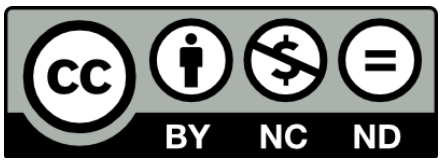
Álgebra II

Los Del DGIIM, losdeldgiim.github.io

Doble Grado en Ingeniería Informática y Matemáticas
Universidad de Granada



Álgebra II

Los Del DGIIM, `losdeldgiim.github.io`

José Juan Urrutia Milán

Granada, 2025

Índice general

En Álgebra I el objeto principal de estudio fueron los anillos conmutativos, conjuntos en los que teníamos definidas dos operaciones, una usualmente denotada con notación aditiva y otra con notación multiplicativa.

Posteriormente, el estudio se centró en los dominios de integridad (DI), anillos conmutativos donde teníamos más propiedades con las que manejar nuestros elementos (como la tan característica propiedad cancelativa). Después, el objeto de estudio fueron los dominios euclídeos (DE), donde ya podíamos realizar un estudio sobre la divisibilidad de los elementos del conjunto.

Finalmente, nos centramos en los dominios de factorización única (DFU), donde realizamos una breve introducción a la irreducibilidad de los polinomios.

En esta asignatura el principal objeto de estudio serán los grupos, conjuntos en los que hay definida una sola operación que entendemos por "buena[1]". Por tanto, los grupos serán estructuras menos restrictivas que los anillos conmutativos, aunque su estudio no será menos interesante.

[1]La operación cumplirá ciertas propiedades deseables.

1. Grupos: definición, generalidades y ejemplos

Comenzamos realizando la primera definición necesaria para entender el concepto de grupo, que es entender qué es una operación dentro de un conjunto.

Definición 1.1 (Operación binaria)**.** Sea G un conjunto, una operación binaria en G es una aplicación

$$\begin{array}{rccc} * : & G \times G & \longrightarrow & G \\ & (a, b) & \longmapsto & a * b \end{array}$$

Ejemplo. Ejemplos de operaciones binarias sobre conjuntos que ya conocemos son:

1. La suma y el producto de números en $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}, \mathbb{C}$.
2. Dado un conjunto X, los operadores $\cap$ y $\cup$ son operaciones binarias sobre el conjunto $\mathcal{P}(X)$.

Antes de dar la definición de grupo, daremos la de monoide, que es menos restrictiva que la de grupo.

Definición 1.2 (Monoide)**.** Un monoide es una tripleta $(G, *, e)$ donde G es un conjunto no vacío, $*$ es una operación binaria en G y e es un elemento destacado de G de forma que se verifica:

i) La propiedad asociativa de $*$:

$$(x * y) * z = x * (y * z) \qquad \forall x, y, z \in G$$

ii) La existencia de un elemento neutro (el elemento destacado de G):

$$\exists e \in G \mid e * x = x * e = x \qquad \forall x \in G$$

Proposición 1.1. *En un monoide, el elemento neutro es único.*

Demostración. Sea $(G, *, e)$ un monoide y sea $f \in G$ tal que $f * x = x * f = x$ $\forall x \in G$:

$$f = f * e = e$$

□

Ejemplo. Ejemplos de monoides ya conocidos son:

1. $(\mathbb{N}, +, 0)$, $(\mathbb{N}, \cdot, 1)$

2. Dado un conjunto X: $(\mathcal{P}(X), \cap, X)$, $(\mathcal{P}(X), \cup, \emptyset)$

Definición 1.3 (Grupo)**.** Un grupo es una tripleta $(G, *, e)$ donde G es un conjunto no vacío, $*$ es una operación binaria en G y e es un elemento destacado de G de forma que se verifica:

i) La propiedad asociativa de $*$:

$$(x * y) * z = x * (y * z) \qquad \forall x, y, z \in G$$

ii) La existencia de un elemento neutro por la izquierda (el elemento destacado de G):

$$\exists e \in G \mid e * x = x \qquad \forall x \in G$$

iii) La existencia de un elemento simétrico por la izquierda para cada elemento de G:

$$\forall x \in G \quad \exists x' \in G \mid x' * x = e$$

Si además se cumple:

iv) La propiedad conmutativa de $*$:

$$x * y = y * x \qquad \forall x, y \in G$$

Entonces, diremos que $(G, *, e)$ es un grupo conmutativo o abeliano.

Notación. Para una mayor comodidad a la hora de manejar grupos, introducimos las siguientes notaciones:

1. Cuando dado un conjunto no vacío G sepamos por el contexto a qué grupo $(G, *, e)$ nos estamos refiriendo, indicaremos simplemente G (o en algunos casos $(G, *)$, para hacer énfasis en la operación binaria) para referirnos al grupo $(G, *, e)$.

