Capítulo

2

Grupos

2.1 Introducción

La estructura de grupo es una de las más comunes en toda la matemática pues aparece en forma natural en muchas situaciones, donde se puede definir una operación sobre un conjunto. Por ser tan simple en su definición, el concepto de grupo se puede considerar como punto de partida para el estudio de otras estructuras algebraicas más complicadas, como son los cuerpos y los anillos.

Muchos objetos matemáticos provenientes de áreas tan disímiles como la Geometría Analítica, la Combinatoria, el Análisis Complejo, la Topología, etc, tienen incorporados la estructura de grupo, aunque esto pase desapercibido para muchos de nosotros. Existen grupos finitos de cualquier tamaño, grandes o pequeños; de estructura muy simple, como los grupos cíclicos o bastantes complicados, como los grupos de simetrías; grupos infinitos con uno o varios generadores, o bien infinitos sin una base finita.

También se pueden crear nuevos grupos, usando los anteriores, por medio de ciertas operaciones entre ellos. Esto, por supuesto, puede hacer pensar al lector que el estudio de la teoría de grupos es una tarea abrumadora, dada la gran cantidad de grupos que intervienen.

Sin embargo existe una relación muy útil que podemos construir entre dos grupos, lo cual permite comparar la estructura de ambos sin hacer consideraciones acerca de la naturaleza misma de los elementos. Este concepto, que juega un papel central dentro de toda esta teoría, es el de isomorfismo de grupos. Si dos grupos son isomorficos, entonces desde el punto de vista del álgebra son casi iguales: esto es, poseen la misma estructura.

Los grupos aparecieron un poco tarde en la historia de las matemáticas, aproximadamente a mediados del siglo XIX.

El concepto de operación binaria o ley de composición interna aparece por vez primera en la obra del matemático alemán C. F. Gauss en relación a un trabajo sobre composición de formas cuadráticas del tipo:

$$f(x, y) = ax^2 + bxy + cy^2$$

con coeficientes enteros.

Gauss da una definición de equivalencia de formas cuadráticas, y luego define una operación de multiplicación de formas, y posteriormente demuestra que esta multiplicación es compatible con la relación de equivalencia.

También Gauss y algunos de sus predecesores en el campo de la Teoría de Números, como Euler y Lagrange habían estudiado las propiedades de suma y multiplicación de los enteros módulo p, con p primo.

Pero fue el genio de Evariste Galois quien dio inicio a la moderna teoría de grupos, al exponer en sus brillantes trabajos la relación entre las ecuaciones algebraicas y el grupo de permutaciones de las raíces. Galois fue el primero que destacó la importancia de los subgrupos normales y estudió en detalle las propiedades abstractas de los grupos.

La definición general de grupo, fue dada por Cayley en 1854. Pero es a partir de 1880 cuando comienza a desarrollarse la teoría general de los grupos finitos con los trabajos de S. Lie, Felix Klein y Henry Poincaré.

2.2 Definiciones Básicas

Definición 2.2.1 *Sea A un conjunto no vacío. Una* **operación binaria en A** *es una función del producto cartesiano $A \times A$ en A.*

Así pues una operación binaria sobre el conjunto A asigna a cada par de elementos (a, b) en $A \times A$ un tercer elemento en A, el cual se denota con algún símbolo especial, por ejemplo $a * b$.

El símbolo que se utiliza para la operación no reviste mucha importancia en si mismo. Lo pertinente es saber que hay un elemento de A, resultado de aplicar la operación a los elementos a y b, el cual estamos denotando por $a*b$. Podemos usar otras notaciones como ab, $a \cdot b$, $a \triangle b$, ..., etc. siempre que no halla confusión.

El elemento $a * b$ será llamado el "producto de a con b".

Ejemplo 1: Sea $A = \{a, b, c\}$ y definamos la operación $*$ en A de la forma siguiente

$$\begin{aligned}(a,a) &\longrightarrow a\\ (a,b) &\longrightarrow a\\ (a,c) &\longrightarrow a\\ (b,a) &\longrightarrow b\\ (b,b) &\longrightarrow b\\ (b,c) &\longrightarrow b\\ (c,a) &\longrightarrow c\\ (c,b) &\longrightarrow c\\ (c,c) &\longrightarrow c\end{aligned}$$

En realidad se ha podido definir la operación en forma más concisa, haciendo

$$(x,y) \longrightarrow x \quad \forall (x,y) \in A \times A$$

o bien

$$x * y = x \quad \forall x, y \in A$$

Ejemplo 2: Definiremos una nueva operación en A, pero esta vez por intermedio de una tabla. La operación la denotamos por $\odot$. El producto $x \odot y$ aparece en la casilla correspondiente a la columna x y la fila y.

