Teoría básica de grupos

Fernando Andrés Benavides
Wilson Fernando Mutis

Editorial
Universidad de Nariño

Editorial
Universidad de **Nariño**

TEORÍA BÁSICA DE GRUPOS

TEORÍA BÁSICA DE GRUPOS

Fernando Andres Benavides Agredo
Wilson Fernando Mutis Catero

Editorial
Universidad de Nariño

Benavides Agredo, Fernando Andrés
Teoría básica de grupos /Fernando Andrés Benavides Agredo, Wilson Fernando Mutis Cantero. - 1ª. Ed.- -San Juan de Pasto: Editorial Universidad de Nariño, 2024
141 p. : ilustraciones, gráficas, tablas.

Incluye referencias bibliográficas p. 126-127 y reseña de los autores p. 128
ISBN: 978-628-7679-49-8

1. Matemáticas—Teoría de grupos. 2. Algebra abstracta—Grupos y subgrupos 3. Operaciones binarias. 4. Grupos cíclicos 5. Subgrupos normales 6. Grupos abelianos. I. Mutis Cantero, Wilson Fernando

512.2 B456t – SCDD-Ed. 22

Sección de Biblioteca "Alberto Quijano Guerrero"

Teoría Básica de Grupos

©Fernando Andés Benavides Agredo
fandresbenavides@udenar.edu.co
©Wilson Fernando Mutis Cantero
wilsonmutis@udenar.edu.co

ISBN digital: 978-628-7679-49-8
Primera edición

Corrección de estilo: Ricardo Erazo Mera
Diseño de portada: Nathaly Johana Rivadeneira
Diagramación: Fernando Andrés Benavides Agredo

Fecha de publicación: abril de 2024
San Juan de Pasto - Nariño - Colombia

Índice general

Introducción

En el vasto y complejo universo de las matemáticas, hay un área que destaca por su elegancia y profundidad: el álgebra abstracta. Es un campo que despierta la curiosidad del intelecto, llevando al lector a explorar las estructuras algebraicas más esenciales y fundamentales.

Si bien el álgebra abstracta como campo formal de estudio no existía en la antigüedad, muchos conceptos algebraicos básicos se desarrollaron en culturas antiguas como la babilónica, la egipcia y la griega. Por ejemplo, los antiguos babilonios tenían tablas de arcilla que mostraban cómo resolver ecuaciones cuadráticas, y los griegos comenzaron a estudiar la teoría de números y las propiedades de los números enteros y racionales. Durante la edad media y el renacimiento, los matemáticos comenzaron a investigar las propiedades algebraicas de estructuras abstractas. Por ejemplo, François Viète, un matemático francés del siglo XVI, desarrolló la notación algebraica moderna y resolvió problemas algebraicos utilizando métodos simbólicos.

Esta área como campo distinto de estudio comenzó a tomar forma en el siglo XIX. Uno de los hitos clave fue el trabajo de Niels Henrik Abel y Évariste Galois en la teoría de ecuaciones y la teoría de grupos. Galois introdujo el concepto de grupo y desarrolló la teoría de grupos para resolver el problema de la solubilidad de las ecuaciones polinómicas por radicales. Este trabajo sentó las bases para gran parte del álgebra abstracta moderna. Posteriormente, durante el siglo XX, el álgebra abstracta experimentó un rápido desarrollo y se convirtió en un campo central en las matemáticas. Grupos como el de Bourbaki tuvieron un impacto significativo en la formalización y unificación de diferentes áreas del álgebra abstracta. Además, se desarrollaron otras estructuras algebraicas como anillos,

cuerpos, módulos y espacios vectoriales, y se establecieron conexiones profundas entre ellas.

La teoría de grupos es una rama fundamental del álgebra abstracta que estudia conjuntos algebraicos estructurados con una operación binaria, llamada operación de grupo, que satisface ciertas propiedades axiomáticas, como la cerradura, la asociatividad, la existencia de elemento neutro y la existencia de inversos. Los grupos son herramientas poderosas para modelar y entender simetrías en diversas áreas, como la geometría, la física y la química. Por ejemplo, en geometría, los grupos de simetría describen las transformaciones que preservan la forma de un objeto, en física los grupos de Lie se utilizan para estudiar simetrías en teorías fundamentales como la mecánica cuántica y la relatividad, mientras que la teoría de números, es esencial en la criptografía y la seguridad informática, como se puede evidenciar en los trabajos de Myasnikov *et al.* (2008), Ameta y Ameta (2016) y Tang *et al.* (2022).

Esta área de las matemáticas permite a los estudiantes desarrollar habilidades analíticas, en resolución de problemas, de abstracción y generalización, entre otras. Por ejemplo, al abstraer conceptos comunes a diferentes áreas de las matemáticas y generalizarlos en términos de estructuras algebraicas facilita el estudio unificado de diversos problemas matemáticos y proporciona herramientas poderosas para resolverlos. Aquellos estudiantes que desarrollen estas habilidades les permitirán pensar de manera lógica y a elaborar argumentos matemáticos rigurosos, cualidades que son valiosas en una amplia gama de campos profesionales. En resumen, la teoría de grupos es un componente crucial en la formación de matemáticos, licenciados en matemáticas, físicos entre otros, ya que les proporciona las habilidades y el conocimiento necesarios para abordar problemas matemáticos complejos, realizar investigación en diversas áreas de las matemáticas y aplicar los conceptos matemáticos en una variedad de campos, incluyendo la informática y la criptografía.

En este libro, nos sumergiremos en el fascinante mundo de la teoría de grupos, donde los números y las operaciones adquieren una nueva dimensión de significado. Aquí, no nos limitamos a manipular números familiares; en su lugar, exploramos conjuntos abstractos dotados de propiedades algebraicas que desafían la intuición y estimulan el pensamiento creativo. A medida que se avanza por las páginas de este libro, se descubre la belleza intrínseca de las estructuras algebraicas, iniciando con el estudio de operaciones binarias distintas a las comúnmente usadas, continuando con algunos de los grupos más simples como son los cíclicos y aquellos formados por las simetrías de un polígono regular, hasta finalizar con uno de los teoremas más importantes de esta área como el de la clasificación de los grupos abelianos finitamente generados. Cada capítulo es una invitación a explorar un nuevo concepto, a desentrañar sus misterios y a deleitarse con su elegancia matemática.

En el capítulo 1 se hace una presentación extensa de conceptos básicos de relaciones, funciones inyectivas y sobreyectivas, relaciones de equivalencia y operaciones binarias. En la construcción de este capítulo se tomaron en cuenta principalmente el texto de Ayres y Jaisingh (2004) y el texto de Judson y Austin (2020) así como material recuperado de la web como Revilla (2019), Escribano (2019), Gonzáles (2019). En el 2 se incluyen

definiciones y ejemplos básicos de la estructura de grupo, subgrupo y orden de un grupo.

En los capítulos 3 y 4 se desarrollan tipos especiales de grupos que serán de gran importancia, con el fin de clasificar los grupos abelianos finitamente generados. En el capítulo 3 se hace un estudio detallado del grupo de permutaciones y del grupo dihédrico. En el capítulo 4 se presentan los grupos cíclicos y se hace una introducción a aquellos grupos generados por un número finito de elementos. En el capítulo 5 se definen los subgrupos normales los cuales se utilizan para generar relaciones de equivalencia y dotar al conjunto cociente de estructura de grupo. Para estos capítulos se estudiaron los textos de Gallian (2017), Judson y Austin (2020) y Lezama (2019) y el material recuperado de la web como Olazábal (2019), Ikenaga (2022b,a), Conrad (2022).

Los capítulos 6 y 7 presentan los homomorfismos e isomorfismos de grupos y los productos directos externos e internos de grupos. En el primer caso, este tipo particular de funciones entre grupos permiten estudiar en detalle la estructura de distintas clases de grupos mediante algunos ya conocidos. En el segundo, se crean nuevos grupos a partir de algunos grupos dados, los cuales son de importancia para comprender la clasificación de los grupos abelianos finitamente generados. En la construcción de estos capítulos se tuvieron en cuenta los textos de Gallian (2017) y Dummit y Foote (1991) así como los documentos Beshenov (2023), Marklof (2023), Smith (2023).

El último capítulo presenta la clasificación de los grupos abelianos finitamente generados. Esta clasificación, se realiza mediante el uso de la Forma Normal de Smith de una matriz con componente enteras, la cual es el análogo de la forma escalonada reducida de una matriz con componentes reales. Además, se estudiaron los artículos de Bradley (1971) y Newman (1997), el texto de Norman (2012) y el material descargado de la web de Villarreal (2023).

Finalmente, bien seas un estudiante ávido de conocimiento, un investigador en busca de inspiración o simplemente un amante de las matemáticas, este libro te guiará a través de un viaje enriquecedor por las profundidades de la teoría de grupos. Prepárate para desafiar tus convicciones, expandir tu comprensión y maravillarte ante la belleza de las estructuras algebraicas ocultas que subyacen en el tejido mismo de las matemáticas.

¡Bienvenido!

Los autores
Universidad de Nariño
Abril de 2023

CAPÍTULO 1

Relaciones y operaciones binarias

Los conceptos de relación y función son de gran importancia en la Teoría de Grupos. En particular los conceptos de operación binaria y relación de equivalencia, puesto que el primero permite definir el concepto de Grupo, y mediante el segundo se construye un tipo importante de grupos que son los grupos cocientes. Por otro lado, será de gran importancia tener claro las relaciones entre una función y su imagen inversa.

1.1 Producto Cartesiano y funciones

En matemáticas existen distintos tipos de relaciones entre los elementos de dos conjuntos, el tipo más importante de relación es el de función. A continuación se presentan conceptos básicos de las relaciones entre dos conjuntos.

Definición 1.1. El producto cartesiano entre los conjuntos A y B, se denota por $A \times B$ y se define como

$$A \times B = \{(a, b) \ : \ a \in A, \ b \in B\}.$$

Un elemento de $A \times B$ se denomina pareja o par ordenado.

Por ejemplo, si $A = \{1, 2\}$, $B = \{u, v, w\}$ y $C = \emptyset$, entonces

$$A \times B = \{(1, u), (2, u), (1, v), (2, v), (1, w), (2, w)\} \text{ y } A \times C = \emptyset.$$

Note que si $|A| = n$ y $|B| = m$, entonces $|A \times B| = nm$. En general, el producto cartesiano entre los conjuntos $A_1, A_2, \ldots, A_n$ se define como

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) \ : \ a_i \in A_i, \ i = 1, 2, \ldots, n\}.$$

Si $A = A_i$ para todo $i = 1, 2, \ldots, n$, entonces el producto cartesiano entre los conjuntos $A_1, A_2, \ldots, A_n$ se denota por A^n.

Definición 1.2. Una relación de A en B es cualquier subconjunto del producto cartesiano $A \times B$. Una función f de A en B es una relación en la cual para cada $a \in A$ existe un único elemento $b \in B$ tal que $(a, b) \in f$.

Un función $f \subset A \times B$ se denotará por $f : A \longrightarrow B$ y el par ordenado $(a, b) \in f$ por $f(a) = b$. El conjunto A es llamado el dominio de f y el conjunto

$$f(A) = \{ \ f(a) \ : \ a \in A\},$$

el rango de f. Por ejemplo, la relación $\mathcal{R}_1 = \{(1, b), (2, c), (3, c)\}$, es una función de $A = \{1, 2, 3\}$ en $B = \{a, b, c\}$ con rango $\{b, c\}$. Por su parte, la relación dada por

$$\mathcal{R}_2 = \{(1, a), (1, b), (2, c), (3, a)\},$$

no es una función de A en B puesto que $(1, a), (1, b) \in \mathcal{R}_2$. Dado un conjunto no vacío A, la función $I_A : A \longrightarrow A$, definida por $I_A(a) = a$, para toda $a \in A$, se denomina función identidad sobre A.

Definición 1.3. Sea f una función de A en B. Se dice que f es inyectiva si para todo par de elementos distintos $a_1, a_2 \in A$ se satisface $f(a_1) \neq f(a_2)$. La función f se denomina sobreyectiva si para todo elemento $b \in B$ existe un elemento $a \in A$ tal que $f(a) = b$.

Note que una función f de A en B es inyectiva si $f(a_1) = f(a_2)$ implica que $a_1 = a_2$. Por ejemplo, la función $f : \mathbb{R}^+ \longrightarrow \mathbb{R}^+$, definida por $f(x) = x^2$ es inyectiva porque si a y

b son reales positivos tales que $f(a) = f(b)$, se tiene $a^2 = b^2$, en consecuencia $|a| = |b|$, y por tanto $a = b$.

Definición 1.4. Sea $f : A \longrightarrow B$ una función y sea $Y \subset B$. La imagen inversa de Y, denota por $f^{-1}(Y)$, se define como

$$f^{-1}(Y) = \{a \in A \ : \ f(a) \in Y\},$$

en particular, si $b \in B$, la imagen inversa de $\{b\}$ se denota $f^{-1}(b)$.

Proposición 1.1. Una función $f : A \longrightarrow B$ es inyectiva si y solo si $|f^{-1}(b)| \leq 1$ para todo $b \in B$.

Demostración. Supongamos que existe $b \in B$ para el cual $|f^{-1}(b)| \geq 2$, lo cual es equivalente a que existen elementos distintos $a_1, a_2 \in A$ tales que $f(a_1) = f(a_2) = b$. Por lo tanto, f no es inyectiva. □

Por ejemplo, de acuerdo con la anterior proposición, la función $f : \mathbb{R} \longrightarrow \mathbb{R}$ dada por $f(x) = x^2$ no es inyectiva puesto que $f^{-1}(4) = \{-2, 2\}$.

Definición 1.5. Sean $f : A \longrightarrow B$ y $g : B \longrightarrow C$ dos funciones. La composición entre f y g es la función de A en C denotada por $g \circ f$ y definida por $(g \circ f)(a) = g(f(a))$.

Por ejemplo, la composición entre las funciones

$$f = \{(1, b), (2, c), (3, a)\} \text{ y } g = \{(a, x), (b, x), (c, z)\}$$

es

$$g \circ f = \{(1, x), (2, z), (3, x)\}.$$

Ahora, si consideramos las funciones de $\mathbb{R}$ en $\mathbb{R}$, dadas por $f(x) = x^2$ y $g(x) = 2x + 3$ se tiene que

$$(g \circ f)(x) = g(f(x)) = g(x^2) = 2x^2 + 3$$

y

$$(f \circ g)(x) = f(g(x)) = f(2x + 3) = (2x + 3)^2 = 4x^2 + 12x + 9.$$

Definición 1.6. Una función $f : A \longrightarrow B$ se denomina biyectiva si es inyectiva y sobreyectiva.

Puesto que una función de este tipo es tanto sobreyectiva como inyectiva se puede

construir la función denotada por $f^{-1} : B \longrightarrow A$ definida por $f^{-1}(b) = a$ si $f(a) = b$. A dicha función se le denomina la función inversa de f y satisface:

- $f^{-1} \circ f = I_A$.
- $f \circ f^{-1} = I_B$.

Las funciones biyectivas son de gran importancia, por ejemplo en Álgebra Lineal una función $T : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ dada por

$$T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$$

es biyectiva si y solo $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ es invertible. En este caso, $T^{-1} : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ está definida mediante la inversa de la matriz A. Las funciones biyectivas definidas en un conjunto no vacío S se denominan permutaciones de S y son de gran importancia en la Teoría de Grupos. En el caso que $S = \{1, 2, \ldots, n\}$ una permutación $\sigma : S \longrightarrow S$ se denotará por

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

Teorema 1.1. Sean $f : A \longrightarrow B$ y $g : B \longrightarrow C$ dos funciones.
1. Si f y g son inyectivas entonces $g \circ f$ es inyectiva.
2. Si f y g son sobreyectivas entonces $g \circ f$ es sobreyectiva.
3. Si f y g son biyectivas entonces $g \circ f$ es biyectiva.

Demostración. Para probar el ítem 1, suponga que las funciones f y g son inyectivas, y sean $a_1, a_2 \in A$ tal que $g(f(a_1)) = g(f(a_2))$. Del hecho que g es inyectiva se obtiene la igualdad $f(a_1) = f(a_2)$, y de manera similar se obtiene que $a_1 = a_2$. La demostración de los ítems 2 y 3 se dejan como ejercicio al lector. □

Teorema 1.2. Si $f : X \longrightarrow Y$ es una función, $A_1, A_2 \subset X$ y $B_1, B_2 \subset Y$, entonces
1. $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.
2. $f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$.
3. $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$.
4. $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$.

Demostración. Sea $a \in f^{-1}(B_1 \cap B_2)$, lo cual es equivalente a $f(a) \in B_1 \cap B_2$ y así $a \in f^{-1}(B_1) \cap f^{-1}(B_2)$. Esto prueba la igualdad del ítem 4, la demostración de los demás ítems se deja como ejercicio al lector. □

1.2 Relaciones de equivalencia

En esta sección se consideran relaciones $\mathcal{R}$ en un conjunto no vacío S, es decir subconjuntos de $S \times S$. Cada pareja $(a, b) \in \mathcal{R}$ también se denotará por $a\mathcal{R}b$ lo cual se lee "a está relacionado con b". Por ejemplo, si se considera el conjunto $S = \{2, 3, 5, 6\}$ y definimos la relación dada por $a\mathcal{R}_1 b$ si a divide a b se tiene que

$$\mathcal{R}_1 = \{(2,2), (2,6), (3,3), (3,6), (5,5), (6,6)\} = \{(a,b) \in S \times S \ : \ a \mid b\}.$$

Ahora, si se considera el conjunto $S = \mathbb{R}$ y la relación dada por

$$\mathcal{R}_2 = \{(x,y) \in \mathbb{R}^2 \ : \ 2x - y = 6\}$$

se obtiene que $\mathcal{R}_2$ es una recta en el plano.

Definición 1.7. Sea $\mathcal{R}$ una relación en el conjunto S y $a, b, c \in S$. Se dice que $\mathcal{R}$ es:

1. Reflexiva si $a\mathcal{R}a$ para todo $a \in S$.
2. Simétrica si $a\mathcal{R}b$ entonces $b\mathcal{R}a$.
3. Transitiva si $a\mathcal{R}b$ y $b\mathcal{R}c$ entonces $a\mathcal{R}c$.

Por ejemplo, si en el conjunto de los números naturales $\mathbb{N}$ se definen las relaciones

$$\mathcal{R}_1 = \left\{(a,b) \in \mathbb{N}^2 : a \text{ es factor de } b\right\},$$

$$\mathcal{R}_2 = \left\{(a,b) \in \mathbb{N}^2 : a \text{ es primo relativo con } b\right\},$$

Observe que $\mathcal{R}_1$ es reflexiva, transitiva pero no es simétrica ya que $(2,4) \in \mathcal{R}_1$ pero $(4,2) \notin \mathcal{R}_1$. Además, $\mathcal{R}_2$ no es reflexiva porque $(2,2) \notin \mathcal{R}_2$, el lector puede comprobar que $\mathcal{R}_2$ tampoco es transitiva pero si es simétrica.

Definición 1.8. Sea $\mathcal{R}$ una relación definida en el conjunto S. Se dice que $\mathcal{R}$ es de equivalencia si ella es reflexiva, simétrica y transitiva.

Ejemplo 1.1. En el conjunto T de todos los triángulos en el plano sea $\mathcal{R}$ la relación dada por "es congruente a". Determinar si la relación es de equivalencia.

Recuerde que dos triángulos son congruentes, si y sólo si, sus lados y ángulos correspondientes son respectivamente congruentes, o en otras palabras, con los lados y ángulos de los dos triángulos se forman tres pares de lados de igual longitud y tres pares de ángulos de igual medida. Por lo cual, la relación de congruencia entre triángulos es claramente reflexiva, simétrica y transitiva, y así la relación $\mathcal{R}$ es de equivalencia.

Ejemplo 1.2. Sea n un entero positivo (fijo). En el conjunto $\mathbb{Z}$ sea $\mathcal{R}$ la relación dada por

$$a\mathcal{R}b \text{ si y solo si } n \mid (a-b).$$

Probar que $\mathcal{R}$ es de equivalencia.

Primero note que la relación se puede reescribir de la siguiente manera:

$$a\mathcal{R}b \text{ si y solo si } a \equiv b \ (\text{mód } n).$$

Esto implica que, por las propiedades de congruencias, la relación $\mathcal{R}$ es reflexiva, simétrica y transitiva. Por lo tanto, $\mathcal{R}$ es de equivalencia.

Definición 1.9. Sea $\mathcal{R}$ una relación de equivalencia definida en el conjunto S y $a \in S$. La clase de equivalencia de a, denotada $[a]$, se define como sigue

$$[a] = \{x \in S \ : \ x\mathcal{R}a\}.$$

Observe que de acuerdo con la anterior definición se obtiene que

$$[a] = [b] \text{ si y solo si } a\mathcal{R}b.$$

En efecto, si $[a] = [b]$ entonces $a \in [b]$ y así $a\mathcal{R}b$. Ahora bien, si $a\mathcal{R}b$ entonces para $x \in [a]$ se tiene que $x\mathcal{R}a$, y por transitividad $x\mathcal{R}b$ por lo cual $x \in [b]$, en consecuencia $[a] \subseteq [b]$. De manera similar se prueba que $[b] \subseteq [a]$ y se garantiza la igualdad $[a] = [b]$.

Definición 1.10. Sea $\mathcal{R}$ una relación de equivalencia definida en el conjunto S. El conjunto cociente de S por $\mathcal{R}$, denotado por $S/\mathcal{R}$, es el conjunto de todas las clases de equivalencia determinadas por $\mathcal{R}$ en S.

$$S/\mathcal{R} = \{[a] \ : \ a \in S\}.$$

Ejemplo 1.3. Considerar en el conjunto $\mathbb{Z}$ la relación de equivalencia definida por

$$x\mathcal{R}y \text{ si y solo si } |x| = |y|.$$

Determinar,

1. La clases de equivalencia de $a = -2, 1$.

2. La cardinalidad de $[a]$ para cualquier $a \in \mathbb{Z}$.

3. El conjunto cociente de la relación.

Para $a \in \mathbb{Z}$ se tiene que

$$[a] = \{x \in \mathbb{Z} \ : \ |x| = |a|\} = \{x \in \mathbb{Z} \ : \ x = \pm a\}.$$

De ahí que $[-2] = \{-2, 2\}$ y $[1] = \{-1, 1\}$. Por otro lado, también se obtiene $|[a]| = 2$ para todo $a \in \mathbb{Z}^* = \mathbb{Z}\backslash\{0\}$, mientras que $|[0]| = 1$. Finalmente

$$\mathbb{Z}/\mathcal{R} = \{\{-a, a\} \ : \ a \in \mathbb{Z}\}.$$

Ejemplo 1.4. Considerar en el conjunto $\mathbb{Z}$ la relación de equivalencia definida por

$$x\mathcal{R}y \text{ si y solo si } x \text{ tiene la misma paridad que } y.$$

Determinar,

1. La clases de equivalencia de $a = -2, 1$.

2. El conjunto cociente de $\mathbb{Z}/\mathcal{R}$.

Para $a \in \mathbb{Z}$ consideramos los casos: Si a es par entonces

$$[a] = \{x \in \mathbb{Z} \ : \ x \text{ es par}\} = 2\mathbb{Z},$$

mientras que si a es impar se tiene

$$[a] = \{x \in \mathbb{Z} \ : \ x \text{ es impar}\} = 2\mathbb{Z} + 1.$$

Esto implica que $[-2] = 2\mathbb{Z}$ y $[1] = 2\mathbb{Z} + 1$. Además, para $a \in \mathbb{Z}$, se tiene

$$a \in [0], \quad \text{cuando } a \text{ es par.}$$

$$a \in [1], \quad \text{cuando } a \text{ es impar.}$$

entonces el conjunto cociente de esta relación está formado solo por estas dos clases de equivalencia, es decir,

$$\mathbb{Z}/\mathcal{R} = \{[0], [1]\}.$$

Ejemplo 1.5. En el conjunto $\mathbb{Z}$ sea $\mathcal{R}$ la relación dada por

$$a\mathcal{R}b \text{ si y solo si } 4 \mid (a - b)$$

Determinar,

1. La clases de equivalencia de $a = -2, 1$.

2. El conjunto cociente $\mathbb{Z}/\mathcal{R}$.

De acuerdo con el Ejemplo 1.2, para $a \in \mathbb{Z}$ se tiene que

$$[a] = \{x \in \mathbb{Z} \ : \ x \equiv a \ (\text{mód } 4)\} = \{a + 4k \ : \ k \in \mathbb{Z}\}.$$

Por tanto, $[-2] = [2] = \{2 + 4k \ : \ k \in \mathbb{Z}\}$ y $[1] = \{1 + 4k \ : \ k \in \mathbb{Z}\}$. Además,

$$\mathbb{Z}/\mathcal{R} = \{[0], [1], [2], [3]\}.$$

Ejemplo 1.6. Sea $S = \mathbb{P}$ el conjunto de todas los polinomios con coeficientes reales. Considerar la relación de equivalencia definida por

$$p \mathcal{R} q \text{ si y solo si } p' = q'$$

en la cual p' es la derivada de p. Determinar,

1. La clases de equivalencia de $q(x) = x^2 + x + 1$ y $p(x) = 2x + 1$.

2. $[r(x)]$ para un polinomio cualquiera.

Primero note que un polinomio $r(x)$ que pertenezca a la clase de equivalencia de $q(x) = x^2 + x + 1$ debe ser de grado 2, luego $r(x) = ax^2 + bx + c$, con $a \neq 0$. Entonces

$$r'(x) = 2ax + b = 2x + 1 = q'(x)$$

y así $a = b = 1$. Por tanto,

$$[q(x)] = \{x^2 + x + c \in \mathbb{P} \ : \ c \in \mathbb{R}\}.$$

De manera similar se obtiene que

$$[p(x)] = \{2x + c \in \mathbb{P} \ : \ c \in \mathbb{R}\}.$$

En general, para $r(x) = a_2x^2 + a_1x + a_0$ con a_2, a_1, a_0 reales fijos se tiene que

$$[r(x)] = [a_2x^2 + a_1x + a_0] = \{a_2x^2 + a_1x + c \in \mathbb{P} \ : \ c \in \mathbb{R}\}.$$

Sea S un conjunto no vacío y $F = \{A_i\}_{i \in I}$ una familia de subconjuntos de S en el

cual I es un conjunto de índices. Entonces se dice que F es una partición de S si satisface las siguientes condiciones:

- $S = \bigcup_{i \in I} A_i$.
- $A_i \cap A_j = \emptyset$ si $i \neq j$.

Teorema 1.3. Si $\mathcal{R}$ es una relación de equivalencia definida en el conjunto S, entonces el conjunto de todas las clases de equivalencia de la relación forman una partición del S.

Demostración. De acuerdo con la Definición 1.9 se tiene que $[a] = [b]$ o $[a] \cap [b] = \emptyset$. Esto implica que la familia de subconjuntos de $S/\mathcal{R}$ es una partición de S. □

Teorema 1.4. Si S es un conjunto no vacío y P una partición de S, entonces existe una relación de equivalencia para la cual P forma el conjunto de todas las clases de equivalencia de la relación.

Demostración. Suponga que $P = \{A_i\}_{i \in I}$ es una partición de S. Entonces se define la relación dada por

$$a \mathcal{R} b \text{ si y solo si } a, b \in A_i \text{ para algún } i \in I.$$

De la igualdad $S = \bigcup_{i \in I} A_i$ se sigue que $\mathcal{R}$ es reflexiva y simétrica. Ahora, si $a \mathcal{R} b$ y $b \mathcal{R} c$, se obtiene que $a, b \in A_i$ y $b, c \in A_j$ para algún $i, j \in I$. En consecuencia, $i = j$ puesto que $b \in A_i \cap A_j$. Por lo tanto, $a, c \in A_i$ y así la relación $\mathcal{R}$ es transitiva. □

Proposición 1.2. Si $\mathcal{R}$ es una relación de equivalencia definida en S, entonces la aplicación

$$\begin{array}{rcl} \pi : S & \longrightarrow & S/\mathcal{R} \\ a & \longmapsto & \pi(a) = [a] \end{array}$$

es una función sobreyectiva.

Demostración. Dado que el conjunto cociente $S/\mathcal{R}$ es una partición, a cada elemento $a \in S$ le corresponde una única clase de equivalencia $[a]$ a la cual pertenece el elemento a. Esto prueba que la aplicación π es una función y por su definición es claramente sobreyectiva. □

Definición 1.11. Sea $\mathcal{R}$ una relación de equivalencia definida en un conjunto no vacío S. La función π definida en la proposición anterior se denomina la proyección canónica.

1.3 Operaciones binarias

Las operaciones usuales que se conocen de suma $(+)$ y multiplicación $(\times)$ en el conjunto de los números reales $\mathbb{R}$ son binarias o cerradas, es decir al operar dos números reales el resultado es nuevamente un número real. En general, una operación binaria se puede definir en un conjunto no vacío cualquiera como sigue:

Definición 1.12. Una operación binaria en un conjunto no vacío S es una función de $S \times S$ en S. Si $* \ : \ S \times S \longrightarrow S$ es una operación binaria, la imagen del par ordenado $(a, b) \in S \times S$ se denota por $a * b \in S$.

En los números reales $\mathbb{R}$ las operaciones básicas de suma $(+)$, resta $(-)$ y multiplicación $(\times)$ son binarias. La división $(\div)$ es binaria en el conjunto $\mathbb{R}^*$ de los reales diferentes de cero. En general, una operación binaria definida en un conjunto S no necesariamente es una operación binaria sobre un subconjunto propio de S, este es el caso de la resta en los números naturales $\mathbb{N}$ o por ejemplo la división en el conjunto de los enteros no cero $\mathbb{Z}^*$. No toda correspondencia define una operación binaria, por ejemplo

1. En $\mathbb{R}$ la operación $a * b = a$.

2. En $\mathbb{Z}^* = \mathbb{Z} - \{0\}$, la operación $x * y = x^y$.

3. En $\mathbb{R}^* = \mathbb{R} - \{0\}$, la operación $x * y = x^y$.

Si se analiza cada una de las anteriores operaciones, se observa que la única que es binaria es la primera, mientras que las dos últimas no satisfacen la condición de la definición puesto que para $x = 2$ y $y = -2$ se tiene $2^{-2} \notin \mathbb{Z}^*$ y para $x = -1$ y $y = \frac{1}{2}$ se obtiene $(-1)^{1/2} \notin \mathbb{R}^*$.

En los casos anteriores el conjunto en el cual se definió cada operación es infinito, en el caso finito se puede determinar si la operación es binaria construyendo la tabla de resultados de la operación. Por ejemplo, para $S_1 = \{-1, 1, i, -i\}$ con la operación usual de multiplicación de números complejos se tiene:

$\times$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Es claro, a partir de la tabla anterior, que la multiplicación usual de complejos es binaria en el conjunto S_1. En general, dado cualquier conjunto finito S se construye una operación binaria mediante una tabla. Por ejemplo, para $S_2 = \{a, b, c, d\}$ se tiene que el siguiente cuadro define una operación binaria.

$*$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

De este análisis surgen las siguientes preguntas.

Ejemplo 1.7. Sea S un conjunto finito de n elementos. ¿Cómo saber cuando una tabla define una operación binaria en S? y ¿cuántas operaciones binarias se pueden definir en S?

La respuesta para la primera pregunta es clara, basta con determinar si todos los elementos de la tabla forman parte del conjunto S. En cambio, para la segunda pregunta observe que existen n^2 parejas $(a, b) \in S \times S$, para cada una de ellas existen n posibilidades de asignarle un elemento de S. Por tanto, se pueden definir n^{n^2} operaciones binarias en S. Por ejemplo, en un conjunto de 4 elementos se pueden definir 4^{16} operaciones binarias.

Definición 1.13. Sea $*$ una operación binaria definida en S. Entonces se dice que $*$ es:

1. Conmutativa si $a * b = b * a$ para todo $a, b \in S$.
2. Asociativa si $a * (b * c) = (a * b) * c$ para todo $a, b, c \in S$.

Se conoce que las operaciones usuales de suma $(+)$ y multiplicación $(\times)$ definidas en el conjunto de los números $\mathbb{R}$ o en restricciones de este conjunto como $\mathbb{N}$, $\mathbb{Z}$ y $\mathbb{Q}$ son también conmutativas y asociativas. A partir de ellas es posible definir nuevas operaciones binarias con estas características.

Ejemplo 1.8. Determinar cuales de las siguientes operaciones binarias definidas en el conjunto $\mathbb{Z}$ son conmutativas o asociativas.

1. $a *_1 b = a + b - ab$.

2. $a *_2 b = a + b - 3$

Sean $a, b, c \in \mathbb{Z}$. Entonces se tiene que

$$a *_1 b = a + b - ab = b + a - ba = b *_1 a$$

y

$$a *_2 b = a + b - 3 = b + a - 3 = b *_2 a,$$

de lo cual se concluye que $*_1$ y $*_2$ son conmutativas. Por otro lado, de las igualdades

$$\begin{aligned}(a *_1 b) *_1 c &= (a + b - ab) *_1 c = (a + b - ab) + c - (a + b - ab)c = \\ &= a + b - ab + c - ac - bc + abc = a + (b + c - bc) - a(b + c - bc) = \\ &= a *_1 (b + c - bc) = a *_1 (b *_1 c)\end{aligned}$$

y

$$\begin{aligned}(a *_2 b) *_1 c &= (a + b - 3) *_2 c = (a + b - 3) + c - 3 = \\ &= a + b - 3 + c - 3 = a + (b + c - 3) - 3 = \\ &= a *_2 (b + c - 3) = a *_2 (b *_2 c)\end{aligned}$$

se obtiene que las operaciones son asociativas.

Note que si se tiene una operación binaria definida en un conjunto finito definida mediante una tabla, es fácil determinar si la operación es conmutativa, basta con analizar si la tabla es simétrica con respecto a la diagonal principal. Por ejemplo, en las siguientes operaciones

$*_1$	a	b	c
a	b	a	c
b	a	c	b
c	c	b	a

$*_2$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

se tiene que las dos son conmutativas. Sin embargo, determinar a simple vista si una operación definida por una tabla es asociativa es difícil.

Definición 1.14. Sea $*$ una operación binaria definida en el conjunto S. Entonces se dice que $*$ tiene la propiedad del

1. Elemento neutro si existe $e \in S$ tal que $a * e = e * a = a$ para todo $a \in S$.
2. Elemento inverso si para todo $a \in S$ existe $b \in S$ tal que $a * b = b * a = e$.

Al elemento e se le denomina el neutro de la operación y en caso que exista el elemento b del ítem (2), entonces este será denotado por a^{-1} (o por $-a$) y se denomina el inverso de a.

Note que en el conjunto de los números naturales $\mathbb{N} = \{1, 2, \ldots\}$ la operación suma

$(+)$ no tiene elemento neutro; sin embargo, este mismo conjunto con la multiplicación $(\times)$ el elemento neutro es el 1. Es decir los naturales con la operación de multiplicación usual satisface la propiedad del elemento neutro, pero no la propiedad del inverso. Si ampliamos el conjunto de los naturales al de los enteros, la suma satisface las dos propiedades de la definición anterior, similarmente la multiplicación si ampliamos los naturales al conjunto de los racionales.

Por otro lado, si se tiene una operación binaria en un conjunto finito es fácil determinar si satisface la propiedad del elemento neutro y del inverso, basta con hacer una inspección de cada fila de la tabla. Por ejemplo, en las siguientes operaciones

$*_1$	a	b	c
a	b	a	c
b	a	c	b
c	c	b	a

$*_2$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

se tiene que la operación $*_1$ no satisface la propiedad del elemento neutro, mientras que en la operación $*_2$ el elemento neutro es $e = a$ y cada elemento de S tiene inverso. El inverso de b es c y viceversa.

Teorema 1.5. Sea $*$ una operación binaria definida en S. Si $*$ tiene la propiedad del elemento neutro, entonces este elemento es único.

Demostración. Suponga que e_1 y e_2 satisfacen la primera condición de la Definición 1.14. Por tanto, para todo $a \in S$ se satisface

$$a * e_1 = e_1 * a = a \quad \text{y} \quad a * e_2 = e_2 * a = a$$

En particular, cuando $a = e_1$ o $a = e_2$ se llega a que

$$e_1 = e_1 * e_2 = e_2.$$

□

Ejemplo 1.9. Determinar cuales de las siguientes operaciones binarias definidas en el conjunto $\mathbb{Z}$ tienen elemento neutro.

