Simetría: Un enfoque utilizando teoría de grupos

1. Preliminares.

1.1. Relaciones.

Definición. *Dados dos conjuntos no vacíos A y B una* ***relación*** *(binaria) entre elementos de A y de B (o simplemente una relación entre A y B) es una terna $\mathcal{R} = (A, B, R)$ en que R es cualquier subconjunto de $A \times B$.*

Si $\mathcal{R} = (A, B, R)$ es una relación, usaremos la notación $a\mathcal{R}b$, que se lee "a está relacionado por $\mathcal{R}$ con b", o simplemente "a está relacionado con b", para indicar el hecho de que $(a, b) \in R$. Si $(a, b) \in (A \times B)/R$ diremos que "a no esta relacionado por $\mathcal{R}$ con b" y usaremos la notación $a\not\mathcal{R}b$. Además, el conjunto A se dirá **conjunto de partida**, y B **conjunto de llegada** (o **recorrido**) de $\mathcal{R}$.

Ejemplos:

1. $\mathcal{R}_1 = (\mathbb{N}, \mathbb{N}, R_1)$, donde $R_1 = \{(a, b) \in \mathbb{N} \times \mathbb{N} \mid \ (\exists k \in \mathbb{Z})\ a - b = 3k\}$ (congruencia módulo 3).
2. $\mathcal{R}_2 = (\mathbb{N}, \mathbb{N}, R_2)$, donde $R_2 = \{(n, m) \in \mathbb{N} \times \mathbb{N} \mid \ (\exists k \in \mathbb{N})\ m = k \cdot n\}$ (divisibilidad en $\mathbb{N}$).
3. $\mathcal{R}_3 = (\mathbb{R}, \mathbb{R}, R_3)$, donde $R_3 = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid 3|x| - 2y \geq 7\}$.

Sea $\mathcal{R} = (A, B, R)$ una relación. Definimos su **dominio** por $\mathrm{Dom}(\mathcal{R}) = \{a \in A \mid \ (\exists b \in B)\ a\mathcal{R}b\}$, y su **imagen** por $\mathrm{Im}(\mathcal{R}) = \{b \in B \mid \ (\exists a \in A)\ a\mathcal{R}b\}$. El conjunto R suele llamarse **gráfico** de la relación $\mathcal{R}$ y se anota $R = \mathcal{G}(\mathcal{R})$. Es directo que $R \subseteq \mathrm{Dom}(\mathcal{R}) \times \mathrm{Im}(\mathcal{R})$, pero en general no es cierta la igualdad como conjuntos.

Toda función induce a una relación. Si $f : A \to B$ es una función, la relación asociada es $\mathcal{R}_f = (A, B, R_f)$, donde el conjunto de pares ordenados R_f está dado por

$$R_f = \{(a, b) \in A \times B \mid \ b = f(a)\}.$$

Claramente se cumple que $a\mathcal{R}_f b \Leftrightarrow b = f(a)$, $\mathrm{Dom}(\mathcal{R}_f) = \mathrm{Dom}(f)$ e $\mathrm{Im}(\mathcal{R}_f) = \mathrm{Im}(f)$.

Igualdad de relaciones: De la definición de relación como una terna, es directo que dos relaciones $\mathcal{R}_1 = (A_1, B_1, R_1)$ y $\mathcal{R}_2 = (A_2, B_2, R_2)$ son iguales ssi $A_1 = A_2 \wedge B_1 = B_2 \wedge R_1 = R_2$. A su vez, es también claro que si $A_1 = A_2 \wedge B_1 = B_2$, entonces $R_1 = R_2 \Leftrightarrow (\forall a \in A_1)(\forall b \in B_1)\ (a\mathcal{R}_1 b \Leftrightarrow a\mathcal{R}_2 b)$. De aquí que se cumple:

Proposición. *Dos relaciones $\mathcal{R}_1, \mathcal{R}_2$ son iguales ssi*

1. *$\mathcal{R}_1$ y $\mathcal{R}_2$ tienen el mismo conjunto de partida A,*

2. *$\mathcal{R}_1$ y $\mathcal{R}_2$ tienen el mismo conjunto de llegada B, y*

3. *Los elementos se relacionan por $\mathcal{R}_1$ y $\mathcal{R}_2$ de la misma forma, es decir,* $(\forall a \in A_1)(\forall b \in B_1)\ (a\mathcal{R}_1 b \Leftrightarrow a\mathcal{R}_2 b)$.

1.2. Relaciones donde $A = B$.

Sea A un conjunto no vacío. Llamaremos a una relación $\mathcal{R} = (A, A, R)$ de A en sí mismo, una relación binaria en A, o simplemente una relación en A, y abreviaremos su notación como $\mathcal{R} = (A, R)$. En este caso aparecen 4 propiedades claves a ser estudiadas:

1. **Reflexividad:** Decimos que $\mathcal{R}$ es **refleja** (o **reflexiva**) ssi $(\forall a \in A)\ a\mathcal{R}a$.

2. **Simetría:** Decimos que $\mathcal{R}$ es **simétrica** ssi $(\forall a, b \in A) a\mathcal{R}b \Leftrightarrow b\mathcal{R}a$.

3. **Antisimetría:** Decimos que $\mathcal{R}$ es **antisimétrica** ssi $(\forall a, b \in A)\ a\mathcal{R}b \wedge b\mathcal{R}a \Rightarrow a = b$.

4. **Transitividad:** Decimos que $\mathcal{R}$ es **transitiva** ssi $(\forall a, b, c \in A)\ a\mathcal{R}b \wedge b\mathcal{R}c \Rightarrow a\mathcal{R}c$.

La simetría y la antisimetría no se dan usualmente juntas, sin embargo NO son una la negación de la otra. En efecto existen relaciones que satisfacen ambas propiedades, por ejemplo, la relacíon de igualdad en A : $(\forall a, b \in A)\ a\mathcal{R}b \Leftrightarrow a = b$. Aquí $\mathcal{R} = (A, \Delta_A)$, donde $\Delta_A = \{(a, a) \mid a \in A\}$ es la llamada "diagonal"de A.

Ejemplo importante:

Estudiemos las 4 propiedades anteriores para la relación $\mathcal{R}$ en $\mathbb{Z}$ tal que

$$n\mathcal{R}m \Leftrightarrow (\exists k \in \mathbb{Z})\ n = m + k \cdot p.$$

donde $p \in \mathbb{N}$ es un natural fijo. Esta relación se llama de congruencia módulo p y si $n\mathcal{R}m$ decimos que "n es congruente con m módulo p", o que "n es igual a m módulo p". Son usuales las notaciones $n \equiv m \pmod{p}$ o $n \equiv_p m$.

