Una introducción a la teoría de grupos

Noemí Patricia Kisbye

Fa.M.A.F

Facultad de Matemática, Astronomía y Física

Universidad Nacional de Córdoba

Índice general

Una introducción a la teoría de grupos

1. Introducción

La relación de congruencia módulo un entero positivo n determina una relación de equivalencia en el conjunto de los números enteros. Las operaciones de suma y multiplicación entera inducen operaciones similares entre las clases de equivalencia. Cada una de estas clases se identifica con un elemento del conjunto $\{0, 1, \ldots, n-1\}$, al que denotaremos $\mathbb{Z}_n$, y este conjunto queda entonces dotado de dos operaciones: suma y multiplicación módulo n.

Esto da lugar a la construcción de una familia de estructuras algebraicas, $\mathbb{Z}_n$, que reciben el nombre de *grupos de congruencia*. Los grupos, en general, son conjuntos munidos de una operación que es asociativa, con elemento neutro y en la que cada elemento tiene un inverso con respecto a dicha operación. En este texto se desarrolla fundamentalmente los grupos de congruencias $\mathbb{Z}_n$ y los grupos de permutaciones S_n como ejemplos de grupos conmutativos y no conmutativos, respectivamente. Se presenta además la teoría introductoria a la estructura de grupo, definiendo además grupos cíclicos, generadores, subgrupos, coclases y el clásico Teorema de Lagrange.

Estas notas fueron escritas inicialmente como parte de los contenidos de un curso de Álgebra y Matemática Discreta, dictado en FAMAF en los años 2001 y 2002, para estudiantes de primer año. Al final del texto se ha incluído una lista de ejercicios y referencia a bibliografía complementaria para quien desee profundizar en estos temas.

Es mi mayor deseo que estas notas sean útiles, tanto al estudiante como parte de su formación matemática, como al docente en su tarea de formar. Agradezco todas las sugerencias y comentarios que permitan mejorar esta presente edición.

2. Congruencias

Denotaremos con $\mathbb{N}$ y $\mathbb{Z}$ a los números naturales y enteros, respectivamente. Si m y n son números enteros, y $n \neq 0$ diremos que m *divide a* n o que n *es un múltiplo de* m si $n = q \cdot m$ para algún entero q. Equivalentemente, si el resto de la división de n por m es 0.

Se dice que un número entero p es *primo* si p es distinto de 1 y de -1 y sus únicos divisores son p, $-p$, 1 y -1. Por ejemplo, 2, 3, -11 y 53 son números primos. Se dice que dos números enteros son *coprimos* entre sí si no tienen ningún divisor común, excepto el 1 y el -1. Por ejemplo, 10 y 21 son coprimos entre sí, ya que 2, 5 y 10 no son divisores de 21. También podemos decir que dos números enteros a y b son coprimos si los primos que aparecen en la factorización de a no aparecen en la factorización de b.

DEFINICIÓN 2.1. Dado un número natural n, decimos que dos números enteros a y b son *congruentes módulo* n si $(a-b)$ es divisible por n y se escribe

$$a \equiv b \mod (n).$$

Por ejemplo,

$$27 \equiv 12 \mod 5 \qquad \text{y} \qquad -2 \equiv 16 \mod 3$$

puesto que $27 - 12 = 3 \cdot 5$, y $-2 - 16 = -18 = (-6) \cdot 3$.

Notemos que si r es el resto de la división por n de un entero a, entonces a es congruente a r módulo n. Por lo tanto, podemos decir que dos enteros son congruentes módulo n si tienen el mismo resto en la división por n.

Por ejemplo, 27 y 12 tienen resto 2 en la división por 5, mientras que -2 y 16 tienen resto 1 en la división por 3 (notar que $-2 = 3 \cdot (-1) + \mathbf{1}$).

LEMA 2.2. *Si* $a \equiv b \mod (n)$ *y* $c \equiv d \mod (n)$, *entonces*

$$a + c \equiv b + d \mod (n) \quad \textit{y} \quad a \cdot c \equiv b \cdot d \mod (n).$$

PRUEBA. Según la Definición 2.1 debemos mostrar que $(a+c) - (b+d)$ y $(a \cdot c) - (b \cdot d)$ son enteros divisibles por n. En efecto,

$$(a+c) - (b+d) = (a-b) + (c-d)$$

$$(a \cdot c) - (b \cdot d) = (a-b) \cdot c + b \cdot (c-d).$$

En ambos casos el miembro derecho es una suma de múltiplos de n, y por lo tanto es divisible por n. □

Una consecuencia de este lema es que si $a \equiv b \mod (n)$, entonces podemos multiplicar miembro a miembro k congruencias de éstas y obtener

$$a^k \equiv b^k \mod (n),$$

donde a^k y b^k indican el producto repetido k veces de a y b respectivamente.

Dado que además todo número es congruente a sí mismo, es decir $c \equiv c \mod (n)$, tenemos también que si $a \equiv b \mod (n)$ entonces

$$a \cdot c \equiv b \cdot c \mod (n),$$

cualquiera sea el entero c. Pero en general no es cierto que si $a \cdot c \equiv b \cdot c \mod (n)$ entonces $a \equiv b \mod (n)$, es decir no siempre es posible "simplificar". Veamos esto en un ejemplo:

$$6 \cdot 5 \equiv 4 \cdot 5 \mod (10),$$

pero no es cierto que $6 \equiv 4 \mod (10)$. Precisamos esto en el siguiente lema:

LEMA 2.3. *Sean $a, b, c \in \mathbb{Z}$, $n \in \mathbb{N}$ tales que $a \cdot c \equiv b \cdot c \mod (n)$. Si c y n son coprimos entonces $a \equiv b \mod (n)$.*

En efecto, puesto que n divide a $a \cdot c - b \cdot c = (a - b) \cdot c$, entonces los divisores primos de n deben dividir a $(a - b)$ o a c. Al ser n y c coprimos entre sí esto implica que todo divisor primo de n divide a $a - c$, y por lo tanto n divide a $a - c$. Equivalentemente, $a \equiv c \mod (n)$.

Las propiedades que hemos visto en esta sección nos permitirá definir operaciones de suma y multiplicación en el conjunto $\{0, 1, 2, \ldots, n - 1\}$. Presentamos entonces nuestra próxima sección.

3. Aritmética Modular

Consideremos $\mathbb{Z}_n$ el conjunto de los restos posibles de la división de un número entero por n.

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n - 1\}$$

En $\mathbb{Z}_n$ están definidas las operaciones $\oplus$ y $\odot$ del siguiente modo: Si a, b, c y $d \in \mathbb{Z}_n$, entonces

$$a \oplus b = c \qquad \text{si } a + b \equiv c \mod (n),$$

$$a \odot b = d \qquad \text{si } a.b \equiv d \mod (n),$$

Notemos que $a \oplus b$ y $a \odot b$ están bien definidas por la unicidad del resto en la división por n. Veamos un ejemplo:

EJEMPLO 3.1. En $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ tenemos

$$2 \oplus 3 = 5 \qquad \text{pues } 2 + 3 \equiv 5 \ (6),$$

$$2 \odot 3 = 0 \qquad \text{pues } 2 \cdot 3 \equiv 0 \ (6).$$

$$5 \oplus 4 = 3 \qquad \text{pues } 5 + 4 \equiv 3 \ (6),$$

$$5 \odot 4 = 2 \qquad \text{pues } 5 \cdot 4 \equiv 2 \ (6).$$

Las operaciones $\oplus$ y $\odot$ cumplen las siguientes propiedades:

a) Propiedad conmutativa para la suma y para el producto:

$$a \oplus b = b \oplus a, \qquad a \odot b = b \odot a, \qquad \forall a,\ b\ \in \mathbb{Z}_n.$$

b) Propiedad asociativa para la suma y para el producto:

$$(a \oplus b) \oplus c = a \oplus (b \oplus c), \qquad (a \odot b) \odot c = a \odot (b \odot c), \qquad \forall a,\ b,\ c\ \in \mathbb{Z}_n.$$

c) Existencia de un elemento neutro para la suma:

$$a \oplus 0 = a, \qquad \forall a \in \mathbb{Z}_n,$$

d) Existencia de un elemento neutro para el producto:

$$a \odot 1 = a, \qquad \forall a \in \mathbb{Z}_n,$$

e) Propiedad distributiva del producto con respecto a la suma:

$$a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c), \qquad \forall a, b, c \in \mathbb{Z}_n.$$

f) Existencia del opuesto con respecto a $\oplus$:

Para cada $a \in \mathbb{Z}_n$, existe un único $a' \in \mathbb{Z}_n$ tal que $a \oplus a' = 0$

PRUEBA. Los incisos (a) hasta (e) se deducen de las propiedades de la suma y el producto en los números enteros, y las propiedades de la congruencia.

