GRUPOS CÍCLICOS Y ALGUNAS APLICACIONES

SANDRA YANETH ALMEIDA VELANDIA

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE MATEMÁTICAS
BUCARAMANGA
2006

GRUPOS CÍCLICOS Y ALGUNAS APLICACIONES

SANDRA YANETH ALMEIDA VELANDIA

Monografía presentada como
requisito para optar al título
de *Licenciada en Matemáticas*

Rafael Antonio Aponte Carvajal
Director

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE MATEMÁTICAS
BUCARAMANGA

2006

A mi familia quienes son la esencia de mi ser, a mis amigos quienes crecieron junto a mi en esta etapa de mi vida y a mis profesores de matemáticas fuente de mis conocimientos.

AGRADECIMIENTOS

- A *Dios* por darme la vida y la fortaleza para alcanzar mis metas y sueños.
- A *mis padres Samuel y Virginia, a mis hermanos Fabio, Armando y Cristian* por su esfuerzo, sacrificio y compañía, por su ejemplo de constancia y dedicación, por su confianza y su amor.
- A *Josué González Jaramillo* por creer en mi, por devolver mis sueños y proyectos, por enseñarme a crecer, por su compañía, su cariño, sus dones y talentos que desinteresadamente compartió conmigo.
- A mi director *Rafael Antonio Aponte Carvajal* por su confianza y respaldo, por su amistad.
- A *Willy* por su amistad, su compañía, por ser un pilar no solo en mi carrera sino en mi vida.
- A mis amigos quienes fueron cómplices de momentos inolvidables, *Mauro, Caro, Luce, Arturo, Lili, Victor, Fercho, Tilson* y todos aquellos que hicieron de mi vida universitaria una experiencia maravillosa.
- A *mis profesores de la Escuela De Matemáticas* por sus enseñanzas, a *Nubia y Rosalba* secretarias de la Escuela de Matemáticas por su espíritu de colaboración.

TITULO: GRUPOS CÍCLICOS Y ALGUNAS APLICACIONES[*]

AUTOR: ALMEIDA VELANDIA SANDRA YANETH[**]

PALABRAS CLAVES: Grupos cíclicos, grupos localmente cíclicos, redes distributivas, cristalografía .

DESCRIPCIÓN

En esta monografía se analizan ciertas propiedades de los **grupos cíclicos**, enriquecidos en un teorema llamado **Clasificación de los grupos cíclicos**. Los Grupos cíclicos se representan en dos grandes grupos según su orden, el grupo $(\mathbb{Z}, +)$ y $(\mathbb{Z}_n, +)$, todos los demás grupos son isomorfos a estos dos. Aunque los grupos cíclicos aparentemente no tienen mucha utilidad y es un tema poco tratado, en esta monografía se pretende divulgar, analizar y explorar las propiedades de estos grupos y su aplicabilidad en otra rama de la matemática y de la ciencia.

El trabajo consta de cuatro capítulos: Historia de la teoría de grupos e historia de los grupos cíclicos. El segundo capítulo Preliminares. En el tercer capítulo se presentan los grupos cíclicos, algunas propiedades básicas y ejemplos, al final de este capítulo se muestra la relación que existe entre los grupos cíclicos de orden infinito con $(\mathbb{Z}, +)$ y los de orden finito con $(\mathbb{Z}_n, +)$. El cuarto capítulo trata sobre las aplicaciones de tales grupos en las redes distributivas y la cristalografía, se dan algunos ejemplos y la tabla de clasificación de los grupos cíclicos de orden n.

Las redes distributivas permiten mostrar que aunque un grupo no sea cíclico se puede relacionar con estos, se observa la utilidad de tales grupos cumpliendo así uno de los objetivos de está monografía. Cuando hablamos de cristalografía se hace un comentario a grandes rasgos la utilidad de los grupos cíclicos de orden n en otras áreas de la ciencia. Cabe aclarar que estas dos aplicaciones no son las únicas que se tienen con respecto a los grupos cíclicos.

---

[*] Monografía

[**] Facultad de Ciencias. Escuela de matemáticas. Director: Rafael Antonio Aponte Carvajal.

TITLE: CYCLIC GROUPS AND SOME APPLICATIONS [*]

AUTHOR: ALMEIDA VELANDIA SANDRA YANETH[**]

KEY WORDS: Cyclic groups, locally cyclic groups, distributing nets, crystallography.

DESCRIPTION

In this monograph it is analyzed some properties of the **cyclic groups** enrich in a theorem called **Classification of the cyclic groups**. The cyclic groups are represented in two big groups according to their order, the $(\mathbb{Z}, +)$ y $(\mathbb{Z}_n, +)$ group, all the other groups are isomorphs to these two ones. Although the cyclic groups don't apparently have much utility and it is a theme not very much discussed, in this monograph it is pretended to disclose, analyze and explore the properties of these groups and their applicability in another field of the mathematics and the science.

The work consists of four chapters: History of the theory of groups and history of the cyclic groups. The second chapter Preliminaries. In the third chapter, it is presented the cyclic groups, some basic properties and examples, at the end of this chapter it is showed the relation that exists between the cyclic groups of infinitive order with $(\mathbb{Z}, +)$ and the groups of finite order with $(\mathbb{Z}_n, +)$. The fourth chapter talks about applications of these groups in the distributing nets and the crystallography, it is given some examples and the classification table of the cyclic groups of n order.

The distributing nets let to show that although a group is not cyclic, it can be related to these, is observed the utility of such groups fulfilling in this way one of the objectives of this monograph. When we talk about crystallography it is made a comment of the utility of the cyclic groups of n order in other areas of the science. It is important to clarify that these two applications are not the only ones that we have with respect to the cyclic groups.

---

[*] Monograph

[**] Faculty of Sciences. School of Mathematics. Director: Rafael Antonio Aponte Carvajal.

CONTENIDO

INTRODUCCIÓN

A través de la historia se han construido conceptos que se convierten en herramienta principal para la producción de conocimientos, uno de estos conceptos es el de grupo, introducido por Galois, dando origen a la teoría de grupos.
Durante los siglos XIX y XX la teoría de grupos se ramificó, creando el núcleo del álgebra actual. Ella se compone de una serie de teorías: los grupos finitos, los grupos discretos infinitos, entre otros. Aparecen así, los grupos cíclicos muy conocidos en nuestro medio, que al igual que las otras teorías de los grupos, penetran en una serie de disciplinas matemáticas tales como el álgebra, la mecánica, y otras, y además, en sus aplicaciones, dejando ver su gran utilidad y la de las matemáticas en general.

Este trabajo se presenta dividido en cuatro capítulos distribuidos de la siguiente manera: el primer capítulo contiene un recuento histórico sobre los grupos cíclicos, cabe anotar que no es extenso debido a la poca información sobre el origen de dichos grupos; en el segundo capítulo se presentan los preliminares, es decir, conceptos, definiciones, teoremas y resultados necesarios para el desarrollo del trabajo; en el tercer capítulo se hace un tratamiento formal de los grupos cíclicos, base de este trabajo; por último se muestran dos aplicaciones de estos grupos como son las redes distributivas y los grupos localmente cíclicos y aplicaciones en la cristalografía respectivamente.

CAPÍTULO 1

HISTORIA DE LOS GRUPOS CÍCLICOS

En este capítulo inicial se presentará una breve reseña histórica de los grupos cíclicos que nos permitirá entender la aparición de tales grupos. La primera sección se dedicara a un breve resumen de la aparición de la teoría de grupos de cuya clasificación nacen los grupos cíclicos.

La segunda sección se ocupa de los grupos cíclicos, su relación con los grupos abelianos, y aunque su reseña histórica se encuentre restringida a los aspectos mas importantes de su aparición se tratara de proporcionar una idea clara de la importancia de los grupos cíclicos a través de la historia. Los datos históricos existentes sobre estos grupos son escasos

1.1. Historia de la teoría de grupos

La historia del álgebra comienza en el antiguo Egipto y Babilonia, donde se resolvieron ecuaciones lineales y cuadráticas, así como las ecuaciones indeterminadas con varias

incógnitas.

Los matemáticos alejandrinos Heron (C.20-62 d.C) y Diofanto (fl.siglo III d.C.) continuaron la tradición egipcia y babilónica. Tradición que tubo acogida en el mundo islámico donde se llamo ciencia de reducción y equilibrio. En el siglo IX, el matemático Al-Jawarizmi (C.780-C.835) escribió uno de los primeros libros árabes del álgebra, una presentación sistematizada de la teoría fundamental de ecuaciones donde se incluían ejemplos y demostraciones. A finales de este siglo, el matemático egipcio Abu Kamil enunció y demostró las leyes fundamentales e identidades del álgebra y resolvió problemas tales como encontrar x, y, z que satisficieran $x + y + z = 10$ $x^2 + y^2 = z^2$ y $xz = y^2$.
En la edad media los matemáticos árabes desarrollaron el álgebra fundamental de los polinomios sin utilizar símbolos modernos (álgebra que incluía la multiplicación , la división y la extracción de raíces cuadradas de polinomios, y el conocimiento del teorema del binomio). El matemático, poeta y astrónomo persa Omar Jayyan (Khayyam (C.1050-1122)) mostró cómo expresar raíces de ecuaciones cúbicas utilizando los segmentos obtenidos de la intersección de secciones cónicas, sin encontrar una fórmula para dichas raíces. A inicio del siglo XIII, el matemático italiano Leonardo Fibonacci (C.1170-C.2140) encontró una aproximación cercana a la solución de la ecuación cúbica $x^3 + 2x^2 + Cx = d$.

A principios del siglo XVI los matemáticos italianos Scipiene del Ferro, Tartaglia (Niccoló Fontana C1500-1557) y Gerdamo Cardano (1504-1576) resolvieron la ecuación cúbica general en función de las constantes que aparecen en la ecuación. Ludovico Ferrari, alumno de Cardano, encontró la solución exacta de la ecuación de cuarto grado y, en consecuencia, algunos matemáticos de siglos siguientes iniciaron la búsqueda de la fórmula de las raíces de quinto grado y grados superiores. Búsqueda que generó los primeros trabajos sobre *la teoría de grupos* a fines del siglo $XVIII$.

En los tiempos de Carl Friedrich Gauss, el álgebra se encontraba ya en su etapa moderna. El centro de atención iba de las ecuaciones polinómicas al estudio de la estructura de sistemas matemáticos abstractos, cuyos axiomas se basaban en el comportamiento de objetos matemáticos, como los números complejos encontrados por matemáticos que habían estudiado las ecuaciones polinómicas. Los grupos comenzaban como sistemas de permutaciones de raíces de polinomios, pero evolucionaron para llegar a ser uno de los

más importantes conceptos unificadores de las matemáticas en el siglo XIX.

En 1770-1771 el matemático frances Joseph Louis Lagrange (1736-1813) examinó de manera minuciosa y crítica las soluciones existentes de las ecuaciones de segundo, tercero y cuarto grado, a tal punto que se dio cuenta que en cada caso la solución es reducible a la de una ecuación de grado menor donde las raíces son funciones lineales de las raíces de la ecuación dada, y las raíces de la unidad. Aparentemente se tenía un método universal para la solución de dichas ecuaciones. Pero al aplicar su reducción a la ecuación general de quinto grado, Lagrange obtuvo una de sexto grado, resultado que se convirtió en una poderosa muestra de que es imposible obtener una solución por medio de radicales; Lagrange había encontrado el virus de la teoría de los grupos de permutaciones.
Con este descubrimiento, Lagrange dio el primer paso hacía la teoría general de los grupos, paso con gran importancia para las matemáticas, mucho más que el haber resuelto por completo la teoría de ecuaciones algebraicas.

El matemático suizo Leonhard Euler (1707-1783) encontró resultados que no son ajenos a los grupos, por ejemplo la descomposición de un grupo conmutativo en subgrupos o relaciones entre el orden de un subgrupo y el grupo madre.

Los grupos de permutaciones insinuaban los grupos infinitos discontinuos, y por último el concepto de grupo entró en el análisis y en la geometría gracias a Marios Sophus Lie en 1870-80 con el invento de los grupos continuos. Con la invarianza, íntimamente ligada al concepto de grupo, la teoría de grupos en el siglo XIX transformó y unificó partes de las matemáticas que estaban muy separadas, dejando al descubierto analogías no sospechables de estructura en diferentes teorías. Sin embargo Lagrange no admitió los grupos, aunque obtuvo los equivalentes de algunas de las propiedades más sencillas de los grupos.

A principios del siglo XIX el matemático noruego Niels Henrik Abel (1802-1829) comenzó por estudiar la ecuación de quinto grado y, al tratar de hallar la solución general, demostró que era imposible resolverla por métodos algebraicos. Realizó importantes investigaciones sobre funciones elípticas. Una importante clase de funciones trascendentales se denomina (después de su descubrimiento, en su honor) como ecuaciones, grupos

y cuerpos abelianos.

El matemático August Ferdinard Möbius dio, desde la segunda década del siglo, una clasificación de la geometría, notando la existencia de propiedades invariantes bajo un grupo particular que permitían definir una geometría particular. Sin embargo, no llegó a comprender o construir el concepto de grupo.

En 1846 se conoció la mayor parte de los escritos de Evariste Galois (1811-1832);inventor del término grupo, gracias a las obras de Joshep Liouville y Jules Tannery, en estos escritos ya se entreveía la idea de cuerpo desarrollado más tarde por Riemann y Richard Dedekind, y que Galois introduce con motivo de los imaginarios de Galois. Es en estos escritos donde aparecen por primera vez las propiedades más importantes de la teoría de grupos que convierten a Galois en su cabal fundador.

Desde 1854 el matemático británico Arthur Cayley (1821-1895) había publicado dos artículos que contenían la definición abstracta de grupo y mostraba que las matrices y los cuaterniones son grupos. Dedicó más tiempo a este asunto hasta 1878 cuando publicó su libro *The theory of groups*, donde mostraba cómo todo grupo finito se puede representar como un grupo de permutaciones.

Anteriormente se mencionó que la noción de grupo estaba ya insinuado en los trabajos de Lagrange, Gauss, Abel, igual que en los trabajos de Ruffini, Augustin Louis Cauchy y Arthur Cayley, pero es Galois quien muestra una idea clara de la teoría general de grupos con las nociones de subgrupo y de isomorfismo.

Betti, fue el primero en probar que el grupo de Galois asociado a una ecuación era el grupo de permutaciones.
Aunque Joseph Liouville publico los trabajos de Galois, en 1846, y reconoció su relación con los trabajos sobre permutaciones realizados por Cauchy, no puso énfasis en el concepto clave de grupo. Por eso, no es sino hasta que Jordan subraya este concepto en artículos en 1865, 1869 y 1870 (define isomorfismo en grupo de permutaciones).

El punto histórico decisivo se estableció con Felix Klein que utilizó el concepto de forma

central para clasificar geometrías. Otros matemáticos que contribuyeron a la teoría de grupos fueron Hölder, Frobenius y Von Dyck.

1.2. Historia de los grupos cíclicos

Como se dejo ver en la sección 1.1, aún a principios del siglo XIX, el problema central del álgebra seguía siendo el encontrar las formulas para resolver ecuaciones polinómicas de grado superior a cuatro. Problema al cual se dedicaron notables trabajos como los de Lagrange y Vandermonde, enfocándolos adecuadamente hacia la teoría de grupos y de cuerpos.

Ruffini en su Teoría general *delle equazioni* (1799), hablaba de permutación y usaba la propiedad clausurativa, y diferenciaba entre *grupos cíclicos* y no cíclicos llamados de otra manera.

Paolo Ruffini (1765-1822) intento demostrar que la ecuación de quinto grado, llamada *quíntica*, no tenia solución; pero no lo consiguió. Cauchy apreció el trabajo de Ruffini, pero es el noruego Niels Henrik Abel (1802-1829) el que después de haber creído que había solucionado el problema de la quíntica, se da cuenta del error y demuestra en 1825 que esta ecuación no tiene solución por medio de radicales (proceso utilizado por Ruffini).
La mente prodigiosa de Abel es reflejada en sus trabajos, por esto en su memoria se destaca la indagación de las condiciones para la solución algebraica de las ecuaciones de quinto grado, introducción al trabajo de Evariste Galois donde sentó las bases de su teoría de ecuación mediante los grupos. Abel investigó la estructura de los grupos conmutativos (hoy conocidos como grupos abelianos, en su honor) y mostró que tales grupos son producto de *grupos cíclicos*.

En 1861, Mathieu construyó cinco curiosos grupos simples de permutaciones, la lista de los grupos finitos simples conocidos se reducía a los *grupos cíclicos* de orden primo, los grupos de permutaciones pares, los grupos llamados "de tipo Lie"(análogos finitos de los grupos de Lie) y los cinco grupos de Mathieu (esporádicos).

No se sabe con exactitud quien introdujo el término cíclico, pero al parecer fue Ruffini quien los trabajo por primera vez y en forma amplia, seguido de Abel quien centro su atención en los grupos cíclicos de orden finito y Mathie con sus grupos simples. En la actualidad son utilizados para el estudio de importantes problemas de la física y la química, referimos al lector para un tratamiento mas amplio de tales problemas a [12] y [15].

CAPÍTULO 2

PRELIMINARES

En este capítulo se recopilan los conceptos y resultados que usaremos en los siguientes capítulos. Es importante aclarar que no se incluyen demostraciones de tales resultados puesto que se han estudiado detalladamente en los cursos de álgebra moderna, álgebra lineal, análisis matemático entre otros. Además se establece la notación y terminología utilizada en la monografía.

2.1. Nociones preliminares

No se pretende ofrecer un desarrollo riguroso de los conceptos a tratar en este capítulo, sino establecer el lenguaje que se usara en el resto del libro; por ello, algunas de las definiciones de este capítulo serán un tanto vagas, pues se prefiere un tratamiento intuitivo y rápido sobre uno completo y riguroso pues su aplicación podría resultar un tanto excesiva para nuestro propósito.

Un ejemplo de esto es la definición de conjunto. Un conjunto es cualquier colección definida de objetos, elementos, acompañados de una propiedad que determina la pertenencia o no , de un elemento al conjunto. Un conjunto se describe como $A = \{x : x \ satisface \ P\}$. Si el conjunto A no tiene ningún elemento se denomina vacío y se denota $\emptyset$.

Un conjunto A se dice subconjunto de otro B si $A \subseteq B$ o $B \subseteq A$, es decir, $A \subseteq B$ si y solo si para todo elemento x de A, x es elemento de B. Dos conjuntos son iguales cuando cumplen $B \subseteq A$ y $A \subseteq B$.
La unión de A y B se define como $A \cup B = \{x : x \in A \vee x \in B\}$ y la intersección como $A \cap B = \{x : x \in A \wedge x \in B\}$. Es claro que $A \subseteq A \cup B$, $B \subseteq A \cup B$, $A \cap B \subseteq A$ y $A \cap B \subseteq B$.

Definición 2.1.1 (Conjunto parcialmente ordenado). Un *conjunto parcialmente ordenado* es un sistema A de elementos en el que está definida una relación $a \supseteq b$ (se lee a contiene a b) para algunos pares de elementos de A tales que:

- $a \supseteq a$.
- Si $a \supseteq b$ y $b \supseteq c$, entonces $a \supseteq c$.
- Si $a \supseteq b$ y $b \supseteq a$, entonces $a = b$.

Definición 2.1.2 (Cota superior y cota inferior). Una *cota superior* de un subconjunto B de un conjunto A parcialmente ordenado es un elemento a de A tal que $a \supseteq b$ para todo b de B. Análogamente, una *cota inferior* de un subconjunto B es un a' tal que $b \supseteq a'$ para todo b de B.