- Simetría: Sean $n, m \in \mathbb{Z}$ tales que $n \equiv_p m$. Hay que probar que $m \equiv_p n$. Sabemos que $n \equiv_p m \Leftrightarrow (\exists k \in \mathbb{Z})\ n = m + k \cdot p$. Sea $k_0 \in \mathbb{Z}$ tal que $n = m + k_0 \cdot p$. Despejando se tiene que $m = n + (-k_0) \cdot p$, Es decir hemos encontrado un entero $k_1 = -k_0$ tal que $m = n + k_1 \cdot p$ lo que prueba que $m \equiv_p n$.

- Refleja: Sea $n \in \mathbb{Z}$. Debemos probar que $n \equiv_p n$. Es decir hay que encontrar $k \in \mathbb{Z}$ tal que $n = n + k \cdot p$. Basta tomar $k = 0$, con lo cual $n = n + 0 \cdot p = n$ y se concluye que $n \equiv_p n$.

- Transitividad: Sean $n, m, l \in \mathbb{Z}$ tales que $m \equiv_p n \wedge n \equiv_p l$. Hay que probar que $m \equiv_p l$. Se tiene $m \equiv_p n \Leftrightarrow m = n + k_1 \cdot p$ para un cierto $k_1 \in \mathbb{Z}$, y $n \equiv_p l \Leftrightarrow n = l + k_2 \cdot p$ para un cierto $k_2 \in \mathbb{Z}$. Luego, despejando, se obtiene $m = l + (k_1 + k_2) \cdot p$. Hemos encontrado un entero $k_3 = k_1 + k_2$ tal que $m = l + k_3 \cdot p$, luego $m \equiv_p l$.

- Antisimetría: No lo es si $p \neq 0$ pues, por ejemplo si $n = 0, m = p$, se tiene que $0 \equiv_p p$ y además $p \equiv_p 0$ pero $p \neq 0$. Si $p = 0$, la relación $\equiv_0$ es la igualdad en $\mathbb{Z}$, por lo que no es sorprendente que $\equiv_0$ sea también antisimétrica.

Además esta relación cumple las siguientes propiedades:

(a) $(\forall m_1, m_2, n_1, n_2 \in \mathbb{Z})\ m_1 \equiv_p n_1 \wedge m_2 \equiv_p n_2 \Rightarrow m_1 + m_2 \equiv_p n_1 + n_2$.

(b) $(\forall m_1, m_2, n_1, n_2 \in \mathbb{Z})\ m_1 \equiv_p n_1 \wedge m_2 \equiv_p n_2 \Rightarrow m_1 \cdot m_2 \equiv_p n_1 \cdot n_2$.

En efecto, la hipótesis $m_1 \equiv_p n_1 \wedge m_2 \equiv_p n_2$ significa que $m_1 = n_1 + k_1 \cdot p \wedge m_2 = n_2 + k_2 \cdot p$, para algunos $k_1, k_2 \in \mathbb{Z}$.

(a) Sumando estas ecuaciones, obtenemos $m_1 + m_2 = n_1 + n_2 + k_1 \cdot p + k_2 \cdot p = n_1 + n_2 + (k_1 + k_2) \cdot p$, de donde sale que $m_1 + m_2 \equiv_p n_1 + n_2$.

(b) Multiplicando las mismas ecuaciones, obtenemos $m_1 \cdot m_2 = n_1 \cdot n_2 + (n_1 \cdot k_2 + n_2 \cdot k_1 + k_1 \cdot k_2 \cdot p) \cdot p$, de donde sale que $m_1 \cdot m_2 \equiv_p n_1 \cdot n_2$.

Definición.

1. *Decimos que una relación $\mathcal{R}$ en A es de **equivalencia** ssi es refleja, simétrica y transitiva.*
2. *Decimos que una relación $\mathcal{R}$ en A es de **orden** ssi es refleja, antisimétrica y transitiva.*

   *Si $\mathcal{R}$ es una relación de orden en A, entonces si $a\mathcal{R}b$ decimos que a **precede de** b, y diremos que a y b son **comparables** ssi $a\mathcal{R}b \vee b\mathcal{R}a$. Distinguimos dos tipos de ordenes:*

   (a) ***Orden parcial:** Si existe al menos un par de elementos $a, b \in A$ que no son comparables por $\mathcal{R}$.*

   (b) ***Orden total:** Si todo par de elementos $a, b \in A$ son comparables por $\mathcal{R}$.*

Ejemplo: La relación de divisibilidad en $\mathbb{N}$ es un orden parcial y la relación $\leq$ es un orden total.

1.3. Relaciones de equivalencia.

Recordemos que una relación $\mathcal{R}$ en A es de equivalencia ssi es refleja, simétrica y transitiva.

Definición. *Dado $a \in A$ llamamos **clase de equivalencia** de a relativa a $\mathcal{R}$ al conjunto $[a]_{\mathcal{R}} = \{b \in A \mid a\mathcal{R}b\}$ (todos los elementos de A que están relacionados con A).*

Ejemplo: Considere la relación de congruencia módulo 2 en $\mathbb{Z}$ ($\equiv_2$). En esta relación $[0]_{\mathcal{R}}$ es el conjunto de los pares, $[1]_{\mathcal{R}}$ es el conjunto de los enteros impares, $[3]_{\mathcal{R}}$ son los impares, $[4]_{\mathcal{R}} = [0]_{\mathcal{R}}$. En este ejemplo existen sólo 2 clases de equivalencia distintas: $[0]_{\mathcal{R}}$ y $[1]_{\mathcal{R}}$. Observemos que $\mathbb{Z} = [0]_{\mathcal{R}} \cup [1]_{\mathcal{R}}$. Además $[0]_{\mathcal{R}} \cap [1]_{\mathcal{R}} = \emptyset$.

Propiedades:

1. Para cada $a \in A$, $[a]_{\mathcal{R}} \neq \emptyset$.
2. Para cada par de elementos $a, b \in A$, si $a\mathcal{R}b$, entonces $[a]_{\mathcal{R}} = [b]_{\mathcal{R}}$.
3. Para cada par de elementos $a, b \in A$, si $a\not\mathcal{R}b$, entonces $[a]_{\mathcal{R}} \cap [b]_{\mathcal{R}} = \emptyset$.

Las dos propiedades anteriores permiten definir una **partición** de A.

Esto es, una familia de subconjuntos de A, dos a dos disjuntos, cuya unión es A. De manera más precisa, existe un conjunto de subconjuntos no vacíos de A, $P \subseteq \mathcal{P}(A)$ (que será la partición de A), tal que si $B, B' \in P \wedge B \neq B'$ entonces $B \cap B' = \emptyset$ (dos a dos disjuntos) y

$$A = \bigcup_{B \in P} B.$$

Esta última unión se entiende como sigue

$$\bigcup_{B \in P} B = \{x \in A \mid \ (\exists B \in P)\ x \in B\}.$$

La partición que nos interesa construir es la formada por las clases de equivalencia de $\mathcal{R}$, es decir,

$$P_{\mathcal{R}} = \{[a]_{\mathcal{R}} \mid a \in A\}.$$

Este conjunto se llama **conjunto cuociente** de $\mathcal{R}$, y se suele anotar también como $A/\mathcal{R}$.