Veamos f). Si $a = 0$, entonces $a' = 0$. Si $a \neq 0$ entonces $a' = n - a \in \mathbb{Z}_n$. Además $a + (n - a) = n \equiv 0\ (n)$ por lo que $a \oplus a' = a \oplus (n - a) = 0$. Por otro lado, si $a \oplus a' = 0$ y $a \oplus a'' = 0$, entonces $a \oplus a' = a \oplus a''$. Sumando a ambos miembros un opuesto de a, por ejemplo a', concluimos que $a' = a''$, es decir que el opuesto es único. □

Notemos que la suma $\oplus$ es una operación en $\mathbb{Z}_n$ que satisface las siguientes propiedades:

(a) $a \oplus b \in \mathbb{Z}_n$ para todo a, $b \in \mathbb{Z}_n$,

(b) $\oplus$ es asociativa,

(c) existe un elemento neutro para la suma $\oplus$, que denotamos con 0, y

(d) cada elemento $a \in \mathbb{Z}_n$ tiene un opuesto o inverso a' en $\mathbb{Z}_n$.

Un conjunto G con una operación interna que satisface propiedades como las enunciadas anteriormente es un *grupo*. Precisamos este concepto en la próxima sección.

4. Grupos

DEFINICIÓN 4.1. Un grupo es un par $(G, *)$ donde G es un conjunto y $*$ es una operación binaria en G que satisface:

(a) $x * y \in G$ para todo x, $y \in G$,

(b) $x * (y * z) = (x * y) * z$ para todo x, y, $z \in G$,

(c) existe $e \in G$ tal que $e * x = x = x * e$, para todo $x \in G$,

(d) para todo $x \in G$ existe $x' \in G$ tal que $x * x' = x' * x = e$.

EJEMPLO 4.2.

(1) $(\mathbb{Z}, +)$ es un grupo, donde $e = 0$ y $a' = -a$, para cada $a \in \mathbb{Z}$.

(2) $(\mathbb{Z}_m, \oplus)$ es un grupo, donde $e = 0$ y $a' = m - a$ para cada $a \neq 0$

(3) $(\mathbb{Z}, \cdot)$ no es un grupo, pues sólo 1 y -1 tienen inverso.

(4) $(\mathbb{Q} - \{0\}, \cdot)$ es un grupo, donde $e = 1$ y $a' = \frac{1}{a}$.

Notemos que $(\mathbb{Z}_m, \odot)$ no es un grupo pues 0 no tiene inverso respecto de $\odot$. Por otro lado 0 no siempre es el único elemento de $\mathbb{Z}_m$ que no tiene inverso, por ejemplo en $\mathbb{Z}_6$

$$2 \odot 3 = 0$$

por lo que 2 y 3 no pueden tener un inverso.

LEMA 4.3. *$r \in \mathbb{Z}_m$ tiene inverso respecto de $\odot$ si y sólo si $(r, m) = 1$.*

PRUEBA. Si r tiene inverso entonces existe $s \in \mathbb{Z}_m$ tal que $r \odot s = 1$. Eso significa que $r.s \equiv 1\ (m)$. Por lo tanto existe $q \in \mathbb{Z}$ tal que

$$s.r + q.m = 1.$$

Luego r y m son coprimos.

Recíprocamente, si $(r, m) = 1$ entonces existen s y t enteros tales que $s.r + t.m = 1$. Luego $s.r \equiv 1\ (m)$. Por otro lado existe $s_1 \in \mathbb{Z}_m$ tal que $s \equiv s_1\ (m)$ y por lo tanto $s.r \equiv s_1.r\ (n)$ o lo que es lo mismo $s_1 \odot r = 1$. Luego r tiene un inverso. □

No es difícil ver que si a, $b \in \mathbb{Z}_m$ son inversibles, entonces $a \odot b$ también lo es. Sea $\mathbb{Z}_m^*$ el subconjunto formado por los elementos inversibles de $\mathbb{Z}_m$:

$$\mathbb{Z}_m^* = \{k \in \mathbb{Z}_m \mid (k, m) = 1\},$$

entonces $(\mathbb{Z}_m^*, \odot)$ es un grupo.

EJEMPLO 4.4. En adelante, usaremos la notación abreviada $\mathbb{Z}_m$ y $\mathbb{Z}_m^*$ para referirnos a los grupos $(\mathbb{Z}_m, \oplus)$ y $(\mathbb{Z}_m^*, \odot)$, respectivamente.

(i) $\mathbb{Z}_2^* = \{1\}$, es el grupo trivial,

(ii) $\mathbb{Z}_3^* = \{1, 2\}$, y $2 \odot 2 = 1 \odot 1 = 1$ y $2 \odot 1 = 1 \odot 2 = 2$.

(iii) $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$, aquí $a \odot a = 1$, para todo $a \in \mathbb{Z}_{12}^*$.

Si en un grupo $(G, *)$, G tiene una cantidad finita de elementos, podemos hacer una tabla de doble entrada para representar la operación del grupo.

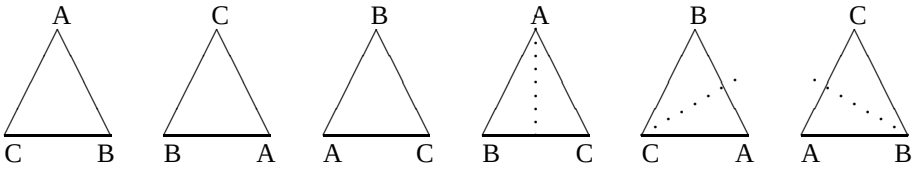
EJEMPLO 4.5. Las operaciones $\oplus$ y $\odot$ en $\mathbb{Z}_4$ y $\mathbb{Z}_5^*$ pueden ser resumidas en las siguientes tablas, donde para calcular $a * b$ debemos mirar en la fila correspondiente a a y la columna correspondiente a b.

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

y

$\odot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

EJEMPLO 4.6. Consideremos un triángulo equilátero $\triangle$ en el plano, y sea G el conjunto de todos los movimientos rígidos del plano que dejan estable al triángulo. Este conjunto tiene 6 elementos, también llamados *simetrías* del triángulo:



La transformación id es la identidad en el plano, r y s son rotaciones en el sentido horario en un ángulo de $\frac{\pi}{3}$ y $\frac{2\pi}{3}$ respectivamente, y x, y y z son reflexiones respecto del eje marcado en

la figura. La composición de dos simetrías es una simetría. Si llamamos

$$G_\Delta = \{id,\ r,\ s, x,\ y,\ z\}$$

y $*$ representa la composición dos transformaciones, entonces $(G_\Delta, *)$ es un grupo.

La tabla correspondiente a $(G_\Delta, *)$ es la siguiente:

*	id	r	s	x	y	z
id	id	r	s	x	y	z
r	r	s	id	y	z	x
s	s	id	r	z	x	y
x	x	z	y	id	s	r
y	y	x	z	r	id	s
z	z	y	x	s	r	id

Notemos que $x * y = s$ y $y * x = r$, es decir que la operación $*$ no es conmutativa. Los inversos están dados por:

$$(id)' = id, \qquad r' = s \qquad\qquad x' = x \quad y' = y \quad z' = z.$$

De ahora en más simplificaremos nuestra notación cuando sea posible. Si $(G, *)$ es un grupo nos referiremos al *grupo G* y usaremos la notación xy en lugar de $x * y$, 1 en lugar de e y x^{-1} en lugar de x'. No debe confundirse esta notación de yuxtaposición con la multiplicación ordinaria de números. Las únicas propiedades que supondremos ciertas son las que definen a un grupo. Es decir, si x, y, $z \in G$, entonces

$$(xy)z = x(yz), \qquad x\,1 = 1\,x = x, \qquad xx^{-1} = x^{-1}x = 1.$$

En particular, no supondremos que $xy = yx$.

DEFINICIÓN 4.7. Sea G un grupo. Se dice que G es *conmutativo* o *abeliano* si $xy = yx$ para todo x, $y \in G$.

EJEMPLO 4.8. $(\mathbb{Z}, +)$, $(\mathbb{Z}_n, \oplus)$ y $(\mathbb{Z}_n^*, \odot)$ son grupos conmutativos. En cambio $(G_\Delta, *)$ no es conmutativo, puesto que por ejemplo $x * y \neq y * x$.

EJEMPLO 4.9. Consideremos S_3 el conjunto formado por las permutaciones de $\{1, 2, 3\}$, con la operación de composición. Luego $(S_3, \circ)$ es un grupo. Si tomamos los elementos π y $\tau \in S_3$ dados por

$$\pi(1) = 2 \qquad \pi(2) = 1 \qquad \pi(3) = 3,$$
$$\tau(1) = 2 \qquad \tau(2) = 3 \qquad \tau(3) = 1,$$

entonces $(\pi \circ \tau)(1) = 1$ pero $(\tau \circ \pi)(1) = 3$, por lo cual $\pi \circ \tau \neq \tau \circ \pi$. Por lo tanto S_3 no es un grupo conmutativo.

El hecho que un grupo no sea conmutativo no significa que para todo a, $b \in G$ deba ser $ab \neq ba$; notemos que por ejemplo en G_Δ, $rs = sr$. Lo que se debe cumplir para que un grupo no sea conmutativo es que exista *algún* par de elementos a y b tales que $ab \neq ba$.

TEOREMA 4.10. *Sean x, y, z, a, b elementos de un grupo G. Entonces*

(1) $xy = xz \quad \Rightarrow \quad y = z$ *(cancelación a izquierda),*

(2) $ax = bx \quad \Rightarrow \quad a = b$ *(cancelación a derecha).*

PRUEBA. Como G es grupo, para todo $x \in G$ existe el inverso x^{-1}, luego

$$xy = xz \;\Rightarrow\; x^{-1}(xy) = x^{-1}xz \;\Rightarrow\; (x^{-1}x)y = (x^{-1}x)z \;\Rightarrow\; 1.y = 1.z \;\Rightarrow\; y = z.$$

La cancelación a derecha se prueba de una manera análoga. □

Hasta ahora hemos hablado del elemento neutro y del inverso de un elemento x, pero no hemos dicho que exista sólo uno. El siguiente teorema asegura que son únicos.

