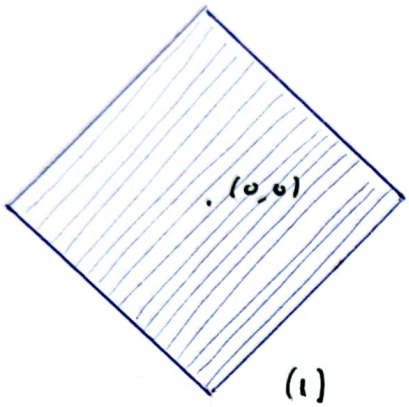
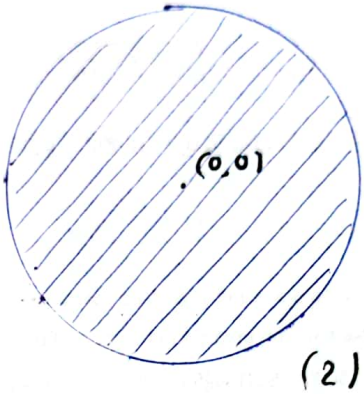
GRUPOS

¿Qué es una simetría?

Considene las siguientes figunas:



(1)

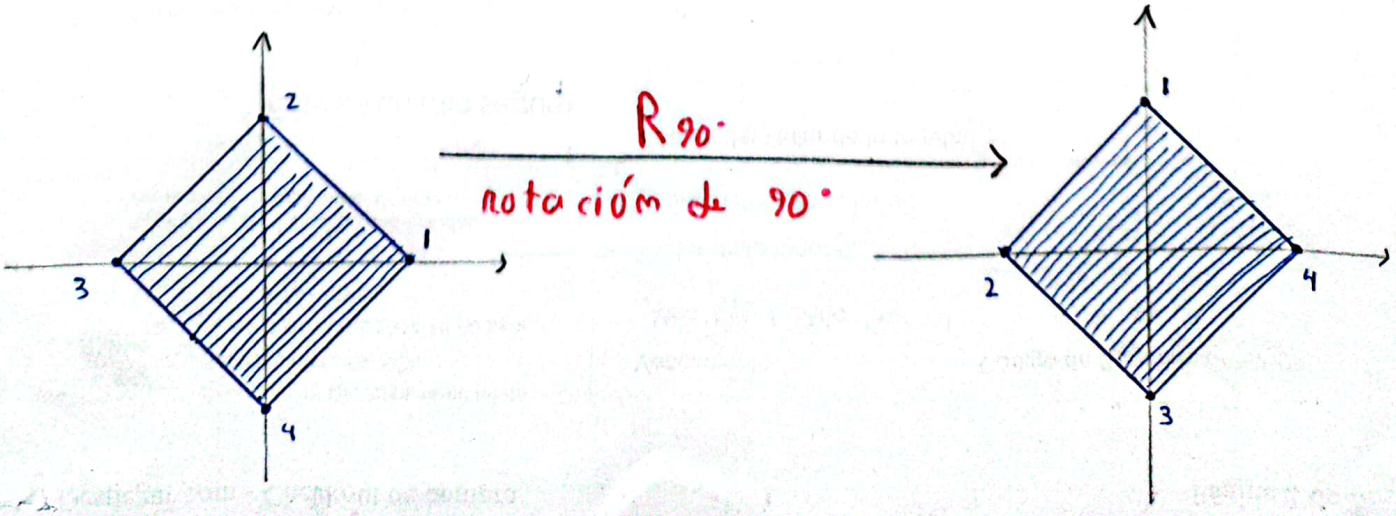


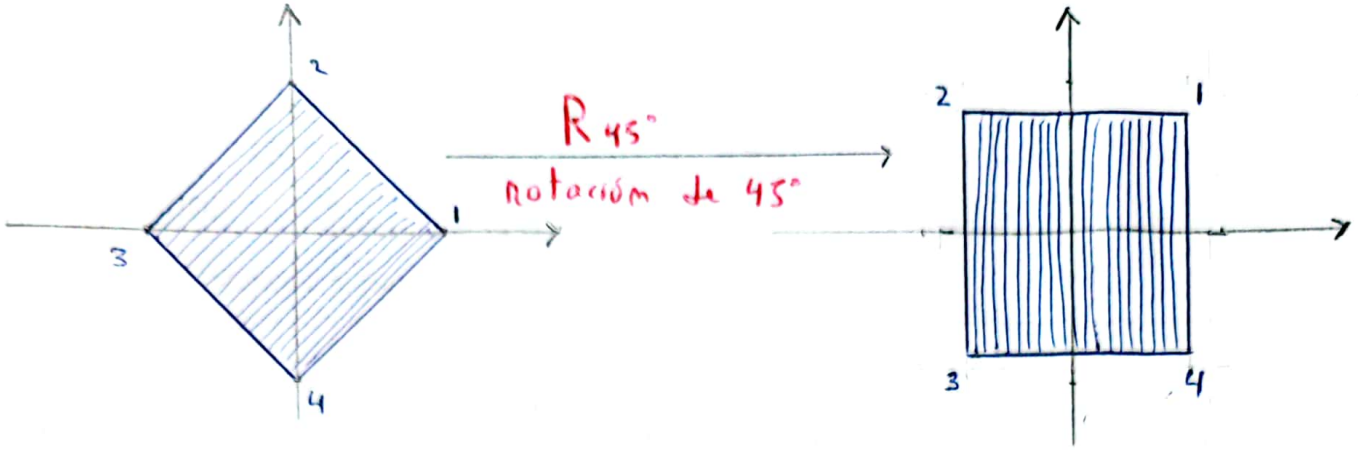
(2)

¿La figuna (1) es simétnica? ¿La (2)?
¿Entne (1) y (2), cuál es más simétnica?

Intuitivamente, podemos pemsan em una simetnía de una figuka como em una tnamsfonmación tal que, una vez aplicada a la figuna, mantieme su posición y fonma inicial.

Pon ejemplo, una notación de 90° alnededon del onigem mantieme la posición y fonma de la figuna (1), mientnas que una notación de 45° no.





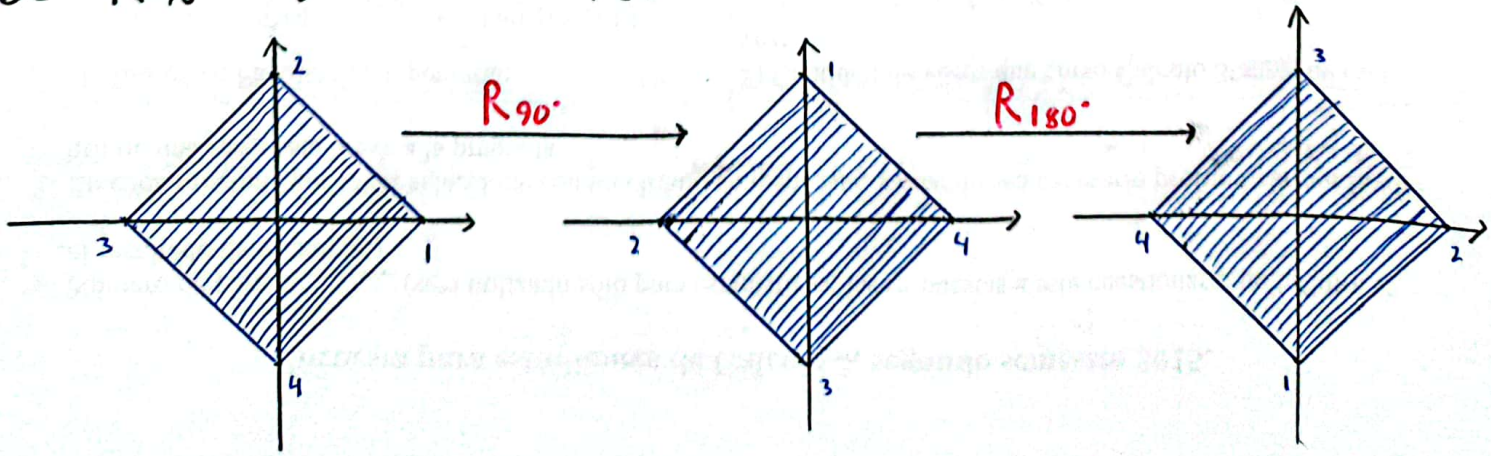
De manera similar, las notaciones de 180°, 270° y 360° son simetrías del cuadrado (1). Existen otras más, por ejemplo, reflejan o voltean (1) respecto a las rectas $x = 0$, $y = 0$, $y = x$ e $y = -x$.

Denotemos por $Sim^{\square}$ al conjunto de todas las simetrías de (1).

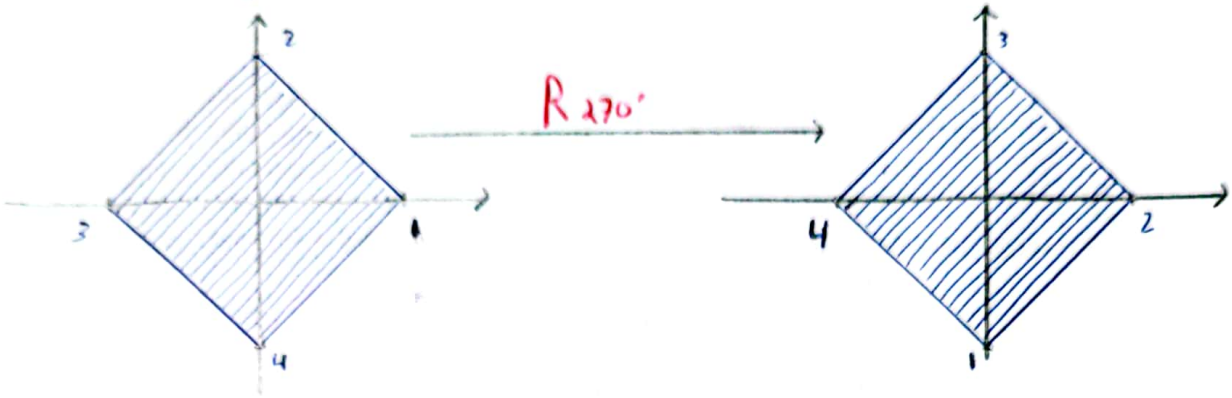
$$Sim^{\square} = \{R_{90°}, R_{180°}, R_{270°}, R_{360°}, L_{x=0}, L_{y=0}, L_{x=y}, L_{y=-x}\}$$

donde $L_{x=0}$, $L_{y=0}$, $L_{y=x}$ y $L_{y=-x}$ son las reflexiones mencionadas anteriormente.