Definición 2.1.3 (Supremo e ínfimo). Un *supremo* (sup) de un subconjunto B de A es un elemento a tal que:

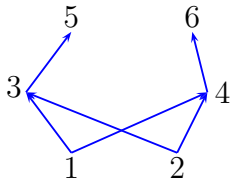
- a es una cota superior de B,
- Si c es una cota superior de B, entonces $c \supseteq a$.

Análogamente, un *ínfimo* (inf) de un subconjunto B es un b tal que:

- b es una cota inferior de B,
- Si c es una cota superior de B, entonces $b \supseteq c$.

Ejemplo 2.1.1. 1. Sea A un conjunto de elementos 1, 2, 3, 4,5, 6, donde la relación de inclusión está dada en la figura 2.1, $x \supseteq y$ si x está sobre y, y conectado a él o si $x = y$. Aquí el subconjunto que está formado por 3 y 4 no tiene ninguna cota superior y tiene dos cotas inferiores que son 1 y 2, pero ningún ínfimo.

Figura 2.1: Un conjunto parcialmente ordenado



2.1.1. Funciones

Definición 2.1.4 (Función). Sea $f : A \longrightarrow B$, f es *función* si a todo elemento de A le es asignado uno y solo uno de B. Es decir, f es una función si y solo si:

- $\forall a \in A, \exists\, b \in B : f(a) = b$.
- $f(a) = b \wedge f(a) = c \Longrightarrow b = c$.

Definición 2.1.5 (Función inyectiva). Sea $f : A \longrightarrow B$ una función, f es *inyectiva* si y solo si para elementos diferentes de A se tienen imágenes diferentes. Es decir, f es inyectiva si: para todo a, a' con $a \neq a'$ elementos de A, $f(a) \neq f(a')$.

Definición 2.1.6 (Función sobreyectiva). Sea $f : A \longrightarrow B$ una función, f es *sobreyectiva* (sobre) si y solo si para todo b elemento de B existe un elemento a de A tal que b sea imagen de a . Es decir, f es sobreyectiva si: para todo b elemento de B, existe un a en A tal que $b = f(a)$.

Definición 2.1.7 (Función biyectiva). Sea $f : A \longrightarrow B$ una función, f es *biyectiva* si y solo si f es inyectiva y sobreyectiva.

2.2. Definiciones y resultados de la teoría de grupos

Definición 2.2.1 (Operación binaria interna). Una *operación binaria interna* $*$ en un conjunto A, es una función de $A \times A$ en A. Es decir:

$$* \text{ es una operación binaria interna en } A \Longleftrightarrow * : A \times A \longrightarrow A \text{ es función.}$$

NOTA:*La definición de operación binaria interna* $*$ *en* A *es equivalente a la propiedad clausurativa de la operación* $*$ *en* A.

Definición 2.2.2. Una operación binaria interna $*$ en un conjunto A, es *asociativa* si para todo x, y, z elementos de A, $(x * y) * z = x * (y * z)$.

Definición 2.2.3. Una operación binaria interna $*$ en un conjunto A, es *conmutativa* si para todo x, y elementos de A, $x * y = y * x$.

Definición 2.2.4. Una operación binaria interna $*$ en un conjunto A, es *modulativa* si para todo elemento x de A existe un elemento e en A tal que $x * e = e * x = x$.

Por lo tanto es conveniente tener en cuenta que dado el sistema $(A, *)$ e es el módulo de $*$ si para todo elemento x de A se tiene $x * e = e * x = x$.

Definición 2.2.5. Una operación binaria interna $*$ en un conjunto A, es *invertiva* si para todo elemento x de A existe un elemento y de A tal que $x * y = y * x = e$. y es llamado elemento inverso de x y se denota x^{-1}.

Definición 2.2.6 (Grupo). Un *grupo* $(A, *)$, es un conjunto A con una operación binaria interna $*$, tal que se satisfacen las siguientes propiedades:

- $*$ es asociativa
- $*$ es modulativa
- $*$ es invertiva

Ejemplo 2.2.1. 1. Considérese el conjunto $V = \{e, a, b, c\}$ con la operación definida por la tabla 2.1. Es claro que este conjunto con la operación correspondiente es un grupo (conocido como el grupo de Klein).

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Tabla 2.1. Grupo de Klein.

Definición 2.2.7 (Grupo abeliano). Un grupo $(A, *)$ es *abeliano* si su operación binaria interna $*$ es conmutativa. Es decir:

$$(A, *) \text{ es un grupo abeliano} \iff \forall x, y \in A : \; x * y = y * x$$

Definición 2.2.8 (Subgrupo). Sean $(A, *)$ un grupo y $B \neq \varnothing$ subconjunto de A, si $(B, *)$ es un grupo entonces se dice que $(B, *)$ es un *subgrupo* de $(A, *)$.

NOTA:*Si B es subgrupo de A, lo notaremos $B \leq A$; además, A es subgrupo impropio de A, $\{e\}$ es el subgrupo trivial y también se conoce como subgrupo impropio de A y los demás, si existen, se llaman subgrupos propios de A.*

Teorema 2.2.1 (Criterio para subgrupos). *Sea A un grupo y B un subconjunto de A, entonces B es subgrupo de A si y solo si:*

1. *$B \neq \emptyset$.*
2. *Para todo x, y elementos de B, $\; x * y^{-1}$ es un elemento de B.*

Es fácil ver la veracidad del enunciado, su demostración se encuentra en los libros de álgebra moderna tales como [9] y [13].
De ahora en adelante utilizaremos la notación xy^{-1} para referirnos a $x * y^{-1}$ y xy para referirnos a $x * y$.

Definición 2.2.9 (Clases Laterales). Si B es un subgrupo de A, y a es un elemento de A, entonces $aB = \{ab : b \in B\}$ se llama *clase lateral izquierda*.

Análogamente se define la clase lateral derecha.

Definición 2.2.10 (Subgrupo normal). Sea B subgrupo de A, B se dice *normal* y se denota $B \lhd A$ si $(xB)(yB) = (xy)B$ para todo x, y elemento de A.

Definición 2.2.11 (Grupo cociente). Sea A un grupo y B un subgrupo normal de A, la operación $(xB)(yB) = (xy)B$ define en el conjunto cociente A/B una estructura de grupo. Este grupo recibe el nombre de *grupo cociente* de A sobre B.

Definición 2.2.12 (Producto directo). Dados los grupos A_1, A_2, ..., A_k definimos su *producto directo* como el grupo formado por los elementos de la forma $(a_1, a_2, \ldots, a_k)$ con a_i elemento de A_j para todo $j = 1, 2, \ldots, k$ con la operación

$$(a_1, a_2, \ldots, a_k)(b_1, b_2, \ldots, b_k) = (a_1 b_1, a_2 b_2, \ldots, a_k b_k)$$

Definición 2.2.13 (Centro de un grupo). *El centro de un grupo* A se define como $Z(A) = \{a \in A : \forall x \in A; ax = xa\}$. El centro es diferente de vacío ya que siempre tendrá como mínimo el modulo.

Definición 2.2.14 (Homomorfismo). Sean $(A, *)$ y $(B, \odot)$ dos grupos y f una función de A en B, f se dice *homomorfismo* de grupos si para todo a, a' elementos de A,

$$f(a * a') = f(a) \odot f(a')$$

Si f es una función biyectiva y un homomorfismo se dirá que f es un *isomorfismo*, si el isomorfismo es entre un mismo grupo se hable de automorfismo.

Definición 2.2.15 (Núcleo de una función). Dado un homomorfismo f entre los grupos A_1 y A_2, definimos el *núcleo de* f mediante $N(f) = \{a \in A : f(a) = e_2\}$, donde e_2 es el módulo de A_2.

Proposición 2.2.1. *Si* f *es un homomorfismo de* A_1 *en* A_2 *de núcleo* $N(f)$ *entonces* $N(f)$ *es subgrupo normal de* A_1.

Para detalles de la demostración se remite al lector a Herstein [9].

Teorema 2.2.2 (Primer teorema de isomorfía). *Sea* $f : A_1 \to A_2$ *un homomorfismo sobreyectivo entre los grupos* A_1 *y* A_2 *con núcleo* $N(f)$ *entonces* $A_1/N(f)$ *es isomorfo a* A_2.

Para ver detalles de la demostración consultar Dorronsoro [6].

Definición 2.2.16 (Permutación). Si α es una función biyectiva de un conjunto A sobre sí mismo, α es llamada una *permutación.*

Ejemplo 2.2.2. 1. Si $A = \{1, 2, 3, 4, 5, 6\}$ la función $\alpha : A \longrightarrow A$ dada por $\alpha(1) = 3$, $\alpha(2) = 1$, $\alpha(3) = 4$, $\alpha(4) = 2$, $\alpha(5) = 6$, $\alpha(6) = 5$, es una permutación sobre A y la notaremos por:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 2 & 6 & 5 \end{pmatrix}$$

Definición 2.2.17 (Ciclo). Sea θ una permutación de $S_n = \{\theta : I_n \longrightarrow I_n \,|\, \theta \text{ es biyectiva}\}$ donde $I_n = \{1, 2, \ldots, n\}$, se dice que θ es un $m-$ciclo, $1 \leq m \leq n$ o también que θ es un ciclo de longitud m si existen m elementos diferentes: a_1, a_2, ..., a_m de I_n tales que:

1. $\theta(a_1) = a_2$; $\theta(a_2) = a_3$; $\theta(a_{m-1}) = a_m$; $\theta(a_m) = a_1$.

2. $\theta(x) = x$ para $x \in I_n \setminus \{a_1\, a_2\, \ldots\, a_{m-1}\, a_m\}$.

El $m-$ciclo se denota por $\theta = (a_1\, a_2\, \ldots\, a_{m-1}\, a_m)$

Ejemplo 2.2.3. 1. $n = 6$, $m = 4$ $\theta = (1\,2\,4\,5)$

$a_1 = 1$, $a_2 = 2$, $a_3 = 4$, $a_4 = 5$.

$\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 5 & 1 & 6 \end{pmatrix}$ nótese que solo hay un 1-ciclo y es la permutación identica.

CAPÍTULO 3

TEORÍA ELEMENTAL DE LOS GRUPOS CÍCLICOS

En este capítulo se analizarán las propiedades fundamentales de los grupos cíclicos. Se presenta una lista de las propiedades fundamentales asociadas a estos grupos y se indica la manera de deducir otras propiedades a partir de ellas.

En aras de la claridad, creemos conveniente no enunciar todas las propiedades de los grupos cíclicos a la vez, sino hacerlo en secciones separadas. Se introduce primero, en la sección 3.1 la definición de grupo cíclico que se basa en las definiciones de la teoría general de grupos muy conocida en nuestro medio. En seguida se introducen, en la sección 3.2, las propiedades de los grupos cíclicos y la ilustración de las mismas.

En la sección 3.3 se incluyen algunas proposiciones de los grupos cíclicos que no fueron estudiadas en la sección anterior. Por último, en la sección 3.4, se estudia la clasificación de grupos cíclicos demostrando que todo grupo cíclico es isomorfo a $\mathbb{Z}_n$ o $\mathbb{Z}$ según sea finito o infinito respectivamente.

El procedimiento de separar los diferentes aspectos de la teoría de grupos cíclicos puede parecer un tanto lento y disperso, pero tiene sus ventajas; son varias propiedades las que intervienen y resulta más conveniente considerar unas cuantas a la vez a fin de ver claramente el papel que éstas desempeñan. Además, parte de la finalidad de este capítulo es ofrecer ejemplos que permitan observar el uso adecuado de propiedades de grupos cíclicos. Así, toda persona que tenga acceso a este trabajo de grado puede adquirir experiencia en la argumentación de la aplicación de la teoría de los grupos cíclicos.

3.1. Definición de grupo cíclico.

Nos preguntamos ¿qué relación existe entre ciclos y los grupos cíclicos?. La relación consiste en que estos últimos son obtenidos ***operando un solo elemento***, en forma similar a como se obtiene un ciclo. El siguiente ejemplo nos permitirá aclarar tal relación:
Sea $S_{10} := \{X_1, X_2, \ldots, X_{10}\}$ el grupo de permutaciones de 10 elementos y sea q un elemento de S_{10}, no necesariamente un ciclo, y considerando cada imagen de X_1,$q(X_1)$,$q^2(X_1)$, ... (infinitos). Cada uno de estos elementos debe ser igual a alguno de los diez elementos que se permutan, no todos serán distintos. Si n es el menor entero positivo[1] tal que $q^n = q_0$, donde q_0 es la permutación identidad, el ciclo $C_1 = (X_1,q(X_1),\ldots,q^{(n-1)}(X_1))$ y q definen la misma permutación de los elementos de S_{10} que están en la notación cíclica.

Antes de dar formalmente la definición de grupo cíclico es necesario recordar que la intersección de subgrupos de un grupo es también un subgrupo de este, lo que permite en algunos casos que un subgrupo pueda ser definido en términos de la intersección de otros subgrupos que cumplan determinada condición.

Definición 3.1.1. Si G es un grupo y H un subconjunto no vacío de G, el subgrupo de G generado por H, denotado $\langle H\rangle$ es la intersección de todos los subgrupos de G que contengan a H. Es decir:

$$\langle H\rangle = \bigcap\{K|K \leq G \wedge H \subset K\}$$

[1] *Para una discusión del entero positivo n véase A. Martinez Algebra Moderna, pág* 38

Lo que permite afirmar que $\langle H \rangle$ es el menor de todos los subgrupos de G que contienen a H, lo cual es equivalente a decir que, si K es un subgrupo de G en el cual $H \subseteq K \subseteq \langle H \rangle$, entonces $K = \langle H \rangle$.

Una definición muy útil e indispensable a la hora de hablar de grupos cíclicos, es la de elemento generador que presentamos a continuación.

Definición 3.1.2. Sea G un grupo y x un elemento de G. Se dice que x es un generador de G si y solo si para todo y elemento de G, existe un entero n tal que $y = x^n$.

Definición 3.1.3 (Grupo cíclico). Un grupo G es un Grupo Cíclico si y solo si para algún elemento x en G, $\langle x \rangle = G$.

Ejemplo 3.1.1. 1. $(H, +)$ es cíclico, siendo $H := \{\text{Horas que marca un reloj}\}$.

+	1	2	3	4	5	6	7	8	9	10	11	12
1	2	3	4	5	6	7	8	9	10	11	12	1
2	3	4	5	6	7	8	9	10	11	12	1	2
3	4	5	6	7	8	9	10	11	12	1	2	3
4	5	6	7	8	9	10	11	12	1	2	3	4
5	6	7	8	9	10	11	12	1	2	3	4	5
6	7	8	9	10	11	12	1	2	3	4	5	6
7	8	9	10	11	12	1	2	3	4	5	6	7
8	9	10	11	12	1	2	3	4	5	6	7	8
9	10	11	12	1	2	3	4	5	6	7	8	9
10	11	12	1	2	3	4	5	6	7	8	9	10
11	12	1	2	3	4	5	6	7	8	9	10	11
12	1	2	3	4	5	6	7	8	9	10	11	12

Tabla 3.1. Grupo $(H, +)$.

Es fácil ver que $H = \langle 1 \rangle$ puesto que:

$1 + 1 = 1^2 = 2$

$1 + 1 + 1 = 1^3 = 3$

$1+1+1+1=1^4=4$

$\vdots$

$1+1+\ldots+1=1^n$

siguiendo este proceso hasta $n=13$ y por la definición 3.1.2 se tiene que 1 es el generador de H y por la definición 3.1.3 H es cíclico. De igual manera es fácil comprobar que $H=\langle 5\rangle$, $H=\langle 7\rangle$ y $H=\langle 11\rangle$.

2. $(\mathbb{Q},+)$ no es cíclico.

   Supongamos que $(\mathbb{Q},+)$ es cíclico, entonces existe un $p=\frac{m}{n}$ con $m,n\in\mathbb{Z}$ y n no nulo, es decir $n\neq 0$ tal que $\mathbb{Q}=\langle p\rangle$. Cada elemento de $\mathbb{Q}$ diferente de cero debe ser de la forma $\underbrace{p+p+\ldots+p}_{r-veces}$, para algún $r\in\mathbb{Z}^+$ conveniente, o de la forma $\underbrace{-p-p-\ldots-p}_{r-veces}$.

   Ahora $\frac{1}{2n}\in\mathbb{Q}$, si $\frac{1}{2n}=\underbrace{p+p+\ldots+p}_{r-veces}$ implica que $\frac{1}{2n}=r(\frac{m}{n})$ de donde $1=2nr\frac{m}{n}$, entonces $1-2rm=0$ pero r y m son enteros; luego la ecuación $1-2rm=0$ no tiene solución en los enteros.

   Si $\frac{1}{2n}=\underbrace{-p-p-\ldots-p}_{r-veces}$ implica que $\frac{1}{2n}=-r\frac{m}{n}$ de donde $1=-2rm$, entonces $1+2rm=0$ pero r y n son enteros; por lo tanto la ecuación $1+2rm=0$ no tiene solución en los enteros.

   Por consiguiente $(\mathbb{Q},+)$ no es un grupo cíclico.

3. $(\mathbb{Z}/5,\odot)$ es cíclico. En efecto puesto que $(\mathbb{Z}/5,\odot)=\langle\overline{4}\rangle=\langle\overline{3}\rangle$

   Recordemos $\mathbb{Z}/5=\{\overline{1},\overline{2},\overline{3},\overline{4}\}$.

Cuando hablamos de un grupo cíclico $G=\langle x\rangle$, suelen utilizarse las expresiones ***G es generado por x, G es cíclico con generador x*** y ***x es el generador del grupo G***. Por otra parte si H es subgrupo de un grupo G que contienen al elemento x, según la definición 3.1.1 debe tenerse que $G=H$, es decir $G=\langle x\rangle$ implica que G es el único de sus subgrupos que contienen al elemento x.

A continuación se muestra una definición que caracteriza a los grupos cíclicos y aclara el sentido que tiene la expresión ***operando un solo elemento***, utilizada en la introducción de este capitulo.

Definición 3.1.4. Sea x un elemento de G y $H = \{x^n : n \in \mathbb{Z}\}$, H es llamado el subgrupo cíclico de G generado por x, y lo notaremos $H = \langle x \rangle$.

Esta definición se puede escribir con notación aditiva, basta tomar $H = \{nx : n \in \mathbb{Z}\}$.

Ejemplo 3.1.2. 1. Los subgrupos cíclicos de $(H, +)$ grupo del ejemplo 3.1.1 (1) son:

$$\langle 2 \rangle = \{2, 4, 6, 8, 10, 12\}$$
$$\langle 3 \rangle = \{6, 9, 12, 3\} = \langle 9 \rangle$$
$$\langle 6 \rangle = \{12, 6\}$$
$$\langle 8 \rangle = \{8, 12, 4\} = \langle 4 \rangle$$

2. Los subgrupos cíclicos de $(\mathbb{Z}_7^*, \times)$ donde $\mathbb{Z}_7^*$ es el conjunto de las clases de equivalencia módulo 7 sin la clase del cero son:

$$\langle \overline{1} \rangle = \{\overline{1}\}$$
$$\langle \overline{2} \rangle = \langle \overline{4} \rangle = \{\overline{2}, \overline{4}, \overline{1}\}$$
$$\langle \overline{5} \rangle = \mathbb{Z}_7^*$$
$$\langle \overline{6} \rangle = \{\overline{6}, \overline{1}\}$$

3.2. Propiedades de los grupos cíclicos

Teorema 3.2.1. *Todo grupo cíclico es un grupo abeliano.*

Demostración.
Sean $z, y \in G = \langle x \rangle$, entonces existen n, m enteros tales que $z = x^n$ y $y = x^m$, así

	zy	$=$	$x^n x^m = x^{n+m}$	por propiedades de potenciación
		$=$	x^{m+n}	la suma de enteros es conmutativa
		$=$	$x^m x^n$	por propiedades de potenciación
		$=$	yz	hipótesis
Luego	zy	$=$	yz	por propiedad transitiva

■

Definición 3.2.1. *El orden de un grupo* G, al que denotaremos por $O(G)$, es el número de elementos en el conjunto G. El orden de un elemento x en G es el orden del grupo $\langle x\rangle$, es decir $O(x) = O(\langle x\rangle)$.

