\alpha_i = 0$ con $i = 1, 2, 3, 4$

El recíproco del lema anterior también es cierto.
Hasta este momento se han mostrado con conjuntos finitos linealmente independientes, ¿pero será posible a partir de un conjunto finito linealmente independiente contruir uno infinito? ¿Cómo se justifica que un conjunto infinito es linealmente independiente?

Ejemplo 5.3.5. Sea V es espacio vectorial de la funciones en los reales. El conjunto $\{e^t, e^{2t}\}$ es un conjunto linealmente independiente dado que

$$\begin{aligned} ae^t + be^{2t} &= 0 && \text{dividiendo por } e^t \text{ se obtine que} \\ a + be^t &= 0 && \text{despejando a } e^t \text{ se tiene que} \\ be^t &= -a. \end{aligned}$$

Como esto se debe cumplir para cualquier $t \in \mathbb{R}$ por lo tanto cuando $t = 0$ implica que $b = -a$ remplazando en la combinación lineal se tiene que:

$$\begin{aligned} ae^t + (-ae^{2t}) &= 0 && \text{factorizando } ae^t \text{ se tiene que} \\ ae^t(1 - e^t) &= 0 && \text{dividiendo por } 1/ae^t \text{ se tiene que} \\ (1 - e^t) &= 0 && \text{despejando a } e^t \text{ tal que} \\ e^t &= 1. \end{aligned}$$

Pero esto solo se cumple cuando $t = 0$, se ha llegado a una contradicción puesto que se debe cumplir para cualquier $t \in \mathbb{R}$; entonces los únicos valores posibles son $a = b = 0$. Se ha demostrado que el conjunto $\{e^t, e^{2t}\}$ es linealmente independiente.

Ahora bien, si incluimos en el conjunto funciones e^{nt} con $n > 2 \in \mathbb{N}$ estos nuevos conjuntos serán también linealemente independientes y tendremos un conjunto infinito numerable en donde cada subconjunto finito es linealmente independiente.

Definición 5.3.6. Sea V un espacio vectorial, si $S \subseteq V$ se dice que S es linealmente independiente si todo subconjunto finito de S es linealmente independiente.

Definición 5.3.7. Sea W un subconjunto no vacío de un espacio vectorial V. Donde W cumple con todas las condiciones de espacio vectorial, entonces W es un subespacio de V. Se notará $W \leq V$

Ejemplo 5.3.8. Sea V el espacio vectorial de las matrices $n \times m$ (Ver Ejemplo 5.2.5). El conjunto conformado por las matrices triangulares superiores $n \times m$ es un subespacio vectorial.

Ejemplo 5.3.9. Sea $\mathbb{C}$ el espacio vectorial de los números complejos sobre $\mathbb{Q}$. El conjunto $\mathbb{R}$ es un subespacio vectorial.

Proposición 5.3.10. *Un subconjunto S no vacío de un espacio vectorial V es un subespacio de V si se sumple:*

1. *Si $x \in S$ y $y \in S$ entonces $x + y \in S$.*
2. *Si $x \in S$ entonces $\alpha x \in S$ para toda α.*

Como un subespacio hereda todas las condiciones de espacio vectorial, cumple entonces con las clausurativas tanto para la adición como la multiplicación por escalares. Por lo tanto se podría decir que ser subespacio vecorial es muy parecido a ser subgrupo puesto que solo se debe verificar que el candidato cumple con las propiedades clausurativas.

Proposición 5.3.11. *Todo subespacio vectorial contiene al módulo de la suma.*

Como se intuye todo subespacio por cumplir con todas las propiedades de espacio vectorial debe este entonces contener al módulo de la suma puesto que de lo contrario no cumplíria con las condiciones para ser espacio vectorial.

Proposición 5.3.12. *Sea $\{S_i\}_{i\in I}$ una colección de subespacios de V entonces $\bigcap_{i\in I} S_i$ es un subespacio de V.*

Demostración. Como cada uno de los S_i es subespacio vectorial entonces la intersección de estos subespacios es diferente de vacío dado que por la Proposición 5.3.11 cada subespacio contiene al módulo de la adición. Ahora bien si $x, y \in \bigcap_{i\in I} S_i$ entonces para cada i se tiene $x, y \in S_i$ y por tanto $x + y \in S_i$ para todo $i \in I$ por tanto $x + y \in \bigcap_{i\in I} S_i$.
Si $x \in \bigcap_{i\in I} S_i$ entonces para cada i se tiene $x \in S_i$ y por tanto $\alpha x \in S_i$ para todo $i \in I$ y todo escalar α, por tanto $\alpha x \in \bigcap_{i\in I} S_i$. ■

Definición 5.3.13. Sean $\upsilon_1, \upsilon_2, \ldots, \upsilon_n$ elementos del espacio vectorial V. Se define

$$\langle \upsilon_1, \upsilon_2, \ldots, \upsilon_n \rangle = \{\alpha_1\upsilon_1 + \alpha_2\upsilon_2 + \ldots + \alpha_n\upsilon_n | \alpha_1, \alpha_2, \ldots, \alpha_n \in F\}.$$

Entonces $\langle \upsilon_1, \upsilon_2, \ldots, \upsilon_n \rangle$ es un espacio vectorial sobre F y es un subespacio de V llamado el ***subespacio generado*** por $\upsilon_1, \upsilon_2, \ldots, \upsilon_n$. Los vectores $\upsilon_1, \upsilon_2, \ldots, \upsilon_n$ es un ***conjunto generador*** del subespacio $\langle \upsilon_1, \upsilon_2, \ldots, \upsilon_n \rangle$. Si el espacio V es igual a $\langle \upsilon_1, \upsilon_2, \ldots, \upsilon_n \rangle$ se dice que V es ***finitamente generado***.

Hay espacios vectoriales finitamente generados (casi todos los que se estudian a nivel elemental) pero hay otros que no admiten un conjunto finito que lo genere.

Ejemplo 5.3.14. Sea el espacio vectorial de los $\mathbb{R}$ sobre $\mathbb{Q}$. Si $\{1, \frac{1}{\sqrt{n}}\}$ con $n \in N$, este conjunto infinito es generador de algun subconjunto de $\mathbb{R}$ pero no existe una combinación lineal de los elementos de este conjunto que exprese a $\sqrt{3}$. Ahora bien si agregamos al conjunto $\sqrt{2}$ el conjunto sigue siendo generador pero de igual forma no exite una combinación lineal de estos elementos que exprese a $\sqrt{3}$. Podríamos continuar así indefinidamente y simpre se encontrará algun $r \in \mathbb{R}$ que no se pueda expresar como combinación lineal de nuestro candidato a conjunto generador. Esta es una forma intuitiva de observar que V no admite un conjunto generador finito.

