Apuntes de Estructuras Algebraicas

Versión del 11 de enero de 2024

Víctor Andrés Osores Escalona
Departamento de Matemática, Física y Estadística
Universidad Católica del Maule, Chile

Índice general

Prefacio

Este libro es el resultado de una recopilación de recursos disponibles en la red. A lo largo de su proceso de escritura, he consultado una variedad de fuentes en línea, desde documentos académicos hasta tutoriales y ejemplos prácticos. Quiero enfatizar que la base de conocimiento en la que se sustenta este libro es el resultado de la generosidad de la comunidad en línea y de aquellos que han compartido su experiencia y conocimientos libremente.

Agradezco profundamente a todas las personas que han contribuido a la creación de este apunte a través de su valiosa información disponible en la red. Sin su generosidad y el espíritu colaborativo de la era digital, este documento no habría sido posible.

CAPÍTULO 1

Preliminares

1.1 Los enteros

En el conjunto de los números enteros, $\mathbb{Z}$, las operaciones de adición y multiplicación verifican las siguientes propiedades:

Para todo $a, b, c \in \mathbb{Z}$:

1. $(a+b)+c = a+(b+c)$ y $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
2. $a+b = b+a$ y $a \cdot b = b \cdot a$
3. $a \cdot (b+c) = a \cdot b + a \cdot c$ y $(a+b) \cdot c = a \cdot c + b \cdot c$
4. $a+0 = a$ y $a \cdot 1 = a$
5. existe $(-a) \in \mathbb{Z}$ tal que $a+(-a) = 0$.
6. $a \cdot b = 0 \Leftrightarrow a = 0 \vee b = 0$. (Sin divisores de cero)

El número entero $a+(-b)$ se escribe $a-b$.

Se define en $\mathbb{Z}$ la relación $<$ por:

$$a < b \Leftrightarrow (b-a) \in \mathbb{N},$$

$a < b$ se lee: "a menor que b". Esta relación satisface:

$$a < b \Rightarrow a+c < b+c, \text{ para todo } c \in \mathbb{Z}$$
$$a < b \Rightarrow a \cdot c < b \cdot c, \text{ para todo } c \in \mathbb{N}$$

La relación en $\mathbb{Z}$:

$$a \leq b \Leftrightarrow a < b \vee a = b,$$

es un *orden* (reflexiva, antisimétrica y transitiva) *total*.

Se supone, como un axioma, que el conjunto $\mathbb{N}$ verifica el *Principio de buen orden*.

Axioma 1 (**Principio de buen orden**) *Todo subconjunto no vacío S de $\mathbb{N}$ tiene un primer elemento (esto es, existe $b \in S$ tal que $b \leq c$ para todo $c \in S$).*

También se tiene:

Teorema 1.1.1 (**Principio de inducción matemática**) *Si $S \subseteq \mathbb{N}$, $1 \in S$ y se cumple al menos una de las condiciones*

(i) $\forall n, n \in S \Rightarrow n+1 \in S$

(ii) $\forall n, \{1, 2, \ldots, n\} \in S \Rightarrow n+1 \in S$

entonces $S = \mathbb{N}$.

Teorema 1.1.2 (**Algoritmo de división**) *Si $a, b \in \mathbb{Z}$ y $a \neq 0$, entonces existen únicos enteros q y r tales que*

$$b = a \cdot q + r \quad y \quad 0 \leq r < |a|.$$

Definición 1.1.1 *Se dice que un entero a, $a \neq 0$, divide a un entero b, se escribe $a \mid b$, si existe un entero k tal que $b = a \cdot k$. Si a no divide a b se escribe $a \nmid b$.*

Definición 1.1.2 *El entero positivo c se dice el máximo común divisor de los enteros $a_1, a_2, \ldots, a_n$ si:*

i) $c \mid a_i$ *para* $1 \leq i \leq n$.

ii) $d \in \mathbb{Z}$ *y* $d \mid a_i$ *para* $1 \leq i \leq n \Rightarrow d \mid c$.

c se denota $(a_1, a_2, \ldots, a_n)$.

Teorema 1.1.3 *Si $a_1, a_2, \ldots, a_n$ son enteros, no todos nulos, entonces $(a_1, a_2, \ldots, a_n)$ existe. Además, existen enteros $k_1, k_2, \ldots, k_n$ tales que*

$$(a_1, a_2, \ldots, a_n) = k_1 a_1 + k_2 a_2 + \ldots + k_n a_n.$$

Definición 1.1.3 *Se dice que los enteros $a_1, a_2, \ldots, a_n$ son primos relativos si $(a_1, a_2, \ldots, a_n) = 1$.*

Definición 1.1.4 *Un entero positivo $p > 1$ es primo si sus únicos divisores son ± 1 y $\pm p$.*

Definición 1.1.5 *Si a y b son primos relativos y $a \mid b \cdot c$, entonces $a \mid c$. Si p es primo y $p \mid a_1 \cdot \ldots \cdot a_n$ entonces $p \mid a_i$ para algún i.*

Teorema 1.1.4 (**Teorema Fundamental de la Aritmetica**) *Todo entero positivo $n > 1$ se puede escribir en forma única como*

$$n = p_1^{t_1} \cdot \ldots \cdot p_k^{t_k},$$

donde $p_1 < p_2 < \ldots p_k$ son primos y $t_i > 0$ para todo i.

CAPÍTULO 2

Teoría de Grupos

2.1 Definición, propiedades elementales y ejemplos de grupos

Definición 2.1.1 (**Grupo**) *El conjunto G provisto de la operación binaria interna (o ley de composición) $\bar{\wedge} : G \times G \to G$, se llama grupo si:*

G1) $\forall a, b, c \in G$: $(a \,\bar{\wedge}\, b) \,\bar{\wedge}\, c = a \,\bar{\wedge}\, (b \,\bar{\wedge}\, c)$.

G2) Existe $e \in G$ tal que

$$\forall a \in G : \; a \,\bar{\wedge}\, e = e \,\bar{\wedge}\, a = a.$$

G3) Para cada $a \in G$ existe $a' \in G$ tal que

$$a \,\bar{\wedge}\, a' = a' \,\bar{\wedge}\, a = e.$$

A $G1$ se le llama *ley asociativa* de $\bar{\wedge}$. $G2$ indica la existencia de un elemento neutro para la operación $\bar{\wedge}$ y $G3$ indica que cada elemento $a \in G$ posee un *elemento simétrico* a'.

Si además, en la definición anterior se verifica

G4) $\forall a, b \in G : a \,\bar{\wedge}\, b = b \,\bar{\wedge}\, a$,

se dice que el grupo G es *abeliano* o *conmutativo*.

Observaciones:

1. Se escribirá $(G, \bar{\wedge})$ para indicar que G es un grupo bajo la operación $\bar{\wedge}$.
2. Generalmente se usará la notación multiplicativa $(\cdot)$ o aditiva $(+)$ para la operación $\bar{\wedge}$, prefiriéndose $+$ en los grupos abelianos.
3. El elemento neutro $e \in G$ se escribirá 1 o 0 (1_G o 0_G) según se use la notación multiplicativa o aditiva, respectivamente.

En la siguiente proposición se dan algunas propiedades elementales de un grupo.

Proposición 2.1.1 *Sea $(G, \bar{\wedge})$ un grupo. Se tiene:*

(i) Existe único elemento neutro para $(G, \bar{\wedge})$.

(ii) Cada elemento $a \in G$ admite único simétrico.

(iii) Valen las leyes de cancelación:

$$\forall a, b, x \in G : a \,\bar{\wedge}\, x = b \,\bar{\wedge}\, x \Rightarrow a = b \quad \textit{(a derecha)}$$

$$\forall a, x, y \in G : a \,\bar{\wedge}\, x = a \,\bar{\wedge}\, y \Rightarrow x = y \quad \textit{(a izquierda)}$$

(iv) Las ecuaciones en x, $a \,\bar{\wedge}\, x = b$ y $x \,\bar{\wedge}\, c = d$ tienen solución única, a saber $x = a' \,\bar{\wedge}\, b$ y $x = d \,\bar{\wedge}\, c'$ respectivamente.

2.1.1 Ejemplos de grupos

Ejemplo 2.1.1 *$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{R}^+, \cdot)$ y $(\mathbb{C} - \{0\}, \cdot)$ son grupos abelianos.*

Ejemplo 2.1.2 *$C = \{z : z \in \mathbb{C} \wedge |z| = 1\}$ con el producto de números complejos es un grupo abeliano.*

Ejemplo 2.1.3 *$GL(n, \mathbb{R}) = \{A : A$ es matriz $n \times n$ sobre $\mathbb{R}$, invertible $\}$ es grupo bajo la multiplicación de matrices. Se llama grupo lineal de orden n sobre $\mathbb{R}$. No es abeliano si $n \geq 2$*

Ejemplo 2.1.4 *Para $N \in \mathbb{N}, C_N = \left\{z \in \mathbb{C} : z^N = 1\right\}$ es un grupo bajo la multiplicación de números complejos.*

Proposición 2.1.2 *Sea $(G, \bar{\wedge})$ un grupo y $a \in G$. Se tiene que $(a')' = a$.*

Dem: *Sea $\tilde{a}$ el inverso de a', luego $\tilde{a} \bar{\wedge} a' = e$. Por otro lado $a \bar{\wedge} a' = e$. Luego $\tilde{a} \,\bar{\wedge}\, a' = e = a \,\bar{\wedge}\, a'$. Finalmente usando la ley de cancelación por la derecha obtenemos $\tilde{a} = a$, es decir $(a')' = a$.*

Proposición 2.1.3 *En un grupo $(G, \bar{\wedge})$ se tiene que $(a \,\bar{\wedge}\, b)' = b' \,\bar{\wedge}\, a'$ para todo $a, b \in G$.*

Proposición 2.1.4 *Sea $(G, \bar{\wedge})$ un grupo. Las siguientes propiedades son equivalentes:*

i) $(G, \bar{\wedge})$ es abeliano.

ii) $(a \,\bar{\wedge}\, b)' = a' \,\bar{\wedge}\, b'$ para todo $a, b \in G$.

2.1.2 Orden de un grupo

Se llama *orden* o *cardinalidad* de un conjunto A al número de elementos que posee A. Este número puede ser finito o infinito.

El *orden* de un conjunto A se denota por cualquiera de los símbolos: $|A|$, $\text{card}(A)$.

Si $f : A \to B$ es *biyección*, entonces $|A| = |B|$.

Existe una aritmética para estos números, en la cual:

i) $A \cap B = \phi \Rightarrow |A \cup B| = |A| + |B|$.

ii) $|A \times B| = |A| \cdot |B|$.

El *orden* del grupo $(G, \bar{\wedge})$ se define como el *orden* del conjunto G. Los grupos finitos pueden definirse totalmente mediante tablas, de manera que el resultado de operar dos elementos a y b del grupo se posiciona en la intersección de la fila de a con la columna de b.

2.1.3 Grupos finitos y tablas de grupo

Puesto que un grupo debe tener al menos un elemento (e), el conjunto más pequeño que puede dar lugar a un grupo es el conjunto $\{e\}$. La única operación binaria $\bar{\wedge}$ posible en $\{e\}$ es tal que $e \bar{\wedge} e = e$. El elemento identidad siempre es su propio inverso.

Veamos si podemos construir un Grupo de dos elementos. Uno de los elementos debe desempeñar el papel de identidad, digamos que el conjunto es $G = \{e, a\}$. Busquemos una tabla para una operación binaria interna $\bar{\wedge}$ de manera que $(G, \bar{\wedge})$ sea un grupo.

$\bar{\wedge}$	e	a
e	e	a
a	a	e

La tabla anterior satisface todos los axiomas de grupo, excepto, quizá, la ley asociativa (corroborar todos los casos).

Condiciones que una tabla que defina una operación binaria interna sobre un conjunto finito debe satisfacer, para dotarlo de una estructura de grupo.

1. Es necesario que algún elemento del conjunto, que denotaremos por e, actúe como identidad o neutro.

2. La condición $e \bar{\wedge} x = x$ significa que la fila de la tabla que contiene a e en el extremo izquierdo, debe contener exactamente los elementos que aparecen arriba de la tabla y en el mismo orden.