Resulta que además podemos dotar al conjunto $Sim^{\square}$ de propiedades algebraicas. Efectivamente, podemos componer simetrías. Hagamos por ejemplo la composición de $R_{90°}$ seguida de $R_{180°}$.



Vemos que el resultado es equivalente a aplicar una notación de 270°.



Es decir,

$$R_{180^\circ} \circ R_{90^\circ} = R_{270^\circ}.$$

¿Qué pasa si la composición suma más de 360°?

Por ejemplo,

$$R_{270^\circ} \circ R_{180} = R_{450^\circ}$$

Pero 450° y 90° equivalen al mismo ángulo, ya que

$$450^\circ \equiv 90^\circ \pmod{360}.$$

Entonces, $R_{270^\circ} \circ R_{180^\circ} = R_{90^\circ} \in \square Sim.$

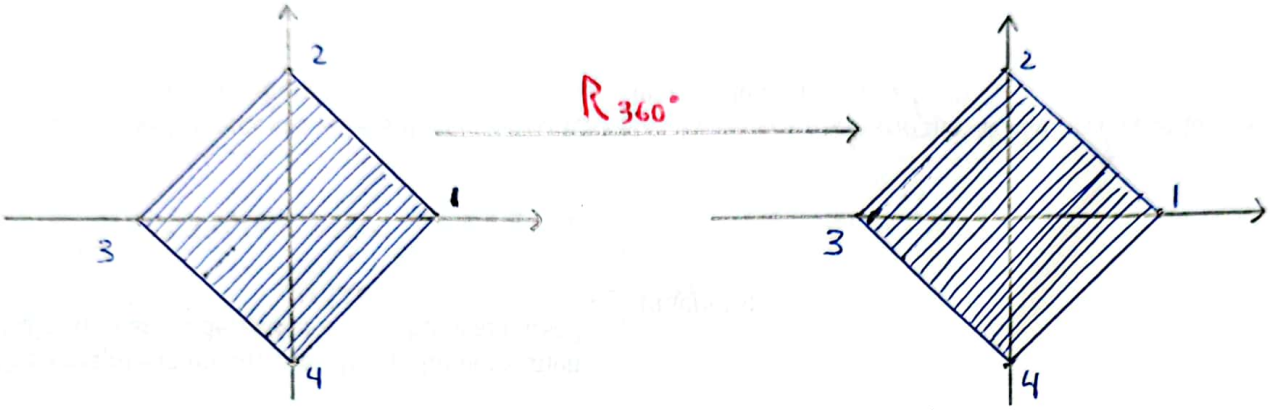
Se puede también probar con cualquier otro par de elementos en $\square Sim$ y ver que su composición cae en $\square Sim$. Es decir, la composición $\circ$ es cerrada en $\square Sim$.

$$\circ : \square Sim \times \square Sim \longrightarrow \square Sim.$$

Otra cosa que podemos notar a partir de lo anterior es que $R_{360°}$ equivale a no rotar la figura. (1).

$$R_{360°} = R_{0°} \quad \text{ya que} \quad 360 \equiv 0 \pmod{360}.$$

Entonces, $R_{0°}$ es el elemento identidad de $Sim^{\square}$.

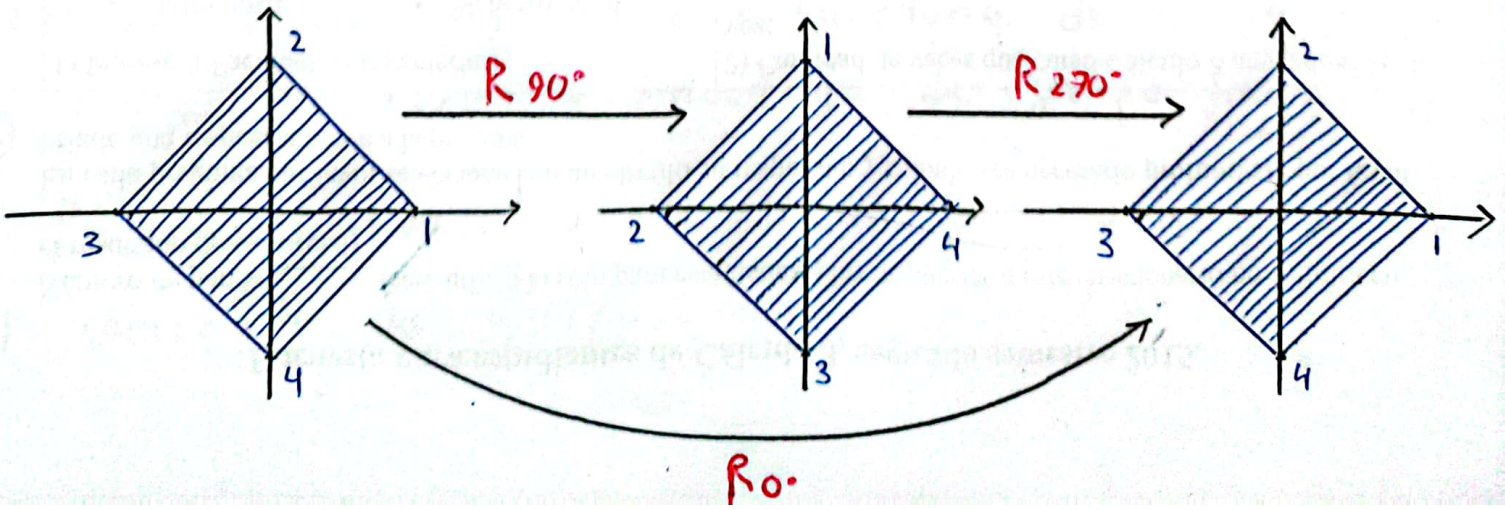


Por otro lado, la composición de simetrías es asociativa (por ser una composición de funciones).

Finalmente, toda rotación se puede deshacer. Por ejemplo,

$$R_{270°} \cdot R_{90°} = R_{360°} = R_{0°}$$

La rotación de 90° puede deshacerse aplicando la rotación de 270°. Es decir, $R_{270°}$ funge como el inverso de $R_{90°}$.



Equivalentemente, $R_{270°} = R_{-90°}$ (rotación de 90° em sentido horario).

Em resumem, podemos notar los siguientes aspectos de $Sim^{\square}$ y $\circ$.

1) $\circ$ es una operación cerrada em $Sim^{\square}$.
2) $\circ$ es asociativa.
3) $R_{0°}$ es el elemento neutro de $Sim^{\square}$ respecto a $\circ$.
4) Toda simetría (rotación o reflexión) em $Sim^{\square}$ posee una simetría inversa.

El par $(Sim^{\square}, \circ)$ constituye entonces lo que em álgebra se conoce como <u>estructura de grupo</u>.

Se puede hacer el mismo análisis anterior com el conjunto de simetrías del círculo (figura (21)), llamémoslo Sim°, junto com la composición de rotaciones o reflexiones. La diferencia com $Sim^{\square}$ es que cualquier rotación (cualquier ángulo) y cualquier reflexión (respecto a cualquier recta que pase por (0,0)) es una simetría del círculo. Em este sentido, $(Sim^{\square}, \circ)$ tiene estructura de grupo finito y $(Sim^{\circ}, \circ)$ tiene estructura de grupo infinito.

Pasemos ahora a analizar de manera formal el concepto de grupo.

Concepto de grupo y ejemplos

Definición: Un **grupo** es un conjunto no vacío G equipado con una operación binaria

$$\cdot : G \times G \longrightarrow G$$

tal que:

1) $\cdot$ es asociativa:

$\forall\, g_1, g_2, g_3 \in G$, se tiene que

$$g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3.$$

2) **Existencia del neutro:**

Existe un elemento $e \in G$ tal que

$$e \cdot g = g \quad y \quad g \cdot e = g,$$

$\forall\, g \in G$.

3) **Existencia de opuestos:**

Para cada $g \in G$, existe $g' \in G$ tal que

$$g \cdot g' = e \quad y \quad g' \cdot g = e.$$

Notación: Si queremos hacer referencia a la operación binaria $\cdot$, denotamos al grupo G como el par $(G, \cdot)$. Si la operación está sobreentendida, denotamos al grupo simplemente por G.

Si dado un grupo $(G, \cdot)$, se cumple que la operación $\cdot$ es conmutativa, es decir si

$$g_1 \cdot g_2 = g_2 \cdot g_1 \quad \forall g_1, g_2 \in G,$$

entonces decimos que $(G, \cdot)$ es un grupo **abeliano**.

Ejemplos:

1) Grupo trivial: $G = \{e\}$ (conjunto con un solo elemento), y

$$- \cdot - : \{e\} \times \{e\} \longrightarrow \{e\}$$

dada por $e \cdot e = e$. $(\{e\}, \cdot)$ es un grupo.

2) $\mathbb{Z}$ con la operación de suma de números enteros es un grupo (abeliano).

0 funge como elemento neutro.

3) $(\mathbb{N}, +)$, donde $+$ es la suma de números naturales, no es un grupo, ya que no se da la existencia de opuestos.