Teorema 3.2.2. *Sea* x *un elemento de orden finito en un grupo y sea* n *el menor entero positivo tal que* $x^n = e$*, entonces* $O(x) = n$.

Demostración.
Definamos $H = \{e, x, x^2, x^3, \ldots, x^{n-1}\} \subseteq \langle x\rangle = \{x^n : n \in \mathbb{Z}\}$ y sea x^t un elemento cualquiera de $\langle x\rangle$, entonces t es un entero y como $n > 0$, por el algoritmo de la división existen q, r enteros tales que $t = nq + r$, con $0 \leq r \leq n - 1$; luego,

$$x^t = x^{nq+r} = x^{nq}x^r = (e^q)x^r = ex^r = x^r$$

donde x^r es un elemento de H, por lo tanto todos los elementos de $\langle x\rangle$ están en H. Esto significa que $\langle x\rangle$ es subconjunto de H y la contenencia contraria siempre se cumple. La igualdad $H = \langle x\rangle$ es establecida por las dos contenencias. Finalmente queremos garantizar que $O(x) = n$, es decir, $e, x, x^2, \ldots, x^{n-1}$ son todos distintos. Supongamos que existen k y l enteros, con $1 \leq l < k \leq n - 1$, si $x^k = x^l$, $x^{k-l} = e$ con $0 < k - l < n$ contradictorio con la escogencia de n, de donde k, l enteros no existen.
Luego $O(H) = O(\langle x\rangle) = O(x) = n$. ■

Ejemplo 3.2.1. 1. Sea $\overline{10}$ un elemento en $(\mathbb{Z}_{18}, +)$ su orden es el menor entero positivo n tal que $n\overline{10} = \overline{0}$, lo cual solo se satisface si 18 divide $10n$. Como el menor entero positivo que satisface tal condición es 9, se tiene que $O(\overline{10}) = 9$.

2. Sea $(R, \circ)$ un grupo con $R = \{\text{rotaciones de } 90^\circ \text{ de un cuadrado}\}$.

$$I = \begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}; \qquad R = \begin{pmatrix} a & b & c & d \\ d & a & b & c \end{pmatrix};$$

$$R^2 = \begin{pmatrix} a & b & c & d \\ c & d & a & b \end{pmatrix}; \quad R^3 = \begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix}.$$

$\circ$	I	R	R^2	R^3
I	I	R	R^2	R^3
R	R	R^2	R^3	I
R^2	R^2	R^3	I	R
R^3	R^3	I	R	R^2

Tabla 3.2. Grupo $(R, \circ)$.

Sea R^3 un elemento de $(R, \circ)$. Puesto que $(R^3)^2 = R^2$, $(R^3)^3 = R$, $(R^3)^4 = I$ y $(R^3)^5 = R^3$ se tiene que $O(R^3) = 4$.

Proposición 3.2.1 (Teorema de Lagrange). *Sea x un elemento en un grupo G tal que $O(x) = n$. Si m es un entero tal que $x^m = e$ entonces m es divisible por n.*

Demostración.
Supongamos que n no divide a m, entonces por teorema fundamental de la aritmética se tiene que $m = nq + r$, $o < r < n$. Ahora

$$x^m = x^{nq+r} = x^{nq}x^r = (x^n)^q x^r = e^q x^r = x^r$$

como $x^m = e$, entonces $x^r = e$ de donde $O(x) = r$, contradicción puesto que $O(x) = n$ y $r < n$. Por lo tanto n divide a m. ■

Regresando al estudio de subgrupos de un grupo cíclico se tiene:

Teorema 3.2.3. *Si G es un grupo cíclico y H es un subgrupo de G, entonces H también es cíclico.*

Demostración.
Si $H = \{e\}$, entonces es inmediato $H = \langle e \rangle$ es cíclico. Sea H diferente de $\{e\}$, sea $G = \langle x \rangle$ y k el menor entero positivo tal que $x^k \in H$. Sea $a = x^k$ demostraremos que $H = \langle a \rangle$. Si $b \in H$, como H es subgrupo de G, $b \in G$ por consiguiente $b = x^n$ para algún entero positivo n, por el algoritmo de la división: existen q, r enteros tales que $n = kq + r$; $0 \leq r \leq k$, por lo tanto

$$x^n = x^{k+qr} = x^{kq}x^r = (x^k)^q x^r$$

de lo anterior $x^r = (x^k)^{-q}x^n$.
Ahora, como x^n es un elemento de H, $\underbrace{x^k x^k x^k \dots x^k}_{q-veces}$ es un elemento de H, de donde $(x^k)^q$ esta en H y por hipótesis H es subgrupo de G, entonces $(x^k)^{-q}$ es también un elemento de H.
Como x^n esta en H, $x^n(x^k)^{-q}$ esta en H, luego x^r es un elemento de H. Dada la escogencia de k y $0 \leq r < k$ se debe tener que $r = 0$, así $x^k = x^{kq} = (x^k)^q$ es un elemento en $\langle x^k \rangle$.
■

Corolario 3.2.1. *Si $G = \langle x \rangle$ tiene orden n y H es un subgrupo de G, entonces H es generado por un elemento de la forma x^m, en donde m es un divisor de n.*

Demostración.
Como $G = \langle x \rangle$ y $O(G) = n$, $G = \{e, x, \dots, x^{n-1}\}$. Como $H \leq G$ cada $y \in H$ es una potencia de x^k para algún $k \in \{1, 2, \dots, n-1\}$.
Sea $m = min\{k = 1, \dots, n-1 : x^k \in H\}$.
Sea $z \in H$, como $H \leq G$ entonces $z = x^j$, $j \in \mathbb{Z}$. Por el algoritmo de la división $j = mi + r$ con $0 \leq r < m$. Luego

$$x^j = x^{mi+r} = x^{mi}x^r$$

por lo tanto $x^r \in H$, pero $0 \leq r < m$, entonces $r = 0$. Se concluye así que $H = \langle x^m \rangle$.
Tomemos $n = mq + t$ con $q, t \in \mathbb{Z}$ y $0 \leq t < m$ luego $x^n = x^{mq+t} = x^{mq}x^t = (x^m)^q x^t$ pero m es el menor entero tal que $x^m \in H$ y como $0 \leq t < m$ se tiene que $t = 0$ luego $n = mq$ de donde se tiene que $m|n$. ■

Ejemplo 3.2.2. 1. Es fácil ver que $\langle R^3 \rangle = R$ con R del ejemplo 3.2.1 (2). De acuerdo al corolario los subgrupos de R son de la forma $\langle (R^3)^m \rangle$, donde m es divisor de $O(R) = 4$ y por tanto los únicos casos posibles son:

   $m = 1 : \langle (R^3)^1 \rangle = \langle R^3 \rangle = R$

   $m = 2 : \langle (R^3)^2 \rangle = \langle R^2 \rangle = \{I, R^2\}$

   $m = 4 : \langle (R^3)^4 \rangle = \langle R^3 \rangle = R$

   Con la aplicación del corolario se hace innecesario considerar el caso para $\langle R \rangle$.

2. Para determinar todos los subgrupos de H, definido H en el ejemplo 3.1.1 (1), de acuerdo al corolario, los subgrupos de H son de la forma $\langle m5 \rangle$, $\langle m7 \rangle$, $\langle m1 \rangle$, $\langle m11 \rangle$ con $m = 1, 2, 3, 4, 6, 12$ puesto que $O(H) = 12$. Consideremos $\langle m5 \rangle$.

$m = 1 : \langle 5 \rangle$

$m = 2 : \langle 2 \times 5 \rangle = \langle 10 \rangle = \{8, 6, 4, 2, 12, 10\}$

$m = 3 : \langle 3 \times 5 \rangle = \langle 3 \rangle = \{6, 9, 12, 3\}$

$m = 4 : \langle 4 \times 5 \rangle = \langle 1 \rangle = H$

$m = 6 : \langle 6 \times 5 \rangle = \langle 11 \rangle = H$

$m = 12 : \langle 12 \times 5 \rangle = \langle 12 \rangle = \{12\}$

Análogamente se analizan los demás casos.

Proposición 3.2.2. *Si $G = \langle x \rangle$ con $O(x) = n$, entonces para todo entero k tal que el máximo común divisor de k y n es d al cual denotaremos $(k, n) = d$, el orden del subgrupo $\langle x^k \rangle$, es $\frac{n}{d}$.*

Demostración.
Como $(n, k) = d$ existen a, b enteros tal que $n = ad$ y $k = bd$. A partir de aquí se puede escribir:

$$(x^k)^{\frac{n}{d}} = x^{ka} = x^{bda} = (x^n)^b = e$$

de donde se deduce que el orden de x^k es divisor de $\frac{n}{d}$.
Sea t el orden de x^k, como $(x^k)^t = e$, entonces n es un divisor de kt y por lo tanto $\frac{n}{d}$ es un divisor de $(\frac{k}{d})t$.
Puesto que $(\frac{n}{d}, \frac{k}{d}) = 1$ se tiene que $\frac{n}{d}$ divide a t.
Por tanto $t = \frac{n}{d}$ como se quería ver. ■

Proposición 3.2.3. *Si G es un grupo cíclico y el orden de G es mayor que 2, G tiene por lo menos dos generadores que son a y a^{-1}.*

Demostración.
$G = \langle a \rangle$ y $x \in G$, entonces existe $m \in \mathbb{Z}$ tal que $x = a^m$, por tanto $x^{-1} = (a^m)^{-1} = a^{-m}$, así $x = (a^{-m})^{-1} = (a^{-1})^{-m}$ de donde $\langle a^{-1} \rangle = G$. Además si $O(G) > 2$ y $G = \langle a \rangle$ se tiene que $a^{-1} \neq a$. ■

Corolario 3.2.2. *Si x es un generador de un grupo de orden n, entonces todos los demás generadores de G son de la forma x^k, en donde $(k, n) = 1$.*

Demostración.
Sea $G = \langle x \rangle$ y $O(x) = n$. Supongamos $G = \langle r \rangle$ lo cual es posible puesto que G tiene por lo menos otro generador además de x. Entonces existe $v \in \mathbb{Z}$ tal que $x^v = r$, $0 < v < n$ y existe $j \in \mathbb{Z}$ tal que $x^j = x$, $0 < j < n$. Como $x^v = r$ y $x^j = x$, $(r^j)^v = r$ lo cual implica que $r^{jv} = r$ de donde $r^{jv} r^{-1} = e$, luego $r^{jv-1} = e$, entonces $n|jv - 1$ ó $jv - 1 = 0$. Ahora falta ver que v y n son primos relativos, esto es, si $p|n$ y $p|v$ se tiene que $p = \pm 1$, $p \in \mathbb{Z}$. Si $p|n$ entonces $n = pq_1$, $q_1 \in \mathbb{Z}$ y si $p|v$ entonces $v = pq_2$, $q_2 \in \mathbb{Z}$.
i) $n|jv-1$ entonces $jv-1 = n\alpha, \alpha \in \mathbb{Z}$, de donde $jv - n\alpha = 1$, luego $j(pq_2) - (pq_1)\alpha = 1$, lo cual es equivalente $p(jq_2 - \alpha q_1) = 1$ entonces $p = 1$ ó $p = -1$.
ii) $jv - 1 = 0$ de donde $jv = 1$, teniendo $v = \pm 1$, luego $x^{-1} = r$ ó $x = r$; obtenemos entonces $(v, n) = 1$ como se quería. ■

Ejemplo 3.2.3. 1. En el grupo $(H, +)$ del ejemplo 3.1.1 (1) al aplicar la proposición 3.3.2 y el corolario anterior se tiene que:

$10 = 10 \times 1$ entonces $O(\langle 10 \rangle) = \frac{12}{(10,12)} = \frac{12}{2} = 6$

$11 = 11 \times 1$ entonces $O(\langle 11 \rangle) = \frac{12}{(11,12)} = \frac{12}{1} = 6$

$3 = 3 \times 1$ entonces $O(\langle 3 \rangle) = \frac{12}{(3,12)} = \frac{12}{3} = 4$

Por lo tanto otro generador de $(H, +)$ es 11

2. En el grupo $(R, \circ)$ del ejemplo 3.2.1 (2) se tiene
$R^3 = R^3 \times I$ entonces $O(\langle R^3 \rangle) = \frac{4}{(3,4)} = \frac{4}{1} = 4$

$R = R \times I$ entonces $O(\langle R^2 \rangle) = \frac{4}{(4,1)} = \frac{4}{1} = 4$

$R^2 = R^2 \times I$ entonces $O(\langle R^2 \rangle) = \frac{4}{(2,4)} = \frac{4}{2} = 2$.

Entonces son generadores de $(R, \circ)$, R^3 y R.

Proposición 3.2.4. *Si G es un grupo cíclico, y x es el único elemento generador de G. Entonces el orden de G es menor o igual a dos.*

Demostración.
Supongamos $O(G) > 2$. Por hipótesis se tiene que G es cíclico, empleando la proposición anterior, G tiene por lo menos dos generadores que son x^{-1} y x. Pero x es el único elemento generador de G. Por consiguiente $O(G) \leq 2$ ■

Proposición 3.2.5. *Un grupo cíclico de orden infinito (con infinitos elementos) tiene exactamente dos generadores. Si a es un generador, a^{-1} es el único otro generador.*

Demostración.
$G = \langle a \rangle$ entonces por proposición 3.2.3 se tiene $G = \langle a^{-1} \rangle$. Si $G = \langle a^k \rangle$ y $a^k \neq a$, existe $i \in \mathbb{Z}$ tal que $(a^k)^i = a$, de donde $a^{ki}a^{-1} = e$ y $O(a) = ki - 1$, lo cual contradice el hecho de que $O(G)$ es infinito. ■

Corolario 3.2.3. *Si el orden de un grupo G es primo entonces G es cíclico.*

Demostración.
Sea $O(G) = p$ y p primo. Sea $x \in G$ tal que $x^p = e$, como G es grupo se tiene que $x^p \in G$. Aplicando el teorema anterior $\langle x \rangle$ es un subgrupo de G y es cíclico. Ahora supongamos $O(\langle x \rangle) = m$, entonces por el teorema de Lagrange m divide a p. Pero p es primo, por tanto $p = m$ deduciendo que $O(G) = O(\langle x \rangle)$. Se tiene entonces que $G = \langle x \rangle$. Concluimos que G es cíclico. ■

3.3. Otras propiedades de los grupos cíclicos

Proposición 3.3.1. *Si G es un grupo de orden $2p$, con p primo, entonces todo subgrupo propio de G es cíclico.*

Demostración.
Sea $O(G) = 2p$ y H subgrupo propio de G. Entonces $1 < O(H) < 2p$. Aplicando el teorema de Lagrange $O(H)$ divide a $2p$. se analizaran los casos $p = 2$ y $p \neq 2$.
i) si $p = 2, O(G) = 4$ entonces[2] $O(H) = 1, 2$, ó 4, pero $1 < O(H) < 4$ por lo tanto $O(H) = 2$. Entonces existe $x \in H$ tal que $x^2 = e$, por lo cual $\langle x \rangle = \{x, e\}$ se concluye que H es cíclico.
ii) si $p \neq 2$ entonces $(p, 2) = 1$ por lo cual $O(H)$ divide a 2 ó $O(H)$ divide a p. Si $O(H)$ divide a 2 se tiene que $O(H) = 1$ ó $O(H) = 2$. Puesto que p es primo y como H es subgrupo propio de G, $O(H) = 2$. Por parte (i) H es cíclico.
Ahora si $O(H)$ divide a p entonces $O(H) = 1$ ó $O(H) = p$ como H es subgrupo propio de G, $O(H) = p$ y existe $x \in H$ tal que $x^p = e$, por tanto $\langle x \rangle = \{x, x^2, \ldots, e\}$, concluyendo que H es cíclico.
De i) y ii) se tiene que H es cíclico. ■

[2] $\tau(n)$ = *Número de divisores positivos de* n

Proposición 3.3.2. *Si G es un grupo diferente de la identidad. Entonces los únicos subgrupos de G son el mismo y la identidad si y solo si G es un grupo cíclico finito de orden primo.*

Demostración.
$\Longrightarrow$) Bajo la hipótesis, si $x \neq e$ es un elemento de G, entonces el grupo cíclico generado por x no es el grupo identidad y por tanto debe ser G.
Si G no es finito por contrarecíproca de teorema 3.2.2, no existe $k \in \mathbb{Z}^+$ tal que $x^k = e$, siendo $x \in G$. Pero $\langle x \rangle \leq G$, luego $\langle x \rangle = G$ ó $\langle x \rangle = \{e\}$ gracias a la hipótesis. Como $e \in G$, existe $k \in \mathbb{Z}^+$ tal que $x^k = e$, luego G es finito.
Ahora supongamos que n no es primo, entonces existen $a, b \in \mathbb{Z}^+$ con $a > 1$ y $b > 1$ tales que $n = ab$. Como $O(G) = n$ para todo $x \in G$, $x^n = e$ de donde

$$x^n = x^{ab} = (x^a)^b = e$$

lo cual implica $\langle x^a \rangle \leq G$ y $O(\langle x^a \rangle) = b$. En virtud de la hipótesis $\langle x^a \rangle = G$ ó $\langle x^a \rangle = \{e\}$, entonces $O(\langle x^a \rangle) = n$; esto es $b = n$, absurdo. Luego n es primo.
Aplicando el corolario 3.2.3 G es cíclico.
$\Longleftarrow$) Sea $O(G) = n$ por hipótesis $H \leq G$, aplicando el teorema de Lagrange $O(H)|n$, como n es primo $O(H) = n$ ó $O(H) = 1$ entonces $H = G$ ó $H = \{e\}$.

■

La siguiente proposición muestra una condición necesaria y suficiente para que el producto de dos subgrupos de un grupo es él mismo, un subgrupo.