Ejemplo importante:

Para $p \in \mathbb{N}$, encontrar el conjunto cuociente de $\mathbb{Z}$ por la relación de equivalencia $\equiv_p$, que anotamos por $\mathbb{Z}_p$ (los "enteros módulo p"). Anotaremos la clase de equivalencia de $n \in \mathbb{Z}$ como $[n]_p$. Veamos primero un par de casos triviales:

- Si $p = 0$, sabemos que $\equiv_0$ es la igualdad en $\mathbb{Z}$, y entonces $[n]_0 = \{n\}$ para cada $n \in \mathbb{Z}$. Luego $\mathbb{Z}_0 = \{\{n\} \mid n \in \mathbb{Z}\}$.
- Si $p = 1$, entonces es directo que $(\forall m, n \in \mathbb{Z})\ m \equiv_1 n$, por lo que hay una sola clase de equivalencia: $[n]_1 = \mathbb{Z}$ para todos los enteros n, y $\mathbb{Z}_1 = \{\mathbb{Z}\}$ (un conjunto con un solo elemento).

Ahora supondremos que $p \geq 2$. Esta es la restricción que generalmente se impone cuando se usan las congruencias módulo p en la práctica. Haremos uso de la división de números enteros, que se puede enunciar como sigue: Si $a, b \in \mathbb{Z}$ y $b \neq 0$, entonces existe una única pareja de enteros q, r, llamados respectivamente cuociente y resto de la división de a por b, tales que $a = q \cdot b + r$, y además $0 \leq r < |b|$.

Si $n \in \mathbb{Z}$ es un entero cualquiera, dividiéndolo por p obtenemos $n = q \cdot p + r$, con $0 \leq r < p$. Pero esta ecuación dice que $n \equiv_p r$, es decir, que $n \in [r]_p$. De aquí que las clases de equivalencia para $\equiv_p$ son sólo $[0]_p, [1]_p, ..., [p-1]_p$. Además estas p clases son distintas entre sí, puesto que si $r_1 \equiv r_2$, para $0 \leq r_1, r_2 < p$, entonces $r_2 = k \cdot p + r_1$. Pero como también $r_2 = 0 \cdot p + r_2$, entonces la unicidad de la división de r_2 por p entrega $r_1 = r_2$.

Concluimos entonces que $\mathbb{Z}_p = \{[0]_p, [1]_p, ..., [p-1]_p\}$, y tiene exactamente p elementos.

1.4. Leyes de composición interna

Definición. *Sea A un conjunto no vacío. Una* ***ley de composicíon interna*** *(abreviado l.c.i.) en A es una función de $A \times A$ en A. Estas funciones también se llaman operaciones binarias (o, simplemente operaciones), y la notación que se usa para indicar el resultado de la ley de composición interna sobre $(a, b) \in A \times A$ es $a * b$, $a + b$, $a \cdot b$, etc. El ente $a * b$ se lee "a operado con b por la operación $*$", por ejemplo. Usamos la notación $(A, *)$ para indicar que el conjunto A esta dotado de la ley de composición interna. También decimos que $(A, *)$ es una* ***estructura algebraica****.*

Ejemplos:

1. En $A = \{0, 1\}$ definimos la ley de composición interna **suma módulo 2** por la siguiente tabla

$+_2$	0	1
0	0	1
1	1	0

   (se lee por ejemplo $0 +_2 1 = 1$). También se define la **multiplicación modulo 2** por

$\cdot_2$	0	1
0	0	1
1	1	0

2. En $A = \{0, 1, 2, 3\}$ definimos la ley de composición interna **suma módulo 4** por la siguiente tabla

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

3. El conjunto $A = \mathbb{Z}$ tiene la operación de suma como l.c.i.

4. El conjunto $\mathbb{R}$ de los numeros reales tiene a la suma como l.c.i.

5. Generalizando los ejemplos 1 y 2, para cada $p \in \mathbb{N}$ con $p \geq 2$, definiremos una suma y una multiplicación en el conjunto $\mathbb{Z}_p$ de los enteros módulo p. Recordemos de los ejemplos importantes anteriores que $\mathbb{Z}_p$ es el conjunto cuociente de los enteros $\mathbb{Z}$ por la relación $\equiv_p$ de congruencia módulo p, y que $\mathbb{Z}_p = \big\{[0]_p, [1]_p, ..., [p-1]_p\big\}$. También vimos que $\equiv_p$ cumplía las siguientes propiedades: $(\forall m_1, m_2, n_1, n_2 \in \mathbb{Z})\ m_1 \equiv_p m_2 \wedge n_1 \equiv_p n_2 \Rightarrow m_1 + m_2 \equiv_p n_1 + n_2 \wedge m_1 \cdot m_2 \equiv_p n_1 \cdot n_2$. Esto se puede reescribir como

   $$(\forall m_1, m_2, n_1, n_2 \in \mathbb{Z})\ [m_1] = [m_2] \wedge [n_1] = [n_2] \Rightarrow [m_1 + m_2] = [n_1 + n_2] \wedge [m_1 \cdot m_2] = [n_1 \cdot n_2].$$

(Hemos omitido el subíndice p de la notación de las clases de equivalencia para facilitar un poco la lectura). Esta última propiedad nos indica que no hay ninguna ambigüedad al definir, para $[m], [n] \in \mathbb{Z}_p$, $[m] +_p [n] = [m+n] \in \mathbb{Z}_p$, $[m] \cdot [n] = [m \cdot n] \in \mathbb{Z}_p$ (ya que, módulo p, las operaciones no dependen del representante de cada clase). Resulta entonces que tenemos dos leyes de composición interna, $+$ y $\cdot$, definidas sobre $\mathbb{Z}_p$.

Para simplificar la notación, muchas veces se eliminan incluso los paréntesis de la notación de clases de equivalencia en $\mathbb{Z}_p$, escribiendo $\mathbb{Z}_p = \{0, 1, ..., p-1\}$. Suele también anotarse el $+$ de $\mathbb{Z}_p$ como $+_p$ y el $\cdot$ de $\mathbb{Z}_p$ como $\cdot_p$. Con estas convenciones, el ejemplo 1 es simplemente la suma y el producto en $\mathbb{Z}_2$, y el ejemplo 2 corresponde a la suma en $\mathbb{Z}_4$.

1.5. Propiedades básicas de las l.c.i

Sea $(A, *)$ una estructura algebraica.

1. **Elementos Neutros:** Decimos que e es un elemento neutro para una ley de composición interna $*$ si se cumple
$$(\forall a \in A)\ e * a = a * e = a.$$
Propiedad: El neutro, cuando existe, es único (y tenemos entonces derecho a hablar de **el** neutro).
En efecto, supongamos que existen neutros e y e'. Luego $e' = e * e' = e$.