$\odot$	a	b	c
a	a	c	a
b	c	a	b
c	b	b	c

Nótese que por ejemplo el producto de a con c es b, mientras que el producto de c con a es a. Luego para esta operación se tiene:

$$a \odot c \neq c \odot a$$

También se puede observar que:

$$(a \odot c) \odot b = b \odot b = a$$

y

$$a \odot (c \odot b) = a \odot b = c$$

luego

$$a \odot (c \odot b) \neq (a \odot c) \odot b$$

Definición 2.2.2 *Sea A un conjunto en donde esta definida una operación binaria $*$. Diremos que la operación es* **asociativa**, *si y sólo si*

$$x * (y * z) = (x * y) * z \tag{2.1}$$

para todo x, y, z en A.

Ejemplo: Sea $A = \{a, b, c\}$, y $*$ la operación $*$ definida en A, en el ejemplo 1. Esta operación es asociativa.

En efecto, si $x, y, z \in A$, se tendrá entonces:

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

luego será cierto que:

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

para todo x, y, z en A.

Definición 2.2.3 *Sea A un conjunto en donde esta definida una operación binaria $*$, y sea S un subconjunto de A. Diremos que S* **es cerrado** *bajo la operación $*$, si se cumple:*

$$x * y \in S \quad \textit{para todo } x, y \text{ en } S.$$

Nota: Cuando $S = A$ se dice que la operación es cerrada.

Ejemplo 1: Sea $\mathbb{Z}^+$ el conjunto de los números enteros positivos y consideremos la operación suma de números enteros, la cual denotamos por "+", como es costumbre. Entonces, si S es el conjunto de los números pares, se tiene que S es cerrado bajo la suma.

Ejemplo 2: Sea $\mathbb{Z}$ el conjunto de enteros, con la operación resta de enteros "$-$". Si $S = \mathbb{Z}^+$ el conjunto de enteros positivos, entonces S no es cerrado bajo la resta.

Por ejemplo 6 y 9 están en S y sin embargo $6 - 9 = -3$ no está en S.

Definición 2.2.4 *Sea A un conjunto no vacío en donde se define una operación binaria $*$. Diremos que A es un* **semigrupo** *con la operación $*$, si la operación es asociativa y cerrada.*

Denotaremos por $(A, *)$ al semigrupo formado por el conjunto A con la operación $*$. Algunas veces se utiliza simplemente la letra A, para denotar este semigrupo, por abuso de notación.

Ejemplo 1: $(\mathbb{Z}, +)$ es un semigrupo.

Ejemplo 2: $(\mathbb{Z}^+, +)$ es un semigrupo.

Definición 2.2.5 *Sea A un conjunto, con operación binaria $*$. Un elemento $e \in A$ que satisface:*

$$a * e = e * a = a \quad \textit{para todo } a \text{ en } A,$$

se llama **elemento neutro** *de A, para la operación $*$.*

Ejemplo 1: Sea $A = \{a, b, c\}$ y $*$ la operación

$$x * y = x \quad \text{para todo } x, y \text{ en } A.$$

Entonces A no posee elemento neutro.

Ejemplo 2: Sea $\mathbb{Z}$ el conjunto de los enteros con la operación de suma. Entonces el 0 es un elemento neutro, pues

$$n + 0 = 0 + n = n \quad \text{para todo } n \text{ entero.}$$

Ejemplo 3: Sea A un conjunto no vacío y consideremos $P(A)$ el conjunto formado por todos los subconjuntos de A. Entonces podemos definir la operación binaria en $P(A)$, dada por la unión de conjuntos. Luego el conjunto $\emptyset$, es el elemento neutro de $P(A)$, pues

$$B \cup \emptyset = \emptyset \cup B = B \quad \text{para todo } B \text{ subconjunto de } A.$$

Definición 2.2.6 *Sea $(A, *)$ un semigrupo. Entonces si A posee un elemento neutro, diremos que $(A, *)$ es un* **monoide**.

Ejemplo 1: $(\mathbb{Z},+)$ es un monoide.

Ejemplo 2: Si A es cualquier conjunto, entonces $(P(A), \cup)$ es un monoide, donde $\cup$ denota la operación de unión de conjuntos.

2.3 Grupos

Definición 2.3.1 *Un* **grupo** *es un conjunto no vacío G en donde hay definida una operación binaria $\cdot$, llamada producto, la cual satisface:*

1. *$a \cdot b \in G$ para todo $a, b \in G$.*
2. *$a \cdot (b \cdot c) = (a \cdot b) \cdot c$ para todo $a, b, c \in G$ (Ley Asociativa).*

3. *Existe un elemento $e \in G$, llamado elemento neutro o identidad de la operación, el cual satisface:*

$$a \cdot e = e \cdot a = a,$$

para todo $a \in G$.

4. *Para todo a en G, existe un elemento $a^{-1} \in G$, llamado el inverso de a, el cual satisface:*

$$a \cdot a^{-1} = a^{-1} \cdot a = e.$$

Definición 2.3.2 *Si el conjunto G es finito, entonces G se dice* **grupo finito**. *Caso contrario, diremos que G es infinito.*

Definición 2.3.3 *El orden de grupo es el cardinal del conjunto G.*

Notación: Usamos la notación de potencias en G.

$$\begin{aligned} e &= a^0 \\ a &= a^1 \\ a^2 &= a \cdot a \\ &\vdots \\ a^{n+1} &= a^n \cdot a \end{aligned}$$

Definición 2.3.4 *Un grupo G se dice* **abeliano** *o* **conmutativo**, *si*

$$a \cdot b = b \cdot a \quad \text{para todo } a, b \in G.$$

Ejemplo 1: $(\mathbb{Z},+)$ los números enteros con la suma es un grupo abeliano.