Proposición 3.3.3. *Si G es grupo, H y K subgrupos de G entonces HK es subgrupo de G si y solo si $HK = KH$.*

Demostración.
$\Longrightarrow$) Por hipótesis HK es subgrupo de G. Aplicando propiedades de subgrupos se tiene que siendo $hk \in HK$, $h^{-1}k^{-1} \in HK$ de donde $kh = (h^{-1}k^{-1})^{-1} \in HK$. Se observa $KH \subset HK$.
Ahora $(hk)^{-1} \in HK$ entonces $k^{-1}h^{-1} \in KH$ por tanto $HK \subset KH$.
Puesto que $KH \subset HK$ y $HK \subset KH$ se tiene $HK = KH$.
$\Longleftarrow$) Sea $hk \in HK$ y sea $HK := \{hk : h \in H \wedge k \in K\}$, entonces $h \in H$ y $k \in K$. Basados en la hipótesis $h^{-1} \in H$ y $k^{-1} \in H$, en consecuencia

$$h^{-1}k^{-1} = (kh)^{-1} = (hk)^{-1} \in HK.$$

Se sabe que $h_0k_0 \in HK$ y $(hk)^{-1} \in HK$, entonces:

$$\begin{aligned} h_0k_0(hk)^{-1} &= (h_0k_0)(k^{-1}h^{-1}) \\ &= (h_ok_0)(h^{-1}k^{-1}) \\ &= (h_0h^{-1})(k_0k^{-1}) \end{aligned}$$

De donde $h_0k_0(hk)^{-1}$ es un elemento de HK. Según el criterio para subgrupos se tiene que HK es un subgrupo de G. ■

Un resultado directo de la proposición 3.3.4 es el siguiente corolario

Corolario 3.3.1. *Si H y K son subgrupos de un grupo abeliano G, entonces HK es un subgrupo de G.*

Demostración.
Bajo la hipótesis $HK = KH$ y aplicando la proposición 3.3.3 se concluye que $HK \leq G$.
■

Teorema 3.3.1. *Si H y K son subgrupos finitos de G de órdenes $O(H)$, $O(K)$ respectivamente, entonces $O(HK) = \frac{O(H)O(K)}{O(H\cap K)}$.*

Demostración.
Si $H \cap K = \{e\}$. Al hacer una lista de todos los elementos hk, $h \in H$ y $k \in K$, para algún $h \neq h_1 \in H$ debe haber $k \neq k_1 \in K$ tal que $hk = h_1k_1$. Pero entonces $(h_1)^{-1}h = k_1k^{-1}$; como $h_1 \in H$, $(h_1)^{-1} \in H$ lo cual implica $(h_1)^{-1}h \in H$. De igual manera $k_1k^{-1} \in K$. Como $(h_1)^{-1}h = k_1k^{-1}$, $(h_1)^{-1} \in H \cap K = \{e\}$, entonces $(h_1)^{-1}h = e$ de donde $h_1 = h$. Contradicción, por tanto $O(HK) = O(H)O(K)$.

Si $H \cap K \neq \varnothing$ y $H \cap K \neq \{e\}$. Sea $h_1 \in H \cap K$, entonces $hk = (hh_1)((h_1)^{-1}k)$ donde $hh_1 \in H$. Como $h \in H, h_1 \in H \cap K \subset H$ y $h^{-1}k \in K$,ya que $(h_1)^{-1} \in H \cap K \subset K$ y $k \in K$, hk está duplicado en el producto al menos $O(H \cap K)$ veces. Pero si $hk = h'k'$,

entonces:

$$\begin{aligned} hk &= h'k' \\ h^{-1}hk &= h^{-1}h'k' \\ k &= h^{-1}h'k' \\ k(k')^{-1} &= h^{-1}h'k'(k')^{-1} \\ k(k')^{-1} &= h^{-1}h' \\ k(k')^{-1} &= h^{-1}h' \end{aligned}$$

Hagamos

$$h^{-1}h' = k(k')^{-1} = u$$

$u \in H \cap K$ y $h' = hu$ además $k' = u^{-1}k$, de donde se tiene que en $hk = (hh_1)((h_1)^{-1}k)$ aparecen todas las duplicaciones. En consecuencia hk aparece en la lista de HK exactamente $O(H \cap K)$ veces, por tanto $O(HK) = \frac{O(H)O(K)}{O(H \cap K)}$. ■

El siguiente resultado es una aplicación de la proposición 3.3.3 para grupos cíclicos.

Proposición 3.3.4. *Sea G un grupo abeliano y H y K subgrupos cíclicos finitos con $O(H) = r$ y $O(K) = s$ entonces G contiene un subgrupo cíclico cuyo orden es el mínimo común múltiplo $([r, s])$ de r y s.*

Demostración.
Como H y K son subgrupos de un grupo abeliano G,en virtud del corolario 3.3.1 se tiene que HK es subgrupo de G.
Según el teorema 3.3.1

$$O(HK) = \frac{O(H)O(K)}{O(H \cap K)} = \frac{rs}{O(H \bigcap K)} = \frac{r}{O(H \cap K)}s$$

por la definición de divisibilidad, $s|O(HK)$. Análogamente $r|O(HK)$.
Si $r|n$ y $s|n$ debemos probar que $O(HK)|n$
$n = O(HK)q + m$ con $0 \leq m \leq O(HK) = \frac{rs}{O(H \cap K)} \leq [r, s]$
como $r|n$ y $r|O(HK)$ entonces $r|m$
como $s|n$ y $s|O(HK)$ entonces $s|m$
por lo cual $[r, s]|m$, pero $0 \leq m \leq [r, s]$, entonces $m = 0$. Así $n = O(HK)q$, de donde $O(HK)|n$. Luego $O(HK) = (r, s)$.
Puesto que $(hk)^{[r,s]} = e$, se tiene que HK es cíclico. ■

Como una particularización de la proposición anterior se tiene el siguiente resultado.

Corolario 3.3.2. *Sea G un grupo abeliano y H, K subgrupos finitos de G con $O(H) = r$ y $O(K) = s$. Si $(r, s) = 1$ entonces G contiene un subgrupo cíclico de orden rs.*

Demostración.
Bajo el corolario 3.3.1 HK es subgrupo de G y en virtud de la proposición 3.3.4, HK es cíclico y $O(HK) = [r, s]$ de donde[3] $O(HK) = \dfrac{rs}{(r, s)}$. Por hipótesis $(r, s) = 1$ entonces $O(HK) = rs$. ■

Proposición 3.3.5. *Sea G un grupo cíclico y $O(G) = n$, entonces G posee tantos generadores como enteros positivos hay menores que n y relativamente primos con n.*

Demostración.
Definamos $A := \{i \in \mathbb{Z}^+ : i < n \wedge (n, i) = 1\}$ y $B := \{g^i \in G : \langle g^i \rangle = G\}$. Sea $m \in A$, por la hipótesis existe $g \in G$ tal que $\langle g^i \rangle = G$, por consiguiente $g^m \in G$, así gracias a la proposición 3.2.2

$$O(g^m) = \tfrac{O(G)}{(O(G),m)} = \tfrac{n}{(n,m)}$$

pero $m \in A$, entonces $O(g^m) = n$. Concluyendo así que para todo $i \in A$ existe $g^i \in G$ tal que $\langle g^i \rangle = G$.
Sea $y \in B$, entonces $\langle y \rangle = G$ por lo cual $y = g^t$, $t \in \mathbb{Z}^+$. En virtud de la proposición 3.2.2

$$O(y) = O(g^t) = \tfrac{n}{(t,n)}$$

pero $O(y) = O(\langle y \rangle)$, lo cual implica $O(\langle y \rangle) = n$. Luego $\frac{n}{(t,n)} = n$, de donde $(t, n) = 1$. Como $t < n$ se cumple que para todo $y \in B$ existe $t \in A$. ■

Proposición 3.3.6. *Sea G un grupo cíclico y $O(G) = n$ y sea $k \in \mathbb{Z}$ tal que $k|n$ entonces existe un único H subgrupo de G tal que $O(H) = k$.*

Demostración.
i) Bajo la hipótesis, existe $x \in G$ tal que $\langle x \rangle = G$. Por la proposición 3.2.2 se tiene

$$O(x^{\frac{n}{k}}) = \frac{n}{(n, \frac{n}{k})}$$

[3] $[x, y] = \frac{xy}{(x,y)}$

como $k|n$, entonces $n = kt$ con $t \in \mathbb{Z}$. Luego

$$O(x^{\frac{n}{k}}) = \frac{kt}{(kt, \frac{kt}{k})} = \frac{kt}{(kt,t)} = \frac{kt}{t(k,1)} = \frac{k}{(k,1)} = \frac{k}{1} = k$$

por transitividad en igualdades $O(x^{\frac{n}{k}}) = k$.
Ahora $\langle x^{\frac{n}{k}} \rangle = H \leq G$ y $O(H) = k$, entonces existe $H \leq G$ tal que $O(H) = k$.
ii) Supongamos que existe H y T subgrupos de G tales que $O(H) = O(T) = k$. Como T y H son subgrupos de G, entonces T y H son cíclicos. Sea $m = inf\{k \in \mathbb{Z}^+ : x^k \in T\}$ se tiene que $\langle x^m \rangle = T$, entonces $x^m \in T$. Como $k = \dfrac{n}{(m,n)}$,

$$x^m = x^{\frac{(m,n)m}{(m,n)}} = (x^{(m,n)})^{\frac{m}{(n,m)}}$$

lo cual implica $x^m \in \langle x^{(n,m)} \rangle$. Entonces $x^m \in \langle x^{\frac{n}{k}} \rangle = H$, esto es $T \subseteq H$.
Si $y \in H, y = (x^m)^s$, con $s \in \mathbf{Z}$ y $(x^m)^s \in T$. Esto es, $y \in T$. Luego $H \subseteq T$.
Como $T \subseteq H$ y $H \subseteq T$, entonces $H = T$. ■

Proposición 3.3.7. *Sean H y G grupos cíclicos de órdenes m y n respectivamente, entonces $H \times G$ es cíclico si y sólo si m y n son primos relativos entre sí.*

Demostración.
$\Longrightarrow$) Por hipótesis $O(H) = m$ y $O(G) = n$, entonces $O(H \times G) = mn$. Supongamos $d = (m,n)$, $d|m$ y $d|n$ entonces $d|mn$.
Ahora, como $H \times G$ es cíclico existe $(h,g) \in H \times G$ tal que $\langle (h,g) \rangle = H \times G$. En virtud de la proposición anterior, existe un único $K \leq H \times G$ tal que $O(K) = d$ y $\langle (h,g)^{\frac{mn}{d}} \rangle = K$. Entonces:

$$(h,g)^{\frac{mn}{d}} = (h^{\frac{mn}{d}}, g^{\frac{mn}{d}}) = ((h^n)^{\frac{m}{d}}, (g^n)^{\frac{m}{d}}) = (e_1, e_2)$$

con e_1 módulo de H y e_2 módulo de G. Por lo cual

$$(h,g)^{\frac{mn}{d}} = (e_1, e_2)$$

luego $\langle (h,g)^{\frac{mn}{d}} \rangle = \langle (e_1, e_2) \rangle$. Así $K = \{(e_1, e_2)\}$, de donde $O(K) = 1$. Se concluye de esta manera que $(m,n) = 1$ puesto que $d = 1$.
$\Longleftarrow$) Sea $mn = O(H \times G)$ y sea $(h,g) \in H \times G$. Aplicando propiedades de grupos finitos, existe $k \in \mathbb{Z}^+$ tal que $(h,g)^k = (e_1, e_2)$, donde $e_1 \in H$ y $e_2 \in G$. Se tiene

$$(h,g)^k = (h^k, g^k) = (e_1, e_2)$$

Basados en la definición de igualdad de pares ordenados, $h^k = e_1$ y $g^k = e_2$. Además, por hipótesis $O(H) = m$ y $O(G) = n$, entonces $h^m = e_1$ y $g^n = e_2$, por el teorema de Lagrange $m|k$ y $n|k$, lo cual implica $[n, m]|k$ de donde $\frac{mn}{(m,n)}|k$ y como $(m, n) = 1$ se tiene que $mn|k$.
Se sabe que

$$(h, g)^{nm} = (h^{nm}, g^{nm}) = ((h^n)^m, (g^n)^m) = (e_1, e_2)$$

luego $k|mn$.
Como $mn|k$ y $k|mn$, entonces $mn = k$, aplicando la definición de orden $O((h, g)) = mn$, por lo cual se tiene que $O(H \times G) = O((h, g))$. Luego $H \times G = \langle (h, g) \rangle$. ■

Ejemplo 3.3.1. 1. $(\mathbb{Z}_8, +)$ es un grupo, si observamos $8 = 2 \times 4$ entonces en virtud de la proposición 3.3.1 se tiene que todos los subgrupos propios de $\mathbb{Z}_8$ son cíclicos.

2. El grupo $G = (\mathbb{Z}_7, +)$ es cíclico y sus únicos subgrupos son el grupo identidad y él mismo. En efecto, pues el $O(G) = 7$ es primo por lo tanto la proposición 3.3.2 garantiza el resultado.

3. $(\mathbb{Z}_{20}, +)$ tiene tantos subgrupos como divisores tenga su orden, en efecto $\mathbb{Z}_{20}$ es un grupo cíclico por la proposición 3.3.5 se obtiene el resultado deseado, veamos:

   $D(20) = \{1, 2, 3, 4, 5, 10, 20\}$ pues $O(\mathbb{Z}_{20}) = 20$, los subgrupos de $\mathbb{Z}_{20}$ son:

   $H_1 = \{0\}$

   $H_2 = \{0, 10\}$

   $H_4 = \{0, 5, 10, 15\}$

   $H_5 = \{0, 4, 8, 12, 16\}$

   $H_{10} = \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18\}$

   $H_{20} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19\} = \mathbf{Z}_{20}$

   Como $\mathbb{Z}_{20}$ es cíclico no existen más subgrupos.

3.4. Clasificación de los grupos cíclicos

El objetivo de esta sección es demostrar que, salvo los isomorfismos los únicos grupos cíclicos existentes son $(\mathbb{Z}, +)$ y $(\mathbb{Z}_n, +)$.

Los grupos $(\mathbb{Z}, +)$ y $(\mathbb{Z}_n, +)$ son grupos cíclicos con generadores 1 y $\overline{1}$ respectivamente.

En seguida se formula un teorema con el cual se demuestra que todos los demás grupos cíclicos son isomorfos a $(\mathbb{Z}, +)$ ó $(\mathbb{Z}_n, +)$ dependiendo de su orden. Para un análisis mejor, recordemos qué es un isomorfismo.

Definición 3.4.1. Sean $(G_1, *)$ y $(G_2, \cdot)$ dos grupos, una función $f : G_1 \to G_2$ se dice que f es *isomorfismo* si y sólo si :
i) f es biyectiva.
ii) f es homomorfismo, es decir, para todo $x, y \in G_1$ se cumple que $f(x * y) = f(x) \cdot f(y)$.
Y se denotará $G_1 \approx G_2$.

Habiendo recordado lo que es un isomorfismo, formularemos a continuación el teorema que caracterizará está sección.

Teorema 3.4.1 (Clasificación de los grupos cíclicos). *Si $(G, *)$ es un grupo cíclico, entonces:*
i) Si G tiene infinitos elementos entonces $(G, *)$ es isomorfo a $(\mathbb{Z}, +)$.
ii) Si $O(G) = n$ (G tiene n elementos) entonces $(G, *)$ es isomorfo a $(\mathbb{Z}_n, +)$.

Demostración.
i) Sea G_1 un grupo cíclico con infinitos elementos, existe $g \in G_1$ tal que $\langle g \rangle = G_1$ definimos $f : z \to G_1$ tal que $f(n) = g^n$. Se debe ver que f es una función biyectiva y un homomorfismo.

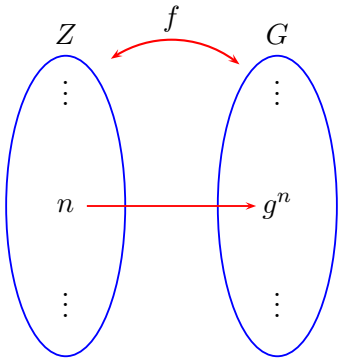
$$N(f) = \{n \in \mathbb{Z} : f(n) = e\} = \{n \in \mathbb{Z} : g^n = e\}$$

donde e es el módulo de G_1 (ver figura 3.1).

Se quiere saber si $g^n = e$, como G_1 es de orden infinito entonces $n = 0$.
Si $n \neq 0$, n sería el orden de G_1 lo que contradice la hipótesis, luego $N(f) = \{0\}$. f es biyectiva.
Ahora sea $x \in G_1$ como G_1 es cíclico $x = g^n, n \in \mathbb{Z}$ luego existe $n \in \mathbb{Z}$ tal que $f(n) = x$ de donde se tiene que f es sobreyectiva. Concluimos[4] que f es una función biyectiva.
Falta ver que f es homomorfismo. Sean $m, n \in \mathbb{Z}$ tales que:

[4] *f es biyectiva $\iff$ f es inyectiva $\wedge$ f es sobreyectiva.*

Figura 3.1: Función de Z sobre G



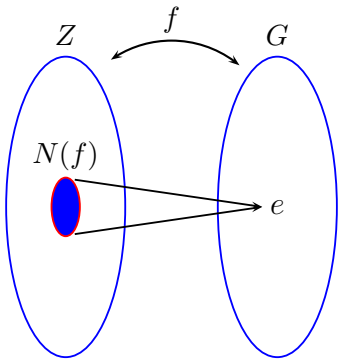
$$f(m+n) \underbrace{=}_{\text{definición de } f} g^{m+n} \underbrace{=}_{\text{propiedades de potenciación}} g^m g^n \underbrace{=}_{\text{definición de } f} f(m)f(n)$$

Por transitividad $f(m+n) = f(m) + f(n)$, entonces f es homomorfismo.
Aplicando la definición 3.4.1, $(\mathbb{Z}, +)$ es isomorfo a $(G, \cdot)$ y lo notaremos $(\mathbb{Z}, +) \approx (G, \cdot)$.
ii) Sea G_2 un grupo cíclico de orden n entonces existe $g \in G_2$ tal que:

$$\langle g \rangle = \{g, g^2, g^3, \ldots, g^{n-1}, g^n = e\} = G_2$$

con $g^i \neq g^j$ si $i \neq j$. Para la demostración de esta parte del teorema se utilizará el primer teorema de isomorfía[5]. El ejercicio consistirá en demostrar $G \approx \mathbb{Z}/n\mathbb{Z} \quad \wedge \quad \mathbb{Z}/n\mathbb{Z} \approx \mathbb{Z}n$ (ver figura 3.2).