TEOREMA 4.11. *Sea G un grupo. Entonces*

(i) *El elemento neutro 1 es único,*

(ii) *El inverso de $x \in G$ es único.*

PRUEBA. (i) Si $1\,x = x$ para todo $x \in G$ y $\tilde{1}\,x = x$ para todo $x \in G$, entonces por la ley de cancelación a derecha concluimos que $1 = \tilde{1}$.

(ii) Si $x\,x' = 1 = x\,x''$, entonces por la ley de cancelación a izquierda, $x' = x''$. Por ello es que podemos llamar x^{-1} al inverso de x.

□

DEFINICIÓN 4.12. Sea G un grupo. Si $|G|$ es finito decimos que G es finito y que el *orden de* G es $|G|$. Si $|G|$ no es finito decimos que G es un grupo infinito.

EJEMPLO 4.13. $\mathbb{Z}$ es un grupo infinito. $\mathbb{Z}_n$, $\mathbb{Z}_n^*$, G_Δ y S_3 son grupos finitos. Tenemos que el orden de $\mathbb{Z}_n$ es n, el de $\mathbb{Z}_n^*$ es la cantidad de números positivos coprimos con n menores que n, y el orden de G_Δ y S_3 es 6.

Si G es un grupo y $x \in G$, definimos las sucesivas potencias positivas y negativas de x como:

$$x^1 = x \qquad\qquad x^r = x\,x^{r-1}, \qquad (r \geq 2),$$

$$x^{-1} = x^{-1} \qquad\qquad x^{-r} = x^{-1}x^{-(r-1)} \qquad (r \geq 2).$$

Convenimos en que $x^0 = 1$.

EJERCICIO 4.1. Probar que $x^{m+n} = x^m x^n$.

EJEMPLO 4.14.

(i) En $\mathbb{Z}_6$, $\quad 2^5 = 2 \oplus 2 \oplus 2 \oplus 2 \oplus 2 = 4$.

(ii) En $\mathbb{Z}$, $\quad 2^5 = 2 + 2 + 2 + 2 + 2 = 10$.

(iii) En $\mathbb{Z}_5^*$, $\quad 2^5 = 2 \odot 2 \odot 2 \odot 2 \odot 2 = 2$.

(iv) En G_Δ, $\quad r^5 = r * r * r * r * r = s$.

Notemos que si un grupo es finito y $x \in G$, las sucesivas potencias de x son elementos de G y en consecuencia no son todas distintas. Luego existen k y h naturales distintos tales que $x^k = x^h$. Si $k > h$, multiplicando ambos miembros por x^{-h} obtenemos que $x^{k-h} = 1$. De aquí que podemos asegurar que existe algún $n \in \mathbb{N}$ tal que $x^n = 1$, y por el Principio de Buena Ordenación existe un natural mínimo con esa propiedad.

DEFINICIÓN 4.15. Sea G un grupo finito, y sea $x \in G$. El menor natural n tal que $x^n = 1$ se llama el orden de x en G. Si G es infinito se define el orden de x del mismo modo si es que tal n existe. De lo contrario se dice que el orden de x es infinito.

EJEMPLO 4.16. Puesto que $6x \equiv 0\ (6)$ para todo $x \in \mathbb{Z}$, tenemos que para todo $x \in \mathbb{Z}_6$, $x^6 = 0$. Sin embargo 6 no es el orden de cada elemento de $\mathbb{Z}_6$, pues

$$3 \oplus 3 = 0 \quad \text{y } 2 \oplus 2 \oplus 2 = 0.$$

Luego el orden de 3 es 2 y el orden de 2 es 3. También el orden de 4 es 3. 5 es el único elemento de orden 6 y 0 tiene orden 1.

EJEMPLO 4.17. En el caso de G_Δ, el orden de r y el orden de s es 3, mientras que el orden de x, y y z es 2.

Notemos que para cualquier grupo G, el orden de 1 es 1.

TEOREMA 4.18. *Sea x un elemento de orden m en un grupo finito G. Entonces $x^s = 1$ si y sólo si s es un múltiplo de m.*

PRUEBA. Si $s = km$ entonces $x^s = x^{km} = (x^m)^k = 1^k = 1$. Recíprocamente, si $x^s = 1$ entonces por definición de orden $s \geq m$. Luego existen q y r, $0 \leq r < m$ tales que

$$s = q.m + r.$$

Entonces $1 = x^s = x^{mq+r} = x^{mq}x^r = 1.x^r$. Luego $x^r = 1$, por lo tanto $r = 0$ y esto implica que s es múltiplo de m.

□

4.1. Isomorfismo de Grupos. Consideremos los grupos $(\mathbb{Z}_4, \oplus)$ y $(\mathbb{Z}_5^*, \odot)$. Tomemos la función $f : \mathbb{Z}_4 \mapsto \mathbb{Z}_5^*$ dada por

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

Notemos que f es una función biyectiva, y cumple que $f(0) = 1$ (la imagen del elemento neutro es el elemento neutro) y además $f(a \oplus b) = f(a) \odot f(b)$ para todo a, $b \in \mathbb{Z}_4$. Se dice entonces que f *preserva la estructura de los grupos*.

DEFINICIÓN 4.19. Sean G_1 y G_2 dos grupos cualesquiera. Una biyección $f : G_1 \mapsto G_2$ se dice un *isomorfismo de grupos* si $f(gg') = f(g)f(g')$, para todo g, $g' \in G_1$. Si existe tal isomorfismo, G_1 y G_2 se dicen isomorfos.

5. Grupos cíclicos

DEFINICIÓN 5.1. Un grupo G se dice cíclico si existe $x \in G$ tal que todo elemento de G es una potencia de x. El elemento x se dice que *genera* a G y escribimos $G = \langle x \rangle$.

EJEMPLO 5.2. $\mathbb{Z}$ con la operación de suma usual es un grupo cíclico infinito, más precisamente, $\mathbb{Z} = \langle 1 \rangle$. Efectivamente, si $n \in \mathbb{N}$, entonces

$$n = \underbrace{1 + 1 + \cdots + 1}_{n \text{ términos}} = 1^n.$$

Si $n \in -\mathbb{N}$ entonces

$$-n = 1^{-n}, \text{ por lo cual } n = 1^n.$$

EJERCICIO 5.1. Probar que los únicos generadores de $\mathbb{Z}$ son 1 y -1.

EJEMPLO 5.3. $\mathbb{Z}_6$ con la operación $\oplus$ es un grupo cíclico finito, generado por 1 y también por 5. En efecto:

$1 = 5 \oplus 5 \oplus 5 \oplus 5 \oplus 5$,

$2 = 5 \oplus 5 \oplus 5 \oplus 5$,

$3 = 5 \oplus 5 \oplus 5$.

$4 = 5 \oplus 5$,

$5 = 5$.

EJEMPLO 5.4. $\mathbb{Z}_7^*$ y $\mathbb{Z}_6$ son grupos cíclicos isomorfos. Una biyección $f : \mathbb{Z}_7^* \mapsto \mathbb{Z}_6$ está dada por

$$f(3) = 1, \quad f(3^k) = f(\underbrace{3 \odot \cdots \odot 3}_{k}) = \underbrace{f(3) \oplus \cdots \oplus f(3)}_{k} = (f(3))^k, \quad \text{para } 1 \leq k \leq 6.$$

De este modo resulta

$$f(3) = 1, \qquad f(2) = 2, \qquad f(6) = 3, \qquad f(4) = 4, \qquad f(5) = 5, \qquad f(1) = 0.$$

EJEMPLO 5.5. El grupo G_Δ no es un grupo cíclico, puesto que ningún elemento de G_Δ tiene orden 6.

6. Subgrupos

Si G es un grupo y $H \subseteq G$, entonces se dice que H es un *subgrupo* de G si los elementos de H forman un grupo con respecto a la operación de G.

EJEMPLO 6.1. En G_Δ, $H = \{id, r, s\}$ es subgrupo pues $r\,r = s$, $s\,s = r$ y $r\,s = id$. En cambio $T = \{id, r, x\}$ no es subgrupo de G_Δ pues $r\,x = y$ e $y \notin T$, y también porque r y x no tienen inverso en T.

El siguiente teorema establece una condición necesaria y suficiente para que un subconjunto de un grupo G sea subgrupo:

TEOREMA 6.2. *Sea G un grupo y sea H un subconjunto de G, no vacío, que satisface:*

(i) $xy \in H$, *para todo* $x, y \in H$,

(ii) *si* $x \in H$, *entonces* $x^{-1} \in H$.

Entonces H es un subgrupo de G. Si G es finito, basta que se cumpla (i).

PRUEBA. La condición (i) nos dice que la operación de grupo es cerrada en H. La asociatividad se obtiene de la asociatividad en G. La existencia del inverso está dada por (ii). La

existencia del elemento neutro en H se debe a que si $x \in H$, entonces $x^{-1} \in H$ y por (i), $1 = x.x^{-1} \in H$.