1. $a *_1 b = a + b - ab$.
2. $a *_2 b = a + 2b$.
3. $a *_3 b = a + b - 3$

En la operación $*_1$ el elemento neutro es $e_1 = 0$. En efecto,

$$0 *_1 a = 0 + a - 0 \cdot a = a = a + 0 - a \cdot 0 = a *_1 0$$

y en la operación $*_3$ su elemento neutro es $e_3 = 3$ dado que

$$a *_3 3 = a + 3 - 3 = a = 3 + a - 3 = 3 *_3 a.$$

Si la operación $*_2$ tiene elemento neutro e se tiene que

$$e *_2 a = e + 2a = a = a + 2e = a *_2 e$$

y así $a = e$ lo cual no es posible. Por tanto, las operación $*_2$ no satisface la propiedad del elemento neutro.

1.4 Ejercicios

1. Considerar los conjuntos $X = \{1, 2, 3, 4\}$, $Y = \{a, b, c\}$ y la función $f : X \longrightarrow Y$ dada por
$$f(1) = a,\ f(2) = a,\ f(3) = c,\ f(4) = c$$
y los conjuntos $A = \{1, 3\}$ y $B = \{a, b\}$. Determinar $f(A)$ y $f^{-1}(B)$.

2. Sean $f : X \longrightarrow Y$ una función, $A \subset X$ y $B \subset Y$. Probar

   a) $f^{-1}(B^C) = (f^{-1}(B))^C$.

   b) $f^{-1}(Y \backslash B) = X \backslash f^{-1}(B)$.

   c) $A \subset f^{-1}(f(A))$ y $f(f^{-1}(B)) \subset B$.

3. Si $f : A \longrightarrow B$ y $g : B \longrightarrow C$ son funciones tales que $g \circ f : A \longrightarrow C$ es inyectiva, probar que f es inyectiva.

4. Si $f : A \longrightarrow B$ y $g : B \longrightarrow C$ son funciones tales que $g \circ f : A \longrightarrow C$ es sobreyectiva, probar que g es sobreyectiva.

5. Si $f : X \longrightarrow Y$ es una función y A_1 y A_2 son subconjuntos de X, mostrar que $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$. Determinar condiciones para las cuales se satisface la igualdad $f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$.

6. En $\mathbb{R}$ considerar la relación $a\mathcal{R}b$ si y solo si $ab \geq 0$. ¿$\mathcal{R}$ es una relación de equivalencia?

7. En el conjunto $\mathbb{Z} \times \mathbb{Z}^*$ considerar la relación $(a, b)\mathcal{R}(c, d)$ si y solo si $ad - bc = 0$.

   a) Probar que $\mathcal{R}$ es una relación de equivalencia.

   b) Determinar el conjunto cociente.

   c) Hallar el conjunto cociente si la relación se define en el conjunto $A \times A$ en el cual $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

8. En $\mathbb{Q}$ se define la relación

$$x\mathcal{R}y \text{ si y solo si existe } h \in \mathbb{Z} \text{ tal que } x = \frac{3y + h}{3}.$$

   a) Probar $\mathcal{R}$ es de equivalencia.

   b) Analizar si $\left[\frac{2}{3}\right] = \left[\frac{4}{5}\right]$.

9. En $\mathbb{Z}$ considerar la relación dada por: $x\mathcal{R}y$ si y solo si $x^2 - y^2 = x - y$.

   a) Probar que $\mathcal{R}$ es de equivalencia.

   b) Hallar [3].

   c) Determinar el conjunto cociente $\mathbb{Z}/\mathcal{R}$.

10. En el conjunto $E = \mathbb{R}^2$ se define la relación

$$(x, y)\mathcal{R}(z, w) \text{ si y solo si } x^2 + y^2 = z^2 + w^2.$$

    a) Demostrar que $\mathcal{R}$ es una relación de equivalencia.

    b) Determinar el conjunto cociente $\mathbb{R}^2/\mathcal{R}$.

11. Sea X el conjunto de todas las funciones de $\mathbb{R}$ en $\mathbb{R}$. Dadas $f, g \in X$ se define la relación

$$f \ \mathcal{R} \ g \text{ si y solo si } \lim_{t \to 0} \frac{f(t) - g(t)}{t^2} = 0.$$

    Demostrar que $\mathcal{R}$ es una relación de equivalencia.

12. Sean $\mathcal{R}_1$ y $\mathcal{R}_2$ dos relaciones de equivalencia definidas en los conjuntos S_1 y S_2

respectivamente. Considerar la relación

$$(a_1, b_1)\mathcal{R}(a_2, b_2) \text{ si y solo si } a_1\mathcal{R}a_2 \text{ y } b_1\mathcal{R}b_2.$$

definida en el conjunto $S = S_1 \times S_2$. Probar que $\mathcal{R}$ es de equivalencia.

13. Sea U un conjunto y $A \subset U$. En $\mathcal{P}(U)$ se define la relación

$$X\mathcal{R}Y \text{ si y solo si } X \cup A = Y \cup A.$$

a) Probar que $\mathcal{R}$ es una relación de equivalencia.

b) Para el caso $U = \{1, 2, 3, 4\}$ y $A = \{1, 2\}$. Determinar el conjunto cociente $\mathcal{P}(U)/\mathcal{R}$.

14. Sea $M = M_{n\times n}(\mathbb{R})$ el conjunto de todas las matrices cuadradas de tamaño n. Definir la relación

$$A\mathcal{R}B \text{ si y solo si } A \text{ y } B \text{ tienen la misma cantidad de ceros.}$$

a) Probar que $\mathcal{R}$ es de equivalencia.

b) Determinar cuántas clases de equivalencia distintas hay.

c) Para $n = 3$ determinar la clase de equivalencia de la siguiente matriz

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

d) Para $n = 2$ determinar el conjunto cociente de $M/\mathcal{R}$.

15. En $\mathbb{Z}^+ \times \mathbb{Z}^+$ considerar la relación

$$(a, b)\mathcal{R}(c, d) \text{ si y solo si } a + d = b + c$$

a) Probar que $\mathcal{R}$ es una relación de equivalencia.

b) Hallar el conjunto cociente.

c) Determinar el conjunto cociente que se obtiene si la relación se define en $A\times A$ en el cual $A = \{1, 2, 3, 4, 5\}$.

16. En $S = \mathbb{R}^2 - \{(0,0)\}$ se define la relación

$$u\mathcal{R}v \text{ si y solo si } u = \lambda v \text{ para algún } \lambda \in \mathbb{R}.$$

   a) Probar que $\mathcal{R}$ es una relación de equivalencia.

   b) Determinar el conjunto cociente.

17. Sea $\mathcal{R}$ una relación de equivalencia definida en el conjunto S. Probar,

   a) Si $c\mathcal{R}a$ y $c\mathcal{R}b$ entonces $a\mathcal{R}b$.

   b) Si $b \in [a]$ entonces $[a] = [b]$.

18. Probar que cada una de las siguientes operaciones son binarias en el conjunto en el cual se definen.

   a) $a * b = a + b - 3$ en $\mathbb{Z}$.

   b) $a * b = \dfrac{3}{2}ab$ en $\mathbb{Q}^+$.

19. Considerar el conjunto $A = \{a, b, c, d, e\}$.

   a) ¿Cuántas funciones de $A \times A$ en A existen?

   b) ¿Cuántas operaciones binarias existen?

   c) ¿Cuántas de estas operaciones son conmutativas?

20. Considerar el conjunto $A = \{x, a, b, c, d\}$.

   a) ¿Cuántas operaciones binarias se pueden definir en el conjunto A tales que $a * b = c$?

   b) ¿Cuántas de las anteriores operaciones tienen a x como elemento neutro?

   c) ¿Cuántas de las operaciones del ítem (a) tienen un elemento neutro?

   d) ¿Cuántas de las operaciones del ítem (c) son conmutativas?

21. En $\mathbb{Q}^*$ considerar la operación $a * b = \dfrac{a}{b}$.

a) Probar que $*$ no es conmutativa ni asociativa.

b) Determinar si $*$ tiene elemento neutro.

22. En $\mathbb{Z}^*$ se define la operación $a * b = \text{m.c.d}\{a, b\}$.

a) Probar que la operación $a * b$ es binaria.

b) Determinar si la operación definida es asociativa o conmutativa.

c) Determinar si la operación tiene elemento neutro.

23. Considerar el conjunto $A = \{2, 4, 8, 16, 32\}$ y considerar la operación $a * b = \text{m.c.d}\{a, b\}$. Determinar si $*$ tiene elemento neutro.

24. Sean p y q primos distintos y considerar el conjunto $A = \{p^n q^m \ : \ 0 \leq n \leq 31, \ 0 \leq m \leq 37\}$.

a) Probar que la operación $a * b = \text{m.c.d}\{a, b\}$ es binaria.

b) Determinar si la operación definida es asociativa o conmutativa.

c) Determinar si la operación tiene elemento neutro.

25. Considerar el conjunto de las matrices de la forma

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}$$

en el cual $x, y, z \in \mathbb{R}$.

a) Probar que la operación usual de multiplicación de matrices es binaria en este conjunto.

b) Probar que esta operación es asociativa y tiene la propiedad del elemento neutro.

26. Considerar el conjunto de las matrices

$$A = \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \ : \ \theta \in \mathbb{R} \right\}.$$

a) Probar que la operación usual de multiplicación de matrices es binaria en este conjunto.

b) Probar que esta operación es asociativa y tiene la propiedad del elemento neutro.

27. Considere la relación definida en $\mathbb{R}$ por:

$$x\mathcal{R}y \text{ si y solo si } \frac{x-y}{2\pi} \in \mathbb{Z}$$

a) Probar que $\mathcal{R}$ es de equivalencia.

b) Determinar el conjunto cociente $\mathbb{R}/\mathcal{R}$.

c) Probar que existe una biyección entre $\mathbb{R}/\mathcal{R}$ y los puntos de la circunferencia $S^1 = \{(x, y) \ : x^2 + y^2 = 1\}$.

d) Probar que la operación de suma usual en los números reales define una operación binaria en el conjunto cociente $\mathbb{R}/\mathcal{R}$.

e) Probar que la operación canónica no está bien definida si la operación en $\mathbb{R}$ es la multiplicación usual en los reales.

28. En el conjunto $\mathbb{Z} \times \mathbb{Z}^*$ considerar la relación de equivalencia:

$$(a, b)\mathcal{R}(c, d) \text{ si y solo si } ad - bc = 0.$$

a) Determinar el conjunto cociente $\mathbb{R}/\mathcal{R}$.

b) Probar que existe una biyección entre $\mathbb{R}/\mathcal{R}$ y el conjunto $\mathbb{Q}$.

c) En $\mathbb{Z} \times \mathbb{Z}^*$ considerar las operaciones.

$$(a, b) * (c, d) = (ad + bc, bd) \qquad \text{y} \qquad (a, b) \circ (c, d) = (ac, bd).$$

Probar que las operaciones canónicas correspondiente a $*$ y $\circ$ están bien definidas en $(\mathbb{Z} \times \mathbb{Z}^*)/\mathcal{R}$.

d) Probar que existe una biyección entre $(\mathbb{Z} \times \mathbb{Z}^*)/\mathcal{R}$ y $\mathbb{Q}$.

CAPÍTULO 2

Grupos y subgrupos

2.1 Estructura de grupo

En matemáticas una estructura algebraica es un conjunto no vacío dotado de una o más operaciones binarias, estas estructuras se clasifican dependiendo de las propiedades que satisfacen las operaciones. Un grupo es un tipo particular de estructura algebraica, este tipo de estructura no es del todo desconocida para los estudiantes de secundaria puesto que algunos ejemplos básicos son los conjuntos numéricos usuales de los enteros, racionales, reales y complejos con la operación de suma.

Definición 2.1. Sea G un conjunto no vacío en el cual se define una operación binaria $*$. Se dice que $\langle G, * \rangle$ tiene estructura de grupo si satisface cada una de las siguientes condiciones:

1. $*$ es asociativa en G.
2. $*$ tiene la propiedad del elemento neutro en G.

3. $*$ tiene la propiedad del elemento inverso en G.

En el caso que $*$ sea conmutativa en G entonces se dice que $\langle G, * \rangle$ tiene estructura de grupo abeliano (o conmutativo).

En el caso que $\langle G, * \rangle$ tenga estructura de grupo se dirá simplemente que G es un grupo siempre y cuando la operación binaria se deduzca del contexto. Como se mencionó en la introducción, algunos sistemas numéricos tienen estructura de grupo y en algunos casos de grupo abeliano. Por ejemplo, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ tienen estructura de grupo abeliano en los cuales la operación es la suma usual. Mientras que $\mathbb{Q}^*$, $\mathbb{R}^*$ y $\mathbb{C}^*$ tienen estructura de grupo abeliano con la multiplicación usual, en cada uno de estos casos el asteristo como superíndice significa que del conjunto no se considera el número 0, por ejemplo $\mathbb{Q}^* = \mathbb{Q} \backslash \{0\}$. Sin embargo, si se considera al conjunto de los números naturales $\mathbb{N}$ con la suma se concluye que no tiene estructura de grupo, puesto que no satisface la propiedad del elemento inverso. Igualmente sucede con el conjunto $\mathbb{Z}^*$ con la multiplicación de enteros. Por otro lado, note que en el conjunto de los números irracionales $\mathbb{I}$ la multiplicación no es una operación binaria.

Del Álgebra Lineal se concluye que el conjunto de las matrices cuadradas de orden n con componentes complejas $M_n(\mathbb{C})$ tiene estructura de grupo abeliano con la operación de suma de matrices. Sin embargo, este mismo conjunto no tiene estructura de grupo con la operación de multiplicación de matrices puesto que no se garantiza la existencia del elemento inverso para toda matriz. Note que esta operación sí satisface la propiedad del elemento neutro puesto que la matriz identidad cumple con la condición (2) de la Definición 2.1. Ahora, si solamente se considera el conjunto de las matrices invertibles $GL(n, \mathbb{R})$ con la operación de multiplicación de matrices, este tiene estructura de grupo, pero no de grupo abeliano.

Ejemplo 2.1. Determinar si cada una de las siguientes estructuras forman un grupo abeliano.

1. $\langle \mathbb{Z}, * \rangle$ en la cual la operación está definida por $a * b = a + b - 3$.

2. $\langle \mathbb{Q}^*, * \rangle$ en la cual la operación está definida por $a * b = \dfrac{ab}{2}$.

En el primer caso, por lo expuesto en los Ejemplos 1.8 y 1.9, es claro que la operación definida es binaria (o cerrada), asociativa, conmutativa y tiene la propiedad del elemento neutro en el conjunto $\mathbb{Z}$ con elemento neutro $e = 3$. Además, para $a \in \mathbb{Z}$, su inverso es $a^{-1} = 6 - a$. Por tanto, la primera estructura es un grupo.

Note que como está definida la operación de la segunda estructura implica que es binaria en el conjunto $\mathbb{Q}^*$, y la asocitividad y conmutatividad de la multiplicación de números racionales implica la asociatividad y conmutatividad de la operación. Por otro

lado, el elemento neutro es $e = 2$, y el elemento inverso del racional no cero a es $a^{-1} = \frac{4}{a}$. Por lo cual, la segunda estructura es un grupo abeliano.

Dado un grupo finito G con operación binaria $*$, a la tabla de resultados de la operación binaria se le denomina la tabla de Cayley de G. Note que la tabla de Cayley facilita determinar, por simple inspección, cual es el elemento neutro de la operación y si la operación es conmutativa.

Ejemplo 2.2. Construir la tabla de Cayley del grupo $U(10) = \{1, 3, 7, 9\}$ en el cual la operación binaria es $a * b = ab$ (mód 10), y determinar el inverso de cada uno de los elementos del grupo.

La tabla de Cayley es

$*$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

de donde se concluye que $3^{-1} = 7$, $7^{-1} = 3$ y $9^{-1} = 9$. Además, observe que el grupo es abeliano por la simetría de la tabla con respecto a la diagonal principal.

Ejemplo 2.3. Construir la tabla de Cayley del grupo S_3 en el que S_3 es el conjunto de las permutaciones de $[1, 3] = \{1, 2, 3\}$ y la operación binaria es la composición de funciones. De acuerdo con la tabla, identifique el elemento neutro de la operación y si esta es conmutativa.

Primero note que el grupo está formado por $S_3 = \{\rho_0, \rho_1, \rho_2, \tau_1, \tau_2, \tau_3\}$ en el cual

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Entonces para construir la tabla de Cayley correspondiente al grupo S_3 se deben calcular los productos entre dos permutaciones, por ejemplo $\rho_1\tau_2$ es igual a

$$\rho_1\tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \tau_1.$$

Por lo cual, la tabla de Cayley de S_3 se muestra en la Figura 2.1.

$\circ$	ρ_0	ρ_1	ρ_2	τ_1	τ_2	τ_3
ρ_0	ρ_0	ρ_1	ρ_2	τ_1	τ_2	τ_3
ρ_1	ρ_1	ρ_2	ρ_0	τ_3	τ_1	τ_2
ρ_2	ρ_2	ρ_0	ρ_1	τ_2	τ_3	τ_1
τ_1	τ_1	τ_2	τ_3	ρ_0	ρ_1	ρ_2
τ_2	τ_2	τ_3	τ_1	ρ_2	ρ_0	ρ_1
τ_3	τ_3	τ_1	τ_2	ρ_1	ρ_2	ρ_0

Figura 2.1: Tabla de Cayley de S_3

De la anterior tabla se puede concluir que el elemento neutro de S_3 es la permutación identidad ρ_0; por otro lado, el grupo no es abeliano puesto que su correspondiente tabla de Cayley no es simétrica con respecto a la diagonal principal.

Para finalizar esta sección se presentan algunos ejemplos de grupos, los cuales serán de importancia a lo largo del texto.

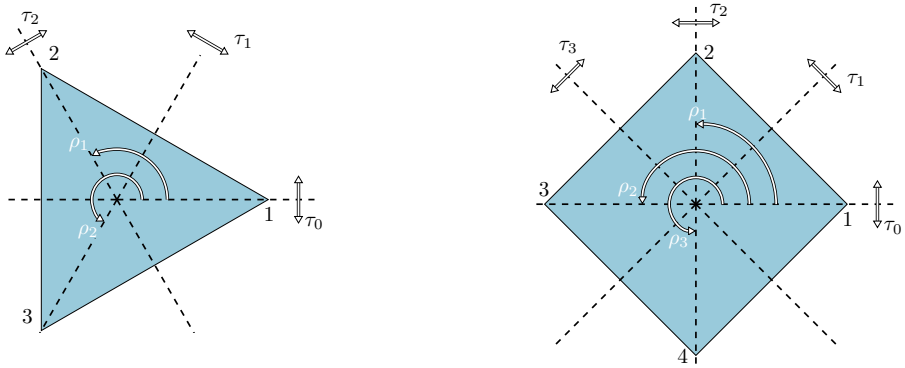
Residuos módulo n $\langle \mathbb{Z}_n, + \rangle$. El conjunto está formado por los residuos módulo n, es decir $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ y la operación es la suma módulo n. Este es un grupo abeliano en el que cualquier elemento se puede generar con el 1, y además el inverso (aditivo) de cualquier elemento $a \in \mathbb{Z}_n$ es $n - a$. Por otro lado, dado que es un grupo finito se puede construir su tabla de Cayley, por ejemplo para $n = 5$ ver la Figura 2.2.

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Figura 2.2: Tabla de Cayley $\mathbb{Z}_5$

Dihédrico $\langle D_n, \circ \rangle$. Este grupo D_n es el conjunto de aquellas transformaciones geométricas de un n-ágono regular de n lados, en el cual una transformación geométrica se considera como un movimiento rígido si su resultado es una copia de la figura geométrica, y la operación del grupo es la composición de funciones. Observe que una transformación con estas características es un caso particular de permutación. Por ejemplo, para el triángulo equilátero se tienen seis transformaciones de un triángulo equilátero, tres simetrías axiales, una con con respecto a cada mediatriz del triángulo y tres rotaciones de $0°$, $120°$ y $240°$, como se aprecia en la Figura 2.3. En este caso, el inverso de cada simetría (con respecto a cada mediana) es ella misma, mientras que la transformación inversa de cada rotación de θ grados es la rotación de $360° - \theta$.

Por otro lado, para el cuadrado se tienen ocho transformaciones geométricas, dos de ellas con respecto a las diagonales del cuadrado, dos más con respecto a las mediatrices de lados opuestos y cuatro rotaciones de 0°, 90°, 180° y 270°, como se puede evidenciar en la Figura 2.7. En este caso, con un simple análisis es sencillo determinar la inversa de cada transformación. En general, la inversa de cada rotación de θ grados en el grupo D_n es la rotación de $360° - \theta$ grados y la inversa de una simetría axial es ella misma.



(a) Grupo D_3 *(b) Grupo D_4*

Figura 2.3: Grupos D_3 y D_4

Permutaciones $\langle S_n, \circ \rangle$. El conjunto S_n consiste de las permutaciones de $[1, n] = \{1, 2, \ldots, n\}$ y la operación es la composición de funciones. El grupo S_n tiene $n!$ elementos. Por ejemplo, para $n = 3$ se tienen 6 permutaciones dadas por

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

de lo cual se obtiene que $S_3 = D_3$. En general, esta igualdad no es cierta puesto que para $n \geq 4$ el número de elementos de S_n es mayor que el número de elementos de D_n.

Unidades módulo n $\langle U(n), \cdot \rangle$. Este grupo está conformado por todas las unidades del grupo $\mathbb{Z}_n$, esto es

$$U(n) = \{a \in [1, n] \ : \ ax \equiv 1 (\text{mód } n) \text{ tiene solución}\}$$

y la operación es la multiplicación módulo n. En otras palabras $U(n)$ está formado por todos los elementos de $\mathbb{Z}_n$ que son primos relativos con n, y así $U(n)$ tiene $\varphi(n)$ elementos con φ la función indicatriz de Euler. Esto implica que $U(12)$ tiene $\varphi(12) = \varphi(3)\varphi(4) = 4$ elementos, los cuales son $1, 5, 7$ y 11. La tabla de Cayley de $U(12)$ es

$\times$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Figura 2.4: Tabla de Cayley de $U(12)$

Por el Pequeño Teorema de Fermat se tiene que el inverso de $a \in U(n)$ es $a^{\varphi(n)-1}$.

2.2 Propiedades básicas

De ahora en adelante, por simplicidad, se denotará $a * b$ por ab. A esta notación se le denomina notación multiplicativa. En ocasiones se utilizará la notación aditiva $a + b$. Por este hecho el siguiente cuadro muestra un comparativo entre la notación usual y las notaciones multiplicativa y aditiva.

Usual	Multiplicativa	Aditiva
$a * b$	ab	$a + b$
e	1	0
$-a$	a^{-1}	$-a$
$\underbrace{a * a * \cdots * a}_{n-\text{veces}}$	a^n	na
$a * (-b)$	ab^{-1}	$a - b$

Figura 2.5: Notación multiplicativa y aditiva

A continuación se presentan algunas propiedades básicas que cumplen aquellos conjuntos que tienen estructura de grupo, estas propiedades permiten solucionar ecuaciones lineales con coeficientes en un grupo.

Teorema 2.1 (Leyes cancelativas)**.** En un grupo G las leyes cancelativas a izquierda y derecha se cumplen. Es decir,

1. Si $ab = ac$ entonces $b = c$.
2. Si $ba = ca$ entonces $b = c$.

Demostración. Sean $a, b, c \in G$ tales que $ab = ac$. Entonces multiplicando a ambos lados

de la igualdad por a^{-1} y aplicando asociatividad se tiene

$$\begin{aligned} a^{-1}(ab) &= a^{-1}(ac) \\ (a^{-1}a)b &= (a^{-1}a)c \\ b &= c \end{aligned}$$

De manera similar se prueba el segundo ítem. □

Teorema 2.2 (Unicidad elemento identidad e inverso)**.** Si G es un grupo, entonces el elemento identidad es único; además, para todo $a \in G$ existe un único elemento inverso para a.

Demostración. La unicidad del elemento identidad es una consecuencia del Teorema 1.5. Para la unicidad del elemento inverso suponga que $a_1, a_2 \in G$ satisfacen $aa_1 = a_1a = 1 = aa_2 = a_2a$. Aplicando las leyes cancelativas a izquierda se obtiene que $a_1 = a_2$. □

Teorema 2.3. Si G es un grupo y $a, b \in G$, entonces las ecuaciones (lineales) $ax = b$ y $ya = b$ tienen solución única x y y en G.

Demostración. Del Teorema 2.1 se sigue que $x = a^{-1}b$ y $y = ba^{-1}$ son soluciones a las ecuaciones lineales. Además, que estas soluciones son únicas □

Ejemplo 2.4. Hallar la solución de las siguientes ecuaciones en el grupo especificado.

1. $5x = 7$ en el grupo $U(12)$.

2. $4 + x = 6$ en el grupo $\mathbb{Z}_{12}$.

Para la primera ecuación observe que en el grupo $U(12)$ se cumple que $5^{-1} = 5$, y así

$$\begin{aligned} 5x &= 7 \\ (5 \cdot 5)x &= 5 \cdot 7 \\ x &= 11. \end{aligned}$$

En la segunda ecuación se tiene que $-4 = 8$ lo cual implica

$$\begin{aligned} 4 + x &= 6 \\ (8 + 4) + x &= 8 + 6 \\ x &= 2. \end{aligned}$$

Proposición 2.1. Si G es un grupo y $a, b \in G$, entonces $(ab)^{-1} = b^{-1}a^{-1}$.

Demostración. Por la unicidad del elemento inverso y de la igualdad

$$(ab)(b^{-1}a^{-1}) = (a(bb^{-1}))a^{-1} = aa^{-1} = 1$$

se sigue la afirmación del teorema. □

Ejemplo 2.5. En el grupo $GL(2,\mathbb{R})$ resolver la ecuación lineal $(AB)X = C$ en la cual

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix},\ B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ y } C = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}.$$

Primero note que en el grupo $GL(2,\mathbb{R})$ se cumple que

$$A^{-1} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \text{ y } B^{-1} = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}.$$

Por tanto,

$$\begin{aligned} (AB)^{-1}(AB)X &= (AB)^{-1}C \\ X &= B^{-1}A^{-1}C \\ X &= \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix} \\ X &= \begin{pmatrix} 0 & -1 \\ -1 & -1 \end{pmatrix}. \end{aligned}$$

2.3 Subgrupos

Cuando se estudian estructuras algebraicas, uno de los aspectos importantes corresponde a aquellos subconjuntos que mantienen la misma estructura con las mismas operaciones. En el caso de la estructura de grupo estas subestructuras se denominan *subgrupos*.

Definición 2.2 (Subgrupo)**.** Sea G un grupo y H un subconjunto no vacío de G. Entonces H se denomina un subgrupo de G, si H también tiene estructura de grupo con la operación definida en G. En dicho caso se denota por $H \leq G$.

En caso de que H sea un subconjunto propio, se dice que H es un subgrupo propio

de G y se denota por $H < G$. Por otro lado, todo grupo G tiene dos subgrupos triviales los cuales son $H = \{1\}$ y $H = G$. De acuerdo con la Definición 2.2, un subconjunto H de un grupo G tiene estructura de subgrupo si satisface cada una de las propiedades de la Definición 2.1; sin embargo, algunas de estas propiedades que se satisfacen en G el subconjunto H las hereda, por ejemplo, la asociatividad de la operación es una condición que la cumplen también los elementos de H. Adicionalmente, por ser G un grupo se garantiza la existencia del elemento neutro e inverso, aunque, no se tiene certeza si estos elementos pertenecen a H. En este sentido se tiene la siguiente proposición.

Proposición 2.2. Sea G un grupo y $H \subseteq G$ no vacío. Si $ab^{-1} \in H$ para todo $a, b \in H$, entonces H es un subgrupo de G.

Demostración. Del hecho que G sea un grupo se concluye que la operación de G también es asociativa en H. Por otro lado, puesto que H es no vacío se obtiene que existen $a \in H$, y así $1 = aa^{-1} \in H$. Esto implica que $b^{-1} = 1 \cdot b^{-1} \in H$ para todo $b \in H$. Por tanto, H es un subgrupo de G. □

Proposición 2.3. Sea G un grupo y $H \subseteq G$ no vacío. Si
1. $ab \in H$ para todo $a, b \in H$ y
2. $a^{-1} \in H$ para todo $a \in H$,

entonces H es un subgrupo de G.

Demostración. De las condiciones 1 y 2 se obtiene que $ab^{-1} \in H$ para todo $a, b \in H$. Por tanto, la Proposición 2.2 implica que H es un subgrupo de G. □

Proposición 2.4. Sea G un grupo y $H \subseteq G$ no vacío finito. Si H es cerrado con la operación de G, entonces H es un subgrupo de G.

Demostración. Supongamos que $H = \{a_1, a_2, \ldots, a_n\}$. Entonces para $a_i \in H$ se tiene que todos los productos $a_i a_j$ son distintos para $j = 1, 2, \ldots, n$ y así

$$a_i H = \{a_i a_1, a_i a_2, \ldots, a_i a_n\} = \{a_1, a_2, \ldots, a_n\}.$$

En tal caso, para alguna $j \in \{1, 2, \ldots, n\}$ se tiene $a_i a_j = a_i$, luego $1 = a_j \in H$. En consecuencia, $a_i a_k = 1$, para algún $a_k \in H$; es decir, H satisface la propiedad del inverso. Por tanto, de la Proposición 2.3, se sigue la afirmación. □

La anterior proposición no se puede generalizar para subconjuntos infinitos, por ejemplo, $\mathbb{N}$ es un subconjunto cerrado con respecto a la suma usual en $\mathbb{Z}$, sin embargo $\mathbb{N}$ no es un subgrupo de $\mathbb{Z}$.

Note que si en la colección de subgrupos de un grupo G se define la relación "es subgrupo de" dada por

$$H \mathcal{R} N \text{ si y solo si } H \leq N$$

entonces $\mathcal{R}$ es reflexiva y transitiva, mas no es simétrica. Por otro lado, de acuerdo con los ejemplos vistos se tiene que

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

2. $SL(n, \mathbb{R}) \leq GL(n, \mathbb{R})$.

3. $D_{2n} \leq S_n$.

Definición 2.3. Sean G un grupo multiplicativo, a un elemento de G y n un número entero. La *n-ésima potencia de a*, denotada a^n, es el elemento de G definido de la forma siguiente:

$$a^n = \begin{cases} 1, & \text{cuando } n = 0. \\ \underbrace{aa\cdots a}_{n \text{ veces}}, & \text{cuando } n > 0. \\ \underbrace{a^{-1}a^{-1}\cdots a^{-1}}_{|n| \text{ veces}}, & \text{cuando } n < 0. \end{cases}$$

Por ejemplo, en el grupo de unidades módulo 10, $U(10) = \{1, 3, 7, 9\}$, se tiene $3^3 = 7$ y $3^{-2} = 3^{-1}3^{-1} = 7(7) = 9$. Observe que de la definición de n-ésima potencia se tiene

$$a^n a^m = a^{n+m} = a^m a^n, \text{ para todo par de enteros } n \text{ y } m.$$

Un tipo de subgrupo de gran importancia en Teoría de Grupos es aquel formado por las potencias de un elemento del grupo.

Proposición 2.5. Si G es un grupo y $a \in G$, entonces

$$\langle a \rangle = \{a^k \ : \ k \in \mathbb{Z}\}$$

es un subgrupo de G.

Demostración. Primero note que la operación es cerrada en el conjunto $\langle a \rangle$. Por otro lado, si no existe un entero positivo k para el cual $a^k = 1$, entonces todas las potencias

de a son distintas. De ahí que el inverso de a^k es a^{-k} y así $\langle a\rangle$ es un subgrupo de G. Sin embargo, si existe un entero positivo k para el cual $a^k = 1$ resulta

$$\langle a\rangle = \{1, a, a^2, \ldots, a^{n-1}\}$$

en el cual $n = \text{mín}\{k \in \mathbb{Z}^+ \ : \ a^k = 1\}$. En efecto, si $m \in \mathbb{Z}$ entonces por el algoritmo de la división existen enteros q y r tales que $m = nq + r$ con $0 \leq r < n$. Esto implica que

$$a^m = a^{nq+r} = (a^n)^q a^r = a^r.$$

Luego, por la Proposición 2.4 se tiene que $\langle a\rangle$ es un subgrupo de G. □

El subgrupo definido en la proposición anterior se denomina el subgrupo cíclico generado por a y al elemento a se le denomina un generador del subgrupo. En el Capítulo 4 se estudiarán en detalle este tipo de subgrupos.

2.4 Orden de un grupo

Este capítulo finaliza con la introducción del orden de un grupo y orden de un elemento.

Definición 2.4. Sea G un grupo y a un elemento del grupo. El orden de G se define como el número de elementos (finito o infinito) de G y se denota por $|G|$. Si existe un entero positivo k tal que $a^k = 1$, entonces el orden de a, denotado $|a|$ o $\text{ord}(a)$, se define de la siguiente manera:

$$|a| = \text{mín}\{k \in \mathbb{Z}^+ : a^k = 1\}.$$

En el caso de que no exista un entero positivo k tal que $a^k = 1$, se dice que a es de orden infinito.

Si se trabaja con la notación aditiva el orden del elemento a, es el mínimo entero positivo k tal que $ka = 0$, siempre que este mínimo exista.

Ejemplo 2.6. Determinar el orden del grupo de los residuos módulo 10 así como el orden de cada uno de sus elementos.

El grupo $\mathbb{Z}_{10}$ está compuesto por todos los residuos módulo 10. De ahí que el residuo 2 tiene orden 4, ya que

$$2 + 2 \equiv 4 \ (\text{mód } 10),\ 2 + 2 + 2 \equiv 6 \ (\text{mód } 10),\ 2 + 2 + 2 + 2 \equiv 8 \ (\text{mód } 10) \text{ y}$$
$$2 + 2 + 2 + 2 + 2 \equiv 0 \ (\text{mód } 10).$$

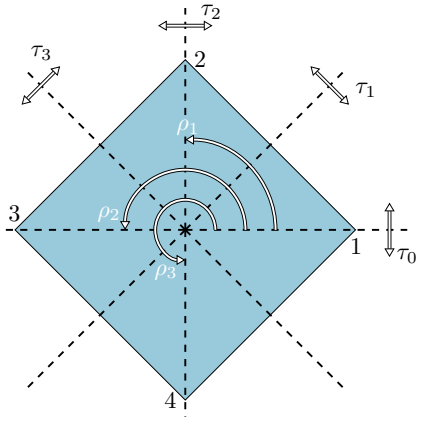
De igual forma se obtiene que el residuo 6 tiene orden 5. En la siguiente figura se muestra el orden de cada uno de los elementos de $\mathbb{Z}_{10}$.

a	0	1	2	3	4	5	6	7	8	9
ord(a)	1	10	5	10	5	4	5	10	5	10

Figura 2.6: Órdenes de los elementos de $\mathbb{Z}_{10}$

Ejemplo 2.7. Determinar el orden del grupo D_4 así como el orden de cada uno de sus elementos.

Tenga presente que el grupo D_4 está conformado por 4 rotaciones de $0^o, 90^o, 180^o$ y 270^o, y 4 simetrías axiales (o reflexiones) dos con respecto a las diagonales y dos más con respecto a las mediatrices de los lados del cuadrado. Por lo cual, el grupo D_4 es de orden 8.



(a) Grupo D_4

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$
$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$
$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$
$$\rho_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$
$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$
$$\tau_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$
$$\tau_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$
$$\tau_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

(b) Elementos de D_4

Figura 2.7: Grupo Dihédrico D_4

Para determinar el orden de cada elemento se puede observar de la anterior figura que cada una de las simetrías axiales es de orden 2. Sin embargo, se puede deducir que las rotaciones ρ_1 y ρ_3 tiene orden 4 mientras que ρ_2 tiene orden 2. Cada uno de los órdenes de los elementos de D_4 se puede obtener realizando la composición de las permutaciones;

por ejemplo para τ_1 se tiene

$$\tau_1^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \rho_0.$$

Ejemplo 2.8. Determinar el orden del grupo de las unidades módulo 15, así como el orden de cada uno de sus elementos.