Ejemplo 5.3.15. Sea $V = F_n[x]$ el espacio de los polinomios de grado n que es un subespacio de todos los polinomios $F[x]$ (ver ejemplo 5.2.2), el conjunto $\{1, x, x^2, x^3, \ldots, x^n\}$ genera $V = F_n[x]$ por lo tanto este espacio vectorial está finitamente generado. Por otra parte el conjunto $\{1, x, x^2, x^3, \ldots, x^n, \ldots\}$ genera el espacio vectorial de todos los polinomios $F[x]$; si se tiene un conjunto finito de polinomios y N es el grado mayor de estos polinomios, por combinaciones lineales nunca se podrá generar un polinomio de grado mayor que N. Por lo tanto el espacio vectorial $F[x]$ no admite un conjunto generador finito.

Lema 5.3.16. *Si V es un espacio vectorial sobre F y $v_1, v_2, \ldots, v_n$ en V son linealmente independientes sobre F entonces todo elemento $v \in \langle v_1, \ldots, v_n \rangle$ tiene una representación única como*

$$v = \alpha_1 v_1 + \ldots + \alpha_n v_n$$

con $\alpha_1, \ldots, \alpha_n$ en F.

Demostración. Supongamos que $v \in \langle v_1, \ldots, v_n \rangle$ tiene dos representaciones $v = \alpha_1 v_1 + \ldots + \alpha_n v_n = \beta_1 v_1 + \ldots + \beta_n v_n$ con los α y los β en F. Esto implica que $(\alpha_1 - \beta_1)v_1 + \ldots + (\alpha_n - \beta_n)v_n = 0$; puesto que $v_1, \ldots, v_n$ son linealmente independientes sobre F, se concluye que $\alpha_1 - \beta_1 = 0, \ldots, \alpha_n - \beta_n = 0$, lo cual da por resultado la unicidad de la representación. ■

La definición que hemos dado de $\langle v_1, v_2, \ldots, v_n \rangle$ es la definicón de generado para un conjunto finito $v_1, \ldots, v_n$, pero se puede dar la definición para cualquier subconjunto de vectores como haremos a continuación.

Definición 5.3.17. S un subconjunto del espacio vectorial V, el generado de S es la intersección de todos lo espacios que contienen a S. Se nota $\langle S \rangle$.

$\langle S \rangle$ se forma haciendo todas las combinaciones lineales finitas de vectores de S. También se puede (y es fácil) demostrar que $\langle S \rangle$ es el menor subespacio que contiene a S.

Proposición 5.3.18. *Sea V un espacio vectorial, S subconjunto de V, $\langle S \rangle$ es el menor subespacio que contiene a S.*

Demostración. Es claro que es un subespacio puesto que por la Proposición 5.3.12 la intersección de subepacios es subespacio. Sea $\mathcal{F}$ la familia de subespacios que contiene a S. Supongamos que existe subespacio W talque $S \subset W$ luego W está en la familia $\mathcal{F}$ por lo tanto $\langle S \rangle = \bigcap \mathcal{F} \subset W$. ■

Para comparar espacios vectoriales es conveniente comparar conjuntos generadores minimos. Un conjunto S es un *conjunto generador mínimo* de V, si $V = \langle S \rangle$ y ningún subconjunto de S genera a V. Es fácil ver que si S es un conjunto generador minimo de V, entonces S es linealmente independiente. Así mismo si S es un conjunto generador de V que además es linealmente independiente entonces S es un conjunto generador mínimo de V. Realmente se tiene la siguiente proposición:

Proposición 5.3.19. *Sea Γ la familia de conjuntos linealmente independientes de V y sea Υ la familia de conjuntos generadores de V. Dichas familias cumplen las siguientes propiedades:*

1. *Tanto Γ como Υ estan ordenados por medio de la inclusión de conjuntos.*
2. *H es el maximal de Γ si y solo si H es el minimal Υ.*

Demostración. Para demostrar la primer propiedad debemos ver que los elementos de las familia tiene un orden por la relación de contenencia por lo tanto se debe verificar que cumpla con todas las propiedades de un conjunto ordenado. Sean $\gamma_1, \gamma_2, \gamma_3 \in \Gamma$ se tiene que:

1. $\gamma_1 \subset \gamma_1$ esto es cierto dado que todo conjunto es subconjunto de si mismo.
2. $\gamma_1 \subset \gamma_2$ y $\gamma_2 \subset \gamma_1$ entonces $\gamma_1 = \gamma_2$. Esto es también cierto dado que todo elemento de γ_1 esta en γ_2 por $\gamma_1 \subset \gamma_2$ de igual forma sucede con los elementos de γ_2, entonces los conjuntos $\gamma_1 = \gamma_2$.
3. $\gamma_1 \subset \gamma_2$ y $\gamma_2 \subset \gamma_3$ entonces $\gamma_1 \subset \gamma_3$. Claramente todos los elementos de γ_1 estan en γ_2 por ser subconjuntos y todos los elementos de γ_2 estan en γ_3 por ser subconjunto entonces todo elemento de γ_1 esta en γ_3 por lo tanto $\gamma_1 \subset \gamma_3$.

Para la segunda parte supongamos que H es un conjunto mínimo de generadores de V. Se probará que H es linealmente independiente. Sea

$$\alpha_1 v_1 + \ldots + \alpha_n v_n = 0$$

con $\alpha_i \in F$, $v_i \in H$. Si alguna $\alpha_j \neq 0$ entonces $v_j \in < H - \{v_j\} >$ entonces $< H - \{v_j\} > = V$ pero esto contradice el hecho que H es el minimo generador. En efecto, sea $y \in V =< H >$, donde existen $\beta_i \in F$, $y_i \in H$ tal que $y = \beta_1 y_1 + \ldots + \beta_m y_m$. Tenemos entonces que:

1. Si $y_i \neq v_j \ \forall i \ i = 1, 2, \ldots, m$ entonces $y \in < H - \{v_j\} >$ que es lo que se quiere demostrar.
2. Si $y_i = v_j$ para alguna $i = 1, \ldots, m$ entonces $y_i \in < H - \{v_j\} >$. Pero también

   $$y_s \in < H - \{v_j\} >$$

   para cualquier $s \neq i$. Así $y = \beta_1 y_1 + \ldots + \beta_m y_m \in < H - \{v_j\} >$.