4) $(\mathbb{Z}, \cdot)$, donde $\cdot$ es el producto de enteros, no es un grupo (no se da la existencia de opuestos).

5) $(\mathbb{Q}^*, \cdot)$ y $(\mathbb{R}^*, \cdot)$, donde $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ y $\cdot$ es el producto usual en ambos casos, son claramente grupos.

6) $G = \{-1, 1\}$ y $\cdot$ el producto usual $(G, \cdot)$ es un grupo

$\cdot$	-1	1
-1	1	-1
1	-1	1

7) $M_{m\times m}(\mathbb{R})$, con la suma de matrices, es un grupo.

8) $GL(2, \mathbb{R}) = \{A \in M_{2\times 2}(\mathbb{R}) / \det(A) \neq 0\}$, equipado con la multiplicación usual de matrices, es un grupo. Se le conoce como <u>grupo lineal general</u>.

- En efecto, $GL(2,\mathbb{R})$ no es vacío ya que $I_{2\times 2} \in GL(2,\mathbb{R})$. La multiplicación de matrices es cerrada en $GL(2,\mathbb{R})$, ya que la multiplicación de matrices invertibles es invertible.

$$\cdot : GL(2,\mathbb{R}) \times GL(2,\mathbb{R}) \longrightarrow GL(2,\mathbb{R})$$

- Sabemos que $\cdot$ es asociativa.
- $I_{2\times 2}$ es claramente un elemento neutro en $GL(2,\mathbb{R})$
- Si $A \in GL(2,\mathbb{R})$, entonces $A^{-1} \in GL(2,\mathbb{R})$, ya que A^{-1} también es invertible.

$$(A^{-1})^{-1} = A.$$

Por lo tanto, $(GL(2,\mathbb{R}), \cdot)$ es un grupo (note que no es abeliano).

De manera similar, $(SL(2,\mathbb{R}), \cdot)$, donde

$$SL(2,\mathbb{R}) = \{ A \in M_{2\times 2}(\mathbb{R}) / \det(A) = 1 \},$$

también es un grupo, conocido como <u>grupo lineal especial</u>.

$GL(2,\mathbb{R})$ y $SL(2,\mathbb{R})$ son importantes en el estudio de simetrías en el plano. En efecto, note que:

$$R_\theta = \begin{pmatrix} \cos(\theta) & -\operatorname{sen}(\theta) \\ \operatorname{sen}(\theta) & \cos(\theta) \end{pmatrix} \in SL(2, \mathbb{R})$$

matriz de rotación de ángulo θ alrededor de $(0,0)$

9) Sea B un conjunto y

$$S_B = \{ f : B \to B \,/\, f \text{ es una función biyectiva} \}.$$

$(S_B, \circ)$, donde $\circ$ es la composición de funciones, es un grupo.

- $S_B \neq \emptyset$ ya que la función identidad $1_B : B \to B$ pertenece a S_B.
- La composición de funciones biyectivas $f : B \to B$ y $g : B \to B$ es una función biyectiva $g \circ f : B \to B$.
- La composición es claramente asociativa en S_B
- 1_B es un elemento neutro de S_B.
- Para cada $f : B \to B$ en S_B, existe su opuesto en S_B, a saber, $f^{-1} : B \to B$.

10) Simetrías del copo de nieve:

Toda rotación (alrededor del centro del copo de nieve) de 60°, o múltiplo de 60°, es una simetría del copo. Además, toda reflexión respecto a los 6 ejes correspondientes a los ángulos anteriores también es una simetría del copo.

Entonces, las seis rotaciones de ángulos 0°, 60°, 120°, 180°, 240°, 300°, junto con las reflexiones asociadas a los ejes de cada ángulo, forman un grupo de doce elementos.

11) $SU(3) = \{ A \in M_{3\times 3}(\mathbb{C}) \,/\, A \text{ es unitaria y } \det(A) = 1 \}$

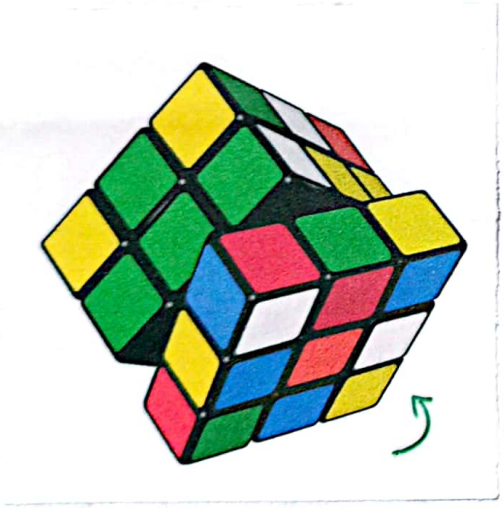
Recuerde que A es <u>unitaria</u> si

$$A \cdot \overline{A}^t = I_{3\times 3} \quad \text{y} \quad \overline{A}^t \cdot A = I_{3\times 3}$$

Con la multiplicación de matrices, $(SU(3), \cdot)$ es un grupo, conocido como grupo unitario especial.

En física de partículas, se utiliza el grupo $SU(3)$ para la clasificación de hadrones.

12) Las permutaciones del cubo de Rubik forman una estructura de grupo (con permutación nos referimos a cualquier rotación "válida" aplicada a cualquiera de las caras del cubo.



Rotación no válida, ya que el estado resultante deja de ser un cubo.

Propiedades de los grupos

Antes de explorar ejemplos más elaborados de grupos, veamos algunas propiedades. Comencemos probando la unicidad del elemento neutro y de los opuestos.

Proposición: Sea $(G, \cdot)$ un grupo. Entonces:

1) El elemento neutro $e \in G$ es único.
2) Para cada $g \in G$, existe un único $g' \in G$ tal que $g \cdot g' = e$ y $g' \cdot g = e$.

Notación: $g' = g^{-1}$.

· **Demostración:**

1) Supongamos que, además de e, existe $e' \in G$ tal que $g \cdot e' = g$ y $e' \cdot g = g$ para todo $g \in G$.

En particular, $e \cdot e' = e$. (haciendo $g = e$)

Por otro lado, $g \cdot e = g$ y $e \cdot g = g$ para todo $g \in G$.

En particular, $e \cdot e' = e'$. (haciendo $g = e'$)

Luego, $e = e \cdot e' = e'$.

2) Sea $g \in G$. Supongamos que existen g' y g'' en G tales que

$$g \cdot g' = e \text{ y } g' \cdot g = e,$$

y

$$g \cdot g'' = e \text{ y } g'' g = e.$$

Así,

$$g \cdot g' = e \Rightarrow g'' \cdot (g \cdot g') = g'' \cdot e \Rightarrow (g'' \cdot g) \cdot g' = g''$$

(prop. aso. + neutro)

$\Rightarrow e \cdot g' = g''$ (ya que $g'' \cdot g = e$)

$\Rightarrow g' = g''$ (pno. del neutno). ■

También podemos pnobar una senie de pnopiedades algebnaicas que se dam em los gnupos. Som vensiomes gemenales de pnopiedades que conocemos pana $(\mathbb{R}^*, \cdot)$ o $(GL(2,\mathbb{R}), \cdot)$, pon ejemplo.

Pnoposición (álgebna de gnupos): Sea $(G, \cdot)$ um gnupo. Las siguientes afinmaciomes se cumplem:

1) $e^{-1} = e$, donde e es el elemento neutno de G.

2) $(g^{-1})^{-1} = g$, $\forall g \in G$.

3) $(g_1 \cdot g_2)^{-1} = g_2^{-1} \cdot g_1^{-1}$, $\forall g_1, g_2 \in G$.

4) Leyes cancelativas a izquienda y a denecha:

$x \cdot g_1 = x \cdot g_2 \Rightarrow g_1 = g_2$

$x, g_1, g_2 \in G$

$g_1 \cdot x = g_2 \cdot x \Rightarrow g_1 = g_2$.

5) Soluciomes de ecuaciomes em G:
Dados $g, h \in G$, existe um único $x \in G$ tal que $g \cdot x = h$.

De manera similar, existe un único $x \in G$ tal que $x \cdot g = h$.

6) Inversos a izquierda o a derecha son inversos:
Si $h \cdot g = e$ o $g \cdot h = e$, entonces $h = g^{-1}$.

7) $(g^n)^{-1} = (g^{-1})^n$, $\forall g \in G$, $\forall n \in \mathbb{N}$,
donde $g^n = g \cdot g \cdots g$ (n veces si $n > 0$), y convenimos que $g^0 = e$.

· Demostración:

1) Como $e \cdot e = e$ y $e \cdot e^{-1} = e$, se tiene por la $e^{-1} \cdot e = e$
unicidad del elemento inverso que $e^{-1} = e$.

2) $g^{-1} \cdot (g^{-1})^{-1} = e$ y $g^{-1} \cdot g = e$
$(g^{-1})^{-1} \cdot g^{-1} = e$ $g \cdot g^{-1} = e$

Por la unicidad del elemento inverso, se tiene que
$(g^{-1})^{-1} = g$.

3) Por un lado, $(g_1 \cdot g_2) \cdot (g_1 \cdot g_2)^{-1} = e$ y
$(g_1 \cdot g_2)^{-1} \cdot (g_1 \cdot g_2) = e$.

Por otro lado,

$$(g_1 \cdot g_2) \cdot (g_2^{-1} \cdot g_1^{-1}) = g_1 \cdot (g_2 \cdot g_2^{-1}) \cdot g_1^{-1} \quad \text{(p. asociativa)}$$
$$= g_1 \cdot e \cdot g_1^{-1} \quad \text{(p. del inverso)}$$
$$= (g_1 \cdot e) \cdot g_1^{-1} \quad \text{(p. asociativa)}$$
$$= g_1 \cdot g_1^{-1} \quad \text{(p. del neutro)}$$
$$= e \quad \text{(p. del inverso)}$$

De manera similar, $(g_2^{-1} \cdot g_1^{-1}) \cdot (g_1 \cdot g_2) = e$.