Tenga presente que $U(15)$ es el grupo de todos los elementos de $\mathbb{Z}_{15}$ que son primos relativos con 15, por lo cual $|U(15)| = \varphi(15) = \varphi(3)\varphi(5) = 2 \times 4 = 8$. Además, este grupo está formado por

$$U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$$

Es claro que el orden de la identidad es 1, por otro lado, el orden de 2 es 4, ya que

$$2^2 \equiv 4 \text{ (mód 15)}, \; 2^3 \equiv 8 \text{ (mód 15)} \text{ y } 2^4 \equiv 1 \text{ (mód 15)}.$$

Lo anterior implica que el orden de 4 es 2. De la misma manera se concluye que el orden de 13 es 4, puesto que $13 \equiv -2$ (mód 15). En la siguiente figura se puede observar el orden de cada uno de los elemento del grupo $U(15)$.

a	1	2	4	7	8	11	13	14
ord(a)	1	4	2	4	4	2	4	2

Figura 2.8: Órdenes de las unidades módulo 15

2.5 Ejercicios

1. En cada uno de los siguientes ejercicios determine si el conjunto dado con la operación tiene estructura de grupo.

   a) $\langle 2\mathbb{Z}, + \rangle$.

   b) $\langle \mathbb{R}^*, * \rangle$ en la que $a * b = \sqrt{ab}$.

   c) $\langle \mathbb{C}, * \rangle$ en la que $a * b = |ab|$.

d) $\langle G, \cdot \rangle$ en el cual G es el conjunto de todas las matrices A tales $\det(A) = \pm 1$ y la operación es la multipicación usual de matrices.

2. Sea $G = \{e, a, b\}$ un grupo finito en el cual e es el elemento identidad. Completar la tabla de Cayley de G

$*$	e	a	b
e	e	a	b
a	a		
b	b		

3. Sea $G = \{e, a, b, c\}$ un grupo finito en el cual e es el elemento identidad y $a^2 = b^2 = e$. Completar la tabla de Cayley de G

$*$	e	a	b	c
e	e	a	b	c
a	a	e		
b	b		e	
c	c			

4. Sea $n \in \mathbb{N}$ un número natural fijo. Considerar el conjunto

$$G = \{e^{\frac{2\pi k}{n} i} \ : \ k = 0, 1, \ldots, n-1\}$$

y la operación multiplicación usual de números complejos. Probar que $\langle G, \cdot \rangle$ tiene estructura de grupo abeliano.

5. Sea $(a, b) \in \mathbb{R}^2$ y definamos las transformación lineal $T_{(a,b)} : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ dada por $T_{(a,b)}(x, y) = (x + a, y + b)$. Probar que el conjunto

$$G = \{ T_{(a,b)} \ : \ (a, b) \in \mathbb{R}^2\}$$

junto con la operación de composición de funciones tiene estructura de grupo.

6. En el conjunto S de los números reales excepto el -1 definir la operación $a * b = a + b + ab$

   a) Probar que $*$ es una operación binaria en S.

   b) Probar que $\langle S, * \rangle$ tiene estructura de grupo abeliano.

   c) Hallar la solución de la ecuación $2 * x * 3 = 7$ en S.

7. Sean a, b elementos de un grupo G y $n \in \mathbb{N}$. Probar que $(a^{-1}ba)^n = a^{-1}b^n a$.

8. Sean a, b elementos de un grupo G. Probar que si $(ab)^2 = a^2b^2$, entonces $ab = ba$.

9. Sean a, b elementos de un grupo G. Probar que si $abc = 1$, entonces $bca = 1$.

10. Sea G un grupo finito. Probar que el número de elementos x de G tales que $x^2 \neq 1$ es par.

11. Sea G un grupo finito. Probar que el número de elementos x de G tales que $x^3 = 1$ es impar.

12. Sea G un grupo. Probar que si $x^2 = 1$ para todo $x \in G$, entonces G es abeliano.

13. Probar que todo grupo de orden 3 es abeliano.

14. Determinar si cada uno de los siguientes subconjuntos son subgrupos de $G = \mathbb{R}^*$ con la multiplicación.

    a) $H = \{x \in G \ : \ x = 1 \text{ o } x \text{ es irracional}\}$.

    b) $K = \{x \in G \ : \ x \geq 1\}$.

15. Sea G un grupo abeliano y $H = \{x \in G \ : \ x^2 = 1\}$. Probar que H es un subgrupo de G.

16. Sea G un grupo abeliano y $H, K \leq G$. Probar que

$$HK = \{hk \ : \ h \in H, \ k \in K\}$$

    es un subgrupo de G.

17. Si H y K son subgrupos de G, probar que $H \cap K$ es un subgrupo de G.

18. Sean G un grupo y $\{H_i\}_{i \in I}$ una familia de subgrupos de G. Probar que $\cap_{i \in I} H_i$ es un subgrupo de G.

19. Sea G un grupo. Probar que

$$\mathcal{Z}(G) = \{x \in G \ : \ ax = xa, \text{para todo } a \in G\}$$

    es un subgrupo de G. Este subgrupo de se denomina el Centro de G.

20. Sea G un grupo y $a \in G$. Entonces probar que

$$C(a) = \{x \in G \ : \ ax = xa\}$$

es un subgrupo de G. Este subgrupo se denomina el centralizador de a.

21. Si H es un subgrupo de G entonces se define

$$C(H) = \{x \in G \ : \ xh = hx \text{ para todo } h \in H\}$$

Probar que $C(H)$ es un subgrupo de G.

22. Sea G un grupo. Probar

a) $\mathcal{Z}(G) = \bigcap_{a \in G} C(a)$.

b) $C(a) = C(a^{-1})$.

c) $C(a) \subseteq C(a^k)$ para todo $k \in \mathbb{Z}$.

23. Sea G un grupo y S un subconjunto de G. Considerar,

$$H = \bigcap_{\substack{S \subseteq K \\ K \leq G}} K$$

Probar que H es un subgrupo de G.

24. Para cada divisor $k > 1$ de n, considerar

$$U_k(n) = \{x \in U(n) \ : \ (x \text{ mód } k) = 1\}.$$

a) Determinar $U_4(20)$ y $U_5(30)$.

b) Probar que $U_k(n)$ es un subgrupo de $U(n)$.

25. Sea $n \in 2\mathbb{Z}^+$ y H un subgrupo de $\mathbb{Z}_n$. Probar que todo elemento de H es par o solo la mitad de los elementos de H son pares.

26. Enumerar todos los elementos de $\langle 3 \rangle$ y $\langle 15 \rangle$ en $\mathbb{Z}_{18}$.

27. En $\mathbb{Z}_{24}$ determinar un generador para el subgrupo $\langle 21 \rangle \cap \langle 10 \rangle$.

28. Sea G un grupo y $a \in G$. ¿Cuál es un generador para el subgrupo $\langle a^m \rangle \cap \langle a^n \rangle$?

29. Para cada uno de los siguientes grupos determinar su orden y el de cada uno de sus elementos.

a) $\mathbb{Z}_{12}$. *b*) $U(10)$. *c*) S_3

30. Sea G un grupo y $a \in G$. Probar que $\text{ord}(a) = \text{ord}(a^{-1})$.

31. Sea G un grupo y $a \in G$ tal que $a^6 = 1$. ¿Cuáles son las posibilidades para $\text{ord}(a)$?

32. Probar que si un grupo abeliano G tiene más de tres elementos de orden 2, entonces G tiene al menos 7 elementos de orden 2.

33. Sea G un grupo y $a \in G$. Si $a^2 \neq 1$ y $a^6 = 1$, probar que $a^4 \neq 1$ y $a^5 \neq 1$. ¿Qué se puede decir del orden de a?

34. Probar que el conjunto

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & 1/a \end{pmatrix} \ : \ a \in \mathbb{R}^*, b \in \mathbb{R} \right\}$$

es un grupo no abeliano con la multiplicación de matrices.

35. Probar que el conjunto

$$SO(2) = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \ : \ a^2 + b^2 = 1 \right\}$$

es un grupo abeliano con la multiplicación de matrices.

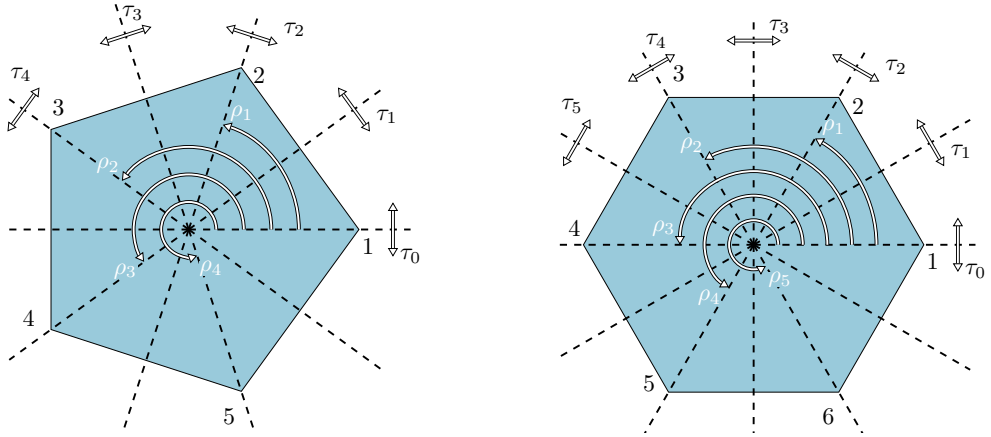
CAPÍTULO 3

Grupo de permutaciones

En la matemática, en general y en la teoría de grupos en particular, el estudio de *las permutaciones* de un conjunto han conducido a obtener grandes avances, por ejemplo, el Teorema de Cayley establece que todo grupo es isomorfo a un grupo de permutaciones. De hecho algunos *software* algebraicos utilizan este resultado para implementar algoritmos que permiten trabajar con diferentes grupos. En líneas generales, una permutación de un conjunto es una reorganización de los elementos del conjunto como sucede con los anagramas de palabras cuyas letras son diferentes. El estudio de las permutaciones es de importancia en teoría de grupos y tiene significativas aplicaciones en otras áreas del conocimiento; por ejemplo, en informática se utilizan para estudiar algoritmos de ordenación, en física cuántica para explicar estados de partículas y en biología para estudiar secuencias del ácido ribonucleico (ARN). En este capítulo se presenta un estudio abstracto de las permutaciones de un conjunto, su estructura de grupo y su representación como producto de ciclos disjuntos y transposiciones.

3.1 Grupo Dihédrico

En esta sección se realiza una introducción a uno de los grupos relevantes en la teoría de grupos, el objetivo es hacer una exposición general de los elementos del grupo y presentar algunos ejemplos, los cuales se pueden generalizar. Recuerde que el grupo Dihédrico D_n está formado por aquellas transformaciones geométricas de un n-ágono regular, las cuales son movimientos rígidos en las que el resultado es una copia de la figura geométrica, y la operación del grupo es la composición de funciones. Con el fin de definir dos presentaciones de este grupo, cada vértice del n-ágono regular será un punto sobre un círculo de radio 1 en el que el primer vértice tiene coordenadas de 1 sobre el eje de las abscisas y 0 sobre el eje de las ordenadas, y los demás son etiquetados en el sentido contrario a las manecillas del reloj, como se muestra en la Figura 3.1.



(a) Grupo D_5 *(b) Grupo D_6*

Figura 3.1: Grupos Dihédricos D_5 y D_6

De acuerdo con lo anterior, el grupo D_n solo tiene dos tipos de transformaciones geométricas.

1. En el primero están las rotaciones con respecto al origen $\rho_0, \rho_1, \ldots, \rho_{n-1}$ en el que el ángulo de rotación de ρ_i es $\left(\frac{360\times i}{n}\right)^\circ$.

2. En el segundo tipo están las simetrías axiales o reflexiones $\tau_0, \tau_1, \ldots, \tau_{n-1}$ en el que la recta de simetría de τ_i es la que pasa por el origen y tienen un ángulo de inclinación de $\left(\frac{180\times i}{n}\right)^\circ$.

En consecuencia, una de las primeras propiedades es que el grupo D_n es de orden $2n$. A continuación se exponen dos maneras de presentar los elementos del grupo D_n; la primera de ellas es mediante permutaciones y la segunda es usando transformaciones lineales en el plano.

Permutaciones. Esta forma de presentar los elementos de D_n es la más usa-

da. En este caso recuerde que una permutación es una función biyectiva del conjunto $[1, n] = \{1, 2, 3 \ldots, n\}$. Como se mencionó anteriormente no toda permutación de S_n es un elemento de D_n, excepto para el caso de $n = 3$. Por otro lado, note que la rotación de $\left(\frac{360}{n}\right)^\circ$ está dada por

$$\rho_1 = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 2 & 3 & \cdots & n & 1 \end{pmatrix},$$

de ahí que para cualquier otra rotación se satisface la igualdad $\rho_i = \rho_1^i$. Por ejemplo, en el grupo D_5 se tiene

$$\rho_3 = \rho_1^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \\ 3 & 4 & 5 & 1 & 2 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix}.$$

En el caso de las simetrías axiales observe que si n es impar, entonces cada eje de simetría pasa a través de uno de los vértices, mientras que para n par el eje de algunas simetrías es la recta que pasa por dos vértices del n-ágono regular y para otras el eje de simetría es la mediatriz de lados opuestos. Por otro lado, note que la primera simetría τ_0 está dada por

$$\tau_0 = \begin{pmatrix} 1 & 2 & 3 & \ldots & k & \ldots & n-1 & n \\ 1 & n & n-1 & \ldots & n+2-k & \ldots & 3 & 2 \end{pmatrix}.$$

Las dos permutaciones definidas anteriomente ρ_1 y τ_0 satisfacen $\text{ord}(\rho_1) = n$ y $\text{ord}(\tau_0) = 2$.

Ejemplo 3.1. En el grupo D_6, sean $x = \rho_1$ y $y = \tau_0$. Calcular cada uno de los siguientes productos xy, x^2y, x^3y, x^4y y x^5y.

Puesto que $x = \rho_1$ y $y = \tau_0$ son elementos del grupo D_6 se tiene que

$$x = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix} \quad \text{y} \quad y = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 5 & 4 & 3 & 2 \end{pmatrix}.$$

Entonces,

- $xy = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 5 & 4 & 3 & 2 \\ 2 & 1 & 6 & 5 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 6 & 5 & 4 & 3 \end{pmatrix} = \tau_1.$

- $x^2y = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 5 & 4 & 3 & 2 \\ 3 & 2 & 1 & 6 & 5 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 6 & 5 & 4 \end{pmatrix} = \tau_2.$

- $x^3y = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 5 & 4 & 3 & 2 \\ 4 & 3 & 2 & 1 & 6 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 1 & 6 & 5 \end{pmatrix} = \tau_3.$

- $x^4y = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 5 & 4 & 3 & 2 \\ 5 & 4 & 3 & 2 & 1 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 2 & 1 & 6 \end{pmatrix} = \tau_4.$

- $x^5y = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 5 & 4 & 3 & 2 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix} = \tau_5.$

Del ejemplo anterior se puede concluir que

$$D_6 = \{1, x, x^2, x^3, x^4, x^5, y, xy, x^2y, x^3y, x^4y, x^5y\}.$$

En general, se puede garantizar que

$$D_n = \{1, x, x^2, \ldots, x^{n-1}, y, xy, x^2y, \ldots, x^{n-1}y\}$$

en el que $x = \rho_1$ y $y = \tau_0$; sin embargo, no es el objetivo de esta sección probar la igualdad.

Ejemplo 3.2. En el grupo D_5 considerar $x = \rho_1$ y $y = \tau_0$.

1. Calcular el producto $xyxy$.

2. Utilizar el ítem anterior para calcular el producto $x^2yx^3yx^4yxy$.

Dado que $x = \rho_1$ y $y = \tau_0$ son elementos del grupo D_5 se tiene que

$$x = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \quad \text{y} \quad y = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 3 & 2 \end{pmatrix}.$$

Entonces,

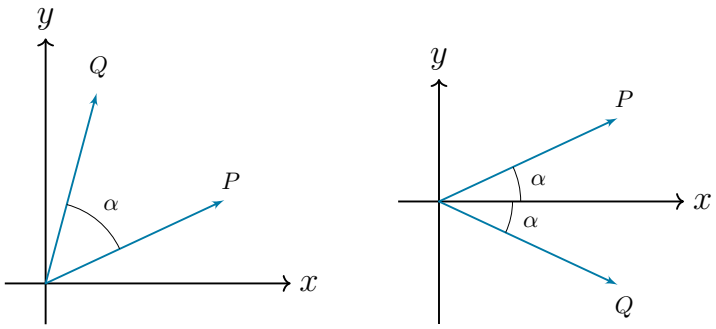
$$xyxy = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 3 & 2 \\ 2 & 1 & 5 & 4 & 3 \\ 5 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = (1).$$

Note que las permutaciones x y y satisfacen $x^5 = (1)$ y $y = y^{-1}$. Luego la igualdad $xyxy = (1)$ implica que $yxy = x^{-1}$; además $(yxy)^k = yx^ky$ para todo entero positivo

k. Por tanto,

$$x^2yx^3yx^4yxy = x^2yx^3yx^3\underbrace{xyxy}_{(1)} = x^2yx^3yx^3 = x^2yx^3yx^{-2} =$$
$$= x^2yx^3y(yxy)^2 = x^2yx^3yyx^2y = x^2.$$

Matrices. Otra manera de representar los elementos del grupo D_n es mediante transformaciones lineales en el plano, lo cual es equivalente a representar los elementos del grupo dihédrico mediante matrices de orden 2×2.



(a) Transformación T_1 *(b) Transformación T_0*

Figura 3.2: Transformaciones lineales de rotación y simetría

Antes de continuar, recuerde que aquellas transformaciones lineales en las cuales dado un ángulo α transforma un punto P del plano en el punto Q en el que el ángulo que se forma entre los puntos P y Q es α, son de la forma

$$T_1\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix}.$$

Por otro lado, la transformación que envia todo punto del plano en su simétrico con respecto al eje de las abscisas es

$$T_0\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix}.$$

En las Figuras 3.2a y 3.2b se representan gráficamente las transformaciones lineales mencionadas.

De acuerdo con lo expuesto, se puede observar que cuando el ángulo de rotación es igual a $\left(\frac{360}{n}\right)^\circ$, la matriz de rotación respectiva corresponde al elemento ρ_0, y de

manera similar la matriz de la transformación de la simetría con respecto al eje horizontal corresponde a la reflexión τ_0. En consecuencia,

$$\rho_0 = \begin{pmatrix} \cos(360/n)^\circ & -\sin(360/n)^\circ \\ \sin(360/n)^\circ & \cos(360/n)^\circ \end{pmatrix} \quad \text{y} \quad \tau_0 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

de lo cual se obtiene que

$$\begin{pmatrix} \cos(360/n)^\circ & -\sin(360/n)^\circ \\ \sin(360/n)^\circ & \cos(360/n)^\circ \end{pmatrix}^n = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Ejemplo 3.3. Determinar la representación mediante matrices de los elementos del grupo D_4, y verificar utilizando la representación por matrices de las igualdades $\rho_2\tau_2 = \tau_0$ y $\rho_1\tau_0\rho_1\tau_0 = (1)$.

Sean $x = \rho_1$ y $y = \tau_0$ elementos de $D_4 = \{1, x, x^2, x^3, y, xy, x^2y, x^3y\}$. Entonces de acuerdo con la representación utilizando matrices de los elementos del grupo Dihédrico se tiene que:

$$x = \begin{pmatrix} \cos\ 90^\circ & -\sin\ 90^\circ \\ \sin\ 90^\circ & \cos\ 90^\circ \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{y} \quad y = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

En consecuencia, el elemento neutro de D_4 es la matriz identidad, y además

- $x^2 = \rho_2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$.
- $x^3 = \rho_3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.
- $xy = \tau_1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.
- $x^2y = \tau_2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$.
- $x^3y = \tau_3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$.

Por otro lado,

$$\rho_1\tau_0\rho_1\tau_0 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

3.2 Grupo Simétrico

Las permutaciones tienen un papel importante en el desarrollo de la teoría de grupos, especialmente en el Teorema de Cayley del Capítulo 6. Por otro lado, son fuente de una gran variedad de ejemplos. Por tal motivo, en este texto se le dedica una sección completa con el fin de que el lector adquiera un manejo adecuado de estos grupos.

Definición 3.1. Una permutación de un conjunto no vacío A es una función biyectiva de A en A.

Recuerde que una función biyectiva es una función la cual es tanto inyectiva como sobreyectiva, hecho que permite construir su función inversa, la cual también es biyectiva. Además, el hecho que la composición de funciones sea asociativa permite afirmar que el conjunto de las permutaciones de un conjunto no vacío A tienen estructura de grupo con la composición de funciones.

Teorema 3.1. El conjunto de las permutaciones de un conjunto no vacío A tiene estructura de grupo con la operación de composición de funciones. Este grupo se denomina el Grupo Simétrico en A y se denota S_A.

Por ejemplo, el conjunto de todas las permutaciones de $[1, 3] = \{1, 2, 3\}$ denotado por S_3 está compuesto por todas las rotaciones y simetrías axiales de un triángulo equilátero.

Definición 3.2. Sea $[1, n] = \{1, 2, \ldots, n\}$. Entonces el conjunto de las permutaciones de $[1, n]$ se denomina el Grupo Simétrico de grado n, y se denota por S_n.

Mediante el principio de la multiplicación es claro que el orden del grupo S_n es $n!$. Por otro lado, si se considera un cuadrado con los vértices etiquetados por los números $1, 2, 3, 4$, entonces algunas permutaciones del grupo S_4 son: 4 rotaciones, 2 simetrías con respecto a las diagonales del cuadrado y 2 simetrías con respecto a las mediatrices de lados opuestos. De lo anterior se concluye que D_8 está contenido propiamente en S_4, esto se debe a que D_8 tiene orden 8 mientras que S_4 tiene orden 24. Esto implica que existen algunas permutaciones del conjunto [4] las cuales no son una rotación o una simetría del

cuadrado, por ejemplo una de ellas es la permutación

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

En general, el grupo D_n es un subconjunto propio de S_n para $n > 3$.

Un tipo de permutación de relevancia para comprender el Grupo Simétrico son los ciclos, los cuales se definen a continuación.

Definición 3.3. Sea $S = \{a_1, a_2, \ldots, a_m\}$ una secuencia de elementos de $[1, n]$. A la permutación definida por

$$\alpha(a_i) = \begin{cases} a_i & \text{si } a_i \notin S \\ a_{i+1} & \text{si } a_i \in S \text{ e } i < m \\ a_1 & \text{si } a_i \in S \text{ e } i = m \end{cases}$$

se le denomina un ciclo de longitud m. El ciclo α se denotará por $\alpha = (a_1 a_2 \cdots a_m)$.

Observe que toda secuencia de elementos de $[1, n]$ induce un ciclo, y todo ciclo induce una secuencia en $[1, n]$. Por otro lado, note que los ciclos

$$\alpha = (a_1 a_2 \cdots a_m) \quad \text{y} \quad \beta = (a_i a_{i+1} \cdots a_m a_1 \cdots a_{i-1}), \quad \text{con } 1 \leq i \leq m,$$

representan la misma permutación.

Ejemplo 3.4. Expresar en la notación de ciclo cada una de las siguientes permutaciones y determine su longitud.

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

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

De acuerdo con la primera permutación se tiene que el 1 es enviado al 2 y este a su vez es enviado al 3, como se muestra en la siguiente figura. Si se le da continudad a este

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

Figura 3.3: Ejemplo permutaciones y orden

proceso obtenemos la secuencia $1 \to 2 \to 3 \to 4 \to 6 \to 5 \to 1$, de lo cual se obtiene que $\alpha = (123465)$ tiene longitud 6. Para la segunda permutación, la secuencia que se obtiene es $2 \to 3 \to 4 \to 5 \to 2$, de este modo $\beta = (2345)$ con longitud igual a 4.

Proposición 3.1. Si α es un ciclo de longitud $m > 1$, entonces
1. $\text{ord}(\alpha) = m$.
2. $\alpha^{-1} = \alpha^{m-1}$.

Demostración. Suponga que $\alpha = (a_1 a_2 \cdots a_m)$ y sea $S_\alpha = \{a_1, a_2, \ldots, a_m\}$ su secuencia asociada. Entonces para cada $a \notin S_\alpha$ se cumple $\alpha^m(a) = a$. Ahora, para cada $a_i \in S_\alpha$ con $1 \leq i \leq m$ se cumple que

$$\alpha^m(a_i) = \alpha^{m-1}(a_{i+1}) = \cdots = \alpha^{m-(m-i)}(a_m),$$

entonces

$$\alpha^m(a_i) = \alpha^{i-1}(a_1) = \alpha^{i-2}(a_2) = \cdots = \alpha(a_{i-1}) = a_i.$$

En consecuencia, m es el mínimo entero positivo para el cual α^m es la permutación identidad. Por otro lado, como el orden de α es m se tiene que $\alpha^m = \alpha^{m-1}\alpha = (1)$, y así por la unicidad del elemento inverso $\alpha^{-1} = \alpha^{m-1}$. □

La anterior proposición implica que si $a \in S_\alpha$ con α, un ciclo de longitud m, entonces este se puede expresar como

$$\alpha = (a\ \alpha(a)\ \alpha^2(a) \cdots \alpha^{m-1}(a)).$$

Definición 3.4. Sean α y β dos ciclos con secuencias asociadas S_α y S_β. Entonces se dice que α y β son ciclos disjuntos si $S_\alpha \cap S_\beta = \emptyset$.

Recuerde que en general la composición de permutaciones no es una operación conmutativa, sin embargo, la definición de ciclos disjuntos implica el siguiente teorema.

Teorema 3.2. Si α y β son ciclos disjuntos, entonces $\alpha\beta = \beta\alpha$.

Demostración. Sea $x \in [1, n]$, si $x \notin S_\alpha \cup S_\beta$, entonces

$$(\alpha\beta)(x) = \alpha(x) = x = \beta(x) = (\beta\alpha)(x).$$

Ahora, suponga que $x \in S_\alpha$. Del hecho que α y β son ciclos disjuntos se tiene $x \notin S_\beta$ y $\alpha(x) \notin S_\beta$. Entonces

$$(\alpha\beta)(x) = \alpha(x) = \beta(\alpha(x)) = (\beta\alpha)(x).$$

El caso $x \in S_\beta$ es similar. Por tanto, $\alpha\beta = \beta\alpha$. □

Teorema 3.3. Toda permutación de S_n se puede expresar como el producto de ciclos disjuntos.

Demostración. Sea α una permutación de S_n. Si α es la permutación identidad no hay nada que probar. Sin embargo, si existe $a \in [1, n]$ tal que $\alpha(a) \neq a$, entonces existe un entero positivo k_1 para el cual $\alpha^{k_1}(a) = a$. Sea α_1 el ciclo dado por $\alpha_1 = (a\ \alpha(a)\ \alpha^2(a) \cdots \alpha^{k_1-1}(a))$.

Si para todo $b \notin S_{\alpha_1}$ se cumple que $\alpha(b) = b$, entonces $\alpha = \alpha_1$. Si por el contrario $\alpha(b) \neq b$ para algún $b \notin S_{\alpha_1}$, entonces existe un entero positivo k_2 para el cual $\alpha^{k_2}(b) = b$. Sea α_2 el ciclo dado por $\alpha_2 = (b\ \alpha(b)\ \alpha^2(b) \cdots \alpha^{k_2-1}(b))$.

Note que si para todo $c \notin S_{\alpha_1} \cup S_{\alpha_2}$ se cumple que $\alpha(c) = c$, entonces $\alpha = \alpha_1\alpha_2$. En caso contrario, se continúa con este proceso y se obtiene que existe un número finito de ciclos disjuntos $\alpha_1, \alpha_2, \ldots, \alpha_r$ tales que

$$\alpha = \alpha_1\alpha_2 \cdots \alpha_r. \qquad \square$$

Ejemplo 3.5. Considerar las siguientes permutaciones de S_6.

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 4 & 6 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 4 & 3 & 5 \end{pmatrix} \quad \text{y}$$
$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 5 & 1 & 6 & 3 \end{pmatrix}$$

1. Expresar cada una de las anteriores permutaciones como producto de ciclos disjuntos.

2. Calcular el producto $\alpha\beta$.

3. Calcular las inversa de las permutaciones α y γ.

De acuerdo con la demostración del Teorema 3.3, se concluye que

$$\alpha = (12)(45), \quad \beta = (16532) \quad \text{y} \quad \gamma = (14)(356).$$

Por otro lado, según la notación utilizada para las permutaciones se tiene que

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 4 & 3 & 5 \\ 6 & 2 & 1 & 5 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 1 & 5 & 3 & 4 \end{pmatrix} = (16453).$$

Ahora observe que si $\alpha_1 = (12)$ y $\alpha_2 = (45)$, entonces $\alpha_1^{-1} = (12)$ y $\alpha_2^{-1} = (45)$. Esto implica que

$$\alpha^{-1} = \alpha_2^{-1}\alpha_1^{-1} = (45)(12) = (12)(45) = \alpha.$$

Finalmente, si $\gamma_1 = (14)$ y $\gamma_2 = (356)$, entonces $\gamma_1^{-1} = (14)$ y $\gamma_2^{-1} = \gamma_2^2 = (365)$. En consecuencia,

$$\gamma^{-1} = \gamma_2^{-1}\gamma_1^{-1} = (365)(14).$$

Teorema 3.4. Si $\alpha = \alpha_1\alpha_2\cdots\alpha_k$ es una permutación en la que los α_i son ciclos disjuntos por pares, entonces

$$\text{ord}(\alpha) = \text{m.c.m}\{\text{ord}(\alpha_1), \text{ord}(\alpha_2), \ldots, \text{ord}(\alpha_k)\}.$$

Demostración. Sea $m_i = \text{ord}(\alpha_i)$ para cada $i = 1, 2, \ldots, k$. Note que $\alpha^m = \alpha_1^m\alpha_2^m\cdots\alpha_k^m$ para todo $m \in \mathbb{Z}$, esto se debe a que los ciclos α_i son disjuntos por pares. De ahí que si $m = \text{m.c.m}\{m_1, m_2, \ldots, m_k\}$, entonces

$$\alpha_i^m = \alpha_i^{m_i s_i} = (\alpha_i^{m_i})^{s_i} = (1)^{s_i} = (1)$$

para algún entero s_i y todo $i = 1, 2, \ldots, k$. Por lo cual, $\alpha^m = (1)$. Ahora bien, si s es un entero positivo menor que m, entonces existe algún i para el cual s no es múltiplo de m_i. Luego por el algoritmo de la división existen enteros q y r tales que $s = m_i q + r$ con $0 < r < m_i$, y así $\alpha_i^s = \alpha_i^r \neq (1)$. Por tanto, para todo entero positivo s menor a $m = \text{m.c.m}\{m_1, m_2, \ldots, m_k\}$ se tiene que $\alpha^s \neq (1)$. □

Ejemplo 3.6. Determinar el orden de la permutación $\alpha = (12745)(3526)$.

Primero note que es equivocado afirmar que el orden de α es 20, ya que no es el producto de ciclos disjuntos. Ahora, si se multiplican los ciclos se obtiene

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 6 & 5 & 4 & 2 & 3 & 7 \\ 2 & 6 & 1 & 5 & 7 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 6 & 1 & 5 & 7 & 3 & 4 \end{pmatrix} = (1263)(457).$$

Por tanto, el orden de α es $\text{m.c.m}\{\text{ord}(1263), \text{ord}(457)\} = \text{m.c.m}\{4, 3\} = 12$.

Ejemplo 3.7. En el grupo simétrico S_4.

1. Determinar el número de permutaciones de orden 3.

2. Hallar todas las permutaciones de orden 3.

Si α es una permutación de S_4 de orden 3, entonces α no puede ser el producto de dos ciclos disjuntos, ya que si $\alpha = \alpha_1\alpha_2$ con $\text{ord}(\alpha_1) = \text{ord}(\alpha_2) = 3$, entonces $|S_{\alpha_1} \cup S_{\alpha_2}| = 6$ lo cual es imposible. Por otro lado, note que los únicos ciclos de orden 3 son de la forma (ijk) e (ikj). Esto implica que para cada subconjunto de 3 elementos de $[1,4] = \{1,2,3,4\}$ se pueden construir dos ciclos distintos de longitud 3. En consecuencia, el número de permutaciones de orden 3 es $\binom{4}{3} \cdot 2 = 8$. Según el anterior análisis, se tiene que los ciclos distintos de longitud 3 en $[1,4]$ son:

- (123).
- (134).
- (124).
- (234).
- (132).
- (143).
- (142).
- (243).

Ejemplo 3.8. Determinar el número de elementos de S_7 de orden 3.

Sea α una permutación de S_7 de orden 3. Entonces α puede ser un ciclo de longitud 3, y en dicho caso existen $\binom{7}{3} \cdot 2 = 70$ permutaciones de este tipo. Ahora, si α es el producto de dos ciclos disjuntos α_1 y α_2, entonces

$$\text{ord}(\alpha) = \text{m.c.m}\{\text{ord}(\alpha_1), \text{ord}(\alpha_2)\} = 3$$

y así $\text{ord}(\alpha_1) = \text{ord}(\alpha_2) = 3$. Por lo cual, existen

$$\binom{7}{3} \cdot 2 \cdot \binom{4}{3} \cdot 2 = 35 \cdot 2 \cdot 4 \cdot 2 = 560$$

permutaciones de orden 3 que son el producto de dos ciclos disjuntos. En consecuencia, se tienen $70 + 560 = 630$ permutaciones en S_7 de orden 3.

Definición 3.5. Una transposición es un ciclo de longitud 2.

Observe que cada ciclo se puede expresar como

$$(a_1 a_2 \cdots a_k) = (a_1 a_k) \cdots (a_1 a_3)(a_1 a_2)$$

lo cual garantiza el Teorema 3.5. Sin embargo, esta representación no es la única manera de expresar un ciclo como producto de transposiciones; por ejemplo

$$(12345) = (15)(14)(13)(12) = (54)(52)(21)(25)(23)(13).$$

Teorema 3.5. Cada permutación de S_n con $n > 1$ es un producto de transposiciones.

Teorema 3.6. Si una permutación α puede expresarse como el producto de un número par (o impar) de transposiciones, entonces cada descomposición de α en producto de transposiciones debe tener un número par (o impar) de transposiciones.

Demostración. Basta probar que la permutación identidad no se puede expresar como el producto de un número impar de transposiciones. Sea $i \in [1, n]$ y considere todos los posibles productos de transposiciones $\tau_1\tau_2$ tales que $i \in S_{\tau_2}$, entonces

- $\tau_1\tau_2 = (ij)(ij) = (1)$.
- $\tau_1\tau_2 = (ik)(ij) = (ijk) = (jki) = (ji)(jk) = (ij)(jk) = \tau_1'\tau_2'$.
- $\tau_1\tau_2 = (jk)(ij) = (ikj) = (kji) = (ki)(kj) = (ik)(kj) = \tau_1'\tau_2'$.
- $\tau_1\tau_2 = (kl)(ij) = (ij)(kl) = \tau_1'\tau_2'$.

Observe que en cualquiera de los últimos tres casos es posible expresar $\tau_1\tau_2$ como el producto de dos nuevas transposiciones $\tau_1'\tau_2'$ en el que $i \in S_{\tau_1'} \backslash S_{\tau_2'}$. Ahora suponga que $(1) = \tau_1\tau_2\cdots\tau_r$ es el producto de r transposiciones y sea i uno de los elementos de la transposición τ_r. Entonces de acuerdo con los anteriores casos es posible transformar el producto $\tau_1\tau_2\cdots\tau_r$ en uno de la siguiente forma

1. $(1) = (ij)(ij)\tau_1'\tau_2'\cdots\tau_{r-2}' = \tau_1'\tau_2'\cdots\tau_{r-2}'$.
2. $(1) = (ij)\tau_1'\tau_2'\cdots\tau_{r-1}'$

en el cual las permutaciones $\tau_1'\tau_2'\cdots\tau_{r-2}'$ y $\tau_1'\tau_2'\cdots\tau_{r-1}'$ dejan invariante a i. Note que el segundo caso no es posible, puesto que la permutación del lado derecho de la igualdad transforma al elemento i en j. En consecuencia, la aplicación reiterada del procedimiento anterior permite concluir que r debe ser par. □

Definición 3.6. Una permutación se denomina par (o impar) si puede expresarse como el producto de un número par (o impar) de transposiciones.