Ahora probaremos que H es un maximal de la familia de los conjuntos linealmente independientes. Para esto se supondrá que $H \subset H_0$. Si existe $x \in H_0 - H$ entonces como H es generador y $x \in < H >$ y $H \cup \{x\}$ es linealmente dependiente por lo tanto H_0 es linealmente dependiente. ■

Definición 5.3.20. Un subconjunto B de un espacio vectorial V que es linealmente independiente y genera a V es una ***base***.

En el Ejemplo 5.3.4 se mostró que el conjunto

$$\left\{\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}, \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}, \begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}, \begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}\right\}$$

es un conjunto linealmente independiente en el espacio vectorial de las matrices 2×2 con coeficientes reales y además es un conjunto generador, puesto que cualquier matriz del espacio se puede expresar como combinación lineal de este conjunto por lo tanto este conjunto es una base.
En el espacio vectorial $\mathbb{C}$ sobre los $\mathbb{R}$ el conjunto $\{1, i\}$ es una base puesto que sus elementos son linealmente independientes y además cualquier $z \in \mathbb{C}$ se puede expresar como combinación lineal de estos dos elementos $z = a1 + bi$ donde $a, b \in \mathbb{R}$.

Definición 5.3.21. Sea V un espacio vectorial y B una base para V. El cardinal de la base B es la dimensión de V y se nota $|B| = \dim_F(V)$.

Ejemplo 5.3.22. La dimensión de las matrices 2×2 con coeficientes reales es 4. Puesto que la base que se mostró es un conjunto finito que tiene 4 elementos.

Ejemplo 5.3.23. El conjunto $\{1, i\}$ es una base para el espacio vectorial $\mathbb{C}$ sobre $\mathbb{R}$, por lo tanto $\dim_{\mathbb{R}}(\mathbb{C}) = 2$.

Ejemplo 5.3.24. La dimensión de $\mathbb{R}$ sobre $\mathbb{Q}$ es no numerable. Como se mencionó en el Ejemplo 5.3.14 $\mathbb{R}$ no admite un conjunto finito que lo genere. Sea $\{r_1, r_2, r_3, \ldots\}$ un conjunto numerable infinito de reales que son linealmente independientes sobre $\mathbb{Q}$; el conjunto

$$A_n = \{\alpha_1 r_1 + \alpha_2 r_2 +, \alpha_3 r_3 + \ldots + \alpha_n r_n \mid \alpha_1, \ldots, \alpha_n \in \mathbb{Q}\}$$

de todas la combinaciones lineales de $\{r_1, r_2, r_3, \ldots r_n\}$ es numerable dado que los $\alpha_i \in \mathbb{Q}$ y $\mathbb{Q}$ es numerable; ahora la posibles combinaciones lineales de $\{r_1, r_2, r_3, \ldots\}$ es la unión $A_1 \cup A_2 \ldots$ que es unión numerable de conjuntos numerables que en consecuencia es numerable. Pero el conjunto de los reales no es numerable, por lo tanto no es posible que $\{r_1, r_2, r_3, \ldots\}$ genere a cualquier $r \in \mathbb{R}$ y no puede ser una base.

Teorema 5.3.25. *Todo conjunto linealmente independiente de un espacio vectorial se puede extender a una base.*

Demostración. Sea V un espacio vectorial, Γ la famila de conjuntos linealmente independientes de V, S un conjunto linealmente independiente de V y $\Gamma_S = \{\gamma \in \Gamma \mid S \subset \gamma\}$; este conjunto está ordenado por la inclusión de conjuntos; tomemos una cadena $\mathcal{H}$ de Γ_S se demostrará que $\bigcup \mathcal{H} \in \Gamma_S$. Sean $h_1, h_2, \ldots, h_n$ elementos de $\bigcup \mathcal{H}$ donde cada $h_i \in H_i$ y los H_i son comparables dado $H_1, H_2, \ldots, H_n \in \mathcal{H}$. Como $\mathcal{H}$ es un conjunto totalmente ordenado, entonces existe un $k \in \{1, 2, \ldots, n\}$ tal que H_k contiene a $H_1, H_2, \ldots, H_n$, por tanto $h_1, h_2, \ldots, h_n \in H_k$ y como H_k es un conjunto linealmente independiente se cumple que:

$$\alpha_1 h_1 + \alpha_2 h_2 + \ldots + \alpha_n h_n = 0 \Rightarrow \alpha_1 = \alpha_2 = \ldots = \alpha_n = 0$$

por lo tanto $\bigcup \mathcal{H}$ es linealmente independiente, $\bigcup \mathcal{H} \in \Gamma_S$ y además $\bigcup \mathcal{H}$ es una cota superior para $\mathcal{H}$.

En virtud del Lema de Zorn el conjunto Γ_S tiene por lo menos un maximal que naturalmente es un conjunto linealmente independiente y por las propiedades de la familia de conjuntos linealmente independientes es un conjunto generador y por tanto es una base que contiene a S. ■

Como colorario de este resultado se tiene que:

Corolario 5.3.26. *Todo espacio vectorial admite una base.*

Por lo tanto se ha mostrado que cualquier conjunto linealmente independiente de un espacio vectorial se puede extender a una base y como se ha mencionado a lo largo de este trabajo este resultado será fundamental en el desarrollo de la demostración del $\mathbb{C}^* \cong S^1$.

5.4. Transformciones Lineales

Definición 5.4.1. Sean V, E espacios vectoriales. Una transformación lineal $T : V \to E$ es una correspondencia que asocia a cada elemento de $v \in V$ un elemento $T(e) = \{Ev \mid Ev \in E\}$ de modo que para cualesquiera $v, u \in E$ y $\alpha \in \mathbb{R}$ se cumple:

1. $T(u + v) = T(u) + T(v)$.
2. $T(\alpha V) = \alpha T(v)$.

Donde Ev es la imagen de v por medio de la transformación T.

Las transformaciones lineales son aplicaciones que preserva la suma y el producto por escalar.