Por lo tanto, usando la unicidad del inverso, se concluye que

$$(g_1 \cdot g_2)^{-1} = g_2^{-1} \cdot g_1^{-1}.$$

4) Supongamos que $x \cdot g_1 = x \cdot g_2$.

Multiplicamos ambos lados de la igualdad por x^{-1}:

$$x^{-1}(x \cdot g_1) = x^{-1} \cdot (x \cdot g_2)$$
$$(x^{-1} \cdot x) \cdot g_1 = (x^{-1} \cdot x) \cdot g_2 \quad \text{(p. asociativa)}$$
$$e \cdot g_1 = e \cdot g_2 \quad \text{(p. del inverso)}$$
$$g_1 = g_2 \quad \text{(p. del neutro)}.$$

De manera similar, se puede probar que

$$g_1 \cdot x = g_2 \cdot x \Rightarrow g_1 = g_2.$$

5) Sea $x = g^{-1} \cdot h$. Entonces,

$$g \cdot x = g \cdot (g^{-1} \cdot h) = (g \cdot g^{-1}) \cdot h \quad (\text{p. asociativa})$$
$$g \cdot x = e \cdot h \quad (\text{p. del inverso})$$
$$g \cdot x = h \quad (\text{p. del neutro})$$

Tenemos así que $x = g^{-1} \cdot h$ es una solución de la ecuación $g \cdot x = h$. Veamos que es única.

Sup. que $x' \in G$ también es solución, es decir, $g \cdot x' = h$. Luego,

$$g \cdot x' = g \cdot (g^{-1} \cdot h).$$

Por la ley cancelativa a izquierda, concluimos que

$$x' = g^{-1} \cdot h.$$

De manera similar, se puede probar que la ecuación $x \cdot g = h$ tiene solución única en G dada por $x = h \cdot g^{-1}$.

6) Supongamos que $h \cdot g = e$ (el caso donde se supone $gh = e$ es análogo). Como $g^{-1} \cdot g = e$, se tiene que

$$h \cdot g = g^{-1} \cdot g.$$

Por la ley cancelativa a derecha, concluimos que $h = g^{-1}$.

7) Para $n=0$, $(g^0)^{-1} = e^{-1} = e$ g

$(g^{-1})^0 = e$.

Luego, $(g^0)^{-1} = (g^{-1})^0$.

Para $n \in \mathbb{Z}^+$, usaremos inducción.

- $n=1$ (paso inicial): Es inmediato.
- Paso inductivo:

Supongamos que $(g^m)^{-1} = (g^{-1})^m$ (hipótesis inductiva)

Luego, para $m+1$ tenemos:

$$(g^{m+1})^{-1} = (g \cdot g^m)^{-1} = (g^m)^{-1} \cdot g^{-1} = (g^{-1})^m (g^{-1})^1$$

↑ parte 3) ↑ hipótesis inductiva

$$(g^{m+1})^{-1} = (g^{-1})^m \cdot (g^{-1})^1 = (g^{-1})^{m+1}.$$

Por el principio de inducción completa, se tiene que

$$(g^n)^{-1} = (g^{-1})^n, \quad \forall n \in \mathbb{Z}^+.$$

■

Dentro de los ejemplos mencionados, vemos que hay grupos finitos e infinitos. La cantidad de elementos de un grupo será un concepto importante más adelante, por ahora nos limitaremos a definirlo y a presentar notación.

Definición: Dado un grupo $(G, \cdot)$, se define su orden como

$$o(G) := \text{Card}(G).$$

Es decir, $o(G)$ es la cantidad de elementos de G como conjunto.

Si $o(G)$ es finito, diremos que G es un grupo finito. De lo contrario, diremos que G es un grupo infinito y denotaremos $o(G) = \infty$.

Además de los ejemplos anteriores, presentaremos cuatro ejemplos de grupos finitos muy importantes. Pero antes de esto, comentaremos algunos aspectos operatorios de los grupos finitos.

Tablas de Cayley

Dado um grupo finito G, podemos anmar uma tabla que contieme todos los nesultados de $g \cdot h$ pana cualesquiena $g, h \in G$. Tales tablas se comocem como <u>tablas de Cayleg</u>.

Supomgamos $o(G) = n \ (\geq 1)$. Luego,

$$G = \{g_1, g_2, \dots, g_n\} \text{ domde } g_1 = e.$$

Se comstnuge la tabla de Cayleg de $(G, \cdot)$ de la siguiemte mamena:

$\cdot$	g_1	g_2	g_3	$\cdots$	g_{m-1}	g_m
g_1	$g_1 \cdot g_1$	$g_1 \cdot g_2$	$g_1 \cdot g_3$	$\cdots$	$g_1 \cdot g_{m-1}$	$g_1 \cdot g_m$
g_2	$g_2 \cdot g_1$	$g_2 \cdot g_2$	$g_2 \cdot g_3$	$\cdots$	$g_2 \cdot g_{m-1}$	$g_2 \cdot g_m$
g_3	$g_3 \cdot g_1$	$g_3 \cdot g_2$	$g_3 \cdot g_3$	$\cdots$	$g_3 \cdot g_{m-1}$	$g_3 \cdot g_m$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
g_{m-1}	$g_{m-1} \cdot g_1$	$g_{m-1} \cdot g_2$	$g_{m-1} \cdot g_3$	$\cdots$	$g_{m-1} \cdot g_{m-1}$	$g_{m-1} \cdot g_m$
g_m	$g_m \cdot g_1$	$g_m \cdot g_2$	$g_m \cdot g_3$	$\cdots$	$g_m \cdot g_{m-1}$	$g_m \cdot g_m$

Note que por tenerse $g_1 = e$, la fila y columna coloreada de la tabla anterior coinciden con

$$(g_1, g_2, g_3, \ldots, g_{m-1}, g_m).$$

Lo anterior es justamente una permutación de los elementos de G. De hecho, se puede demostrar que cualquier fila o columna de la tabla de Cayley es una permutación de los elementos de G, y que esto último es justamente una condición necesaria para que $(G, \cdot)$ sea un grupo.

Proposición: En la tabla de Cayley de un grupo finito $(G, \cdot)$, con $G = \{g_1, g_2, g_3, \ldots, g_{m-1}, g_m\}$, cada elemento g_i aparece exactamente una vez en cada fila y en cada columna de la tabla.

· Demostración: Sea $g_i \cdot g_1$ el elemento de la columna g_1 y fila i. Supongamos que el mismo elemento aparece otra vez a lo largo de la fila i y en la columna j. Luego, $g_i \cdot g_1 = g_i \cdot g_j$. Por la ley cancelativa a izquierda, se tiene que $g_1 = g_j$, lo cual es una contradicción. Por lo tanto, $g_i \cdot g_1$ solo aparece una vez en la fila i. De manera similar, se puede probar que $g_i \cdot g_1$ aparece solo una vez en la

columma 4.

Observación: 1) Sea G um conjunto finito equipado com uma operación bimania

$$\cdot : G \times G \longrightarrow G.$$

Al pan $(G, \cdot)$ se le comoce como magma. Al tenen uma openación bimania $\cdot$ em G, se puede completaa la tabla de Cayley de um magma. Por la propoisición anteiion, si alguma fila o columma de esta tabla contiene repeticiones de algúm elemento de G, entonces G no es um gnupo.

2) Um gnupo fimito $(G, \cdot)$ es abeliamo si y sólo si su tabla de Cayley es simétnica.

Gnupo aditivo de emtenos módulo n

Sea $n \in \mathbb{Z}^+$ fijo, y $a \in \mathbb{Z}$. Recondemos que la clase de congnuencia de a módulo n se defime como

$$\bar{a} := \{ b \in \mathbb{Z} \,/\, b \equiv a \pmod{n} \}.$$

A cualquien $b \in \bar{a}$ se le comoce como repnesentamte de la clase $\bar{a}$. Nonmalmente se toma como nepnesem-tamte de $\bar{a}$ al nesto de dividin a emtne n.

Recuerde además que $\bar{a}_1 = \bar{a}_2$ si y solamente si $a_1 \equiv a_2 \pmod{n}$.

Entonces, existen exactamente n clases de congruencias módulo n, a saber,

$$\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}.$$

Denotamos por $\mathbb{Z}_n$ al conjunto de todas las clases de congruencia módulo n.

$$\mathbb{Z}_n := \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}.$$

Equipamos a $\mathbb{Z}_n$ con la siguiente operación binaria:

$$+ : \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$$

$$\bar{a} + \bar{b} := \overline{a+b}, \text{ donde } a+b \text{ es la suma en } \mathbb{Z}.$$

<u>Proposición</u>: $(\mathbb{Z}_n, +)$ es un grupo abeliano, conocido como el grupo aditivo de enteros módulo n. Además, $o(\mathbb{Z}_n) = n$.

· <u>Demostración</u>: La asociatividad y conmutatividad de $+$ en $\mathbb{Z}_n$ se sigue de las mismas propiedades en $\mathbb{Z}$.

$\bar{0}$ es el elemento neutro de + en $\mathbb{Z}_m$, ya que

$$\bar{0} + \bar{a} = \overline{0+a} = \bar{a}, \quad \forall\, \bar{a} \in \mathbb{Z}_m.$$

Finalmente, para cada $\bar{a} \in \mathbb{Z}_m$, el elemento inverso respecto a + viene dado por $\overline{-a}$, ya que

$$\bar{a} + (\overline{-a}) = \overline{a+(-a)} = \bar{0}.$$

■

<u>Ejemplos</u>: Hallan las tablas de Cayley de $\mathbb{Z}_3$ y de $\mathbb{Z}_6$.