El anterior teorema permite clasificar los elementos de S_n en pares o impares, en este sentido A_n denotará el conjunto de todas las permutaciones pares de S_n.

Teorema 3.7. El conjunto A_n es un subgrupo de S_n.

Demostración. Sean $\alpha, \beta \in A_n$ y suponga que

$$\alpha = \tau_1\tau_2\cdots\tau_{2r} \quad \text{y} \quad \beta = \rho_1\rho_2\cdots\rho_{2s}$$

en el cual τ_i y ρ_j son transposiciones. Entonces

$$\alpha\beta^{-1} = \tau_1\tau_2\cdots\tau_{2r}\rho_{2s}^{-1}\cdots\rho_2^{-1}\rho_1^{-1} = \underbrace{\tau_1\tau_2\cdots\tau_{2r}\rho_{2s}\cdots\rho_2\rho_1}_{2(r+s)-\text{transposiciones}}$$

y así por el Teorema 3.6 se concluye que $\alpha\beta^{-1} \in A_n$. □

Definición 3.7. El subgrupo A_n se denomina el subgrupo alternante de S_n.

Ejemplo 3.9. Clasificar en par o impar cada una de las permutaciones de S_3.

Recuerde que S_3 está conformado por 3 rotaciones y 3 simetrías con respecto a cada una de las bisectrices de los ángulos de un triángulo equilátero. Cada una de las rotaciones son ciclos de longitud 3 y las simetrías son transposiciones, por lo cual, las rotaciones son permutaciones pares y las simetrías axiales son impares. De ahí que $A_3 = \{(1), (123), (132)\}$.

Proposición 3.2. Para $n > 1$, el orden de A_n es $\dfrac{n!}{2}$.

Demostración. Sean B_n el conjunto de todas las permutaciones impares y $\tau = (12)$. Considere la función $F : A_n \to B_n$ dada por $F(\alpha) = \alpha\tau$. Si $\alpha_1, \alpha_2 \in A_n$ son tales que $F(\alpha_1) = F(\alpha_2)$ entonces por las leyes cancelativas en el grupo S_n se concluye que $\alpha_1 = \alpha_2$. Por otro lado, observe que para $\beta \in B_n$ la permutación $\beta\tau$ es par y además $F(\beta\tau) = \beta$. En consecuencia, la función F es biyectiva lo cual implica que $|A_n| = |B_n|$ y por tanto,

$$2|A_n| = |A_n| + |B_n| = |S_n| = n!.$$ □

3.3 Ejercicios

1. Para cada una de las siguientes permutaciones.

   - (1235)(413).
   - (13256)(23)(46512).
   - (345)(245).

   a) Escribir cada una de las siguientes permutaciones como el producto de ciclos disjuntos.

b) Determinar su orden.

c) Determinar cuales son pares o impares.

2. Probar que A_8 tiene un elemento de orden 15.

3. Encontrar un elemento en A_{12} de orden 30.

4. Si $\beta = (123)(145)$, expresar β^{99} como producto de ciclos.

5. ¿Cuántos elementos de orden 4 tiene S_6?

6. Sean $(a_1a_2a_3a_4)$ y (a_5a_6) ciclos disjuntos en S_{10}. Probar que no existe una pemutación $\alpha \in S_{10}$ tal que $\alpha^2 = (a_1a_2a_3a_4)(a_5a_6)$.

7. Para $\beta = (135798)(246)$ ¿Cuál es el entero positivo más pequeño n para el cual $\beta^n = \beta^{-5}$?

8. Considerar $H = \{\beta \in S_5 \ : \ \beta(1) = 1, \ \beta(3) = 3\}$.

   a) Probar que H es un subgrupo de S_5.

   b) Determinar el orden de H.

   c) ¿Es H un subgrupo cuando se reemplaza S_5 por S_n con $n \geq 3$?

   d) ¿Cuántos elementos tiene H cuando se reemplaza S_5 por A_n con $n \geq 4$?

9. En el grupo D_n sean $x = \rho_1$ y $y = \tau_0$.

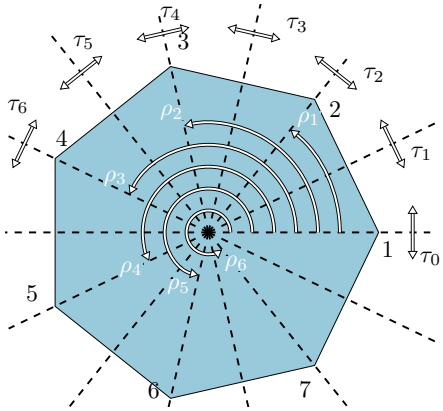
   a) Probar que todo elemento de la forma x^ky es de orden 2.

   b) Probar que $x(x^ky)x^{-1} = x^{k+2}y$ para $k = 0, 1, \ldots, n-2$ y $x(x^{n-1}y)x^{-1} = xy$

10. Determinar la representación mediante matrices de los elementos de D_3.

11. Determinar el centro de los grupos D_6 y D_7.

12. Determinar la representación mediante permutaciones de los elementos de D_7, y calcular los productos $x^2, x^3, x^4, x^5, x^6, xy, x^2y, x^3y, x^4y, x^5y, x^6y$ en los cuales $x = \rho_1$ y $y = \tau_0$.



13. Determinar el centro del grupo D_n.

CAPÍTULO 4

Grupos cíclicos y finitamente generados

El estudio de la estructura de los grupos, en general, se realiza analizando los subgrupos que tienen la estructura más simple, estos son los *grupos cíclicos* que son una subclase de la clase de grupos finitamente generados. En este capítulo se presenta un estudio detallado de los grupos cíclicos, necesario para alcanzar el teorema de clasificación de grupos abelianos finitamentemente generados.

4.1 Grupos cíclicos

Como sucede con el grupo de permutaciones los grupos cíclicos juegan un papel importante en la teoría de grupos, puesto que permiten caracterizar muchos de los grupos conocidos. Además, por su estructura simple muchas de sus propiedades son fáciles de comprender y probar. Recuerde que para un grupo G y $a \in G$ el subgrupo cíclico generado

por a es el conjunto

$$\langle a\rangle = \{a^k \ : \ k \in \mathbb{Z}\}.$$

En este sentido se tiene la siguiente definición.

Definición 4.1. Un grupo G se denomina cíclico si $G = \langle a\rangle$ para algún $a \in G$. Al elemento a se le denomina un generador del grupo.

De acuerdo con la definición anterior, note que un grupo cíclico es abeliano, además puede tener más de un generador, por ejemplo los enteros 1 y -1 generan a los enteros, puesto que

$$\mathbb{Z} = \{1 \cdot k \ : \ k \in \mathbb{Z}\} = \{(-1) \cdot k \ : \ k \in \mathbb{Z}\},$$

en el cual

$$1 \cdot k = \underbrace{1 + 1 + \cdots + 1}_{k \text{ veces}}$$

si k es un entero positivo, y en caso contrario

$$1 \cdot k = \underbrace{-1 - 1 - \cdots - 1}_{-k \text{ veces}}.$$

Otro ejemplo es el grupo de residuos módulo n en el que uno de sus generadores es el elemento 1, este grupo tiene más generadores como se probará más adelante. Un ejemplo más es el grupo $U(10) = \{1, 3, 7, 9\}$ de las unidades módulo 10, el cual es generado por 3, puesto que $3^0 = 1$, $3^1 = 3$, $3^2 = 9$ y $3^4 = 7$. Sin embargo, es importante mencionar que no todos los grupos son cíclicos, por ejemplo los no abelianos como el grupo dihédrico D_n o el grupo simétrico S_n, pero además existen grupos abelianos que no son cíclicos como por ejemplo el grupo de los números reales $\mathbb{R}$ o el de los números racionales $\mathbb{Q}$.

Por otro lado, según la demostración de la Proposición 2.5 se tiene que todo grupo cíclico es finito o equipotente con el conjunto de los números enteros.

Proposición 4.1. Sea G un grupo y $a \in G$.

1. Si $\text{ord}(a) = n$, entonces $\langle a\rangle = \{1, a, a^2, \ldots, a^{n-1}\}$.
2. Si $a^k = 1$ para algún $k \in \mathbb{Z}$, entonces $\text{ord}(a)$ divide a k.
3. Si $\text{ord}(a) = n$, $a^i = a^j$ si y solo si n divide a $i - j$.

Demostración. Cada una de las afirmación son consecuencia de la demostración de la Proposición 2.5. □

Note que si $\text{ord}(a)$ es infinito, entonces se satisface que $a^i = a^j$ siempre y cuando $i = j$. Además, a partir de la anterior proposición se puede concluir que para cualquier elemento a de un grupo G se cumple la relación $\text{ord}(a) = |\langle a\rangle|$. El conocimiento de la

estructura de los subgrupos de un grupo es de gran importancia en esta área y en el caso de los grupos cíclicos se conoce su estructura.

Teorema 4.1. Si G es un grupo cíclico generado por a, entonces
1. Todo subgrupo de G es también cíclico.
2. Si G es finito, entonces por cada divisor positivo d del orden de G existe un subgrupo de G de orden d.

Demostración. Sean H un subgrupo no trivial de G y m la mínima potencia positiva de a que pertenece a H, es decir

$$m = \text{mín}\{i \in \mathbb{Z}^+ \ : \ a^i \in H\}.$$

De ahí que $\langle a^m \rangle \subseteq H$. Sea k un entero tal que $a^k \in H$, entonces existen enteros q y r tales que $k = qm + r$ con $0 \leq r < m$ y así

$$a^r = a^k a^{-mq} \in H.$$

Por tanto, $r = 0$ puesto que en caso contrario se contradice la minimalidad de m. Esto implica que $H \subseteq \langle a^m \rangle$ y se prueba la primera afirmación.

Para segunda afirmación suponga que $|G| = n$ y sea d un divisor positivo de n. Note que el elemento $a^{\frac{n}{d}}$ satisface la igualdad

$$(a^{\frac{n}{d}})^d = a^n = 1,$$

además si para algún $0 < i < d$ se cumple que $(a^{\frac{n}{d}})^i = 1$, entonces del primer ítem de la Proposición 4.1 se obtiene que

$$n \leq \frac{ni}{d}.$$

Ello conduce a la contradicción $d \leq i$, y en consecuencia $|\langle a^{\frac{n}{d}} \rangle| = d$. □

El anterior teorema garantiza la existencia de un subgrupo por cada divisor positivo del orden de un grupo cíclico finito y, además, su demostración construye dicho subgrupo. Por ejemplo, el grupo $\mathbb{Z}_{12}$ es de orden 12 y un subgrupo de orden 4 es

$$\left\langle \frac{12}{4} \right\rangle = \langle 3 \rangle = \{0, 3, 6, 9\}.$$

Adicionalmente, se concluye que si $d \mid n$ con $d > 0$, entonces $\text{ord}(a^d) = \frac{n}{d}$. Por otro lado, es importante mencionar que la relación que se presenta en el segundo ítem del Teorema 4.1 no es cierta para todo grupo finito, como se verá en el siguiente capítulo.

Ejemplo 4.1. Considerar el subconjunto de los enteros

$$H = \{30x + 42y \ : \ x, y \in \mathbb{Z}\}.$$

Probar que H es un subgrupo de $\mathbb{Z}$ y determinar uno de sus generadores.

Sean $a = 30x_1 + 42y_1$ y $b = 30x_2 + 42y_2$ elementos de H. Entonces

$$a - b = 30x_1 + 42y_1 - 30x_2 - 42y_2 = 30(x_1 - x_2) + 42(y_1 - y_2)$$

y así $a - b \in H$, por tanto $H \leq \mathbb{Z}$. Por otro lado, observe que

$$6 = \text{m.c.d}\{30, 42\} = 30 \times (-4) + 42 \times (3),$$

con lo cual se obtiene que $6 \in H$. Por otro lado, para todo $x, y \in \mathbb{Z}$ se cumple que

$$30x + 42y = 6(5x + 7y).$$

En consecuencia, $H = \langle 6 \rangle$.

Ejemplo 4.2. Sea n un entero positivo y considerar el subconjunto de los números complejos

$$H = \{z \in \mathbb{C}^* \ : \ z^n = 1\}.$$

Probar que H es un subgrupo cíclico de $\mathbb{C}^*$, y determinar uno de sus generadores.

Recuerde que en el grupo $\mathbb{C}^*$ la operación binaria es la multiplicación de números complejos. Note además que por el Teorema Fundamental del Álgebra el orden de H es n, y que si $z \in H$, entonces $z^{-1} = \frac{1}{z} \in H$. Ahora bien, para $z_1, z_2 \in H$ se tiene que

$$(z_1 z_2)^n = z_1^n z_2^n = 1.$$

Por tanto, H es un subgrupo de $\mathbb{C}^*$. Puesto que $z^m = \cos(m\theta) + i\sin(m\theta)$ con $z = \cos\theta + i\sin\theta$, se obtiene que las soluciones de la ecuación $z^n = 1$ son:

$$z_k = \cos\left(\frac{2\pi k}{n}\right) + i\sin\left(\frac{2\pi k}{n}\right)$$

para $k = 0, 1, \ldots, n-1$. Esto implica que

$$H = \langle z_1 \rangle = \{1, z_1, z_1^2, \ldots, z_1^{n-1}\}.$$

Teorema 4.2. Si G es un grupo cíclico generado por a con $\text{ord}(a) = n$, entonces

1. $\langle a^k \rangle = \langle a^d \rangle$.

2. $\text{ord}(a^k) = \dfrac{n}{d}$.

con $d = \text{m.c.d}\{k, n\}$.

Demostración. Para $d = \text{m.c.d}\{k, n\}$ existen enteros x y y tales que $d = nx + ky$. Esto implica que

$$a^d = a^{nx+ky} = a^{ky}$$

y así $a^d \in \langle a^k \rangle$, con lo cual se obtiene $\langle a^d \rangle \subseteq \langle a^k \rangle$. En el otro sentido, se conoce que $k = dk_1$ para algún entero k_1 lo cual conduce a que $a^k \in \langle a^d \rangle$, y así $\langle a^k \rangle \subseteq \langle a^d \rangle$. En consecuencia, $\langle a^k \rangle = \langle a^d \rangle$. La segunda afirmación se obtiene de la igualdad

$$\text{ord}(a^k) = \text{ord}(a^d).$$ □

Un hecho importante que se deduce de los Teoremas 4.1 y 4.2 es que para todo divisor positivo del orden de un grupo cíclico G existe un único subgrupo de ese orden. Por otro lado, si a es un generador de G entonces a^k es también un generador de G siempre y cuando n y k sean primos relativos. Esto implica que G cuenta con $\varphi(n)$ generadores en la que φ es la función indicatriz de Euler.

Ejemplo 4.3. Determinar todos los generadores del grupo cíclico $\mathbb{Z}_{18}$.

El número de generadores con los que cuenta $\mathbb{Z}_{18}$ es $\varphi(18)$, con

$$\varphi(18) = \varphi(2 \cdot 3^2) = \varphi(2)\varphi(3^2) = (2-1)(3^2-3) = 6.$$

Además, los generadores de $\mathbb{Z}_{18}$ son los elementos $a \in \mathbb{Z}_{18}$ que sean primos relativos con 18, esto es, los generadores de $\mathbb{Z}_{18}$ son:

$$1, 5, 7, 11, 13, 17.$$

Ejemplo 4.4. Sea G un grupo cíclico de orden 30 y a uno de sus generadores. Hallar,

1. $\langle a^{18} \rangle$.
2. $\text{ord}(a^{18})$.
3. $\langle a^{26} \rangle$.
4. $\text{ord}(a^{26})$.

Utilizando el Teorema 4.2 se tiene que

$$\text{ord}(a^{18}) = \frac{30}{\text{m.c.d}\{30, 18\}} = \frac{30}{6} = 5$$

y

$$\langle a^{18} \rangle = \langle a^6 \rangle = \{1, a^6, a^{12}, a^{18}, a^{24}\}.$$

De manera similar se obtiene

$$\text{ord}(a^{26}) = \frac{30}{\text{m.c.d}\{30, 26\}} = \frac{30}{2} = 15$$

y

$$\langle a^{26}\rangle = \langle a^2\rangle = \{1, a^2, a^4, a^6, a^8, a^{10}, a^{12}, a^{14}, a^{16}, a^{18}, a^{20}, a^{22}, a^{24}, a^{26}, a^{28}\}.$$

Esta sección finaliza con algunas consecuencias de los Teoremas 4.1 y 4.2, y con un ejemplo en el que se aplican varios resultados de esta sección.

Corolario 4.1. Sean G un grupo.

1. Si G es cíclico finito, entonces $\text{ord}(a)$ divide a $|G|$ para todo $a \in G$.
2. Si $\text{ord}(a) = n$, entonces
   a) $\langle a^i\rangle = \langle a^j\rangle$ si y solo si $\text{m.c.d}\{n, i\} = \text{m.c.d}\{n, j\}$.
   b) $\text{ord}(a^i) = \text{ord}(a^j)$ si y solo si $\text{m.c.d}\{n, i\} = \text{m.c.d}\{n, j\}$.

Ejemplo 4.5. Determinar todos los subgrupos de $\mathbb{Z}_{30}$, así como los generados de cada uno de ellos.

Dado $|\mathbb{Z}_{30}| = 30 = 2 \cdot 3 \cdot 5$, se tiene que los únicos órdenes de subgrupos de $\mathbb{Z}_{30}$ son: $1, 2, 3, 5, 6, 10, 15$ y 30. En la siguiente tabla se presenta para cada orden el respectivo subgrupo y sus generados.

$\lvert\langle x\rangle\rvert$	$\langle x\rangle$	x
1	$\langle 0\rangle$	0
2	$\langle 15\rangle$	15
3	$\langle 10\rangle$	10, 20
5	$\langle 6\rangle$	6, 12, 18, 24
6	$\langle 5\rangle$	5, 25
10	$\langle 3\rangle$	3, 9, 21, 27
15	$\langle 2\rangle$	2, 4, 8, 14, 16, 22, 26, 28
30	$\mathbb{Z}_{30}$	1, 7, 11, 13, 17, 19, 23, 29

Figura 4.1: Subgrupos de $\mathbb{Z}_{30}$

A partir del cuadro anterior se construye el diagrama de Hasse del retículo del conjunto de subgrupos de $\mathbb{Z}_{30}$, ver Figura 4.2.

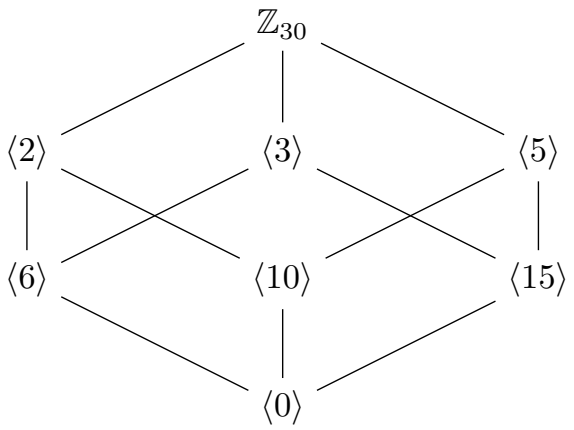


Figura 4.2: Diagrama de Hasse de los subgrupos de $\mathbb{Z}_{30}$

4.2 Grupos finitamente generados

En la sección anterior se consideran grupos generados por un solo elemento, con lo cual es lógico pensar si existen grupos generados por más de un elemento, como es el caso del grupo Dihédrico D_n estudiado en la Sección 3.1, el cual es un grupo generado por dos elementos uno de orden 2 y otro de orden n.

Antes de entrar a definir el subgrupo generado por más de un elemento, es importante tener en cuenta que de acuerdo con el ejercicio 18 del conjunto de Problemas 2.5 si $\{H_i\}_{i\in I}$ es una familia de subgrupos de un grupo G, entonces

$$\bigcap_{i\in I} H_i$$

es un subgrupo de G. Esto implica que si para un subconjunto $S \subseteq G$ se considera la familia de subgrupos H_i tales que $S \subseteq H_i$, entonces la intersección de los elementos de la familia es el mínimo (bajo contenencia) subgrupo de G que contiene a S.

Definición 4.2. Sea G un grupo y S un subconjunto de G. Entonces se define el subgrupo generado por S como el subgrupo de G que se obtiene por la intersección de los subgrupos de la familia $\{H_i\}_{i\in I}$, con $S \subseteq H_i$ para todo $i \in I$. Este subgrupo se denota por $\langle S \rangle$ y a S se le denomina un conjunto de generadores de $\langle S \rangle$.

En caso de que el conjunto S sea finito, se dice que el sugbrupo $\langle S \rangle$ es un subgrupo

finitamente generado. Esto no implica que el orden de $\langle S\rangle$ sea finito; por ejemplo $\mathbb{Z}$ es un grupo infinito y finitamente generado ya que $\langle 1\rangle = \mathbb{Z}$. Por otro lado, note que el conjunto de todos los subgrupos del grupo G forman un conjunto parcialmente ordenado, con lo cual se deduce que el subgrupo generado por S es el mínimo subgrupo de G que contiene a S.

Teorema 4.3. Si G es un grupo y $S \subseteq G$, entonces $\langle S\rangle$ está compuesto por todos los elementos de la forma

$$x_1^{a_1} x_2^{a_2} \cdots x_r^{a_r}$$

en el cual $x_1, x_2, \ldots, x_r \in S$ y $a_1, a_2, \ldots, a_r \in \{-1, 1\}$.

Demostración. Considere el conjunto

$$H = \{x_1^{e_1} x_2^{e_2} \cdots x_r^{e_r} \ : \ x_1, x_2, \ldots, x_r \in S, \ e_1, e_2, \ldots, e_r \in \{-1, 1\}\}.$$

Entonces para $a = x_1^{e_1} x_2^{e_2} \cdots x_r^{e_r}$ y $b = y_1^{f_1} y_2^{f_2} \cdots y_k^{f_k}$ elementos de H se cumple que $ab \in H$. Además, note que

$$b^{-1} = y_k^{-f_k} y_{k-1}^{-f_{k-1}} \cdots y_1^{-f_1},$$

es un elemento de H. Por tanto, H es un subgrupo de G tal que $S \subseteq H$. Por otro lado, si se considera la familia de subgrupos de G que contienen a S dada por $\{H_i\}_{i\in I}$ se tiene que $H \subseteq H_i$. Esto se debe al hecho que para cada $a = x_1^{e_1} x_2^{e_2} \cdots x_r^{e_r} \in H$ los elementos $x_1, x_2, \ldots, x_r \in H_i$ y por ser H_i un subgrupo se cumple que $a \in H_i$ para todo $i \in I$. Por tanto, se garantiza que

$$H = \bigcap_{i\in I} H_i = \langle S\rangle. \qquad \square$$

Según el anterior resultado se tiene que si el grupo G es abeliano, entonces los elementos de $\langle S\rangle$ son de la forma $x_1^{k_1} x_2^{k_2} \cdots x_r^{k_r}$ con $k_i \in \mathbb{Z}$ y los elementos $x_1, x_2, \ldots, x_r$ son todos distintos.

Por otro lado, note que este resultado está en concordancia con la definición de subgrupo cíclico generado por un elemento $a \in G$. Además, se conoce que si a es un elemento de orden finito de un grupo G, entonces todo elemento del subgrupo $\langle a\rangle$ es de orden finito, sin embargo, esto no sucede en general cuando el conjunto generador tiene más de un elemento, excepto en el caso que G sea abeliano. Por ejemplo en $GL(2, \mathbb{R})$ las matrices

$$x = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{y} \quad y = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

son de orden finito, específicamente $\text{ord}(x) = 4$ y $\text{ord}(y) = 3$, pero no todo elemento de $\langle x, y\rangle$ es orden finito. Considere las matrices

$$xy = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{y} \quad yx = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix},$$

entonces

$$(xy)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \quad \text{y} \quad (yx)^n = \begin{pmatrix} 1 & 0 \\ -n & 1 \end{pmatrix}.$$

Ejemplo 4.6. En el grupo de los enteros $\mathbb{Z}$ determinar el subgrupo $\langle n, m\rangle$.

De acuerdo con el Teorema 4.3, se tiene

$$\langle n, m\rangle = \{nx + my \ : \ x, y \in \mathbb{Z}\}.$$

Siguiendo el procedimiento del Ejemplo 4.1 se tiene que

$$\langle n, m\rangle = \{nx + my \ : \ x, y \in \mathbb{Z}\} = \langle d\rangle$$

en el cual $d = \text{m.c.d}\{m, n\}$.

Ejemplo 4.7. En el grupo de los racionales $\mathbb{Q}$ determinar el subgrupo

$$\left\langle \frac{1}{2}, \frac{1}{3} \right\rangle.$$

Aplicando el Teorema 4.3, se tiene

$$\left\langle \frac{1}{2}, \frac{1}{3} \right\rangle = \left\{ \frac{x}{2} + \frac{y}{3} \ : \ x, y \in \mathbb{Z} \right\} = \left\{ \frac{3x + 2y}{6} \ : \ x, y \in \mathbb{Z} \right\}.$$

Sin embargo, puesto que m y n son primos relativos se tiene que $\langle 2, 3\rangle = \mathbb{Z}$, lo cual implica que

$$\left\langle \frac{1}{2}, \frac{1}{3} \right\rangle = \left\{ \frac{k}{6} \ : \ k \in \mathbb{Z} \right\}.$$

Ejemplo 4.8. Sea G un grupo en el cual existen elementos x y y tales que $\text{ord}(x) = n$, $\text{ord}(y) = 2$ y se cumple $xyx = y$. Probar que

$$\langle x, y\rangle = \{1, x, x^2, \ldots, x^{n-1}, y, xy, x^2y, \ldots, x^{n-1}y\}.$$

Sea $a \in \langle x, y\rangle$ tal que $a \notin \langle x\rangle \cup \langle y\rangle$. Según el Teorema 4.3

$$a = x^r y x^s b_1, \text{ para algunos } r, s \in \mathbb{Z} \text{ y algún } b_1 \in \langle x, y\rangle.$$

Observe que

$$yx^s = x^{-1}(xyx)x^{s-1} = x^{-1}yx^{s-1} = \cdots = x^{-s}(xyx) = x^{-s}y,$$

en consecuencia, $a = x^{r-s}yb_1$. Repitiendo este proceso en el factor yb_1, en una cantidad finita de pasos, se obtiene

$$a = x^k \quad \text{o} \quad a = x^k y, \text{ para algún } k \in \mathbb{Z}.$$

Ahora, por el algoritmo de la división existen enteros q y r tal que

$$k = nq + r, \text{ con } 0 \leq r < n,$$

entonces $x^k = x^{nq}x^r = x^r$. Así que

$$a = x^r \quad \text{o} \quad a = x^r y, \text{ con } 0 \leq r < n.$$

Ejemplo 4.9. Considerar el conjunto

$$H = \left\{ \begin{pmatrix} 1 & x & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \ : \ x, y \in \mathbb{Z} \right\}.$$

Probar que H es un grupo abeliano finitamente generado con la multiplicación usual de matrices.

Primero observe que si $x_1, x_2, y_1, y_2 \in \mathbb{Z}$ entonces

$$\begin{pmatrix} 1 & x_1 & y_1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x_2 & y_2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x_2 + x_1 & y_2 + y_1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x_2 & y_2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x_1 & y_1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

En consecuencia, la operación es cerrada y conmutativa. De la anterior igualdad también se evidencia que la operación definida en H es asociativa y tiene las propiedades del elemento neutro e inverso. Por tanto, H es un grupo abeliano.

Por otro lado, para $x, y, n \in \mathbb{Z}$, con $n > 0$, se tiene

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & nx & ny \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

de lo cual se concluye que H no puede ser cíclico. Ahora, si se consideran las matrices

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{y} \quad B = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

entonces para cada elemento $C = \begin{pmatrix} 1 & m & k \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in H$, se tiene $C = A^m B^k$. Por ejemplo, para la matriz

$$C = \begin{pmatrix} 1 & -2 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^2 \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^3 = \left(A^{-1}\right)^2 B^3 = A^{-2} B^3.$$

Por tanto, H es un grupo abeliano generado por las matrices A y B, esto es $H = \langle A, B \rangle$.

4.3 Ejercicios

1. Encontrar todos los generadores de $\mathbb{Z}_6$, $\mathbb{Z}_8$ y $\mathbb{Z}_{20}$.

2. Supongamos que $\langle a \rangle$, $\langle b \rangle$ y $\langle c \rangle$ son grupos cíclicos de órdenes 6, 8 y 20, respectivamente. Encontrar todos los generadores de $\langle a \rangle$, $\langle b \rangle$ y $\langle c \rangle$.

3. Enumerar todos los elementos de $\langle 3 \rangle$ y $\langle 15 \rangle$ en $\mathbb{Z}_{18}$.

4. Sea a un elemento de un grupo de orden 18. Enumerar todos los elementos de $\langle a^3 \rangle$ y $\langle a^{15} \rangle$.

5. Sea a un elemento de un grupo tal que $\text{ord}(a) = 15$. Calcular el orden de los siguientes elementos.

   a) a^3.

   b) a^6.

   c) a^4.

   d) a^8.

6. En $\mathbb{Z}_{24}$ determinar un generador para el subgrupo $\langle 21 \rangle \cap \langle 10 \rangle$.

7. Construir el diagrama de Hasse del subgrupo $\mathbb{Z}_{24}$.

8. Supongamos que a es un elemento de un grupo tal que $\text{ord}(a) = 24$, encontrar un generador para el subgrupo $\langle a^{21} \rangle \cap \langle a^{10} \rangle$.

9. ¿Cuál es un generador para el subgrupo $\langle a^m \rangle \cap \langle a^n \rangle$?

10. Supongamos que G es un grupo cíclico que tiene exactamente tres subgrupos: los triviales G y $\{e\}$, y un subgrupo de orden 7.

    a) ¿Qué se puede decir acerca de $|G|$?

    b) ¿Qué se puede decir si 7 es reemplazado por un número primo p?

11. Sea G un grupo en el cual existen elementos a y b tales que $\text{ord}(a) = 4$, $a^2 = b^2$ y $ba = a^3 b$. Probar que

$$\langle a, b \rangle = \{1, a, a^2, a^3, b, ab, a^2 b, a^3 b\}.$$

12. Según las condiciones del Ejemplo 4.8, si $\text{ord}(x) = 25$, simplificar el producto

$$x^{10} y x^{12} y x^9 y x^5 y x y.$$

13. En el grupo $\mathbb{Z}_{24}$ considerar los subgrupos $H_1 = \langle 10 \rangle$ y $H_2 = \langle 12 \rangle$. Determinar el mínimo subgrupo de G que contiene la unión $H_1 \cup H_2$.

14. Sea G un grupo y $H_1 = \langle a^n \rangle$ y $H_2 = \langle a^m \rangle$ subgrupos cíclicos de G. Determinar el subgrupo de G generado por $H_1 \cup H_2$.

CAPÍTULO 5

Subgrupos normales y grupo cociente

Uno de los conceptos más importantes en teoría de grupos es el de *subgrupo normal*. El estudio de los subgrupos normales de un grupo es relevante en el desarrollo de la teoría de Galois y en el estudio de la estructura de grupos en general. En un grupo abeliano todo subgrupo es normal pero, en general, esto no es cierto en grupos no abelianos, lo que dificulta el estudio estructural de esta clase de grupos; sin embargo, se conoce la estructura de los grupos finitos no abelianos en el que todo subgrupo es normal. Los subgrupos normales de un grupo permiten construir un nuevo grupo denominado *grupo cociente* por medio del cual se pueden obtener importantes propiedades del grupo original.

5.1 Clases laterales y Teorema de Lagrange

En el primer capítulo se estudiaron distintas clases de equivalencia, las cuales son de gran importancia en las matemáticas, dadas sus valiosas propiedades. Dos de las clases de equivalencia de mayor relevancia en álgebra abstracta son las que se originan a partir de un sugbrupo.

Proposición 5.1. Si G es un grupo y H un subgrupo de G, entonces la relación (a izquierda)

$$a\mathcal{R}_i b \text{ si y solo si } a^{-1}b \in H$$

es de equivalencia en G.

Demostración. Dado que H es un subgrupo de G, para cada $a \in G$, se tiene

$$a^{-1}a = 1 \in H,$$

en consecuencia $\mathcal{R}_i$ es reflexiva. Este mismo hecho implica que $b^{-1}a = (a^{-1}b)^{-1} \in H$ siempre y cuando $a^{-1}b \in H$. Del cual se obtiene que $\mathcal{R}_i$ es simétrica. Finalmente, si $a^{-1}b, b^{-1}c \in H$, entonces

$$(a^{-1}b)(b^{-1}c) = a^{-1}c \in H.$$

Por tanto, $\mathcal{R}_i$ es una relación de equivalencia. □

Recuerde que una relación de equivalencia definida en un conjunto no vacío permite particionar el conjunto en clases de equivalencia. En el caso particular de la relación $\mathcal{R}_i$ se tiene que para $a \in G$

$$[a] = \{x \in G \ : \ a\mathcal{R}_i x\} = \{x \in G \ : \ a^{-1}x \in H\}$$

y así

$$[a] = \{ah \ : \ h \in H\} = aH.$$

De igual manera que se definió la relación de equivalencia (a izquierda) $\mathcal{R}_i$ se define la relación (a derecha)

$$a\mathcal{R}_d b \text{ si y solo si } ab^{-1} \in H$$

la cual también es una relación de equivalencia. En este caso, se tiene que

$$[a] = \{x \in G \ : \ a\mathcal{R}_d x\} = \{x \in G \ : \ ax^{-1} \in H\}$$

y así

$$[a] = \{ha \ : \ h \in H\} = Ha.$$

Es importante tener claro que a pesar que $\mathcal{R}_i$ y $\mathcal{R}_d$ se definen de manera similar, las relaciones no necesariamente determinan la misma partición de G, como se evidencia en el siguiente ejemplo.

Ejemplo 5.1. Considerar el grupo $S_3 = \{\rho_0, \rho_1, \rho_2, \tau_1, \tau_2, \tau_3\}$ y el subgrupo cíclico

$H = \langle \tau_3 \rangle = \{\rho_0, \tau_3\}$, en el cual

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Determinar,

1. La tabla de Cayley de S_3.
2. Calcular las parejas de las relaciones de equivalencia $\mathcal{R}_i$ y $\mathcal{R}_d$.
3. Hallar las distintas clases de equivalencia para cada una de las relaciones $\mathcal{R}_i$ y $\mathcal{R}_d$.

Al realizar los distintos cálculos se tiene que la tabla de Cayley de S_3 es

$\circ$	ρ_0	ρ_1	ρ_2	τ_1	τ_2	τ_3
ρ_0	ρ_0	ρ_1	ρ_2	τ_1	τ_2	τ_3
ρ_1	ρ_1	ρ_2	ρ_0	τ_3	τ_1	τ_2
ρ_2	ρ_2	ρ_0	ρ_1	τ_2	τ_3	τ_1
τ_1	τ_1	τ_2	τ_3	ρ_0	ρ_1	ρ_2
τ_2	τ_2	τ_3	τ_1	ρ_2	ρ_0	ρ_1
τ_3	τ_3	τ_1	τ_2	ρ_1	ρ_2	ρ_0

De acuerdo con la tabla anterior se obtiene que

$$\mathcal{R}_i = \{(\rho_0, \rho_0), (\rho_1, \rho_1), (\rho_2, \rho_2), (\tau_1, \tau_1), (\tau_2, \tau_2), (\tau_3, \tau_3), (\rho_0, \tau_3), (\rho_1, \tau_2), (\rho_2, \tau_1), (\tau_1, \rho_2), (\tau_2, \rho_1), (\tau_3, \rho_0)\}$$

y

$$\mathcal{R}_d = \{(\rho_0, \rho_0), (\rho_1, \rho_1), (\rho_2, \rho_2), (\tau_1, \tau_1), (\tau_2, \tau_2), (\tau_3, \tau_3), (\rho_0, \tau_3), (\rho_1, \tau_1), (\rho_2, \tau_2), (\tau_1, \rho_1), (\tau_2, \rho_2), (\tau_3, \rho_0)\}$$

Por tanto,

$$\begin{aligned} \rho_0 H = \tau_3 H = \{\rho_0, \tau_3\} \quad & H\rho_0 = H\tau_3 = \{\rho_0, \tau_3\} \\ \rho_1 H = \tau_2 H = \{\rho_1, \tau_2\} \quad & H\rho_1 = H\tau_1 = \{\rho_1, \tau_1\} \\ \rho_2 H = \tau_1 H = \{\rho_2, \tau_1\} \quad & H\rho_2 = H\tau_2 = \{\rho_2, \tau_2\} \end{aligned}$$

Ejemplo 5.2. Considerar el grupo $G = \mathbb{Z}_9$ y el subgrupo $H = \langle 3 \rangle = \{0, 3, 9\}$. Deter-

minar las clases de equivalencia de $\mathcal{R}_i$ y $\mathcal{R}_d$.