2. **Asociatividad:** Decimos que la l.c.i. en A es **asociativa** ssi
$$(\forall a, b, c \in A) \qquad (a * b) * c = a * (b * c).$$

3. **Elementos inversos:** Si existe neutro e, decimos que $a \in A$ tiene a $b \in A$ como inverso, o que b es un inverso para a ssi
$$a * b = b * a = e.$$
En general, un inverso b para $a \in A$ no es único. Cuando sea único lo anotaremos a^{-1}. Una condición de unicidad es la siguiente,
Propiedad: Si $*$ tiene neutro y es asociativa entonces los inversos son únicos.
En efecto, sean $a \in A$, $b_1, b_2 \in A$ tales que $a * b_1 = b_1 * a = e$ y $a * b_2 = b_2 * a = e$. Luego operando por b_2 la primera igualdad por la izquierda se obtiene $b_2 * (a * b_1) = b_2 * e$. Como la ley es asociativa entonces $(b_2 * a) * b_1 = b_2$, de lo que deducimos que $b_1 = e * b_1 = b_2$.

4. **Conmutatividad:** Decimos que la l.c.i. $*$ en A es **conmutativa** ssi
$$(\forall a, b \in A) \qquad a * b = b * a.$$

Supongamos que $(A, *)$ es una estructura algebraica asociativa y con neutro e.

1. Si $a \in A$ tiene inverso que llamamos a^{-1} entonces a^{-1} tiene inverso y es $(a^{-1})^{-1} = a$. En efecto, buscamos $b \in A$ tal que $a^{-1} * b = b * a^{-1} = e$. Pero sabemos que $a * a^{-1} = a^{-1} * a = e$, luego por unicidad $b = a$.

2. Si $a \in A$ tiene inverso a^{-1} y $b \in A$ tiene inverso b^{-1} entonces $a * b$ tiene inverso y es $(a * b)^{-1} = b^{-1} * a^{-1}$.

   Verifiquemos que $(a * b) * (b^{-1} * a^{-1}) = (b^{-1} * a^{-1}) * (a * b) = e$.

$$\begin{array}{rcll} (a * b) * (b^{-1} * a^{-1}) & = & a * (b * b^{-1}) * a^{-1} & \text{(asociatividad)} \\ & = & a * e * a^{-1} & (b^{-1} \text{ inverso de } b) \\ & = & (a * e) * a^{-1} = a * a^{-1} = e, & \text{(razones similares)} \\ (b^{-1} * a^{-1}) * (a * b) & = & b^{-1} * (a^{-1} * a) * b & \\ & = & (b^{-1} * e) * b & \\ & = & b^{-1} * b = e. & \end{array}$$

   Por unicidad, $(b^{-1} * a^{-1})$ es el inverso.

Veamos algunas propiedades adicionales de las l.c.i.:

1. **Cancelabilidad:** Un elemento $a \in A$ es **cancelable** ssi

$$(\forall b, c \in A)\ (a * b = a * c \Rightarrow b = c) \wedge (b * a = c * a \Rightarrow b = c).$$

   Algunos elementos cancelables: Si existe neutro e, este es cancelable; si existe neutro e y la l.c.i. es asociativa, entonces si a tiene inverso, será cancelable. En efecto

$$\begin{array}{rl} a * b = a * c & /a^{-1}* \\ a^{-1} * (a * b) = a^{-1} * (a * c) & \\ (a^{-1} * a) * b = (a^{-1} * a) * c & \text{(asociatividad)} \\ e * b = e * c & (a^{-1} \text{ inverso de } a) \\ b = c & (e \text{ neutro}) \end{array}$$

   Análogamente se prueba que $(b * a = c * a \Rightarrow b = c)$ si a es invertible.

2. **Elemento Absorbente (cero):** $a \in A$ es un **elemento absorbente** ssi

$$(\forall b \in A)\ a * b = a \wedge b * a = a.$$

   Por ejemplo en $(\mathbb{R}, \cdot)$ el 0 es absorbente.

3. **Elemento Idempotente:** $a \in A$ es un elemento idempotente ssi $a * a = a$. A modo de ejemplo, un neutro y un absorbente son siempre idempotentes.

2. Teoría de Grupos

2.1. Definiciones Básicas

Definición (Grupo). *Sea $(A, *)$ una estructura algebraica con una ley de composición interna. Decimos que $(A, *)$ es un* ***grupo*** *si:*

1. *$*$ es asociativa.*
2. *$*$ tiene neutro $1 \in G$.*
3. *toda $g \in G$ tiene inverso $g^{-1} \in G$ para $*$.*

Con esta definición de grupo, es directo que el neutro es único, al igual que el inverso g^{-1} de $g \in G$.

También se tienen las siguientes propiedades:

1. $(g^{-1})^{-1} = g$.
2. $(g * h)^{-1} = h^{-1} * g^{-1}$.

Un grupo $(G, *)$, donde $*$ es conmutativo, se denomina **Abeliano**.

Ejemplos: Los siguientes son algunos ejemplos de grupos

- $(\mathbb{Z}, +)$ es un grupo abeliano.
- $(\mathbb{Z}_p, +)$ es un grupo abeliano.
- Sea $A = \{\pi : \{1,2,3\} \to \{1,2,3\} \mid \pi \text{ es función biyectiva } \}$ y se considera la operación $*$: "composición de funciones". Este conjunto tiene 6 elementos que se pueden nombrar $\pi_0, \pi_1, \pi_2, \pi_3, \pi_4, \pi_5$. Luego la operación se puede ver en la tabla

$*$	π_0	π_1	π_2	π_3	π_4	π_5
π_0	π_0	π_1	π_2	π_3	π_4	π_5
π_1	π_1	π_0	π_4	π_5	π_2	π_3
π_2	π_2	π_3	π_0	π_1	π_5	π_4
π_3	π_3	π_2	π_5	π_4	π_0	π_1
π_4	π_4	π_5	π_1	π_0	π_3	π_2
π_5	π_5	π_4	π_3	π_2	π_1	π_0

  Con esta operación $(A, *)$ es un grupo, pero no es abeliano.

Definición (Morfismo de grupos). *Una función $f : G \to H$, entre dos grupos $(G, *), (H, \diamond)$ se dice* ***morfismo (u homomorfismo)*** *ssi:*

$$\forall x, y \in G \qquad f(x * y) = f(x) \diamond f(y).$$

Un morfismo inyectivo suele llamarse **monomorfismo**, uno sobreyectivo se llama **epimorfismo**, y finalmente un morfismo biyectivo se llama **isomorfismo**.

$$(G, \cdot) \cong (H, *) \Leftrightarrow G \text{ isomorfo a } H$$

Endomorfismo es un morfismo de un grupo en si mismo; un **automorfismo** es un isomorfismo endomorfo.

Propiedades

Si $f : G \to H$ es un morfismo de grupos, entonces

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

Si $f : G \to H$ es un morfismo de grupos llamaremos **Núcleo** de f a $Ker(f) = f^{-1}(1)$.