Ejemplo 2: Sea $A = \{a,\ b,\ c\}$ y consideremos en este conjunto la operación $*$ definida por la tabla siguiente:

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

Mostraremos que $(A, *)$ es un grupo, para lo cual probaremos que se verifican las cuatro condiciones de la definición.

En primer lugar, la operación es cerrada, pues al multiplicar dos elementos de A se obtiene otro elemento de A.

También observamos que el elemento a sirve de elemento neutro para esta operación, pues $x * a = a * x = x$, para todo x en A.

Además, todo elemento de A posee inverso. En efecto, se tienen las relaciones

$$a * a = a, \quad b * c = c * b = a$$

luego $a^{-1} = a,\ b^{-1} = c,\ c^{-1} = b$.

Solo resta probar la asociatividad de esta operación. Esto no se puede deducir directamente de la tabla y debe hacerse caso por caso. Aceptando que la operación es asociativa, se tiene entonces que $(A, *)$ es un grupo. Finalmente se demuestra que este grupo es abeliano a partir de relaciones:

$$a * b = b * a, \ \ a * c = c * a, \ \ b * c = c * b.$$

Nótese que la tabla de esta operación es simétrica respecto de la diagonal. Esto es otra indicación de que el grupo es abeliano.

Ejemplo 3: Sea $G = Z \times Z$ el producto cartesiano de Z consigo mismo, cuyos elementos son las parejas ordenadas de números enteros (m, n). Podemos definir una operación en este conjunto mediante:

$$(m_1, n_1) \oplus (m_2, n_2) = (m_1 + m_2, n_1 + n_2),$$

donde $+$ denota la suma de números enteros.

Entonces probaremos que G satisface todas las propiedades de la definición de grupo.

Claramente la operación es cerrada, pues la suma de enteros es cerrada y por lo tanto el par $(m_1 + m_2, n_1 + n_2)$ esta en G.

Probaremos que $\oplus$ es asociativa, para lo cual usaremos la asociatividad de los números enteros. En efecto, se tiene

$$\begin{aligned}(m_1, n_1) \oplus [(m_2, n_2) \oplus (m_3, n_3)] &= (m_1, n_1) \oplus [(m_2 + m_3, n_2 + n_3)] \\ &= (m_1 + (m_2 + m_3), n_1 + (n_2 + n_3)) \\ &= ((m_1 + m_2) + m_3), (n_1 + n_2) + n_3) \\ &= ((m_1 + m_2), (n_1 + n_2)) \oplus (m_3, n_3) \\ &= [(m_1, n_1) \oplus (m_2, n_2)] \oplus (m_3, n_3)\end{aligned}$$

También se demuestra que $(0, 0)$ es el elemento neutro para esta suma. Sea (m, n) un elemento cualquiera en G, luego

$$(0, 0) + (m, n) = (m, n) + (0, 0) = (m, n).$$

Finalmente se deduce que todo elemento (m, n) de G posee un inverso, el cual viene dado por $(-m, -n)$ pues

$$(m, n) \oplus (-m, -n) = (m - m, n - n) = (0, 0)$$

$$(-m, -n) \oplus (m, n) = (-m + m, -n + n) = (0, 0)$$

Por lo tanto G es un grupo. Además este grupo es abeliano, pues para todo par de elementos (m_1, n_1) y (m_2, n_2) en G se tiene

$$\begin{aligned}(m_1, n_1) \oplus (m_2, n_2) &= (m_1 + m_2, n_1 + n_2) \\ &= (m_2 + m_1, n_2 + n_1) \\ &= (m_2, n_2) \oplus (m_1, n_1)\end{aligned}$$

Ejemplo 4: Sea S un conjunto finito y $A(S)$ el conjunto de todas las aplicaciones biyectivas de S en si mismo. Entonces definimos una

operación binaria en este conjunto por medio de la composición de aplicaciones. Entonces se puede verificar que $A(S)$ con esta operación es un grupo, basándonos en los siguientes hechos, muy bien conocidos, sobre funciones:

1. La composición de dos aplicaciones biyectivas, es biyectiva.
2. La composición de aplicaciones es asociativa.
3. La aplicación identidad

$$I : A \longrightarrow A$$

$$x \longrightarrow x$$

   es biyectiva
4. Si una aplicación f es biyectiva, entonces su inversa f^{-1} existe y es biyectiva.

Observación Cuando S es un conjunto finito, entonces $A(S)$ es también finito. Además, si S tiene n elementos, entonces $|A(S)| = n!$. (ver problema 9)

Ejemplo 5: Sea $S = \{x_1, x_2, x_3\}$ y G el grupo de aplicaciones biyectivas de S en si mismo. Este grupo se denomina **grupo de permutaciones de** S y se denota por S_3.