Supongamos ahora que G es finito. Luego para $x \in H$, $x^m \in H$, para todo $m \in \mathbb{N}$. Luego existe $n \in \mathbb{N}$ tal que $x^{n+1} = 1$, por lo tanto x^n es el inverso de x. □

EJEMPLO 6.3. Sea G un grupo y sea $x \in G$ un elemento de orden m. Entonces las potencias de x

$$1,\ x,\ x^2, \ldots, x^{m-1}$$

forman un subgrupo de G, llamado *subgrupo cíclico* generado por x, y se denota $\langle x \rangle$. El orden del subgrupo $\langle x \rangle$ es el orden del elemento x.

Consideremos el grupo $\mathbb{Z}_{12}$. Entonces 2 y 8 generan subgrupos de órdenes 6 y 3 respectivamente. Estos son:

$$\langle 2 \rangle = \{2^0, 2^1, 2^2, 2^3, 2^4, 2^5\} = \{0, 2, 4, 6, 8, 10\},$$
$$\langle 8 \rangle = \{8^0, 8^1, 8^2\} = \{0, 8, 4\}.$$

Por otro lado, el subgrupo cíclico generado por 5 es el grupo $\mathbb{Z}_{12}$ pues $5^m = 0$ en $\mathbb{Z}_{12}$ ocurre sólo cuando $5 \cdot m \equiv 0\ (12)$. Puesto que $(5, 12) = 1$ debe ser m un múltiplo de 12.

7. Grupos de Permutaciones

Una *permutación* de un conjunto finito X es una biyección de X en X. Nuestro objetivo será estudiar el conjunto de permutaciones de un conjunto X de cardinal n. Sin pérdida de generalidad podemos considerar a X como el intervalo natural $[1, n]$, al que denotaremos por $\mathbb{N}_n$.

EJEMPLO 7.1. Por ejemplo, una permutación del conjunto $\mathbb{N}_4$ es la función σ dada por

$$\sigma(1) = 3 \qquad \sigma(2) = 4 \qquad \sigma(3) = 2 \qquad \sigma(4) = 1. \tag{3}$$

Llamaremos S_n al conjunto de permutaciones de $\mathbb{N}_n$. Puesto que la composición de funciones biyectivas es biyectiva, que la inversa de una función biyectiva es biyectiva tenemos que $(S_n, \circ)$ es un grupo finito. Recordemos que el orden de S_n es $|S_n| = n!$.

EJEMPLO 7.2. En este ejemplo y en otros posteriores, usaremos una notación con flechas para representar una permutación σ, indicando con

$$\begin{array}{cccc} 1 & 2 & \dots & n \\ \downarrow & \downarrow & \downarrow & \downarrow \\ a_1 & a_2 & \dots & a_n \end{array}$$

si $a_i = \sigma(i)$, para $1 \leq i \leq n$.

(i) S_3 contiene las siguientes permutaciones:

$$\begin{array}{ccc} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 \end{array} \qquad \begin{array}{ccc} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 3 & 2 \end{array} \qquad \begin{array}{ccc} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \end{array}$$

$$\begin{array}{ccc} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 1 & 3 \end{array} \qquad \begin{array}{ccc} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 1 & 2 \end{array} \qquad \begin{array}{ccc} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 2 & 1. \end{array}$$

(ii) S_2 contiene las siguientes permutaciones:

$$\begin{array}{cc} 1 & 2 \\ \downarrow & \downarrow \\ 2 & 1 \end{array} \qquad \begin{array}{cc} 1 & 2 \\ \downarrow & \downarrow \\ 1 & 2. \end{array}$$

Podemos interpretar una permutación como un reordenamiento de los elementos de $\{1, 2, \ldots, n\}$. Supongamos que β es la permutación en S_4 dada por

$$\begin{array}{cccc} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 4 & 1 & 3. \end{array}$$

Si σ es como en el Ejemplo 7.1, entonces $(\sigma \circ \beta)$ y $(\beta \circ \sigma)$ vienen dadas por:

$$\begin{array}{cccc} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 4 & 1 & 3 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 1 & 3 & 2 \end{array} \qquad \begin{array}{cccc} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 4 & 2 & 1 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 3 & 4 & 2 \end{array}$$

$$(\sigma \circ \beta) \qquad\qquad (\beta \circ \sigma).$$

De ahora en más usaremos la notación $\sigma\beta$ para denotar la aplicación $(\sigma \circ \beta)$, esto quiere decir, *primero se aplica β y luego se aplica σ*.

Es conveniente tener una notación más compacta para denotar una determinada permutación. Notemos que la permutación σ de (7.1) aplica el 1 en el 3, el 3 en el 2, el 2 en el 4 y el 4 en el 1. Esto dice que los símbolos 1, 2, 3 y 4 forman un *ciclo* de longitud 4, y escribimos

$$\sigma = (1324).$$

EJEMPLO 7.3. Consideremos en S_8 la permutación π dada por

$$\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 8 & 5 & 2 & 1 & 6 & 4 & 7. \end{array}$$

Entonces π aplica el 1 en el 3, el 3 en el 5 y el 5 nuevamente al 1. Aplica el 2 en el 8, el 8 en el 7, el 7 en el 4 y el 4 en el 2. Por último, $\pi(6) = 6$. Entonces 1, 3 y 5 forman un ciclo de longitud 3; 2, 8, 7 y 4 forman un ciclo de longitud 4 y 7 forma un ciclo de longitud 1. Es entonces que podemos escribir

$$\pi = (135)(2874)(7) = (2874)(7)(135).$$

Esta es la llamada *notación cíclica* para π.

Precisamos este concepto en la siguiente definición:

DEFINICIÓN 7.4. Sean i_1, i_2, i_r, ($r \leq n$) elementos distintos de $\mathbb{N}_n$. Entonces $(i_1 i_2 \dots i_r)$ denota la permutación que aplica $i_1 \mapsto i_2$, $i_2 \mapsto i_3$, $\dots$, $i_r \mapsto i_1$ y los demás elementos de $\mathbb{N}_n$ los aplica en sí mismos. $(i_1 i_2 \dots i_r)$ se llama un *ciclo* de longitud r; un ciclo de longitud 2 se llama una *trasposición*.

Diremos que dos ciclos $(i_1 i_2 \dots i_r)$ y $(j_1 j_2 \dots j_k)$ son *disjuntos* si ninguno de los i_t, $1 \leq t \leq r$, aparece entre los j_t, $1 \leq t \leq k$.

EJEMPLO 7.5. En S_7, los ciclos (135) y (2476) son disjuntos, en cambio (135) y (2346) no lo son, pues el 3 aparece en ambos ciclos.

Notemos que si σ_1 y σ_2 son ciclos disjuntos, entonces conmutan entre sí, es decir, $\sigma_1\sigma_2 = \sigma_2\sigma_1$, puesto que ningún símbolo permutado por σ_1 es permutado por σ_2, y viceversa.

La notación para un determinado ciclo no es única, por ejemplo $(123) = (231) = (312)$.

LEMA 7.6. *Un ciclo de longitud r es un elemento de orden r en S_n. El inverso del ciclo $(i_1 i_2 \dots i_r)$ es el ciclo de longitud r dado por $(i_r i_{r-1} \dots i_2 i_1)$.*

PRUEBA. Sea $\sigma = (i_1 i_2 \dots i_r)$. Entonces σ^j es la permutación que aplica $i_1 \mapsto i_{[1+j]}$, $i_2 \mapsto i_{[2+j]}$, $\dots$, $i_r \mapsto i_{[r+j]}$, donde con los corchetes hemos querido indicar que $1 \leq [t+r] \leq r$ y que $t+r \equiv [t+r]\ (r)$. Por ejemplo, σ^3 aplica i_{r-1} en i_2, pues $(r-1+3) \equiv 2\ (r)$, y σ^3 aplica i_{r-3} en i_r, pues $r-3+3 \equiv r\ (r)$.

Luego $\sigma^j \neq id$ si $j < r$ pues $\sigma^j(i_1) = i_{1+j} \neq i_1$, pero $\sigma^r(i_t) = i_{[t+r]} = i_t$, para todo t, $1 \leq t \leq r$. Luego el orden de σ es r.

Por otro lado, vemos que $(i_1 i_2 \dots i_r)(i_r \dots i_2 i_1)$ es la permutación identidad, por lo que queda probado el lema.

□

Así por ejemplo, el inverso de una trasposición (ij) es $(ji) = (ij)$, y el inverso de un ciclo de longitud 3, (ijk) es (kji). Notemos que la permutación identidad puede ser escrita como un ciclo de longitud 1, por ejemplo (1).

Cualquier permutación τ en S_n puede ser escrita como producto de ciclos disjuntos de la siguiente manera:

se comienza con cualquier símbolo, por ejemplo el 1, y se lista la imagen del mismo y de sus sucesores hasta llegar nuevamente al 1, de esta manera obtenemos un primer ciclo;

se elige ahora otro símbolo al que no se haya llegado en el ciclo anterior y se construye otro ciclo a partir de él;

se repite el procedimiento hasta que todos los símbolos hayan sido listados.

En general, en la notación cíclica se omiten los ciclos de longitud 1. Así, en el Ejemplo 7.3, $\pi = (135)(2874)$.