+	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

$(\mathbb{Z}_3, +)$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

$(\mathbb{Z}_6, +)$

Definamos ahora en $\mathbb{Z}_n$ la siguiente operación de multiplicación:

$$\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$$

$\bar{a} \cdot \bar{b} := \overline{a \cdot b}$, donde $a \cdot b$ es la multiplicación en $\mathbb{Z}$.

A partir de la propiedad conmutativa y asociativa de la multiplicación en $\mathbb{Z}$, se puede notar lo siguiente.

Proposición: La operación binaria $\cdot$ es conmutativa y asociativa en $\mathbb{Z}_n$.

Vemos además que $\bar{1} \cdot \bar{a} = \overline{1 \cdot a} = \bar{a}$ para todo $\bar{a} \in \mathbb{Z}_n$.

Proposición: $\bar{1}$ es el elemento neutro de la multiplicación $\cdot$ en $\mathbb{Z}_n$.

Sin embargo, el par $(\mathbb{Z}_n, \cdot)$ no es un grupo, ya que no existe $\bar{a} \in \mathbb{Z}_n$ tal que $\bar{0} \cdot \bar{a} = \bar{1}$.

Descantamos $\bar{0}$ y consideramos

$$\mathbb{Z}_n^* := \mathbb{Z}_n \setminus \{\bar{0}\}.$$

¿Es $(\mathbb{Z}_n^*, \cdot)$ un grupo? Veamos algunos ejemplos.

Ejemplos: Hallan las tablas de Cayley de $\mathbb{Z}_3^*$ y $\mathbb{Z}_6^*$.

$\cdot$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{2}$	$\bar{1}$

$(\mathbb{Z}_3^*, \cdot)$

$\cdot$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

$(\mathbb{Z}_6^*, \cdot)$

Vemos que en $(\mathbb{Z}_6^*, \cdot)$, $\bar{2} \cdot \bar{3} = \bar{0}$, por lo cual $\cdot$ ni siquiera es cerrada en $\mathbb{Z}_6^*$. Sin embargo, $(\mathbb{Z}_3^*, \cdot)$ sí es un grupo. Note que 3 es primo y 6 es compuesto, y esto no es casual.

Proposición: $(\mathbb{Z}_n^*, \cdot)$ es un grupo si y solamente si, n es primo. En tal caso, $o(\mathbb{Z}_n^*) = n-1$.

- Demostración: Supongamos primero que n es primo. Para ver que $(\mathbb{Z}_n^*, \cdot)$ es un grupo, faltaría probar la cerradura de $\cdot$ y el axiomas de

la existencia de inversos.

Sean $\bar{a}, \bar{b} \in \mathbb{Z}_m^*$. Entonces, $\bar{a} \cdot \bar{b} = \overline{ab} \in \mathbb{Z}_m^*$ si y solamente si $\overline{ab} \neq \bar{0}$. Supongamos lo contrario, es decir, $\overline{ab} = \bar{0}$. Luego, $m \mid a \cdot b$. Pero como m primo, se tiene que $m \mid a$ o $m \mid b$, es decir, $\bar{a} = \bar{0}$ o $\bar{b} = \bar{0}$, lo cual es una contradicción. Por lo tanto, $\bar{a} \cdot \bar{b} \in \mathbb{Z}_m^*$.

Dado ahora $\bar{a} \in \mathbb{Z}_m^*$, veamos que existe $\bar{b} \in \mathbb{Z}_m^*$ tal que $\bar{a} \cdot \bar{b} = \bar{1}$. Como m es primo, se tiene que $mcd(a, m) = 1$ tomando $a < m$ (se puede hacer cambiando el representante por el correspondiente resto de dividir a por m). Luego, la ecuación de congruencia $ax \equiv 1 \pmod{m}$ tiene solución única módulo m, digamos $x \equiv b \pmod{m}$. Entonces, $ab \equiv 1 \pmod{m}$, es decir, $\bar{a} \cdot \bar{b} = \bar{1}$.

Ahora supongamos que $(\mathbb{Z}_m^*, \cdot)$ es un grupo. Sea d un divisor de m, con $0 < d < m$. Luego, existe $0 < q < m$ en $\mathbb{Z}$ tal que $m = q \cdot d$, de donde $\bar{d} \cdot \bar{q} = \bar{0}$. Por otro lado, $\bar{d} \in \mathbb{Z}_m^*$, y posee inverso, llamémoslo $\bar{d}'$. Entonces,

$$\begin{aligned} \bar{d} \cdot \bar{q} = \bar{0} &\Rightarrow \bar{d}' \cdot (\bar{d} \cdot \bar{q}) = \bar{d}' \cdot \bar{0} \\ &\Rightarrow (\bar{d}' \cdot \bar{d}) \cdot \bar{q} = \bar{0} \\ &\Rightarrow \bar{1} \cdot \bar{q} = \bar{0} \\ &\Rightarrow \bar{q} = \bar{0} \end{aligned}$$

Así, $m \mid q$, lo cual es una contradicción.

Por lo tanto, m es primo ya que su único divisor positivo menor que m es 1. ∎

A manera más general, cuando m no es primo, aún es posible construir un grupo con la misma operación de multiplicación, a saber:

$$U(m) := \{ \bar{a} \in \mathbb{Z}_m : mcd(a, m) = 1 \}.$$

Proposición: $(U(m), \cdot)$ es un grupo abeliano.

· Demostración: Ya sabemos que $\cdot$ es conmutativo y asociativo en $\mathbb{Z}_m$, y en particular lo va a ser en $U(m)$. Además, $\bar{1}$ funge como elemento neutro.

- Cerradura de $\cdot$: Sean $\bar{a}, \bar{b} \in U(m)$.

Para ver que $\bar{a} \cdot \bar{b} = \overline{ab} \in U(m)$, debemos probar que $mcd(ab, m) = 1$.

$$\bar{a} \in U(m) \Rightarrow mcd(a, m) = 1 \Rightarrow \exists\, x_0, y_0 \in \mathbb{Z} \,/\, ax_0 + my_0 = 1.$$

$$\bar{b} \in U(m) \Rightarrow mcd(b, m) = 1 \Rightarrow \exists\, x_1, y_1 \in \mathbb{Z} \,/\, bx_1 + my_1 = 1.$$

Luego,

$$1 = (ax_0 + my_0)(bx_1 + my_1)$$

$1 = (ab)(x_0 x_1) + m(a x_0 y_1 + b x_1 y_0 + m y_0 y_1)$.

Lo anterior implica que $\text{mcd}(ab, m) = 1$.

Por lo tanto, $\bar{a} \cdot \bar{b} \in U(m)$.

- Existencia de inversos: Se demuestra de la misma manera que para $(\mathbb{Z}_m^*, \cdot)$ para el caso donde m es primo en la proposición anterior. ■

Grupo de permutaciones

A partir de cualquier conjunto B, puede construirse un grupo S_B de la siguiente forma

$$S_B := \{ f : B \to B \;/\; f \text{ es una función biyectiva} \},$$

donde la operación $\circ : S_B \times S_B \to S_B$ es la composición de funciones.

Para el caso particular en el cual

$$B = \{1, 2, \ldots, n\},$$

se obtiene el llamado <u>grupo de permutaciones de n elementos</u>, denotado por S_n.

$$S_n := \{ \sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\} \;/\; f \text{ es biyectiva} \}$$

Los elementos de S_n suelen denotarse de la siguiente manera:

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

Ejemplo: Para $n=3$, tenemos las siguientes permutaciones de tres elementos:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Luego, $S_3 = \{e, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5\}$.

Las permutaciones σ_1, σ_2 y σ_3 sólo intercambian dos elementos de $\{1,2,3\}$, y se conocen como trasposiciones.

- Toda permutación de S_n es una composición de trasposiciones.