Definamos las aplicaciones:

$$\phi : \begin{array}{l} x_1 \longrightarrow x_2 \\ x_2 \longrightarrow x_1 \\ x_3 \longrightarrow x_3 \end{array}$$

$$\psi : \begin{array}{l} x_1 \longrightarrow x_2 \\ x_2 \longrightarrow x_1 \\ x_3 \longrightarrow x_1 \end{array}$$

Sabemos que G tiene 6 elementos. Calcularemos todos los elementos de G y construiremos una tabla para la operación binaria $\cdot$ de composición.

Nota: Usaremos la convención

$$\sigma \cdot \tau = \text{ primero aplicar } \sigma \text{ y luego } \tau$$

También si $s \in S$ y $\sigma \in A(S)$, usaremos la notación $s \cdot \sigma = \sigma(s)$.

Tenemos entonces

$$\phi \cdot \psi : \begin{array}{l} x_1 \longrightarrow x_3 \\ x_2 \longrightarrow x_2 \\ x_3 \longrightarrow x_1 \end{array}$$

$$\psi \cdot \phi : \begin{array}{l} x_1 \longrightarrow x_1 \\ x_2 \longrightarrow x_3 \\ x_3 \longrightarrow x_2 \end{array}$$

Observamos que $\phi \cdot \psi \neq \psi \cdot \phi$ y por lo tanto G no es abeliano.
Calcularemos ahora todas las potencias de los elementos ϕ y ψ

$$\phi^2 : \begin{array}{l} x_1 \longrightarrow x_1 \\ x_2 \longrightarrow x_2 \\ x_3 \longrightarrow x_3 \end{array}$$

luego $\phi^2 = 1$, identidad. Por otra parte:

$$\psi^2 : \begin{array}{l} x_1 \longrightarrow x_3 \\ x_2 \longrightarrow x_1 \\ x_3 \longrightarrow x_2 \end{array}$$

y

$$\psi^3 : \begin{array}{l} x_1 \longrightarrow x_1 \\ x_2 \longrightarrow x_2 \\ x_3 \longrightarrow x_3 \end{array}$$

luego $\psi^3 = 1$, identidad.

Notemos que

$$\psi \cdot \phi = \phi \cdot \psi^2$$

Mediante esta relación, podemos escribir todos los elementos de G en la forma: $\phi^i \cdot \psi^j$, con $0 \leq i$, $0 \leq j$.

Entonces los seis elementos del grupo G son

$$1,\ \psi,\ \psi^2,\ \phi,\ \phi\psi,\ \phi\psi^2.$$

Seguidamente, construiremos una tabla de multiplicación para G.

$\cdot$	1	ψ	ψ^2	ϕ	$\phi\psi$	$\phi\psi^2$
1	1	ψ	ψ^2	ϕ	$\phi\psi$	$\phi\psi^2$
ψ	ψ	ψ^2	1	$\phi\psi$	$\phi\psi^2$	ϕ
ψ^2	ψ^2	1	ψ	$\phi\psi^2$	ϕ	$\phi\psi$
ϕ	ϕ	$\phi\psi^2$	$\phi\psi$	1	ψ^2	ψ
$\phi\psi$	$\phi\psi$	ϕ	$\phi\psi^2$	ψ	1	ψ^2
$\phi\psi^2$	$\phi\psi^2$	$\phi\psi$	ϕ	ψ^2	ψ	1

El grupo G se denomina **grupo simétrico** de grado 3, y lo denotaremos por S_3.

Dejaremos como un ejercicio para el lector, la verificación de cada uno de los productos en la tabla anterior.

Ejemplo 6: Sea n un entero y a un símbolo. Construimos un conjunto G cuyos elementos son los n símbolos

$$a^0 = e,\ a,\ a^2, \ldots, a^{n-1}$$

Definimos un producto en G mediante la siguiente regla de multiplicación:

$$a^i a^j = \begin{cases} a^{i+j}, & \text{si} \quad i+j \leq n \\ a^{i+j-n}, & \text{si} \quad n < i+j \end{cases}$$

Se puede verificar entonces que G con esta operación es un grupo. Este grupo se denota por C_n y se llama **grupo cíclico de orden** n**.**

Ejemplo 7: Sea S el conjunto de los enteros y $A(S)$ el conjunto de las aplicaciones biyectivas de $\mathbb{Z}$ en si mismo. Sea $G \subseteq A(S)$ el conjunto de aquellas aplicaciones que mueven un número finito de elementos.

Esto es, $\sigma \in G$ sí y sólo si

$$A = \{x | \sigma(x) \neq x\}$$

es finito. Entonces G es un grupo (Verificarlo!).