Obviamente el ciclo (123) y el ciclo (231) representan la misma permutación, como así también $(135)(24)$ y $(24)(135)$. Lo importante en la notación cíclica es la longitud y el número de ciclos que componen a la permutación, ya que estos nos indican el orden de la permutación.

PROPOSICIÓN 7.7. *El orden de una permutación es el mínimo común múltiplo de los órdenes de los ciclos que la componen.*

PRUEBA. Sea $\sigma = \sigma_1\sigma_2 \dots \sigma_k$, donde σ_1, σ_2, $\dots$, σ_k son ciclos disjuntos entre sí. Sea m el mínimo común múltiplo de los ordenes de estos ciclos. Como los ciclos conmutan entre sí tenemos que

$$\sigma^m = \sigma_1^m\sigma_2^m \dots \sigma_k^m = (1).$$

Por otro lado, si $\sigma^d = (1)$, entonces $\sigma_i^d = (1)$, para $1 \leq i \leq k$, luego el orden de σ_i divide a d para todo $1 \leq i \leq k$. El menor d con esa propiedad es precisamente el mínimo común múltiplo de los órdenes de los ciclos.

□

EJEMPLO 7.8. Se tienen 12 cartas numeradas del 1 al 12, y se disponen sobre la mesa de la manera que se muestra el la figura de abajo, a la izquierda. Si las cartas se sacan por fila y se las reordena por columna, como se indica a la derecha, ¿cuántas veces debe hacerse este procedimiento para que las cartas reaparezcan en su posición original?

$$\begin{matrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \\ 10 & 11 & 12 \end{matrix} \quad , \quad \begin{matrix} 1 & 5 & 9 \\ 2 & 6 & 10 \\ 3 & 7 & 11 \\ 4 & 8 & 12. \end{matrix}$$

PRUEBA. Sea π la permutación que produce dicha reordenación. Es decir $\pi(i) = j$ si la carta numerada con i aparece en el lugar de la carta j. Luego la notación cíclica de π es

$$\pi = (1)(2\ 4\ 10\ 6\ 5\ )(3\ 7\ 8\ 11\ 9\ )(12).$$

Los ciclos (1) y (12) indican que las cartas 1 y 12 siempre aparecen en el mismo lugar. Los otros dos ciclos tienen longitud 5, y esto significa que aplicados 5 veces se vuelve a la posición original.

Esto significa entonces que el orden de la permutación π es 5.

□

8. Clasificación de las permutaciones

El objetivo de esta sección es clasificar a las permutaciones según los ciclos que la componen. Una permutación se puede escribir de manera única como producto de ciclos disjuntos, salvando el orden de los mismos y de los elementos que los componen, aunque no daremos aquí una demostración de este hecho.

DEFINICIÓN 8.1. Si $\pi \in S_n$ tiene α_i ciclos de longitud i entonces diremos que π es del tipo $[1^{\alpha_1} 2^{\alpha_2} \dots n^{\alpha_n}]$.

EJEMPLO 8.2. La permutación π del Ejemplo **??** es del tipo $[134]$ pues está compuesta por un ciclo de longitud 1, uno de longitud 3 y uno de longitud 4. La permutación π del Ejemplo 7.8 es del tipo $[1^2 5^2]$ pues está compuesta por dos ciclos de longitud 1 y dos ciclos de longitud 5.

Es posible clasificar a los elementos de S_n según su tipo. Contemos cuántas permutaciones hay de un determinado tipo $[1^{\alpha_1} \dots n^{\alpha_n}]$. Hagamos primero un ejemplo. Consideremos en S_{14} las permutaciones del tipo $[2^2 3^2 4]$. Una permutación de este tipo será de la forma

$$(\,.\,.\,)(\,.\,.\,)(\,.\,.\,.\,)(\,.\,.\,.\,)(\,.\,.\,.\,.\,).$$

Existen

$$\binom{14}{2}\binom{12}{2}\binom{10}{3}\binom{7}{3}\binom{4}{4}$$

maneras de ubicar los símbolos 1,2,. . . , 14 en una permutación de este tipo. Si además consideramos que cada ciclo de longitud k se puede escribir de k formas distintas, entonces debemos dividir esta cantidad por

$$2 \cdot 2 \cdot 3 \cdot 3 \cdot 4 = 2^2 3^2 4.$$

Por otro lado, el orden en que se ubiquen los ciclos de igual longitud es irrelevante, por lo tanto aún nos falta dividir por

$$2!2!.$$

Luego la cantidad total de permutaciones de este tipo es

$$\frac{14!}{2^2 3^2 4\, 2!\, 2!}.$$

En el caso general, se prueba que el número de permutaciones del tipo $[1^{\alpha_1} 2^{\alpha_2} \dots n^{\alpha_n}]$ es

$$\frac{n!}{1^{\alpha_1} 2^{\alpha_2} \dots n^{\alpha_n} \alpha_1! \alpha_2! \dots \alpha_n!}.$$

Diremos que dos permutaciones α y β en S_n son *conjugadas* si existe una permutación $\sigma \in S_n$ tal que

$$\sigma\alpha\sigma^{-1} = \beta.$$

TEOREMA 8.3. *Dos permutaciones son conjugadas si y sólo si son del mismo tipo.*

PRUEBA. Supongamos que α y β son conjugadas. Lo que haremos es ver que por cada ciclo $(x_1 x_2 \dots x_k)$ en la descomposición de α hay un ciclo $(y_1 y_2 \dots y_k)$ en la descomposición de β. Tomemos x_1. Sea $x_2 = \alpha(x_1)$ y sean $y_1 = \sigma(x_1)$, $y_2 = \sigma(x_2)$. Entonces

$$\beta(y_1) = \sigma\alpha\sigma^{-1}(y_1) = \sigma\alpha(x_1) = \sigma(x_2) = y_2.$$

Ahora, si $\alpha(x_2) = x_3$ y $\sigma(x_3) = y_3$ entonces $\beta(y_2) = y_3$. Luego por cada ciclo $(x_1 x_2 \dots x_k)$ tenemos un correspondiente ciclo $(y_1 y_2 \dots y_k)$. Se sigue entonces que α y β son del mismo tipo.

Recíprocamente, supongamos que α y β son del mismo tipo. Dado que están compuestas por el mismo número de ciclos por cada longitud de ciclo, haremos una correspondencia entre los ciclos de la misma longitud que componen a α y a β. Dado un ciclo $(x_1 x_2 \dots x_k)$ en α y un ciclo $(y_1 y_2 \dots y_r)$ en β, definimos $\sigma(x_i) = y_i$, y usamos la misma regla para los demás ciclos. Entonces tenemos que

$$\sigma\alpha\sigma^{-1}(y_1) = \sigma\alpha(x_1) = \sigma(x_2) = y_2 = \beta(y_1),$$

y así sucesivamente, luego $\sigma\alpha\sigma^{-1} = \beta$.. □

EJEMPLO 8.4. Consideremos en S_5 las siguientes permutaciones del tipo $[2\,3]$:

$$\tau = (12)(345), \qquad \pi = (13)(254).$$

Encontrar $\sigma \in S_5$ tal que $\sigma\tau\sigma^{-1} = \pi$.

PRUEBA. Usando el argumento de la prueba del Teorema 8.3, tomamos primeramente los ciclos (12) y (13). Definimos $\sigma(1) = 1$ y $\sigma(2) = 3$. Tomando ahora los ciclos de longitud 3, definimos $\sigma(3) = 2$, $\sigma(4) = 5$ y $\sigma(5) = 4$. Entonces

$$\sigma = (1)(23)(45),$$

y

$$\sigma\tau\sigma^{-1} = (1)(23)(45)\ (12)(345)\ (45)(23)(1) = (13)(254) = \pi$$

como queríamos ver. □

9. Permutaciones pares e impares

El principal resultado que veremos en esta sección es que el grupo de permutaciones S_n posee un subgrupo A_n de orden $\dfrac{n!}{2}$.

Primero veamos que toda permutación se puede escribir como producto de trasposiciones, obviamente no serán disjuntas entre sí. Es decir, toda permutación se puede lograr intercambiando sucesivamente 2 elementos de $[[1, n]]$. Por ejemplo, la permutación que transforma 123456 en 342165 es $(56)(14)(21)(13)$. En general, el ciclo $(x_1x_2 \ldots x_r)$ se expresa como producto de trasposiciones de la siguiente manera:

$$(x_1x_2 \ldots x_r) = (x_1x_r) \ldots (x_1x_3)(x_1x_2).$$

Es fácil probar este resultado por inducción, si se tiene en cuenta que el ciclo de longitud $k+1$, $(x_1x_2 \ldots x_{k+1})$ puede escribirse como $(x_1, x_{k+1})(x_1x_2 \ldots x_k)$.

Luego como cada ciclo puede ser escrito como producto de trasposiciones y cada permutación puede ser escrita como producto de ciclos, concluimos que toda permutación puede ser escrita como producto de trasposiciones.

EJEMPLO 9.1. Escribir la permutación $(1342)(5876)$ como producto de trasposiciones.

PRUEBA. Usando el argumento anterior, escribimos

$$(1342)(5876) = (12)(14)(13)(56)(57)(58).$$

□

Sin embargo, no hay una única manera de escribir una permutación como producto de trasposiciones, por ejemplo en S_5, la permutación (245) puede ser escrita como $(25)(24)$ o como $(13)(25)(31)(24)$. Lo que sí veremos es que todas las representaciones como producto de trasposiciones de una misma permutación tienen una característica en común.