3. La condición $x \bar{\wedge} e = x$ significa que la columna de la tabla bajo e, debe contener los elementos que aparecen en el extremo izquierdo, en el mismo orden.

4. El hecho de que cada elemento a tenga un inverso ($a \barwedge a' = a' \barwedge a = e$), quiere decir que en la fila frente a a debe aparecer el elemento e y que en la columna bajo a debe aparecer e.

5. Dado que las ecuaciones $a \barwedge x = b$ y $y \barwedge x = b$ tienen única solución, se concluye, por un argumento análogo, que cada elemento b del grupo debe aparecer una y sólo una vez en cada fila y en cada columna de la tabla.

Recíprocamente, supongamos que una tabla asociada a una operación binaria interna $\barwedge$ en un conjunto finito es tal, que hay un elemento actuando como identidad y que cada elemento del conjunto aparece precisamente una vez en cada fila y en cada columna. Se puede probar, que $(G, \barwedge)$ es un grupo si y sólo si se cumple la ley asociativa.

Ejemplo 2.1.5

1. *Complete la siguiente tabla (asumiendo que la operación $\barwedge$ es asociativo) de manera que $(G, \barwedge)$ sea un grupo, con $G = \{e, a, b\}$ y e elemento neutro (o identidad).*

$\barwedge$	e	a	b
e			
a			
b			

2. *¿Es $(\{1, i, -1, -i\}, \cdot)$ un grupo Abeliano?*

3. *El conjunto $G = \{a_0, a_1, \ldots, a_6\}$ con la ley de composición . definida por*

$$a_i \cdot a_j = \begin{cases} a_{i+j} & si, \quad i+j < 7 \\ a_{i+j-7} & si, \quad i+j \geq 7 \end{cases}$$

es un grupo abeliano.

2.2 Subgrupos

Definición 2.2.1 *Un conjunto B es un subconjunto de un conjunto A denotado por $B \subseteq A$ o $A \supseteq B$ si cada elemento de B está en A. Las notaciones $B \subset A$ o $A \supset B$ se usarán para $B \subseteq A$, pero $B \neq A$.*

Definición 2.2.2 *Sea G un grupo y sea S un subconjunto de G. Si para cada $a, b \in S$ es cierto que el producto $a \cdot b$ calculado en G también está en S, entonces S es cerrado bajo la operación binaria del grupo G. La operación binaria en S, definida de esta manera, es la operación inducida en S desde G.*

Definición 2.2.3 *Sea $(G, \cdot)$ un grupo y $H \subseteq G$, diremos que H es un subgrupo de $(G, \cdot)$, y se escribe $(H, \cdot) \leq (G, \cdot)$, si H es un grupo con respecto a la operación $\cdot$ definida en G.*

Dado que $\cdot$ es asociativa en G, también lo será en cualquier subconjunto H de G.

Teorema 2.2.1 *Un subconjunto H de un grupo G es un subgrupo de G si y sólo si*

i) H es cerrado bajo la operación binaria de G.

ii) el elemento neutro e de G pertenece a H.

iii) si $x \in H$, su inverso, x^{-1}, también pertenece a H.

Ejemplo 2.2.1

1. *Si $(G, \cdot)$ es un grupo, entonces $\{1_G\}$ y G son subgrupos de G. Se llaman subgrupos triviales.*
2. *$(\mathbb{Z}, +)$ es un subgrupo de $(\mathbb{Q}, +)$.*
3. *$(\mathbb{R}, +)$ es un subgrupo de $(\mathbb{C}, +)$.*
4. *Si n es un entero positivo, luego el conjunto $n\mathbb{Z} := \{nk : k \in \mathbb{Z}\}$ de todos los multiplos de n es un subgrupo de $(\mathbb{Z}, +)$.*
5. *Considere los siguientes grupos*

$\mathbb{Z}_4$: $+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

V $\bar{\wedge}$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Muestre que $(\{0, 2\}, +)$ es subgrupo (único subgrupo no trivial) de $\mathbb{Z}_4$ y que $(\{0, 3\}, +)$ no lo es. Por otro lado, muestre que $\{e, a\}$, $\{e, b\}$, y $\{e, c\}$ son tres subgrupos no triviales de V.

Proposición 2.2.1 *Sea H un subconjunto del grupo $(G, \cdot)$. Son equivalentes:*

I) $H \leq G$.

II)
$$\begin{cases} i)\ H \neq \phi \\ ii)\ a, b \in H \Rightarrow a \cdot b \in H \\ iii)\ a \in H \Rightarrow a^{-1} \in H \end{cases}$$

III)
$$\begin{cases} i)\ H \neq \phi \\ ii)\ a, b \in H \Rightarrow a^{-1} \cdot b \in H \quad \left(a \cdot b^{-1} \in H\right) \end{cases}$$

Proposición 2.2.2 *Si H es un subconjunto no vacío y finito de un grupo $(G, \cdot)$ y H es cerrado para la multiplicación, entonces $H \leq G$.*

Dem: De acuerdo a la proposición anterior (II), basta probar la condición iii). Sea $a \in H$. Las potencias $a^2 = a \cdot a, a^3 = a^2 \cdot a, \ldots, a^n$ pertenecen a H que es finito. Luego, existen r, s tales que $r > s > 0$ y $a^r = a^s$. De aquí, $a^{r-s} = e$ y $a \cdot a^{r-s-1} = e$. Por lo tanto, $a^{-1} = a^{r-s-1} \in H$.

2.2.1 Subgrupos cíclicos

Sea G un grupo y sea $a \in G$. Un subgrupo de G que contenga a debe contener a $a \cdot a$, lo que denotaremos por a^2. Entonces, debe contener $a^2 \cdot a$ lo que denotamos por a^3. En general, debe contener a^n (en notación aditiva denotaríamos esto por na). Estas potencias enteras positivas de a conforman un conjunto cerrado bajo multiplicación. Sin embargo, es posible que el inverso de a no esté en este conjunto. Desde luego, un subgrupo que contenga a debe contener también a^{-1} y, por tanto, $a^{-1} \cdot a^{-1}$ lo que denotamos por a^{-2} y en general, debe contener a^{-m} para todo $m \in \mathbb{Z}^+$. Debe contener la identidad $e = a \cdot a^{-1}$. Denotamos $e = a^0$. Se ha mostrado que un subgrupo de G que contenga a, debe contener a $\{a^n : n \in \mathbb{Z}\}$.

Teorema 2.2.2 *Sea G un grupo y sea $a \in G$. Entonces*

$$H = \{a^n : n \in \mathbb{Z}\}$$

es un subgrupo de G y es el menor subgrupo de G que contiene a a, esto es, cada subgrupo que contiene a contiene a H.

Nota: *Si usamos la notación "$+$", como en el caso de los enteros con la operación de suma, escribimos $\langle a \rangle = \{na : n \in \mathbb{Z}\}$.*

Definición 2.2.4 *El grupo H del Teorema 2.2.2 es el subgrupo cíclico de G generado por a y se denotará por $\langle a \rangle$.*

Si G contiene algún elemento a tal que $G = \langle a \rangle$, entonces G es un *grupo cíclico*. En ese caso a es un generador de G. Si a es un elemento de un grupo G, definimos el orden de a como el menor entero positivo n tal que $a^n = e$, y escribimos $|a| = n$. Si no hay tal entero n, decimos que el orden de a es infinito y escribimos $|a| = \infty$ para denotar el orden de a.

Teorema 2.2.3 *Todo grupo cíclico es Abeliano.*

Dem: *Sea G un grupo cíclico y sea $a \in G$ un generador para G. Si g y h están en G, entonces pueden ser escritos como potencias de a, digamos $g = a^r$ y $h = a^s$. Como*

$$gh = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = hg,$$

G es abeliano.

Ejemplo 2.2.2

1. *Muestre que $\mathbb{Z}_4$ es cíclico.*
2. *Muestre que V no es cíclico.*
3. *Muestre que $(\mathbb{Z}, +)$ es un grupo cíclico.*

4. *Considere el grupo* $(\mathbb{Z}, +)$ *y calcule el subgrupo cíclico generado por 5,* $\langle 5 \rangle$.

5. *¿Un grupo cíclico puede tener más que un generador?*

Teorema 2.2.4 *Todo subgrupo de un grupo cíclico es cíclico.*

Dem: Las principales herramientas usadas en esta demostración son el algoritmo de división y el principio del buen orden. Sea G un grupo cíclico generado por a y supongamos que H es un subgrupo de G. Si $H = \{e\}$, entonces H es cíclico trivialmente. Supongamos que H contiene algún otro elemento g distinto de la identidad. Entonces g puede ser escrito como a^n para algún entero n. Como H es un subgrupo, $g^{-1} = a^{-n}$ también debe estar en H. Como n o $-n$ es positivo, podemos suponer que H contiene potencias positivas de a y que $n > 0$. Sea m el menor número natural tal que $a^m \in H$. Tal m existe por por el principio del buen orden. Afirmamos que $h = a^m$ es un generador para H. Debemos demostrar que todo $h' \in H$ puede ser escrito como una potencia de h. Como $h' \in H$ y H es un subgrupo de G, $h' = a^k$ para algún entero k. Usando el algoritmo de la división, podemos encontrar q y r tales que $k = mq + r$ con $0 \leq r < m$; luego,

$$a^k = a^{mq+r} = (a^m)^q a^r = h^q a^r.$$

Así $a^r = a^k h^{-q}$. Como a^k y h^{-q} están en H, a^r también debe estar en H. Pero m era el menor número positivo tal que a^m está en H; por lo tanto, $r = 0$ y $k = mq$. Luego,

$$h' = a^k = a^{mq} = h^q$$

y H está generado por h.

Corolario 2.2.1 *Los subgrupos de* $\mathbb{Z}$ *son exactamente* $n\mathbb{Z}$ *con* $n = 0, 1, 2, \ldots$

Proposición 2.2.3 *Sea* G *un grupo cíclico de orden* n *y supongamos que* a *es un generador para* G. *Entonces* $a^k = e$ *si y solo si* n *divide a* k.

Dem:

Antes de introducir el siguiente grupo cíclico, recordaremos propiedades de los números complejos.

Recordatorio números complejos

Los *números complejos* están definidos como

$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\},$$

con $i^2 = -1$. Si $z = a + bi$, entonces a es la *parte real* de z y b es la *parte imaginaria* de z. Para sumar dos números complejos $z = a + bi$ y $w = c + di$, debemos simplemente sumar las partes

reales y las imaginarias respectivamente:

$$z + w = (a + bi) + (c + di) = (a + c) + (b + d)i.$$

Recordando que $i^2 = -1$, podemos multiplicar los números complejos como si fueran polinomios. El producto de z y w es

$$(a + bi)(c + di) = ac + bdi^2 + adi + bci = (ac - bd) + (ad + bc)i.$$

Todo número complejo no nulo $z = a + bi$ tiene un inverso multiplicativo; es decir, existe un $z^{-1} \in \mathbb{C}^*$ tal que $zz^{-1} = z^{-1}z = 1$. Si $z = a + bi$, entonces

$$z^{-1} = \frac{a - bi}{a^2 + b^2}.$$

El *conjugado* de un número complejo $z = a+bi$ se define como $\overline{z} = a-bi$. El *módulo* de $z = a+bi$ es $|z| = \sqrt{a^2 + b^2}$.

Existen varias formas de representar gráficamente a los números complejos. Podemos representar un número complejo $z = a+bi$ como un par ordenado en el plano x, y donde a es la coordenada x (o real) y b coordenada y y (o imaginaria). Esta se llama representación *rectangular* o *cartesiana*.

Los número complejos no nulos se pueden representar también con sus *coordenadas polares*. Para especificar un punto no cero en el plano, basta con dar un ángulo θ desde el eje x positivo en dirección antihoraria y una distancia r desde el origen. Podemos ver que

$$z = a + bi = r(\cos\theta + i\sin\theta).$$

Luego,

$$r = |z| = \sqrt{a^2 + b^2}$$

y

$$a = r\cos\theta$$
$$b = r\sin\theta.$$

A veces abreviaremos $r(\cos\theta + i\sin\theta)$ como $r\text{cis}\theta$. Para garantizar que la representación de z esté bien definida, también pediremos que $0 \leq \theta < 2\pi$.