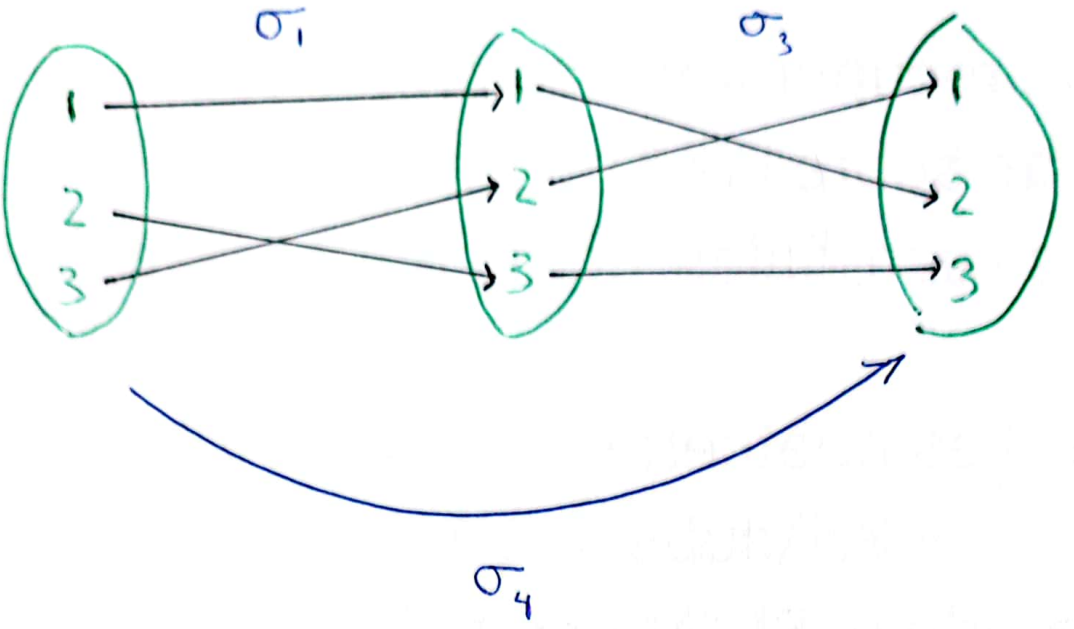
Para el caso de S_3, se tiene

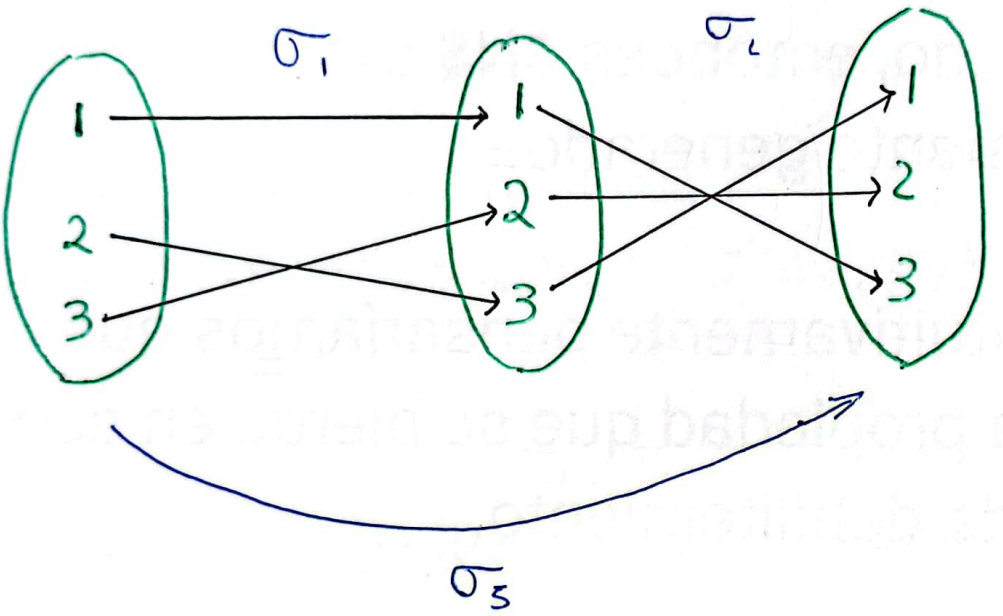
$e = \sigma_1 \circ \sigma_1$ $\qquad$ $\sigma_4 = \sigma_3 \circ \sigma_1$

$\sigma_1 = \sigma_1$ $\qquad$ $\sigma_5 = \sigma_2 \circ \sigma_1$

$\sigma_2 = \sigma_2$

$\sigma_3 = \sigma_3$





Note además que $o(S_3) = 6 = 3!$

Proposición: $(S_m, \circ)$ es un grupo finito no abeliano con

$$o(S_m) = m!$$

• Demostración: $\circ$ es cerrada en S_m porque la composición de funciones biyectivas es biyectiva.

La composición es claramente asociativa, y la función identidad sobre $\{1, 2, \dots, n\}$ es el elemento neutro de la composición. Finalmente, como la inversa de una función biyectiva es biyectiva, se tiene que toda permutación tiene inversa en S_n.

Para contar el número de elementos de S_n, tomamos $\sigma \in S_n$ arbitrario.

$$\sigma: \{1, 2, \dots, n\} \longrightarrow \{1, 2, \dots, n\}$$

- Hay n maneras de escoger $\sigma(1) \in \{1, 2, \dots, n\}$.
- Una vez escogido $\sigma(1)$, hay $n-1$ maneras de escoger $\sigma(2) \in \{1, 2, \dots, n\} \setminus \{\sigma(1)\}$, ya que σ es biyectiva.

⋮

- Hay $n-(i-1)$ maneras de escoger $\sigma(i)$.

⋮

- Hay una sola manera de escoger $\sigma(n)$, una vez elegidos $\sigma(1), \sigma(2), \dots, \sigma(n-1)$.

Por lo tanto, hay $n!$ maneras de definir σ (por medio de la elección de sus imágenes). ∎

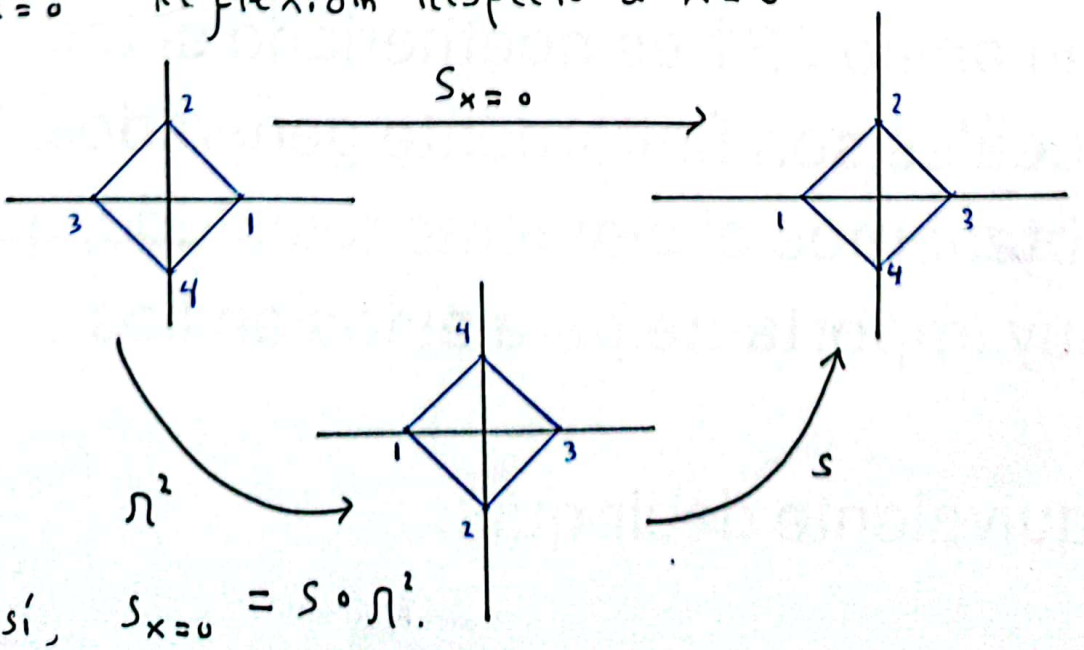
Grupo diedral

Al principio de estas notas consideramos el cuadrado de vértices $(1,0)$, $(0,1)$, $(-1,0)$ y $(0,-1)$, junto con el conjunto de rotaciones de ángulos $0°$, $90°$, $180°$ y $270°$, y las reflexiones de dicha figura respecto a $y=0$, $x=0$, $y=x$ e $y=-x$. Formalicemos la estructura de grupo mencionada para este conjunto de rotaciones y reflexiones.

- id = Rotación de $0°$.
- R = Rotación de $90°$.
- R^2 = Rotación de $180°$.
- R^3 = Rotación de $270°$.

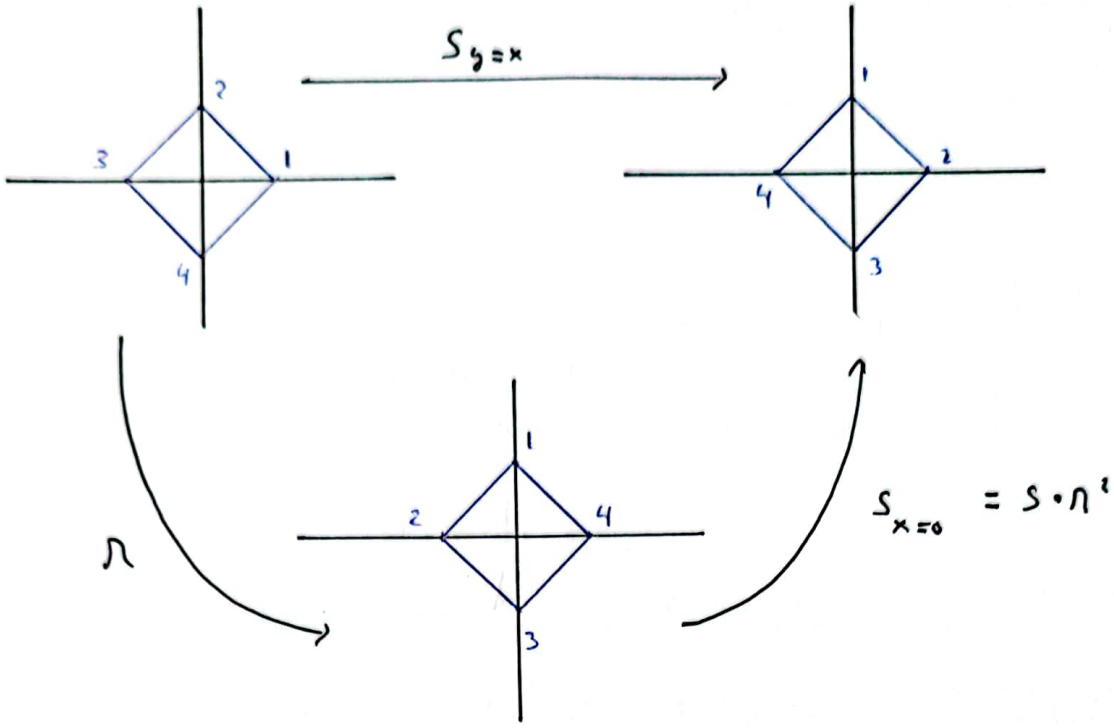
Por otro lado, denotemos por s la reflexión respecto al eje $y=0$. Veamos si se pueden obtener las otras tres reflexiones en términos de las simetrías restantes.