Note que el grupo es abeliano, lo cual implica que $a + H = H + a$ para todo $a \in G$. Por lo cual, las dos relaciones determinan la misma partición, y así las distintas clases de equivalencia son:

$$\begin{aligned} 0 + H = 3 + H = 6 + H &= \{0, 3, 6\} \\ 1 + H = 4 + H = 7 + H &= \{1, 4, 7\} \\ 2 + H = 5 + H = 8 + H &= \{2, 5, 8\}. \end{aligned}$$

Observe que el hecho que el grupo G sea abeliano permite afirmar que $a + H = H + a$ para todo $a \in G$. Sin embargo, como se vio en el Ejemplo 5.1 esto no se cumple en general para grupos no abelianos.

Definición 5.1. Sean G un grupo y H un subgrupo de G. Entonces al conjunto aH se le denomina la clase lateral izquierda de H en G que contiene a a. De manera similar Ha es la clase lateral derecha de H en G que contiene a a. Al elemento a se le denomina un representante de la clase.

Ejemplo 5.3. Sea $G = GL(2, \mathbb{R})$ y $H = SL(2, \mathbb{R}) = \{h \in G \ : \det(h) = 1\}$. Probar que la clase lateral izquierda aH con $a \in GL(2, \mathbb{R})$ es

$$aH = \{x \in GL(2, \mathbb{R}) \ : \ \det(x) = \det(a)\}$$

Para $x = ah \in aH$ se tiene

$$\det(x) = \det(ah) = \det(a)\det(h) = \det(a).$$

Por otro lado, si $x \in G$ es tal que $\det(x) = \det(a)$, entonces para $h = a^{-1}x$ se cumple

$$\det(h) = \det(a^{-1}x) = \det(a^{-1})\det(x) = \frac{\det(x)}{\det(a)} = 1.$$

En consecuencia, $h \in H$ y así $x \in aH$.

Ejemplo 5.4. Describir como se particiona el grupo $G = \mathbb{R}^3$ de acuerdo con la relación de equivalencia definida por un plano H que pasa por el origen.

Observe que una traslación de un conjunto de puntos en el espacio está caracterizada por un vector fijo, en la cual cada punto del conjunto es transformado en un nuevo punto que se encuentra en la misma dirección del vector dado, y a una distancia igual a la magnitud del vector. En este sentido, la clase lateral $(a, b, c) + H$ es el plano paralelo a

H que pasa por el punto (a, b, c), por lo cual las clases laterales izquierdas (o derechas) particionan al espacio en planos paralelos al plano H.

Teorema 5.1. Si H es un subgrupo de G y $a, b \in G$, entonces

1. $a \in aH$.
2. $aH = H$ si y solo si $a \in H$.
3. $(ab)H = a(bH)$ y $H(ab) = (Ha)b$.
4. $aH = bH$ si y solo si $a \in bH$.
5. $aH = bH$ o $aH \cap bH = \emptyset$.
6. $aH = bH$ si y solo si $a^{-1}b \in H$.
7. $|aH| = |bH|$.
8. $aH = Ha$ si y solo si $H = aHa^{-1}$.
9. aH es un subgrupo de G si y solo si $a \in H$.

Demostración. El primer, segundo y tercer ítem son consecuencia de que $1 \in H$ y la operación de G es cerrada y asociativa en H. Las afirmaciones cuarta, quinta y sexta son consecuencias directa de que $\mathcal{R}_i$ es una relación de equivalencia. Para garantizar la séptima considere la función $f : aH \to bH$ dada por $f(ah) = bh$ con $h \in H$. Entonces la igualdad $bh_1 = bh_2$ con $h_1, h_2 \in H$ implica que $h_1 = h_2$ y así $ah_1 = ah_2$. Por otro lado, observe que para todo $h \in H$ se garantiza que $f(ah) = bh$. En consecuencia, la función f es biyectiva y así $|aH| = |bH|$. Además, note que

$$ah_1 = h_2a, \text{ con } h_1, h_2 \in H,$$

es equivalente a $h_2 = ah_1a^{-1}$, con lo cual se garantiza la octava propiedad.

Finalmente, si aH es un subgrupo de G, entonces $1 = ah$ para algún $h \in H$, del cual se obtiene que $a \in H$. En el otro sentido, si $a \in H$, entonces es claro que $aH = H$. □

Las propiedades descritas en el teorema anterior son también aplicables a las clases laterales derechas. Además, observe que las propiedades 2 y 7 del teorema anterior implican que todas las clases laterales izquierdas (o derechas) tiene la misma cardinalidad del subgrupo H. Este hecho tiene una consecuencia importante como es el Teorema de Lagrange.

Teorema 5.2 (Teorema de Lagrange)**.** Si G es un grupo finito y H un subgrupo de G, entonces el orden de H divide al orden del grupo G. Además, el número de clases laterales izquierdas (o derechas) es igual $\dfrac{|G|}{|H|}$.

Demostración. Dado que G es un grupo finito y la relación $\mathcal{R}_i$ es de equivalencia, existen

elementos $a_1, a_2, \ldots, a_m$ de G, tales que

$$G = a_1H \cup a_2H \cup \cdots \cup a_mH.$$

con $a_iH \cap a_jH = \emptyset$, siempre que $i \neq j$. Con lo cual se obtiene

$$|G| = |a_1H| + |a_2H| + \cdots + |a_mH| = m|H|.$$

□

Es importante observar que el Teorema de Lagrange implica que el orden de un subgrupo divide al orden del grupo. Note que el recíproco es verdadero en el caso de que el grupo G sea cíclico, como se establece en el Teorema 4.1. Sin embargo, en general es falso, como se establece en el Ejemplo 5.5.

Corolario 5.1. Si G es un grupo finito, H un subgrupo de G y $a \in G$, entonces
1. El orden de H divide al orden de G.
2. El orden de a divide al orden de G.
3. Si $|G| = p$ con p primo entonces G es cíclico.

Demostración. Las dos primeras afirmaciones son consecuencia directa del Teorema de Lagrange. Para el tercero suponga que $a \neq 1$, entonces por el segundo ítem $d = \text{ord}(a)$ divide a $|G| = p$. De alli se obtiene que $\text{ord}(a) = p$, y por tanto $G = \langle a \rangle$. □

Otra de las consecuencias del Teorema de Lagrange es que el número de clases laterales tanto izquierdas como derechas es el mismo. Por lo cual, la siguiente definición tiene sentido.

Definición 5.2. Sean G un grupo finito y H un subgrupo. Entonces al número de clases laterales (izquierdas o derechas) de H en G se denomina el índice de H en G y se denota por $[G : H]$.

Ejemplo 5.5. Probar que el grupo alternante A_4 no tiene subgrupos de orden 6.

Suponga que existe un subgrupo H de A_4 tal que $|H| = 6$. Entonces

$$[A_4 : H] = \frac{|A_4|}{|H|} = \frac{12}{6} = 2,$$

lo cual es equivalente a que existen únicamente dos clases laterales izquierdas (distintas) H y σH para alguna $\sigma \in A_4$. Observe que $H \cap H\sigma = \emptyset$; caso contrario, por el literal 2 del Teorema 5.1, se obtiene que $\sigma \in H$ llegando a una contradicción. Esto implica que las dos clases laterales derechas son H y $H\sigma$, y así $\sigma H = H\sigma$. Esta última igualdad es

equivalente a $H = \sigma H \sigma^{-1}$. Por otro lado, note que existen solamente 8 ciclos de longitud 3 dados por

$$\sigma_1 = (123) \qquad \sigma_3 = (134) \qquad \sigma_5 = (124) \qquad \sigma_7 = (234)$$

$$\sigma_2 = (132) \qquad \sigma_4 = (143) \qquad \sigma_6 = (142) \qquad \sigma_8 = (243)$$

Esto implica que al menos uno de los anteriores ciclos pertenece a H. Suponga sin pérdida de generalidad que $\sigma_1 = (123) \in H$. Entonces $\sigma_2 = \sigma_1^{-1} = (132) \in H$ y de igual manera los elementos

$$(124)(123)(124)^{-1} = (124)(123)(142) = (243)$$
$$(243)(123)(243)^{-1} = (243)(123)(234) = (142)$$

En consecuencia, la cardinalidad de H es mayor a 6, lo cual es una contradicción. Por tanto, A_4 no contiene subgrupos de orden 6.

Ejemplo 5.6. Sea K un subgrupo propio de H, y este a su vez es un subgrupo propio de G. Si $|K| = 42$ y $|G| = 420$, ¿cuáles son las posibilidades para el orden de H?

Por el Teorema de Lagrange se tiene que 42 debe ser un divisor positivo de $|H|$, y este su vez es un divisor positivo de $|G| = 420$. Sea $m = |H|$, entonces $m = 42k_1$ y $420 = mk_2$ con $k_1, k_2 > 1$ enteros positivos. Esto implica que $k_1 k_2 = 10$ y así $k_1, k_2 \in \{2, 5\}$. En consecuencia, las posibilidades para el orden de H son:

$$|H| = 84 \quad \text{y} \quad |H| = 210.$$

5.2 Subgrupos normales y grupo cociente

Según la sección anterior, en general las relaciones de equivalencia $\mathcal{R}_i$ y $\mathcal{R}_d$ no definen la misma partición como se evidenció en el Ejemplo 5.1. La pregunta que surge es ¿cuándo un subgrupo H de un grupo G define iguales particiones de acuerdo con las relaciones $\mathcal{R}_i$ y $\mathcal{R}_d$?

Definición 5.3. Un subgrupo H de un grupo G se denomina normal y se denota por $H \triangleleft G$ si $aH = Ha$ para todo $a \in G$.

Como se ha mencionado todos los subgrupos de un grupo abeliano son normales. En el caso general, los subgrupos triviales $H = \{1\}$ y $H = G$ son normales, así como el centro

del grupo

$$\mathcal{Z}(G) = \{x \in G \ : \ ax = xa \text{ para todo } a \in G\}.$$

Proposición 5.2. Un subgrupo H de un grupo G es normal si y solo si $aHa^{-1} \subseteq H$ para todo $a \in G$.

Demostración. Suponga que H es normal en G. Entonces el ítem 8 del Teorema 5.1 garantiza la afirmación. En el otro sentido, para $h \in H$ se tienen que los elementos aha^{-1} y $a^{-1}ha$ pertenecen a H. Por lo que, $h = a(a^{-1}ha)a^{-1} \in aHa^{-1}$, con lo cual se garantiza que $H \subseteq aHa^{-1}$ y así $aH = Ha$ para todo $a \in G$. □

Ejemplo 5.7. Mostrar que el subgrupo $H = SL(2, \mathbb{R})$ es normal de $G = GL(2, \mathbb{R})$.

Sean $a \in G$ y $h \in H$. Entonces

$$\det(aha^{-1}) = \det(a)\det(h)\det(a^{-1}) = \det(h) = 1,$$

de lo cual se obtiene que $aHa^{-1} \subseteq H$ para todo $a \in G$. Por tanto, $H \triangleleft G$.

Ejemplo 5.8. Sea G un grupo finito. Probar que si G tienen un único subgrupo H de orden d entonces H es normal en G.

Sea $a \in G$ y considere el conjunto $H' = aHa^{-1}$. Para $x = ah_1a^{-1}$ y $y = ah_2a^{-1}$ con $h_1, h_2 \in H$ se cumple

$$xy^{-1} = (ah_1a^{-1})(ah_2a^{-1})^{-1} = ah_1a^{-1}ah_2^{-1}a^{-1} = ah_1h_2^{-1}a^{-1} = ah_3a^{-1}$$

donde $h_3 = h_1h_2^{-1} \in H$. Por tanto, H' es un subgrupo de G de orden d y así $aHa^{-1} = H$.

Note que la solución del Ejemplo 5.5 se puede generalizar para cualquier grupo.

Proposición 5.3. Sean G un grupo y $H \leq G$. Si $[G : H] = 2$, entonces $H \triangleleft G$.

Demostración. Dado que $[G : H] = 2$ existen únicamente dos clases laterales izquierdas H y aH para algún $a \in G$. Por otro lado observe que $H \cap Ha = \emptyset$; caso contrario se obtiene $H = Ha$ y así $a \in H$, lo cual es imposible. Por tanto, las clases laterales derechas son H y Ha, de este modo se concluye que $aH = Ha$. En consecuencia, H es normal en G. □

Ejemplo 5.9. Probar las siguientes afirmaciones.

1. El subgrupo alternante A_n es normal de S_n.

2. El subgrupo cíclico $H = \langle \rho_1 \rangle$ es normal en D_n.

Note que los subgrupos alternante A_n y $H = \langle \rho_1 \rangle$ satisfacen

$$\frac{|S_n|}{|A_n|} = [S_n : A_n] = 2 = [D_n : H] = \frac{|D_n|}{|H|}.$$

Por tanto, según la Proposición 5.3 se tiene que A_n y H son subgrupos normales en S_n y D_n, respectivamente.

En el Ejercicio 16 del Capítulo 2, se solicita probar que el conjunto

$$HK = \{hk \ : \ h \in H, \ k \in K\}$$

es un subgrupo del grupo abeliano G si H y K son subgrupos. Sin embargo, esto no se satisface en general en el caso no abeliano, por ejemplo considerar en $G = S_3$ los subgrupos

$$H = \langle (12) \rangle = \{(1), (12)\} \quad \text{y} \quad K = \langle (23) \rangle = \{(1), (23)\}.$$

Entonces,

$$HK = \{(12), (23), (312)\}$$

el cual no es un subgrupo de S_3, ya que no contiene la permutación identidad de S_3. Sin embargo, si se imponen condiciones en uno de los subgrupos, entonces HK es un subgrupo de G.

Proposición 5.4. Si G es un grupo, $H \triangleleft G$ y $K \leq G$, entonces $HK \leq G$.

Demostración. Sean $x = h_1k_1$ y $y = h_2k_2$ elementos de HK. Entonces

$$xy^{-1} = h_1k_1k_2^{-1}h_2^{-1} = h_1\left(k_1k_2^{-1}h_2^{-1}k_2k_1^{-1}\right)k_1k_2^{-1},$$

pero $k_1k_2^{-1} \in K$ y dado que $H \triangleleft G$ se tiene $k_1k_2^{-1}h_2^{-1}k_2k_1^{-1} \in H$. Por tanto, $xy^{-1} \in HK$. □

Los subgrupos normales, aparte de generar iguales particiones del grupo, permiten definir en el conjunto de las clases laterales (izquierdas o derechas) una operación binaria y dotar a este conjunto de una estructura de grupo. Para un subgrupo normal H de G se tiene que

$$G/\mathcal{R}_i = G/\mathcal{R}_d$$

por lo cual el conjunto de clases laterales del subgrupo H se denotará simplemente por

$$G/H.$$

Además, de aquí en adelante cuando se considere un subgrupo normal H la clase lateral (izquierda o derecha) de $a \in G$ se denotará por $\overline{a}$.

Teorema 5.3. Si G es un grupo y H un subgrupo normal de G, entonces el conjunto cociente G/H tiene estructura de grupo con la operación

$$(aH)(bH) = (ab)H.$$

Demostración. Sean $a_1, a_2, b_1, b_2 \in G$ tales que $\overline{a_1} = \overline{a_2}$ y $\overline{b_1} = \overline{b_2}$. Entonces $a_1 \in a_2H$ y $b_1 \in b_2H$, lo cual es equivalente a que $a_1 = a_2h_1$ y $b_1 = b_2h_2$ con $h_1, h_2 \in H$, entonces

$$a_1b_1 = (a_2h_1)(b_2h_2) = a_2b_2(b_2^{-1}h_1b_2)h_2.$$

Dado que H es normal en G se tiene $(b_2^{-1}h_1b_2)h_2 \in H$. Por tanto, $\overline{a_1b_1} = \overline{a_2b_2}$ y esto implica que la operación está bien definida. Según como se define la operación, esta es asociativa puesto que la operación en el grupo G es asociativa. Además, el elemento neutro de la operación es la clase $\overline{1} = H$ y el elemento inverso de $\overline{a} = aH$ es la clase $\overline{a^{-1}} = a^{-1}H$. □

Ejemplo 5.10. Determinar las clases laterales del subgrupo $4\mathbb{Z}$ en $\mathbb{Z}$, y calcular su tabla de Cayley.

Primero note que $\overline{0} = 4\mathbb{Z} = \{4n \ : \ n \in \mathbb{Z}\}$. Entonces para $a, b \in \mathbb{Z}$ con $\overline{a} = \overline{b}$ se tiene que $a - b \in 4\mathbb{Z}$. En otras palabras $4 \mid (a-b)$ lo cual es equivalente a que a y b tienen igual residuo al dividirse por 4. Esto implica que existen solamente 4 clases laterales distintas dadas por

$$\mathbb{Z}/4\mathbb{Z} = \{4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}\} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}.$$

Por tanto, su tabla de Cayley es

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

En general, para el grupo $\mathbb{Z}$ y el subgrupo $n\mathbb{Z}$ con $n > 1$.

$$\mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + 4\mathbb{Z}\} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

Ejemplo 5.11. Sea $G = \mathbb{Z}_{18}$ y $H = \langle 6 \rangle$. Hallar el conjunto de clases laterales y calcular su tabla de Cayley.

Primero note que por el Teorema de Lagrange existen

$$[\mathbb{Z}_{18} : \langle 6 \rangle] = \frac{|\mathbb{Z}_{18}|}{|\langle 6 \rangle|} = \frac{18}{3} = 6$$

clases laterales distintas, las cuales son:

$$\overline{0} = 0 + \langle 6 \rangle = \{0, 6, 12\} \qquad \overline{3} = 3 + \langle 6 \rangle = \{3, 9, 15\}$$

$$\overline{1} = 1 + \langle 6 \rangle = \{1, 7, 13\} \qquad \overline{4} = 0 + \langle 6 \rangle = \{4, 10, 16\}$$

$$\overline{2} = 2 + \langle 6 \rangle = \{2, 8, 14\} \qquad \overline{5} = 0 + \langle 6 \rangle = \{5, 11, 17\}$$

Luego, su tabla de Cayley es:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

Ejemplo 5.12. Sea $G = U(32)$ y $H = U_{16}(32)$. Determinar el conjunto de clases laterales y calcular su tabla de Cayley.

Primero recuerde que

$$U(32) = \{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31\}$$

y

$$U_{16}(32) = \{x \in U(32) \ : \ (x \text{ mód } 16) = 1\} = \{1, 17\}.$$

El Teorema de Lagrange implica que el grupo cociente $U(32)/U_{16}(32)$ tiene 8 elementos dados por

$$\overline{1} = \{1, 17\} \qquad \overline{5} = \{5, 21\} \qquad \overline{9} = \{9, 25\} \qquad \overline{13} = \{13, 29\}$$

$$\overline{3} = \{3, 19\} \qquad \overline{7} = \{7, 23\} \qquad \overline{11} = \{11, 27\} \qquad \overline{15} = \{15, 31\}$$

Por tanto, la tabla de Cayley del grupo cociente es:

$*$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$	$\overline{9}$	$\overline{11}$	$\overline{13}$	$\overline{15}$
$\overline{1}$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$	$\overline{9}$	$\overline{11}$	$\overline{13}$	$\overline{15}$
$\overline{3}$	$\overline{3}$	$\overline{9}$	$\overline{15}$	$\overline{5}$	$\overline{11}$	$\overline{1}$	$\overline{7}$	$\overline{13}$
$\overline{5}$	$\overline{5}$	$\overline{15}$	$\overline{9}$	$\overline{3}$	$\overline{13}$	$\overline{7}$	$\overline{1}$	$\overline{11}$
$\overline{7}$	$\overline{7}$	$\overline{5}$	$\overline{3}$	$\overline{1}$	$\overline{15}$	$\overline{13}$	$\overline{11}$	$\overline{9}$
$\overline{9}$	$\overline{9}$	$\overline{11}$	$\overline{13}$	$\overline{15}$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
$\overline{11}$	$\overline{11}$	$\overline{1}$	$\overline{7}$	$\overline{13}$	$\overline{3}$	$\overline{1}$	$\overline{15}$	$\overline{5}$
$\overline{13}$	$\overline{13}$	$\overline{7}$	$\overline{1}$	$\overline{11}$	$\overline{5}$	$\overline{15}$	$\overline{9}$	$\overline{3}$
$\overline{15}$	$\overline{15}$	$\overline{13}$	$\overline{11}$	$\overline{9}$	$\overline{7}$	$\overline{5}$	$\overline{3}$	$\overline{1}$

5.3 Conjugados

Una relación de equivalencia de importancia en el estudio de la estructura de ciertos grupos es la relación de conjugación. A continuación se presenta un estudio introductorio de la conjugación, y sus implicaciones es el estudio de grupos finitos.

Definición 5.4. Sea G un grupo y sean a y b dos elementos de G. Se dice que b es un conjugado de a, denotado por $a \sim b$, si existe $g \in G$ tal que $b = gag^{-1}$.

Por ejemplo, según la Tabla de Cayley 5.1 para el grupo simétrico S_3, dos conjugados de la permutación $\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ son

$$\tau_2\tau_1\tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \\ 2 & 3 & 1 \\ 2 & 1 & 3 \end{pmatrix} = \tau_3 \quad \text{y} \quad \rho_1\tau_1\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 1 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \tau_2.$$

Proposición 5.5. Si G es un grupo, entonces la relación de conjugación es una relación de equivalencia en G.

Demostración. Sea $a, b, c \in G$. Observe que $a = 1a1$, así que $a \sim a$. Es decir, la relación de conjugación es reflexiva. Ahora, suponga que $a \sim b$, entonces existe $g \in G$ tal que $b = gag^{-1}$, luego

$$a = g^{-1}bg = g^{-1}b\left(g^{-1}\right)^{-1}, \text{ esto significa que } b \sim a.$$

En consecuencia, la relación de conjugación es simétrica. Finalmente, suponga que $a \sim b$

y $b \sim c$, entonces existen elementos $g, h \in G$ tal que $b = gag^{-1}$ y $c = hbh^{-1}$, entonces

$$c = h\left(gag^{-1}\right)h^{-1} = (hg)a\left(g^{-1}h^{-1}\right) = (hg)a(hg)^{-1}.$$

Por tanto, $a \sim c$, es decir, la relación de conjugación es transitiva. □

Proposición 5.6. Sean G un grupo y $a \in G$. Respecto de la relación de conjugación en G, se tiene $[a] = \{a\}$, si y sólo si, $a \in \mathcal{Z}(G)$.

Demostración. Observe que $[a] = \{gag^{-1} : g \in G\}$. Si $[a] = \{a\}$, se tiene

$$gag^{-1} = a, \text{ para toda } g \in G,$$

luego, $ga = ag$, para toda $g \in G$. Por tanto, $a \in \mathcal{Z}(G)$. El recíproco es consecuencia directa de la definición del centro del grupo G. □

Proposición 5.7. Si G es un grupo y a es un elemento de G, entonces el conjunto $G_a = \{g \in G : gag^{-1} = a\}$ es un subgrupo de G denominado subgrupo estacionario de a.

Demostración. Claramente $1 \in G_a$ y para $g, h \in G_a$ se tiene $gxg^{-1} = x = hxh^{-1}$, entonces

$$x = gxg^{-1} = g\left(hxh^{-1}\right)g^{-1} = (gh)x(gh)^{-1}$$

En consecuencia, $gh^{-1} \in G_a$ y se tiene que G_a es un subgrupo de G. □

Proposición 5.8. Sea G un grupo y sea $a \in G$. Respecto de la relación de conjugación se tiene

1. Para cada $b \in [a]$ existe $g \in G$, tal que $G_b = gG_ag^{-1} = \left\{ghg^{-1} : h \in G_a\right\}$.
2. Si G es finito, entonces $|[a]| = \dfrac{|G|}{|G_a|}$.

Demostración. Para probar el ítem 1 sea $b \in [a]$, entonces existe $g \in G$ tal que $b = gag^{-1}$. Ahora, dado $x \in G_b$ se tiene $xbx^{-1} = b$, entonces

$$a = g^{-1}bg = \left(g^{-1}x\right)b\left(x^{-1}g\right) = \left(g^{-1}xg\right)a\left(g^{-1}x^{-1}g\right) = \left(g^{-1}xg\right)a\left(g^{-1}xg\right)^{-1},$$

luego, $g^{-1}xg = h$, para alguna $h \in G_a$. En consecuencia, $x = ghg^{-1} \in gG_ag^{-1}$ y se tiene la contenencia $G_b \subseteq gG_ag^{-1}$. La contenencia $gG_ag^{-1} \subseteq G_b$ se justifica de forma similar y se deja como ejercicio para el lector.

Ahora, recuerde que el conjunto $\mathcal{A} = \{xG_a : x \in G\}$ de clases laterales izquierdas módulo el subgrupo G_a es una partición del grupo G, y para el caso en que G es finito satisface $|\mathcal{A}| = \dfrac{|G|}{|G_a|}$. Entonces se puede probar el ítem 2 mostrando que $|\mathcal{A}| = |G_a|$. Para esto considere la función

$$f : [a] = \{xax^{-1} : x \in G\} \longrightarrow \mathcal{A}, \quad \text{definida por } f(xax^{-1}) = xG_a.$$

Note que f es claramente sobreyectiva. Ahora, para garantizar que f es inyectiva considere $xax^{-1}, yay^{-1} \in G_a$, tal que $f(xax^{-1}) = f(yay^{-1})$, entonces $xG_a = yG_a$. Así que $y^{-1}x \in G_a$, y en consecuencia

$$\left(y^{-1}x\right) a \left(y^{-1}x\right)^{-1} = a,$$

de aquí se obtiene $xax^{-1} = yay^{-1}$. Por tanto f es biyectiva y la prueba está completa. □

Teorema 5.4. Sea p un número primo. Si G es un grupo finito de orden p^n, para algún $n \in \mathbb{Z}^+$, entonces $\mathcal{Z}(G) \neq \{1\}$.

Demostración. Para el caso en que G es abeliano, se tiene $\mathcal{Z}(G) = G \neq \{1\}$. Ahora, si G no es abeliano sea $\mathcal{Z}(G) = \{a_1, \ldots, a_k\}$. Dado que p es primo, el teorema de Lagrange garantiza que $k = p^m$, en el que $0 \leq m < n$. Considerando la relación de conjugación se conoce que

$$[a_i] = \{a_i\}, \text{ para } i = 1, \ldots, k.$$

Dado que $k < |G|$, deben existir clases de equivalencia $[b_1], \ldots, [b_r]$, tal que $\left|[b_j]\right| > 1$ y $[a_1], \ldots, [a_k], [b_1], \ldots, [b_r]$ es la partición de G inducida por la relación de conjugación. Entonces

$$G = (\{a_1\} \cup \cdots \cup \{a_k\}) \cup ([b_1] \cup \cdots \cup [b_r]) = \mathcal{Z}(G) \cup ([b_1] \cup \cdots \cup [b_r]).$$

Por el ítem 2 de la proposición 5.8 se concluye que para cada $j = 1, \ldots, r$ existe un entero positivo t_j tal que $\left|[b_j]\right| = p^{t_j}$, en consecuencia

$$|G| = |\mathcal{Z}(G)| + \sum_{j=1}^{r} \left|[b_j]\right|,$$

así que

$$|\mathcal{Z}(G)| = p^n - \sum_{j=1}^{r} p^{t_j} = p\left(p^{n-1} - \sum_{j=1}^{r} p^{t_j - 1}\right)$$

en el que n y los t_j son enteros positivos. Entonces p es un divisor de $|\mathcal{Z}(G)|$, por tanto $\mathcal{Z}(G) \neq \{1\}$. □

Para terminar esta sección se presenta el teorema de estructura para grupos de orden p^2, en el cual p es un número primo.

Teorema 5.5. Si p es un número primo, entonces todo grupo de orden p^2 es abeliano.

Demostración. Por contradicción suponga que existe un grupo no abeliano G de orden p^2. Por el teorema 5.4, $\mathcal{Z} \neq \{1\}$, y de aquí se debe tener $|\mathcal{Z}(G)| = p$. En consecuencia debe existir un elemento no central $a \in G$. Considere el subgrupo estacionario

$$C_a = \{g \in G : gag^{-1} = a\} = \{g \in G : ga = ag\},$$

observe que $a \in C_a$ y $\mathcal{Z}(G) \subseteq C_a$, entonces $|G_a| > p$ y por el teorema de Lagrange se obtiene que $|G_a| = p^2$. Así que $G_a = G$, es decir, $a \in \mathcal{Z}(G)$, lo que es una contradicción. Por tanto todo grupo de orden p^2 es abeliano. □

5.4 Ejercicios

1. Sea $H = \langle \rho_1 \rangle$ el subgrupo cíclico de D_4. Calcular todos los conjuntos $\sigma H \sigma^{-1}$ para $\sigma \in S_4$.

2. Sea $H = 3\mathbb{Z}$. Determinar todas las clases laterales de H en $\mathbb{Z}$.

3. Determinar todas las clases laterales izquierdas de $H = \{1, 11\}$ en U(30).

4. Sea $a \in G$, tal que $\text{ord}(a) = 30$. ¿Cuántas clases laterales izquierdas existen de $\langle a^4 \rangle$ en $\langle a \rangle$?. Listar todas las clases.

5. Sean H y K subgrupos de un grupo G. Probar que HK es un subgrupo de G si y solo si $HK = KH$.

6. Sean H y K dos subgrupos finitos de un grupo G, considerar el conjunto $HK = \{hk \ : \ h \in H, \ k \in K\}$. Probar que

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

7. Sean $a, b \in G$ y H y K subgrupos de G. Probar que si $aH = bK$, entonces $H = K$.

8. Sean H y K subgrupos de G. Probar que $g(H \cap K) = gH \cap gK$ con $g \in G$.

9. Sea H un subgrupo de $\mathbb{R}^*$. Probar que si $\mathbb{R}^+ \subseteq H \subseteq \mathbb{R}^*$, entonces $H = \mathbb{R}^+$ o $H = \mathbb{R}^*$.

10. Sea $\mathbb{C}^*$ el grupo de los números complejos no cero con la multiplicación y $H = \{a + ib \in \mathbb{C}^* \ : \ a^2 + b^2 = 1\}$. Dar una descripción geométrica de la clase lateral $(3 + 4i)H$.

11. Sea $H = \{(1), (12)\}$. Determinar si H es normal en S_3.

12. Sea
$$H = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \ : \ a, b, c \in \mathbb{R}, \ ac \neq 0 \right\}$$
¿Es H un subgrupo normal de $GL(2, \mathbb{R})$?

13. Sea $G = GL(2, \mathbb{R})$ y K un subgrupo de $\mathbb{R}^*$. Probar que
$$H = \{A \in G \ : \ \det(A) \in K\}$$
es un subgrupo normal de G.

14. Considerar el subgrupo $H = \{(1), (12)(34)\}$ de A_4. Probar que H no es normal en A_4.

15. Determinar todos los subgrupos normales de D_{12} de orden 2.

16. Sea $H = \{(1), (12)\}$. Determinar si H es normal en S_3.

17. Sea
$$H = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \ : \ a, b, c \in \mathbb{R}, \ ac \neq 0 \right\}$$
¿Es H un subgrupo normal de $GL(2, \mathbb{R})$?

18. Sea $G = GL(2, \mathbb{R})$ y K un subgrupo de $\mathbb{R}^*$. Probar que
$$H = \{A \in G \ : \ \det(A) \in K\}$$
es un subgrupo normal de G.

19. Sea G un grupo y suponga que G contiene un subgrupo de orden d. Mostrar que la intersección de todos los subgrupos normales de G de orden d es también un subgrupo normal de G.

20. Sean $\langle 3\rangle$ y $\langle 12\rangle$ subgrupos de $\mathbb{Z}$. Determinar la tabla de Cayley de $\langle 3\rangle/\langle 12\rangle$.

21. Sean $\langle 8\rangle$ y $\langle 48\rangle$ subgrupos de $\mathbb{Z}$. Determinar la tabla de Cayley de $\langle 8\rangle/\langle 48\rangle$.

22. Probar que el grupo factor de un grupo cíclico es cíclico.

23. Probar que el grupo factor de un grupo abeliano es abeliano.

24. ¿Cuál es el orden del elemento $14 + \langle 8\rangle$ en el grupo factor $\mathbb{Z}_{24}/\langle 8\rangle$.

25. Determinar los elementos del grupo factor $U(20)/U_5(20)$.

CAPÍTULO 6

Homomorfismos e isomorfismos

En la teoría de grupos un *homomorfismo* es una función que preserva la estructura de grupo. Esto permite transferir algunas propiedades del dominio al codominio y viceversa. En particular los homomorfismos biyectivos o isomorfismos establecen que los dos grupos son estructuralmente idénticos. En este capítulo se exponen las definiciones y resultados más importantes del estudio de los homomorfismos de grupos.

6.1 Homomorfismos de grupos

Como se ha visto en secciones anteriores, existen grupos que tienen propiedades en común como puede ser cíclico, el orden, abeliano, etc. Por ejemplo, si consideramos el subgrupo $H = \langle \rho_1 \rangle$ de D_4 se puede ver que tiene propiedades en común con el subgrupo $H_1 = \langle 2 \rangle$ del grupo $\mathbb{Z}_8$, y estos dos a su vez con el grupo $\mathbb{Z}_4$. En esta sección se estudia un tipo especial de función entre grupos, denominada *homomorfismo*, con el fin de estudiar propiedades en común entre un par de grupos.

Definición 6.1. Un homomorfismo ϕ de un grupo $\langle G, * \rangle$ a otro $\langle G', *' \rangle$ es una función que satisface

$$\phi(a * b) = \phi(a) *' \phi(b)$$

para todo $a, b \in G$.

En adelante, la condición expuesta en la definición anterior se escribirá simplemente por

$$\phi(ab) = \phi(a)\phi(b)$$

siempre y cuando se tengan en cuenta las operaciones binarias definidas en cada uno de los grupos G y G'. Observe que si se tienen dos homomorfismos de grupos $\phi : G \longrightarrow G'$ y $\psi : G' \longrightarrow G''$, entonces la composición $\psi\phi : G \longrightarrow G''$ es de nuevo un homomorfismo del grupo G en el grupo G''.

Definición 6.2. Sea ϕ un homomorfismo de G en G'. Entonces el kernel de ϕ se denota por $\mathrm{Ker}(\phi)$ y es el conjunto dado por

$$\mathrm{Ker}(\phi) = \{x \in G \ : \ \phi(x) = 1'\}.$$

En distintas áreas de las matemáticas se encuentran homomorfismos; un ejemplo básico es la función $\mod : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ la que asigna a cada entero su residuo módulo n. Observe que en este caso el kernel es el conjunto de todos los múltiplos de n. Por otro lado, la función valor absoluto cumple con la propiedad que $|nm| = |n||m|$, lo cual implica que la función $|\ | : \mathbb{R}^* \longrightarrow \mathbb{R}^*$ es un homomorfismo de grupos en el que su kernel está conformado por -1 y 1. Otros ejemplos involucran la función exponencial $f(x) = e^x$ o la función logaritmo $g(x) = \ln x$, ejemplos más sofisticados involucran la valuación p-ádica de un entero no cero o el símbolo de Legendre, para estos ejemplos ver la Sección 6.3.

Ejemplo 6.1. Mostrar que la función

$$\det : GL(2, \mathbb{R}) \longrightarrow \mathbb{R}^*$$

es un homomorfismo de grupos y describir su kernel.