Proposición 2.2.4 *Sean $z = r\,\text{cis}\,\theta$ y $w = s\,\text{cis}\,\phi$ dos números complejos. Entonces*

$$zw = rs\,\text{cis}\,(\theta + \phi).$$

Teorema 2.2.5 (**DeMoivre**) *Sea* $z = r$
mathrmcisθ *un número complejo distinto de cero. Entonces*

$$[r\text{cis}\theta]^n = r^n\text{cis}(n\theta)$$

para $n = 1, 2, \ldots$.

Grupo de la circunferencia y las raíces de la unidad

Consideremos el *grupo de la circunferencia*,

$$\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}.$$

Proposición 2.2.5 *El grupo de la circunferencia es un subgrupo de* $\mathbb{C}^*$.

Teorema 2.2.6 *Si* $z^n = 1$, *entonces las raíces n-ésima de uno son*

$$z = \text{cis}\left(\frac{2k\pi}{n}\right),$$

con $k = 0, 1, \ldots, n-1$. *Más aún, la raíces n-ésimas de uno forman un subgrupo cíclico de* $\mathbb{T}$ *de orden* n.

Un generador para el grupo de las raíces n-ésimas de uno se llama *raíz n-ésima primitiva* de la unidad.

Ejemplo 2.2.3

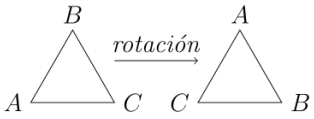
1. *Las raíces terceras o cúbicas de la unidad son* $\left\{1, \frac{-1+i\sqrt{3}}{2}, \frac{-1-i\sqrt{3}}{2}\right\}$, *las dos últimas primitivas.*
2. *Las raíces cuartas de la unidad son* $\{1, i, -1, -i\}$, *de las cuales* $+i$ *y* $-i$ *son primitivas.*

2.2.2 Grupos de Permutaciones

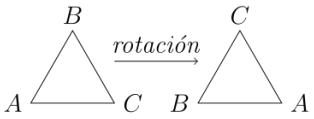
Los grupos de permutaciones tienen un rol central en el estudio de simetrías geométricas, en la teoría de Galois y en el estudio de la búsqueda de soluciones de ecuaciones polinomiales. Además son una fuente de muchos ejemplos de grupos no abelianos.

Una *simetría* de una figura geométrica es un reposicionamiento de la figura que preserva las relaciones entre sus lados y vértices tal como las distancias y los ángulos. Una función del plano en sí mismo que preserva la simetría de un objeto se llama *movimiento rígido*. Las simetrías del triángulo ΔABC son:

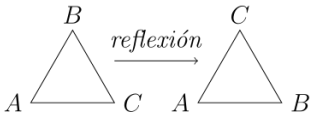
$$id = \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}$$



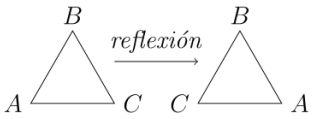
$$\rho_1 = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$$



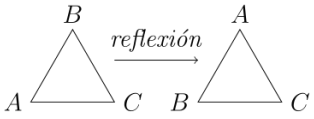
$$\rho_2 = \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}$$



$$\mu_1 = \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}$$



$$\mu_2 = \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}$$



$$\mu_3 = \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}$$

¿Qué simetría es $\mu_1\rho_1$; es decir, si realizamos la permutación ρ_1 y luego la permutación μ_1?.

$$\begin{aligned}(\mu_1\rho_1)(A) &= \mu_1(\rho_1(A)) = \mu_1(B) = C \\ (\mu_1\rho_1)(B) &= \mu_1(\rho_1(B)) = \mu_1(C) = B \\ (\mu_1\rho_1)(C) &= \mu_1(\rho_1(C)) = \mu_1(A) = A.\end{aligned}$$

Esta es la misma simetría que μ_2. Supongamos que hacemos estas mismas operaciones en el orden opuesto, $\rho_1\mu_1$. Es fácil determinar que esto es lo mismo que la simetría μ_3; luego, $\rho_1\mu_1 \neq \mu_1\rho_1$. Una tabla de multiplicación de simetrías de un triángulo equilátero ΔABC se encuentra en la tabla 2.1.

Note que en la tabla de multiplicación para las simetrías de un triángulo equilátero, para cada movimiento α del triángulo, hay otro movimiento β tal que $\alpha\beta = \mathrm{Id}$; es decir, para cada movimiento hay otro movimiento que devuelve al triángulo a su orientación original.

$\circ$	Id	ρ_1	ρ_2	μ_1	μ_2	μ_3
Id	Id	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	Id	μ_3	μ_1	μ_2
ρ_2	ρ_2	Id	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	Id	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	Id	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	Id

Cuadro 2.1: Tabla de multiplicación de simetrías de un triángulo equilátero

Las simetrías de hecho consisten en permutaciones de los tres vértices, donde una *permutación* del conjunto $S = \{A, B, C\}$ es una biyección $\pi : S \to S$. Los tres vértices tienen la siguientes seis permutaciones.

$$\begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix} \quad \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix} \quad \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$$
$$\begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix} \quad \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix} \quad \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}$$

Hemos usado el arreglo

$$\begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$$

para denotar la permutación que envía A en B, B en C, y C en A. Es decir,

$$A \mapsto B$$
$$B \mapsto C$$
$$C \mapsto A.$$

Las simetrías de un triángulo forman un grupo.

En general, las permutaciones de un conjunto X forman el grupo S_X. Si X es un conjunto finito, podemos suponer que $X = \{1, 2, \ldots, n\}$. En este caso escribiremos S_n en lugar de S_X. El siguiente teorema dice que S_n es un grupo. A este grupo lo llamaremos *grupo simétrico* en n símbolos.

Teorema 2.2.7 *El grupo simétrico en n símbolos, S_n, es un grupo con $n!$ elementos, con la operación binaria de composición de funciones.*

Dem: La identidad de S_n es simplemente la función identidad que envía 1 en 1, 2 en 2, ..., n en n. Si $f : S_n \to S_n$ es una permutación, entonces f^{-1} existe, pues f es biyectiva; luego, toda permutación tiene una inversa. La composición de funciones es asociativa, lo que hace que la operación del grupo sea asociativa. $|S_n| = n!$.

Definición 2.2.5 *Un subgrupo de S_n se llama grupo de permutaciones.*

Ejemplo 2.2.4 *Considere el subgrupo G de S_5 que consiste de la permutación* Id *y las permutaciones*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix}$$
$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}$$
$$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}.$$

La siguiente tabla nos indica como multiplicar elementos en el grupo de permutaciones G.

$\circ$	Id	σ	τ	μ
Id	Id	σ	τ	μ
σ	σ	Id	μ	τ
τ	τ	μ	Id	σ
μ	μ	τ	σ	Id

Ejemplo 2.2.5 *La multiplicación de permutaciones no es conmutativa en general. Sean*

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

Entonces

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix},$$

pero

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

Notación cíclica

Una permutación $\sigma \in S_X$ es un *ciclo de largo* k si existen elementos $a_1, a_2, \ldots, a_k \in X$ tales que

$$\sigma(a_1) = a_2$$
$$\sigma(a_2) = a_3$$
$$\vdots$$
$$\sigma(a_k) = a_1$$

y $\sigma(x) = x$ para todos los demás elementos $x \in X$. Escribiremos $(a_1, a_2, \ldots, a_k)$ para denotar al ciclo σ.

Ejemplo 2.2.6 *La permutación*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 3 & 5 & 1 & 4 & 2 & 7 \end{pmatrix} = (162354)$$

es un ciclo de largo 6, mientras

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 3 & 5 & 6 \end{pmatrix} = (243)$$

es un ciclo de largo 3. No toda permutación es un ciclo. Considere la permutación

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix} = (1243)(56).$$

Esta permutación de hecho contiene un ciclo de largo 2 y un ciclo de largo 4.

Ejemplo 2.2.7 *Suponga que*

$$\sigma = (1352) \quad y \quad \tau = (256).$$

Calcule $\sigma\tau$, luego si $\mu = (1634)$, calcule $\sigma\mu$.

Definición 2.2.6 *Dos ciclos en S_X, $\sigma = (a_1, a_2, \ldots, a_k)$ y $\tau = (b_1, b_2, \ldots, b_l)$, son disjuntos si $a_i \neq b_j$ para todo i y para todo j.*

Ejemplo 2.2.8 *Los ciclos (135) y (27) son disjuntos; mientras los ciclos (135) y (347) no lo son. Además*

$$(135)(27) = (135)(27)$$
$$(135)(347) = (13475).$$

El producto de dos ciclos que no son disjuntos a veces se puede reducir a algo menos complicado; el producto de dos ciclos disjuntos no puede ser simplificado.

Proposición 2.2.6 *Sean σ y τ dos ciclos disjuntos en S_X. Entonces $\sigma\tau = \tau\sigma$.*

Dem: Sea $\sigma = (a_1, a_2, \ldots, a_k)$ and $\tau = (b_1, b_2, \ldots, b_l)$. Debemos mostrar que $\sigma\tau(x) = \tau\sigma(x)$ para todo $x \in X$. Si x no está en $\{a_1, a_2, \ldots, a_k\}$ ni en $\{b_1, b_2, \ldots, b_l\}$, entonces tanto σ como τ fijan x. Es decir, $\sigma(x) = x$ y $\tau(x) = x$. Luego,

$$\sigma\tau(x) = \sigma(\tau(x)) = \sigma(x) = x = \tau(x) = \tau(\sigma(x)) = \tau\sigma(x).$$

Ahora supongamos que $x \in \{a_1, a_2, \ldots, a_k\}$. Entonces $\sigma(a_i) = a_{(i \text{ mód } k)+1}$; es decir,

$$\begin{aligned} a_1 &\mapsto a_2 \\ a_2 &\mapsto a_3 \\ &\vdots \\ a_{k-1} &\mapsto a_k \\ a_k &\mapsto a_1. \end{aligned}$$

Pero, $\tau(a_i) = a_i$ pues σ y τ son disjuntos. Por lo tanto,

$$\begin{aligned} \sigma\tau(a_i) &= \sigma(\tau(a_i)) \\ &= \sigma(a_i) \\ &= a_{(i \text{ mód } k)+1} \\ &= \tau(a_{(i \text{ mód } k)+1}) \\ &= \tau(\sigma(a_i)) \\ &= \tau\sigma(a_i). \end{aligned}$$

Similarmente, si $x \in \{b_1, b_2, \ldots, b_l\}$, entonces σ y τ también conmutan.

Teorema 2.2.8 *Toda permutación en S_n puede ser escrita como producto de ciclos disjuntos.*

Dem: Podemos suponer que $X = \{1, 2, \ldots, n\}$. Si $\sigma \in S_n$ y definimos X_1 como $\{\sigma(1), \sigma^2(1), \ldots\}$, entonces el conjunto X_1 es finito pues X es finito. Ahora sea i el primer entero en X que no está en X_1 y definamos X_2 como $\{\sigma(i), \sigma^2(i), \ldots\}$. Nuevamente, X_2 es un conjunto finito. Continuando de esta manera, podemos definir conjuntos finitos disjuntos $X_3, X_4, \ldots$. Como X es un conjunto finito, estamos seguros que este proceso terminará y que habrá un número finito de estos conjuntos, digamos r. Si σ_i es el ciclo definido por

$$\sigma_i(x) = \begin{cases} \sigma(x) & x \in X_i \\ x & x \notin X_i, \end{cases}$$

entonces $\sigma = \sigma_1\sigma_2 \cdots \sigma_r$. Como los conjuntos $X_1, X_2, \ldots, X_r$ son disjuntos, los ciclos $\sigma_1, \sigma_2, \ldots, \sigma_r$ también lo son.

Ejercicio 2.2.1 *Considere $X = \{1, 2, \ldots, 7\}$ y $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 6 & 2 & 7 & 1 & 5 \end{pmatrix}$. Descomponga σ en ciclos disjuntos.*

Nota: Desde ahora nos resultará conveniente usar la notación cíclica para representar las permutaciones. Cuando usemos la notación cíclica, frecuentemente representaremos la permutación identidad por (1) o por ( ).