Si π es una permutación del tipo $[1^{\alpha_1}2^{\alpha_2}\dots n^{\alpha_n}]$ llamaremos $c(\pi)$ al número de ciclos que componen a π, luego

$$c(\pi) = \alpha_1 + \alpha_2 + \cdots + \alpha_n.$$

¿Qué ocurre si componemos a π con una trasposición τ? ¿Cuántos ciclos componen a $\tau\pi$?

Supongamos que τ permuta a con b, es decir $\tau(a) = b$, $\tau(b) = a$ y $\tau(k) = k$ para $k \neq a,\ b$. Pueden ocurrir dos casos:

(i) a y b ocurren en un mismo ciclo de π, esto es, existe un ciclo en la descomposición de π de la forma $(ax\dots yb\dots z)$. Entonces al hacer $\tau\pi$ este ciclo se desdobla en

$$(ax\dots y)(b\dots z).$$

En este caso, $c(\tau\pi) = c(\pi) + 1$.

(ii) Si a y b están en diferentes ciclos de π, entonces en la descomposición de π aparecen ciclos de la forma $(ax \dots y)(b \dots z)$. Luego al componer con τ obtendremos el ciclo

$$(b \dots zax \dots y),$$

y en este caso $c(\tau\pi) = c(\pi) - 1$.

Luego en ambos casos el efecto de una trasposición luego de una permutación altera el número de ciclos en uno. Este hecho nos ayuda a probar el siguiente teorema:

TEOREMA 9.2. *Supongamos que una permutación π en S_n puede ser escrita como la composición de k trasposiciones y también de k' trasposiciones. Entonces k y k' son ambos pares o ambos impares.*

PRUEBA. Sea $\pi = \tau_{k-1}\tau_{k-2} \dots \tau_2\tau_1$, donde τ_i, $1 \leq i \leq k$ son trasposiciones. Como τ_1 es una permutación del tipo $[1^{n-2}2]$, el número de ciclos de τ_1 es $c(\tau_1) = (n-2) + 1 = n - 1$. Al hacer las sucesivas composiciones con τ_2, τ_3, ..., el número de ciclos se va aumentando o disminuyendo en 1. Supongamos que aumenta g veces en 1 y disminuye h veces en 1. Luego

$$c(\pi) = (n-1) + g - h.$$

Por otro lado, $g + h$ es el número de composiciones sucesivas desde τ_2 hasta τ_k, luego $g + h = k - 1$. Luego

$$k = 1 + g + h = 1 + g + (n - 1 + g - c(\pi)) = n - c(\pi) + 2g.$$

Por el mismo argumento, dado que π se puede escribir como producto de k' trasposiciones, existirá un entero g' tal que

$$k' = n - c(\pi) + 2g'.$$

Pero entonces

$$k - k' = 2(g - g'),$$

es decir que k y k' tienen la misma paridad.

□

Como consecuencia de este teorema podemos definir qué es una permutación par y una permutación impar.

DEFINICIÓN 9.3. Una permutación se dice *par* (respectivamente *impar*) si puede escribirse como producto de un número par (respectivamente impar) de permutaciones.

PROPOSICIÓN 9.4. *Para $n \geq 2$, el conjunto A_n de todas las permutaciones pares es un subgrupo de S_n.*

PRUEBA. Es suficiente con probar que $A_n \neq \emptyset$ y que $\tau\sigma \in A_n$, para todo τ, $\sigma \in A_n$. $A_n \neq \emptyset$, pues $(12)(12) \in A_n$. Además, si $\tau = \tau_1\tau_2 \ldots \tau_r$ y $\sigma = \sigma_1\sigma_2 \ldots \sigma_k$, donde cada τ_i y cada σ_j son trasposiciones y donde r y k son pares, entonces su composición $\tau\sigma$ se escribe como

$$\tau_1\tau_2 \ldots \tau_r\sigma_1\sigma_2 \ldots \sigma_k,$$

que es un producto de $(k + r)$ trasposiciones, y $(k + r)$ también es par.

□

PROPOSICIÓN 9.5. *A_n es un subgrupo de orden $\dfrac{n!}{2}$.*

PRUEBA. Veamos que S_n se puede *partir* en dos subconjuntos A_n y B_n de igual cardinalidad. En efecto, sabemos que toda permutación $\pi \in S_n$ es par o es impar. Llamemos A_n al conjunto de permutaciones pares, y B_n al conjunto de permutaciones impares, y veamos que existe una biyección entre ellos. Sea τ una trasposición cualquiera, por ejemplo, $\tau = (12)$. Entonces la función $\Phi : A_n \mapsto B_n$ dada por

$$\Phi(\pi) = \tau\pi$$

es una biyección. Claramente, Φ aplica permutaciones pares en impares, ya que incrementa el número de trasposiciones en 1. Veamos que Φ es inyectiva: si $\tau\pi = \tau\sigma$, por la ley de cancelación a izquierda resulta $\pi = \sigma$. Además Φ es suryectiva, pues si π es una permutación impar, entonces $\tau\pi$ es par, luego

$$\pi = \tau(\tau\pi) = \Phi(\tau\pi).$$

Luego $|A_n| = |B_n|$ y $S_n = A_n \cup B_n$. Dado que esta unión es disjunta, concluimos que $|S_n| = 2|A_n|$, como queríamos ver.

□

EJEMPLO 9.6. En S_2, $A_2 = \{(1)\}$. En S_3,

$$A_3 = \{(1), (12)(13), (13)(12)\} = \{id, (132), (123)\}.$$

EJEMPLO 9.7. Ocho bloques rotulados con las letras A, E, I, O, U, Q, L e Y, están ubicados en un cuadrado como se muestra en el primer diagrama de la figura siguiente. Si los movimientos que se pueden hacer consisten en desplazar un bloque hacia el espacio vacío, pruebe que es imposible lograr el segundo diagrama de la figura con una sucesión de movimientos legales.

A	E	I
O	U	Q
L	Y	

A	Y	Q
U	E	L
I	O	

PRUEBA. Llamemos □ a nuestro espacio vacío. La disposición inicial de las letras es AEIOUQLY□, y la final es AYQUELIO□. Desplazar una letra X al espacio vacío corresponde a una trasposición (X□). Ahora bien, para llegar a la disposición final, se deberán hacer tantos corrimientos de □ hacia arriba como hacia abajo, y tantos a la izquierda como a la derecha. Por

lo tanto el número total de trasposiciones es par, es decir que la permutación que produce dicha reordenación de las letras debe ser *par*.

Por otro lado, esta permutación se puede escribir como producto de ciclos de la manera

$$(\text{A})(\text{EUOY})(\text{ILQ})(\square),$$

pero esto corresponde a un producto de un número impar de trasposiciones, es decir que es una permutación impar. Se sigue que es imposible lograr la disposición final con una sucesión de movimientos legales. □

10. Coclases y el Teorema de Lagrange

En esta sección volvemos a la teoría general de grupos, para probar un importante resultado acerca de los grupos finitos. El Teorema de Lagrange asegura que si G es un grupo finito y H es un subgrupo de G entonces $|H|$ divide al $|G|$. Así por ejemplo, un grupo de orden 18 sólo puede tener subgrupos de orden 1, 2, 3, 6, 9 y 18. La idea de la demostración de este teorema es *particionar* al grupo G en subconjuntos disjuntos de cardinal igual a $|H|$, luego si existen k subconjuntos de estos tendremos que $|G| = k|H|$.

DEFINICIÓN 10.1. Sea H un subgrupo de un grupo G (no es necesario suponer que G es finito). La *coclase a izquierda* gH de G con respecto a un elemento g en G se define como el conjunto obtenido por la multiplicación de cada elemento de H a izquierda por g, esto es

$$gH = \{x \in G \mid x = gh \text{ para algún } h \in H\}.$$

La *coclase a derecha* de H con respecto a g se define análogamente:

$$Hg = \{x \in G \mid x = hg \text{ para algún } h \in H\}.$$

EJEMPLO 10.2. $H = \{0, 3, 6, 9\}$ es un subgrupo del grupo $\mathbb{Z}_{12}$. La coclase a izquierda $2H$ es entonces:

$$2H = \{x \in \mathbb{Z}_{12} \mid x = 2 \oplus h \text{ para algún } h \in H, \}$$

esto es

$$2H = \{2, 5, 8, 11\}.$$

Notemos que $2H$ no es un subgrupo de G, y también notemos que $2H = 5H$.

Si H es un subgrupo finito, digamos $H = \{h_1, h_2, \ldots, h_m\}$, entonces los elementos de la coclase a izquierda gH son $gh_1, gh_2, \ldots, gh_m$. Dado que se tiene una biyección entre H y gH dada por

$$h \mapsto gh, \qquad \forall h \in H,$$

se tiene que $|H| = |gH|$, para cualquier $g \in G$.

EJEMPLO 10.3. Consideremos el grupo $S_3 = \{(1), (12), (13), (23), (123), (132)\}$, y su subgrupo $H = \{(1), (12)\}$. Hemos denotado con (1) a la permutación identidad. Las coclases a izquierda de H son las siguientes:

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

Notemos que hay exactamente 3 subconjuntos de S_3 que son coclases de H, y estos 3 subconjuntos son disjuntos. Así es que tenemos la partición

$$S_3 = \{(1), (12)\} \cup \{(13), (123)\} \cup \{(23), (132)\}.$$

Este es un hecho general que se deduce del siguiente resultado.