Ejemplo 5.4.2. Sea $\mathbb{C}$ el espacio vectorial de los complejos y sea $\alpha \in \mathbb{R}$. Dada la transformación

$$T : \mathbb{C} \to \mathbb{C}$$

tal que a $z = a + bi$ le corresponde $T(z) = T(a + bi) = 0 + bi$, esta es una transformación lineal puesto que: Si $z_1 = a + bi, z_2 = c + di \in \mathbb{C}$ entonces

$$\begin{aligned}
T(z_1 + z_2) &= T((a + bi) + (c + di)) \\
&= T((a + c) + (b + d)i) \quad \text{por adición } \mathbb{C} \\
&= 0 + (b + d)i \quad \text{por definición de } T \\
&= (0 + bi) + (0 + di) \quad \text{por ley distributiva} \\
&= T(0 + bi) + T(0 + di) \quad \text{por definición de las imagenes de } T(z) \\
&= T(a + bi) + T(c + di) \quad \text{por definición de } T \\
&= T(z_1) + T(z_2).
\end{aligned}$$

Si $\alpha \in \mathbb{R}$ se debe ver que T respete el producto por un escalar.

$$\begin{aligned}
T(\alpha z_1) &= T(\alpha(a + bi)) \\
&= T(\alpha a + \alpha bi) \quad \text{por ley distributiva} \\
&= 0 + \alpha bi \quad \text{por definición de } T \\
&= \alpha(0 + bi) \quad \text{ley distributiva} \\
&= \alpha T(z_1) \quad \text{por definición de las imagenes de } T(z)
\end{aligned}$$

Por lo tanto la aplicación T es una transformación lineal.

Definición 5.4.3. Sea V, E espacios vectoriales, la transformación lineal $T : V \to E$ es es una biyección entre V y E entonces V y E son isomorfos.

Ejemplo 5.4.4. Sea $F_n[x]$ el espacio vectorial de los polinomios de grado menor o igual a n, entonces la transformación

$$T : F_n[x] \to \mathbb{R}^n$$

es un isomorfismo en donde a cada $T(\alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n) = (0, x, \ldots, x^n)$.

Proposición 5.4.5. *[4] Si B es una base de V, B' es una base de V y $f : B \to B'$ es una función biyectiva; entonces f puede extenderse de manera única a $F : V \to W$ con F función (isomorfismo).*

Demostración. Como B es una base para el espacio vectorial V entonces todo elemento de $v \in V$ se puede expresar como combinación lineal de B.

$$v = \alpha_1 b_1 + \ldots + \alpha_j b_j + \ldots + \alpha_n b_n$$

Como f es biyeción por lo tanto es uno a uno, se tiene que:

$$F(v) = \alpha_1 f(b_1) + \ldots + \alpha_j f(b_j) + \ldots + \alpha_n f(b_n)$$

Por ser f sobre se cumple que cada uno de los $f(v_i) \in B'$ es una imagen de v_i por lo tanto, es decir cada $f(v_i) = b'_j \in B'$ por lo tanto se tiene que:

$$\alpha_1 f(b_1) + \ldots + \alpha_j f(b_j) + \ldots + \alpha_n f(b_n) = \alpha_1(b'_1) + \ldots + \alpha_j(b'_j) + \ldots + \alpha_n(b'_n) = w$$

donde $w \in W$, es decir $F : V \to W$ es una extensión de f puesto que va de las bases a los espacio vectoriales. Además F es una función es una biyección por lo tanto $F : V \to W$ es un isomorfismo. ■

Se puede afirmar por este resultado y el Colorario 5.3.26, $T : V \to E$ es un isomorfismo entre espacios vectoriales de tal manera que a una base de V se la envía en una base de E. Recíprocamente, si una transformación lineal $T : V \to E$ lleva alguna base de V en una base de E entonces T es un isomorfismo.

Teorema 5.4.6. *Los espacios vectoriales $\mathbb{R} \times \mathbb{R}$ y $\mathbb{R}$ son isomorfos. Se puede construir el isomorfismo de tal manera que a $\{0\} \times \mathbb{Z}$ lo envía en $\mathbb{Z}$.*

Demostración. Comenzaremos por considerar el espacio vectorial de los reales $\mathbb{R}$ sobre el campo de los racionales $\mathbb{Q}$. Sea el conjunto unitario $\{1\}$ este conjunto es linealmente independiente sobre $\mathbb{Q}$ puesto que todo conjunto de un único elemento no nulo es linealmente independiente. Por el Teorema 5.3.25 podemos extender nuestro conjunto unitario a una base $\mathcal{B}$ de $\mathbb{R}$ sobre $\mathbb{Q}$ tal que $1 \in \mathcal{B}$
Sea el conjunto $\mathcal{B}^* = \mathcal{B} \times \{0\} \bigcup \{0\} \times \mathcal{B}$, éste es una base del espacio vectorial $\mathbb{R} \times \mathbb{R}$ sobre $\mathbb{Q}$, donde la multiplicación por escalar está dada por componentes, es decir, $q \cdot (r, s) = (qr, qs)$. Ahora bien, es claro que $\mathcal{B}^*$ es la unión de dos conjuntos disjuntos, cada uno de estos conjunto es equipotente con el conjunto infinito $\mathcal{B}$, por tanto $\mathcal{B}^*$ es equipotente a $\mathcal{B}$.

Sea pues $\phi : \mathcal{B}^* \to \mathcal{B}$ una correspondencia uno a uno que a la pareja $(0,1)$ la envía a 1. Esta biyección ϕ se puede extender de manera única a un isomorfismo $\Phi : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ de espacios vectoriales sobre $\mathbb{Q}$ por la Proposición 5.4.5, cuando son un isomorfismo de grupos. Si n es un entero, entonces

$$\Phi((0,n)) = \Phi(n.(0,1)) = n.\Phi((0,1)) = n.\phi((0,1)) = n1 = n.$$

Luego la imagen de $\{0\} \times \mathbb{Z}$ por medio Φ es $\mathbb{Z}$. ■

CAPÍTULO 6

CONSTRUCCIÓN DEL ISOMORFISMO

En el artículo de *Duffy* la demostración del isomorfismo que existe entre los complejos sin el cero y el círculo de radio uno ($\mathbb{C}^* \cong S^1$), se construye sin utilizar el teorema fundamental de grupos divisibles: "Todo grupo divisible es una suma directa de grupos isomorfos a $\mathbb{Q}$ o grupos $\mathbb{C}_{p^\infty}$" ; donde la demostración del isomorfismo de $\mathbb{C}^* \cong S^1$ es un resultado clásico de este teorema, para estos grupos multiplicativos. En cambio el autor del artículo emplea una de las consecuencias del lema de Zorn y elementos del algebra.