2. En algunos casos, usaremos (por comodidad) la notación multiplicativa de los grupos. De esta forma, dado un grupo $(G, \cdot, 1)$, en ciertos casos notaremos la operación binaria $\cdot$ simplemente por yuxtaposición:

   $$x \cdot y = xy \qquad \forall x, y \in G$$

   Además, nos referiremos al elemento neutro como "uno" y al simétrico de cada elemento como "inverso", sustituyendo la notación de x' por la de x^{-1}.

3. Otra notación que también usaremos (aunque de forma menos frecuente que la multiplicativa) será la aditiva. Dado un grupo $(G, +, 0)$, nos referiremos al elemento neutro como "cero" y al simétrico de cada elemento como "opuesto", sustituyendo la notación de x' por la de $-x$.

Ejemplo. Ejemplos de grupos que se usarán con frecuencia en la asignatura son:

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ con su respectiva suma son grupos abelianos.

2. $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ con su respectivo producto son grupos abelianos.

   Notemos la importancia de eliminar el 0 de cada conjunto para que todo elemento tenga inverso, así como que $\mathbb{Z}^*$ no es un grupo, ya que el inverso de cada elemento (para el producto al que estamos acostumbrados) no está dentro de $\mathbb{Z}^*$.

3. $\{1, -1, i, -i\} \subseteq \mathbb{C}$ con el producto heredado[1] de $\mathbb{C}$ también es un grupo abeliano.

4. $(\mathcal{M}_2(\mathbb{R}), +)$ es un grupo abeliano.

5. Dado un cuerpo $\mathbb{K}$, el grupo lineal de orden 2 con coeficientes en dicho cuerpo:

   $$\mathrm{GL}_2(\mathbb{K}) = \{M \in \mathcal{M}_2(\mathbb{K}) : \det(M) \neq 0\}$$

   con el producto heredado de $\mathcal{M}_2(\mathbb{K})$ es un grupo que no es conmutativo.

6. $\mathbb{Z}_n$ con su suma es un grupo abeliano, $\forall n \in \mathbb{N}$.

7. $\mathcal{U}(\mathbb{Z}_n) = \{[a] \in \mathbb{Z}_n \mid \mathrm{mcd}(a, n) = 1\}$ con el producto es un grupo abeliano, $\forall n \in \mathbb{N}$. También lo notaremos por $\mathbb{Z}_n^\times$.

8. Dado $n \geqslant 1$, consideramos:

   $$\mu_n = \{\text{raíces complejas de } x^n - 1\} = \left\{\xi_k = \cos\frac{2k\pi}{n} + i\,\mathrm{sen}\,\frac{2k\pi}{n} : k \in \{0, \ldots, n-1\}\right\}$$
   $$= \left\{1, \xi, \xi^2, \ldots, \xi^{n-1} : \xi = \cos\frac{2\pi}{n} + i\,\mathrm{sen}\,\frac{2\pi}{n}\right\}$$

   Este conjunto es un grupo abeliano con el producto heredado de $\mathbb{C}$.

9. Dado un cuerpo $\mathbb{K}$, el grupo lineal especial de orden 2 sobre dicho cuerpo:

   $$\mathrm{SL}_2(\mathbb{K}) = \{M \in \mathcal{M}_2(\mathbb{K}) : \det(M) = 1\}$$

   con el producto heredado de $\mathcal{M}_2(\mathbb{K})$ es un grupo que no es conmutativo.

10. Sean $(G, \square, e), (H, \triangle, f)$ dos grupos, si consideramos sobre $G \times H$ la operación binaria $* : (G \times H) \times (G \times H) \to G \times H$ dada por:

    $$(x, u) * (y, v) = (x \square y, u \triangle v) \qquad \forall (x, u), (y, v) \in G \times H$$

    Entonces, $G \times H$ es un grupo, al que llamaremos grupo directo de G y H.

11. Si X es un conjunto no vacío y consideramos

    $$S(X) = \{f : X \to X \mid f \text{ biyectiva}\} = \mathrm{Perm}(X)$$

    es un grupo no abeliano con la operación de composición de funciones $\circ$.

    En el caso en el que X sea finito y tenga n elementos: $X = \{x_1, x_2, \ldots, x_n\}$, notaremos:

    $$S_n = S(X)$$

[1] Será común hablar de "operación heredada" cuando consideramos un subconjunto de un conjunto en el que ya hay definida una operación interna, haciendo referencia a la restricción en dominio y recorrido de dicha operación interna al subconjunto considerado.

12. Sea $(G, *, e)$ un grupo y X un conjunto, consideramos el conjunto:

$$\mathrm{Apl}(X, G) = G^X = \{f : X \to G \mid f \text{ aplicación}\}$$

junto con la operación binaria $* : G^X \times G^X \to G^X$ dada por:

$$(f * g)(x) = f(x) * g(x) \qquad \forall x \in X, \quad \forall f, g \in G^X$$

Entonces, $(G^X, *, g)$ es un grupo, con elemento neutro:

$$g(x) = e \qquad \forall x \in X$$

de esta forma, dada $f \in G^X$, la aplicación simétrica de f será:

$$f'(x) = (f(x))' \qquad \forall x \in X$$

Casos a destacar son:

a) Si $X = \emptyset$, entonces $G^X = \{\emptyset\}$.

b) Si $X = \{1, 2\}$, entonces G^X se identifica con $G \times G$.