Transposiciones

La permutación (no trivial) más simple es un ciclo de largo 2. Tales ciclos se llaman *transposiciones*. Como

$$(a_1, a_2, \ldots, a_n) = (a_1 a_n)(a_1 a_{n-1}) \cdots (a_1 a_3)(a_1 a_2),$$

cualquier ciclo puede ser escrito como el producto de transposiciones, llevándonos a la siguiente proposición.

Proposición 2.2.7 *Cualquier permutación de un conjunto finito que contenga al menos dos elementos puede ser escrita como producto de transposiciones.*

Ejemplo 2.2.9 *Considere la permutación*

$$(16)(253) = (16)(23)(25) = (16)(45)(23)(45)(25).$$

Como podemos ver, no hay una única forma de representar la permutación como producto de transposiciones. Por ejemplo, podemos escribir la identidad como $(12)(12)$*, como* $(13)(24)(13)(24)$*, y en muchas otras formas. Sin embargo, resulta ser, que ninguna permutación se puede escribir tanto como un producto de un número par como de un número impar de transposiciones. Por ejemplo, podemos representar la permutación* (16) *por*

$$(23)(16)(23)$$

o por

$$(35)(16)(13)(16)(13)(35)(56),$$

pero (16) *siempre será el producto de un número impar de transposiciones.*

Lema: Si la identidad se escribe como el producto de r transposiciones,

$$\mathrm{Id} = \tau_1 \tau_2 \cdots \tau_r,$$

entonces r es un número par.

Teorema 2.2.9 *Si una permutación* σ *puede ser expresada como el producto de un número par de transposiciones, entonces cualquier otro producto de transposiciones igual a* σ *debe también contener un número par de transposiciones. De forma similar, si* σ *puede ser expresada como el producto de un número impar de transposiciones, entonces cualquier otro producto de transposiciones igual a* σ *debe también contener un número impar de transposiciones.*

Dem:

Definición 2.2.7 (**Permutación par e impar**) *Una permutación es par si puede ser expresada como el producto de un número par de transposiciones e impar si puede ser expresada como el producto de un número impar de transposiciones.*

Grupos alternantes

Uno de los subgrupos más importantes de S_n es el conjunto de todas las permutaciones pares, A_n. El grupo A_n se llama *grupo alternante en n símbolos*.

Teorema 2.2.10 *El conjunto A_n es un subgrupo de S_n.*

Ejercicio 2.2.2 *Demostrar el Teorema 2.2.2.*

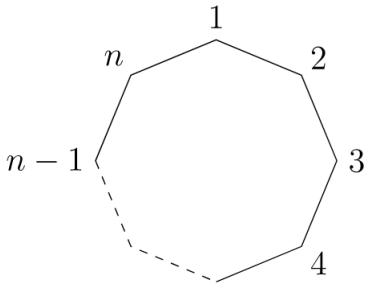
Ejemplo 2.2.10 *El grupo A_4 es el subgrupo de S_4 que consiste de las permutaciones pares. Hay doce elementos en A_4:*

(1)	(12)(34)	(13)(24)	(14)(23)
(123)	(132)	(124)	(142)
(134)	(143)	(234)	(243).

Nota: Lagrange fue el primero en pensar las permutaciones como funciones de un conjunto en sí mismo, pero fue Cauchy quién desarrolló los teoremas básicos y la notación para las permutaciones. Él fue el primero en usar la notación cíclica. Augustin-Louis Cauchy (1789–1857) nació en París durante en el apogeo de la Revolución Francesa. Su familia dejó París y se fue al pueblo de Arcueil para escapar del Reino del Terror. Uno de los vecinos de la familia allí, fue Pierre-Simon Laplace (1749–1827), quien lo motivó a iniciar una carrera en matemáticas. Cauchy comenzó su carrera como matemático resolviendo un problema de geometría que le planteó Lagrange. Cauchy escribió más de 800 trabajos en diversos tópicos, como ecuaciones diferenciales, grupos finitos, matemáticas aplicadas, y análisis complejo. Fue uno de los matemáticos responsables de hacer que el Cálculo Diferencial fuera riguroso. Es probable que haya más teoremas y conceptos en matemáticas asociados al nombre de Cauchy que al de cualquier otro matemático.

Grupos Dihedrales

Estos grupos consisten de los movimientos rígidos de un polígono regular de n lados o n-ágono regular. Para $n = 3, 4, \ldots$, definimos el *n-ésimo grupo dihedral* como el grupo de los movimientos rígidos del n-ágono regular. Denotaremos este grupo por D_n. Podemos numerar los vértices de un n-ágono regular con $1, 2, \ldots, n$. Note que hay exactamente n posibilidades para reemplazar al primer vértice. Si reemplazamos al primer vértice por k, entonces el segundo vértice debe ser reemplazado por el vértice $k + 1$ o por el vértice $k - 1$; luego, hay $2n$ movimientos rígidos posibles del n-ágono. Resumimos estos resultados en el siguiente teorema.



Teorema 2.2.11 *El grupo dihedral, D_n, es un subgrupo de S_n de orden $2n$.*

Teorema 2.2.12 *El grupo D_n, $n \geq 3$, consiste de todos los productos de los dos elementos r y s, que satifacen las relaciones*

$$r^n = 1$$
$$s^2 = 1$$
$$srs = r^{-1}.$$

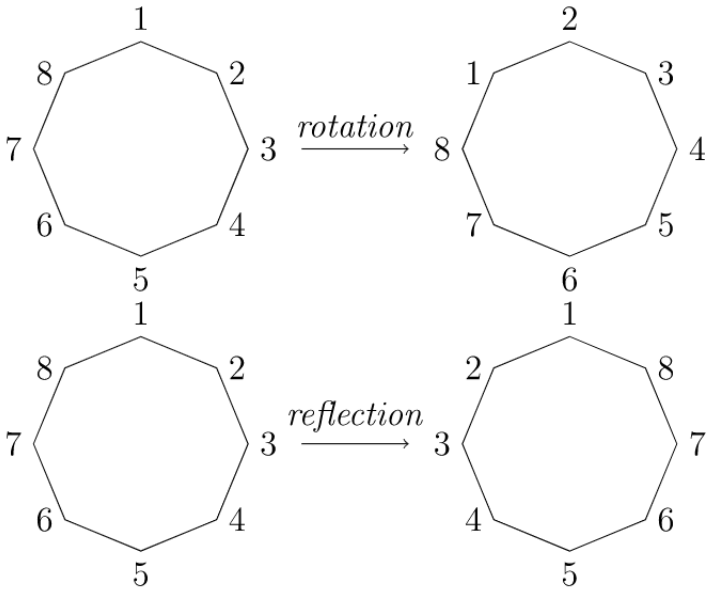


Figura 2.1: Rotaciones y reflexiones de un n-ágono regular.

Dem: Los posibles movimientos de un n-ágono regular son reflexiones y rotaciones. Hay exactamente n rotaciones posibles:

$$\mathrm{Id}, \frac{360^\circ}{n}, 2 \cdot \frac{360^\circ}{n}, \ldots, (n-1) \cdot \frac{360^\circ}{n}.$$

Denotaremos la rotación en $360^\circ/n$ por r. La rotación r genera todas las rotaciones. Es decir,

$$r^k = k \cdot \frac{360^\circ}{n}.$$

Etiquete las n reflexiones $s_1, s_2, \ldots, s_n$, donde s_k es la reflexión que fija el vértice k. Hay dos casos, dependiendo de si n es par o impar. Si hay un número par de vértices, entonces una reflexión fija dos de ellos, y $s_1 = s_{n/2+1}, s_2 = s_{n/2+2}, \ldots, s_{n/2} = s_n$. Si hay un número impar de vértices, entonces una reflexión fija solamente un vértice y $s_1, s_2, \ldots, s_n$ son distintas. Sea $s = s_1$. Entonces $s^2 = 1$ y $r^n = 1$. Como cualquier movimiento rígido t del n-ágono reemplaza al primer vértice por el vértice k, el segundo vértice será reemplazado por el $k+1$ o por el $k-1$. Si el segundo se reemplaza por $k+1$, entonces $t = r^k$. Si el segundo se reemplaza por $k-1$, entonces $t = sr^k$. Luego, r y s generan D_n. Es decir, D_n consiste de todos los productos finitos de r y s,

$$D_n = \{1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}.$$

Dejaremos la demostración de que $srs = r^{-1}$ como un ejercicio.

Ejemplo 2.2.11 *El grupo de movimientos de un cuadrado, D_4, consiste de ocho elementos. Con los vértices numerados $1, 2, 3, 4$, las rotaciones son*

$$\begin{aligned} r &= (1234) \\ r^2 &= (13)(24) \\ r^3 &= (1432) \\ r^4 &= (1) \end{aligned}$$

y las reflexiones son

$$\begin{aligned} s_1 &= (24) \\ s_2 &= (13). \end{aligned}$$

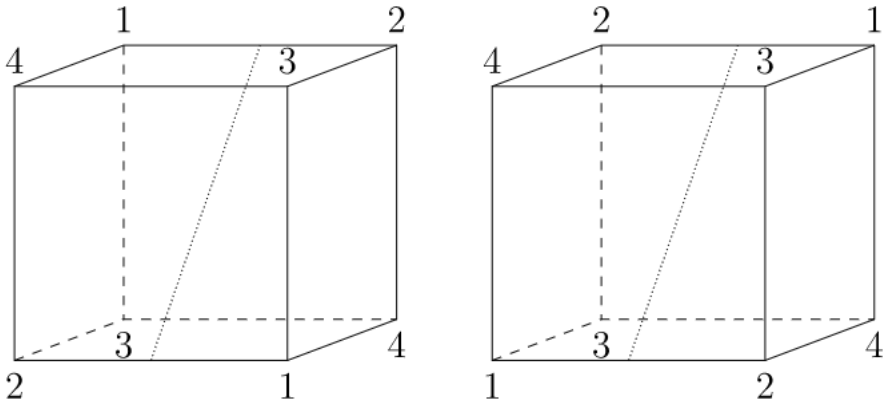
El orden de D_4 es 8. Los dos elementos restantes son

$$\begin{aligned} rs_1 &= (12)(34) \\ r^3 s_1 &= (14)(23). \end{aligned}$$

El grupo de movimientos de un Cubo

Proposición 2.2.8 *El grupo de movimientos rígidos de un cubo contiene 24 elementos.*

Teorema 2.2.13 *El grupo de movimientos rígidos de un cubo es S_4.*



Ejercicio 2.2.3 *Describa todos los elementos de S_4. Escriba los elementos de S_4 en notación cíclica. Identifíque las 6 transposiciones de S_4. Note que todo elemento de S_4 puede ser escrito como producto de estas transposiciones.*

2.3 Clases Laterales y Teorema de Lagrange

El Teorema de Lagrange es uno de los resultados más importantes en la teoría de grupos finitos. Dice que el orden de un subgrupo debe dividir el orden del grupo completo. Para comprender dicho teorema se introduce el siguiente concepto.

2.3.1 Clases Laterales

Sea G un grupo y H un subgrupo de G. Se define una *clase lateral izquierda* de H con *representante* $g \in G$ como el conjunto

$$gH = \{gh : h \in H\}.$$

Las *clases laterales derechas* pueden ser definidas similiarmente como

$$Hg = \{hg : h \in H\}.$$

Si las clases laterales izquierda y derecha coinciden o si es claro del contexto a qué tipo de clases laterales nos estamos refiriendo, diremos *clase lateral* sin especificar izquierda o derecha.