Primero tenga en cuenta que la operación binaria en el grupo $GL(2, \mathbb{R})$ es la multiplicación de matrices y la operación en el grupo $\mathbb{R}^*$ es la multiplicación de reales. Entonces la propiedad

$$\det(AB) = \det(A)\det(B)$$

para $A, B \in GL(2, \mathbb{R})$ garantiza que la función dada es un homomorfismo de grupos. En este sentido se tiene que

$$\mathrm{Ker}(\det) = \{A \in GL(2, \mathbb{R}) \ : \ \det(A) = 1\} = SL(2, \mathbb{R}).$$

Ejemplo 6.2. Mostrar que la función

$$\frac{d}{dx} : \mathbb{R}[x] \longrightarrow \mathbb{R}[x]$$

en la cual $\mathbb{R}[x]$ representa todos los polinomios con coeficientes en los reales en la indeterminada x es un homomorfismo de grupos y describir su kernel.

La operación binaria del grupo $\mathbb{R}[x]$ es la suma de polinomios. De manera similar que en el ejemplo anterior la propiedad de la derivada de la suma de dos funciones dada por

$$\frac{d}{dx}(p(x) + q(x)) = \frac{d}{dx}p(x) + \frac{d}{dx}q(x)$$

implica que la función es un homomorfismo de grupos. Además, como se conoce que

$$\frac{d}{dx}k = 0$$

para toda constante $k \in \mathbb{R}$ se obtiene que

$$\text{Ker}\left(\frac{d}{dx}\right) = \mathbb{R}.$$

Ejemplo 6.3. Mostrar que la función $\phi : \mathbb{R} \longrightarrow SO(2)$ dada por

$$\phi(t) = \begin{pmatrix} \cos(t) & -\sin(t) \\ \sin(t) & \cos(t) \end{pmatrix}$$

es un homomorfismo de grupos y describir su kernel.

Recuerde que en el grupo

$$SO(2) = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \ : \ a, b \in \mathbb{R}, \ a^2 + b^2 = 1 \right\}$$

su operación binaria es la multiplicación de matrices. Por otro lado, para $t_1, t_2 \in \mathbb{R}$ se cumple

$$\begin{aligned} \cos(t_1 + t_2) &= \cos(t_1)\cos(t_2) - \sin(t_1)\sin(t_2) \\ \sin(t_1 + t_2) &= \sin(t_1)\cos(t_2) + \cos(t_1)\sin(t_2) \end{aligned}$$

Por tanto,

$$\begin{aligned}\phi(t_1+t_2) &= \begin{pmatrix}\cos(t_1+t_2) & -\sin(t_1+t_2)\\ \sin(t_1+t_2) & \cos(t_1+t_2)\end{pmatrix}\\ &= \begin{pmatrix}\cos(t_1) & -\sin(t_1)\\ \sin(t_1) & \cos(t_1)\end{pmatrix}\begin{pmatrix}\cos(t_2) & -\sin(t_2)\\ \sin(t_2) & \cos(t_2)\end{pmatrix}\\ &= \phi(t_1)\phi(t_2).\end{aligned}$$

Además, se tiene que

$$\begin{aligned}\mathrm{Ker}(\phi) &= \left\{ t\in\mathbb{R} \ : \ \begin{pmatrix}\cos(t) & -\sin(t)\\ \sin(t) & \cos(t)\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\right\}\\ &= \{2\pi k \ : \ k\in\mathbb{Z}\}.\end{aligned}$$

La condición en la Definición 6.1 establece que un homomorfismo preserva la operación en el segundo grupo, lo cual implica que propiedades del primer grupo se conserven en el segundo como se puede evidenciar en el siguiente teorema.

Teorema 6.1. Si ϕ es un homomorfismo de un grupo G en G', entonces
1. $\phi(1) = 1'$.
2. $\phi(g^n) = \phi(g)^n$ para todo $g \in G$ y todo $n \in \mathbb{Z}$.
3. Si $\mathrm{ord}(g)$ es finito, entonces $\mathrm{ord}(\phi(g))$ divide a $\mathrm{ord}(g)$.
4. $\mathrm{Ker}(\phi)$ es un subgrupo normal de G.
5. $\phi(a) = \phi(b)$ si y solo si $ab^{-1} \in \mathrm{Ker}(\phi)$.
6. Si $\phi(g) = g'$, entonces

$$\phi^{-1}(g') = \{x \in G \ : \ \phi(x) = g'\} = g\mathrm{Ker}(\phi).$$

Demostración. Según la definición de homomorfismo se tiene que

$$1'\phi(1) = \phi(1\cdot 1) = \phi(1)\phi(1)$$

y por las leyes cancelativas se sigue que $\phi(1) = 1'$. Para el segundo ítem, note que la igualdad es clara para $n = 0$. Para un entero positivo n, suponga que la igualdad $\phi(g^{n-1}) = \phi(g)^{n-1}$ se cumple. De allí se obtiene que

$$\phi(g^n) = \phi(g^{n-1}g) = \phi(g^{n-1})\phi(g) = \phi(g)^{n-1}\phi(g) = \phi(g)^n.$$

En el caso que n sea un entero negativo la prueba es similar.

Suponga ahora que $m = \mathrm{ord}(g)$. Entonces por el ítem 2 se obtiene que

$$\phi(g)^m = \phi(g^m) = \phi(1) = 1'.$$

Luego, de acuerdo con la Proposición 4.1, el ord($\phi(g)$) divide a $m = \text{ord}(g)$.

Para el ítem 4 sean $a, b \in \text{Ker}(\phi)$, entonces

$$\phi(ab^{-1}) = \phi(a)\phi(b)^{-1} = 1'1' = 1'$$

lo cual implica que $ab^{-1} \in \text{Ker}(\phi)$ y así el kernel del homomorfismo ϕ es un subgrupo de G. Además, para $x \in G$ se tiene

$$\phi(xax^{-1}) = \phi(x)\phi(a)\phi(x^{-1}) = \phi(x)1'\phi(x^{-1}) = \phi(xx^{-1}) = \phi(1) = 1'.$$

Por tanto $xax^{-1} \in Ker(\phi)$, en consecuencia, $Ker(\phi) \triangleleft G$.

Por otro lado, note que la igualdad $\phi(a) = \phi(b)$ es equivalente a

$$1' = \phi(a)\phi(b)^{-1} = \phi(a)\phi(b^{-1}) = \phi(ab^{-1}),$$

y en consecuencia, $ab^{-1} \in \text{Ker}(\phi)$.

Finalmente, para $x \in \phi^{-1}(g)$ considere el elemento $h = g^{-1}x$. Entonces

$$\phi(h) = \phi(g^{-1}x) = \phi(g)^{-1}\phi(x) = (g')^{-1}g' = 1'$$

y así $h \in \text{Ker}(\phi)$. Por tanto, $x = gh \in g\text{Ker}(\phi)$. En el otro sentido si $x = gh$ para algún $h \in \text{Ker}(\phi)$, entonces

$$\phi(x) = \phi(gh) = \phi(g)\phi(h) = g'1' = g'$$

es decir $x \in \phi(g')^{-1}$. □

Ejemplo 6.4. Sea $\phi : \mathbb{Z}_{50} \longrightarrow \mathbb{Z}_{15}$ un homomorfismo en el cual $\phi(7) = 6$. Determinar la imagen del homomorfismo, el kernel de ϕ y $\phi^{-1}(6)$.

De acuerdo con la propiedad 2 del Teorema 6.1 se tiene que

$$\phi(7) = \phi(7 \cdot 1) = 7\phi(1) = 6$$

de lo cual se obtiene que $\phi(1) = 3$. Es importante anotar que este homomorfismo es único, puesto que la congruencia $7x \equiv 6(\text{mód } 15)$ tiene solución única. En consecuencia, $\phi(x) = 3x$ para todo $x \in \mathbb{Z}_{50}$ y así

$$\phi(\mathbb{Z}_{50}) = \{0, 3, 6, 9, 12\} \quad \text{y} \quad \text{Ker}(\phi) = \{0, 5, 10, 15, 20, 25, 30, 35, 40, 45\}.$$

Luego, aplicando la propiedad 6 del Teorema 6.1 se obtiene

$$\phi^{-1}(6) = 7 + \text{Ker}(\phi) = \{2, 7, 12, 17, 22, 27, 32, 37, 42, 47\}.$$

Ejemplo 6.5. Determinar todos los homomorfismos del grupo $\mathbb{Z}_8$ en el grupo $\mathbb{Z}_{20}$.

Primero note que si $x \in \mathbb{Z}_8$, entonces

$$\phi(x) = \phi(\underbrace{1+1+\cdots+1}_{x-\text{veces}}) = \underbrace{\phi(1)+\phi(1)+\cdots+\phi(1)}_{x-\text{veces}} = x\phi(1).$$

Por tanto, el homomorfismo está determinado por la imagen del generador 1 del grupo $\mathbb{Z}_8$. Por otro lado, según el ítem 3 del Teorema 6.1, se tiene que

$$\operatorname{ord}\phi(1) \in \{1,2,4,8\} \quad \text{y} \quad \operatorname{ord}\phi(1) \in \{1,2,4,5,10,20\}.$$

Aplicando el Teorema 4.2, se obtiene que

1. Si $\operatorname{ord}\phi(1) = 1$, entonces $\phi(1) = 0$.
2. Si $\operatorname{ord}\phi(1) = 2$, entonces $\phi(1) = 10$.
3. Si $\operatorname{ord}\phi(1) = 4$, entonces $\phi(1) = 5, 15$.

En consecuencia, existen 4 homomorfismos del grupo $\mathbb{Z}_8$ en el grupo $\mathbb{Z}_{20}$.

En general, es posible clasificar aquellas funciones $\phi : \mathbb{Z}_n \longrightarrow \mathbb{Z}_m$ las cuales son homomorfismos de grupos, ver el ejercicio 4 de la Sección 6.3.

Ejemplo 6.6. Considerar la función $\phi : \mathbb{R}[x] \longrightarrow \mathbb{R}$ dada por $\phi(p(x)) = p(0)$. Probar que ϕ es un homomorfismo y determinar su imagen, el kernel y $\phi^{-1}(1)$.

Sean $p(x), q(x) \in \mathbb{R}[x]$. Entonces se cumple que $(p+q)(0) = p(0) + q(0)$, y así $\phi(p(x)+q(x)) = \phi(p(x)) + \phi(q(x))$, lo cual prueba que ϕ es un homomorfismo. Note que para todo $a \in \mathbb{R}$ el polinomio $p(x) = x + a$ satisface la igualdad $\phi(p(x)) = a$. Por tanto, ϕ es una función sobreyectiva y así la imagen de ϕ es el conjunto de los números reales.

Por otro lado, si $p(x)$ es tal que $\phi(p(x)) = p(0) = 0$, entonces el término constante del polinomio debe ser igual a cero. Esto conduce a que

$$\operatorname{Ker}(\phi) = \{xq(x) \ : \ q(x) \in \mathbb{R}[x]\}.$$

Finalmente, como $\phi(x+1) = 1$ se sigue que

$$\phi^{-1}(1) = (x+1) + \operatorname{Ker}(\phi) = \{xq(x)+1 \ : \ q(x) \in \mathbb{R}[x]\}.$$

El Ejemplo 6.5 es un caso que se puede generalizar para grupos cíclicos.

El Teorema 6.1 evidencia que existe una relación muy estrecha entre las propiedades del primer grupo y las segundo grupo. Como por ejemplo si $\phi : G \longrightarrow G'$ es un homomorfismo de grupos y G es cíclico (o abeliano), entonces la imagen de ϕ es un subgrupo cíclico (o abeliano) de G'. A continuación se presenta una serie de consecuencias del Teorema anterior.

Corolario 6.1. Si $\phi : G \longrightarrow G'$ es un homomorfismo de grupos, entonces
1. Si $H \leq G$, entonces $\phi(H) \leq G'$.
2. Si $H \lhd G$, entonces $\phi(H) \lhd \phi(G)$.
3. Si $|H| = n$, entonces $|\phi(H)|$ divide a n.
4. Si $K' \leq G'$, entonces $\phi^{-1}(K') \leq G$.
5. Si $K' \lhd G'$, entonces $\phi^{-1}(K') \lhd G$.
6. $\text{Ker}(\phi) = \{1\}$ si y solo si ϕ es inyectiva.

Demostración. Sean $\phi(a), \phi(b) \in \phi(H)$. Entonces

$$\phi(a)\phi(b)^{-1} = \phi(a)\phi(b^{-1}) = \phi(ab^{-1}).$$

Dado que $a, b \in H$ se tiene que $ab^{-1} \in H$. Esto implica que $\phi(ab^{-1}) \in \phi(H)$ y por tanto $\phi(H) \leq G'$.

Para el segundo ítem primero note que la imagen $\phi(G)$ es un subgrupo de G'. Sean $\phi(g) \in \phi(G)$ y $\phi(h) \in \phi(H)$, entonces

$$\phi(g)\phi(h)\phi(g)^{-1} = \phi(ghg^{-1}),$$

pero del hecho que $H \lhd G$ se obtiene que $ghg^{-1} \in H$ y así su imagen es un elemento de $\phi(H)$ lo cual prueba la normalidad de $\phi(H)$ en $\phi(G)$.

Para el ítem 3 considere el homomorfismo ϕ_H dado por la restricción de ϕ al subgrupo H. Entonces se tiene que $\text{Ker}(\phi_H) = H \cap \text{Ker}(\phi)$. Suponga que $|H| = n$, $\phi(H) = \{h'_1, h'_2, \ldots, h'_m\}$ y $|\text{Ker}(\phi_H)| = k$. Entonces la propiedad 6 del Teorema 6.1 implica que

$$n = |H| = \left| \bigcup_{i=1}^{m} \phi_H^{-1}(h'_i) \right| = \sum_{i=1}^{m} |\phi_H^{-1}(h'_i)| = \sum_{i=1}^{m} k = mk.$$

En consecuencia, $m = |\phi(H)|$ divide a $n = |H|$. La prueba de los ítems 4 y 5 se dejan como ejercicio al lector.

Finalmente, si se tiene que $\text{Ker}(\phi) = \{1\}$, entonces la igualdad $\phi(a) = \phi(b)$ implica que $ab^{-1} = 1$ y así $a = b$, es decir la función ϕ es inyectiva. En el otro sentido, si ϕ es inyectiva y $\phi(a) = \phi(1)$, entonces $a = 1$ con lo cual se prueba el hecho que

$\text{Ker}(\phi) = \{1\}$. □

Dado que el kernel de un homomorfismo $\phi : G \longrightarrow G'$ es un subgrupo normal de G, entonces el conjunto formado por todas las clases laterales del kernel de ϕ tiene estructura de grupo. Esto es,

$$G/\text{Ker}(\phi) = \{a\text{Ker}(\phi) \ : \ a \in G\}$$

es un grupo con la multiplicación de clases laterales. El siguiente corolario prueba que la implicación es realmente una equivalencia.

Corolario 6.2. Si H es un subgrupo normal de un grupo G, entonces existe un homomorfismo de grupos en el que H es su kernel.

Demostración. Como $H \triangleleft G$ el conjunto de todas las clases laterales G/H tiene estructura de grupo. Entonces considere la aplicación canónica

$$\pi : G \longrightarrow G/H$$

dada por $\pi(a) = aH$. Según el Teorema 5.3 se cumple

$$\pi(ab) = (ab)H = (aH)(bH) = \pi(a)\pi(b),$$

lo cual es equivalente a que π es un homomorfismo, en el que $\text{Ker}(\pi) = H$. □

6.2 Isomorfismos de grupos

Uno de los grandes problemas en el Teoría de Grupos es la clasficación de todos los grupos finitos (o infinitos). Es decir, dado un entero positivo n determinar todos los grupos finitos de orden n. En este sentido, es importante no tener en cuenta aquellos grupos que se denominan *isomorfos*, esto es aquellos grupos que tienen un comportamiento igual, pero en forma son distintos. Por ejemplo, de todos los grupos cíclicos de orden n solo se tiene en cuenta al grupo $\mathbb{Z}_n$.

Definición 6.3. Sean $\langle G, * \rangle$ y $\langle G', *' \rangle$ dos grupos. Un isomorfismo entre los grupos G y G' es una función biyectiva ϕ, tal que

$$\phi(a * b) = \phi(a) *' \phi(b)$$

para todo $a, b \in G$. En este caso se dice que los grupos G y G' son isomorfos y se denota por $G \cong G'$.

Note que básicamente un isomorfismo es un homomorfismo cuya función es biyectiva. Cuando dos grupos son isomorfos ellos tienen las mismas características o propiedades, sin embargo en forma sus elementos son distintos.

Ejemplo 6.7. Sea $G = \{e, a, b\}$ un grupo de orden 3. Construya la tabla de Cayley de G y muestre que G es isomorfo a $\mathbb{Z}_3$.

En la tabla de Cayley de G se conoce tanto la primera fila como la primera columna ya que e es el elemento neutro del grupo. Ahora bien, si $a^2 = e$ se obtiene que $ab = b$ y así $a = e$, lo cual es una contradicción. Por tanto, $a^2 = b$ y $ab = e$, y su tabla de Cayley hasta el momento es la siguiente

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b		

Por otro lado, si $ba = a$ se llega a que $b = e$ lo cual es imposible. De este modo, $ba = e$ y así $b^2 = a$. En consecuencia, la tabla de Cayley de un grupo de orden 3 es

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Finalmente, la Figura 6.1 permite hacer una comparación de las tablas de Cayley de los grupos G y $\mathbb{Z}_3$ y concluir que la función $\phi : G \longrightarrow \mathbb{Z}_3$ dada por $\phi(e) = 0$, $\phi(a) = 1$ y $\phi(b) = 2$ es un isomorfismo de grupos.

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

(a) Tabla de Cayley grupo orden 3

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

(b) Tabla Cayley $\mathbb{Z}_3$

Figura 6.1: Comparación tablas de Cayley de G y $\mathbb{Z}_3$

El ejemplo anterior muestra que existe un único grupo de orden 3 salvo isomorfismo. Es decir, que entre todos los grupos de orden 3 solo se estudian aquellos que no son isomorfos y en este caso existe uno solo. Sin embargo, como se estudiará en el siguiente capítulo existen únicamente dos grupos de orden 4 salvo isomorfismo.

Ejemplo 6.8. Mostrar que los grupos $\mathbb{R}$ con la adición y $\mathbb{R}^+$ con la multiplicación son isomorfos mediante la función $\phi(x) = 2^x$.

Primero note que para $x_1, x_2 \in \mathbb{R}$ se cumple

$$\phi(x_1 + x_2) = 2^{x_1+x_2} = 2^{x_1}2^{x_2} = \phi(x_1)\phi(x_2)$$

y por tanto ϕ es un homomorfismo. Por otro lado, la ecuación $2^x = 1$ implica que $x = 0$ con lo cual se obtiene que $\text{Ker}(\phi) = \{0\}$. Además, para $y \in \mathbb{R}^+$ se tiene que $\phi(\log_2 y) = 2^{\log_2 y} = y$. En consecuencia, ϕ es un isomorfismo.

Proposición 6.1. Si G es un grupo cíclico, entonces G es isomorfo a $\mathbb{Z}_n$ para algún entero $n > 1$ o es isomorfo a $\mathbb{Z}$.

Demostración. Sea $a \in G$ tal que $G = \langle a \rangle$. Suponga $|G| = \text{ord}(a) = n$ y considere la función $\phi : G \longrightarrow \mathbb{Z}_n$ dada por $\phi(a^k) = k$ para todo $k = 0, 1, \ldots, n-1$. Entonces para i, j existen enteros q y r, tal que $i + j = nq + r$ y $0 \leq r < n$. Luego,

$$\phi(a^i a^j) = \phi(a^{i+j}) = \phi(a^r) = r = nq + r = i + j = \phi(a^i) + \phi(a^j).$$

Además, es claro que $\text{Ker}(\phi) = \{1\}$, lo cual implica que el homomorfismo es inyectivo, y dado que G y $\mathbb{Z}_n$ tienen el mismo orden se conluye que ϕ es sobreyectiva. Por tanto, $G \cong \mathbb{Z}_n$ siempre y cuando G sea cíclico y de orden n.

Por otro lado, si G es de orden infinito considere la función $\phi : G \longrightarrow \mathbb{Z}$ dada por $\phi(a^k) = k$ para todo $k \in \mathbb{Z}$ con lo cual se obtiene que ϕ es un homomorfismo. Por otro lado, dado que a es de orden infinito la igualdad $\phi(a^i) = \phi(a^j)$ implica que $i = j$ y así $\text{Ker}(\phi) = \{1\}$. Además, según como se ha definido el homomorfismo, este es sobreyectivo. De ahí que, $G \cong \mathbb{Z}$ siempre y cuando G sea cíclico y de orden infinito. □

Ejemplo 6.9. Determinar si $U(10)$ o $U(5)$ es isomorfo a $\mathbb{Z}_4$.

Según la Proposición 6.1 basta con analizar si los grupos $U(10)$ o $U(5)$ son cíclicos. Para ello observe que en el grupo $U(5)$ se cumple $3^1 = 3$, $3^2 = 4$, $3^3 = 2$ y $3^4 = 1$. Por otro lado, en el grupo $U(10)$ se cumple $3^1 = 3$, $3^2 = 9$, $3^3 = 7$ y $3^4 = 1$. Por tanto, ambos grupos son cíclicos de orden 4 e isomorfos a $\mathbb{Z}_4$.

En el Teorema 6.1 y Corolario 6.1 se presentan una serie de propiedades que satisfacen los homomorfismos, y en particular cumplen los isomorfismos. En este sentido observe que para un isomorfismo $\phi : G \longrightarrow G'$ se cumple que:

1. Si $H \leq G$, entonces $\phi(H) \leq G'$.

2. $\text{ord}(a) = \text{ord}(\phi(a))$ para todo $a \in G$.

3. G es cíclico si y solo G' es cíclico.

4. G es abeliano si y solo G' es abeliano.

5. Si $K' \leq G'$, entonces $\phi^{-1}(K') \leq G$.

Observe que de las propiedades 2 y 3 se concluye que si $G \cong G'$ mediante el isomorfismo ϕ, entonces a y $\phi(a)$ deben ser generadores de G y G', respectivamente. Por otro lado, observe que si se considera el conjunto Group de todos los grupos y se define la relación "es isomorfo a", entonces para todo $G, G', G'' \in \text{Group}$

1. $G \cong G$.

2. Si $G \cong G'$, entonces $G' \cong G$.

3. Si $G \cong G'$ y $G' \cong G''$, entonces $G \cong G''$.

En otras palabras, la relación definida es de equivalencia, y en este sentido, con respecto al problema planteado al inicio de la sección, interesa estudiar los representantes de cada una de las clases de equivalencia distintas de esta relación.

Teorema 6.2. Si $\phi : G \longrightarrow G'$ es un isomorfismo, entonces
1. ϕ^{-1} es un isomorfismo de G' en G.
2. Para $b \in G$ y $k \in \mathbb{Z}$. La ecuación $x^k = b$ tiene el mismo número de soluciones en G que la ecuación $x^k = \phi(b)$ en G'.
3. Si G es finito, entonces G y G' tienen el mismo número de elementos de cada orden.

Demostración. Primero note que la función inversa está definida por $\phi^{-1}(y) = x$ si $\phi(x) = y$. Para $y_1, y_2 \in G'$ existen $x_1, x_2 \in G$, tales que $\phi(x_1) = y_1$ y $\phi(x_2) = y_2$. Dado que ϕ es un isomorfismo se cumple que

$$\phi(x_1x_2) = \phi(x_1)\phi(x_2) = y_1y_2,$$

de lo cual se obtiene que $\phi^{-1}(y_1y_2) = x_1x_2 = \phi^{-1}(y_1)\phi^{-1}(y_2)$. La biyectividad de ϕ^{-1} se garantiza por la biyectividad de ϕ. Por tanto, ϕ^{-1} es un isomorfismo de G' en G.

Para el ítem 2 considere los conjuntos

$$A_k = \{x \in G \ : \ x^k = b\} \qquad \text{y} \qquad B_k = \{y \in G' \ : \ y^k = \phi(b)\}.$$

Note que para cada $x \in A_k$ el elemento $\phi(x) \in B_k$. Entonces la función

$$F : A_k \longrightarrow B_k, \text{ definida por } F(x) = \phi(x),$$

es biyectiva, lo cual garantiza que $|A_k| = |B_k|$. Finalmente, para el caso $b = 1$ se tiene que A_k y B_k están conformados por los elementos de G y G' de orden k, respectivamente. Por tanto, el ítem 3 es una consecuencia del ítem 2. □

Teorema 6.3. Si $\phi : G \to G'$ es un homorfismo de grupos, entonces

$$G/\text{Ker}(\phi) \cong \phi(G).$$

Demostración. Sea $H = \text{Ker}(\phi)$ y considere la aplicación

$$\overline{\phi} : G/H \longrightarrow \phi(G)$$

definida por $\overline{\phi}(\overline{a}) = \phi(a)$. Observe que $\overline{\phi}$ es una función ya que si $\overline{a} = \overline{b}$, entonces $ab^{-1} \in H$ y se tiene

$$\phi(a) = \phi(ab^{-1})\phi(b) = 1'\phi(b) = \phi(b).$$

Por tanto, $\overline{\phi}(\overline{a}) = \overline{\phi}(\overline{b})$. Por otro lado, el hecho que ϕ es un homomorfismo implica que $\overline{\phi}$ también lo sea. Suponga que $\overline{\phi}(\overline{a}) = \overline{\phi}(\overline{b})$, entonces $\phi(a) = \phi(b)$, de lo cual se obtiene que $ab^{-1} \in H$. Luego $\overline{a} = \overline{b}$, es decir el homomorfismo $\overline{\phi}$ es inyectivo. Finalmente, note que por construcción la función $\overline{\phi}$ es sobreyectiva. □

Ejemplo 6.10. Probar que $\mathbb{Z}_{12}/\langle 2\rangle \cong \mathbb{Z}_2$.

Considere la función dada por $\phi : \mathbb{Z}_{12} \longrightarrow \mathbb{Z}_2$ definida por $\phi(x) = x$ mód 2. Observe que ϕ es un homomorfismo en el cual $\text{Ker}(\phi) = \langle 2\rangle = \{0, 2, 4, 6, 8, 10\}$. Además, según como se definió el homomorfismo, este es sobreyectivo. Por tanto, según el Teorema 6.3

$$\mathbb{Z}_{12}/\langle 2\rangle \cong \mathbb{Z}_2.$$

Ejemplo 6.11. Mostrar que $\mathbb{Z}/\langle n\rangle \cong \mathbb{Z}_n$.

Considere la función $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ definida por $\phi(x) = (x \text{ mód } n)$. Como ya se expuso, esta función es un homomorfismo sobreyectivo de grupos en el cual $\text{Ker}(\phi) = n\mathbb{Z}$. En consecuencia, de acuerdo con el Teorema 6.3

$$\mathbb{Z}/\langle n\rangle \cong \mathbb{Z}_n.$$

Ejemplo 6.12. Sea $\mathbb{S}^1 = \{z \in \mathbb{C}^* \ : \ |z| = 1\}$. Probar que $\mathbb{R}/\langle 2\pi \rangle \cong \mathbb{S}^1$.

Primero tenga en cuenta que para cada $t \in \mathbb{R}$ se tiene que el número complejo

$$z = e^{it} = \cos t + i \sin t$$

tiene norma 1. En otras palabras, para cada $t \in \mathbb{R}$ se cumple que $e^{it} \in \mathbb{S}^1$. Por tanto, considere la función $\phi : \mathbb{R} \longrightarrow \mathbb{S}^1$ dada por $\phi(t) = e^{it}$. Esta función satisface la igualdad

$$\phi(t_1 + t_2) = e^{i(t_1+t_2)} = e^{it_1} e^{it_2} = \phi(t_1)\phi(t_2),$$

del cual se obtiene que ϕ es un homomorfismo sobreyectivo de grupos. Además, observe que $\phi(t) = 1$ siempre y cuando

$$\cos t = 1$$
$$\sin t = 0$$

lo cual se cumple si $t = 2\pi k$ con $k \in \mathbb{Z}$. Es decir, $\text{Ker}(\phi) = \{2\pi k \ : \ k \in \mathbb{Z}\}$ y así

$$\mathbb{R}/\langle 2\pi \rangle \cong \mathbb{S}^1.$$

Un tipo particular de isomorfismo que se utiliza en el estudio de la clasificación de grupos son los denominados *automorfismos* que se definen a continuación.

Definición 6.4. Un isomorfismo de un grupo G en si mismo se denomina un automorfismo de G.

Si se denota por $\text{Aut}(G)$ como el conjunto de automorfismos del grupo G, observe que la operación de composición es binaria en dicho conjunto. Además, la función identidad actúa como elemento neutro y por el Teorema 6.2 se tiene que la operación satisface la propiedad del elemento inverso. Por tanto, el conjunto $\text{Aut}(G)$, junto con la composición de funciones, tiene estructura de grupo. Algunos ejemplos básicos de automorfismos son $\phi(z) = \overline{z}$ con $z \in \mathbb{C}$ y $\phi(a, b) = (b, a)$ para $(a, b) \in \mathbb{R}^2$ ambos grupos con la operación de adición de complejos y vectores del plano, respectivamente.

Ejemplo 6.13. Sea $G = SL(2, \mathbb{R})$ y $M \in G$. Probar que $\phi(A) = MAM^{-1}$ es un isomorfismo de G en G.

Para $A, B \in G$ se cumple

$$\phi(AB) = M(AB)M^{-1} = (MAM^{-1})(MBM^{-1}) = \phi(A)\phi(B).$$

Por otro lado, observe que si $A \in \text{Ker}(\phi)$, entonces $MAM^{-1} = I$ en el que I es la matriz identidad. Luego, $A = I$ y por tanto el homomorfismo es inyectivo. Por otro lado, note

que la matriz $M^{-1}AM \in G$ satisface la igualdad $\phi(M^{-1}AM) = A$, con lo cual se obtiene que ϕ es un automorfismo de $SL(2,\mathbb{R})$.

Ejemplo 6.14. Determinar todos los isomorfismo de $\mathbb{Z}_6$ en $\mathbb{Z}_6$.

Primero observe que si ϕ es un isomorfismo de $\mathbb{Z}_6$ en $\mathbb{Z}_6$, entonces se satisface que

$$\phi(k) = \phi(\underbrace{1+1+\cdots+1}_{k-\text{veces}}) = k\phi(1)$$

lo cual implica que basta conocer el valor que toma $\phi(1)$ para determinar el isomofismo completo. Por otro lado, se debe tener en cuenta que $\phi(1)$ debe ser un generador de $\mathbb{Z}_6$. Por tanto, existen dos isomorfismos definidos por

$$\phi(1) = 1 \qquad \text{y} \qquad \phi(1) = 5.$$

Observe que el primero de ellos corresponde a la función identidad.

Teorema 6.4. Para cada entero positivo n, $\text{Aut}(\mathbb{Z}_n)$ es isomorfo a $\text{U}(n)$.

Demostración. Considere la función $\Phi : \text{U}(n) \longrightarrow \text{Aut}(\mathbb{Z}_n)$ dada por $\Phi(a) = \phi_a$ en la cual

$$\begin{array}{rccc} \phi_a & : & \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_n \\ & & x & \longmapsto & \phi_a(x) = ax. \end{array}$$

Note que para $a, b \in \text{U}(n)$ se cumple

$$\phi_{ab}(x) = (ab)x = a(bx) = \phi_a(bx) = \phi_a\phi_b(x),$$

lo cual equivale a que Φ es un homomorfismo de grupos. Además, si $a \in \text{Ker}(\Phi)$, entonces $\phi_a(x) = x$ para todo $x \in \mathbb{Z}_n$, en particular para $x = 1$ se tiene que $a = 1$. De ahí que $\text{Ker}(\Phi) = \{1\}$ y así la función es inyectiva. Por otro lado, observe que si ϕ es un automorfismo de $\mathbb{Z}_n$, entonces $\phi(x) = ax$ con $a = \phi(1)$, por tanto $\phi = \phi_a$. En consecuencia, $\text{Aut}(\mathbb{Z}_n) \cong \text{U}(n)$. □

Ejemplo 6.15. Determinar todos los automorfismos de $\mathbb{Z}_{10}$ y construir la tabla de Cayley de $\text{Aut}(\mathbb{Z}_{10})$.

De acuerdo con el Teorema 6.4 se tiene que cada automorfismo de $\mathbb{Z}_{10}$ es de la forma $\phi(x) = ax$ en el que a es un generador del grupo. Por tanto, los automorfismos de $\mathbb{Z}_{10}$ son

$$\phi_1(x) = x \qquad \phi_3 = 3x \qquad \phi_7(x) = 7x \qquad \text{y} \qquad \phi_9(x) = 9x.$$

Por otro lado, observe que si $\phi_a, \phi_b \in \text{Aut}(\mathbb{Z}_{10})$, entonces $\phi_a\phi_b = \phi_{ab}$. Por tanto,

$\cdot$	ϕ_1	ϕ_3	ϕ_7	ϕ_9
ϕ_1	ϕ_1	ϕ_3	ϕ_7	ϕ_9
ϕ_3	ϕ_3	ϕ_9	ϕ_1	ϕ_7
ϕ_7	ϕ_7	ϕ_1	ϕ_9	ϕ_3
ϕ_9	ϕ_9	ϕ_7	ϕ_3	ϕ_1

Existe un tipo particular de automorfismo el cual permite medir porque falla la conmutatividad del grupo.

Definición 6.5. Sean G un grupo y $a \in G$. La función ϕ_a definida por

$$\phi_a(x) = axa^{-1}, \text{ para todo } x \in G,$$

se denomina el automorfismo interno de G inducido por a. El conjunto de todos los automorfismos internos de G se denota por $\text{Inn}(G)$.

Note que si el grupo G es abeliano, entonces el único automorfismo interno de G es la función identidad. Los automorfismo internos de un grupo suministran una manera de crear subgrupos isomorfos. Por ejemplo, si

$$H = \{(1), (1234), (13)(24), (1432), (12)(34), (24), (14)(23), (13)\}$$

entonces

$$(12)H(12) \qquad \text{y} \qquad (123)H(321)$$

son subgrupos isomorfos a H.

Teorema 6.5. El conjunto $\text{Inn}(G)$ tiene estructura de subgrupo normal de $\text{Aut}(G)$ con la operación de composición.

Demostración. Para $a, b \in G$ observe que $\phi_a^{-1} = \phi_{a^{-1}}$, ya que

$$\phi_{a^{-1}}\phi_a(x) = \phi_{a^{-1}}(axa^{-1}) = a^{-1}(axa^{-1})a = x.$$

De ahí que

$$\phi_a\phi_b^{-1}(x) = \phi_a\phi_{b^{-1}}(x) = \phi_a(b^{-1}xb) = a(b^{-1}xb)a^{-1} = (ab^{-1})x(ab^{-1})^{-1} = \phi_{ab^{-1}}(x),$$

y así $\phi_a\phi_b^{-1} \in \text{Inn}(G)$. Por otro lado, si $\phi_a \in \text{Inn}(G)$ y $\phi \in \text{Aut}(G)$, entonces

$$\phi\phi_a\phi^{-1}(x) = \phi(a\phi^{-1}(x)a^{-1}) = \phi(a)x\phi(a)^{-1} = \phi_b(x)$$

en el que $b = \phi(a) \in G$. Esta última igualdad implica que $\phi\phi_a\phi^{-1} \in \mathrm{Inn}(G)$, es decir, $\mathrm{Inn}(G) \triangleleft \mathrm{Aut}(G)$. □

Ejemplo 6.16. Sean G un grupo y $\mathcal{Z}(G)$ es el centro de G. Probar que

$$G/\mathcal{Z}(G) \cong \mathrm{Inn}(G)$$

Considere la función $\Phi : G \longrightarrow \mathrm{Inn}(G)$ dada por $\Phi(a) = \phi_a$. Entonces

$$\Phi(ab)(x) = \phi_{ab}(x) = (ab)x(ab)^{-1} = a(bxb^{-1})a^{-1} = \phi_a\phi_b(x) = \Phi(a)\Phi(b)(x).$$

De ahí que $\Phi(ab) = \Phi(a)\Phi(b)$ para todo $a, b \in G$. Por tanto, la función Φ es un homomorfismo sobreyectivo, tal que

$$\begin{aligned}\mathrm{Ker}(\Phi) =& \{a \in G \ : \ \phi_a(x) = \phi_e(x) \text{ para todo } x \in G \ \}\\ =& \{a \in G \ : \ ax = xa \text{ para todo } x \in G\}\\ =& \mathcal{Z}(G).\end{aligned}$$

Por tanto, del Teorema 6.3 se obtiene la afirmación.