6.1. El isomorfismo ($\mathbb{C}^* \cong S^1$) como resultado del teorema de grupos divisibles

En la Sección 2.5 se estudio a $\mathbb{C}^*$, como grupo divisible y además se estudiaron algunos conceptos básicos de los grupos divisibles. Se ilustrará a continuación que grupo multiplicativo $\mathbb{C}_{p^\infty}$ es un grupo divisible, lo que permitirá entender y poder ejemplarizar más fácilmente el teorema estructural de grupos divisibles.

Lema 6.1.1. *Siendo p un número primo, $\mathbb{C}_p = \{z \in \mathbb{C} \mid z^p = 1\}$ es un grupo (ver seción 2.5.1) "casi divisible" puesto que para $n = 1, 2, \ldots, p-1$, la ecuación $x^n = z$ tiene solución en $\mathbb{C}_p$ para todo $z \in \mathbb{C}_p$.*

Demostración. Como ya se mostró $\mathbb{C}_p \in \mathbb{C}_{p^\infty}$, si $n = 1, 2, \ldots, p-1$ entonces n es primo relativo con p y por la Proposición 2.5.4 se obtiene el resultado. ■

Proposición 6.1.2. *El grupo multiplicativo $\mathbb{C}_{p^\infty}$ es un grupo divisible.*

Demostración. Por la definición de grupo divisible, se debe ver la ecuación $x^n = z$ tiene solución en el grupo $\mathbb{C}_{p^\infty}$ para todo elemento de $z \in \mathbb{C}_{p^\infty}$ y $n \in \mathbb{N}$. Como ya se vio en la Sección 2.4.2 todo número complejo tiene n raíces, en consecuencia todo elemento que se

tome de $\mathbb{C}_{p^\infty}$ tiene n soluciones en $\mathbb{C}$ para la ecuación, solo falta ver que una de estas n soluciones es la única solución y está en $\mathbb{C}_{p^\infty}$. Según el Lema 2.5.6 se tiene que $\mathbb{C}_{p^\infty} \subset (\mathbb{C}_{p^\infty})^q$ para q un número primo.
Si $q \neq p$ entonces $(q,p) = 1$ y por la Proposición 2.5.4 se cumple. En el caso que $p = q$ entonces es necesario mostrar que:

$$\mathbb{C}_{p^\infty} \subseteq [\mathbb{C}_{p^\infty}]^p$$

Si $z \in \mathbb{C}_{p^\infty}$ se cumple que $z^{p^n} = 1$, ahora bien si z es raíz de algun w entonces $w^p = z$ se tiene que $w \in \mathbb{C}_{p^\infty}$. Pero como z es raíz de w entonces $z^{p^n} = (w^p)^{p^n} = w^{p^{n+1}}$ por consiguiente $w \in \mathbb{C}_{p^\infty}$ ■

El teorema estructural de grupos divisibles asegura que todos se forman a partir de $\mathbb{Q}$ y $\mathbb{Z}_{p^\infty}$ con p primo, por intermedio de sumas directas. Aunque el interés no es demostrar este poderoso resultado para ilustrarlo antes es necesario denifir la suma directa de grupos.

Definición 6.1.3. Sea $\{A_i\}_{i\in I}$ una colección de grupos (aditivos); el producto $\prod_{i\in I}(A_i)$ es el grupo cuyos elementos son funciones

$$\prod_{i\in I}(A_i) = \{f : I \to \bigcup_{i\in I} A_i \mid \forall i \in I \ (f(i) \in A_i)\}$$

que se operan de manera natural es decir si $f, g \in \prod_{i\in I}(A_i)$ para cada $i \in I$ se tiene

$$(f+g)(i) = f(i) + g(i) \in A_i$$

Ejemplo 6.1.4. Para todo $i \in [0,1]$, sea $A_i = \mathbb{R}$; el producto $\prod_{i\in[0,1]} A_i$ es el grupo cuyos elementos son funciones en los reales

$$\mathbb{R}^{[0,1]} = \prod_{i\in[0,1]} A_i = \{f : [0,1] \to \mathbb{R} \mid \forall i \in [0,1] \mid f(i) \in \mathbb{R}\},$$

Al operar para cada par de funciones del producto como intiutivamente se puede pensar se operan naturalmente es decir si $f, g \in \prod_{i\in[0,1]} A_i$ para cada $i \in [0,1]$ se tiene

$$(f+g)(i) = f(i) + g(i) \in A_i.$$

Si $\{f : [0,1] \to \mathbb{R} \mid \ |f(x)| \leq x\}$ entonces los valores posibles de $f(x)$ estan en $[-x,x]$ entonces bajo la notación de producto este conjunto sería:

$$\prod_{i\in[0,1]} [-x,x] = \{f : [0,1] \to [-x,x] \mid \forall i \in [0,1] \mid f(i) \in [-x,x]\}.$$

Ejemplo 6.1.5. Para todo $i \in \mathbb{N}$, sea $\{A_i\}_{i\in N}$; el producto $\prod_{i\in\mathbb{N}} A_i$ es el grupo cuyos elementos son sucesiones

$$\prod_{i\in\mathbb{N}} A_i = \{f : \mathbb{N} \to \mathbb{R} \mid \forall i \in \mathbb{N} \ (f(i) \in \mathbb{R})\}.$$

Al operar para cada par de funciones del producto como intuitivamente se puede pensar se operan naturalmente es decir si $f, g \in \prod_{i\in\mathbb{N}}(A_i)$ para cada $i \in \mathbb{N}$ se tiene

$$(f+g)(i) = f(i) + g(i) \in A_i.$$

Este producto define el conjunto de todas las sucesiones de los reales.

Definición 6.1.6.

$$\bigoplus_{i\in I} A_i \leq \prod_{i\in I}(A_i).$$

en donde $\bigoplus_{i\in I} A_i = \{f \in \prod_{i\in I}(A_i) \mid f(i) \neq 0\}$ [1].

Ejemplo 6.1.7. Sea F el campo de todos los polinomios, sea $\phi : F[x] \to \bigoplus_{i\in\mathbb{N}} F$ donde para cada $p \in F$ se define $\phi(p(x)) = \phi(a_o + a_1x + a_2x^2 + \ldots + a_nx^n) = f$ con

$$f(i) = \begin{cases} a_i & \text{si } 0 \leq i \leq n, \\ 0 & \text{si } i > n, \end{cases}$$

como por definición $\bigoplus_{i\in N} F = \{f \in \prod_{i\in\mathbb{N}}(F) \mid f \neq 0\}$ entonces $f \in \bigoplus_{i\in\mathbb{N}} F$ resulta fácil ver que ϕ es un isomorfismo.