Ejemplo 2.3.1 *Sea H el subgrupo de S_3 definido por las permutaciones $\{(1), (123), (132)\}$. Las clases laterales izquierdas de H son*

$$(1)H = (123)H = (132)H = \{(1), (123), (132)\}$$
$$(12)H = (13)H = (23)H = \{(12), (13), (23)\}.$$

Las clases laterales derechas de H son exactamente las mismas que las clases laterales izquierdas:

$$H(1) = H(123) = H(132) = \{(1), (123), (132)\}$$
$$H(12) = H(13) = H(23) = \{(12), (13), (23)\}.$$

No siempre es el caso que una clase lateral derecha sea igual a una clase lateral izquierda. Sea K el subgrupo de S_3 definido por las permutaciones $\{(1),(12)\}$. Entonces las clases laterales izquierdas de K son

$$(1)K = (12)K = \{(1),(12)\}$$
$$(13)K = (123)K = \{(13),(123)\}$$
$$(23)K = (132)K = \{(23),(132)\};$$

pero, las clases laterales derechas de K son

$$K(1) = K(12) = \{(1),(12)\}$$
$$K(13) = K(132) = \{(13),(132)\}$$
$$K(23) = K(123) = \{(23),(123)\}.$$

Lemma 2.3.1 *Sea H un subgrupo de un grupo G y supongamos que $g_1, g_2 \in G$. Las siguientes condiciones son equivalentes.*

i) $g_1H = g_2H$;

ii) $Hg_1^{-1} = Hg_2^{-1}$;

iii) $g_1H \subset g_2H$;

iv) $g_2 \in g_1H$;

v) $g_1^{-1}g_2 \in H$.

Ejercicio 2.3.1 *Demostrar el Lemma 2.3.1.*

Teorema 2.3.1 *Sea H un subgrupo de un grupo G. Entonces las clases laterales izquierdas de H en G particionan G. Es decir, el grupo G es la unión disjunta de las clases laterales izquierdas de H en G.*

Dem: Sean g_1H y g_2H dos clases laterales de H en G. Debemos mostrar que ya sea $g_1H \cap g_2H = \emptyset$ o $g_1H = g_2H$. Supongamos que $g_1H \cap g_2H \neq \emptyset$ y $a \in g_1H \cap g_2H$. Entonces por la definición de clase lateral izquierda, $a = g_1h_1 = g_2h_2$ para ciertos elementos h_1 y h_2 en H. Luego, $g_1 = g_2h_2h_1^{-1}$ y $g_1 \in g_2H$. Por el Lema 2.3.1, $g_1H = g_2H$.

Definición 2.3.1 *Sea G un grupo y H un subgrupo de G. Se define el índice de H en G como el número de clases laterales izquierdas distintas de H en G. Denotaremos este índice por $[G : H]$.*

Ejercicio 2.3.2 *Suponga que $G = S_3$. Calcule $[G : H]$ y $[G : K]$, H el subgrupo de S_3 definido por las permutaciones $\{(1),(123),(132)\}$ y K el subgrupo de S_3 definido por las permutaciones $\{(1),(12)\}$, respectivamente.*

Teorema 2.3.2 *Sea H un subgrupo de un grupo G. El número de clases laterales izquierdas de H en G es el mismo que el número de clases laterales derechas de H en G.*

Proposición 2.3.1 *Sea H un subgrupo de G con $g \in G$ y definamos una función $\phi : H \to gH$ como $\phi(h) = gh$. La función ϕ es biyectiva; luego el número de elementos en H es el mismo que el número de elementos en gH.*

Ejercicio 2.3.3 *Demostrar la proposición 2.3.1.*

Teorema 2.3.3 (**Teorema de Lagrange**) *Sea G un grupo finito y sea H un subgrupo de G. Entonces $|G|/|H| = [G : H]$ es el número de clases laterales izquierdas diferentes de H en G. En particular, el número de elementos en H debe dividir al número de elementos en G.*

Dem: El grupo G está particionado en $[G : H]$ clases laterales izquierdas diferentes. Cada clase lateral izquierda tiene $|H|$ elementos; por lo tanto, $|G| = [G : H]|H|$.

Corolario 2.3.1 *Supongamos que G es un grupo finito y que $g \in G$. Entonces el orden de g divide al número de elementos en G.*

Corolario 2.3.2 *Sea $|G| = p$ con p primo. Entonces G es cíclico y cualquier $g \in G$ tal que $g \neq e$ es un generador.*

Ejercicio 2.3.4 *Demostrar el Corolario 2.3.2.*

Corolario 2.3.3 *Sean H y K subgrupos de un grupo finito G tales que $G \supset H \supset K$. Entonces*

$$[G : K] = [G : H][H : K].$$

El recíproco del Teorema de Lagrange es falso: Recordemos que: El grupo A_4 es el subgrupo de S_4 que consiste de las permutaciones pares. Hay doce elementos en A_4:

(1)	(12)(34)	(13)(24)	(14)(23)
(123)	(132)	(124)	(142)
(134)	(143)	(234)	(243).

Sin embargo, se puede demostrar que no tiene ningún subgrupo de orden 6. De acuerdo al *Teorema de Lagrange*, los subgrupos de un grupo de orden 12 pueden tener orden 1, 2, 3, 4, o 6. Pero no hay garantía de que existan subgrupos de todos los posibles órdenes.

Proposición 2.3.2 *El grupo A_4 no tiene subgrupo de orden 6.*

Idea: *Supondremos que sí tiene un subgrupo H de orden 6 y buscaremos una contradicción. Como A_4 contiene ocho 3-ciclos, sabemos que H debe contener un 3-ciclo. Mostraremos que si H contiene un 3-ciclo, entonces debe contener más de 6 elementos.*

Dem: *Por teorema de Lagrange tenemos $[A_4 : H] = 2$, hay solo dos clases laterales de H en A_4. Luego una de las clases laterales es el mismo H, además clases laterales derechas e izquierdas deben coincidir; por lo tanto, $gH = Hg$ o $gHg^{-1} = H$ para todo $g \in A_4$. Como existen ocho 3-ciclos en A_4, al menos uno de los 3-ciclos debe estar en H. Sin perdida de generalidad, supongamos que (123) está en H. Entonces $(123)^{-1} = (132)$ también debe estar en H. Como $ghg^{-1} \in H$ para todo $g \in A_4$ y todo $h \in H$ y*

$$(124)(123)(124)^{-1} = (124)(123)(142) = (243)$$
$$(243)(123)(243)^{-1} = (243)(123)(234) = (142)$$

concluimos que H debe tener al menos los siete elementos.

$$(1), (123), (132), (243), (243)^{-1} = (234), (142), (142)^{-1} = (124).$$

Por lo tanto, A_4 no tiene subgrupo de orden 6.

CAPÍTULO 3

Homomorfismos de grupos

3.1 Isomorfismos

Algunos grupos pueden parecer diferentes a primera vista, pero pueden reconocerse como iguales después de un cambio de nombre de sus elementos y entre las operaciones de grupo de ambos. En tal caso diremos que los grupos son *isomorfos*.

Definición 3.1.1 *Dos grupos $(G, \cdot)$ y $(H, \circ)$ son isomorfos si existe una función biyectiva $\phi : G \to H$ que preserve la operación de grupo; es decir,*

$$\phi(a \cdot b) = \phi(a) \circ \phi(b)$$

para todo a y b en G. Si G es isomorfo con H, escribimos $G \cong H$. La función ϕ se llama un isomorfismo.

Ejemplo 3.1.1

1. *Para demostrar que $\mathbb{Z}_4 \cong \langle i \rangle$, defina una función $\phi : \mathbb{Z}_4 \to \langle i \rangle$ como $\phi(n) = i^n$. Debemos mostrar que ϕ es biyectiva y que preserva la operación de grupo. La función ϕ es biyectiva pues*

$$\begin{aligned} \phi(0) &= 1 \\ \phi(1) &= i \\ \phi(2) &= -1 \\ \phi(3) &= -i. \end{aligned}$$

   Como

$$\phi(m+n) = i^{m+n} = i^m i^n = \phi(m)\phi(n),$$

   se preserva la operación de grupo.

2. *Podemos definir un isomorfismo ϕ del grupo aditivo de los números reales $(\mathbb{R}, +)$ al grupo multiplicativo de los números reales positivos $(\mathbb{R}^+, \cdot)$ mediante la función exponencial; es decir,*

$$\phi(x+y) = e^{x+y} = e^x e^y = \phi(x)\phi(y).$$

   Falta mostrar que ϕ es una biyección.

3. *Si bien S_3 y $\mathbb{Z}_6$ poseen el mismo número de elementos, podríamos sospechar que no son isomorfos, pues $\mathbb{Z}_6$ es abeliano y S_3 es no abeliano. Para demostrar que esto es así, supongamos que $\phi : \mathbb{Z}_6 \to S_3$ es un isomorfismo. Sean $a, b \in S_3$ dos elementos tales que $ab \neq ba$. Como ϕ es un isomorfismo, existen elementos m y n en $\mathbb{Z}_6$ tales que*

$$\phi(m) = a \quad and \quad \phi(n) = b.$$

Pero,

$$ab = \phi(m)\phi(n) = \phi(m+n) = \phi(n+m) = \phi(n)\phi(m) = ba,$$

lo que contradice el hecho de que a y b no conmutan.

Teorema 3.1.1 *Sea $\phi : G \to H$ un isomorfismo de grupos. Entonces se cumplen las siguientes proposiciones.*

1. *$\phi^{-1} : H \to G$ es un isomorfismo.*
2. *$|G| = |H|$.*
3. *Si G es abeliano, entonces H es abeliano.*
4. *Si G es cíclico, entonces H es cíclico.*
5. *Si G tiene un subgrupo de orden n, entonces H tiene un subgrupo de orden n.*

Dem: *Trabajo colaborativo en clases.*

Teorema 3.1.2 *Todo grupo cíclico de orden infinito es isomorfo a $\mathbb{Z}$.*

Dem: *Sea G un grupo cíclico de orden infinito y supongamos que a es un generador de G. Definamos la función $\phi : \mathbb{Z} \to G$ como $\phi : n \mapsto a^n$. Entonces*

$$\phi(m+n) = a^{m+n} = a^m a^n = \phi(m)\phi(n).$$

Para mostrar que ϕ es inyectiva, supongamos que m y n son dos elementos en $\mathbb{Z}$, con $m \neq n$. Podemos suponer que $m > n$. Debemos mostrar que $a^m \neq a^n$. Supongamos lo contrario; es decir, $a^m = a^n$. En ese caso $a^{m-n} = e$, con $m - n > 0$, lo que contradice el hecho de que a tiene orden infinito. Nuestra función es sobreyectiva pues todo elemento en G puede ser escrito como a^n para algún entero n y $\phi(n) = a^n$.

3.2 Subgrupos Normales y Grupos Cociente

Si H es un subgrupo de un grupo G, no siempre se cumple que $gH = Hg$ para todo $g \in G$. Los subgrupos que tienen esta propiedad permiten la construcción de una nueva clase de grupos, llamados *grupos cociente*. Los grupos cociente pueden ser estudiados directamente o usando *homomorfismos*, una generalización de los *isomorfismos*. Estudiaremos homomorfismos en la siguiente sección.

3.2.1 Subgrupos Normales

Definición 3.2.1 *Un subgrupo H de un grupo G es normal en G si $gH = Hg$ para todo $g \in G$. Es decir, un subgrupo normal de un grupo G es un subgrupo para el que las clases laterales derechas e izquierdas coinciden.*

Ejercicio 3.2.1

1. *Sea G un grupo abeliano. Muestre que todo subgrupo H de G es un subgrupo normal.*
2. *Sea H el subgrupo de S_3 que consiste de los elementos (1) y (12). Use (123) para mostrar que H no es un subgrupo normal de S_3.*
3. *Muestre que el subgrupo N, que consiste de las permutaciones (1), (123), y (132), es normal.*

Teorema 3.2.1 *Sea G un grupo y N un subgrupo de G. Entonces las siguientes proposiciones son equivalentes.*

1. *El subgrupo N es normal en G.*
2. *Para todo $g \in G$, $gNg^{-1} \subseteq N$.*
3. *Para todo $g \in G$, $gNg^{-1} = N$.*

Dem: *(1) $\Rightarrow$ (2). Como N es normal en G, $gN = Ng$ para todo $g \in G$. Luego, para un $g \in G$ dado y para $n \in N$, existe n' en N tal que $gn = n'g$. Por lo tanto, $gng^{-1} = n' \in N$ y $gNg^{-1} \subseteq N$.*

(2) $\Rightarrow$ (3). Sea $g \in G$. Como $gNg^{-1} \subseteq N$, solo debemos demostrar que $N \subseteq gNg^{-1}$. Para $n \in N$, $g^{-1}ng = g^{-1}n(g^{-1})^{-1} \in N$. Luego, $g^{-1}ng = n'$ para algún $n' \in N$. Por lo tanto, $n = gn'g^{-1}$ está en gNg^{-1}.