Con esto, f es monomorfismo $\Leftrightarrow Ker(f) = \{1\}$.

Ejemplos:

- La función logaritmo (en cualquier base), $log : (\mathbb{R}_+, \cdot) \to (\mathbb{R}, +)$ tiene la conocida propiedad $log(a \cdot b) = log(a) + log(b)$, y como es biyectiva, es un isomorfismo entre $(\mathbb{R}_+, \cdot)$ y $(\mathbb{R}, +)$. Asi $(\mathbb{R}_+, \cdot)$ y $(\mathbb{R}, +)$ son estructuras isomorfas.
- Si $\alpha \in \mathbb{R}$ es un real fijo, la función $f : (\mathbb{R}, +) \to (R, +)$ tal que $f(x) = \alpha \cdot x$ es un homomorfismo, dado que $f(x_1 + x_2) = \alpha \cdot (x_1 + x_2) = \alpha \cdot x_1 + \alpha \cdot x_2 = f(x_1) + f(x_2)$. Si además $\alpha \neq 0$, entonces f es un automorfismo.

Definición (Subgrupo). *Si $(G, *)$ es un grupo, y $H \subseteq G$, diremos que H es un **subgrupo** de G si $(H, *)$ es también un grupo.*

Si H es un subgrupo de $(G, *)$, el neutro de $(H, *)$ es el mismo que el de $(G, *)$, y para cada $g \in H$, si $g^{-1} \in G$ es su inverso en $(G, *)$, también g^{-1} es el inverso de g en $(H, *)$ (y por lo tanto $g^{-1} \in H$).

Una caracterización de los subgrupos es la siguiente:

$H \subseteq G$ es subgrupo ssi:

1. $H \neq \emptyset$.
2. $(\forall x, y \in H) \qquad x * y^{-1} \in H$.

Definición. *Si $(G, *)$ es grupo, una relación de equivalencia $\sim$ en G se dice compatible con $*$ ssi:*

$$(\forall x, x', y, y' \in G) \qquad x \sim x' \wedge y \sim y' \Rightarrow x * y \sim x' * y'.$$

Dada una relación de equivalencia $\sim$ compatible con $*$, podemos definir una l.c.i. en el conjunto cuociente $G/\sim$.

$$[x] * [y] = [x * y].$$

La compatibilidad hace que la operación $*$ en $G/\sim$ esté bien definida. Es directo que en este caso $(G/\sim, *)$ resulta ser un grupo, y la sobreyección canónica

$$\begin{array}{rccc} \nu: & G & \to & G/\sim \\ & x & \to & \nu(x) = [x]. \end{array}$$

es un epimorfismo. (Por este motivo ν también recibe el nombre de epimorfismo canónico).

Ahora, si $\sim$ es compatible con $*$, entonces

$$\begin{aligned} x \sim y &\Leftrightarrow 1 = x^{-1} * x \sim x^{-1} * y \quad \text{(compatibilidad y } \sim \text{ refleja).} \\ &\Leftrightarrow x^{-1} * y \in [1]. \end{aligned}$$

Llamemos $H = [1]$ (subgrupo). Con esto se tiene la siguiente propiedad:

Si $h \in H$ y $x \in G$ es un elemento cualquiera de G, entonces $x * h * x^{-1} \in H$. En efecto:

$$\begin{aligned} h \in H &\Leftrightarrow h \sim 1. \\ &\Rightarrow x * h \sim x * 1 = x \qquad \text{(compatibilidad de } \sim \text{ con } *). \\ &\Rightarrow (x * h) * x^{-1} \sim x * x^{-1} = 1 \quad \text{(compatibilidad de } \sim \text{ con } *). \\ &\Rightarrow x * h * x^{-1} \in H = [1] \qquad \text{(asociatividad para eliminar paréntesis).} \end{aligned}$$

O sea, $(\forall x \in G)\ x * H * x^{-1} = \{x * h * x^{-1} \mid h \in H\} \subseteq H$.

Definición (Subgrupo normal). *Un subgrupo H de G tal que satisface*

$$(\forall x \in G) \quad x * H * x^{-1} \subseteq H.$$

se llama ***subgrupo normal*** *de G.*

Se usará la siguiente notación para designar a los subgrupos normales de G

$$H \lhd G \Leftrightarrow \ H \text{ subgrupo normal de } G.$$

Esto caracteriza completamente a las relaciones compatibles con $*$. En efecto, si partimos de un subgrupo normal $H \lhd G$ dado, definimos la relación $\sim_H$ en G tal que

$$x \sim_H y \Leftrightarrow x^{-1} * y \in H$$

Entonces

1. $\sim_H$ es de equivalencia en G.

2. $\sim_H$ es compatible con $*$.

3. $[1] = H$.

Notación: Si G es un grupo, y $H \lhd G$, el cuociente $G/\sim_H$ se anota como G/H. **Ejemplos:**

- Cualquier subgrupo de un grupo Abeliano $(A, *)$ es un subgrupo normal, gracias a la conmutatividad de la operación $*$. En efecto, sea H subgrupo de A. Entonces

$$x * H * x^{-1} = \{x * h * x^{-1} \mid h \in H\} \overset{*\text{ conmuta}}{=} \{(x * x^{-1}) * h \mid h \in H\} = H.$$

- El núcleo de todo morfismo de grupos $f : G \to H$ es un subgrupo normal de G; es más, todos los subgrupos normales de G son núcleos de algun morfismo. En efecto
  - Si $a \in G$ y $x \in Ker(f)$

$$f(a * x * a^{-1}) \overset{f\text{ morfismo}}{=} f(a) * \cancelto{1}{f(x)} * f(a^{-1}) = 1.$$

    Por lo tanto $a * x * a^{-1} \in Ker(f) \Rightarrow Ker(f)$ subgrupo normal.
  - Si $K \lhd G$, tomemos $H = G/K$ y $f = \nu_K : G \to G/K$ morfismo. Luego

$$\nu_K(x) = 1 \in G/K \Leftrightarrow [x] = [1] = K \Leftrightarrow x \in K.$$

    Luego $Ker(\nu_K) = K$.

Definición (Subgrupo generado por un subconjunto). *Sea G un grupo, y $A \subseteq G$ un subconjunto cualquiera. Denotemos*

$$< A >= \bigcap_{\substack{A \subseteq H \\ H\ subgrupo}} H.$$

el subgrupo generado por A.

Se tiene $A \subseteq < A >$. Mas aun, $< A >$ es más pequeño (en el sentido de la inclusión) de los subgrupos de G que contiene a A. Evidentemente, si A es subgrupo de G entonces $< A >= A$.