Ejemplo 8: Sea G el conjunto de matrices 2×2 de la forma:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

donde a, b, c, d son números reales y $ad - bc \neq 0$. Podemos dotar a G de una operación binaria, dada por la multiplicación de matrices, la cual se define mediante:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x & y \\ w & z \end{pmatrix} = \begin{pmatrix} ax + bw & ay + bz \\ cx + dw & cy + dz \end{pmatrix}$$

Notemos que

$$\begin{aligned} (ax + bw)(cy + dz) - (cx + dw)(ay + bz) &= acxy + adxz + \\ & \quad bcwy + bdwz - acxy - \\ & \quad bcxz - dawy - bdwz \\ &= xz(ad - bc) \end{aligned}$$

$$\begin{aligned} & +wy(bc-da) \\ = \; & (xz-wy)(ad-bc) \\ \neq \; & 0 \end{aligned}$$

Luego G es cerrado bajo esta operación.

También la matriz

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

actua como la identidad, y además I está en G.

Finalmente si

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G,$$

entonces $ad - bc \neq 0$, luego la matriz

$$B = \begin{pmatrix} \dfrac{d}{ad-bc} & \dfrac{-b}{ad-bc} \\ \dfrac{-c}{ad-bc} & \dfrac{a}{ad-bc} \end{pmatrix}$$

es real y además es un elemento de G, pues

$$\frac{ad-bc}{(ad-bc)^2} = \frac{1}{ad-bc} \neq 0$$

También se puede verificar que

$$A \cdot B = I$$

Luego G es un grupo. Este grupo se llama **grupo lineal de** $\mathbb{R}^2$ y se denota por $L_2(\mathbb{R})$.

Ejemplo 9: Sea G el Conjunto de matrices 2×2 de la forma

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

donde a, b, c y d son números reales y $ad-bc = 1$. Se puede ver entonces que G es un grupo.

Ejercicios

1) Sea $A = \{a, b, c\}$ con la operación $\oplus$ dada por la siguiente tabla

$\oplus$	a	b	c
a	a	b	c
b	b	c	a
c	c	c	a

Hallar un elemento identidad para A.
¿Es $(A, \oplus)$ un semigrupo?
¿Es $(A, \oplus)$ un monoide?

2) Sea A cualquier conjunto y $\cap$, la intersección de conjuntos en $P(A)$. Demuestre que $(P(A), \cap)$ es un monoide.

3) Demuestre que todo grupo de 3 elementos debe ser abeliano.

4) Demuestre que todo grupo G, en donde se tiene la relación: $a^2 = e$, para todo $a \in G$, debe ser abeliano.

5) Demuestre que $A(S)$, el conjunto de todas las aplicaciones biyectivas de S en si mismo es un grupo.

6) Demuestre que la resta de números enteros no es una operación asociativa.

7) Para cada una de las operaciones siguientes, definidas en los números enteros $\mathbb{Z}$, responder las siguientes interrogantes

a) ¿Es asociativa? b) ¿Es cerrada?
c) ¿Hay elemento neutro? d) ¿Es conmutativa?

1) $a * b = a * b + 1$
2) $a * b = \max\{a, b\}$
3) $a * b = \min\{a, b\}$
4) $a * b = 2ab$

5) $a * b = (ab)^2$
6) $a * b = a$

8) Si G es un grupo finito, probar que existe un entero positivo t, tal que $a^t = e$, para todo a en G.

9) Probar que si S es un conjunto con n elementos, entonces $A(S)$ posee $n!$ elementos.

10) Probar que el conjunto de matrices reales 2×2 con determinante no nulo, es un grupo bajo la multiplicación de matrices.

11) Probar la propiedad asociativa para el grupo $L_2(\mathbb{R})$.

12) Probar que el grupo $L_2(\mathbb{R})$ no es abeliano.

13) Sea A el conjunto formado por todas las funciones $f : [0, 1] \longrightarrow \mathbb{R}$. Probar que $(A, +)$ es un grupo, donde $+$ es la operación de suma de funciones.

14) Construya todas las posibles tablas de multiplicación para un grupo de orden 4.

15) Demuestre que el conjunto de los números racionales distintos de cero forman un grupo bajo el producto.

16) Demuestre que el grupo $(Z, +)$ no tiene subgrupos finitos.

17) Demuestre que el grupo $(Q, +)$ no tiene subgrupos finitos.

18) Sea Q^* el conjunto de los números racionales distintos de cero. Probar que $(Q^*, .)$ es un grupo.

19) Hallar un subgrupo finito dentro de $(Q^*, .)$.

20) Probar, mediante el principio de inducción, la existencia y unicidad de las potencias positivas de un elemento a, dentro de un grupo G.

2.4 Simetrías

Una **simetría** de una figura plana es un movimiento rígido del plano que hace coincidir dicha figura consigo misma. Todo movimiento rígido del plano tiene la propiedad de conservar las distancias y por esto se le

da el nombre de **isometría**. El estudio de las simetrías es una de las relaciones mas interesantes que se conocen entre álgebra y geometría.