- $s_{x=0}$ = Reflexión respecto a $x=0$



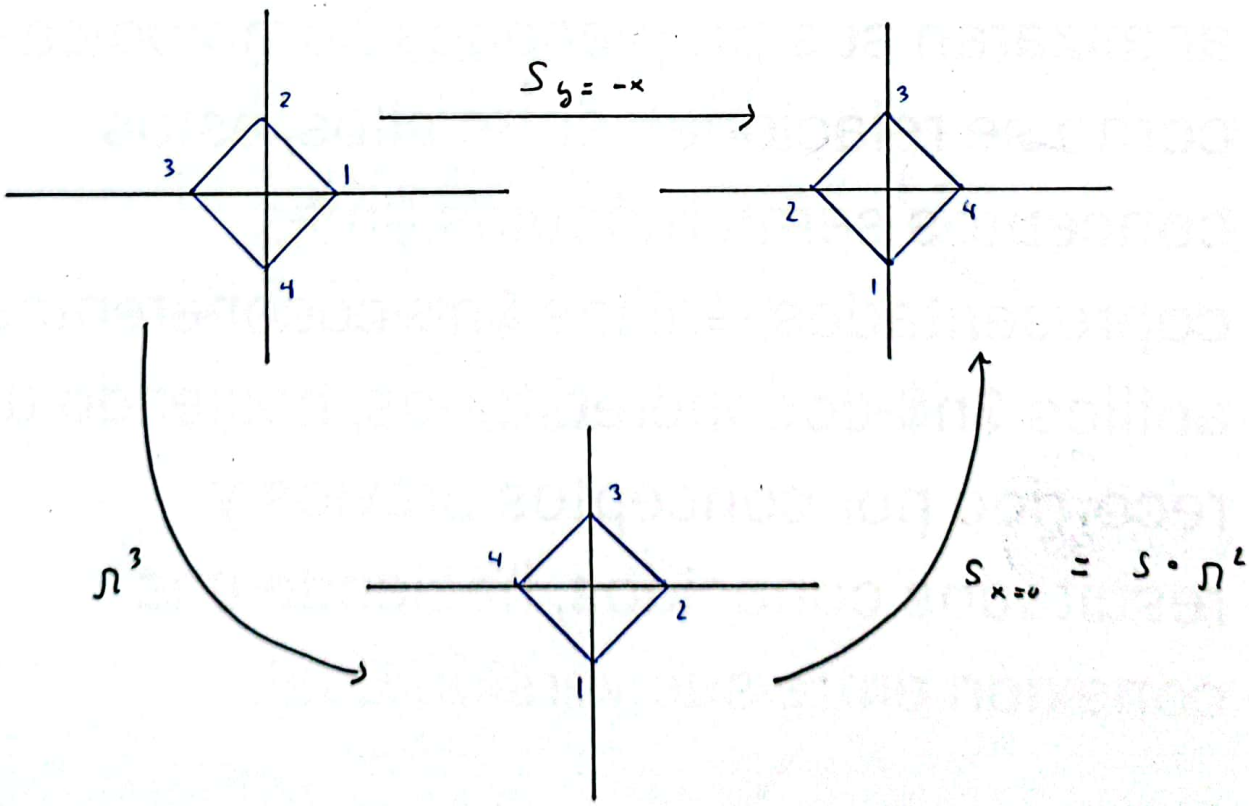
Así, $s_{x=0} = s \circ R^2$.

- $S_{y=x}$ = Reflexión respecto a $y = x$.



Así, $S_{y=x} = S \circ \Pi^3$

- $S_{y=-x}$: Reflexión respecto a $y = -x$.



Así, $S_{y=-x} = S \circ \Pi^3 = S \cdot \Pi$

Denotemos por D_4 al conjunto de rotaciones y reflexiones del cuadrado mencionados

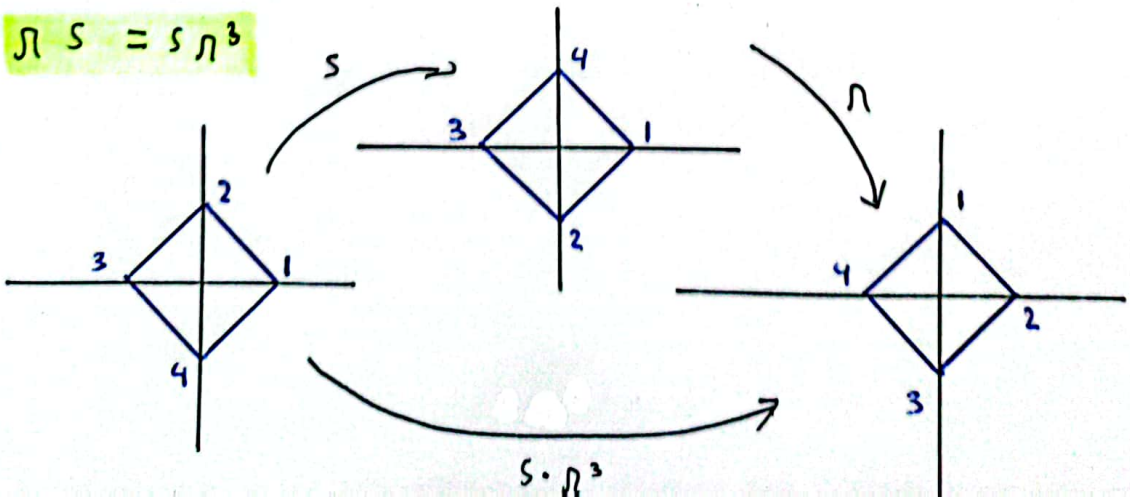
$$D_4 = \{ id, r, r^2, r^3, s, sr, sr^2, sr^3 \}$$

Proposición: Con la composición $\circ$ de simetrías, $(D_4, \circ)$ es un grupo no abeliano de orden 8.

- **Demostración:** Para ver que $\cdot$ es cerrada en D_4, calculamos la tabla de Cayley

$\circ$	id	r	r^2	r^3	s	sr	sr^2	sr^3
id	id	r	r^2	r^3	s	sr	sr^2	sr^3
r	r	r^2	r^3	id	sr^3	s	sr	sr^2
r^2	r^2	r^3	id	r	sr^2	sr^3	s	sr
r^3	r^3	id	r	r^2	sr	sr^2	sr^3	s
s	s	sr	sr^2	sr^3	id	r	r^2	r^3
sr	sr	sr^2	sr^3	s	r^3	id	r	r^2
sr^2	sr^2	sr^3	s	sr	r^2	r^3	id	r
sr^3	sr^3	s	sr	sr^2	r	r^2	r^3	id

- $r\,s = sr^3$



- $r(sr) = (rs)r = (sr^3)r = s.$
- $r(sr^2) = sr^3r^2 = sr.$
- $r(sr^3) = sr^3r^3 = sr^2.$
- $r^2s = r(rs) = r(sr^3) = sr^6 = sr^2.$
- $r^2(sr) = (r^2s)r = sr^2r = sr^3.$
- $r^2(sr^2) = sr^2r^2 = s.$
- $r^2(sr^3) = sr^2r^3 = sr.$
- $r^3s = r(r^2s) = rsr^2 = sr^3r^2 = sr.$
- $r^3(sr) = srr = sr^2.$
- $r^3(sr^2) = sr^2r = sr^3.$
- $r^3(sr^3) = sr^3r = s.$
- $s(sr) = s^2r = r.$
- $s(sr^2) = r^2.$
- $s(sr^3) = r^3.$
- $(sr)s = ssr^3 = r^3.$
- $(sr)(sr) = ssr^3r = id.$
- $(sr)(sr^2) = id \cdot r = r$
- $(sr)(sr^3) = r^2.$
- $(sr^2)s = ssr^2 = r^2.$
- $(sr^2)(sr) = r^2r = r^3.$
- $(sr^2)(sr^2) = r^3r = id.$
- $(sr^2)(sr^3) = id \cdot r = r.$
- $(sr^3)s = ssr = r.$
- $(sr^3)(sr) = r^2.$
- $(sr^3)(sr^2) = r^3.$
- $(sr^3)(sr^3) = r^4 = id.$

- Tenemos entonces que la composición de simetrías es cerrada en D_4. Dicha composición, al actuar como una composición de funciones, es claramente asociativa.
- id = notación de $0°$ (= función identidad) es claramente el elemento neutro de D_4.
- Al ver la tabla de Cayley, vemos que también se cumple la propiedad del inverso:

$(id)^{-1} = id \in D_4$.

$(r)^{-1} = r^3 \in D_4$

$(r^2)^{-1} = r^2 \in D_4$.

$(r^3)^{-1} = r \in D_4$.

$(s)^{-1} = s \in D_4$.

$(sr)^{-1} = sr \in D_4$.

$(sr^2)^{-1} = sr^2 \in D_4$.

$(sr^3)^{-1} = sr^3 \in D_4$. ■

Subgrupos

Estudiaremos ahora los subconjuntos $H \subseteq G$ de un grupo $(G, \cdot)$ que heredan la estructura de grupo de G.

Definición: Sea $(G, \cdot)$ un grupo y $H \subseteq G$ un subconjunto no vacío. Diremos que H es un **subgrupo de G**, denotado por $H < G$, si:

1) • es cerrada en H: Si $h_1, h_2 \in H$, entonces $h_1 \cdot h_2 \in H$.

2) H es cerrado bajo inversos: Si $h \in H$, entonces $h^{-1} \in H$.

Observaciones: Sea $(G, \cdot)$ un grupo y $\emptyset \neq H \subseteq G$.

1) Si $H < G$, entonces podemos restringir la operación $\cdot : G \times G \to G$ sobre $H \times H$ y obtenemos

$$\cdot|_{H \times H} : H \times H \to H,$$

ya que $\cdot$ es cerrada en H. Podemos notar que $(H, \cdot|_{H \times H})$ es un grupo. En efecto:

- La propiedad asociativa se cumple en H, ya que se cumple en G y $H \subseteq G$.
- El elemento neutro de G funge también como el elemento neutro de H.

2) Cuando se habla de H como subgrupo de G, se entiende que para H se considera como operación binaria la misma operación en G. En otras palabras, no nos referimos a $(H, *)$ como subgrupo de $(G, \cdot)$ si $* \neq \cdot$.