Teorema 6.1.8 (Teorema estructural de grupos divisibles)**.** *Todo grupo divisible es una suma directa de grupos isomorfos a* $\mathbb{Q}$ *o grupos* $\mathbb{C}_{p^\infty}$.

Tanto la demostración del teorema como su aplicación para ver estrictamente que $\mathbb{C}^*$ y S^1 son isomorfos, están fuera del alcance de este trabajo; sin embargo, se intentará ilustrar someramente cómo el anterior teorema plantea el isomorfismo de $\mathbb{C}^* \cong S^1$; se debe expresar a estos dos grupos como sumas directas de grupos isomorfos a $\mathbb{Q}$ o a grupos $\mathbb{C}_{p^\infty}$. Para ello veremos algunos ejemplos.

Ejemplo 6.1.9. Sabemos que $\mathbb{R}$ es divisible ¿cómo se aplica el resultado del teorema estructural de grupos divisibles? Se mostrará que $\mathbb{R}$ es una suma directa no numerable de $\mathbb{Q}$. Sea B una base (no numerable) del espacio vectorial $\mathbb{R}$ sobre $\mathbb{Q}$ (ver Ejemplo 5.3.24), es inmediato ver que $\mathbb{Q}r \cong \{rq \mid q \in \mathbb{Q}\}$ con $r \in B$ cuando se consideran los grupos aditivos. Aseguramos que

$$\mathbb{R} \cong \bigoplus_{r\in B} \mathbb{Q}r.$$

En efecto dado un elemento $x \in \mathbb{R}$ se le asocia la función $f_x : B \longrightarrow \bigcup Qr$ así: Como B es base existe una combinación lineal, es decir existen $r_1, r_2, \ldots r_n$ elementos de B y $q_1, q_2, \ldots, q_n$ racionales tales que

$$x = q_1r_1 + q_2r_2 + \ldots + q_nr_n$$

$$f_x(r) = \begin{cases} q_ir_i & \text{si } r = r_i, \\ 0 & \text{si } r \neq r_i \text{ para } i : 1, \ldots, n. \end{cases}$$

Es de rutina ver que esta asociación es un isomorfismo.

La pregunta natural que sigue después de este resultado es si P es el conjunto de números primos ¿a qué grupo es equivalente $\bigoplus_{p\in P} \mathbb{C}_{p^\infty}$?. Aunque no podemos demostrarlo afirmamos que $\bigoplus_{p\in P} \mathbb{C}_{p^\infty}$ es isomorfo al subgrupo de $\mathbb{C}^*$ consistente en todos los complejos de orden finito. Intentando visualizar esto presentamos el siguiente ejemplo.

Ejemplo 6.1.10. $\mathbb{C}_{2^\infty} \times \mathbb{C}_{3^\infty}$ es isomorfo al grupo multiplicativo de los complejos cuyo orden es de la forma 2^i3^j.

$\mathbb{C}_{2^\infty}, \mathbb{C}_{3^\infty} \in \mathbb{C}_{p^\infty}$ por la Definición de producto para grupos 6.1.3 y por una de las conclusiones para el producto de grupos (ver página 29), $\mathbb{C}_{2^\infty} \times \mathbb{C}_{3^\infty} \cong \mathbb{C}_{2^i3^j\infty}$.

[1] $\leq$ es la notación que se uso para subgrupos, ver Lema 2.3.1

6.2. Presentación del isomorfismo

El isomorfismo se presenta a partir de la relación que envía a $re^{i\theta}$ en el par $(\log r, \theta/2\pi + \mathbb{Z})$ con la ad ción como operación. Esta relación establece un isomorfismo entre $\mathbb{C}^* \approx \mathbb{R} \times \mathbb{R}/\mathbb{Z}$. La relación citada arriba es una función, donde los conjuntos de llegada y salida son estructuras ya conocidas.
Esta claro que la relación presentada arriba es una función, donde el conjunto de llegada es un subgrupo del plano cartesiano conformado por todas aquellas parejas tales que la primera componente es la funcíón $\log r$, la cual respeta las operaciones entre los conjuntos $(\mathbb{C}^*, \mathbb{R} \times \mathbb{R})$ como se vio en el Ejemplo 4.1.2. La segunda componente de cada pareja del conjunto de llegada está integrado por las clases laterales de $\mathbb{Z}$ en $\mathbb{R}$, es decir, $\mathbb{R}/\mathbb{Z}$ este es un resultado ya obtenido en el Ejemplo 4.2.8, además por el Ejemplo 4.2.7 este conjunto tiene estructura de grupo. Se puede afirmar entonces que $\mathbb{C}^* \approx \mathbb{R} \times \mathbb{R}/\mathbb{Z}$, este isomorfismo se plantea gracias a los resultados que se han obtenido durante este trabajo.
Ahora se revisará que $S^1 \approx \mathbb{R}/\mathbb{Z}$ con la multiplicación y adición como operaciones respectivamente. Como ya se estudio en la Sección 2.3 el conjunto S^1 es subgrupo $\mathbb{C}^*$; además, como se ilustró en el Ejemplo 4.2.8 las clases laterales de $\mathbb{Z}$ son equivalente a sumar angulos y además en el Ejemplo 4.2.5 se mostró cómo son las clases laterales de S^1. Por estos dos resultados y el Teorema 4.3.4 se cumple que $S^1 \approx \mathbb{R}/\mathbb{Z}$, es decir, S^1 se puede ver como el conjunto de rotaciones repecto al origen en el plano.
Lo que resta por hacer es mostrar que $\mathbb{R} \times \mathbb{R}/\mathbb{Z} \approx \mathbb{R}/\mathbb{Z}$ y para esto se necesitarán los siguientes tres resultados.

Proposición 6.2.1. *En un espacio vectorial, un conjunto linealmente independiente se puede se puede extender a una base.*

Este resultado se realizó detalladamente en el capítulo anterior (ver Proposición 5.3.25).