Comenzaremos por estudiar el **grupo de simetrías del cuadrado**. Para facilitar el estudio de este grupo, tome un pedazo de papel o cartulina en forma de cuadrado y numere los vértices por ambos lados de acuerdo con la figura

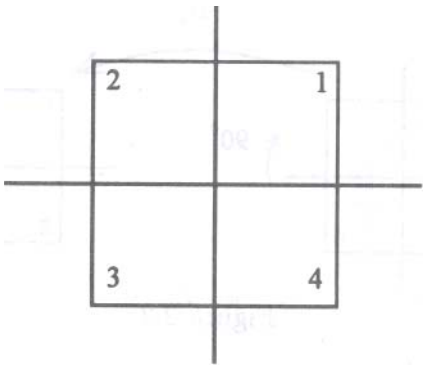


Figura 2.1:

Coloque el cuadrado sobre un sistema de ejes perpendiculares con su centro en el punto de corte de los ejes y lados paralelos a los ejes.

El eje horizontal lo llamamos **X** y al vertical lo llamamos **Y**.

Comenzamos ahora nuestro trabajo, considerando todos los posibles movimientos del cuadrado que lo hagan coincidir consigo mismo. Este se puede mover deslizándose sobre el plano y también está permitido levantarlo y voltearlo al revés (Recuérdese que los vértices han sido marcados por ambos lados).

Podemos decir en primer lugar que el cuadrado tiene **simetría rotacional**, pues cada rotaci6n de 90° con eje de rotación en el origen, no altera la figura. Estas rotaciones, por conveniencia, serán realizadas en sentido contrario a las agujas del reloj. Podemos denotarlas por

R_l - Rotación de 90°

$R2$	-	Rotación de	180°
$R3$		Rotación de	270°
I		Rotación de	360°

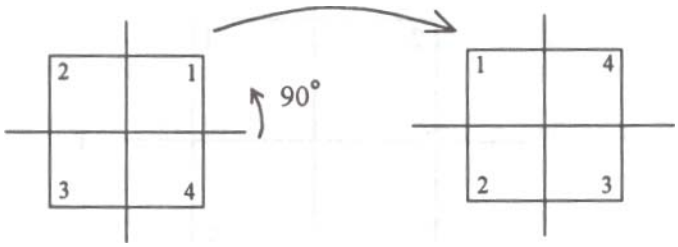


Figura 2.2:

También el cuadrado se puede hacer girar 180º sobre un eje que puede ser el eje X, o bien el eje Y, o bien un eje diagonal que pase por dos vértices. Estos movimientos también son simetrías, pues no se altera la figura del cuadrado al ejecutarlos. Estas **simetrías, llamadas simetrías axiales, producen** el mismo efecto que la reflexión sobre un espejo colocado sobre un eje de simetría. Ver la figura.