Figura 3.2: Núcleo de una función



[5] *Sea $f : G_1 \to G_2$ un homomorfismo sobreyectivo entre los grupos G_1 y G_2 con núcleo $N(f)$ entonces $G_1/N(f)$ es isomorfo a G_2.*

$f : \mathbb{Z} \to G_2$ es un homomorfismo sobreyectivo la demostración es análoga a la parte (i) de este teorema.
f no es inyectiva lo cual se prueba al encontrar el $N(f)$.

$$\begin{aligned} N(f) &= \{m \in \mathbb{Z} : f(m) = e\} \\ &= \{m \in \mathbb{Z} : g^m = e\} \\ &= \{k \in \mathbb{Z} : k\text{es múltiplo de n}\} \qquad \text{Puesto que } O(G) = n \\ &= n\mathbb{Z} \end{aligned}$$

Como f es homomorfismo sobreyectivo y $N(f) = n\mathbf{Z}$, en virtud del primer teorema de isomorfía, $\mathbb{Z}/n\mathbb{Z} \approx G_2$.
Definamos $g : \mathbb{Z} \to \mathbb{Z}n$ tal que $g(n) = \overline{n}$, sea $m, m \in \mathbb{Z}$ entonces:

$$g(m+n) \underbrace{=}_{\text{definición de } g} \overline{m+n} \underbrace{=}_{\text{definición clas equivalencia}} \overline{m} + \overline{n} \underbrace{=}_{\text{definición de } g} g(m) + g(n)$$

de donde $g(m+n) = g(m) + g(n)$. Luego g es homomorfismo. Ahora sea $y \in \mathbb{Z}_n$ lo cual implica $y = \overline{a}$ y $a \in \mathbb{Z}$, entonces $y = g(a)$. g es sobreyectiva.
Ya tenemos que g es un homomorfismo sobreyectivo.
g no es inyectivo lo cual se prueba al encontrar el $N(g)$,

$$\begin{aligned} N(g) &= \{m \in \mathbb{Z} : g(m) = \overline{0}\} \\ &= \{m \in \mathbb{Z} : \overline{m} = \overline{0}\} \\ &= \{k \in \mathbb{Z} : k\textit{es múltiplo de } n\} \\ &= n\mathbb{Z}. \end{aligned}$$

(ver figura 3.3) En virtud del primer teorema de isomorfía se tiene $\mathbb{Z}/n\mathbb{Z} \approx \mathbb{Z}_n$. Como $\mathbb{Z}/n\mathbb{Z} \approx G_2 \quad \wedge \quad \mathbb{Z}/n\mathbb{Z} \approx \mathbb{Z}_n, \quad G_2 \approx \mathbb{Z}_n$. ■

Ejemplo 3.4.1. 1. $A = \{1, -1, i, -i\}$, $(A, \cdot)$ es isomorfo a $(\mathbb{Z}_4, +)$. En efecto; definimos $f : \mathbb{Z}_4 \to A$ tal que $f(\overline{n}) = i^n$.
(ver figura 3.4)

Para todo $\overline{n}, \overline{m} \in \mathbb{Z}_4$ entonces:

$$f(\overline{n} + \overline{m}) = f(\overline{n+m}) \underbrace{=}_{\text{definición de } f} i^{n+m} = i^n i^m \underbrace{=}_{\text{definición de } f} f(\overline{n}) \cdot f(\overline{m})$$

Figura 3.3: Isomorfismo de funciones

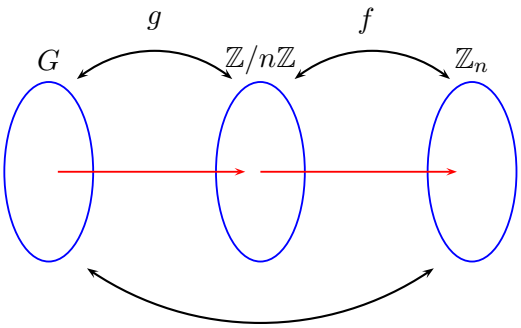
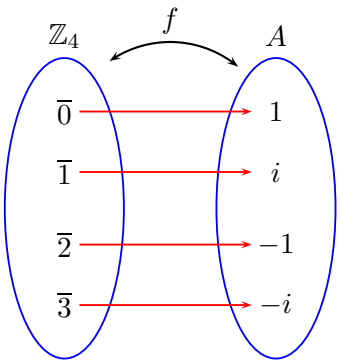


Figura 3.4: $f : \mathbb{Z}_4 \longrightarrow A$



por lo tanto $f(\overline{n}+\overline{m}) = f(\overline{n}) \cdot f(\overline{m})$. Ahora $\overline{n}, \overline{m} \in \mathbb{Z}_4$ tal que $f(\overline{n}) = f(\overline{m})$ y gracias a la definición de f, $i^n = i^m$. Así tendremos $i^n i^{-m} = i^m i^{-m} = i^0 = 1$ luego $\overline{n-m} = \overline{4} = \overline{0}$, esto es $\overline{n} - \overline{m} = \overline{0}$. Como $\overline{n} = \overline{0} + \overline{m} = \overline{m}$, $\overline{n} = \overline{m}$. Entonces f inyectiva.

Sea $y \in A$, como A es cíclico, $y = i^n$, y por la definición de f se tiene que $i^n = f(\overline{n})$, con $\overline{n} \in \mathbb{Z}_4$. Por tanto $y = f(\overline{n})$, así f es sobre.

2. Todos los subgrupos de $(\mathbb{Z}, +)$ son cíclicos. Es decir, $(H, +) \leq (\mathbb{Z}, +)$ y $H \neq \{0\}$ entonces H es cíclico. En efecto, sea $m = inf\{h | h \in H \cap \mathbb{Z}^+\}$; $m \in H$ por hipótesis $\langle m \rangle \subseteq H$, sea $h \in H$ en virtud del algoritmo de la división se tiene que $h = cm + r$ y $0 \leq r < m$ de donde $r = h - cm$ lo cual indica que $r = h + (-c)m$, entonces $r \in \langle m \rangle \subseteq H$. Como $r \in H$ en virtud de la definición de m y puesto que $0 \leq r < m$ se sigue que $r = 0$ por lo cual $h = cm$, como $h \in \langle m \rangle$ se concluye que $H \subseteq \langle m \rangle$. Se

tiene entonces $H = \langle m \rangle$.

Como se vio en el teorema 3.2.3 todo subgrupo de un grupo cíclico también es cíclico, en particular podemos demostrar que $n\mathbb{Z} \cap m\mathbb{Z}$ y $n\mathbb{Z} + m\mathbb{Z}$ son subgrupos de $\mathbb{Z}$ y por tanto son cíclicos.

Proposición 3.4.1. *Sean* $(n\mathbb{Z}, +)$ *y* $(m\mathbb{Z}, +)$ *subgrupos cíclicos de* $(\mathbb{Z}, +)$*, entonces* $(n\mathbb{Z} + m\mathbb{Z}, +)$ *y* $(nZ \cap mZ, +)$ *son subgrupos cíclicos de* $(\mathbb{Z}, +)$.

Demostración.
Veamos que $n\mathbb{Z} \cap m\mathbb{Z} \neq \varnothing$. como $0 \in n\mathbb{Z}$ y $0 \in m\mathbb{Z}$ se ve que $0 \in n\mathbb{Z} \cap m\mathbb{Z}$.
Ahora por el criterio para subgrupos se debe probar que dados $x, y \in n\mathbb{Z} \cap m\mathbb{Z}$ se tiene $x + y^{-1} \in n\mathbb{Z} \cap m\mathbb{Z}$.
Sea $x, y \in n\mathbb{Z} \cap m\mathbb{Z}$, por tanto existen $z_1, z_2 \in \mathbb{Z}$ tal que $x = mz_1$ y $x = nz_2$, y existen $z_3, z_4 \in \mathbb{Z}$ tal que $y = mz_3$ y $y = nz_4$. Entonces $x = [m, n]k_1$ y $y = [m, n]k_2$. Como

$$\begin{aligned} x + y^{-1} &= [m, n]k_1 + (-[m, n]k_2) \\ &= [m, n]k_1 - [m, n]k_2 \\ &= [m, n](k_1 - k_2) \\ &= \frac{mn}{(m, n)}(k_1 - k_2). \end{aligned}$$

$x + y^{-1} \in n\mathbb{Z}$ y $x + y^{-1} \in m\mathbb{Z}$. Se concluye entonces que $x + y^{-1} \in nZ \cap m\mathbb{Z}$ como se quería.
Ahora $n\mathbb{Z} + m\mathbb{Z} \neq \varnothing$ puesto que $0 \in n\mathbb{Z}$ y $0 \in m\mathbb{Z}$ entonces $0 = 0 + 0 \in n\mathbb{Z} + m\mathbb{Z}$.
Para ver si $n\mathbb{Z} + m\mathbb{Z}$ es subgrupo de $\mathbb{Z}$, haremos una prueba similar a la hecha con $nZ \cap mZ$, sea $x, y \in n\mathbb{Z} + m\mathbb{Z}$, existen $z_1, z_2, z_3, z_4 \in \mathbb{Z}$ tales que $x = mz_1 + n_2$ y $y = mz_3 + nz_4$. Sabemos que $y \in \mathbb{Z}$, lo cual garantiza la existencia de $y^{-1} = -(mz_3 + nz_4)$, entonces:

$$\begin{aligned} x + y^{-1} &= mz_1 + nz_2 - (mz_3 + nz_4) \\ &= mz_1 + nz_2 - mz_3 - nz_4 \\ &= m(z_1 - z_2) + n(z_3 - z_4) \end{aligned}$$

lo que implica $x + y^{-1} \in n\mathbb{Z} + m\mathbb{Z}$. Según el criterio para hallar subgrupos, se tiene que $n\mathbb{Z} + m\mathbb{Z}$ es subgrupo de $\mathbb{Z}$.

Se ha probado que tanto $(n\mathbb{Z} \cap m\mathbb{Z}, +)$ como $(n\mathbb{Z} + m\mathbb{Z}, +)$ son subgrupos de $(\mathbb{Z}, +)$. El teorema 3.2.3 garantiza que estos subgrupos son cíclicos. ■

La siguiente proposición relaciona los grupos cíclicos y los grupos cocientes mediante los subgrupos normales.

Proposición 3.4.2. *Si G es un grupo cíclico y N un subgrupo normal de G entonces G/N es un grupo cíclico.*

Demostración.
Definamos $G/N := \{g^i \in g^iN : \langle g \rangle = G\} = g^iN$ y como N es subgrupo normal de G $g^iN = Ng^i$. Consideremos $f : G \to G/N$ homomorfismo tal que $f(g^i) = Ng^i$, f es homomorfismo puesto que para todo $g^i, g^j \in G$; $i \neq j$;

$$f(g^ig^j) = N(g^ig^j) = Ng^iNg^j = f(g^i)f(g^j)$$

por transitividad de igualdades

$$f(g^ig^j) = f(g^i)f(g^j).$$

Debemos ver que para todo $g^iN \in G$ tal que $\langle g \rangle = G$ se cumple que $Ng^i = (Ng)^i$.
Para ver que todo elemento de G/N se puede escribir una como una potencia potencia de $b = Ng, Ng \in G/N$, miraremos que $f(g^i) = Ng^i$ y $f(g^i) = (Ng)^i$, como $\langle g \rangle = G$, $g^i \in G$.
Aplicando el homomorfismo f se tiene que:

$$f(g^i) = (f(g))^i = (Ng)^i$$

por lo cual $Ng^i = (Ng)^i, g^iN \in G/N$ como se quería ver. Luego $\langle gN \rangle = G/N$. ■

Proposición 3.4.3. *Sea G un grupo no abeliano entonces $G/Z(G)$ no es cíclico.*

Demostración.
Para esta prueba utilizaremos la contradicción. Supongamos $G/Z(G)$ es cíclico entonces existe $gZ(G) \in G/Z(G)$ tal que $\langle gZ(g) \rangle = G/Z(G)$ y aplicando el teorema 3.1.2

$$\langle gZ(g) \rangle = \{(gZ(G))^n : n \in \mathbb{Z}\}$$

como $Z(G)$ es subgrupo normal de G por la definición de dicho grupo tenemos:

$$(gZ(G))^n = g^n Z(G).$$

Ahora sean $g_1, g_2 \in G$, entonces $g_1 \in g^n Z(G)$ y $g_2 \in g^m Z(G)$ por lo tanto existen $h_1, h_2 \in Z(G)$ tales que $g_1 = g^n h_1$ y $g_2 = g^m h_2$. Entonces

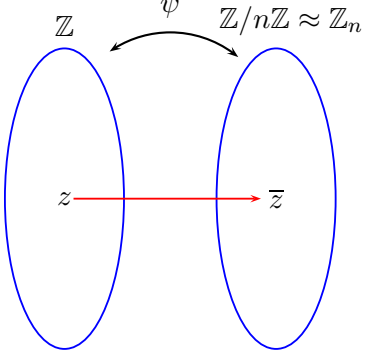
$$\begin{aligned} g_1 g_2 &= g^n h_1 g_m h_2 = h_1 g^n g^m h_2 \\ &= h_1 g^{n+m} h_2 = h_1 g^{m+n} h_2 \\ &= h_1 g^m g^n h_2 = g^m h_1 h_2 g^n \\ &= g^m h_2 h_1 g^n = g^m h_2 g^n h_1 \\ &= g_2 g_1 \end{aligned}$$

por transitividad se tiene que $g_1 g_2 = g_2 g_1$, contradicción G no es abeliano. En conclusion $G/Z(G)$ no es cíclico. ■

Proposición 3.4.4. *Sea H subgrupo de $\mathbb{Z}_n$ entonces:*
i) Existe $m \in \mathbb{Z}^+$ que divide a n tal que H es isomorfo a $m\mathbb{Z}/n\mathbb{Z}$.
ii) H es cíclico.

Demostración.
i) Definamos $\psi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ tal que para todo $z \in \mathbb{Z}$ $\psi(z) = \overline{z}$. (ver figura 3.5)

Figura 3.5: $f_{\psi} : \mathbb{Z} \longrightarrow \mathbb{Z}_n$



Existe una correspondencia biyectiva entre los subgrupos de $\mathbb{Z}n$ y los subgrupos de $\mathbb{Z}$ que contiene a $N(\psi)$. (ver figura 3.6)
entonces $N(\psi) = n\mathbb{Z}$

Figura 3.6: $N(\psi)$

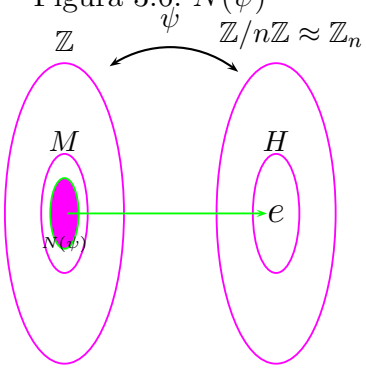
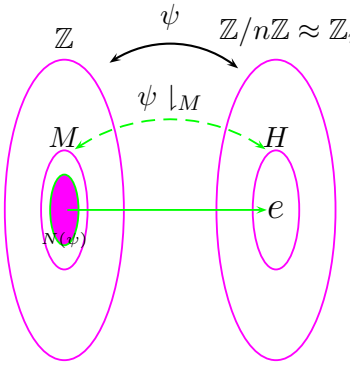


Figura 3.7: Función restringida



definamos M subgrupo de $\mathbb{Z}$ como $M = \psi^{-1}(H) = \{z \in \mathbb{Z} : \psi(z) \in H\}$, M es de la forma $m\mathbb{Z}$. Por ser ψ biyectiva se puede definir $\psi \restriction_M : m\mathbb{Z} \to H$. (ver figura 3.7)
El $N(\psi \restriction_M) = n\mathbb{Z}$ entonces $H \approx m\mathbb{Z}/n\mathbb{Z}$. Ahora si $n\mathbb{Z} \subseteq m\mathbb{Z}$, se tiene que m divide a n. En efecto, sea $n \in n\mathbb{Z}$, existe $k \in \mathbb{Z}$ tal que $n = mk$.
El recíproco de esta afirmación también es verdadera. Como $m|n$ se tiene $r \in \mathbb{Z}$ tal que $n = rm$; sea $x \in n\mathbb{Z}$ entonces existe $k \in \mathbb{Z}$ tal que $x = nk = nmk = m(rk)$ con lo cual se concluye que $m\mathbb{Z} \subseteq n\mathbb{Z}$.
ii) Como H es subgrupo de $\mathbb{Z}_n$ que es un grupo cíclico entonces H es cíclico. ■

CAPÍTULO 4

APLICACIONES DE LOS GRUPOS CÍCLICOS

Algunos resultados del álgebra moderna tienen aplicaciones dentro de ella misma o en otras ramas de las matemáticas, y no son ajenos a esta situación los grupos tratados en este trabajo de grado.
Es de gran importancia aclarar que las definiciones, los conceptos y resultados que aparecen en la primera sección de este capítulo, han sido tomados principalmente de [11].

4.1. Grupos localmente cíclicos

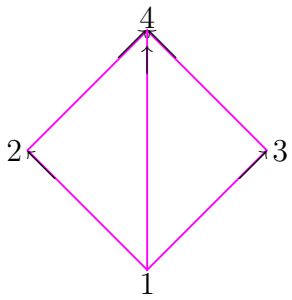
En los capítulos precedentes se trataron definiciones y resultados de los grupos cíclicos conocidos por el lector en los cursos básicos de álgebra moderna, pero estos no son los únicos resultados que se tienen de los grupos cíclicos; el hecho de que no se hayan tratado todas las conexiones de tales grupos, no indica que no existan. Son muchas las aplicaciones que tienen estos grupos en el estudio de la misma álgebra moderna, tal es el caso de su aplicación en los grupos de torsión, que no se tratará en esta monografía a la espera de que sean objeto de estudio en otro trabajo de grado.

Se considera primero su aplicación en las redes distributivas. Para tal objetivo es necesario dar unas definiciones básicas.

Definición 4.1.1. Si A es un conjunto parcialmente ordenado tal que cualesquiera dos de sus elementos a, b tienen un supremo (sup) [al que se indicara como $a \cup b$] y un ínfimo (inf) [al cual llamaremos $a \cap b$], entonces, se dice que A es una *red*; y se notara $L(A)$ o L.

Ejemplo 4.1.1. 1. Sea, $A = \{1, 2, 3, 4\}$ donde la relación inclusión esta dada por el diagrama de la figura 4.1.

Figura 4.1: Diagrama de la relación del conjunto A



$a \supseteq b$ si a está arriba de b (1 esta conectado a 3 y a 2 pero ellos no están conectados a 1) y conectada a él o si $a = b$.
Es fácil ver que A es un conjunto parcialmente ordenado según la relación inclusión. Veamos que $2, 3 \in A$ y $2, 3$ tienen supremo que es 4 y tienen también ínfimo que es 1, por lo cual A es una red.

Como tanto el ínfimo como el supremo son únicos y la unión e intersección son dos operaciones binarias bien definidas en una red, entonces se cumplen ciertas leyes que se plasman en el siguiente teorema.

Teorema 4.1.1. *En una red se verifican las siguientes leyes.*
L1. Leyes de idempotencia $x \cap x = x$ *y* $x \cup x = x$.
L2. Leyes conmutativas $x \cap y = y \cap x$ *y* $y \cup x = y \cup x$.

L3. Leyes asociativas $x \cap (y \cap z) = (x \cap y) \cap z$ *y* $x \cup (y \cup z) = (x \cup y) \cup z$.
L4. Leyes de absorción $x \cap (x \cup y) = x$ *y* $x \cup (x \cap y) = x$.

Demostración.
$L1, L2, L4$ son una consecuencia inmediata de las definiciones[6] de ínfimo y supremo.
Para L_3: Sea A un conjunto parcialmente ordenado y sean x, y, $z \in A$. Como L es una red, existe el ínfimo de y y de z, esto es $y \cap z = u$; y existe el ínfimo de x y u, $x \cap u = w$. Según la definición de ínfimo, w es cota inferior de x y u y por tanto cota inferior de x, y y z. Cualquier cota inferior de x, y y z es cota inferior de u, entonces w es el ínfimo de x, y y z por la definición de ínfimo. Equivalente a $w = x \cap (y \cap z)$.
Pero por hipótesis $L(A)$ es una red, entonces existen el ínfimo de x y y, digamos $x \cap y = k$ y existe el ínfimo de k y z, $k \cap z = t$.
De manera análoga a la indicada en el párrafo anterior, t es el ínfimo de x, y y z. Es decir $t = (x \cap y) \cap z$.
Entonces:

$$x \cap (y \cap z) = (x \cap y) \cap z.$$

Sean h y m los supremos de y, z y x, h respectivamente, $(y \cup z) = h$ y $(x \cup h) = m$, basados en la definición de supremo m es una cota superior de x y h, por tanto es cota superior de x, y y z. Puesto que cada cota superior de x, y y z también lo es de m, se tiene que m es el supremo de x, y y z en virtud de la definición de supremo. Luego $x \cup (y \cup z) = m$.
Pero por hipótesis existen el supremo de x y y, es decir $x \cup y = p$ y el supremo de p y z, digamos $p \cup z = q$. Entonces q es cota superior de p y z y por consiguiente lo es de x, y y z. Además, como cada cota superior de x, y y z lo es de q, q es el supremo de x, y y z. Luego $(x \cup y) \cup z = t$. Como el supremo es único entonces:

$$x \cup (y \cup z) = (x \cup y) \cup z.$$

■

Es natural preguntarse si existen algunas otras leyes que caractericen a las redes,por ello el siguiente teorema nos mostrara que $L1$, $L2$, $L3$, $L4$ son suficientes y necesarias para

[6] *Para una discusión más extensa sobre ínfimo y supremo, ver Introducción al análisis matemático de una variable, Bartle. Sherbert*

caracterizar las redes.