TEOREMA 10.4. *Sea H un subgrupo de un grupo G. Si g_1 y g_2 son elementos cualesquiera de G entonces las coclases g_1H y g_2H son idénticas o son disjuntas.*

PRUEBA. Probaremos que si g_1H y g_2H tienen un elemento en común, entonces $g_1H = g_2H$. En efecto, sea $x \in g_1H \cap g_2H$. Entonces existen h_1, $h_2 \in H$ tales que

$$x = g_1h_1, \qquad \text{y} \qquad x = g_2h_2.$$

Veamos que $g_1H \subseteq g_2H$. Si $y = g_1h$, para algún $h \in H$, entonces

$$y = g_1h = (xh_1^{-1})h = x(h_1^{-1}h) = (g_2h_2)(h_1^{-1}h) = g_2(h_2h_1^{-1}h).$$

Dado que H es un subgrupo, $(h_2h_1^{-1}h)$ es un elemento de H, y por lo tanto $y \in g_2H$.. Luego $g_1H \subseteq g_2H$.

Por un argumento similar podemos probar que $g_2H \subseteq g_1H$, y por lo tanto g_1H y g_2H son coclases idénticas. □

Notemos que si H es un subgrupo de G, la relación $\sim$ dada por

$$x \sim y \quad \text{si y sólo si} \quad x^{-1}y \in H$$

es una relación de equivalencia en G. Las clases de equivalencia son precisamente las coclases a izquierda de H. Esto demuestra nuevamente que las coclases son disjuntas o son idénticas, y que el conjunto de las coclases forma una partición del grupo G.

TEOREMA DE LAGRANGE . Si G es un grupo finito de orden n y H es un subgrupo de orden m, entonces m es un divisor de n.

PRUEBA. Hemos visto que cada coclase a izquierda tienen la misma cardinalidad que H, y que el conjunto de todas las coclases *distintas* forman una partición de G en subconjuntos disjuntos. Luego si hay k coclases a izquierda distintas debe ser que $n = km$. □

DEFINICIÓN 10.5. Sea G un grupo finito, y H un subgrupo de G. El número de coclases a izquierda de H se llama el *índice* de H en G y se denota $|G : H|$; luego

$$|G| = |G : H||H|.$$

EJEMPLO 10.6. A_n es un grupo de índice 2 en S_n.

También el índice se puede definir como el número de coclases a derecha, y obtendríamos los mismos resultados. Sin embargo, a pesar de que el número de coclases a izquierda y a derecha es el mismo, no necesariamente producen la misma partición de G.

EJEMPLO 10.7. Las coclases a derecha del grupo H en el Ejemplo 10.3 son

$$\begin{aligned} H(1) &= \{(1), (12)\}, \\ H(13) &= \{(1)(13), (12)(13)\} = \{(13), (132)\}, \\ H(23) &= \{(1)(23), (12)(23)\} = \{(23), (123)\}, \end{aligned}$$

que son distintas a las coclases a izquierda. Las mismas producen la siguiente partición de S_3:

$$S_3 = \{(1), (12)\} \cup \{(13), (132)\} \cup \{(23), (123)\}.$$

COROLARIO 10.8. *Si G es un grupo de orden p, y p es primo, entonces los únicos subgrupos de G son $\{1\}$ y G.*

COROLARIO 10.9. *Si g es un elemento de un grupo finito G y $|G| = n$, entonces*

(i) *el orden de g divide a n,*

(ii) $g^n = 1$.

PRUEBA. Dado que $\langle g \rangle$ es un subgrupo de G entonces $d = |\langle g \rangle|$ divide a n. Pero $|\langle g \rangle|$ es igual al orden de g, de donde queda probado (i). Por otro lado, como $dk = n$, para algún $k \in \mathbb{N}$, entonces

$$g^n = g^{dk} = (g^d)^k = 1^k = 1.$$

□

EJERCICIO 10.1. Probar que todo grupo de orden p, p primo, es cíclico.

11. Automorfismos de un grafo

Un subgrupo importante del grupo de permutaciones S_n es el subgrupo A_n de las permutaciones pares, llamado el grupo alternante. Otros subgrupos importantes de S_n surgen como grupos de simetrías de un polígono regular, por ejemplo, $G_\Delta = S_3$.

En efecto, toda simetría de un polígono regular de n lados queda determinada por la acción sobre los vértices. Enumerando los vértices del polígono, cada simetría se identifica con una permutación en S_n . Dado que la composición de simetrías es una simetría, se sigue que el conjunto de simetrías de un polígono regular es isomorfo a un subgrupo de S_n.

EJEMPLO 11.1. Calcular el grupo $G_\square$ de simetrías de un cuadrado y encontrar un subgrupo de S_4 isomorfo a $G_\square$.

PRUEBA. Numeramos los vértices de 1 a 4. Las simetrías son:

- (1): identidad.
- $(12)(34)$, $(14)(23)$: simetrías axiales con respecto a ejes perpendiculares a los lados.
- (13), (24), simetrías axiales con respecto a la diagonal.
- (1234), (1432): rotaciones en un ángulo de 90 grados, en sentido horario y antihorario.

□

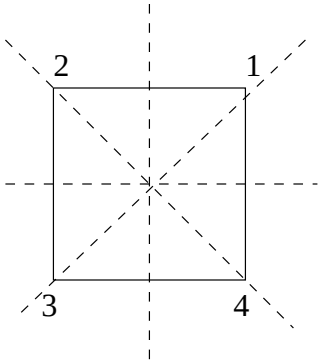


FIGURA 1. Simetrías de un cuadrado

Consideremos ahora un grafo $G = (V, E)$, donde V es el conjunto de vértices y E el conjunto de aristas. Un *automorfismo* de un grafo es una biyección $\sigma : V \mapsto V$ tal que para todo $\{v, w\} \in E$ se verifica que $\{\sigma(v), \sigma(w)\} \in E$. Es claro que la composición de automorfismos es un automorfismo, y la inversa de un automorfismo también lo es.

Por lo tanto, si $|V| = n$, se puede identificar el conjunto de automorfismos de G con un subgrupo del grupo de permutaciones S_n.

EJEMPLO 11.2. La permutación $(15)(24)$ es un automorfismo del grafo de la Figura 2, mientras que (12345) no es un automorfismo dado que la arista $\{2, 4\}$ se transforma en $\{3, 5\}$, que no es una arista.

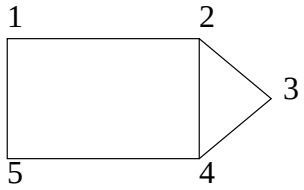


FIGURA 2

Notemos que si α es un automorfismo del grafo (V, E), y $v \in V$, entonces α induce un isomorfismo entre los vértices adyacentes a v y los vértices adyacentes a $\alpha(v)$. Por lo tanto el

grado de v es el mismo que el grado de $\alpha(v)$ (Ver Figura 3). Análogamente, puede verse que α mapea ciclos de longitud k en ciclos de longitud k.

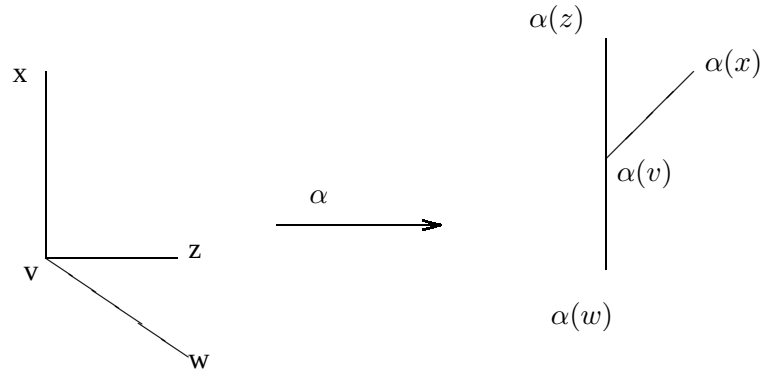


FIGURA 3

Finalizamos esta sección estas notas con el siguiente ejemplo:

EJEMPLO 11.3. Encontrar el grupo de automorfismos del grafo siguiente:

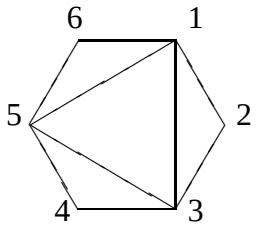


FIGURA 4

SOLUCIÓN: Tenemos que

$$V = \{1, 2, 3, 4, 5, 6\} \qquad \text{y}$$

$$E = \{\{1, 2\}, \{1, 3\}, \{1, 5\}, \{1, 6\}, \{2, 3\}, \{3, 4\}, \{3, 5\}, \{4, 5\}, \{5, 6\}\}.$$

Los vértices 1, 3 y 5 tienen grado 4 y los vértices 2, 4 y 6 tienen grado 2. Ningún automorfismo puede aplicar un vértice de grado 4 en un vértice de grado 2, y viceversa.

Probaremos que cada permutación del conjunto $\{1, 3, 5\}$ está en correspondencia con un automorfismo del grafo, y viceversa.