Se finaliza esta sección con uno de los teoremas más importantes del álgebra abstracta.

Teorema 6.6 (Teorema de Cayley)**.** Cada grupo es isomorfo a un grupo de permutaciones.

Demostración. Sea G un grupo y considere el grupo simétrico en G,

$$S_G = \{\alpha : G \to G \ : \ \alpha \text{ es una permutación de } G\}.$$

Sea $\Phi : G \longrightarrow S_G$ dada por $\Phi(a) = \alpha_a$ con $\alpha_a(g) = ag$. Primero note que Φ está bien definida puesto que α_a es una función biyectiva de G en G. En efecto, si $\alpha_a(g_1) = \alpha_a(g_2)$, entonces $ag_1 = ag_2$ y aplicando leyes cancelativas se obtiene $g_1 = g_2$. Además, para $g \in G$ se tiene $\alpha_a(a^{-1}g) = g$. Por otro lado, para $a, b \in G$ se cumple

$$\alpha_{ab}(g) = (ab)g = a(bg) = \alpha_a(bg) = \alpha_a\alpha_b(g)$$

para todo $g \in G$, con lo cual se obtiene que $\Phi(ab) = \Phi(a)\Phi(b)$. Por tanto, Φ es un homomorfismo de grupos con $\mathrm{Ker}(\Phi) = \{1\}$. En consecuencia, según el Teorema 6.3

$$G \cong \Phi(G)$$

en el que $\Phi(G)$ es un subgrupo del grupo simétrico S_G. □

Ejemplo 6.17. Consideremos el grupo $G = U(12) = \{1, 5, 7, 11\}$. Hallar el grupo de permutaciones isomorfo al grupo $U(12)$ y determinar su tabla de Cayley.

Según la prueba del Teorema 6.6 se tiene que

$$P_G = \{T_1, T_5, T_7, T_{11}\}$$

en el cual

$$T_1 = \begin{pmatrix} 1 & 5 & 7 & 11 \\ 1 & 5 & 7 & 11 \end{pmatrix} \qquad T_5 = \begin{pmatrix} 1 & 5 & 7 & 11 \\ 5 & 1 & 11 & 7 \end{pmatrix}$$

$$T_7 = \begin{pmatrix} 1 & 5 & 7 & 11 \\ 7 & 11 & 1 & 5 \end{pmatrix} \qquad T_{11} = \begin{pmatrix} 1 & 5 & 7 & 11 \\ 11 & 7 & 5 & 1 \end{pmatrix}.$$

6.3 Ejercicios

1. Considerar la función ϕ de $\mathbb{Z}_{12}$ en $\mathbb{Z}_{12}$ dada por $\phi(x) = 3x$.

   a) Probar que ϕ es un homomorfismo.

   b) Hallar Ker(ϕ).

   c) Determinar $\phi^{-1}(6)$.

   d) Para $K' = \{0, 6\}$, hallar $\phi^{-1}(K')$.

2. Considerar la función ϕ de $\mathbb{C}^*$ en $\mathbb{C}^*$ dada por $\phi(x) = x^4$.

   a) Probar que ϕ es un homomorfismo.

   b) Hallar Ker(ϕ).

   c) Determinar el conjunto $\phi^{-1}(2)$.

   d) Sea $H = \langle \cos 30^o + i \sin 30^o \rangle$. Determinar $|H|$ y $|\phi(H)|$.

3. Determinar todos los homorfismo de $\mathbb{Z}_{12}$ en $\mathbb{Z}_{30}$.

4. Probar que la función $\phi : \mathbb{Z}_n \longrightarrow \mathbb{Z}_m$ dada por $\phi(x) = ax$ es un homomorfimos de grupos si y solo si $na \equiv 0 (\text{mód } m)$.

5. Sean $\sigma : G \longrightarrow H$ y $\phi : H \longrightarrow K$ dos homomorfismos. Probar que $\phi\sigma$ es un homomorfismo de G en K.

6. Sea G un grupo de permutaciones. Para cada $\sigma \in G$ se define la aplicación

$$\operatorname{sgn}(\sigma) = \begin{cases} +1 & \text{si } \sigma \text{ es par} \\ -1 & \text{si } \sigma \text{ es impar} \end{cases}$$

   a) Probar que sgn es una función.

   b) Probar que sgn es un homomorfismo.

   c) Hallar el kernel de sgn.

7. Sea p un número primo. Para un número entero n no nulo se define su *valuación p-ádica* como el máximo entero k para el cual p^k divide a n, esto es

$$v_p(n) = \text{máx}\{k \in \mathbb{Z} \ : \ p^k \mid n\}.$$

   Considere la aplicación $v_p : \mathbb{Q}^* \longrightarrow \mathbb{Z}$ dada por

$$v_p\left(\frac{m}{n}\right) = v_p(m) - v_p(n).$$

   a) Probar que v_p es una función.

   b) Probar que v_p es un homomorfismo.

   c) Hallar el kernel de v_p.

8. Sea p un número primo. Se dide $a \in \mathbb{Z}$ es un residuo cuadrático módulo p si existe un entero b tal que $a \equiv b^2 (\text{mód } p)$. El *símbolo de Legendre* del entero a se define como

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{si } p \nmid a \text{ y } a \text{ es un residuo cuadrático módulo } p \\ -1 & \text{si } p \nmid a \text{ y } a \text{ no es un residuo cuadrático módulo } p \\ 0 & \text{si } p \mid a \end{cases}.$$

   Considerar la aplicación $\left(\frac{\cdot}{p}\right) : \mathbb{Z}_p^* \longrightarrow \{\pm 1\}$ definida por el símbolo de Legendre.

   a) Probar que la aplicación es una función.

b) Probar que la aplicación es un homomorfismo de grupos.

c) Hallar su kernel.

9. Probar que dos grupos cualesquiera de orden 3 son isomorfos.

10. Explique porque dos grupos cualesquiera de orden 3 son isomorfos.

11. Probar que no existe un isomorfismo del grupo $\mathbb{Q}$ al grupo $\mathbb{Q}^*$.

12. Probar que los enteros con la adición es isomorfo al conjunto de los enteros pares con la adición.

13. Determinar el conjunto Aut($\mathbb{Z}_6$).

14. Determinar el conjunto Aut($\mathbb{Z}$).

15. Mostrar que U(8) no es isomorfo a U(10).

16. Encontrar dos grupos G y H tales que $G \ncong H$ pero Aut(G) $\cong$ Aut(H).

17. Sea $\phi \in \text{Aut}(\mathbb{Z}_n)$ y $(a, n) = 1$. Si $\phi(a) = b$ determinar una fórmula para $\phi(x)$.

18. Sean $H = \{\beta \in S_5 \ : \ \beta(1) = 1\}$ y $K = \{\beta \in S_5 \ : \ \beta(2) = 2\}$. Probar que H y K son isomorfos. ¿La afirmación también será cierta si se reemplaza S_5 por S_n para $n \geq 3$?

19. Mostrar que $\mathbb{Z}$ tiene un número infinito de subgrupos isomorfos a $\mathbb{Z}$.

20. Sea ϕ un automorfismo de un grupo G. Probar que $H = \{x \in G \ : \ \phi(x) = x\}$ es un subgrupo de G.

21. Determinar un subgrupo de orden más pequeño, tal que contiene un subgrupo isomorfo a $\mathbb{Z}_{12}$ y uno isomorfo a $\mathbb{Z}_{20}$. Justificar la respuesta.

22. Sea $\phi : \mathbb{Z}_{20} \longrightarrow \mathbb{Z}_{20}$ un automorfismo, tal que $\phi(5) = 5$. ¿Cuáles son las posibilidades para $\phi(x)$?

23. Sean ϕ y γ son isomorfismos de un grupo cíclico $\langle a \rangle$ en otro grupo, tales que $\phi(a) = \gamma(a)$. Probar que $\phi = \gamma$.

24. Suponga que G es un grupo abeliano finito que no contiene un elemento de orden 2. Probar que la aplicación $\phi(g) = g^2$ es un automorfismo de G.

25. Suponga que g y h inducen el mismo automorfismo interno de un grupo G. Probar que $h^{-1}g \in \mathcal{Z}(G)$.

26. Sea k un divisor de n. Probar que $\mathbb{Z}_n/\langle k \rangle \cong \mathbb{Z}_k$.

27. Sea $\phi : \mathbb{Z}_{30} \to \mathbb{Z}_{30}$ un homomorfismo de grupos, tal que $\text{Ker}(\phi) = \{0, 10, 20\}$. Si $\phi(23) = 9$ determinar los elementos que son enviados al 9.

28. Utilizar el Teorema de Cayley para hallar el grupo de permutaciones isomorfo al grupo D_3 y construir su tabla de Cayley.

CAPÍTULO 7

Producto directo de grupos

En este capítulo se presenta nuevas construcciones de grupos, los cuales serán de importancia en el objetivo de clasificar los grupos abelianos finitamente generados. Una de ellas es dotar de estructura de grupo al producto cartesiano de grupos, y la segunda es mediante la descomposición de un grupo por medio de algunos subgrupos con ciertas características.

7.1 Producto directo externo

La primera construcción es definir la operación binaria componente a componente en el producto cartesiano de grupos. Esto permitirá estudiar las propiedades estructurales de un grupo.

Teorema 7.1. Si $\langle G_1, *_1\rangle$ y $\langle G_2, *_2\rangle$ son dos grupos, entonces el producto cartesiano $G_1 \times G_2$ tiene estructura de grupo con la operación binaria definida por

$$(g_1, g_2)(h_1, h_2) = (g_1 *_1 h_1, g_2 *_2 h_2).$$

Demostración. Primero observe que la cerradura de las operaciones $*_1$ y $*_2$ implican que la operación definida en el producto cartesiano $G_1 \times G_2$ es cerrada igualmente. Por otro lado, por la asociatividad de las operaciones en los grupos dados se cumple que

$$\begin{aligned}[(g_1, g_2)(h_1, h_2)](k_1, k_2) =& (g_1 *_1 h_1, g_2 *_2 h_2)(k_1, k_2)\\ =& ((g_1 *_1 h_1) *_1 k_1, (g_1 *_2 h_2) *_2 k_2)\\ =& (g_1 *_1 (h_1 *_1 k_1), g_1 *_2 (h_2 *_2 k_2))\\ =& (g_1, g_2)[(h_1, h_2)(k_1, k_2)]\end{aligned}$$

con $(g_1, g_2), (h_1, h_2), (k_1, k_2) \in G_1 \times G_2$. Si se considera al elemento (e_1, e_2) en el que e_1 y e_2 son los elementos neutros de los grupos G_1 y G_2, respectivamente, entonces se satisface que

$$(e_1, e_2)(g_1, g_2) = (e_1 *_1 g_1, e_2 *_2 g_2) = (g_1, g_2) = (g_1 *_1 e_1, g_2 *_2 e_2) = (g_1, g_2)(e_1, e_2).$$

Finalmente, de acuerdo con la operación definida en el producto cartesiano, para todo (g_1, g_2) se cumple que

$$(g_1, g_2)(g_1^{-1}, g_2^{-1}) = (e_1, e_2) = (g_1^{-1}, g_2^{-1})(g_1, g_2).$$

Por tanto, el producto cartesiano de dos grupos tiene estructura de grupo con la operación componente a componente. □

El grupo definido en el Teorema 7.1 se denomina el producto directo externo de G_1 y G_2. Observe que en el caso que los grupos G_1 y G_2 sean de orden finito, entonces el orden de $G_1 \times G_2$ es igual al producto de los respectivos órdenes, es decir

$$|G_1 \times G_2| = |G_1||G_2|.$$

Note además que esta construcción se puede generalizar a un conjunto finito de grupos como se evidencia en el siguiente corolario, su demostración se deja como ejercicio al lector. En general, si se tiene que G_i es un grupo para cada $i \in I$ en un conjunto de índices, entonces los elementos del producto cartesiano $\Pi_{i\in I} G_i$ son vistos como funciones, ver el ejercicio 12 de la Sección 7.3.

Corolario 7.1. Si $\langle G_i, *_i\rangle$ es un grupo para $i = 1, 2, \ldots, m$, entonces el producto cartesiano $G_1 \times G_2 \times \cdots \times G_m$ tiene estructura de grupo con la operación binaria

dada por

$$(g_1, g_2, \ldots, g_n)(h_1, h_2, \ldots, h_m) = (g_1 *_1 h_1, g_2 *_2 h_2, \ldots, g_m *_m h_m)$$

Algunos ejemplos básicos del producto directo de grupos están por un lado $\mathbb{R}^2$ o en general $\mathbb{R}^n$, y por otro el grupo de Klein dado por $\mathbb{Z}_2 \times \mathbb{Z}_2$. En este último grupo observe que cada elemento no cero tiene orden 2, por lo cual no es cíclico.

Ejemplo 7.1. Hallar la tabla de Cayley del grupo $\mathbb{Z}_2 \times \mathbb{Z}_3$ y determinar si es cíclico. En caso afirmativo, hallar sus generadores.

Primero observe que el grupo $\mathbb{Z}_2 \times \mathbb{Z}_3$ es de orden 6 y sus elementos son:

$$(0,0),\ (0,1),\ (0,2),\ (1,0),\ (1,1) \text{ y } (1,2).$$

Por lo cual su tabla de Cayley es

$+$	$(0,0)$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$
$(0,0)$	$(0,0)$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$
$(0,1)$	$(0,1)$	$(0,2)$	$(0,0)$	$(1,1)$	$(1,2)$	$(1,0)$
$(0,2)$	$(0,2)$	$(0,0)$	$(0,1)$	$(1,2)$	$(1,0)$	$(1,1)$
$(1,0)$	$(1,0)$	$(1,1)$	$(1,2)$	$(0,0)$	$(0,1)$	$(0,2)$
$(1,1)$	$(1,1)$	$(1,2)$	$(1,0)$	$(0,1)$	$(0,2)$	$(0,0)$
$(1,2)$	$(1,2)$	$(1,0)$	$(1,1)$	$(0,2)$	$(0,0)$	$(0,1)$

Note que solamente tiene dos generadores $(1,1)$ y $(1,2)$.

Ejemplo 7.2. Hallar la tabla de Cayley del grupo $\mathrm{U}(4) \times \mathrm{U}(6)$ y determinar si es cíclico. En caso afirmativo, hallar sus generadores.

Primero observe que el grupo $\mathrm{U}(4) \times \mathrm{U}(6)$ es de orden 4 y sus elementos son:

$$(1,1),\ (1,5),\ (3,1) \text{ y } (3,5).$$

Por lo cual su tabla de Cayley es

$\cdot$	$(1,1)$	$(1,5)$	$(3,1)$	$(3,5)$
$(1,1)$	$(1,1)$	$(1,5)$	$(3,1)$	$(3,5)$
$(1,5)$	$(1,5)$	$(1,1)$	$(3,5)$	$(3,1)$
$(3,1)$	$(3,1)$	$(3,5)$	$(1,1)$	$(1,5)$
$(3,5)$	$(3,5)$	$(3,1)$	$(1,5)$	$(1,1)$

En este caso note que ningún elemento genera al grupo completo, por lo que $\mathrm{U}(4) \times \mathrm{U}(6)$ no es cíclico.

Ejemplo 7.3. Sean $x = \rho_1$ y $y = \tau_0$ las permutaciones de D_6 dadas por

$$x = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix} \quad \text{y} \quad y = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 5 & 4 & 3 & 2 \end{pmatrix}.$$

En el grupo $D_6 \times \mathrm{U}(6)$ determinar el elemento $(x^3y, 5)^{-1}(xy, 5)$.

Primero note que $\mathrm{ord}(x) = 6$ y $\mathrm{ord}(y) = 2$, de ahí que

$$(x^3y, 5)^{-1}(xy, 5) = (y^{-1}x^{-3}, 5^{-1})(xy, 5) = (yx^3, 5)(xy, 5) = (yx^4y, 1).$$

Por otro lado, se tiene que $(yxy)^k = yx^ky$ para $k \in \mathbb{Z}$. Además, del hecho que $xyxy = (1)$ se obtiene $yxy = x^5$, y así $yx^4y = x^2$. En consecuencia,

$$(x^3y, 5)^{-1}(xy, 5) = (yx^4y, 1) = (x^2, 1).$$

Ejemplo 7.4. Probar que los únicos grupos de orden 4 salvo isomorfismo son $\mathbb{Z}_4$ y $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Sea $G = \{e, a, b, c\}$ un grupo de orden 4 con e su elemento neutro. Si G es cíclico, entonces por Teorema 6.1 se tiene que G es isomorfo a $\mathbb{Z}_4$. Sin embargo, si G no es cíclico, entonces por el Teorema de Lagrange el orden de todo elemento distinto al neutro es de orden 2, es decir

$$a^2 = b^2 = c^2 = e.$$

Esto implica que $ab = ba = c$, $ac = ca = b$ y $bc = cb = a$. En la Figura 7.1 se presentan las tablas de Cayley del grupo G y $\mathbb{Z}_2 \times \mathbb{Z}_2$, en la cual se puede apreciar que si se define la función $\phi : G \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$ dada por $\phi(e) = (0,0)$, $\phi(a) = (1,0)$, $\phi(b) = (0,1)$ y $\phi(c) = (1,1)$, entonces $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$+$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(1,0)$	$(1,0)$	$(0,0)$	$(1,1)$	$(0,1)$
$(0,1)$	$(0,1)$	$(1,1)$	$(0,0)$	$(1,0)$
$(1,1)$	$(1,1)$	$(0,1)$	$(1,0)$	$(0,0)$

Figura 7.1: Tablas de Cayley de un grupo de orden 4 y el grupo de Klein

Proposición 7.1. Si (g, h) es un elemento del producto directo externo $G_1 \times G_2$, entonces

$$\mathrm{ord}(g, h) = \mathrm{m.c.m}\{\mathrm{ord}(g), \mathrm{ord}(h)\}.$$

Demostración. Suponga que el entero positivo M satisface

$$(g,h)^M = \underbrace{(g,h)(g,h)\cdots(g,h)}_{M-\text{veces}} = (g^M, h^M) = (1,1).$$

Entonces de acuerdo con la Proposición 4.1 se tiene que M es un múltiplo de $\text{ord}(g)$ y $\text{ord}(h)$. Por tanto, según la definición de orden de un elemento se tiene que

$$\text{ord}(g,h) = \text{m.c.m}\{\text{ord}(g), \text{ord}(h)\}. \qquad \square$$

La anterior proposición se puede generalizar al producto directo externo de un número finito de grupos.

Corolario 7.2. Si $(g_1, g_2, \ldots, g_n)$ es un elemento del producto directo externo $G_1 \times G_2 \times \cdots \times G_n$, entonces

$$\text{ord}(g_1, g_2, \ldots, g_n) = \text{m.c.m}\{\text{ord}(g_1), \text{ord}(g_2), \ldots, \text{ord}(g_n)\}.$$

Ejemplo 7.5. Determinar todos los elementos de $\mathbb{Z}_{25} \times \mathbb{Z}_5$ de orden 5.

Sea $(a,b) \in \mathbb{Z}_{25} \times \mathbb{Z}_5$, tal que $\text{ord}(a,b) = 5$. Entonces según la Proposición 7.1 se tiene que

$$\text{m.c.m}\{\text{ord}(a), \text{ord}(b)\} = 5.$$

Esto implica que $5 = \text{ord}(a)k_1 = \text{ord}(b)k_2$ con k_1 y k_2 enteros positivos. Por tanto,

$$\text{ord}(a), \text{ord}(b) \in \{1, 5\}$$

con la salvedad de que ambos no pueden tener orden 1 al mismo tiempo. El análisis anterior implica que $a = 0$ o $a \in \{5, 10, 15, 20\}$ y $b = 0$ o $b \in \{1, 2, 3, 4\}$. En consecuencia, los elementos de orden 5 en el grupo $\mathbb{Z}_{25} \times \mathbb{Z}_5$ son:

$$(0,1),\ (0,2),\ (0,3),\ (0,4),\ (5,0),\ (5,1),\ (5,2),\ (5,3),\ (5,4),\ (10,0),\ (10,1),\ (10,2),\ (10,3),\ (10,4),\ (15,0),\ (15,1),\ (15,2),\ (15,3),\ (15,4),\ (20,0),\ (20,1),\ (20,2),\ (20,3) \text{ y } (20,4).$$

Proposición 7.2. Si G y H son grupos cíclicos finitos, entonces el grupo $G \times H$ es cíclico si y solo $|G|$ y $|H|$ son primos relativos.

Demostración. Sean $n = |G|$ y $m = |H|$. Suponga que $G \times H$ es cíclico, luego existe un elemento $(a,b) \in G \times H$ para el cual $\langle (a,b) \rangle = G \times H$. Entonces por la Proposición 7.1 se tiene que

$$nm = |G||H| = \text{m.c.m}\{\text{ord}(a), \text{ord}(b)\} = \text{m.c.m}\{n, m\}.$$

Dado que $\text{m.c.m}\{n, m\} = \dfrac{nm}{\text{m.c.d}\{n, m\}}$ se sigue que $\text{m.c.d}\{n, m\} = 1$.

En el otro sentido, sean $a \in G$ y $b \in H$, tales que $\text{ord}(a) = n$, $\text{ord}(b) = m$ y $\text{m.c.d}\{m, n\} = 1$. Entonces

$$\text{m.c.m}\{n, m\} = mn.$$

Por tanto, $\text{m.c.m}\{\text{ord}(a), \text{ord}(b)\} = mn$ y en consecuencia $G \times H = \langle (a, b) \rangle$. □

Si observa los Ejemplos 7.1 y 7.2, se tiene que el grupo $\mathbb{Z}_2 \times \mathbb{Z}_3$ es cíclico mientras que el grupo $U(4) \times U(6)$ no lo es, ya que los ordenes de $U(4)$ y $U(6)$ no son primos relativos. Sin embargo, del Ejemplo 7.4, se conoce que $U(4) \times U(6) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

La anterior proposición se puede generalizar a un número finito de grupos, su demostración se deja como ejercicio al lector.

Corolario 7.3. Si $G_1, G_2, \ldots, G_n$ son grupos cíclicos finitos con $n > 1$, entonces $G_1 \times G_2 \times \cdots \times G_n$ es cíclico si y solo $|G_i|$ y $|G_j|$ son primos relativos para todo $i \neq j$.

Teorema 7.2. Si N y M son subgrupos normales de los grupos G y H, respectivamente, entonces $N \times M$ es un subgrupo normal de $G \times H$, y además

$$(G \times H)/(N \times M) \cong (G/N) \times (H/M).$$

Demostración. Sean $(x, y) \in N \times M$ y $(g, h) \in G \times H$. Entonces

$$(g, h)(x, y)(g, h)^{-1} = (g, h)(x, y)(g^{-1}, h^{-1}) = (gxg^{-1}, hyh^{-1})$$

de lo cual se obtiene que $(gxg^{-1}, hyh^{-1}) \in N \times M$, ya que $N \triangleleft G$ y $M \triangleleft H$.

Por otro lado, considere la función sobreyectiva $\phi : G \times H \longrightarrow (G/N) \times (H/M)$ definida por $\phi(x, y) = (\overline{x}, \overline{y})$. Luego, para $(x_1, y_1), (x_2, y_2) \in G \times H$ se cumple que

$$\begin{aligned}\phi((x_1, y_1)(x_2, y_2)) =& \phi(x_1x_2, y_1y_2) = (\overline{x_1x_2}, \overline{y_1y_2}) = \\ =& (\overline{x_1}, \overline{y_1})(\overline{x_2}, \overline{y_2}) = \phi(x_1, y_1)\phi(x_2, y_2).\end{aligned}$$

Además, el homomorfismo de grupos satisface

$$\text{Ker}(\phi) = \{(x, y) \in G \times H \ : \ x \in N, \ y \in M\} = N \times M.$$

Por tanto, según el Teorema 6.3 se tiene que

$$(G \times H)/(N \times M) \cong (G/N) \times (H/M).$$ □

Ejemplo 7.6. Considerar el grupo abeliano

$$H = \left\{ \begin{pmatrix} 1 & x & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \ : \ x, y \in \mathbb{Z}_3 \right\}$$

en el cual la operación binaria es la multiplicación de matrices. Probar que H es isomorfo a $\mathbb{Z}_3 \times \mathbb{Z}_3$.

De forma similar al Ejemplo 4.9 se puede concluir que H es un grupo abeliano y que $H = \langle A, B \rangle$ con

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{y} \quad B = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Por tanto, se puede considerar la función sobreyectiva $\phi : \mathbb{Z}\times\mathbb{Z} \longrightarrow H$ dada por $\phi(m, k) = A^m B^k$. Note que dados los pares ordenados $(m_1, k_1), (m_2, k_2) \in \mathbb{Z} \times \mathbb{Z}$ se satisface

$$\begin{aligned} \phi((m_1, k_1) + (m_2, k_2)) = \phi(m_1 + m_2, k_1 + k_2) = A^{m_1+m_2} B^{k_1+k_2} = \\ = (A^{m_1} B^{k_1})(A^{m_2} B^{k_2}) = \phi(m_1, k_1)\phi(m_2, k_2). \end{aligned}$$

Así que ϕ es un homomorfismo sobreyectivo y se tiene

$$\begin{aligned} \text{Ker}(\phi) &= \{(m, k) \in \mathbb{Z} \times \mathbb{Z} \ : A^m B^k = I\} \\ &= \{m(3, 0) + k(0, 3) \ : \ m, k \in \mathbb{Z}\} \\ &= \langle (3, 0), (0, 3) \rangle = \langle 3 \rangle \times \langle 3 \rangle \end{aligned}$$

con I la matriz identidad con componentes en $\mathbb{Z}_3$. Por tanto, según el Teorema 7.2 se tiene que

$$H \cong (\mathbb{Z} \times \mathbb{Z})/(\langle 3 \rangle \times \langle 3 \rangle) \cong (\mathbb{Z}/\langle 3 \rangle) \times (\mathbb{Z}/\langle 3 \rangle) \cong \mathbb{Z}_3 \times \mathbb{Z}_3.$$

Finalmente, observe que si N y M son subgrupos normales de G y H, entonces $N \times \{1\}$ y $\{1\} \times M$ son subgrupos normales de $G \times H$. En particular, $G \cong G \times \{1\}$ y $H \cong \{1\} \times H$ son subgrupos normales de $G \times H$ y además satisfacen

$$(G \times \{1\})(\{1\} \times H) = G \times H.$$

Es decir, todo elemento de $(a, b) \in G \times H$ se puede expresar en la forma

$$(a, b) = (a, 1)(1, b).$$

7.2 Producto directo interno

En la anterior sección se estudió el producto directo externo de grupos, en el cual estos últimos pueden ser vistos como subgrupos del producto directo. Específicamente, dados los grupos G y H, el producto cartesiano $G \times H$ tiene estructura de grupo en el cual se satisface que $G \times \{1\} \cong G$ y $\{1\} \times H \cong H$. En esta sección, se analiza el problema inverso, es decir a partir de un grupo G determinar condiciones para que dos subgrupos H y K satisfagan que $G \cong H \times K$.

Definición 7.1. Sea G un grupo y sean H y K subgrupos normales de G. Entonces G es el producto directo interno de H y K si para todo elemento $g \in G$ existen únicos $h \in H$ y $k \in K$, tales que $g = hk$.

Según el ejercicio 5 de la Sección 5.4, se conoce que para subgrupos H y K de un grupo G el conjunto HK tiene estructura de grupo si y solo si $HK = KH$. Por lo cual, observe que en la definición anterior la normalidad de los subgrupos implican la condición suficiente para que el conjunto HK posea estructura de grupo.

Ejemplo 7.7. Probar que el grupo de los números complejos no cero $\mathbb{C}^*$ es el producto directo interno de los subgrupos $\mathbb{R}^+$ y $\mathbb{S}^1$ en el que

$$\mathbb{S}^1 = \{z \in \mathbb{C} \ : \ |z| = 1\}.$$

Primero note que $\mathbb{R}^+$ y $\mathbb{S}^1$ son subgrupos normales de $\mathbb{C}^*$, ya que el grupo de los números complejos distintos de cero es abeliano. Ahora, para todo $w \in \mathbb{C}^*$ se tiene que

$$w = |w|\frac{w}{|w|}$$

en el cual $|w| \in \mathbb{R}^+$ y $\dfrac{w}{|w|} \in \mathbb{S}^1$. Por otro lado, si $w = rz$ con $r \in \mathbb{R}^+$ y $z \in \mathbb{S}^1$ se tiene que $|w| = |rz| =$ y así $r = |w|$, con lo cual se garantiza la unicidad en la representación de todo $w \in \mathbb{C}^*$. Por tanto, $\mathbb{C}^*$ es el producto directo interno de los subgrupos normales $\mathbb{R}^+$ y $\mathbb{S}^1$.

Ejemplo 7.8. Probar que $G = \mathbb{Z}_6$ es el producto directo interno de dos subgrupos propios.

Considere a los subgrupos normales $H = \langle 2 \rangle$ y $K = \langle 3 \rangle$ de G. Entonces

$$0 = 0 + 0,\ 1 = 4 + 3,\ 2 = 2 + 0,\ 3 = 0 + 3,\ 4 = 4 + 0 \quad \text{y} \quad 5 = 2 + 3.$$

De donde se obtiene que $H + K = \mathbb{Z}_6$. Además, observe que dicha representación de cada elemento del grupo es única. Por tanto, $\mathbb{Z}_6$ es el producto directo interno de los subgrupos $\langle 2 \rangle$ y $\langle 3 \rangle$.

Teorema 7.3. Si H y K son subgrupos normales de un grupo G, entonces G es el producto directo interno de H y K si y solo si $G = HK$ y $H \cap K = \{1\}$.

Demostración. Suponga que G es el producto directo interno de los subgrupos normales H y K. Entonces, de acuerdo con la Definición 7.1, se tiene que $G = HK$. Por otro lado, si $g \in H \cap K$ entonces $g \cdot 1 = 1 \cdot g$ son dos representaciones distintas. Por tanto, $g = 1$ y así $H \cap K = \{1\}$.

En el otro sentido, del hecho de que $G = HK$ se obtiene $HK = KH$. Por tanto H y K son subgrupos normales G. Ahora, suponga que $h_1k_1 = h_2k_2$ con $h_1, h_2 \in H$ y $k_1, k_2 \in K$. Entonces $h_1^{-1}h_2 = k_1k_2^{-1}$, y así por hipótesis $h_1^{-1}h_2 = k_1k_2^{-1} = 1$. En consecuencia, todo elemento $g \in G$ se representa de manera única como $g = hk$ para algún $h \in H$ y $k \in K$. Es decir, G es el producto directo de H y K. □

Es importante tener en cuenta que la condición $G = HK$ en el teorema anterior, a parte de implicar que todo elemento de g es de la forma hk con $h \in H$ y $k \in K$, significar que el conjunto HK tiene estructura de grupo, ver Ejemplo 7.9.

Lema 7.1. Sea G un grupo y H, K subgrupos normales de G. Si $H \cap K = \{1\}$, entonces $hk = kh$ para todo $h \in H$ y $k \in K$.

Demostración. Para $h \in H$ y $k \in K$ considere el elemento $x = hkh^{-1}k^{-1}$. Note que la normalidad de los subgrupos implica que $hkh^{-1} \in K$ y $kh^{-1}k^{-1} \in H$. Por tanto, $x \in H \cap K$ y así $x = 1$, de lo cual se obtiene la afirmación. □

Teorema 7.4. Si G es el producto directo interno de los subgrupos normales H y K, entonces $G \cong H \times K$.

Demostración. Considere la función $\phi : H \times K \longrightarrow G$ dada por $\phi(h, k) = hk$. Para $(h_1, k_1), (h_2, k_2)$, y de acuerdo con el Teorema 7.3 y el Lema 7.1 se tiene que

$$\phi((h_1, k_1), (h_2, k_2)) = \phi(h_1h_2, k_1k_2) = h_1h_2k_1k_2 = h_1k_1h_2k_2 = \phi(h_1, k_1)\phi(h_2, k_2).$$

Por otro lado, el hecho de que $G = HK$ implica que ϕ sea sobreyectiva. Finalmente, si $(h, k) \in \text{Ker}(\phi)$, entonces $hk = 1$ y así $h = k$. Luego, por el Teorema 7.3 se tiene que $h = k = 1$, y en consecuencia $G \cong H \times K$. □

Esta sección finaliza con algunas aplicaciones del producto directo interno.

Ejemplo 7.9. Justificar porque cualquier grupo no cíclico G de orden 6 no es el producto directo interno de subgrupos no triviales de G.

Suponga que existen dos subgrupos normales H y K de G, tales que $G \cong H \times K$. Entonces por el Teorema de Lagrange se tiene que $|H| = 2$ y $|K| = 3$. Por tanto, H y K deben ser cíclicos e isomorfos a $\mathbb{Z}_2$ y $\mathbb{Z}_3$, respectivamente. De ahí que $G \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$, llegando así a una contradicción.

Ejemplo 7.10. Sea G un grupo de orden p^2 con p primo. Probar que G es isomorfo a $\mathbb{Z}_{p^2}$ o a $\mathbb{Z}_p \times \mathbb{Z}_p$.

Por el teorema 5.5, el grupo G debe ser abeliano. Para el caso en que G sea cíclico se tiene $G \cong \mathbb{Z}_{p^2}$. Caso contrario, para todo $g \in G$ con g distinto del neutro se cumple que $\text{ord}(g) = p$. Sean $a, b \in G$ distintos del neutro, tales que $b \notin \langle a \rangle$, y considere los subgrupos $H = \langle a \rangle$ y $K = \langle b \rangle$. Entonces $H \cap K = \{1\}$, y por el Ejercicio 6 de la Sección 5.4 se tiene que

$$|KH| = |HK| = \frac{|H||K|}{|H \cap K|} = p^2 = |G|.$$

Por tanto, $G = HK$. En consecuencia, $G \cong H \times K \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

7.3 Ejercicios

1. Probar que $(1, 1)$ es uno de los elementos de mayor orden en $\mathbb{Z}_r \times \mathbb{Z}_s$. Establecer un caso general.

2. Probar que $G \times H$ es abeliano si y solo si G y H son abelianos.

3. Probar que $\mathbb{Z} \times \mathbb{Z}$ no es cíclico. ¿La demostración es aplicable también para $\mathbb{Z} \times G$ cuando G es cualquier grupo con más de un elemento?

4. Dar un ejemplo de un grupo de orden 12 que contenga más de un grupo de orden 6.

5. ¿Cuántos elementos de orden 9 tiene $\mathbb{Z}_3 \times \mathbb{Z}_9$?

6. Encontrar dos subgrupos de orden 12 del grupo $\mathbb{Z}_{40} \times \mathbb{Z}_{30}$, tal que uno de ellos sea cíclico y el otro no.

7. ¿Cuántos subgrupos de orden 3 hay en $\mathbb{Z}_3 \times \mathbb{Z}_3$, y cuántos tiene $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$?

8. ¿Cuál es el orden del subgrupo cíclico más grande de $\mathbb{Z}_6 \times \mathbb{Z}_{10} \times \mathbb{Z}_{15}$?

9. ¿Cuál es el orden del subgrupo cíclico más grande de $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$?

10. Supongamos que $n_1, n_2, \ldots, n_k$ son enteros positivos pares. ¿Cuántos elementos de orden 2 tiene el grupo $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$? ¿Qué sucede si eliminamos la condición de paridad?

11. Sea p primo. Probar que $\mathbb{Z}_p \times \mathbb{Z}_p$ tiene exactamente $p+1$ subgrupos de orden p.

12. Sea I un conjunto no vacío y $\langle G_i, *_i \rangle$ un grupo para cada $i \in I$. Entonces el producto cartesiano $\Pi_{i \in I} G_i$ está formado por todas las funciones

$$f : I \longrightarrow \cup_{i \in I} G_i$$

tales que $f(i) \in G_i$. Si $f, g \in \Pi_{i \in I} G_i$, entonces $f \cdot g$ es la función dada por $(f \cdot g)(i) = f(i) *_i g(i)$. Probar que el producto cartesiano tiene estructura de grupo bajo la operación binaria definida.