Es también claro que

$$A \subseteq \underbrace{\{{a_1}^{n_1} \cdots {a_k}^{n_k} \mid k \geq 0,\ a_1, \cdots, a_k \in A\ ;\ n_1, \cdots, n_k \in \mathbb{Z}\}}_{\text{es subgrupo}} \subseteq < A > .$$

Por lo tanto:

$$< A >= \{{a_1}^{n_1} \cdots {a_k}^{n_k} \mid k \geq 0,\ a_1, \cdots, a_k \in A\ ;\ n_1, \cdots, n_k \in \mathbb{Z}\}.$$

Caso interesante

Si $A = \{a\}$ entonces $< A >= \{a^n \mid n \in \mathbb{Z}\}$ y se denomina **subgrupo cíclico generado por a**.

Un grupo G se dice **cíclico** si

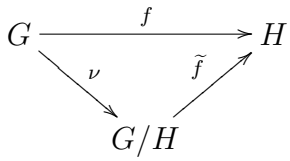
$$\exists a \in G \text{ tal que } \quad < \{a\} >= G.$$

Así $G = \{a^n \mid n \in \mathbb{Z}\}$. Veremos que los grupos cíclicos son "pocos", y para eso nos ayudaremos del siguiente resultado.

Teorema (Teorema del factor). *Si G, H grupos, $f : G \to H$ morfismo, y $K \lhd G$ tal que $K \subseteq Ker(f)$. Entonces:*

$$\exists! \ \ morfismo \ \ \widetilde{f} : G/K \to H.$$

tal que el diagrama siguiente es conmutativo



*Con ν el epimorfismo canónico (introducido anteriormente). Es claro que $f = \widetilde{f} \circ \nu$. Se dice que f se **factoriza** a través de G/K. Además*

$$\begin{array}{lcl} f \text{ es un epimorfismo} & \Leftrightarrow & \widetilde{f} \text{ es un epimorfismo.} \\ \widetilde{f} \text{ es monomorfismo} & \Leftrightarrow & K = Ker(f). \end{array}$$

Usando este resultado se puede demostrar la siguiente proposición

Proposición. *Si G es un grupo cíclico, entonces:*

- *Si G es infinito $\Rightarrow$ $G \cong (\mathbb{Z}, +)$.*
- *Si G es finito $\Rightarrow$ $G \cong (\mathbb{Z}_p, +)$.*

Donde $p \geq 1$ (notemos que $p = |G|$).

3. Acciones de Grupos

Definición. *Sea $(G, *)$ un grupo, y $X \neq \emptyset$ un conjunto. Una **acción** (izq) de G en X es una función*

$$\begin{array}{rccc} \mu: & G \times X & \to & X \\ & (g, x) & \to & \mu(g, x) \overset{notación}{=} g \cdot x. \end{array}$$

Con las siguientes propiedades

1. $(\forall x \in X) \quad 1 \cdot x = x.$
2. $(\forall g, h \in G) \quad g \cdot (h \cdot x) = (g * h) \cdot x.$

Ahora veamos algunos ejemplos de acciones:

1. Sea G un grupo cualquiera de $(Biy(X), \circ)$, donde $Biy(X) = \{f \mid f : X \to X \text{ es biyectiva}\}$. La siguiente es una acción de G en X:

$$\begin{array}{ccc} G \times X & \to & X \\ (g, x) & \to & g \cdot x = g(x). \end{array}$$

2. Sea $X = G$. La siguiente es una acción de G (como grupo) en G (como conjunto).

$$\begin{array}{ccc} G \times G & \to & G \\ (g, x) & \to & g \cdot x = g * x. \end{array}$$

3. Acción de G sobre si mismo por conjugación

$$\begin{array}{ccc} G \times G & \to & G \\ (g, x) & \to & g \cdot x = g * x * g^{-1}. \end{array}$$

Observación: Si $(G, *)$ es un grupo y $X \neq \emptyset$, una **acción derecha** de G en X es una función:

$$\begin{array}{rccc} \delta: & G \times X & \to & X \\ & (g, x) & \to & \delta(g, x) \overset{\text{notación}}{=} x \cdot g. \end{array}$$

Tal que:

1. $(\forall x \in X) \quad x \cdot 1 = x.$
2. $(\forall g, h \in G) \quad (x \cdot g) \cdot h = x \cdot (g * h).$

Nótese que no es igual a una acción izquierda, porque G no es necesariamente abeliano. Dada una acción derecha cualquiera $(\cdot)$, tiene asociada una acción izquierda canónica $(\diamond)$:

$$\begin{array}{lll} G \times X & \to & X \\ (g, x) & \to & g \diamond x \stackrel{\text{def}}{=} x \cdot g^{-1}. \end{array}$$

Otra posible definición de una acción:

Si

$$\begin{array}{lll} G \times X & \to & X \\ (g, x) & \to & g \cdot x. \end{array}$$

es una acción, y se deja $g \in G$ fijo, se define una función:

$$\begin{array}{lll} \mu_g : & X & \to & X \\ & x & \to & \mu_g(x) = g \cdot x. \end{array}$$

μ_g es una **biyección**, y su inversa es $\mu_{g^{-1}}$. Además

$$\mu_g \circ \mu_h = \mu_{g*h}.$$

$$\mu_1 = id_X.$$

Se tiene que entonces existe una función:

$$\begin{array}{lll} \phi : & G & \to & Biy(X) \\ & g & \to & \phi(g) = \mu_g. \end{array}$$

que es un morfismo de $(G, *)$ en $(Biy(X), \circ)$. Con esto μ (acción) produce ϕ (morfismo).

Al reves, si

$$\psi : (G, *) \to (Biy(X), \circ)$$

es un morfismo, definamos

$$\begin{array}{lll} \mu : & G \times X & \to & X \\ & (g, x) & \to & \psi(g)(x) \stackrel{\text{notación}}{=:} g \diamond x. \end{array}$$

Es una acción de G en X. En efecto:

1. $1 \diamond x = \psi(1)(x) = id_X(x) = x.$
2. $g \diamond (h \diamond x) = \psi(g)\big(\psi(h)(x)\big) = [\psi(g) \circ \psi(h)](x) = \psi(g * h)(x) = (g * h) \diamond x.$

Así, las acciones de G en X son exactamente los morfismos de $(G, *)$ en $(Biy(X), \circ)$.

Notación: Si

$$\begin{array}{lll} G \times X & \to & X \\ (g, x) & \to & g \cdot x \end{array}$$

es una acción, se denotara **órbita** de un elemento $x \in X$ por la acción de G, al conjunto

$$Orb(x) = \{g \cdot x \mid g \in G\}.$$

Acá lo que hay escondido es una relación de equivalencia en X

$$x \sim y \Leftrightarrow (\exists g \in G) \quad y = g \cdot x.$$

Con esto $Orb(x) = [x]$ y

$$X = \coprod_{\lambda \in \Lambda} Orb(x_\lambda)$$

$\{x_\lambda : \lambda \in \Lambda\}$ contiene un representante por órbita.