3) Si $e \notin H$, entonces H no es subgrupo de G. Supongamos que $H < G$ y sea $h \in H$ $(H \neq \emptyset)$. Luego, $h^{-1} \in H$. Además, $h \cdot h^{-1} \in H$ ya que $\cdot$ es cerrada en H. Es decir, $e = h \cdot h^{-1} \in H$, lo cual contradice la hipótesis.

4) Si $N < H$ y $H < G$, entonces $N < G$.

Ejemplos:

1) Sea $(G, \cdot)$ un grupo. Entonces, G y $\{e\}$ son subgrupos de G, llamados subgrupos triviales

2) $2\mathbb{Z} = \{2a / a \in \mathbb{Z}\}$ es un subgrupo de $(\mathbb{Z}, +)$.

"

números pares

Sin embargo, el subconjunto de $\mathbb{Z}$ formado por los números impares no es un subgrupo de $(\mathbb{Z}, +)$, ya que 0 no es impar.

De manera más general,

$n\mathbb{Z} = \{na / a \in \mathbb{Z}\}$ es un subgrupo de $(\mathbb{Z}, +)$.

3) $(GL(2, \mathbb{C}), \cdot)$

↳ producto usual de matrices.

↳ matrices invertibles en $M_{2\times 2}(\mathbb{C})$.

$$SL(2, \mathbb{C}) = \{A \in M_{2\times 2}(\mathbb{C}) / \det(A) = 1\}$$

$$SU(2) = \{A \in M_{2\times 1}(\mathbb{C}) / \det(A) = 1 \text{ y } A^{-1} = \overline{A^t}\}.$$

$$SU(2) < SL(2, \mathbb{C}) < GL(2, \mathbb{C}).$$

4) $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ es un subgrupo de $(\mathbb{R} \setminus \{0\}, \cdot)$.

Proposición (caracterizaciones de subgrupos):

Sea $(G, \cdot)$ un grupo y $\emptyset \neq H \subseteq G$.

1) $H < G$ si y solamente si $h_1 h_2^{-1} \in H$, $\forall h_1, h_2 \in H$.

2) Si H es finito, entonces $H < G$ si y solamente si $h_1 h_2 \in H$ $\forall h_1, h_2 \in H$.

- **Demostración:**

1) Supongamos que $H < G$ y sean $h_1, h_2 \in H$.

$h_2 \in H \underset{H<G}{\Longrightarrow} h_2^{-1} \in H$, y $h_1, h_2^{-1} \in H \underset{H<G}{\Longrightarrow} h_1 h_2^{-1} \in H$.

Ahora supongamos que $h_1 \cdot h_2^{-1} \in H$, $\forall h_1, h_2 \in H$.

Sea $h \in H$ cualquiera. Luego, $e = h \cdot h^{-1} \in H$. Y usando nuevamente la hipótesis, se tiene que $h^{-1} = e \cdot h^{-1} \in H$ ya que $e, h \in H$. Finalmente, sean $h_1, h_2 \in H$. Entonces, $h_2^{-1} \in H$, de donde $h_1 (h_2^{-1})^{-1} \in H$. Es decir,

$$h_1 h_2 = h_1 (h_2^{-1})^{-1} \in H.$$

2) La implicación directa es inmediata a partir de la definición de subgrupo. Supongamos ahora que $h_1 \cdot h_2 \in H$ $\forall h_1, h_2 \in H$. Sea $h \in H$. Queremos ver que $h^{-1} \in H$ para poder concluir que $H < G$.

Consideremos el conjunto

$$\{ h^m \,/\, m \in \mathbb{Z}^+ \} \subseteq G.$$

Note por la hipótesis que $h^m \in H$ $\forall m \in \mathbb{Z}^+$. Luego, como H es finito, existen $n > m$ en $\mathbb{Z}^+$ tales que:

$$h^n = h^m.$$

De donde $h^{n-m} = e$, es decir,

$$h \cdot h^{n-m-1} = e. \quad (*)$$

- Si $n-m-1 = 0$, entonces $h^m \cdot h = h^m$, y así $h = e$ por la ley cancelativa. Note que $e \in H$ pues $e = h^{n-m} \in H$ con $n-m \in \mathbb{Z}^+$. Se tiene entonces en este caso que $h^{-1} = e^{-1} = e \in H$.
- Si $n-m-1 > 0$, entonces la igualdad $(*)$ implica que

$$h^{-1} = h^{n-m-1} \in H.$$

En cualquier caso, $h^{-1} \in H$. $\forall\, h \in H$. ■

Ejemplos:

1) Considere el grupo S_3 de permutaciones de tres elementos.

Sea $T = \{id, \sigma_1, \sigma_2, \sigma_3\}$ el subconjunto de trasposiciones con la identidad. Vemos que T no es un subgrupo de S_3, ya que $\sigma_3 \circ \sigma_1 = \sigma_4 \notin T$.

Por otro lado, $H = \{id, \sigma_4, \sigma_5\}$ sí es un subgrupo de S_3, ya que $\sigma_4 \circ \sigma_4 = \sigma_5$, $\sigma_5 \circ \sigma_5 = \sigma_4$, $\sigma_4 \circ \sigma_5 = id$ y $\sigma_5 \circ \sigma_4 = id$.

2) Dentro del grupo diedral D_4, considere los subconjuntos de rotaciones y reflexiones dados por

$$Rot = \{id, r, r^2, r^3\} \quad y \quad Reflex = \{id, s, sr, sr^2, sr^3\}$$

Viendo la tabla de Cayley de D_4, vemos que la composición de simetrías es cerrada en Rot pero no en Reflex (e.g., $s \cdot sr = r \notin Reflex$). Por lo tanto, al ser Rot y Reflex subconjuntos finitos de D_4, se tiene que Rot es un subgrupo de D_4 pero Reflex no.

Además de tener maneras de verificar si un subconjunto de un grupo dado es un subgrupo, también existen métodos para generar subgrupos nuevos a partir de subgrupos conocidos de un mismo grupo. Más precisamente, la intersección (arbitraria) de subgrupos de un grupo $(G, \cdot)$ es un subgrupo de $(G, \cdot)$. Bajo ciertas condiciones, la unión de subgrupos de un grupo $(G, \cdot)$ es también un subgrupo de $(G, \cdot)$, aunque en general esto no es así, como muestra el siguiente ejemplo.

Ejemplo: Considere el grupo $(\mathbb{Z}, +)$ y los subgrupos $2\mathbb{Z}$ y $3\mathbb{Z}$. Sean $2, 3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$. Notamos que $2+3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$, ya que 5 no es múltiplo de 2 ni de 3. Entonces, la operación $+$ no es cerrada en $2\mathbb{Z} \cup 3\mathbb{Z}$

Proposición: Sea $(H_m : m \in \mathbb{N})$ una familia de subgrupos de un grupo $(G, \cdot)$, es decir, H_m es un subgrupo de $(G, \cdot)$ para todo $m \in \mathbb{N}$. Entonces:

1) $\bigcap_{m\in\mathbb{N}} H_m = \{h \in G \,/\, h \in H_m \ \forall m \in \mathbb{N}\}$ es un subgrupo de $(G, \cdot)$.

2) Si $H_0 \subseteq H_1 \subseteq \cdots \subseteq H_m \subseteq H_{m+1} \subseteq \cdots$, entonces

$$\bigcup_{m\in\mathbb{N}} H_m = \{h \in G \,/\, h \in H_m \text{ para algún } m \in \mathbb{N}\}$$

es un subgrupo de $(G, \cdot)$.

• **Demostración**:

1) Veamos primero que la operación $\cdot$ es cerrada en $\bigcap_{m\in\mathbb{N}} H_m$.

Sean $h, h' \in \bigcap_{m\in\mathbb{N}} H_m$. Luego,

$$h \in H_m \text{ y } h' \in H_m, \quad \forall m \in \mathbb{N}.$$

Dado $m \in \mathbb{N}$, como H_m es un subgrupo de $(G, \cdot)$, tenemos que $h \cdot h' \in H_m$.

Así, $h \cdot h' \in H_m \ \forall m \in \mathbb{N}$. Entonces, $h \cdot h' \in \bigcap_{m\in\mathbb{N}} H_m$.

De manera similar, si $h \in \bigcap_{m\in\mathbb{N}} H_m$ entonces $h^{-1} \in \bigcap_{m\in\mathbb{N}} H_m$ ya que:

$$h \in \bigcap_{m\in\mathbb{N}} H_m \Rightarrow h \in H_m, \ \forall m \in \mathbb{N} \underset{H_m < G}{\Longrightarrow} h^{-1} \in H_m, \ \forall m \in \mathbb{N} \Rightarrow h^{-1} \in \bigcap_{m\in\mathbb{N}} H_m.$$

2) Procedamos de manera similar a 1).

Sean $h, h' \in \bigcup_{m \in \mathbb{N}} H_m$. Luego, existen $n, m \in \mathbb{N}$ tales que

$$h \in H_m \quad y \quad h' \in H_m.$$

Sin pérdida de generalidad, podemos suponer $n \leq m$. Luego, como $H_n \subseteq H_m$, tenemos que

$$h, h' \in H_m.$$

Como H_m es un subgrupo de G, tenemos que

$$h \cdot h' \in H_m.$$

Por otro lado, para $h \in \bigcup_{m \in \mathbb{N}} H_m$, como $h \in H_m$ para algún $m \in \mathbb{N}$, tenemos que $h^{-1} \in H_m$ ya que H_m es un subgrupo de G. Luego, $h^{-1} \in H_m \subseteq \bigcup_{m \in \mathbb{N}} H_m$. (Note que para demostrar la "cerradura por inversos" no hace falta la hipótesis de contención $H_0 \subseteq H_1 \subseteq \cdots \subseteq H_m \subseteq H_{m+1} \subseteq \cdots$).

■