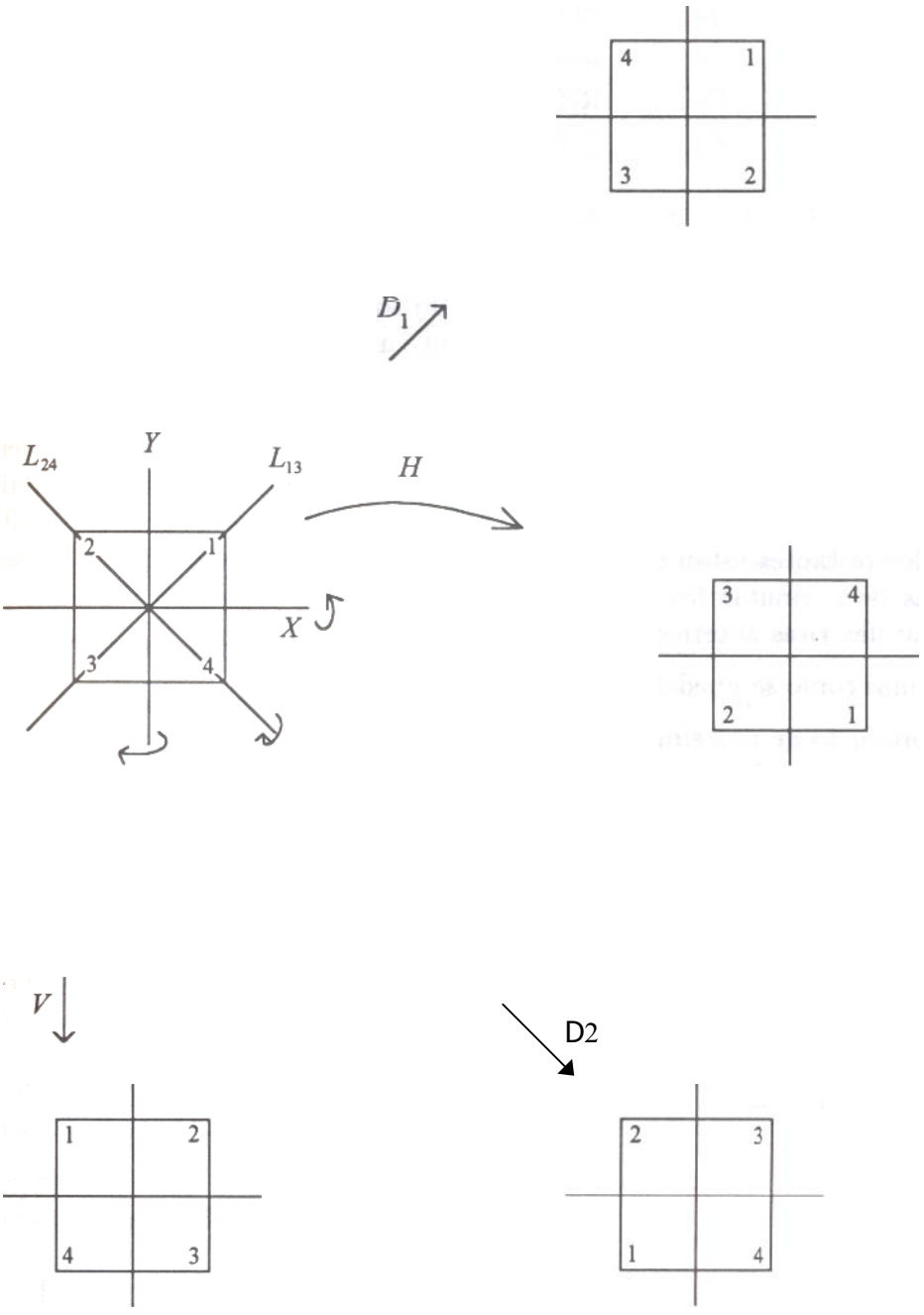


Figura 2.3:

Tendremos entonces

H -	Reflexión alrededor del eje	X
V -	Reflexión alrededor del eje	Y
D_1 -	Reflexión alrededor del eje	L_{13}
D_2 -	Reflexión alrededor del eje	L_{24}

Estas 8 simetrías del cuadrado son todas las posibles. Cualquiera otra simetría necesariamente induce una permutación sobre los vértices.

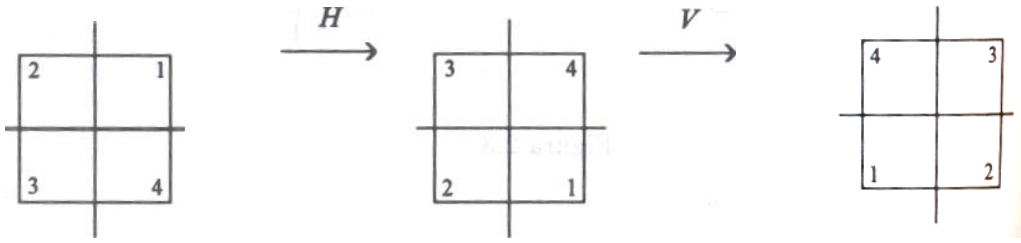
Al mover el cuadrado cada vértice debe ir sobre otro. Para el vértice 1 tenemos 4 posibilidades. Una vez fijado el primer vértice, se tienen dos posibilidades de ubicar el vértice 2. Al estar fijados los vértices 1 y 2, los restantes están determinados, luego hay 4 x 2 = 8 posibles maneras de permutar los vértices, lo cual equivale a los 8 tipos de simetrías descritas anteriormente.

Veamos como se pueden multiplicar las simetrías entre si.

El producto de una simetría A_1 por otra simetría A_2, denotado por A_1A_2, consiste en efectuar el movimiento del cuadrado determinado por A1, seguido del movimiento dado por A_2.

Así por ejemplo, para calcular HV, reflejamos el cuadrado sobre el eje horizontal y seguidamente lo reflejamos sobre el eje vertical. Esto produce el mismo efecto que hacer una rotación del cuadrado de 180° (Ver la figura).

Figura 2.4:



Luego $HV = R_2$.

El producto de dos simetrías da como resultado otra simetría de las ya descritas. Podemos calcular todos los posibles productos para estar seguro de ello.

También el producto de simetrías es asociativo por lo siguiente. Si se tiene A_1, A_2 y A_3 tres simetrías, entonces podemos multiplicarlas de dos maneras distintas. En primer lugar si movemos el cuadrado ejecutando en sucesión A_1 y A_2 obtendremos otra simetría B. Entonces movemos nuevamente el cuadrado para ejecutar A_3. El resultado obtenido será igual a

$$(A_1A_2)A_3$$

Por otro lado, podríamos haber efectuado en sucesión las simetrías A_2 y A_3 para obtener una simetría C. Luego llevamos el cuadrado a la posición original y desde allí efectuamos A_1 seguida de C. El resultado será igual a

$$A_1(A_2A_3)$$

Es fácil ver entonces que

$$(A_1A_2)A_3 = A_1(A_2A_3)$$

Antes de calcular todos los productos de simetrías en una tabla, veamos como se obtienen algunas relaciones interesantes entre ellas.