Una acción se dice **transitiva** si produce una sola órbita, es decir ssi:

$$(\forall x, y \in X)(\exists g \in G) \text{ tal que} \quad y = g \cdot x.$$

Nomenclatura: Si $\mu : G \times X \to X$ es una acción de G en X, diremos que X es un G-espacio. El G-espacio se dice homogéneo, si la acción es transitiva.

Si $(G, *)$ es un grupo, y X, Y son dos G-espacios. Un morfismo de G-espacios es una función $f : X \to Y$ tal que :

$$(\forall x \in X)(\forall y \in Y) \quad f(g \cdot x) = g \cdot f(x).$$

Tal función f se denotara función G-equivariante.

Sea X un G-espacio, y sea $x_0 \in X$. Se denotara **estabilizador** de x_0 al subconjunto de G:

$$Est(x_0) = \{g \in G \mid g \cdot x_0 = x_0\}.$$

Claramente el estabilizador es subgrupo de G.

Teorema. *Si X es un G-espacio homogéneo, entonces*

$$X \cong G/H \qquad \textit{isomorfismo de } G\textit{-espacios.}$$

donde $H = Est(x_0)$, $x_0 \in X$ cualquiera.

4. Simetría

Para poder analizar la simetría usando la teoría de grupos, se debe dar una definición de la misma ambientada en el campo de la teoría de grupos.

Definición (Simetría). *Sea $A \subseteq X$, con X un G-espacio. Si*

$$(\exists g \in G,\ g \neq 1) \quad g \cdot A = \{g \cdot x \mid x \in A\} = A.$$

A se denotara simétrico con respecto a la acción de $g \in G$. En este caso se dirá que g es ***núcleo de simetrías*** *de A y se denotara por $g \rhd A$*

Supongamos ahora que μ es una acción de G en X tal que $(\exists g \in G) \quad g \cdot A = A$ para $A \subseteq X$. ¿Que pasa con el conjunto $g \cdot (g \cdot A)$?

Pues en este caso resulta ser también igual a A.

En efecto:

$$g \cdot (g \cdot A) = \{g \cdot y \mid y \in g \cdot A\} \overset{g \cdot A = A}{=} \{g \cdot x \mid x \in A\} = A.$$

Notando también que $g \cdot (g \cdot A) = g^2 \cdot A$, se tiene, aplicando inducción, que

$$(\forall \tilde{g} \in H =< \{g\} >) \quad \tilde{g} \cdot A = A.$$

Definición. *$A \subseteq X$, X G-espacio se dirá simétrico con respecto al grupo G ssi:*

$$(\forall g \in G) \qquad g \cdot A = A.$$

Con esto, se tiene que si $\exists g \in G$ tal que $g \cdot A = A$, A es simétrico con respecto al grupo $H =< \{g\} >$. Ahora si definimos

$$Sim(G, A) =< \bigcup_{g \rhd A} g >\subseteq G$$

se tiene que A es simétrico respecto al subgrupo $Sim(G, A) \subseteq G$ y se tiene que este es el subgrupo maximal tal que A sea simétrico con respecto a algún subgrupo de G.

En efecto, supongamos que $\exists \tilde{g} \notin Sim(G, A)$ tal que $\tilde{g} \cdot A = A$.

Luego

$$\tilde{g} \rhd A \quad \Rightarrow \quad < \{\tilde{g}\} >\subseteq Sim(G, A) \quad \Rightarrow \quad \tilde{g} \in Sim(G, A) \rightarrow\leftarrow .$$

Ahora supongamos que tenemos dos G-espacios X, Y, y una función G-equivariante f. También supongamos que $g \rhd A$. Se tiene:

$$f(A) \overset{g \rhd A}{=} f(g \cdot A) = \{f(g \cdot x) \mid x \in A\} = \{g \cdot f(x) \mid x \in A\} = g \cdot f(A).$$

Luego

$$g \rhd f(A) \quad \forall f \ \text{ función } G\text{-equivariante.}$$

Ahora supongamos que $\exists! g \in G$ tal que $g \rhd A$. En este caso g es el único núcleo de simetrías de A, a lo cual de dirá que A tiene **simetría cíclica** con respecto a g. En este caso el subgrupo maximal de simetría es $\widetilde{G} =< \{g\} >$.

5. Aplicación

5.1. Simetría e invariabilidad ante transformaciones.

Habitualmente, el término simetría se utiliza para designar una suerte de "buena proporción"entre las diversas partes que constituyen un todo. En este sentido, la simetría se asocia a algún tipo de equilibrio en la manera en que distintos elementos se integran para formar un objeto, y se le suele asociar con la belleza en las formas de la naturaleza y en el arte.

Un ejemplo importante de simetría es la bilateral, que en términos generales se puede describir diciendo que si la mitad de la izquierda se refleja en un espejo entonces se obtiene la de la derecha. De esta forma, una forma que posee simetría bilateral permanece invariable cuando se realiza una reflexión en torno a su eje.

Este ejemplo sugiere que una forma de formalizar matemáticamente la noción de simetría consiste en estudiar las transformaciones que dejan invariable el objeto en observación.

Una transformación es una regla para realizar movimientos de objetos. Estos movimientos pueden ser rígidos : rotaciones, traslaciones y reflexiones. Una dilatación es un cambio de escala dado por una expansión o una contracción uniforme en torno a algún punto fijo determinado que se denomina centro de la dilatación.

Si la forma de un objeto permanece invariable luego de aplicarle una transformación dada, entonces decimos que posee la simetría asociada a dicha transformación. Por ejemplo, si a un círculo se le aplica una rotación en un ángulo arbitrario en torno a su centro, se conserva la forma del círculo. Todo objeto con esta propiedad se dice que posee **simetría circular.**

Veamos que las rotaciones, traslaciones y reflexiones pueden ser vistas como acciones de grupos.
Nota: Desde ahora el objeto en cuestión será un conjunto acotado de $\mathbb{R}^3$.

- **Rotaciones.**
  Primero notemos que $(\mathbb{R}, +)$ es un grupo abeliano. Sea $\equiv_{2\pi}$ la relación dada por

  $$x \equiv_{2\pi} y \Leftrightarrow (\exists z \in \mathbb{R})\ x = 2\pi \cdot z + y.$$

  Claramente $\equiv_{2\pi}$ es una relación de equivalencia compatible con $+$. Luego podemos hablar del grupo cuociente $(\mathbb{R}_{2\pi}, +)$. Sea μ la siguiente acción de $\mathbb{R}_{2\pi}$ en $\mathbb{R}^3$.

  $$\begin{array}{rll} \mu: & (\mathbb{R}_{2\pi}, +)^2 \times \mathbb{R}^3 \to & \mathbb{R}^3 \\ & ((\alpha, \beta), \vec{x}) \to & \mu((\alpha, \beta), \vec{x}) = \vec{\alpha} \cdot \vec{x} \end{array}$$