En efecto, cada automorfismo σ produce una permutación en el conjunto de vértices $\{1, 3, 5\}$. Además, la acción de σ sobre los vértices 1, 3 y 5 determina unívocamente la acción sobre los vértices 2, 4 y 6. Por ejemplo, si un automorfismo permuta los vértices 1 y 3, entonces el vértice 2 permanece fijo, el vértice 6 debe aplicarse en 4 y el vértice 4 debe aplicarse en 6.

Recíprocamente, cada permutación del conjunto $\{1, 3, 5\}$ determina un único automorfismo del grafo, que consiste en la misma permutación del los vértices rotulados con 1, 3 y 5, con la consecuente permutación de los vértices 2, 4 y 6.

Enumeramos a continuación todas las permutaciones del grafo, y su correspondencia con las permutaciones de $\{1, 3, 5\}$:

(1) id, determinada por la permutación $(1)(3)(5)$ de $\{1, 3, 5\}$,

(2) $(13)(46)$, determinada por $(13)(5)$,

(3) $(15)(24)$, determinada por $(15)(3)$,

(4) $(35)(26)$, determinada por $(35)(1)$,

(5) $(135)(246)$, determinada por (135) y

(6) $(153)(264)$, determinada por (153).

Concluimos entonces que el grupo de automorfismos del grafo G tiene orden 6, tiene 3 elementos de orden 2 y 2 elementos de orden 3.

Recordemos que $|S_6| = 6!$, y podemos comprobar que el orden del grupo de automorfismos de G divide al orden de $|S_6|$. □

COROLARIO 11.4. *Probar que el grupo de automorfismos del grafo del Ejemplo 11.3 es isomorfo al grupo S_3.*

12. Guía de ejercicios

En esta última sección presento una lista de ejercicios que complementan la teoría y ejemplos desarrollados en las secciones anteriores. Algunos ejercicios están señalados con un asterisco (*) indicando que los mismos son de una dificultad mayor que los demás.

1. Pruebe que las operaciones en los siguientes conjuntos definen una estructura de grupo:
   a) $\mathbb{Q} - \{0\}$ con la operación del producto.
   b) $\mathbb{Z}$ con la operación de la suma.
   c) $\mathbb{Z}_p - \{0\}$ con la operación $\odot$, con p un número primo.
2. Dar la tabla de $\mathbb{Z}_4$ y $\mathbb{Z}_5$ para las operaciones de $\oplus$ y $\odot$.
3. Encontrar los inversos de 2 en $\mathbb{Z}_{11}$, 7 en $\mathbb{Z}_{15}$, 7 en $\mathbb{Z}_{16}$ y de 5 en $\mathbb{Z}_{13}$.
4. Calcular el orden de 8 en $\mathbb{Z}_{12}$, de 15 en $\mathbb{Z}_{20}$ y de 14 en $\mathbb{Z}_{210}$.
5. Probar que G_Δ es isomorfo al grupo de permutaciones S_3.
6. a) Describir las cuatro simetrías de un rectángulo y construir la tabla de multiplicar.
   b) Sea G el grupo con la tabla de multiplicar:

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

   Hallar un isomorfismo entre G y el grupo de simetrías del rectángulo. ¿Es G conmutativo?, ¿es isomorfo a $\mathbb{Z}_4$?
7. (*) Analizando las posibles tablas de multiplicar, mostrar que (salvo por isomorfismos), existe un solo grupo de orden 2 y un solo grupo de orden 3.
8. Decir cuáles de los siguientes son subgrupos de G_Δ.

$$K_1 = \{id, x\}, \qquad K_2 = \{id, x, y\}, \qquad K_3 = \{id, r, s, x, y\}.$$

9. ¿Es S_n un grupo cíclico?

10. $\mathbb{Z}_n$ es un grupo cíclico generado por $\langle 1 \rangle$. Pruebe que x genera $\mathbb{Z}_n$ si y sólo si x y n son coprimos.

11. Encontrar todos los subgrupos cíclicos en $\mathbb{Z}_{13}$ y $\mathbb{Z}_{45}$. Encontrar todos los subgrupos de S_4.

12. Escribir la siguiente permutación usando la notación cíclica:

$$\begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 5 & 7 & 8 & 4 & 6 & 1 & 2 & 9. \end{array}$$

13. Sean $\sigma = (123)(456)(78)$ y $\tau = (1357)(26)(4)(8)$ permutaciones (en notación cíclica) de $\{1, 2, 3, 4, 5, 6, 7, 8\}$. Escriba en notación cíclica $\sigma\tau$, $\tau\sigma$, σ^2, σ^{-1} y τ^{-1}.

14. Muestre que existen sólo tres elementos en S_4 que tienen 2 ciclos de longitud 2 disjuntos.

15. ¿Cuáles son todas las permutaciones de S_4 de orden 2?

16. Escribir los siguientes elementos de S_8 como producto de trasposiciones, y encuentre el signo de cada uno:

$$\alpha = (1357)(2468), \qquad \beta = (127)(356)(48), \qquad \gamma = (135)(678)(2)(4).$$

17. Probar que $sgn(\pi\sigma\pi^{-1}) = sgn(\sigma)$, para todo $\pi, \sigma \in S_n$.

18. Sean $\alpha = (15)(27436)$ y $\beta = (1372)(46)(5)$ permutaciones en S_7. Calcular los órdenes de α, β, $\alpha\beta$ y $\beta\alpha$.

19. (*) Describir explícitamente la partición de G_Δ como coclases a derecha del subgrupo $H = \{i,\ x\}$. Verficar que la partición no es la misma que se obtiene de las coclases a izquierda.

20. (*) Supongamos que G es un grupo finito,que p es un número primo y que G tiene exactamente m subgrupos de orden p. Mostrar que el número de elementos de orden p en G es $m(p-1)$.

21. (*) Muestre que un grupo no cíclico de orden 55 tiene por lo menos un subgrupo de orden 5 y un subgrupo de orden 11.

22. ¿Cuáles de los siguientes son subgrupos de S_5?
    a) $\{(12345), (124)(35)\}$.
    b) $\{id, (12345), (13524), (14253), (15432)\}$.
    c) $\{id, (12)(34), (13)(24), (14)(23)\}$.
    d) $\{id, (12)(345), (135)(24), (15324), (12)(45), (134)(25), (143)(25)\}$.

23. (*) Un conjunto de 52 tarjetas se divide en dos partes iguales y se intercala, de tal manera que si el orden original es 1, 2, 3, 4, ..., el nuevo orden es 1, 27, 2, 28, ... ¿Cuántas veces debe repetirse el procedimiento para que las tarjetas vuelvan a su ubicación original?

24. (*) El orden de cualquier elemento en S_8 es un divisor de $|S_8| = 8!$. Sabiendo que toda permutación puede ser escrita como producto de ciclos, ¿cuáles son los órdenes realmente posibles? Dé ejemplos de divisores de $8!$ tal que no haya ningún elemento de S_8 con ese orden.

25. (*)
    a) Hallar las simetrías del cuadrado, consideradas como permutaciones de vértices 1, 2, 3 y 4, rotulados en orden cíclico.
    b) Liste todas las simetrías de un pentágono regular, consideradas como permutaciones de los vértices 1, 2, 3, 4, 5, rotuladas en orden cíclico.

26. Encuentre el grupo de automorfismos del grafo dado por la lista de adyacencia siguiente:

1	2	3	4	5	6	7	8
2	1	1	1	2	3	4	4
3	3	2	7	7	7	5	5
4	5	6	8	8	8	6	6

27. Encuentre el grupo de automorfismos de cada uno de los grafos de la Figura 5:

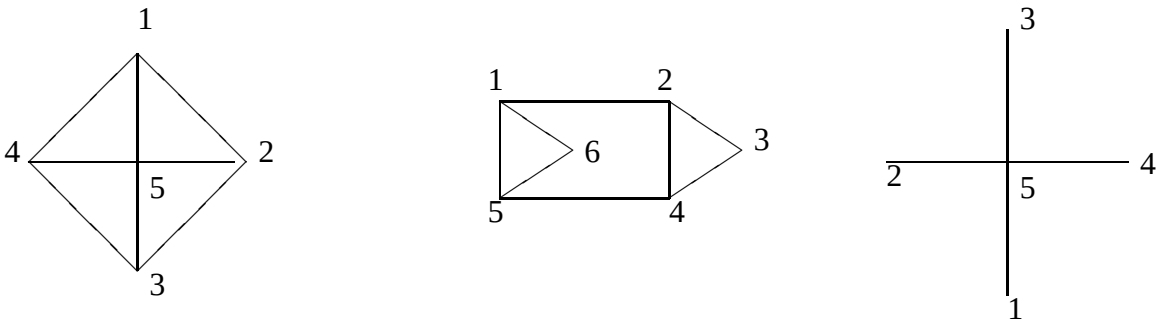


FIGURA 5

Bibliografía

[1] *Matemáticas Discretas*. Norman L. Biggs Editorial Vicens Vives, 1994

[2] *Notas de Álgebra I/Matemática Discreta I*. N. P. Kisbye y R. J.Miatello. Publicaciones de FAMAF. Serie C. 2005.

[3] *Notas de Álgebra*. Enzo Gentile. Editorial Eudeba. 1973.