(3) $\Rightarrow$ (1). Supongamos que $gNg^{-1} = N$ para todo $g \in G$. Entonces para cualquier $n \in N$ existe $n' \in N$ tal que $gng^{-1} = n'$. Por lo tanto, $gn = n'g$ y $gN \subseteq Ng$. Similarmente, $Ng \subseteq gN$.

3.2.2 Grupos cociente

Si N es un subgrupo normal de un grupo G, entonces las clases laterales de N en G forman un grupo G/N con la operación $(aN)(bN) = abN$. Este grupo se llama *cociente* de G por N. Nuestra primera tarea es demostrar que G/N es realmente un grupo.

Teorema 3.2.2 *Sea N un subgrupo normal de un grupo G. Las clases laterales de N en G forman un grupo G/N de orden $[G : N]$.*

Dem: *La operación de grupo en G/N es $(aN)(bN) = abN$. Debemos verificar que esta operación está bien definida; es decir, el producto en el grupo es independiente de la elección de representantes para*

las clases laterales. Sean $aN = bN$ *y* $cN = dN$*. Por demostrar que*

$$(aN)(cN) = acN = bdN = (bN)(dN).$$

Entonces $a = bn_1$ *y* $c = dn_2$ *para algún* n_1 *y algún* n_2 *en* N*. Luego,*

$$\begin{aligned} acN &= bn_1dn_2N \\ &= bn_1dN \\ &= bn_1Nd \\ &= bNd \\ &= bdN. \end{aligned}$$

El resto del teorema es fácil: $eN = N$ *es la identidad y* $g^{-1}N$ *es el inverso de* gN*. El orden de* G/N *es, por supuesto, el número de clases laterales de* N *en* G*.*

Nota: A diferencia de los grupos y subgrupos que hemos analizado, los elementos de un grupo cociente son *conjuntos de elementos*.

Ejercicio 3.2.2

1. *Muestre que* $N = \{(1), (123), (132)\}$ *es subgrupo normal de* S_3*,. Encuentre la tabla de multiplicación del grupo cociente* S_3/N*.*

2. *Considere el subgrupo normal* $3\mathbb{Z}$ *de* $\mathbb{Z}$*. Las clases laterales de* $3\mathbb{Z}$ *en* $\mathbb{Z}$ *son*

$$\begin{aligned} 0 + 3\mathbb{Z} &= \{\ldots, -3, 0, 3, 6, \ldots\} \\ 1 + 3\mathbb{Z} &= \{\ldots, -2, 1, 4, 7, \ldots\} \\ 2 + 3\mathbb{Z} &= \{\ldots, -1, 2, 5, 8, \ldots\}. \end{aligned}$$

   Encuentre la tabla de multiplicación del grupo cociente $\mathbb{Z}/3\mathbb{Z}$*.*

3.3 Homomorfismos

Dos grupos están relacionados de la forma más fuerte posible si son isomorfos; sin embargo una relación más débil puede también existir entre dos grupos. Una de las ideas clásicas del álgebra es el concepto de homomorfismo, una generalización natural de isomorfismo. Si relajamos el requerimiento de que un isomorfismo sea biyectivo, obtenemos un homomorfismo.

Definición 3.3.1 *Un homomorfismo entre los grupos* $(G, \cdot)$ *y* $(H, \circ)$ *es una función* $\phi : G \to H$ *tal que*

$$\phi(g_1 \cdot g_2) = \phi(g_1) \circ \phi(g_2) \qquad \forall g_1, g_2 \in G$$

La imagen de ϕ *en* H *se llama imagen homomorfa de* ϕ*.*

Ejemplo 3.3.1

1. *Sea G un grupo y $g \in G$. Defina una función $\phi : \mathbb{Z} \to G$ como $\phi(n) = g^n$. Entonces ϕ es un homomorfismo de grupos, pues*

$$\phi(m+n) = g^{m+n} = g^m g^n = \phi(m)\phi(n).$$

Este homomorfismo envía a $\mathbb{Z}$ en el subgrupo cíclico de G generado por g.

2. *Sea $G = GL_2(\mathbb{R})$. Si*

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

está en G, entonces el determinante es distinto de cero; es decir, $\det(A) = ad - bc \neq 0$. Además, para dos elementos A y B en G, $\det(AB) = \det(A)\det(B)$. Usando el determinante, podemos definir un homomorfismo $\phi : GL_2(\mathbb{R}) \to \mathbb{R}^*$ como $A \mapsto \det(A)$.

3. *Recuerde que el grupo de la circunferencia $\mathbb{T}$ consiste de todos los números complejos z tales que $|z| = 1$. Podemos definir un homomorfismo ϕ del grupo aditivo de los números reales $\mathbb{R}$ a $\mathbb{T}$ por $\phi : \theta \mapsto \cos\theta + i\sin\theta$. De hecho,*

$$\begin{aligned} \phi(\alpha+\beta) &= \cos(\alpha+\beta) + i\sin(\alpha+\beta) \\ &= (\cos\alpha\cos\beta - \sin\alpha\sin\beta) + i(\sin\alpha\cos\beta + \cos\alpha\sin\beta) \\ &= (\cos\alpha + i\sin\alpha)(\cos\beta + i\sin\beta) \\ &= \phi(\alpha)\phi(\beta). \end{aligned}$$

Geométricamente, estamos enrollando la recta real sobre la circunferencia unitaria.

Propiedades básicas de los homomorfismos de grupos.

Proposición 3.3.1 *Sea $\phi : G_1 \to G_2$ un homomorfismo de grupos. Entonces*

1. *Si e es la identidad de G_1, entonces $\phi(e)$ es la identidad de G_2;*
2. *Para cualquier elemento $g \in G_1$, $\phi(g^{-1}) = [\phi(g)]^{-1}$;*
3. *Si H_1 es un subgrupo de G_1, entonces $\phi(H_1)$ es un subgrupo de G_2;*
4. *Si H_2 es un subgrupo de G_2, entonces $\phi^{-1}(H_2) = \{g \in G_1 : \phi(g) \in H_2\}$ es un subgrupo de G_1. Más aún, si H_2 es normal en G_2, entonces $\phi^{-1}(H_2)$ es normal en G_1.*

Ejercicio 3.3.1 *Demostrar la Proposición 3.3.1.*

Definición 3.3.2 *Sea $\phi : G \to H$ un homomorfismo de grupos y supongamos que e es la identidad de H. Por la Proposición 3.3.1, $\phi^{-1}(\{e\})$ es un subgrupo de G. Este subgrupo se llama núcleo de ϕ y se denotará por* $\ker\phi$.

De hecho, este subgrupo es un subgrupo normal de G pues el subgrupo trivial es normal en H.

El siguiente teorema dice que a cada homomorfismo de grupos podemos asociar de forma natural un subgrupo normal.

Teorema 3.3.1 *Sea $\phi : G \to H$ un homomorfismo de grupos. Entonces el núcleo de ϕ es un subgrupo normal de G.*

Ejemplo 3.3.2

1. *Examinemos el homorfismo $\phi : GL_2(\mathbb{R}) \to \mathbb{R}^*$ definido por $A \mapsto \det(A)$. Como 1 es la identidad de $\mathbb{R}^*$, el núcleo de este homomorfismo consiste de toda las matrices de 2×2 que tienen determinante uno. Es decir, $\ker \phi = SL_2(\mathbb{R})$.*
2. *El núcleo del homomorfismo de grupos $\phi : \mathbb{R} \to \mathbb{C}^*$ definido por $\phi(\theta) = \cos\theta + i \sin\theta$ es $\{2\pi n : n \in \mathbb{Z}\}$. Notemos que $\ker \phi \cong \mathbb{Z}$.*
3. *Sea G un grupo. Supongamos que $g \in G$ y ϕ es el homomorfismo de $\mathbb{Z}$ a G dado por $\phi(n) = g^n$. Si el orden de g es infinito, entonces el núcleo de este homomorfismo es $\{0\}$ pues ϕ envía $\mathbb{Z}$ en el subgrupo cíclico de G generado por g. Si en cambio, el orden de g es finito, digamos n, entonces el núcleo de ϕ es $n\mathbb{Z}$.*

3.4 Teoremas de Isomorfía

En la sección anterior vimos que con cada homomorfismo de grupos $\phi : G \to H$ podemos asociar un subgrupo normal de G, $\ker \phi$. El recíproco también es cierto; es decir, todo subgrupo normal de un grupo G da lugar a un homomorfismo de grupos.

Ejercicio 3.4.1 *Sea H un subgrupo normal de G. Muestre que*

$$\phi : G \to G/H$$

definida por

$$\phi(g) = gH.$$

es un homomorfismo. Este homomorfismo se llama homorfismo natural o homomorfismo canónico.

Note que el núcleo de este homomorfismo es H. Los siguientes teoremas describen la relación entre homomorfismos de grupos, subgrupos normales, y grupos cociente.

Teorema 3.4.1 (**Primer Teorema de Isomorfía**) *Si $\psi : G \to H$ es un homomorfismo de grupos con $K = \ker \psi$, entonces K es normal en G. Sea $\phi : G \to G/K$ el homomorfismo canónico. Entonces existe un único isomorfismo $\eta : G/K \to \psi(G)$ tal que $\psi = \eta\phi$.*

Ejemplo 3.4.1 *Sea G un grupo cíclico con generador g. Definamos una función $\phi : \mathbb{Z} \to G$ por $n \mapsto g^n$. Esta función es un homomorfismo sobreyectivo pues*

$$\phi(m+n) = g^{m+n} = g^m g^n = \phi(m)\phi(n).$$

Claramente ϕ es sobreyectivo. Si $|g| = m$, entonces $g^m = e$. Luego, $\ker\phi = m\mathbb{Z}$ y $\mathbb{Z}/\ker\phi = \mathbb{Z}/m\mathbb{Z} \cong G$. Por otra parte, si el orden de g es infinito, entonces $\ker\phi = \{0\}$ y ϕ es un isomorfismo de G en $\mathbb{Z}$. Luego, dos grupos cíclicos son isomorfos exactamente cuando tienen el mismo orden.

Teorema 3.4.2 (**Segundo Teorema de Isomorfía**) *Sea H un subgrupo de G (no necesariamente normal) y sea N un subgrupo normal de G. Entonces HN es un subgrupo de G, $H \cap N$ es un subgrupo normal de H, y*

$$H/H \cap N \cong HN/N.$$

Teorema 3.4.3 (**Tercer Teorema de Isomorfía**) *Sea G un grupo y sean N y H subgrupos normales de G con $N \subset H$. Entonces*

$$G/H \cong \frac{G/N}{H/N}.$$

3.5 Ejercicios propuestos (Guía 4)

1. Demuestre que $\mathbb{Z} \cong n\mathbb{Z}$ para $n \neq 0$.
2. Demuestre que $\mathbb{C}^*$ es isomorfo al subgrupo de $GL_2(\mathbb{R})$ que consiste de las matrices de la forma
$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$
3. Sea $\phi : G \to H$ un isomorfismo de grupos. Muestre que $\phi(x) = e_H$ si y solo si $x = e_G$, donde e_G y e_H son las identidades de G y H, respectivamente.
4. Sea $G \cong H$. Muestre que si G es cíclico, entonces también lo es H.
5. Un *automorfismo* de un grupo G es un isomorfismo consigo mismo. Demuestre que la conjugación compleja es un automorfismo del grupo aditivo de los números complejos; es decir, muestre que la función $\phi(a+bi) = a - bi$ es un isomorfismo de $\mathbb{C}$ a $\mathbb{C}$.
6. Para cada uno de los siguientes grupos G, determine si es que H es un subgrupo normal de G. Si H es un subgrupo normal, escriba una tabla de Cayley para el grupo cociente G/H.
   a) $G = S_4$ and $H = A_4$.
   b) $G = A_5$ and $H = \{(1), (123), (132)\}$.
   c) $G = S_4$ and $H = D_4$.
   d) $G = \mathbb{Z}$ and $H = 5\mathbb{Z}$.