13. Sean G_1 y G_2 grupos. Probar que

$$G_1 \times G_2 \cong G_2 \times G_1.$$

14. Sean $G_1, G_2, \ldots, G_n$ grupos. Probar que

$$\mathcal{Z}(G_1 \times G_2 \times \cdots \times G_n) \cong \mathcal{Z}(G_1) \times \mathcal{Z}(G_2) \times \cdots \times \mathcal{Z}(G_n).$$

15. Probar que si m y n son primos relativos, entonces $\mathrm{U}(nm) \cong \mathrm{U}(n) \times \mathrm{U}(m)$.

16. Expresar el grupo dihédrico D_5 como un producto directo interno no trivial.

CAPÍTULO 8

Grupos abelianos finitamente generados

En la actualidad se tiene un gran conocimiento de algunas estructuras algebraicas como los grupos. En este sentido, se conoce la clasificación de los grupos abelianos finitamente generados. Sin embargo, aun se desconoce una clasificación general para grupos finitos. En este capítulo se presenta una descripción completa de los grupos abelianos finitamente generados mediante el uso de elementos de Álgebra Lineal, con el fin de que los estudiantes tengan una mejor comprensión, específicamente se utiliza la forma normal de Smith de matrices con componentes enteras.

8.1 Forma normal de Smith

La forma normal de Smith de una matriz entera se puede ver como el análogo a la forma escalonada reducida en las matrices reales. Su nombre se debe a Henry John Smith,

y esta matriz es utilizada para determinar las soluciones enteras de un sistema lineal de ecuaciones diofánticas; para mayor información se puede consultar los trabajos de Bradley (1971) y Newman (1997). A lo largo de esta sección todas las matrices consideradas tienen sus componentes en el conjunto $\mathbb{Z}$ de los enteros.

Definición 8.1. Sea $D = (d_{ij})$ una matriz entera de tamaño $m \times n$. Se dice que D está en la forma normal de Smith (FNS) si satisface las siguientes condiciones

1. $d_{ij} = 0$ para todo $i \neq j$.
2. Para algún entero positivo $k \leq m$ se cumple $d_{ii} \neq 0$ para $i \leq k$ y $d_{ii} = 0$ para $i > k$.
3. Si $d_i = d_{ii}$, entonces $d_i \mid d_{i+1}$ para $i = 1, 2, \ldots, k-1$.

En Álgebra Lineal se conoce que toda matriz con componentes reales puede ser transformada en una matriz escalonada reducida, proceso denominado como el método de eliminación de Gauss-Jordán, utilizado para estudiar el conjunto solución de un sistema de ecuaciones lineales con coeficientes en el conjunto $\mathbb{R}$ de los números reales. En el proceso de eliminación de Gauss-Jordán se utilizan tres tipos de operaciones elementales. En este sentido, en el Teorema 8.1 se garantiza que toda matriz entera tiene asociada una matriz que está en la forma normal de smith, y con el fin de determinarla se utilizan tres tipos de operaciones elementales entre filas o columnas. A continuación se enumeran los tres tipos de operaciones elementales con sus respetivas notaciones.

1. Permutar dos filas (columnas). $F_i \rightleftarrows F_j \quad (C_i \rightleftarrows C_j)$.

2. Multiplicar una fila (columna) por -1. $F_i \to (-1)F_i \quad (C_i \to (-1)C_i)$.

3. Sumar a una fila (columna) un múltiplo entero de otra fila (columna). $F_i \to F_i + kF_j$ $(C_i \to C_i + kC_j)$.

Definición 8.2. Una matriz entera A se denomina equivalente a una matriz B si esta última puede obtenerse a partir de A mediante la aplicación de una secuencia finita de operaciones elementales.

Observe que cada una de las operaciones elementales tienen su operación inversa; es decir, si a una matriz A se le aplica una operación elemental con lo cual se obtiene una matriz B, entonces existe una operación elemental del mismo tipo la cual permite reducir la matriz B a la matriz A. Esto implica que si en el conjunto de las matrices de tamaño $m \times n$ se define la relación *"es equivalente a"* se obtiene una relación de equivalencia.

Proposición 8.1. Sea A una matriz entera de tamaño $m \times n$. Si A es equivalente a la matriz B, entonces existen matrices enteras invertibles P y Q de tamaños $m \times m$ y $n \times n$, respectivamente, tales que $B = PAQ$.

Demostración. Se deja como ejercicio al lector. □

Note que las matrices invertibles P y Q de la proposición anterior se originan a partir de las operaciones elementales efectuadas. Además, la matriz inversa tanto de P como de Q también son enteras.

Corolario 8.1. Sean A y B matrices enteras equivalentes de tamaño $m \times n$ y sean P y Q matrices invertibles, tal que $A = PBQ$. Si los vectores $b, c \in \mathbb{Z}^n$ satisfacen la igualdad $c = bQ^{-1}$, entonces el sistema lineal (diofántico) $xA = b$ es consistente si y solo si $yB = c$ es consistente.

Demostración. Suponga que el sistema $xA = b$ es consistente, luego existe un vector $w \in \mathbb{Z}^n$, tal que $wA = b$. Dado que $A = PBQ$, se tiene

$$\begin{aligned} wPBQ &= b \\ wPB &= bQ^{-1} \end{aligned}$$

En consecuencia, wP es una solución del sistema $yB = c$. De forma similar se justifica el recíproco y de esta forma se completa la prueba. □

Con el fin de comprender la factorización que se detalla en la proposición anterior se exponen los siguientes ejemplos.

Ejemplo 8.1. Considerar la matriz

$$A = \begin{pmatrix} 5 & 0 & 1 \\ 1 & -2 & 3 \end{pmatrix}.$$

Determinar la matriz B que se obtiene al aplicar la siguiente secuencia de operaciones elementales y hallar la secuencia de operaciones elementales (inversas) que reducen la matriz B en la matriz A.

$$F_1 \rightleftarrows F_2, \quad C_2 \to C_2 + 2C_1, \quad C_3 \to C_3 - 3C_1 \quad \text{y} \quad F_2 \to (-1)F_2.$$

Al aplicar la secuencia de operaciones elementales se obtiene

$$A = \begin{pmatrix} 5 & 0 & 1 \\ 1 & -2 & 3 \end{pmatrix} F_1 \rightleftarrows F_2 \begin{pmatrix} 1 & -2 & 3 \\ 5 & 0 & 1 \end{pmatrix} C_2 \to C_2 + 2C_1 \begin{pmatrix} 1 & 0 & 3 \\ 5 & 10 & 1 \end{pmatrix}$$
$$C_3 \to C_3 - 3C_1 \begin{pmatrix} 1 & 0 & 0 \\ 5 & 10 & -14 \end{pmatrix} F_2 \to (-1)F_2 \begin{pmatrix} 1 & 0 & 0 \\ -5 & -10 & 14 \end{pmatrix} = B$$

Según el proceso anterior, se deduce que la secuencia de operaciones elementales que reducen la matriz B en la matriz A es:

$$F_2 \to (-1)F_2, \quad C_3 \to C_3 + 3C_1, \quad C_2 \to C_2 - 2C_1 \quad \text{y} \quad F_1 \rightleftarrows F_2.$$

Ejemplo 8.2. Considerar la matriz del Ejemplo 8.1. Determinar las matrices P y Q que tratan en la Proposición 8.1 y verificar la igualdad $B = PAQ$.

Para calcular la matriz P se considera la matriz identidad de tamaño 2×2 y se le aplica únicamente las operaciones elementales ejecutadas sobre las filas de la matriz A en el mismo orden. Esto es,

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} F_1 \rightleftarrows F_2 \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} F_2 \to (-1)F_2 \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = P.$$

Con el fin de hallar la matriz Q se realiza el mismo proceso, pero con las operaciones realizadas sobre las columnas iniciando con la matriz identidad de tamaño 3×3.

$$I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} C_2 \to C_2 + 2C_1 \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} C_3 \to C_3 - 3C_1 \begin{pmatrix} 1 & 2 & -3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = Q.$$

Finalmente, note que el producto PAQ es igual a:

$$\underbrace{\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}}_{P} \underbrace{\begin{pmatrix} 5 & 0 & 1 \\ 1 & -2 & 3 \end{pmatrix}}_{A} \underbrace{\begin{pmatrix} 1 & 2 & -3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}}_{Q} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 5 & 10 & -14 \\ 1 & 0 & 0 \end{pmatrix}$$

$$= \underbrace{\begin{pmatrix} 1 & 0 & 0 \\ -5 & -10 & 14 \end{pmatrix}}_{B}.$$

Para cualquier matriz entera $A = (a_{ij})$ de tamaño $m \times n$ sea

$$d = d(A) = \text{m.c.d}\{a_{ij} \ : \ 1 \leq i \leq m, \ 1 \leq j \leq n\}.$$

Al entero positivo $d(A)$ se le denomina el máximo común divisor de la matriz A.

Lema 8.1. Si A es una matriz equivalente a B, entonces $d(A) = d(B)$.

Demostración. Note que la aplicación de cualquier operación elemental del tipo 1 o 2 implica claramente que $d(A) = d(B)$. Por otro lado, observe que si a y b son enteros, entonces $\text{m.c.d}\{a, b\} = \text{m.c.d}\{a + kb, b\}$ para todo entero k, lo cual implica que la aplicación de una operación del tercer tipo satisface que $d(A) = d(B)$. □

Teorema 8.1. Toda matriz entera A puede ser reducida a una matriz que está en forma normal de Smith.

Demostración. Sean $A = (a_{ij})$ una matriz no nula de tamaño $m \times n$ y

$$t = t(A) = \text{mín}\{|a_{ij}| \ : \ a_{ij} \neq 0, \ 1 \leq i \leq m, \ 1 \leq j \leq n\}.$$

Para determinar una FNS de la matriz se aplican los siguientes pasos.

1. Determinar el valor de $t = t(A)$ y aplicar operaciones elementales del tipo 1 o 2 con el fin de que $a_{11} = t$.

2. Si existe $a_{1l} \neq 0$ para algún $1 < l \leq n$, tal que $t \nmid a_{1l}$, entonces por el algoritmo de la división existen enteros q_l y b_{1l} tales que $a_{1l} = q_l a_{11} + b_{1l}$ con $0 < b_{1l} < a_{11}$. Entonces a la matriz A se le aplica la operación elemental $C_l \to C_l - q_l C_1$ con lo que se obtiene una matriz equivalente B. Regresar al paso 1 con la matriz B.

3. Si existe $a_{l1} \neq 0$ para algún $1 < l \leq m$, tal que $t \nmid a_{l1}$, entonces por el algoritmo de la división existen enteros q_l y b_{l1}, tales que $a_{l1} = q_l a_{11} + b_{l1}$ con $0 < b_{l1} < a_{11}$. Entonces a la matriz A se le aplica la operación elemental $F_l \to F_l - qF_1$, con lo que se obtiene una matriz equivalente B. Regresar al paso 1 con la matriz B.

4. Para cada componente a_{1l} existe un entero q_l, tal que $a_{1l} = q_l a_{11}$. A la matriz A se le aplica la operación elemental $C_l \to C_l - q_l C_1$.

5. Para cada componente a_{l1} existe un entero q_l, tal que $a_{l1} = q_l a_{11}$. A la matriz A se le aplica la operación elemental $F_l \to F_l - q_l F_1$.

Observe que el algoritmo de Euclides para calcular el máximo común divisor entre dos enteros no cero garantiza que con la aplicación de los anteriores pasos exista una matriz equivalente a la matriz A de la forma

$$B = \left(\begin{array}{c|c} t & 0 \cdots 0 \\ \hline 0 & \\ \vdots & C \\ 0 & \end{array}\right).$$

Por otro lado, si existe una componente c_{lp} de la matriz C, tal que $t \nmid c_{lp}$, entonces a la matriz B se le aplica la operación elemental $F_1 \to F_1 + F_l$ y se aplican de nuevo los pasos descritos anteriormente a la nueva matriz. El Lema 8.1 y este proceso lleva a obtener una

matriz de la forma

$$\left(\begin{array}{c|c} d & 0\cdots 0 \\ \hline 0 & \\ \vdots & E \\ 0 & \end{array}\right)$$

en la cual $d = d(A)$. En consecuencia, aplicando el procedimiento anterior de manera consecutiva se obtiene una FNS de A. □

El Teorema 8.1 garantiza la existencia de una FNS para toda matriz entera A, además es posible probar que esta FNS es única, consultar el Corolario 1.20 de Norman (2012).

Ejemplo 8.3. Hallar la FNS de la matriz

$$A = \begin{pmatrix} 5 & 0 & 1 \\ 1 & -2 & 3 \end{pmatrix}.$$

Primero observe que $1 = d(A)$, y al seguir el algoritmo planteado en la demostración del Teorema 8.1 se obtiene

$$A = \begin{pmatrix} 5 & 0 & 1 \\ 1 & -2 & 3 \end{pmatrix} F_1 \rightleftarrows F_2 \begin{pmatrix} 1 & -2 & 3 \\ 5 & 0 & 1 \end{pmatrix} \begin{array}{l} C_2 \to C_2 + 2C_1 \\ C_3 \to C_3 - 3C_1 \end{array}$$
$$\begin{pmatrix} 1 & 0 & 0 \\ 5 & 10 & -14 \end{pmatrix} F_2 \to F_2 - 5F_1 \begin{pmatrix} 1 & 0 & 0 \\ 0 & 10 & -14 \end{pmatrix}$$

Según el algoritmo planteado en el Teorema 8.1 se aplica nuevamente el procedimiento a la submatriz $(10 \ \ -14)$ con lo que se obtiene

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 10 & -14 \end{pmatrix} C_3 \to C_3 + 2C_2 \begin{pmatrix} 1 & 0 & 0 \\ 0 & 10 & 6 \end{pmatrix} C_2 \rightleftarrows C_3 \begin{pmatrix} 1 & 0 & 0 \\ 0 & 6 & 10 \end{pmatrix}$$
$$C_3 \to C_3 - C_2 \begin{pmatrix} 1 & 0 & 0 \\ 0 & 6 & 4 \end{pmatrix} C_2 \rightleftarrows C_3 \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 6 \end{pmatrix} C_3 \to C_3 - C_2$$
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 2 \end{pmatrix} C_2 \rightleftarrows C_3 \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 4 \end{pmatrix} C_3 \to C_3 - 2C_2 \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix}.$$

Por tanto, la matriz

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

es la FNS de la matriz A.

8.2 Clasificación

Finalmente en esta sección se presenta la clasificación de los grupos abelianos finitamente generados.

Proposición 8.2. Sea n un entero positivo. Cada subgrupo de $\mathbb{Z}^n$ es finitamente generado por a lo más n generadores.

Demostración. La prueba se desarrolla por inducción sobre n. Según el Teorema 4.1 todo subgrupo de $\mathbb{Z}$ es cíclico, lo cual garantiza el caso base. Suponga que la afirmación se cumple para todo subgrupo de $\mathbb{Z}^{n-1}$ y sea H un subgupo de $\mathbb{Z}^n$. Considere el homomorfismo de grupos $\pi : H \longrightarrow \mathbb{Z}$ dado por $\pi(x_1, x_2, \ldots, x_n) = x_1$. Si $\pi(H) = \{0\}$ entonces por la hipótesis de inducción H es finitamente generado. Caso contrario, según el Corolario 6.1 la imagen $H_1 = \pi(H)$ es un subgrupo (no cero) de $\mathbb{Z}$ por lo cual existe un entero positivo d_1, tal que $H_1 = \langle d_1 \rangle$. Ahora, para $h_1 = (d_1, a_2, \ldots, a_n) \in H$ se considera el subgrupo de H dado por

$$H' = \{(kd_1, x_2, \ldots, x_n) - k(d_1, a_2, \ldots, a_n) \ : \ k \in \mathbb{Z}, \ (kd_1, x_2, \ldots, x_n) \in H\}.$$

Observe que la primera componente de cada elemento de H' es igual a 0, por lo cual este subgrupo es isomorfo a un subgrupo de $\mathbb{Z}^{n-1}$. Esto implica, de acuerdo con la hipótesis de inducción, que H' es finitamente generado; es decir

$$H' = \langle h_2, \ldots, h_r \rangle$$

para algunos $h_2, \ldots, h_r \in H'$ y $r \leq n - 1$. Por tanto,

$$H = \langle h_1, h_2, \ldots, h_r \rangle.$$ □

Teorema 8.2. Si K es un subgrupo de $\mathbb{Z}^n$, entonces

$$K \cong \langle d_1 \rangle \times \cdots \times \langle d_k \rangle$$

para algunos enteros positivos d_i, tales que $d_i \mid d_{i+1}$ para todo $i = 1, 2, \ldots, k - 1$.

Demostración. Por la Proposición 8.2 existen elementos $k_1, k_2, \ldots, k_m \in \mathbb{Z}^n$, con $m \leq n$, tales que

$$K = \langle k_1, k_2, \ldots, k_m \rangle = \{xA \ : \ x \in \mathbb{Z}^m\} = \{b \in \mathbb{Z}^n \ : \ xA = b \text{ es consistente}\}$$

en el que la i-ésima fila de A es k_i. Si D es la FNS de la matriz A, entonces por la Proposición 8.1 existen matrices enteras invertibles P y Q, tales que

$$A = PDQ.$$

Considere el subgrupo H de $\mathbb{Z}^n$ dado por

$$H = \{yD \ : \ y \in \mathbb{Z}^m\} = \{c \in \mathbb{Z}^n \ : \ yD = c \text{ es consistente}\}.$$

Sea $\phi : K \longrightarrow H$ la función dada por $\phi(b) = bQ^{-1}$. Note que el Corolario 8.1 muestra que ϕ está bien definida y claramente es un homomorfismo de grupos. Puesto que

$$\text{Ker}(\phi) = \{b \in \mathbb{Z}^n \ : \ bQ^{-1} = 0\} = \{0\}$$

se obtiene que ϕ es inyectiva. Por otro lado, note que para $c \in \mathbb{Z}^n$, tal que el sistema lineal $yD = c$ es consistente con solución y_0, se cumple que $x_0 = y_0P^{-1}$ es solución del sistema lineal $xA = cQ$. Luego $cQ \in K$ y además $\phi(cQ) = c$. Por tanto, ϕ es un isomorfismo y así $K \cong H$.

Finalmente, como $D = (d_{ij})$ es la FNS de la matriz A se tiene que existen enteros positivos $d_1, d_2, \ldots, d_k$, tales que $d_i \mid d_{i+1}$ para $i = 1, 2, \ldots, k-1$, con $k \leq m$. En consecuencia,

$$K \cong H \cong \langle d_1 \rangle \times \cdots \times \langle d_k \rangle.$$ □

Teorema 8.3 (Clasificación de grupos abelianos finitamente generados)**.** Si G es un grupo abeliano finitamente generado, entonces existen enteros positivos $d_1, d_2, \ldots, d_k$, tales que $d_i \mid d_{i+1}$ para $i = 1, 2, \ldots, k$, y

$$G \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_k} \times \mathbb{Z}^r$$

para algún entero no negativo r.

Demostración. Dado que G es abeliano y finitamente generado, se tiene que

$$G = \langle g_1, g_2, \ldots, g_m \rangle = \left\{ g_1^{x_1} g_2^{x_2} \cdots g_m^{x_m} \ : \ x_i \in \mathbb{Z} \right\},$$

para algunos $g_1, g_2, \ldots, g_m \in G$. Además, la función $\phi : \mathbb{Z}^m \longrightarrow G$ definida por

$$\phi(x) = \phi(x_1, x_2, \ldots, x_m) = g_1^{x_1} g_2^{x_2} \cdots g_m^{x_m}$$

es un homomorfismo de grupos. Note que ϕ es sobreyectiva, por lo cual el Teorema 6.3 implica que

$$\mathbb{Z}^m / \text{Ker}(\phi) \cong G.$$

Finalmente, se conoce que el kernel de ϕ es un subgrupo de $\mathbb{Z}^m$, de ahí que el Teorema 8.2 garantiza la existencia de enteros positivos $d_1, d_2, \ldots, d_k$, tales que $d_i \mid d_{i+1}$ para $i = 1, 2, \ldots, k-1$ y

$$\text{Ker}(\phi) \cong \langle d_1 \rangle \times \cdots \times \langle d_k \rangle.$$

Por tanto, del Teorema 7.2 se obtiene

$$\mathbb{Z}^m/\langle d_1\rangle \times \cdots \times \langle d_k\rangle \times \{0\}^{m-k} \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_k} \times \mathbb{Z}^{m-k} \cong G. \qquad \square$$

Observe que los elementos de un grupo abeliano G de orden finito conforman un subgrupo de G. A este grupo, denotado por

$$T(G) = \{g \in G \ : \ \text{ord}(g) \text{ es finito}\}$$

se le denomina el grupo de Torsión de G. En este sentido, si G es abeliano finitamente generado, entonces a los enteros positivos $d_1, d_2, \ldots, d_k$ del Teorema 8.3 se les denomina los coeficientes de torsión de G y a r el número de Betti de G.

Corolario 8.2. Cada grupo abeliano finito G es isomorfo al producto directo de grupos cíclicos, es decir

$$G \cong \mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \cdots \times \mathbb{Z}_{p_r^{n_r}}$$

en el cual los p_i son primos no necesariamente distintos y los n_i son enteros positivos.

Demostración. Observe que si G es abeliano finito, entonces por el Teorema 8.3

$$G \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_k}.$$

Para cada coeficiente de torsión se considera su descomposición prima

$$d_i = q_{i1}^{s_1} q_{i2}^{s_2} \cdots q_{il}^{s_l}$$

y en consecuencia,

$$\mathbb{Z}_{d_i} \cong \mathbb{Z}_{q_{i1}^{s_1}} \times \mathbb{Z}_{q_{i2}^{s_2}} \times \cdots \times \mathbb{Z}_{q_{il}^{s_l}}.$$

Por tanto, la afirmación es clara. $\square$

Ejemplo 8.4. Utilizar la forma normal de Smith para probar que

$$(\mathbb{Z}/\langle 2\rangle) \times (\mathbb{Z}/\langle 3\rangle) \cong (\mathbb{Z}/\langle 6\rangle).$$

Sea H el subgrupo de $\mathbb{Z}^2$ generado por $(2,0)$ y $(0,3)$. Es decir,

$$H = \langle (2,0),(0,3)\rangle = \{x(2,0) + y(0,3) \ : \ x, y \in \mathbb{Z}\}.$$

Considere la matriz entera

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}.$$

De acuerdo con los Teoremas 8.2 y 8.3 se busca la FNS de A. En este sentido se tiene

que

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} F_1 \to F_1 + F_2 \begin{pmatrix} 2 & 3 \\ 0 & 3 \end{pmatrix} C_2 \to C_2 - C_1 \begin{pmatrix} 2 & 1 \\ 0 & 3 \end{pmatrix}$$
$$\rightleftarrows \begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix} C_2 \to C_2 - 2C_1 \begin{pmatrix} 1 & 0 \\ 3 & -6 \end{pmatrix} F_2 \to F_2 - 3F_1 \begin{pmatrix} 1 & 0 \\ 0 & -6 \end{pmatrix}$$
$$F_2 \to (-1)F_2 \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix} = D.$$

En consecuencia, $H \cong \mathbb{Z} \times \langle 6 \rangle$ y por tanto

$$(\mathbb{Z}/\langle 2 \rangle) \times (\mathbb{Z}/\langle 3 \rangle) \cong \mathbb{Z}^2/H \cong \mathbb{Z}^2/(\mathbb{Z} \times \langle 6 \rangle) \cong \mathbb{Z}/\langle 6 \rangle.$$

Ejemplo 8.5. Determinar los coeficientes de torsión y el número de Betti del grupo abeliano finitamente generado definido por

$$H = \langle a, b, c \ : \ a^3 b^4 c^{-5} = 1, \ a^7 c^9 = 1 \rangle.$$

Según la demostración del Teorema 8.3 se tiene que

$$\mathbb{Z}^2/K \cong H$$

con $K = \langle (3, 4, -5), (7, 0, 9) \rangle$. Considere la matriz entera dada por

$$A = \begin{pmatrix} 3 & 4 & -5 \\ 7 & 0 & 9 \end{pmatrix}.$$

Entonces, según los Teoremas 8.2 y 8.3 se busca la FNS de A. Por tanto, se tiene

$$A = \begin{pmatrix} 3 & 4 & -5 \\ 7 & 0 & 9 \end{pmatrix} \begin{matrix} C_2 \to C_2 - C_1 \\ C_3 \to C_3 + 2C_1 \end{matrix} \begin{pmatrix} 3 & 1 & 1 \\ 7 & -7 & 23 \end{pmatrix} C_1 \rightleftarrows C_2 \begin{pmatrix} 1 & 3 & 1 \\ -7 & 7 & 23 \end{pmatrix}$$
$$\begin{matrix} C_2 \to C_2 - 3C_1 \\ C_3 \to C_3 - C_1 \end{matrix} \begin{pmatrix} 1 & 0 & 0 \\ -7 & 28 & 30 \end{pmatrix} F_2 \to F_2 + 7F_1 \begin{pmatrix} 1 & 0 & 0 \\ 0 & 28 & 30 \end{pmatrix}$$
$$C_3 \to C_3 - C_2 \begin{pmatrix} 1 & 0 & 0 \\ 0 & 28 & 2 \end{pmatrix} C_2 \rightleftarrows C_3 \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 28 \end{pmatrix}$$
$$C_3 \to C_3 - 14C_2 \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix} = D.$$

En consecuencia, $K \cong \mathbb{Z} \times \langle 2 \rangle$, y así

$$H \cong \mathbb{Z}^2/(\mathbb{Z} \times \langle 2 \rangle) \cong \mathbb{Z}_2.$$

Luego, el único coeficiente de torsión de H es 2 y su número de Betti es 0.

Ejemplo 8.6. Determinar todos los grupos abelianos (salvo isomorfismo) de orden 12.

Dado que $12 = 2^2\ 3$, por el Corolario 8.2, los únicos subgrupos de orden 12 son:

- $\mathbb{Z}_{12}$.
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$.
- $\mathbb{Z}_2 \times \mathbb{Z}_6$.

8.3 Ejercicios

1. Determinar la forma normal de Smith D de la matriz

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix}$$

y determinar matrices enteras invertibles P y Q, tales que $A = PDQ$.

2. Determinar la forma normal de Smith D de la matriz

$$A = \begin{pmatrix} 0 & 2 & 2 & 2 \\ -6 & 8 & 8 & 2 \\ -6 & 4 & 4 & -2 \end{pmatrix}$$

y determinar matrices enteras invertibles P y Q, tales que $A = PDQ$.

3. Para cada una de las matrices de los literales 1 y 2 determinar todas las soluciones enteras del sistema lineal homogéneo $AX = 0$.

4. Determinar los coeficientes de torsión y el número de Betti del grupo abeliano finitamente generado definido por

$$H = \langle a, b, c \ : \ ab^3c = a^3bc^3 = ab^3c^5 = 1 \rangle.$$

5. Determinar los coeficientes de torsión y el número de Betti del grupo abeliano finitamente generado definido por

$$H = \langle a, b, c \ : \ a^2b^4c^6 = a^8b^{10}c^{12} = a^{14}b^{16}c^{18} = 1 \rangle.$$

6. Determinar los coeficientes de torsión y el número de Betti del grupo abeliano finitamente generado definido por

$$H = \langle a, b, c \ : \ a^4b^{-1}c^5 = a^{14}b^7c^7 = 1 \rangle.$$

7. Determinar los coeficientes de torsión de los grupos

   a) $\mathbb{Z}_4 \times \mathbb{Z}_9$.

   b) $\mathbb{Z}_6 \times \mathbb{Z}_{12} \times \mathbb{Z}_{20}$.

8. Determinar los coeficientes de torsión y el número de Betti del grupo

$$\mathbb{Z}_{20} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}_{15} \times \mathbb{Z}_6.$$

9. Determinar todos los grupos (salvo isomorfismo) de orden 100.

10. Determinar si los grupos $\mathbb{Z}_4 \times \mathbb{Z}_{18} \times \mathbb{Z}_{15}$ y $\mathbb{Z}_3 \times \mathbb{Z}_{36} \times \mathbb{Z}_{10}$ son isomorfos.

11. Determinar si los grupos $\mathbb{Z}_8 \times \mathbb{Z}_{10} \times \mathbb{Z}_{24}$ y $\mathbb{Z}_4 \times \mathbb{Z}_{12} \times \mathbb{Z}_{40}$ son isomorfos.

Notación

$\mathbb{N}$	Conjunto de los números naturales
$\mathbb{Z}$	Conjunto de los números enteros
$\mathbb{Q}$	Conjunto de los números racionales
$\mathbb{R}$	Conjunto de los números reales
$\mathbb{C}$	Conjunto de los números complejos
$[a]$	Clase de equivalencia del elemento a
$X \setminus Y$	Elementos del conjunto X que no pertenecen al conjunto Y
$[m, n]$	Conjunto de los enteros x tales que $m \leq x \leq n$
φ	Función indicatriz de Euler
$H \leq G$	H es un subgrupo del grupo G
$\langle a \rangle$	Subgrupo cíclico generado por el elemento a
$\lvert G \rvert$	Orden del grupo G
$\text{ord}(a)$	Orden del elemento a
$\lvert z \rvert$	Norma del número complejo z
$\mathcal{Z}(G)$	Centro del grupo G
$C(a)$	Centralizador de un elemento a
$\text{m.c.m}\{m, n\}$	Mínimo común multiplo de los enteros m y n
$\text{m.c.d}\{m, n\}$	Máximo común divisor de los enteros m y n
$\langle S \rangle$	Subgrupo de un grupo G generado por el subconjunto S
$[H : G]$	Índice del subgrupo H en el grupo G
$H \triangleleft G$	H es un subgrupo normal del grupo G

Bibliografía

Ameta, R. y Ameta, S. (2016). *Chemical Applications of Symmetry and Group Theory*. Apple Academic Press Inc.

Ayres, F. y Jaisingh, L. R. (2004). *Theory and problems of abstract algebra*. McGraw-Hill.

Beshenov, A. (25 de enero de 2023). *Homomorfismo de grupos*. Medio. https://cadadr.org/teaching/san-salvador/algebra/2018/5-homomorfismos.pdf.

Bradley, G. H. (1971). Algorithms for hermite and smith normal matrices and linear diophantine equations. *Mathematics of Computation*, 25(116):897–907.

Conrad, K. (19 de octubre de 2022). *Dihedral Groups*. Medio. https://kconrad.math.uconn.edu/blurbs/grouptheory/dihedral.pdf.

Dummit, D. S. y Foote, R. M. (1991). *Abstract algebra*. Prentice Hall, 3rd edition edición.

Escribano, C. (15 de marzo de 2019). *Relaciones de equivalencia y aplicaciones*. Medio. https://www.cartagena99.com/recursos/alumnos/apuntes/.

Gallian, J. (2017). *Contemporary abstract algebra*. Cengage Learning, ninth edition edición.

Gonzáles, F. J. (20 de marzo de 2019). *Relaciones de equivalencia*. Medio. https://docplayer.es/23917721-Apuntes-de-matematica-discreta-8-relaciones-de-equivalencia.html.

Ikenaga, B. (17 de junio de 2022b). *Normal Subgroups and Quotient Groups*. Medio. https://sites.millersville.edu/bikenaga/abstract-algebra-1/normal-subgroups/normal-subgroups.pdf.

Ikenaga, B. (9 de noviembre de 2022a). *Cyclic Groups*. Medio. https://sites.millersville.edu/bikenaga/abstract-algebra-1/cyclic-groups/cyclic-groups.pdf.

Judson, T. W. y Austin, S. F. (2020). *Abstract Algebra: Theory and Applications*. EBooks.

Lezama, O. (15 de marzo de 2019). *Cuadernos de álgebra: Grupos*. Medio. https://sites.google.com/a/unal.edu.co/sac2/cuadernos-de-algebra.

Marklof, J. (25 de enero de 2023). *Group theory (course notes)*. Medio. https://people.maths.bris.ac.uk/~majm/bib/talks/grouptheory.pdf.

Myasnikov, A., Ushakov, A., y Shpilrain, V. (2008). *Group-based Cryptography*. Birkhäuser Basel.

Newman, M. (1997). The smith normal form. *Linear Algebra and its Applications*, 254(1):367–381. Proceeding of the Fifth Conference of the International Linear Algebra Society.

Norman, C. (2012). *Finitely Generated Abelian Groups and Similarity of Matrices over a Field*. Springer Undergraduate Mathematics Series. Springer London.

Olazábal, J. M. D. (20 de abril de 2019). *Grupo Dihédrico*. Medio. https://personales.unican.es/olazabaj/Docencia/T_Grupos/Apuntes/diedricos.pdf.

Revilla, F. (15 de marzo de 2019). *Relación de equivalencia y conjunto cociente*. Medio. https://fernandorevilla.es/2014/02/03/relacion-de-equivalencia-conjunto-cociente/.

Smith, K. (26 de enero de 2023). *Homomorphisms of groups*. Medio. https://dept.math.lsa.umich.edu/~kesmith/Homomorphism-ANSWERS.pdf.

Tang, D., Wang, Z., y Yue, B. (2022). Applications of group theory. *Journal of Physics: Conference Series*, 2381(1):012110.

Villarreal, R. (30 de enero de 2023). *Aplicaciones de la Forma Normal de Smith de una Matriz Entera*. Medio. https://docplayer.es/31031678-Aplicaciones-de-la-forma-normal-de-smith-de-una-matriz-entera.html.

Acerca de los autores

Fernando Andrés Benavides Agredo

Matemático de la Universidad del Cauca. Realizó estudios de Maestría en Matemáticas en la Universidad de Antioquia y Doctorado en Ciencias Matemáticas en la Universidad Nacional Autónoma de México. Actualmente es profesor asociado adscrito al Departamento de Matemáticas y Estadística de la Universidad de Nariño, prestando sus servicios principalmente en la Licenciatura en Matemáticas. En su trayectoria como docente investigador se ha desempeñado como miembro del Comité Organizador de las Olimpiadas Regionales de Matemáticas de la Universidad de Nariño, y forma parte del Grupo de Investigación en Algebra, Teoría de Números y Aplicaciones: ERM.

Wilson Fernando Mutis Cantero

Licenciado en Matemáticas de la Universidad del Cauca. Realizó estudios de Maestría en Matemáticas en la Universidad de Antioquia y Doctorado en Ciencias Matemáticas en la Universidad de Sao Paulo, Brasil. Actualmente es profesor asociado adscrito al Departamento de Matemáticas y Estadística de la Universidad de Nariño, prestando sus servicios principalmente en la Licenciatura en Matemáticas, y es miembro del Grupo de Investigación en Algebra, Teoría de Números y Aplicaciones: ERM.

Índice de figuras y tablas

Editorial
Universidad de **Nariño**

Fecha de publicación: abril de 2024
San Juan de Pasto - Nariño - Colombia

En algebra abstracta, el área de la teoría de grupos se encarga de estudiar aquellas estructuras algebraicas conocidas como *Grupos*, las cuales son básicamente un conjunto no vacío en el que se define una operación binaria que satisface algunas propiedades axiomáticas. En el mundo real estamos rodeados de una gran variedad de dichas estructuras, por este motivo, su estudio es de gran importancia para áreas como la Física, Química, Criptografía, entre otras. En el texto **Teoría Básica de Grupos** se introduce al lector desde los conceptos básicos de la teoría de conjuntos hasta finalizar con la clasificación de una clase importante de grupos, los abelianos finitamente generados.

El presente texto está dividido en ocho capítulos distribuidos de la siguiente manera. En el Capítulo 1, se presentan conceptos elementales de relaciones, funciones y operaciones binarias. En el 2, se define formalmente el concepto de Grupo, y se presentan algunas propiedades importantes. En los Capítulos 3 y 4, se presentan algunas clases particulares de grupos como son los grupos de permutaciones, cíclicos y finitamente generados. Con el fin de estudiar en más detalle este tipo de estructura, en el Capítulo 4 se introducen aquellos subgrupos denominados normales. En el Capítulo 6, se define un tipo importante de función denominado *homomorfismo*, el cual permite clasificar muchos de los grupos básicos conocidos. En el 7, se construyen nuevos tipos de grupos con los cuales, finalmente, en el Capítulo 8 se presenta la clasificación de los grupos abelianos finitamente generados.

ISBN: 978-628-7679-49-8

Universidad de Nariño
FUNDADA EN 1904

Universidad de Nariño
ACREDITADA EN ALTA CALIDAD
RESOLUCIÓN MEN 000003 - ENERO 11 DE 2023

Universidad de Nariño

Editorial
Universidad de Nariño