En primer lugar observamos que todas las rotaciones se obtienen como potencias de R_1

$$\begin{aligned} R_1 &= R_1 \\ R_1^2 &= R_2 \\ R_1^3 &= R_3 \\ R_1^4 &= I \end{aligned} \tag{2.2}$$

También se demuestra que toda reflexión es igual al producto de H por alguna rotación

$$\begin{aligned} H &= H \\ V &= HR_1^2 \\ D_1 &= HR_1 \\ D_2 &= HR_1^3 \end{aligned} \tag{2.3}$$

Para calcular cualquier producto de simetrías, necesitamos la relación

$$R_1 H = D_2 = HR_1^3 \tag{2.4}$$

Vemos que en general este producto no es conmutativo, pues $R_1 H \neq HR_1$.

Teniendo todos estos elementos a la mano, pasamos a construir la tabla de esta operación.

$\cdot$	I	R_1	R_1^2	R_1^3	H	HR_1	HR_1^2	HR_1^3
I	I	R_1	R_1^2	$R_1^3 H$	H	R_1	HR_1^2	HR_1^3
R_1	R_1	R_1^2	R_1^3	I	HR_1	HR_1^2	HR_1^3	H
R_1^2	R_1^2	R_1^3	I	R_1	HR_1^2	HR_1^3	H	HR_1
R_1^3	R_1^3	I	R_1	R_1^2	HR_1^3	H	HR_1	HR_1^2
H	H	HR_1^3	HR_1^2	HR_1	I	R_1^3	R_1^2	R_1
HR_1	HR_1	H	HR_1^3	HR_1^2	R_1	I	R_1^3	R_1^2
HR_1^2	HR_1^2	HR_1	H	HR_1^3	R_1^2	R_1	I	R_1^3
HR_1^3	HR_1^3	HR_1^2	HR_1	H	R_1^3	R_1^2	R_1	I

Podemos extraer muchas conclusiones importantes al observar esta tabla. En primer lugar el elemento I actúa como elemento neutro. También todo elemento posee inverso bajo este producto, pues el elemento I aparece en cada una de las columnas.

Por el momento queda demostrado que el conjunto de todas las simetrías del cuadrado es un grupo con la operación producto de simetrías. Este grupo de orden 8, no es abeliano. De ahora en adelante lo llamaremos **Grupo de simetrías del cuadrado**.

Podemos dar una formulación completamente abstracta de este grupo, sin hacer referencia a los movimientos rígidos de un cuadrado. El lector estará, de acuerdo en que el grupo que definiremos a continuación
y el anterior tienen la misma tabla de multiplicación y por lo tanto la misma estructura.

Definición 2.4.1 El grupo diédrico de orden 4 *es aquel cuyos elementos son los símbolos* $a^i\ b^i$, *con* $i = 0, 1,\ \ j = 0, 1, 2, 3$ *y la operación de multiplicación, dada por las relaciones*

$$a^2 = e, \quad b^4 = e, \quad ba = ab3$$

Este grupo se denota por D_4.

Aparte de las simetrías del cuadrado, podemos construir simetrías de otro tipo de figuras planas.
Por ejemplo la figura plana

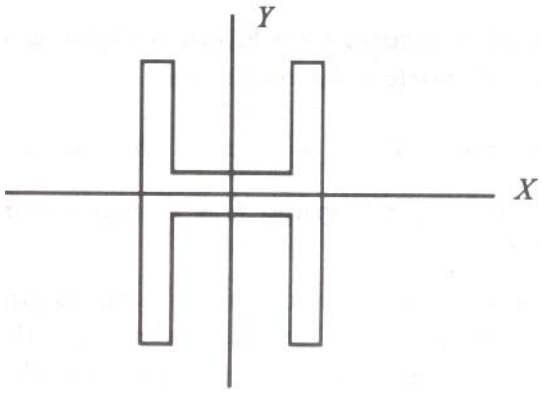


Figura 2.5:

Tiene las siguientes simetrías

$$\begin{array}{lll} H & \text{- reflexión en el eje} & X \\ V & \text{- reflexión en el eje} & Y \\ R & \text{- rotación de} & 180^\circ \end{array}$$

Estos tres elementos satisfacen las relaciones

$$H^2 = V^2 = R^2 = I$$

La tabla de multiplicación es la siguiente

$\cdot$	I	H	V	R
I	I	H	V	R
H	H	I	R	V
V	V	R	I	H
R	R	V	H	I

Este grupo de simetrías, que llamaremos **grupo H**, se puede definir en abstracto usando solamente las relaciones de multiplicación entre sus elementos.

Definición 2.4.2 *El* **grupo** 4 **de Klein** *se define como el conjunto de símbolos* $\{I, a, b, c\}$ *sujeto a las relaciones*

$$a^2 = b^2 = c^2 = I \quad , \quad ab = c \quad , \quad bc = a \quad , \quad ca = b$$

Es claro entonces que el grupo H y el grupo 4 de Klein tienen la misma estructura.

La idea de relacionar grupos de simetría con las propiedades geométricas de las figuras planas se debe al matemático alemán Felix Klein $(1849-1925)$, en su famoso trabajo sobre geometría llamado Programa de Erlangen, el cual fue publicado en 1872.