Teorema 4.1.2. *Las leyes $L1, L2, L3, L4$ caracterizan completamente las redes.*

Demostración.
En cualquier sistema que satisface $L1$,$L2$,$L3$,$L4$, $x \cap y = y$ si y solo si $x \cup y = x$.
Definamos $y \subseteq x$ si y solo si $x \cap y = y$.
Para demostrar que $L(A)$ es una red, veamos que el sistema es un conjunto parcialmente ordenado con respecto a la relación inclusión, y que dos elementos cualesquiera de A tienen supremo e ínfimo.
Sean k, x, y y z elementos de A, entonces:

1. El ínfimo de x y x es x, esto es $x \cap x = x$ equivalente a $x \subseteq x$.

2. Si el ínfimo de x y y es y y el ínfimo de y y z es z,

$$x \cap z = x \cap (y \cap z) = (x \cap y) \cap z = y \cap z = z$$

   probando que si $y \subseteq x$ y $z \subseteq y$ entonces $z \subseteq x$.

3. Si $y \subseteq x$ entonces $y \cap x = y$, si $x \subseteq y$ entonces $x \cap y = x$.
   Como $x \cap y = y \cap x$ por ley transitiva $x = y$.
   De 1, 2 y 3 se ha demostrado que bajo la definición de inclusión el sistema es un conjunto parcialmente ordenado.

4. Veamos que para todo $x, y \in A$, existe $x \cap y$ y $x \cup y$. Como:

$$x \cap (x \cap y) = (x \cap x) \cap y = x \cap y \qquad \text{y} \qquad y \cap (y \cap x) = x \cap y$$

   $x \cap y$ es una cota inferior de x y y; pero si $z \subseteq x$ y $z \subseteq y$, $x \cap z = z$ y $y \cap z = z$, lo cual implica:

$$(x \cap y) \cap z = x \cap (y \cap z) = x \cap z = z$$

   Por tanto $x \cap y$ es el ínfimo de x y y.

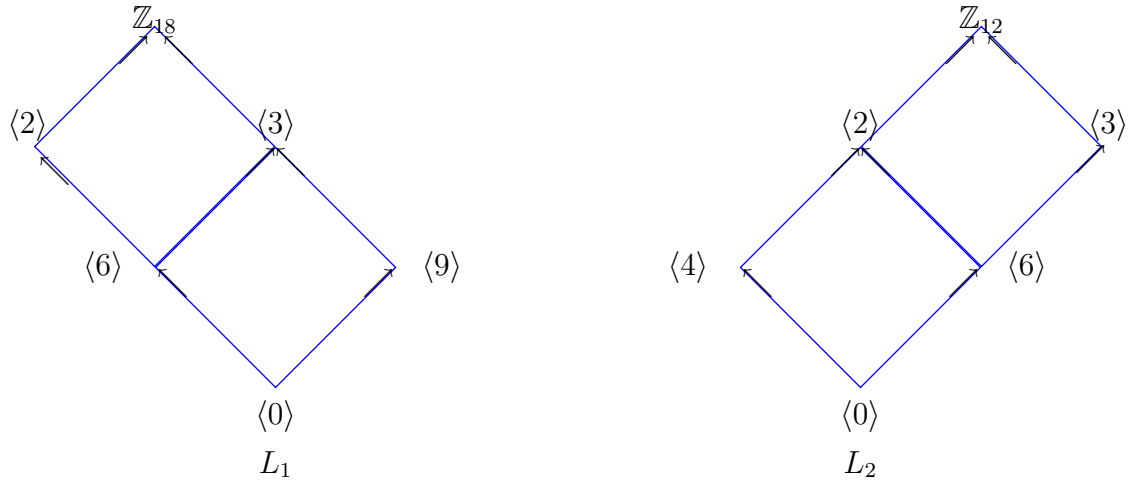
   Análogamente, si $x \subseteq k$ y $y \subseteq k$, $x \cup z = z$ y $y \cup z = z$.
   Luego $(x \cup y) \cup z$, de donde se sigue que $x \cup y$ es una cota superior, específicamente $x \cup y$ es el supremo de x y y.

Por tanto de 1,2,3 y 4 A es una red. ■

Definición 4.1.2. Una red L' se dice isomorfa a una red L'' si existe una correspondencia biyectiva $x_i \rightleftarrows y_j$ entre los elementos x_i de L' y los y_j de L'' tal que $x_i \cap x_j \rightleftarrows y_i \cap y_j$ y $x_i \cup x_j \rightleftarrows y_i \cup y_j$.

Ejemplo 4.1.2. 1. Sean L_1 y L_2 las redes correspondientes a $\mathbb{Z}_{18}$ y $\mathbb{Z}_{12}$ respectivamente (ver figura 4.2).

Figura 4.2: Redes de grupos isomorfas



Estas redes son isomorfas puesto que se puede establecer una función $\phi : L_1 \longrightarrow L_2$ biyectiva tal que cada $\phi(x_1 \cap x_2) = \phi(x_1) \cap \phi(x_2)$ y a su vez $\phi(x_1 \cup x_2) = \phi(x_1) \cup \phi(x_2)$ para cada par de elementos de la red L_1, por ejemplo:
$\phi(\langle 6\rangle \cup \langle 9\rangle) = \phi(\langle 3\rangle) = \langle 2\rangle = (\langle 6\rangle \cup \langle 4\rangle)$ y $\phi(\langle 6\rangle \cap \langle 9\rangle) = \phi(\langle 0\rangle) = \langle 0\rangle = \langle 6\rangle \cap \langle 4\rangle$.

Algunas redes poseen más propiedades, para nuestro propósito solo necesitaremos definir cuando una red es completa.

Definición 4.1.3. Una red L se dice *completa* si todo subconjunto de L tiene un supremo y un ínfimo.

Si el conjunto de todos los elementos de L tienen supremo, entonces este supremo es llamado *elemento total*, y si tiene ínfimo a este se le llamará *elemento cero*.
En el ejemplo 4.1.1, el elemento total es 4 y el elemento cero es 1.

4.1.1. Redes de subgrupos

PROPIEDADES GENERALES

Los subgrupos de un grupo G se pueden tomar como elementos de una red $L(G)$ respecto a la operación de intersección y el generado por la unión de subgrupos de un grupo. La siguiente proposición muestra que la intersección de subgrupos es un subgrupo y es precisamente el ínfimo, y que el generado por la unión es también un subgrupo y es el supremo

Proposición 4.1.1. *Sea G un grupo y H_1, H_2 subgrupos de G:*

- *$H_1 \cap H_2$ es un subgrupo de G y es el ínfimo de H_1 y H_2.*
- *$\langle H_1 \cup H_2 \rangle$ es subgrupo de G y es el supremo de H_1 y H_2.*

Demostración.
Dados $x \in H_1 \cap H_2$ y $y \in H_1 \cap H_2$, tanto x, y son elementos de H_1 y H_2, por hipótesis xy es también un elemento de H_1 y H_2, por lo tanto xy es un elemento de $H_1 \cap H_2$.
Por hipótesis e pertenece a H_1 y a H_2 entonces e pertenece a $H_1 \cap H_2$.
Dado $x \in H_1 \cap H_2$, x pertenece tanto a H_1 como a H_2, por hipótesis x^{-1} es también un elemento de H_1 y de H_2, por tanto x^{-1} es un elemento de $H_1 \cap H_2$.
Según la definición de subgrupo se tiene que $H_1 \cap H_2$ es un subgrupo de G.
Falta ver que $H_1 \cap H_2$ es el ínfimo de H_1 y de H_2. Es claro que $H_1 \cap H_2$ es una cota inferior de H_1 y de H_2. Sea K subgrupo de G una cota inferior de H_1 y H_2, entonces $K \subseteq H_1$ y $K \subseteq H_2$, de donde $K \subseteq H_1 \cap H_2$. Por tanto $H_1 \cap H_2$ es el ínfimo de H_1 y H_2.

Definamos ahora $\langle H_1 \cup H_2 \rangle =: \bigcap\{H \leq G \,:\, H_1 \cup H_2 \subseteq H\}$. Como la intersección de subgrupos es un subgrupo se tiene que $\langle H_1 \cup H_2 \rangle$ es un subgrupo de G.
Falta ver que $\langle H_1 \cup H_2 \rangle$ es el supremo de H_1 y H_2.
$H_1 \subseteq \bigcap\{H \leq G \,:\, H_1 \cup H_2 \subseteq H\}$ y $H_2 \subseteq \bigcap\{H \leq G \,:\, H_1 \cup H_2 \subseteq H\}$, por tanto $\langle H_1 \cup H_2 \rangle$ es una cota superior de H_1 y H_2.
Sea T subgrupo de G tal que $H_1 \subseteq T$ y $H_2 \subseteq T$, entonces $H_1 \cup H_2 \subseteq T$ y como $H_1 \cup H_2 \subseteq \bigcap\{H \leq G \,:\, H_1 \cup H_2 \subseteq H\}$, luego $\langle H_1 \cup H_2 \rangle \subseteq T$ quedando demostrado así que $\langle H_1 \cup H_2 \rangle$ es el supremo de H_1 y H_2. ■

Cada grupo cíclico G de orden primo tiene como subgrupos únicamente a G y al subgrupo identidad (la proposición 3.3.3 garantiza dicha afirmación), de donde se tiene que todos

los grupos cíclicos de orden primo tienen la misma red de subgrupos, que consiste en una cadena de dos elementos. Se ha demostrado ya (proposición 3.3.3) que, recíprocamente, un grupo sin subgrupo propios es la identidad o un grupo cíclico finito de orden primo.

Un grupo G determina una única $L(G)$, pero no se tiene que $L(G)$ determine únicamente a G, esto se debe a que una red puede ser isomorfa a otra (definición 4.1.2).

4.1.2. Grupos localmente cíclicos y redes distributivas

Proposición 4.1.2. *En una red L, las dos leyes distributivas*

$$\begin{aligned} D_1) \qquad & a \cap (b \cup c) = (a \cap b) \cup (a \cap c) \\ D_2) \qquad & a \cup (b \cap c) = (a \cup b) \cap (a \cup c) \end{aligned}$$

son equivalentes.

Demostración.
Veamos que D_1 implica D_2.
Usando D_1 :

$$\begin{aligned} (a \cup b) \cap (a \cup c) &= [(a \cup b) \cap a] \cup [(a \cup b) \cap c] \quad \text{por } D_1 \\ &= a \cup [(a \cap c) \cup (b \cap c)] \\ &= [a \cup (a \cap c)] \cup (b \cap c) \\ &= a \cup (b \cap c) \end{aligned}$$

Luego $(a \cup b) \cap (a \cup c) = a \cup (b \cap c)$ como se quería ver.
D_2 nos garantiza que:

$$\begin{aligned} (a \cap b) \cup (a \cap c) &= [(a \cap b) \cup a] \cap [(a \cap b) \cup c] \quad \text{por } D_2 \\ &= a \cap [(a \cup c) \cap (b \cup c)] \\ &= [a \cap (a \cup c)] \cap (b \cup c) \\ &= a \cap (b \cup c) \end{aligned}$$

Por tanto $(a \cap b) \cup (a \cap c) = a \cap (b \cup c)$ que es D_1.
■

Definición 4.1.4 (Red distributiva). Una red L se dice que es distributiva si satisface la ley:

$$D_1) \qquad a \cap (b \cup c) = (a \cap b) \cup (a \cap c).$$

La ley distributiva es una condición muy fuerte en redes.

Ejemplo 4.1.3. 1. Considérese el grupo $(S_3, \circ)$, el grupo de todas las biyecciones sobre un conjunto de 3 elementos. $S_3 = \{\rho_0, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3\}$, donde:

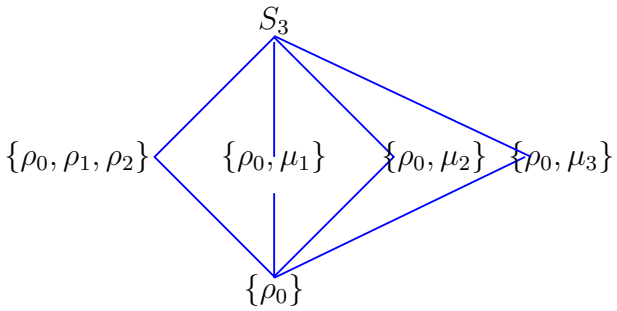
$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \qquad \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \qquad \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

$$\mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \qquad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

La figura 4.3 representa la red $L(S_3)$.

Figura 4.3: Red $L(S_3)$



Veamos si esta red es distributiva, para ello verificaremos D_1.
Tomemos los subgrupos $\{\rho_0, \mu_2\}$, $\{\rho_0, \mu_3\}$ y $\{\rho_0, \mu_1\}$, según la ley distributiva se debe cumplir que:

$$\{\rho_0, \mu_1\} \cap (\{\rho_0, \mu_2\} \cup \{\rho_0, \mu_3\}) = (\{\rho_0, \mu_1\} \cap \{\rho_0, \mu_2\}) \cup (\{\rho_0, \mu_1\} \cap \{\rho_0, \mu_3\})$$

pero: $\{\rho_0, \mu_1\} \cap (\{\rho_0, \mu_2\} \cup \{\rho_0, \mu_3\}) = \{\rho_0, \mu_1\} \cap S_3 = \{\rho_0, \mu_1\}$ y
$(\{\rho_0, \mu_1\} \cap \{\rho_0, \mu_2\}) \cup (\{\rho_0, \mu_1\} \cap \{\rho_0, \mu_3\}) = \{\rho_0\} \cup \{\rho_0\} = \{\rho_0\}$.
Entonces la red $L(S_3)$ no es una red distributiva.

A continuación se demostrará que si $L(G)$ es distributiva entonces G es localmente cíclico.

Definición 4.1.5 (Grupo localmente cíclico). Un grupo G es un *grupo localmente cíclico* si y sólo si todo conjunto finito de elementos en G genera un grupo cíclico.

Ejemplo 4.1.4. 1. Considérese el grupo $T = \{a, b, c, d\}$ con la operación suma definida por la tabla 4.1

$+$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

Tabla 4.1 Grupo $(T, +)$.

Este grupo no es cíclico, puesto que ninguno de sus elementos lo genera.

Debemos ver si todo subconjunto finito de elementos de T genera un grupo cíclico.

$\langle\{a, b\}\rangle = \{a, b\}$; $\langle\{a, c\}\rangle = \{a, c\}$;
$\langle\{a, d\}\rangle = \{a, d\}$; $\langle\{a\}\rangle = \{a\}$;
$\langle\{b, c\}\rangle = \{a, b, c, d\}$; $\langle\{b, d\}\rangle = \{a, b, c, d\}$;
$\langle\{a, b, c\}\rangle = \{a, b, c, d\}$; $\langle\{a, b, d\}\rangle = \{a, b, c, d\}$;
$\langle\{a, c, d\}\rangle = \{a, b, c, d\}$; $\langle\{b, c, d\}\rangle = \{a, b, c, d\}$;
$\langle\{b\}\rangle = \{a, b\}$; $\langle\{c\}\rangle = \{a, c\}$;
$\langle\{d\}\rangle = \{a, d\}$.

Como se ve todo subconjunto no vacío y finito de T no genera un grupo cíclico, por tanto T no es localmente cíclico.

2. El grupo $(\mathbb{Q}, +)$ es localmente cíclico.

Consideremos un subgrupo de $(\mathbb{Q}, +)$ generado por el conjunto finito de elementos $\frac{a_1}{b_n}, \frac{a_2}{b_2}, \ldots, \frac{a_n}{b_n}$.

Sus elementos deben ser números de la forma:

$$\frac{m_1 a_1}{b_1} + \frac{m_2 a_2}{b_2} + \ldots + \frac{m_n a_n}{b_n}$$

donde las m_i son enteros arbitrarios.

Éstos pueden ser expresados en la forma:

$$\frac{m_1a_1b_2\dots b_n+\dots+m_na_nb_1\dots b_{n-1}}{b_1\dots b_n}.$$

Es fácil ver que los numeradores forman un subgrupo aditivo de los enteros, y por el teorema 3.2.3 los numeradores forman un grupo cíclico que consiste en todos los múltiplos enteros de algún entero k. Así pues, el grupo consistente en los números de la forma $\dfrac{sk}{b_1b_2\dots b_n}$ es un grupo cíclico.

Consideremos el subconjunto finito de $\mathbb{Q}$, $A=\{\frac{1}{3},\frac{2}{5}\}$.
Veamos que ocurre con $\langle\{\frac{1}{3},\frac{2}{5}\}\rangle$.
$x\in\langle\{\frac{1}{3},\frac{2}{5}\}\rangle$ si y solo si $x=k_1(\frac{1}{3})+k_2(\frac{2}{5})$; $k_1,k_2\in\mathbb{Z}$, entonces:

$$\begin{aligned} x &= k_1(\frac{1}{3})+k_2(\frac{2}{5}) \\ &= \frac{k_1}{3}+\frac{2k_1}{5} \\ &= \frac{5k_1+6k_2}{15} \\ &= \frac{1}{15}(5k_1+6k_2) \end{aligned}$$

Algunos de los elementos serán $\frac{11}{15},\frac{22}{15},\frac{17}{15},0,\frac{1}{15}$; se observa que $\langle\{\frac{1}{3},\frac{2}{5}\}\rangle=\langle\frac{1}{15}\rangle$.
$\langle A\rangle$ es cíclico.

Algunas proposiciones importantes de los grupos localmente cíclicos se estudiaran a continuación:

Proposición 4.1.3. *Sea G un grupo localmente cíclico y H un subgrupo de G, entonces H es localmente cíclico.*

Demostración.
Como H es subgrupo de G, $H\subset G$ por tanto todo subconjunto finito de H es también subconjunto finito de G, por hipótesis todo subconjunto finito de G genera a un grupo cíclico luego cada subconjunto finito de H también genera a un grupo cíclico, por lo tanto H es localmente cíclico. ■

Proposición 4.1.4. *Si G es un grupo localmente cíclico, entonces G es un grupo abeliano.*

Demostración.
Sean x, y elementos de G, se debe mostrar que $xy = yx$. Sea $\langle\{x, y\}\rangle = \langle\{z\}\rangle$, sean x, y elementos de $\langle\{x, y\}\rangle$, entonces $x = z^n$ y $y = z^m$ para algunos n, m enteros.
$z^n z^m = xy$ elemento de $\langle\{x, y\}\rangle$ por lo tanto:

$$xy = z^n z^m = z^{n+m} = z^{m+n} = z^m z^n = yx$$

luego $xy = yx$ concluyendo así que G es abeliano. ■

Proposición 4.1.5. *Sea G un grupo localmente cíclico y H un subgrupo de G, entonces G/H es localmente cíclico.*

Demostración.
Sean xH, yH elementos de G/H.
Ahora:

$$\begin{aligned}
\langle\{xH, yH\}\rangle &= \{(xH)^i (yH)^j : i, j \in \mathbb{Z}\} \\
&= \{x^i H y^j H : i, j \in \mathbb{Z}\} \\
&= \{x^i y^j H : i, j \in \mathbb{Z}\} \\
&= \langle\{x, y\}\rangle H \\
&= \langle z\rangle H \\
&= \{z^k H : k \in \mathbb{Z}\} \\
&= \{(zH)^k : k \in \mathbb{Z}\} \\
&= \langle zH\rangle
\end{aligned}$$

luego $\langle\{xH, yH\}\rangle = \langle zH\rangle$, por lo tanto G/H es localmente cíclico. ■

Proposición 4.1.6. *Un grupo G es localmente cíclico si y solo si cada par de elementos de G genera a un grupo cíclico.*

Demostración.
⇒) Inmediata po la definición de grupo localmente cíclico.
⇐ Sean a, b elementos de G con $a \neq b$, por hipótesis $\langle\{a, b\}\rangle$ es cíclico, entonces todo elemento de $\langle\{a, b\}\rangle$ se puede escribir de la forma $a^{i_0} b^{j_0}$ para i_0, j_0 enteros. Luego $\langle\{a, b\}\rangle = \langle\{a^{i_0}, b^{j_0}\}\rangle$ para algún i_0, j_0 entero.