7. Encuentre todos los subgrupos de D_4. ¿Cuáles subgrupos son normales? ¿Cuáles son todos los grupos cociente de D_4 salvo isomorfismo?

8. Muestre que la intersección de dos subgrupos normales es un subgrupo normal.

9. Sea G un grupo. Considere el conjunto

$$Z(G) = \{x \in G : xg = gx \text{ para todo } g \in G\}.$$

   a) Calcule $Z(S_3)$.

   b) Calcule $Z(GL_2(\mathbb{R}))$.

   c) Es $Z(S_3)$ un subgrupo normal de S_3.

10. Sea $\varphi : (\mathbb{R}, +) \to (\mathbb{R} - \{0\}, \cdot)$ definida por:

$$\varphi(x) = 5^x$$

    ¿Es φ un homomorfismo?

11. Sea G un grupo abeliano. Se define la función $f : G \to G$ como $f(g) = g^2$. Demuestre que f es un homomorfismo.

12. Considere $\varphi : (\mathbb{Z}, +) \to (\{1, -1\}, \cdot)$ la función definida por:

$$\varphi(n) = (-1)^n$$

    a) ¿φ esta bien definida como función?

    b) ¿ φ es un homomorfismo?

13. Sea $G = \{e, g, g^2\}$ un grupo de orden 3 bajo la operación definida según la tabla:

$*$	e	g	g^2
e	e	g	g^2
g	g	g^2	e
g^2	g^2	e	g

    Considere la función $h : G \to G$ definida por:

$$h(e) = e \quad , \quad h(g) = g^2 \quad y \quad h\left(g^2\right) = g$$

    Decida si h es un homomorfismo.

14. Sea $\varphi : G \to H$ un homomorfismo del grupo $(G, \cdot)$ al grupo $(H, *)$. Demuestre que:

    a) $\varphi\left(e_G\right) = e_H$.

    b) $\varphi\left(g^{-1}\right) = (\varphi(g))^{-1}$.

c) Si $g_1 \cdot g_2 = g_2 \cdot g_1$, entonces $\varphi(g_1) * \varphi(g_2) = \varphi(g_2) * \varphi(g_1)$.

15. Construya un homomorfismo entre los grupos $(\mathbb{R}^+, \cdot)$ y $(\mathbb{R}, +)$.

16. Considere los grupos G, G' y G''. Sea $\varphi : G \to G'$ un homomorfismo de G en G' y $\psi : G' \to G''$ un homomorfismo de G' en G''. Decida si :

$$\psi \circ \varphi = \psi(\varphi) : G \to G''$$

es un homomorfismo de G en G''.

17. Considere los grupos $G = \mathbb{R}^2$ con la suma usual de vectores y $H = \mathbb{R}$ con la suma usual. Se define $\phi : \mathbb{R}^2 \to \mathbb{R}$ como $\phi(x, y) = x$ (la proyección sobre el Eje X). Pruebe que ϕ es un homomorfismo.

18. Considere el conjunto:

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{R} \wedge ac \neq 0 \right\}$$

Sea $\varphi : G \to \mathbb{R} - \{0\}$ definida por:

$$\varphi \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = a$$

a) Pruebe que $G \leq GL_2(\mathbb{R})$.

b) Demuestre que φ es un homomorfismo entre los grupos G y $\mathbb{R} - \{0\}$ (cada uno con la operación multiplicación usual).

CAPÍTULO 4

Acciones de grupos

Las acciones de grupo generalizan la multiplicación en el grupo. Si G es un grupo y X es un conjunto arbitrario, entonces una acción de grupo de un elemento $g \in G$ en un elemento $x \in X$ es un producto, gx, que está en X. Muchos problemas en álgebra se pueden enfrentar mejor con acciones de grupo.

4.1 Grupos Actuando en Conjuntos

Sea X un conjunto y sea G un grupo. Una *acción* (izquierda) de G en X es una función $G \times X \to X$ dada por $(g, x) \mapsto g \cdot x$, donde

1. $e \cdot x = x$ para todo $x \in X$;
2. $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$ para todo $x \in X$ y todo $g_1, g_2 \in G$.

Con estas condiciones X se denomina *G-conjunto*. Notemos que no pedimos que X esté relacionado con G de ninguna forma. Es verdad que cualquier grupo G actúa en cualquier X con la acción trivial $(g, x) \mapsto x$; pero, las acciones de grupo resultan más interesantes si el conjunto X tiene alguna relación con G.

Ejemplo 4.1.1

1. *Sea $G = D_4$ el grupo de simentría de un cuadrado. Si $X = \{1, 2, 3, 4\}$ es el conjunto de vértices del cuadrado, entonces podemos considerar D_4 como el conjunto de las siguientes permutaciones:*

$$\{(1), (13), (24), (1432), (1234), (12)(34), (14)(23), (13)(24)\}.$$

   Los elementos de D_4 actúan en X como funciones. La permutación $(13)(24)$ actúa en el vértice 1 enviándolo al vértice 3, en el vértice 2 enviándolo al vértice 4, y así sucesivamente.

En general, si X es cualquier conjunto y G es un subgrupo de S_X, el grupo de todas las permutaciones actuando en X, entonces X es un G-conjunto con la acción de grupo

$$(\sigma, x) \mapsto \sigma(x)$$

para $\sigma \in G$ y $x \in X$.

Ejercicio 4.1.1

1. *Si tomamos $X = G$, entonces cualquier grupo G actúa en sí mismo por medio de su representación regular izquierda; es decir, $(g, x) \mapsto \lambda_g(x) = gx$, donde λ_g es multiplicación a la izquierda:*

$$e \cdot x = \lambda_e(x) = x$$
$$(gh) \cdot x = \lambda_{gh}(x) = \lambda_g\lambda_h(x) = \lambda_g(hx) = g \cdot (h \cdot x).$$

   Si H es un subgrupo de G, entonces G es un H-conjunto bajo multiplicación izquierda por elementos de H.

2. *Sea G un grupo y supongamos que $X = G$. Si H es un subgrupo de G, entonces G es un H-conjunto bajo conjugación; es decir, podemos definir una acción de H en G,*

$$H \times G \to G,$$

   via

$$(h, g) \mapsto h \cdot g = hgh^{-1}$$

   para $h \in H$ y $g \in G$. Claramente, se satisface el primer axioma para una acción de grupo. Observando que

$$\begin{aligned}(h_1h_2) \cdot g &= h_1h_2g(h_1h_2)^{-1} \\ &= h_1(h_2gh_2^{-1})h_1^{-1} \\ &= h_1(h_2 \cdot g)h_1^{-1} \\ &= h_1 \cdot (h_2 \cdot g),\end{aligned}$$

   vemos que la segunda condición también se satisface.

3. *Sea H un subgrupo de G y $\mathcal{L}_H$ el conjunto de clases laterales izquierdas de H. El conjunto $\mathcal{L}_H$ es un G-conjunto bajo la acción*

$$(g, xH) \mapsto gxH.$$

   Nuevamente, es fácil ver que se satisface el primer axioma. Como $(gg')xH = g(g'xH)$, el segundo axioma también es válido.

Definición 4.1.1 *Si G actúa en un conjunto X y $x, y \in X$, entonces x se dice G-equivalente a y si existe $g \in G$ tal que $g \cdot x = y$. Escribimos $x \sim_G y$ o $x \sim y$ si dos elementos son G-equivalentes.*

Recordatorio:
Una noción fundamental en matemáticas es la de igualdad. Podemos generalizar la igualdad por medio de las *relaciones de equivalencia* y las *clases de equivalencia*. Una *relación de equivalencia* en un conjunto X es una relación $R \subset X \times X$ tal que

i) $(x, x) \in R$ para todo $x \in X$ (**propiedad refleja**)

ii) $(x, y) \in R$ implica $(y, x) \in R$ (**propiedad simétrica**)

iii) (x, y) y $(y, z) \in R$ implica $(x, z) \in R$ (**propiedad transitiva**)

Dada una relación de equivalencia R en un conjunto X, usualmente escribiremos $x \sim y$ en lugar de $(x, y) \in R$. Si la relación de equivalencia ya tiene asociada una notación como $=$, $\equiv$, o $\cong$, usaremos esa notación.

Proposición 4.1.1 *Sea X un G-conjunto. Entonces la G-equivalencia es una relación de equivalencia en X.*

Dem: *Parte Tarea 1 (RA3).*

Definición 4.1.2 *Sea X un G-conjunto. Para un elemento $x \in X$ su órbita $\mathcal{O}_x \subseteq X$ es el conjunto de sus imágenes respecto a las acciones de G:*

$$\mathcal{O}_x := \{g \cdot x : g \in G\}.$$

Ejemplo 4.1.2 *Sea G el grupo de permutaciones definido por*

$$G = \{(1), (123), (132), (45), (123)(45), (132)(45)\}$$

y $X = \{1, 2, 3, 4, 5\}$. Entonces X es un G-conjunto. Las órbitas son $\mathcal{O}_1 = \mathcal{O}_2 = \mathcal{O}_3 = \{1, 2, 3\}$ y $\mathcal{O}_4 = \mathcal{O}_5 = \{4, 5\}$.

Supongamos que G es un grupo actuando en un conjunto X y sea g un elemento de G. El *conjunto de puntos fijos* de g en X, denotado por X_g, es el conjunto de todos los $x \in X$ tales que $g \cdot x = x$. Podemos también estudiar los elementos g del grupo que fijan un $x \in X$ dado. Este conjunto es más que un subconjunto de G, es un *subgrupo*. Este subgrupo se llama el *subgrupo estabilizador* o *subgrupo de isotropía* de x. Denotaremos el *subgrupo estabilizador* de x por G_x.

$$G_x := \{g \in G : g \cdot x = x\} \subseteq G.$$

Ejemplo 4.1.3 *Sea $X = \{1, 2, 3, 4, 5, 6\}$ y supongamos que G es el grupo de permutaciones dado por las permutaciones*

$$\{(1), (12)(3456), (35)(46), (12)(3654)\}.$$

Entonces los conjuntos de puntos fijos de X bajo la acción de G son

$$X_{(1)} = X,$$
$$X_{(35)(46)} = \{1, 2\},$$
$$X_{(12)(3456)} = X_{(12)(3654)} = \emptyset,$$

y los subgrupos estabilizadores son

$$G_1 = G_2 = \{(1), (35)(46)\},$$
$$G_3 = G_4 = G_5 = G_6 = \{(1)\}.$$

Es fácil ver que G_x es un subgrupo de G para cada $x \in X$.

Proposición 4.1.2 *Sea G un grupo actuando en un conjunto X y sea $x \in X$. El estabilizador de x, G_x, es un subgrupo de G.*

Dem: *En clases.*

El número de elementos en el conjunto de puntos fijos de un elemento $g \in G$ lo denotaremos por $|X_g|$ y el número de elementos en la órbita de $x \in X$ lo denotaremos por $|\mathcal{O}_x|$. El siguiente teorema establece la relación entre las órbitas de un elemento $x \in X$ y las clases laterales izquierdas de G_x en G.

Teorema 4.1.1 *Sea G un grupo finito y sea X un G-conjunto finito. Si $x \in X$, entonces $|\mathcal{O}_x| = [G : G_x]$.*

Dem: *Sabemos que $|G|/|G_x|$ es el número de clases laterales izquierdas de G_x en G por el Teorema de Lagrange. Definiremos una función biyectiva ϕ de la órbita $\mathcal{O}_x$ de x al conjunto de clases laterales izquierdas $\mathcal{L}_{G_x}$ de G_x en G. Sea $y \in \mathcal{O}_x$. Entonces existe g en G tal que $gx = y$. Definamos ϕ de forma que $\phi(y) = gG_x$. Para mostrar que ϕ es 1-1, supongamos que $\phi(y_1) = \phi(y_2)$. Entonces*

$$\phi(y_1) = g_1G_x = g_2G_x = \phi(y_2),$$

donde $g_1x = y_1$ y $g_2x = y_2$. Como $g_1G_x = g_2G_x$, existe $g \in G_x$ tal que $g_2 = g_1g$,

$$y_2 = g_2x = g_1gx = g_1x = y_1;$$

por lo tanto, la función ϕ es 1-1. Finalmente, debemos mostrar que ϕ es sobreyectiva. Sea gG_x una clase lateral izquierda. Si $gx = y$, entonces $\phi(y) = gG_x$.