  Con $\vec{\alpha} = (\alpha, \beta)$. μ consiste en rotar en un ángulo α la componente θ y en un ángulo β la componente ϕ del vector $\vec{x}$ visto con coordenadas esféricas (r, θ, ϕ).
  Veamos que efectivamente se trata de una acción:

a) $\vec{1}\cdot\vec{x}$ consiste en rotar $\vec{x}$ en el neutro de $(\mathbb{R}_{2\pi},+)^2$, el cual es el $\vec{1}=(0,0)$, luego $\vec{x}$ no sufre ninguna rotación, luego

$$1\cdot\vec{x}=\vec{x}.$$

b) $\vec{\alpha}\cdot(\vec{\beta}\cdot\vec{x})$ consiste en primero rotar $\vec{x}$ primero en el vector angular $\vec{\beta}$, para luego rotarlo en vector angular $\vec{\alpha}$, lo cual claramente es lo mismo que rotar $\vec{x}$ en el vector angular $\vec{\alpha}+\vec{\beta}$, el cual es la operación en el grupo $(\mathbb{R}_{2\pi},+)^2$ de $\vec{\alpha}$ con $\vec{\beta}$. Luego

$$\vec{\alpha}\cdot(\vec{\beta}\cdot\vec{x})=(\vec{\alpha}+\vec{\beta})\cdot\vec{x}.$$

Luego efectivamente estamos hablando de una acción. Esta es la acción rotación respecto al origen. Cabe señalar que una rotación de un vector $\vec{x}$ en $\mathbb{R}^2$ corresponde a la proyección sobre el plano XY de la rotación de un vector $\vec{z}$ tal que $\Pi_{XY}(\vec{z})=\vec{x}$.

- **Traslaciones.**
En este caso el grupo que usaremos será $(\mathbb{R}^3,+)$, y la acción es simplemente la acción de $\mathbb{R}^3$ como conjunto sobre $\mathbb{R}^3$ como grupo, es decir

$$\begin{array}{lcl}\mu:\mathbb{R}^3\times\mathbb{R}^3 & \to & \mathbb{R}^3\\ (\vec{g},\vec{x}) & \to & \mu(\vec{g},\vec{x})=\vec{g}+\vec{x}.\end{array}$$

μ es claramente una acción. Así queda definida la acción traslación.

- **Reflexiones.**
Para hablar de reflexión , primero debemos considerar que se entiende por reflexión. La idea del reflejado con respecto a un eje nos da la idea de como definirla de manera conveniente. La reflexión será entendida como sigue: Dado un hiperplano $\Pi\subset\mathbb{R}^3$, la reflexión de $\vec{x}$ seria el reflejado del vector sobre el hiperplano. Sin perdida de generalidad podemos suponer que son hiperplanos que pasan por el origen, ya que una reflexión por un hiperplano Π cualquiera puede ser entendida como una traslación en $\vec{y}$ combinada con una reflexión por hiperplano $\widetilde{\Pi}$ que pasa por el origen. Claramente se debe tener que $\Pi=\vec{y}+\widetilde{\Pi}$. Ahora tenemos que dar una definición del reflejado de $\vec{x}$ con respecto a un hiperplano $\widetilde{\Pi}$ que pasa por el origen. La reflexión de $\vec{x}$ sobre $\widetilde{\Pi}$ es un vector $\vec{y}$ tal que en la componente según $\vec{n}$, la normal del hiperplano $\widetilde{\Pi}$, tenga el signo opuesto que la componente según $\vec{n}$ del vector $\vec{x}$, mientras que la componente de $\vec{x}$ sobre $\widetilde{\Pi}$ se mantiene constante.
Como estamos suponiendo que los hiperplanos pasan por el origen, el único dato relevante es la normal al hiperplano. Claramente el conjunto de todas las normales de todos los hiperplanos que pasan por el origen es $\mathbb{R}^3$. La siguiente es una acción de $\mathbb{R}^3$ (como grupo) sobre $\mathbb{R}^3$ (como conjunto)

$$\begin{array}{lcl}\mu:\mathbb{R}^3\times\mathbb{R}^3 & \to & \mathbb{R}^3\\ (\vec{n},\vec{x}) & \to & \mu(\vec{n},\vec{x}).\end{array}$$

Donde $\mu(\vec{n}, \vec{x})$ consiste en cambiar de signo la componente $\vec{n}$ de $\vec{x}$. Mas explicitamente

$$\mu(\vec{n}, \vec{x}) = \vec{x} - 2 < \vec{x}, \vec{n} > \vec{n}.$$

- **Dilataciones.**
  Las dilataciones las entenderemos como una expansión o una disminución en el tamao de un vector $\vec{x}$ en un factor α. La acción correspondiente es de $(\mathbb{R}_+/\{0\}, \cdot)$ sobre $\mathbb{R}^3$.

$$\begin{array}{lcl} \mu : \mathbb{R} \times \mathbb{R}^3 & \rightarrow & \mathbb{R}^3 \\ (n, \vec{x}) & \rightarrow & \mu(n, \vec{x}). \end{array}$$

  Donde $\mu(n, \vec{x})$ consiste en la ponderación por el escalar n del vector $\vec{x}$. Es directo ver que es una acción.

6. Aplicaciones.

Veamos como utilizar la simetría vista como acción de grupos para analizar la simetría presente en la espiral equiangular.
La espiral logaritmica en coordenadas polares esta descrita por la siguiente formula :

$$r(\theta) = ce^{a\theta}.$$

con c, a constantes. Con $a < 0$ se logra la espiral que aparece en la concha del nautilus, cuando θ va de cero a infinito.
Supongamos que primero aplicamos una dilatación en un factor $\alpha > 0$ con lo cual la formula queda

$$r'(\theta) = \alpha \cdot [ce^{a\theta}].$$

Ahora aplicar una rotación del vector $r(\theta)$ en un angulo φ en coordenadas polares consiste en encontrar $r'(\theta)$ tal que

$$r'(\theta + \varphi) = r(\theta).$$

Claramente $r'(\theta) = r(\theta - \varphi)$ resuelve el problema. Apliquemos una rotación en un angulo φ_0 a nuestro vector $r'(\theta)$, con lo cual obtendremos:

$$r''(\theta) = r'(\theta - \varphi_0) = \alpha \cdot [ce^{a(\theta-\varphi_0)}] = [\alpha \cdot e^{-a\varphi_0}] \cdot ce^{a\theta}.$$

Ahora elegimos φ_0 tal que

$$e^{-a\varphi_0} = \frac{1}{\alpha}.$$

Esto se logra tomando $\varphi_0 = \frac{\ln(\alpha)}{a}$ (bien definido pues $\alpha > 0$), y la formula resultante es:

$$r''(\theta) = ce^{a\theta} = r(\theta).$$

Luego la acción conjunta de una dilatación en un escalar $\alpha > 0$ con una rotación en un angulo $\varphi_0 = \frac{ln(\alpha)}{a}$ dejan invariante la curva de la espiral equiangular.