Ahora, dados a, b, c elementos de G queremos ver si $\langle\{a, b, c\}\rangle$ genera un grupo cíclico, se sabe que:

$$\langle\{a, b, c\}\rangle = \langle\{a, b\}, c\rangle$$

se debe probar que $\langle\{a^i b^j, c\}\rangle = \langle\{a, b\}, c\rangle$ donde $a^i b^j$ elementos de $\langle\{a, b\}\rangle$ con j, i fijos y $\langle a^i b^j\rangle = \langle\{a, b\}\rangle$.

Sea $x \in \langle\{a, b, c\}\rangle$, existen n, m y p enteros tales que $x = a^n b^m c^p = (a^n b^m)c^p$ pero $a^n b^m \in \langle\{a, b\}\rangle = \langle a^i b^j\rangle$, luego $a^n b^m = (a^i b^j)^q$ para algún q entero; de donde se tiene $x = (a^n b^m)c^p = (a^i b^j)^q c^p$, entonces $x \in \langle\{a^i b^j, c\}\rangle$. Se concluye que $\langle\{a, b, c\}\rangle \subset \langle\{a^i b^j, c\}\rangle$. Ahora, sea y elemento de $\langle\{a^i b^j, c\}\rangle$ por tanto existen n_0, m_0 enteros tales que:

$$y = (a^i b^j)^{n_0} c^{m_0} = a^{in_0} b^{jn_0} c^{m_0} = a^r b^s c^{m_0}$$

entonces $y \in \langle\{a, b, c\}\rangle$. Luego $\langle\{a^i b^j, c\}\rangle \subset \langle\{a, b, c\}\rangle$.

Como $\langle\{a, b, c\}\rangle \subset \langle\{a^i b^j, c\}\rangle$ y $\langle\{a^i b^j, c\}\rangle \subset \langle\{a, b, c\}\rangle$ se concluye que $\langle\{a^i b^j, c\}\rangle = \langle\{a, b, c\}\rangle$.

Como $\langle\{a, b, c\}\rangle = \langle\{a, b\}, c\rangle = \langle\{a^i b^j, c\}\rangle$ y por hipótesis cualquier par de elementos de G genera a un grupo cíclico.

Análogamente para $\langle\{a, b, c, d\}\rangle$, siguiendo este proceso se obtiene que G es localmente cíclico. ■

Teorema 4.1.3. *La red $L(G)$ es distributiva si y sólo si G es un grupo localmente cíclico.*

Demostración.

$\Longleftarrow$) Supongamos primero que G es un grupo localmente cíclico. Sean A, B, C tres conjuntos finitos cualesquiera de G.

Por propiedades de conjuntos

$$A \cap B \subseteq A \cap (B \cup C) \quad \wedge \quad A \cap C \subseteq A \cap (B \cup C)$$

Por tanto

$$(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C) \qquad (4.1)$$

Falta demostrar que $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

Sea $y \in A \cap (B \cup C)$, $y \in A \cap B \cap C$ por lo tanto donde $y \in \langle A \cap B \cap C\rangle$, pero como G es localmente cíclico; $\langle A \cap B \cap C\rangle$, luego existen $b \in B$, $c \in C$ y $a \in A$ tal que $y = bca$. Pero $\{b, c\} \subseteq G$, luego $\langle\{b, c\}\rangle$ es cíclico, por lo tanto existen enteros r, s tales

que $(bc)^r = b$ y $(bc)^s = c$.

Además,

$\{b\} \subseteq G$, luego $\langle\{b\}\rangle$ es cíclico y existe $m \in \mathbb{Z}$ tal que $b^m = b$.

$\{c\} \subseteq G$, luego $\langle\{c\}\rangle$ es cíclico y existe $n \in \mathbb{Z}$ tal que $c^n = c$.

Por lo tanto:

$$bc = (b)^m(c)^n = ((bc)^r)^m((bc)^s)^n = (bc)^{rm}(bc)^{sn} = (bc)^{rm+sn}$$

Consideremos ahora un elemento arbitrario $a \in A \cap (B \cup C)$. Aquí a es de la forma $a = bc$, $a \in A$, $b \in B$, $c \in C$, luego $a = bc = (bc)^r(bc)^s = (bc)^{r+s}$.

Se tiene que:

$$a^r = (bc)^r = ((bc)^r)^r((bc)^r)^s = b^r b^s = b^{r+s} \in A \cap B \qquad \text{y}$$
$$a^s = (bc)^s = ((bc)^r)^s((bc)^s)^s = ((bc)^s)^r((bc)^s)^s = c^r c^s = c^{r+s} \in A \cap C.$$

Entonces:

$$\begin{aligned} a &= (bc)^{r+s} \\ &= ((bc)^{rm+sn})^{r+s} \\ &= ((bc)^{rm}(bc)^{sn})^{r+s} \\ &= (bc)^{rm(r+s)}(bc)^{sn(r+s)} \\ &= ((bc)^r)^{m(r+s)}((bc)^s)^{n(r+s)} \\ &= b^{m(r+s)}c^{n(r+s)} \\ a &= (b^{r+s})^m(c^{r+s})^n \end{aligned}$$

Luego $a = (b^{r+s})^m(c^{r+s})^n$ es un elemento de $(A \cap B) \cup (A \cap C)$.

Se cumple así:

$$A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C) \qquad (4.2)$$

De (4.1) y (4.2) se tiene para todos los casos:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \qquad (D_1)$$

y como D_1 implica D_2 se tiene que $L(G)$ es distributiva.

$\Longrightarrow$) Supongamos que $L(G)$ es una red distributiva (satisface D_1 y D_2).

Sean $b, c \in G$ y $a = bc$ y $A = \langle\{a\}\rangle$, $B = \langle\{b\}\rangle$, $C = \langle\{c\}\rangle$, entonces $a \in B \cup C$.

$$A = A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \text{ por } D_1$$

Por el teorema 3.2.3 $A \cap B$ y $A \cap C$ son cíclicos, luego $A \cap B = \langle \{a, b\} \rangle$ y $A \cap C = \langle \{a, c\} \rangle$ en donde para algunos m, n, r enteros

$$a^n = b^m = ab, \qquad a^n = c^r = ac$$

En vista de que a se puede escribir como una potencia de ab y ac y como $A = \langle \{a, b\} \rangle \cup \langle \{a, c\} \rangle$ entonces

$$a = (ab)^t (ac)^s = (ac)^s (ab)^r$$

Como $a \in A$ y $a = bc$

$$bc = a = (ab)^t (ac)^s = b^{nt} c^{ns} = c^{ns} b^{nt}$$

donde $b^{1-nt} = c^{sr-1}$.
Del párrafo anterior $c^{-sr+1} = b^{nt-1}$ ó $(ac)^{-s} c = (ab)^r b^{-1}$, lo cual implica

$$cb = (ac)^s (ab)^r = (ab)^r (ac)^s = bc.$$

G es abeliano.
Miremos que G no puede contener un elemento a diferente de la identidad cuyo orden sea finito y un elemento b de orden infinito. Sea $c = ab$ un elemento de G con orden infinito y $\langle \{a\} \rangle = \langle \{a\} \rangle \cap (\langle \{b\} \rangle \cup \langle \{c\} \rangle)$ ya que $a = b^{-1} c$, mientras que:

$$(\langle \{a\} \rangle \cap \langle \{b\} \rangle) \cup (\langle \{a\} \rangle \cap \langle \{c\} \rangle) = \{e\} \cup \{e\} = \{e\} \neq \langle \{a\} \rangle$$

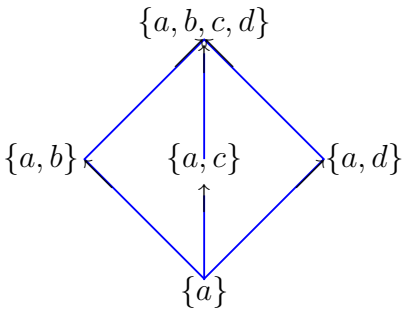
debido a que los grupos $\langle \{b\} \rangle$ y $\langle \{c\} \rangle$ de orden infinito que no contienen elementos diferentes de la identidad cuyo orden sea finito, intersecan a $\langle \{a\} \rangle$ en la identidad.
Consideremos dos casos, que G sea un grupo en el que ningún elemento excepto la identidad es de orden finito (aperiódico) y que G sea un grupo donde todos sus elementos son de orden finito (periódico).
En ambos casos si dos elementos no generan un grupo cíclico, tales elementos deben generar el producto directo de dos grupos cíclicos $\langle \{b\} \rangle$, $\langle \{c\} \rangle$.
Si G es aperiódico.
Sea $a = bc$ un elemento de G y $A = \langle \{a\} \rangle, B = \langle \{b\} \rangle$ y $\langle \{c\} \rangle$, $A = A \cap (B \cup C)$ y $(A \cap B) \cup (A \cap C) = \{e\} \cup \{e\} = \{e\}$, falla D_1.
Si G es periódico, supongamos $O(b) = m$ y $O(c) = n$ con $(m, n) = 1$, $\langle \{b\} \rangle \cup \langle \{c\} \rangle = \langle \{b, c\} \rangle$, genera un grupo cíclico según la proposición 3.3.5. Pero el producto directo de dos grupos cíclicos $\langle \{b\} \rangle$ y $\langle \{c\} \rangle$ con $(m, n) = p$, con p primo, no tiene una red $L(G)$

distributiva, veamos: $b_1 \in \langle\{b\}\rangle$ y $c_1 \in \langle\{c\}\rangle$ con $O(b_1) = O(c_1) = p$ y $a_1 = b_1c_1$, $A = A \cap (B \cup C)$ y $(A \cap B) \cup (A \cap C) = \{e\} \cup \{e\} = \{e\}$, falla D_1.
G es un grupo localmente cíclico como se afirmó. ■

Ejemplo 4.1.5. 1. El grupo $(\mathbb{Q}, +)$ es localmente cíclico, luego se tiene que la red $L(\mathbb{Q})$ es distributiva gracias al teorema 4.1.3.

2. La figura 4.4 representa la red $L(T)$ del grupo T del ejemplo 4.1.4 (1):

Figura 4.4: Red $L(T)$



Veamos si esta red es distributiva, para ello verificaremos D_1.
Tomemos los subgrupos $\{a, b\}$, $\{a, c\}$ y $\{a, d\}$, según la ley distributiva se debe cumplir que $\{a, b\} \cap (\{a, c\} \cup \{a, d\}) = (\{a, b\} \cap \{a, c\}) \cup (\{a, b\} \cap \{a, d\})$, pero:

$$\{a, b\} \cap (\{a, c\} \cup \{a, d\}) = \{a, b\} \cap \{a, b, c, d\} = \{a, b\} \quad \text{y}$$
$$(\{a, b\} \cap \{a, c\}) \cup (\{a, b\} \cap \{a, d\}) = \{a\} \cup \{a\} = \{a\}$$

Entonces la red $L(T)$ no es una red distributiva.

4.2. Aplicación de los grupos cíclicos en la cristalografía

La teoría de grupos es una parte muy importante del análisis físico y químico. Hasta aquí se ha familiarizado al lector con aquellos resultados básicos y necesarios para resolver los problemas mas sencillos de la teoría de grupos, tales como los que pueden surgir en la mecánica cuántica y en el campo de la estructura molecular. Haremos un comentario del papel que desempeñan los grupos cíclicos en la cristalografía, pues uno

de los objetivos es mostrar la utilidad de su concepto y no indagar sobre cristalografía puesto que es un trabajo ya realizado. Los grupos cíclicos utilizados en la cristalografía son los de orden finito y hacen parte de los 32 grupos puntuales utilizados para tratar los cristales de la naturaleza.

Se han realizado estudios de la aplicación de grupos en la cristalografía, tal es el caso de la monografía[7] realizada por el ***Licenciado Soren Arenas Obregon*** titulada ***aplicación de grupos en la cristalografía***, trabajo que nos dio bases para la realización de la presente monografía.

4.2.1. Representación de un grupo

Definición 4.2.1. Sean a, b y c tres elementos cualesquiera de un grupo; entonces, si $b = c^{-1}ac$, b se dice que es el *transformado* de a por c; equivalente a decir a y b son *conjugados* entre si.

PROPIEDADES

Sean a y b elementos cualesquiera de un grupo, si a y b son conjugados entre sí, se cumple:

* Cada elemento es conjugado consigo mismo.

** Si a es conjugado de b, b será conjugado de a.

*** Si a es conjugado de b y de c, b y c serán conjugados entre si.

El siguiente ejemplo ilustrara las propiedades anteriormente mencionadas.

Ejemplo 4.2.1. 1. Sea D_3 el grupo determinado por la tabla 4.2:

$*$	E	A	B	C	D	F
E	E	A	B	C	D	F
A	A	B	E	D	F	C
B	B	E	A	F	C	D
C	C	F	D	E	B	A
D	D	C	F	A	E	B
F	F	D	C	B	A	E

Tabla 4.2. Grupo $(D_3, *)$.

[7] *Para un estudio más completo aplicación de los grupos a la cristalografía ver* [10]

Cada uno de los elementos es conjugado con si mismo, veamos:

$E = A^{-1}EA$

$A = E^{-1}AE$

$B = E^{-1}BE$

$C = E^{-1}CE$

$D = E^{-1}DE$

$F = E^{-1}FE$

Además se tiene que $A = C^{-1}BC$ y $B = C^{-1}AC$ lo que garantiza la segunda propiedad, si observamos $D = B^{-1}FB$ y $D = F^{-1}CF$ también $C = D^{-1}FD$ mostrando que la tercera propiedad se cumple.

Definición 4.2.2 (Clases). Una *clase* de un grupo es el conjunto completo de elementos $a_1, a_2, \ldots, a_n$, que son conjugados entre sí.

Si el grupo contiene los elementos $a_1(= e), a_2, \ldots, a_n$, la clase de a puede ser encontrado al calcular $e^{-1}ae = a, (a_2)^{-1}aa_2, \ldots, (a_n)^{-1}aa_n$, no todos estos elementos serán distintos. Un grupo se puede separar en un cierto número de clases diferentes, todas ellas disjuntas. Es importante aclarar que si hay p elementos de un grupo que transforman un elemento dado en otro perteneciente a la misma clase, el número de elementos de dicha clase es $r = \frac{n}{p}$ donde n es el orden del grupo.

Definición 4.2.3 (Representación de un grupo). *La representación de un grupo* es el conjunto de matrices cuadradas $D(a_1)$, $D(a_2)$, ... que se pueden asociar a cada miembro de un grupo a_1, a_2, ... de tal manera que si $a_i a_j = a_k$ y $D(a_i)D(a_j) = D(a_k)$ forma por si mismo un grupo isomorfo al grupo dado.

Ejemplo 4.2.2. 1. Sea $D_3 = E, A, B, C, D, F$ el grupo dado, para hallar la representación de este grupo, haremos $X = (x_1, x_2, x_3)$ un vector y los elementos de este grupo como las operaciones que transforman a X en un nuevo vector X' con las mismas componentes pero en diferente orden. La matriz que se requiere D debe ser una matriz tal que $X' = DX$ donde filas y columnas estén identificadas con las componentes x_1, x_2, x_3. E es la operación que reemplaza cada componente por si misma, donde $D(E)$ es la matriz unidad. Por otra parte, A cambia x_1 en x_2, B cambia x_1 en x_3, y así sucesivamente, si se observa detenidamente en $D(A)$,

aparece la unidad E en la intersección de la fila x_1 con la columna x_2, en $D(B)$ la unidad E esta en la intersección de la fila x_1 y la columna x_3, etc. Siguiendo con este proceso se encuentran:

$$D(E)=\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix},\quad D(A)=\begin{bmatrix}0&1&0\\0&0&1\\1&0&0\end{bmatrix},\quad D(B)=\begin{bmatrix}0&0&1\\1&0&0\\0&1&0\end{bmatrix}$$

$$D(C)=\begin{bmatrix}1&0&0\\0&0&1\\0&1&0\end{bmatrix},\quad D(D)=\begin{bmatrix}0&0&1\\0&1&0\\1&0&0\end{bmatrix},\quad D(F)=\begin{bmatrix}0&1&0\\1&0&0\\0&0&1\end{bmatrix}$$

Al multiplicar estas matrices entre sí, se tiene:

$D(E)D(A)=D(A)$; $D(E)D(B)=D(B)$; $D(E)D(C)=D(C)$;
$D(E)D(D)=D(D)$; $D(E)D(F)=D(F)$; $D(A)D(E)=D(A)$;
$D(A)D(A)=D(B)$; $D(A)D(B)=D(E)$; $D(A)D(C)=D(D)$;
$D(A)D(D)=D(F)$; $D(B)D(E)=D(B)$; $D(B)D(A)=D(E)$;
$D(B)D(B)=D(A)$; $D(B)D(C)=D(F)$; $D(B)D(D)=D(C)$;
$D(B)D(F)=D(D)$; $D(C)D(E)=D(C)$; $D(C)D(A)=D(F)$;
$D(C)D(B)=D(D)$; $D(C)D(C)=D(E)$; $D(C)D(D)=D(B)$;
$D(C)D(F)=D(A)$; $D(D)D(E)=D(D)$; $D(D)D(A)=D(C)$;
$D(D)D(B)=D(F)$; $D(D)D(C)=D(A)$; $D(D)D(D)=D(E)$;
$D(D)D(F)=D(B)$; $D(F)D(E)=D(F)$; $D(F)D(A)=D(D)$;
$D(F)D(B)=D(C)$; $D(F)D(C)=D(B)$; $D(F)D(D)=D(A)$;
$D(F)D(F)=D(A)$.

Se reproduce la tabla dada en el ejemplo 4.1.1 para D_3, luego estas matrices son una representación de D_3

Definición 4.2.4. Una *representación es irreducible* si no es posible encontrar una transformación del tipo $Q^{-1}DQ$ (Q matriz no singular[8]) tal que cada matriz D se cambia a la forma:

$$\begin{bmatrix}D_1&0\\0&D_2\end{bmatrix}$$

[8] *La matriz A es no singular si A es invertible*

donde el orden de D_1 es m, $m < n$ y D_2 es de orden $(n-m)$ (n es el orden del grupo); además

$$Q^{-1}DQ = diag[\psi^1, \psi^2, \psi^3, \ldots, \psi^s] = \Psi \qquad (4.3)$$

donde las $\psi^{(i)}$ son matrices.