4.2 La Ecuación de Clase

Sea X un G-conjunto finito y X_G el conjunto de puntos fijos en X; es decir,

$$X_G = \{x \in X : g \cdot x = x \text{ para todo } g \in G\}.$$

Como las óribitas de la acción particionan a X,

$$|X| = |X_G| + \sum_{i=k}^{n} |\mathcal{O}_{x_i}|,$$

donde $x_k, \ldots, x_n$ son representantes de las distintas órbitas no triviales de X (aquellas órbitas que contienen más de un elemento).

Ahora consideremos el caso especial en el que G actúa en sí mismo por conjugación, $(g, x) \mapsto gxg^{-1}$. El centro de G,

$$Z(G) = \{x : xg = gx \text{ para todo } g \in G\},$$

es el conjunto de puntos que quedan fijos por conjugación. La órbitas de la acción se llaman *clases de conjugación* de G. Si $x_1, \ldots, x_k$ son representantes de cada una de las clases de conjugación no-triviales de G y $|\mathcal{O}_{x_1}| = n_1, \ldots, |\mathcal{O}_{x_k}| = n_k$, entonces

$$|G| = |Z(G)| + n_1 + \cdots + n_k.$$

Cada uno de los subgrupos estabilizadores de uno de los x_i, $C(x_i) = \{g \in G : gx_i = x_i g\}$, se llama *subgrupo centralizador* de x_i. Por el Teorema (4.1.1), obtenemos la *ecuación de clase*

$$|G| = |Z(G)| + [G : C(x_1)] + \cdots + [G : C(x_k)].$$

Una de las consecuencias de la *ecuación de clase* es que el orden de cada clase de conjugación divide al orden de G.

Ejemplo 4.2.1

1. *Es fácil verificar que las clases de conjugación en S_3 son las siguientes:*

$$\{(1)\}, \quad \{(123), (132)\}, \quad \{(12), (13), (23)\}.$$

   La ecuación de clase es $6 = 1 + 2 + 3$.

2. *El centro de D_4 es $\{(1), (13)(24)\}$, y las clases de conjugación*

$$\{(13), (24)\}, \quad \{(1432), (1234)\}, \quad \{(12)(34), (14)(23)\}.$$

   Por lo tanto, la ecuación de clase para D_4 es $8 = 2 + 2 + 2 + 2$.

Teorema 4.2.1 *Sea G un grupo de orden p^n donde p es primo. Entonces G tiene centro no-trivial.*

Dem: *Aplicamos la ecuación de clase*

$$|G| = |Z(G)| + n_1 + \cdots + n_k.$$

Como cada $n_i > 1$ y $n_i \mid |G|$, concluimos que p divide a cada n_i. Además, $p \mid |G|$; luego, p divide a $|Z(G)|$. Como la identidad siempre está en el centro de G, $|Z(G)| \geq 1$. Por lo tanto, $|Z(G)| \geq p$, y existe algún $g \in Z(G)$ tal que $g \neq 1$.

Corolario 4.2.1 *Sea G un grupo de orden p^2 donde p es primo. Entonces G es abeliano.*

Dem: *Por el Teorema (4.2.1), $|Z(G)| = p$ o p^2. Si $|Z(G)| = p^2$, estamos listos. Supongamos que $|Z(G)| = p$. Entonces $Z(G)$ y $G/Z(G)$ ambos tienen orden p y por ende ambos son cíclicos. Eligiendo un generador $aZ(G)$ para $G/Z(G)$, podemos escribir cualquier elemento $gZ(G)$ en el cociente como $a^m Z(G)$ para algún entero m; luego, $g = a^m x$ para algún x en el centro de G. Similarmente, si $hZ(G) \in G/Z(G)$, entonces existe y en $Z(G)$ tal que $h = a^n y$ para algún entero n. Como x e y están en el centro de G, conmutan con todos los elementos de G; por lo tanto,*

$$gh = a^m x a^n y = a^{m+n} xy = a^n y a^m x = hg,$$

y G es abeliano.

4.3 Teorema de conteo de Burnside

Supongamos que deseamos pintar los vértices de un cuadrado con dos colores diferentes, digamos blanco y negro. Podríamos sospechar que habría $2^4 = 16$ coloreados diferentes. Pero, algunos de estos son equivalentes. Si pintamos el primer vértice negro y los demás vértices blancos, es lo mismo que pintar el segundo vértice negro y los demás blancos pues podemos obtener el segundo coloreado simplemente rotando el cuadrado 90°.

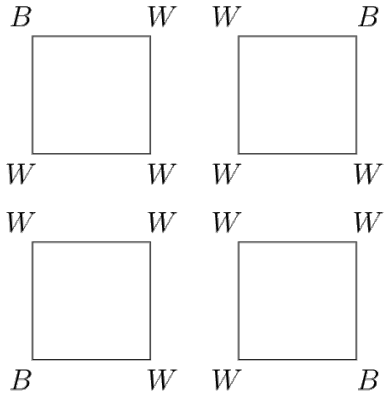


Figura 4.1: Coloreados equivalentes del cuadrado.

El *Teorema de Conteo de Burnside* ofrece un método de calcular el número de maneras distinguibles en que algo puede ser realizado. Además de sus aplicaciones geométricas, el teorema tiene interesantes aplicaciones en teoría de conmutación (switching theory) y en química. La demostración del Teorema de Conteo de Burnside depende del siguiente lema.

Lema 4.3.1 *Sea X un G-conjunto y supongamos que $x \sim y$. Entonces G_x es isomorfo a G_y. En particular, $|G_x| = |G_y|$.*

Dem: *Supongamos que la acción de G en X está dada por $(g, x) \mapsto g \cdot x$. Como $x \sim y$, existe $g \in G$ tal que $g \cdot x = y$. Sea $a \in G_x$. Como*

$$gag^{-1} \cdot y = ga \cdot g^{-1}y = ga \cdot x = g \cdot x = y,$$

podemos definir una función $\phi : G_x \to G_y$ por $\phi(a) = gag^{-1}$. La función ϕ es un homomorfismo pues

$$\phi(ab) = gabg^{-1} = gag^{-1}gbg^{-1} = \phi(a)\phi(b).$$

Supongamos que $\phi(a) = \phi(b)$. Entonces $gag^{-1} = gbg^{-1}$ y $a = b$; es decir, la función es inyectiva. Para mostrar que ϕ es sobreyectiva, sea b en G_y; entonces $g^{-1}bg$ está en G_x pues

$$g^{-1}bg \cdot x = g^{-1}b \cdot gx = g^{-1}b \cdot y = g^{-1} \cdot y = x;$$

y $\phi(g^{-1}bg) = b$.

Teorema 4.3.1 (**Burnside**) *Sea G un grupo finito que actuando en un conjunto X y sea k el número de órbitas de X. Entonces*

$$k = \frac{1}{|G|}\sum_{g\in G}|X_g|.$$

Dem: *Consideramos todos los puntos fijos de x para cada elemento $g \in G$; es decir, consideramos todos los g y todos los x tales que $gx = x$. En términos de conjuntos de puntos fijos, el número de todos los g que fijan a x es*

$$\sum_{g\in G}|X_g|.$$

Pero, en términos de subgrupos estabilizadores, este número es

$$\sum_{x\in X}|G_x|;$$

luego, $\sum_{g\in G}|X_g| = \sum_{x\in X}|G_x|$. Por el Lema (4.3.1)

$$\sum_{y\in\mathcal{O}_x}|G_y| = |\mathcal{O}_x|\cdot|G_x|.$$

Por el Teorema (4.1.1) y el Teorema de Lagrange, esta expresión es igual a $|G|$. Sumando en las k órbitas distintas, concluimos que

$$\sum_{g\in G}|X_g| = \sum_{x\in X}|G_x| = k\cdot|G|.$$

Ejemplo 4.3.1 *Sea $X = \{1,2,3,4,5\}$ y supongamos que G es el grupo de permutaciones $G = \{(1),(13),(13)(25),(25)\}$. Las órbitas en X son $\{1,3\}$, $\{2,5\}$, y $\{4\}$. Los conjuntos de puntos fijos son*

$$\begin{aligned} X_{(1)} &= X \\ X_{(13)} &= \{2,4,5\} \\ X_{(13)(25)} &= \{4\} \\ X_{(25)} &= \{1,3,4\}. \end{aligned}$$

El Teorema de Burnside dice que

$$k = \frac{1}{|G|}\sum_{g\in G}|X_g| = \frac{1}{4}(5+3+1+3) = 3.$$

Ejemplo 4.3.2 (**Geométrico**) *Antes de aplicar el Teorema de Burnside a problemas de teoría de conmutación, examinemos el número de maneras en que se pueden colorear los vértices de un cuadrado utilizando dos colores, blanco y negro. Notemos que a veces obtendremos coloreados equivalentes simplemente aplicando un movimiento rígido al cuadrado. Por ejemplo, como mencionamos antes, si pintamos un vértice negro y los restantes blancos, no importa cuál es el vértice negro pues una rotación nos dará una forma equivalente de pintarlos.*

El grupo de simetría de un cuadrado, D_4, está dado por las siguientes permutaciones:

(1)	(13)	(24)	(1432)
(1234)	(12)(34)	(14)(23)	(13)(24)

El grupo G actúa en el conjunto de vértices $\{1,2,3,4\}$ en la forma usual. Podemos describir los diferentes coloreados como funciones de X en $Y = \{N, B\}$ donde N y B representan los colores negro y blango, respectivamente. Cada función $f : X \to Y$ describe una forma de colorear las esquinas del cuadrado. Cada $\sigma \in D_4$ induce una permutación $\widetilde{\sigma}$ de los posibles coloreados dada por $\widetilde{\sigma}(f) = f \circ \sigma$ para $f : X \to Y$. Por ejemplo, supongamos que f está definida por

$$\begin{aligned} f(1) &= N \\ f(2) &= B \\ f(3) &= B \\ f(4) &= B \end{aligned}$$

y $\sigma = (12)(34)$. Entonces $\widetilde{\sigma}(f) = f \circ \sigma$ envía el vértice 2 en N y los restantes vértices en B. El conjunto de tales $\widetilde{\sigma}$ es un grupo de permutaciones $\widetilde{G}$ en el conjunto de los posibles coloreados. Digamos que $\widetilde{X}$ denota el conjunto de todos los posibles coloreados; es decir, $\widetilde{X}$ es el conjunto de todas las posibles funciones de X en Y. Ahora debemos calcular el número de clases de equivalencia respecto a $\widetilde{G}$.

1. *$\widetilde{X}_{(1)} = \widetilde{X}$ pues la identidad fija todos los posibles coloreados. $|\widetilde{X}| = 2^4 = 16$.*
2. *$\widetilde{X}_{(1234)}$ consiste de todas las $f \in \widetilde{X}$ tales que f no cambia al aplicarle la permutación (1234). En este caso $f(1) = f(2) = f(3) = f(4)$, de manera que todos los valores de f deben ser iguales; es decir, ya sea $f(x) = N$ o $f(x) = B$ para todos los vértices x del cuadrado. Así $|\widetilde{X}_{(1234)}| = 2$.*
3. *$|\widetilde{X}_{(1432)}| = 2$.*
4. *Para $\widetilde{X}_{(13)(24)}$, $f(1) = f(3)$ y $f(2) = f(4)$. Luego, $|\widetilde{X}_{(13)(24)}| = 2^2 = 4$.*
5. *$|\widetilde{X}_{(12)(34)}| = 4$.*
6. *$|\widetilde{X}_{(14)(23)}| = 4$.*
7. *Para $\widetilde{X}_{(13)}$, $f(1) = f(3)$ y las demás esquinas pueden ser de cualquier color; luego, $|\widetilde{X}_{(13)}| = 2^3 = 8$.*
8. *$|\widetilde{X}_{(24)}| = 8$.*

Por el Teorema de Burnside, podemos conluir que hay exactamente

$$\frac{1}{8}(2^4 + 2^1 + 2^2 + 2^1 + 2^2 + 2^2 + 2^3 + 2^3) = 6.$$

Índice alfabético