Proposición 6.2.2. *Si $\phi : G \to H$ es un isomorfismo de grupos y $A \leq G$, luego $\phi(A) \leq H$ y los dos grupos cocientes G/A y $H/\phi(A)$ son isomorfos.*

Demostración. Se mostrará primero que $\phi(A) \leq H$.
Sean $\phi(a_1), \phi(a_2) \in \phi(A)$ con $a_1, a_2 \in A$, se debe ver que $\phi(a_1)\phi(a_2) \in \phi(A)$ como $a_1a_2 \in A$ por ser A subgrupo, entonces $\phi(a_1a_2) \in A$. Dado que ϕ es un isomorfismo se tiene que $\phi(a_1a_2) = \phi(a_1)\phi(a_2) \in \phi(A)$. Para ver la existencia de los inversos se tiene que si $\phi(a) \in \phi(A)$ con $a \in A$, entonces por ser A subgrupo $a^{-1} \in A$ y por tanto $\phi(a^{-1}) = \phi(a)^{-1} \in \phi(A)$.
Se mostrará que $G/A \cong H/\phi(A)$. Sea la función $\beta : G/A \to H/\phi(A)$ tal que si $Ag \in G/A$ se define $\beta(Ag) = \phi(A)\phi(g)$.
Se verá que $\beta(Ag_1Ag_2) = \beta(Ag_1)\beta(Ag_2)$. Como ϕ es homomorfismo se tiene que:

$$\begin{aligned} \beta(Ag_1Ag_2) &= \beta(Ag_1g_2) = \phi(A)\phi(g_1g_2) = \phi(A)\phi(g_1)\phi(g_2) = \\ &= \phi(A)\phi(g_1)\phi(A)\phi(g_2) = \beta(Ag_1)\beta(Ag_2) \end{aligned}$$

Sólo falta mostrar que β es uno a uno y sobre. Para mostrar que es uno a uno debemos ver que si $\beta(Ag_1) = \beta(Ag_2)$ entonces $Ag_1 = Ag_2$ con $Ag_1, Ag_2 \in G/A$. Si $\beta(Ag_1) = \beta(Ag_2)$ entonces $\phi(A)\phi(g_1) = \phi(A)\phi(g_2)$ en consecuencia $\phi(g_1) \in \phi(A)\phi(g_2)$ por lo tanto existe

$a \in A$ tal que $\phi(g_1) = \phi(a)\phi(g_2) = \phi(ag_2)$ como ϕ es isomorfismo $g_1 = ag_2$ entonces $g_1 \in Ag_2$ por lo tanto $Ag_1 = Ag_2$.
Ahora se debe demostrar que para cada elemento $\phi(A)h$ que pertenece a $H/\phi(A)$ existe un elemento g de G tal que $\phi(A)h = \beta(Ag)$. Pero esto se cumple de manera inmediata dado que ϕ es sobre, en consecuencia para cualquier $h \in H$ existe un elemento $g \in G$ tal que $\phi(g) = h$ por lo tanto $\phi(A)h = \beta(Ag)$. ■

Proposición 6.2.3. *Si G, H son dos grupos con subgrupos A, B respectivamente, entonces $A \times B \leq G \times H$ y $(G \times H)/(A \times B) \cong G/A \times H/B$.*

Demostración. Sea

$$\varphi : G \times H \longrightarrow G/A \times H/B$$

un homomorfismo tal que a cada $(g, h) \in G \times H$ lo envía en (Ag, Bh). Es fácil ver que φ es un homomorfismo sobreyectivo, donde el $\ker(\varphi) = A \times B$ entonces por el Teorema 4.3.2 se tiene que $(G \times H)/(A \times B) \cong G/A \times H/B$. ■

Las dos proposiciones anteriores son validas también para grupos no abelianos, siempre y cuando los subgrupos mencionados en cada una de las proposiciones sean subgrupos normales[2].
Para establecer el isomorfismo entre $\mathbb{C}^* \cong S^1$ se mostrarán unos isomorfismos enlazados, los cuales están apoyados sobre gran parte de los resultados que se han venido obteniendo al transcurso de este trabajo y en especial las Proposiciones 6.2.1, 6.2.2, 6.2.3. Lo que se debe ver es:

$$\mathbb{C}^* \cong \mathbb{R}^+ \times \mathbb{R}/\mathbb{Z} \cong \mathbb{R} \times \mathbb{R}/\mathbb{Z} \cong \frac{\mathbb{R} \times \mathbb{R}}{\{0\} \times \mathbb{Z}} \cong \mathbb{R}/\mathbb{Z} \cong S^1.$$

Proposición 6.2.4. *$\mathbb{C}^*$ es isomorfo a $\mathbb{R}^+ \times \mathbb{R}/\mathbb{Z}$.*

Demostración. Como ya se mencionó al inicio de esta sección por los resultados de los Ejemplos 4.2.8 y 4.2.5 $\mathbb{R}/\mathbb{Z} \cong S^1$ y ahora bien en el Ejemplo 4.1.9 se mostró que $\mathbb{C}^* \cong \mathbb{R}^+ \times S^1$ pero como $\mathbb{R}/\mathbb{Z} \cong S^1$ entonces $\mathbb{C}^* \cong \mathbb{R}^+ \times \mathbb{R}/\mathbb{Z}$. ■

Proposición 6.2.5. *$\mathbb{R}^+ \times \mathbb{R}/\mathbb{Z}$ es isomorfo a $\mathbb{R} \times \mathbb{R}/\mathbb{Z}$.*

Demostración. El isomorfismo $\mathbb{C}^* \cong \mathbb{R} \times \mathbb{R}/\mathbb{Z}$ se plantea a partir de la relación que envía $(re^{i\theta})$ en la pareja $(\log r, \theta/2\pi + \mathbb{Z})$, ahora bien como para todo $r \in \mathbb{R}$ se tiene que $\log r \in \mathbb{R}^+$ pero como se mostró en el Ejemplo 4.1.2 $\log(xy) = \log(x) + \log(y)$, es decir la función respeta las operaciones entre $\mathbb{R}^+$ y $\mathbb{R}$ por lo tanto por medio de esta relación se puede afirmar que $\mathbb{R}^+ \times \mathbb{R}/\mathbb{Z} \cong \mathbb{R} \times \mathbb{R}/\mathbb{Z}$. ■

Proposición 6.2.6. *$\mathbb{R} \times \mathbb{R}/\mathbb{Z}$ es isomorfo a $\frac{\mathbb{R} \times \mathbb{R}}{\{0\} \times \mathbb{Z}}$.*

Demostración. Como el Ejemplo 4.2.8 presenta las clases de equivalencia de $\mathbb{Z}$ en $\mathbb{R}$, es decir el grupo $\mathbb{R}/\mathbb{Z}$, y como las clase de equivalencia del conjunto $\{0\}$ en $\mathbb{R}$ es es mismo $\mathbb{R}$ por el Teorema 4.3.4 se tiene que $\mathbb{R}/\{0\} \cong \mathbb{R}$. El conjunto $\{0\} \times \mathbb{Z}$ es subgrupo de $\mathbb{R} \times \mathbb{R}$ donde por cada uno de los subgrupos que conforman en producto son el nucleo de un isomorfismo por lo tanto y gracias al resultado de la Proposición 6.2.3 se tiene que $\mathbb{R} \times \mathbb{R}/\mathbb{Z} \cong \mathbb{R} \times \mathbb{R}/\{0\} \times \mathbb{Z}$. ■

[2]Un subgrupo A de G es un subgrupo normal si todas las clases laterales a izquierda y derecha son iguales.