Si hay p elementos en el grupo entonces hay p ecuaciones como (4.3), una para cada elemento. Además, si existen q clases de elementos en el grupo, hay exactamente q representaciones irreducibles diferentes y

$$(d_1)^2 + (d_2)^2 + \ldots + (d_q)^2 = p \qquad (4.4)$$

donde d_j es la dimension de ψ^i. Es importante aclarar que dos representaciones irreducibles son siempre ortogonales[9].

Ejemplo 4.2.3. 1. Encontraremos todas las representaciones irreducibles de D_3. El orden de D_3 es 6, veamos cuántas clases tiene este grupo, como se menciono las clases de D_3 se pueden encontrar al calcular:

$E^{-1}AE = A$ $A^{-1}AA = E$ $B^{-1}AB = A$ $C^{-1}AC = B$ $D^{-1}AD = B$
$F^{-1}AF = B$
$E^{-1}BE = B$ $A^{-1}BA = B$ $B^{-1}BB = E$ $C^{-1}BC = A$ $D^{-1}BD = A$
$F^{-1}BF = A$
$E^{-1}CE = C$ $A^{-1}CA = D$ $B^{-1}CB = F$ $C^{-1}CC = C$ $D^{-1}CD = F$
$F^{-1}CF = D$
$E^{-1}DE = D$ $A^{-1}DA = F$ $B^{-1}DB = D$ $C^{-1}DC = F$ $D^{-1}DD = D$
$F^{-1}DF = C$
$E^{-1}FE = F$ $A^{-1}FA = C$ $B^{-1}FB = D$ $C^{-1}FC = D$ $D^{-1}FD = C$
$F^{-1}FF = F$

Se observa que solo existen 3 clases:

$$(\zeta_1)^+ = \{E, A, B\} \quad (\zeta_2)^- = \{C, D, F\} \quad \zeta_3 = \{A, B, C, D, F\}$$

resulta de (4.4) que las dimensiones de las representaciones son 1, 1 y 2. Para encontrar las dos representaciones de grado 1, debemos considerar el grupo cociente dado por la tabla 4.3:

[9] *A es ortogonal si $AA^T = A^TA = I$*

	$\hbar$	$\Im$
$\hbar$	$\hbar$	$\Im$
$\Im$	$\Im$	$\hbar$

Tabla 4.3. Grupo cociente.

con $\hbar = \{E, A, B\}$ asociado a $[1]$ y $[-1]$ asociada a $\Im = \hbar C = \{C, D, F\}$, con dos clases, ζ^+ que contiene a $\hbar$, y ζ^- que contiene a $\Im$. Sus dos representaciones de primer grado son $\psi^1(\zeta^+) = \psi^1(\zeta^-) = 1$ (se construye una función tal que las permutaciones impares de esta representación de D_3 sean enviadas a 1), $\psi^2(\zeta^+) = 1$ y $\psi^2(\zeta^-) = -1$.

Para obtener las representaciones de dos dimensiones, se deben reducir las matrices que aparecen en el ejemplo 4.1.2 para lo cual se utiliza la matriz ortogonal[10]

$$Q = \begin{bmatrix} \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & 0 & -\sqrt{\frac{2}{3}} \end{bmatrix}$$

para $D(A)$, obtenemos

$$Q^{-1}D(A)Q = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ 0 & -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix}$$

Las demás matrices se reducen de la misma forma. Se obtienen así todas las representaciones irreducibles:

$\psi^1(E) = \psi^1(A) = \psi^1(B) = \psi^1(C) = \psi^1(D) = \psi^1(F) = 1$

$\psi^2(E) = \psi^2(A) = \psi^2(B) = 1$

$\psi^2(C) = \psi^2(D) = \psi^2(F) = -1$

$$\psi^3(E) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad \psi^3(A) = \begin{bmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix} \qquad \psi^3(B) = \begin{bmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix}$$

$$\psi^3(C) = \begin{bmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix} \qquad \psi^3(D) = \begin{bmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix} \qquad \psi^3(F) = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$$

[10] *Argumentación dada por Baver,≪ introduction a la théorie desgroupes, París, 1933, pág 79≫*

Es fácil ver que dichas representaciones son ortogonales (se deja como ejercicio para el lector por ser un problema de algebra lineal).

Definición 4.2.5 (Carácter). El *carácter*[11] es la traza o magnitud de las representaciones irreducibles de un grupo.

El carácter de ψ^i se indicara por $\chi^i = \chi^i(A_1), \chi^i(A_2)$, etc. En los elementos de una misma clase el carácter es idéntico debido a que los elementos de una misma clase se obtienen unos de otros por una transformación desemejanza.

La tabla 4.4 recopila todos los caracteres, las columnas indican las clases y las filas las representaciones irreducibles

	ζ_1	ζ_2	$\cdots$	ζ_s
ψ^1	$(\chi_1)^1$	$(\chi_2)^1$	$\cdots$	$(\chi_s)^1$
ψ^2	$(\chi_1)^2$	$(\chi_2)^2$	$\cdots$	$(\chi_s)^2$
$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$
ψ^s	$(\chi_1)^s$	$(\chi_2)^s$	$\cdots$	$(\chi_s)^s$

Tabla 4.4 Caracteres.

4.2.2. Un grupo especial

El grupo Cíclico de orden n es considerado un grupo especial puesto que si a partir de $\{A\}$, se forma un grupo cíclico, $A^n = e$ y X es un elemento del grupo definido por $X = A^m$, $m = 1, 2, \ldots, n$, entonces $X^{-1}AX = A$.
Cada elemento de un grupo cíclico forma por si solo una clase, además por (4.4) se puede ver que las n representaciones irreducibles serán todas de primer grado, por lo cual cada representación sera también un carácter.
Si $\xi = exp(2\Pi\frac{i}{n})$, ξ sera una representación y carácter para A y ξ^m sera un carácter para $A^m(m = 1, 2, \ldots, n)$ puesto que estos n números satisfacen las propiedades de multiplicación de los elementos de un grupo. La misma razón garantiza que ξ^{2m} sera un conjunto de caracteres, las n distintas potencias de $\xi^m(m = 1, 2, \ldots, n)$ deducen los n caracteres de cada uno de los n elementos del grupo.
Si se usa el teorema de Moivre:

[11] *El carácter es tratado con detalle en D. E. Littlewood, ≪ Theory of Group character≫, Oxford University Press,1940*

$$\xi^p = \cos 2\pi\tfrac{p}{n} + i \sin 2\pi\tfrac{p}{n}$$

simplifica la tabla de dichos caracteres. Por ejemplo si $n = 4$ en la tabla los únicos números que aparecen son ± 1 y $\pm i$.

	$\mathbf{C} = A^n = e$	$\mathbf{C_2} = A$	$\mathbf{C_3} = A^2$	...	$\mathbf{C_n} = A^{n-1}$
ψ^1	1	1	1	...	1
ψ^2	1	ξ	ξ^2	...	ξ^{n-1}
$\vdots$	$\vdots$	$\vdots$	$\vdots$	...	$\vdots$
ψ^m	1	ξ^{m-1}	$\xi^{2(m-1)}$	...	$\xi^{(n-1)(m-1)}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	...	$\vdots$
ψ^n	1	ξ^{n-1}	$\xi^{2(n-1)}$	...	$\xi^{(n-1)^2}$

Tabla 4.5 Tabla general de caracteres de los grupos $\mathbf{C_n}$.

Se muestra a continuación la tabla 4.6, que representa los caracteres para los grupos cíclicos.

$\mathbf{C_1}$	e
$A; x, y, z$	1

$\mathbf{C_2}$	e	C_2
$A; z$	1	1
$B; x, y$	1	-1

$\mathbf{C_3}$	e	C_3	$(C_3)^2$
$A; z$	1	ε^*	ε
$e; x \pm iy$	1	ε	ε^*

$$\varepsilon = e^{\frac{2\pi i}{n}}$$

$\mathbf{C_4}$	e	C_2	C_4	$(C4)^3$
$A; z$	1	1	1	1
B	1	1	-1	-1
$e = x \pm iy$	1	-1	$-i$	i
	1	-1	i	$-i$

$\mathbf{C_6}$	e	C_6	C_3	C_2	$(C_3)^2$	$(C_6)^5$
$A; z$	1	1	1	1	1	1
B	1	-1	1	-1	1	-1
e_1	1	$-\varepsilon^*$	$-\varepsilon$	1	$-\varepsilon^*$	$-\varepsilon$
	1	$-\varepsilon$	$-\varepsilon^*$	1	$-\varepsilon$	$-\varepsilon^*$
$e_2 = x \pm iy$	1	ε^*	$-\varepsilon$	-1	$-\varepsilon^*$	ε
	1	ε	ε^*	-1	ε	ε^*

$$\varepsilon = e^{\frac{2\pi i}{6}}$$

Tabla 4.6 Caracteres de los grupos cíclicos.

4.2.3. Nociones de cristalografía

Sistemas cristalográficos*[12] *y redes de Bravais

Definición 4.2.6 (Cristal). Un *cristal* o solido pude ser definido como un rango periódico de átomos o moléculas en 3 dimensiones.

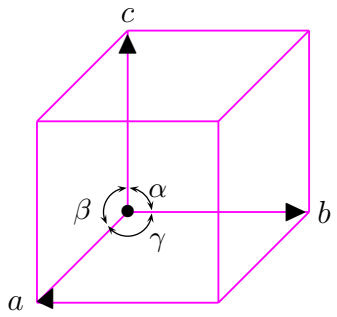
Un cristal está limitado por caras, las intersecciones de estas caras se llaman aristas, y la intersección de las aristas se conocen como vertices.

Definición 4.2.7 (Red). Una *red* es una entidad matemática donde se ignora la composición atómica real del cristal y los átomos son sustituidos por un conjunto de puntos imaginarios que guardan una relación fija con el rango atómico real.

El conjunto de puntos de una red se puede construir imaginando un espacio dividido por tres conjuntos de planos paralelos entre si e igualmente espaciados produciendo un conjunto de celdas idénticas en tamaño, forma y orientación.
Como todas las celdas son idénticas, se pueden separar y cada una de ellas se llama celda unitaria, si colocamos puntos de red en los vertices de las celdas unitarias se construyen sistemas cristalográficos conocidos como redes de Bravais, estos sistemas se enfocan como una consecuencia de la distribución de los átomos, iones o moléculas, en el espacio $\mathbf{R^3}$. Las fuerzas que unen entre si a los átomos, hacen que éstos tomen formas geométricas específicas. Se hablan de 14 redes de Bravais distribuidas de la siguiente manera:

[12] *Parga, Manuel. Conceptos básicos de cristalografía.*

Figura 4.5: Celda unitaria perteneciente a una red de puntos



7 constituidas por celdas unitarias primitivas (aquellas que poseen puntos solo en los vértices), y 7 constituidas por celdas unitarias no primitivas (aquellas que poseen más de un punto de red por celda).

Las 14 redes de Bravais se muestran en la tabla 4.7:

SISTEMAS CRISTALOGRÁFICOS	TIPOS DE REDES
Cúbico	Simple
	Centrado en el cuerpo
	centrado en las caras
Tetragonal	Simple
	Centrado en el cuerpo
Rómbico	Simple
	Centrado en el cuerpo
	Centrado en las caras
	Centrado en las bases
Romboédrico	Simple
Monoclínico	Simple
	Centrado en las bases
Triclínico	Simple
Hexagonal	Simple

Tabla 4.7 Redes de Bravais

Al considerar todas las operaciones que transforman figuras geométricas solidas en ellas

mismas, se obtiene un número de subgrupos finitos de $\mathbf{R^3}$ a los cuales llamaremos grupos de puntos cristalográficos.
Estos grupos cumplen cuatro propiedades fundamentales que son:

1. Rotación propia C_n en un ángulo $\varphi = 2\frac{\pi}{n}$ al rededor de un eje de rotación de orden n (indica el número de veces que se debe repetir la operación para que el cuerpo vuelva a su posición original).

2. Reflexión en un plano, indicada por σ_h σ_d, σ_v donde h, d y v se refieren a los planos horizontal, diagonal y vertical respectivamente (intercambia puntos situados en los lados opuestos de un plano).

3. Rotación impropia S_n (es un proceso en dos etapas: una rotación de $2\frac{\pi}{n}$ radianes, seguida de una reflexión en un plano perpendicular al eje de rotación).

4. Inversión, indicada por I (cada punto se intercambia con uno correspondiente al lado opuesto del centro de simetría. Por ejemplo, si el punto (z, y, z) es enviado a $(-x, -y, -z)$ existe una inversión respecto a $(0, 0, 0)$).

Los elementos de estos grupos son conjugados escogidos de tales operaciones junto con un elemento unidad que deja inalterado cada punto. Existen 32 grupos para tratar los cristales de la naturaleza, como existen algunos isomorfos entre los grupos, no es necesario construir 32 tablas de caracteres.
Los siguientes son los símbolos y nombres de tales grupos:

- Grupos cíclicos $\mathbf{C_n}$ $(n = 1, 2, 3, 4, 6)$
- Grupos diédricos D_n $(n = 2, 3, 4, 6)$
- Grupos cúbicos T y O

Los restantes grupos $C_{nh}(n = 1, 2, 3, 4, 6)$; C_{nv} y $D_{nh}(n = 2, 3, 4, 6)$; $D_{nd}(n = 2, 3)$; $C_{ni}(n = 1, 3)$; S_4, T_h, T_d y O_h, o son isomorfos con algún grupo precedente de la lista o son el producto directo de algún grupo de esta por I siendo I isomorfo con C_2.

4.2.4. Grupo cíclico de orden n. ($\mathbf{C_n}$)

Nuestra atención estará centrada en el grupo $\mathbf{C_n}$ (Grupo cíclico de orden finito), este grupo contiene elementos de la forma C_n, es útil denotar una clase del grupo $\mathbf{C_n}$ con

el símbolo C_n; en caso de que un número anteponga a $C_n(n = 1, 2, 3, 4, 6)$, éste será el número de elementos de tal clase, en caso contrario dicha clase tendrá un elemento.
El grupo $\mathbf{C_n}$, es el grupo de todas las rotaciones en torno a un eje n-ario; como este grupo es cíclico es generado por uno de sus elementos c, los demás elementos tienen la forma: $(c_n)^k$ con $k = 0, 1, 2, \ldots, n-1$. Claramente este grupo es conmutativo y su orden es n.

Ejemplo 4.2.4. 1. El conjunto de rotaciones en torno a un eje cuaternario de moléculas C_4H_8 (Ciclobutano) y en torno a C_6H_2 (Ciclohezano), estos están contenidos en $\mathbf{C_4}$ y $\mathbf{C_6}$ respectivamente. Entonces los cuatro átomos de C (C_4) pertenecen a $\mathbf{C_4}$ y los seis átomos de C (C_6) pertenecen a $\mathbf{C_6}$. Es de utilidad observar las gráficas de la figura 4.6.

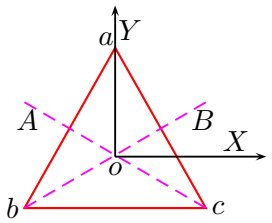
Figura 4.6: Moléculas de ciclobutano y ciclohexano

El grupo $\mathbf{C_1}$ contiene solamente el elemento identidad e, por lo tanto este es el correspondiente a la ausencia total de simetría.

4.2.5. Clasificación de los grupos puntuales cristalográficos $\mathbf{C_n}$

Grupo $\mathbf{C_3}$: Consideremos los vertices de un triángulo equilátero en el plano XY como lo muestra la figura 4.7. Sean las rotaciones del triángulo (contraria a las manecillas del reloj) en torno al eje Z, los elementos de $\mathbf{C_3}$ son 120^o, 240^o y $360^o = e$. Claramente el producto de dos elementos se define como una operación seguida a la otra. Así $C_3(C_3)^2$ equivale a $(C_3)^2$ seguida de C_3 (ó una rotación de 240^o seguida de 120^o para ser equivalente a la identidad).
El triángulo abc es equivalente, sus vertices a, b, c son equivalentes y los ejes OA y OB son fijos en el espacio.

Figura 4.7: Representación del grupo cíclico $\mathbf{C_3}$



La tabla 4.8 representa el grupo $\mathbf{C_3}$:

	e	C_3	$(C_3)^2$
e	e	C_3	$(C_3)^2$
C_3	C_3	$(C_3)^2$	e
$(C_3)^2$	$(C_3)^2$	e	C_3

Tabla 4.8 Grupo $\mathbf{C_3}$

Los demás grupos $\mathbf{C_n}$, se trabajan de manera similar. Por ejemplo el grupo $\mathbf{C_4}$ se representa considerando los vertices de un cuadrado, se realiza un proceso similar al expuesto anteriormente; para $\mathbf{C_6}$ la figura geométrica a utilizar será un exágono regular.

La clasificación de los grupos $\mathbf{C_n}$ se muestra en la tabla 4.9.

Símbolos	Generadores	Sistemas Cristalográficos
$\mathbf{C_1}$	e	Triclínico
$\mathbf{C_2}$	Rotación de 180^o	Monoclínico
$\mathbf{C_3}$	Rotación de 120^o	Romboédrico
$\mathbf{C_4}$	Rotación de 90^o	Tetragonal
$\mathbf{C_6}$	Rotación de 60^o	Hexagonal

Tabla 4.9 Clasificación de los grupos $\mathbf{C_n}$.

Nota: Si el lector desea indagar más acerca de la aplicación de la teoría de grupos en la cristalografía, se recomienda ver la bibliografía dada al final del trabajo.

BIBLIOGRAFÍA

[1] KADEMOVA. Krasimira *Matemática avanzada para físicos e ingenieros.* Parte II. Bucaramanga: UIS, 1981.

[2] HOLLINCSWORTH, Charles A. *Vectores matrices y teoria de grupos para cientificos e ingenieros.* Departamento de química, University of Pittsburg, Continental, 1969.

[3] MILLER, G. A. BLICHEFLDT, H. I., DICKSON, L. E. *Theory and applications of groups.* New York, Dover publications.inc. 1961.

[4] FUCHS, Laszlo.*Infinite Abelian Groups.*Volumen II, Louisiana: Tulane University New Orleans, 1973.

[5] ZASSENHAUS, Hans J. *The theory of groups.* Segunda edición. New York: Chelsea Publishing Company, 1958.

[6] DORRONSORO, José. y HERNÁNDEZ, Eugenio. *Álgebra moderna.* Addison-Wesley Iberoamericana S.A. 1996.

[7] FRALEIG, Jhon B.*Álgebra Abstracta.* Addison-Wesley Iberoamericana S.A. 1987.

[8] FRANK AYRES, JR.*Teoría y problemas de Álgebra moderna.* México: MC Graw Hill, 1979.

[9] HERSTEIN,I. N. *Álgebra moderna.* Editorial Trillas, 1973.

[10] ARENAS, Soren. *Aplicación de la teoría de grupos en la cristalografía.* Monografía: UIS, 1991.

[11] MARSHALL, Hall Jr. *Teoría de los grupos.* Centro Regional de Ayuda Tecnica (A.I.D.) Editorial F. Trillas, México 1979.

[12] MARGENAU H., MOSELEY G. *Las matemáticas de la física y de la química.* Madrid, MNMII. 1943.

[13] MARTÍNEZ C. Arturo *Álgebra Moderna.* UIS, Bucaramanga 1976.

[14] APONTE C. Rafael A. *Notas personales.* UIS. Bucaramanga

[15] RODRIGUEZ L., Jaime. *Fundamentos de Cristalografía Física.* OEA, 1986.