Proposición 6.2.7. $\frac{\mathbb{R}\times\mathbb{R}}{\{0\}\times\mathbb{Z}}$ *es isomorfo a* $\mathbb{R}/\mathbb{Z}$.

Demostración. En el Teorema 5.4.6 se muestra que $\Phi : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ es un isomorfismo de espacios vectoriales, pero como todo espacio vectorial tiene inmerso un grupo por lo tanto Φ es un isomorfismo de grupos donde la imagen de $\{0\} \times \mathbb{Z}$ atravez de Φ es $\mathbb{Z}$, y por la Proposición 6.2.2, se tiene que $\frac{\mathbb{R}\times\mathbb{R}}{\{0\}\times\mathbb{Z}} \cong \mathbb{R}/\mathbb{Z}$. ■

Por lo tanto podemos concluir que $\mathbb{R} \times \mathbb{R}/\mathbb{Z} \cong \mathbb{R}/\mathbb{Z}$, es decir que $\mathbb{C}^* \cong S^1$. Terminando entonces con la construcción de isomorfismo.

CONCLUSIONES

Durante el desarrollo de este trabajo, se estudiaron algunos grupos abelianos y algunos otros conceptos indispensables para poder lograr el objetivo principal: demostrar el isomorfismo que existe entre $\mathbb{C}^*$ y S^1. Mientras se construía el trabajo se obtuvieron resultados significativos tales como poder ver gran que parte de los grupos abelianos o caracterizaciones de estos se encuentran en el grupo de los complejos.

La importancia de ciertas propiedades estructurales como lo son el orden de los elementos de un conjunto y producto directos de grupos cíclicos, los cuales fueron fundamentales para ilustrar al grupo $\mathbb{C}_{p^\infty}$ como grupo divisible. Este resultado no solo fue importante en este trabajo para la ilustración de este teorema sino que se mostró la relación que existe entre el producto interno y el producto directo de grupos abelianos y por medio de estos elementos fue posible mostrar el isomorfismo entre los conjuntos $\mathbb{R} \times \mathbb{R}^+$ y $\mathbb{C}^*$.

Dentro de las propiedades estructurales que se estudiaron también se destaca los grupos cocientes y los isomorfismos que estos permiten generar, junto a los teoremas de homomorfismo para grupos. Puesto que gracias a estos se mostró que $S^1 \cong \mathbb{R}/\mathbb{Z}$, este isomorfismo permitió ver que multiplicar elementos de S^1 es equivalente a sumar ángulos; estos isomorfismos fueron piezas claves para lograr el objetivo principal la demostración de $\mathbb{C}^* \cong S^1$.

Otro resultado que se presentó en este trabajo es el isomorfismo que existe entre los espacios vectoriales $\mathbb{R} \times \mathbb{R} \cong \mathbb{R}$, en su demostración se utilizaron no solo elementos del álgebra lineal sino una de las más importantes herramientas de la teoría de conjuntos el Lema de Zorn. Pero este lema no solo es interesante por su demostración sino que al restringir el isomorfismo de los espacios vectoriales a los grupos abelianos inmersos en ellos se obtiene un isomorfismo entre los grupos aditivos, este resultado es clave en el desarrollo del objetivo principal de este trabajo. Generalizando la demostración de $\mathbb{R} \times \mathbb{R} \cong \mathbb{R}$ se puede ver fácilmente que si V es un espacio vectorial infinto dimensional entonces $V \times V \cong V$. La pregunta natural que surge es ¿será posible mostrar el isomorfismo de los grupos abelianos inmersos en espacios vectoriales infinito dimensionales $V \times V$ y V sin tener que usar la estructura de espacio vectorial? Un resultado que aparentemente sería fácil de obtener es mostrar que $\mathbb{Q} \times \mathbb{Q} \cong \mathbb{Q}$ pero lamentablemente no se cuentan con los elementos suficientes para poder afirmarlo o refutarlo.

Además tambien se ilustró como apartir de la suma directa de grupos es posible construir isomorfismo conocidos o estructuras interesantes como la que se mostró al final del trabajo al mostrar las sucesiones como suma directa de funciones en los naturales e ilustrar la representación del grupo $\mathbb{C}$ como suma directas de $\mathbb{C}_{p^\infty}$ y $\mathbb{Q}$

BIBLIOGRAFÍA

[1] Duffy, L. Richard, *An elementary proof of the isomorfismo* $\mathbb{C}^* \simeq S^1$, The American mathematical monthly, Vol 90 Number, 1983, p. 201.

[2] Fraleigh J., *Algebra Abstracta: primer curso*, Addison Wesley, Iberoamericana, 1987.

[3] Churchill, Ruel V., *Variáveis complexas e suas aplicações*, MacGraw Hill,Brasil, 1975, p.1-17.

[4] Herstein I.N., *Algebra moderna*, F. Trillas S.A., México, 1970, Cap 2.

[5] Dean Richard A., *Elements of Abstract Algebra*, John Wiley An Sons Inc, New York, 1966, p 182.

[6] Marshall Hall, *Teoría de los grupos*, Ingramex S.A., México, 1969, p.208-p.209.

[7] Muñoz Quevedo, José M.*Introducción a la teoría de conjuntos*, Universidad Nacional de Colombia, Bogotá, 1994, Cáp. 7.

[8] Macho Stalder, Marta, *La paradoja de Banach- Tarski: como construir el sol apartir de un guisante*,Unibertsitatea, Universidad del país Vasco- Euskal Herriko, 2002-2003, p.106-p.109. Disponible en el sitio web "http://www.ehu.es/ mtwmastm/Datos.html"