13. El grupo más pequeño que se puede considerar es el único grupo válido sobre un conjunto unitario $X = \{e\}$. Es decir, el grupo $(X, *, e)$ con $X = \{e\}$ y $* : X \times X \to X$ dada por:

$$e * e = e \qquad e \in X$$

A este grupo (independientemente de cual sea el conjunto X, ya que todos tendrán la misma[2] estructura) lo llamaremos grupo trivial.

Ejemplo. Consideramos en $\mathbb{Z}$ la operación binaria $* : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ dada por:

$$a * b = a + b + 1 \qquad \forall a, b \in \mathbb{Z}$$

Donde usamos $+$ para denotar la suma de $\mathbb{Z}$. Se pide demostrar que $(\mathbb{Z}, *)$ es un grupo abeliano.

Demostración. Demostramos cada una de las propiedades de la definición de grupo abeliano:

- La propiedad asociativa de $*$ es consecuencia de las propiedades asociativa y conmutativa de $+$:

$$\begin{aligned} (a * b) * c &= (a + b + 1) * c = a + b + 1 + c + 1 = a + b + c + 2 \\ a * (b * c) &= a * (b + c + 1) = a + b + c + 1 + 1 = a + b + c + 2 \\ &\forall a, b, c \in \mathbb{Z} \end{aligned}$$

[2]Concepto que luego formalizaremos.

- Buscamos $x \in \mathbb{Z}$ de forma que $x * a = a$ para todo $a \in \mathbb{Z}$, por lo que queremos resolver la ecuación:

$$X * a = a \iff X + a + 1 = a \implies X = -1$$

Por lo que $-1 \in \mathbb{Z}$ es el elemento neutro para $*$:

$$-1 * a = -1 + a + 1 = a \qquad \forall a \in \mathbb{Z}$$

- Fijado $x \in \mathbb{Z}$, tratamos de buscar un elemento simétrico para x, por lo que buscamos resolver la ecuación:

$$X * x = -1 \iff X + x + 1 = -1 \iff X = -x - 2$$

Por lo que dado $x \in \mathbb{Z}$, su elemento simétrico es $-x - 2 \in \mathbb{Z}$:

$$(-x - 2) * x = -x - 2 + x + 1 = -1 \qquad \forall x \in \mathbb{Z}$$

- La propiedad conmutativa de $*$ es consecuencia de la propiedad conmutativa de $+$:

$$a * b = a + b + 1 = b + a + 1 = b * a \qquad \forall a, b \in \mathbb{Z}$$

□

Propiedades

Aunque estas propiedades parezcan ya conocidas y familiares (por ejemplo para el caso $(\mathbb{Z}, +, 0)$), es una buena observación darnos cuenta de que son válidas para **cualquier grupo** que consideremos, por raros y difíciles que sean sus elementos y operación interna.

Proposición 1.2. *Sea $(G, *, e)$ un grupo, destacamos sus primeras propiedades:*

i) $x * x' = e \ \forall x \in G$.

ii) $x * e = x \ \forall x \in G$.

iii) *El elemento neutro de $*$ es único. Simbólicamente:*

$$\exists_1 e \in G \mid e * x = x \qquad \forall x \in G$$

iv) *Fijado $x \in G$, el simétrico de x es único. Simbólicamente:*

$$\forall x \in G \quad \exists_1 x' \in G \mid x' * x = e$$

Demostración. Demostramos cada una a partir de la anterior:

i) En primer lugar, observemos que:

$$x' * (x * x') = (x' * x) * x' = e * x' = x' \tag{1.1}$$

Ahora:

$$x * x' = e * (x * x') = \left((x')' * x'\right) * (x * x') = (x')' * (x' * (x * x')) \overset{(*)}{=} (x')' * x' = e$$

Donde en $(*)$ hemos usado (1.1).

ii) Usando *i*) en $(*)$:

$$x * e = x * (x' * x) = (x * x') * x \overset{(*)}{=} e * x = x$$

iii) Sea $f \in G$ de forma que $f * x = x \ \forall x \in G$, entonces:

$$f = f * e \overset{(*)}{=} e$$

Donde en $(*)$ hemos usado *ii*).

De otra forma, podríamos haber argumentado que gracias a *ii*), todo grupo es un monoide, por lo que podemos aplicar la Proposición 1.1 y ya habríamos terminado.

iv) Dado $x \in G$, sea $x'' \in G$ de forma que $x'' * x = e$, entonces:

$$x'' = x'' * e \overset{(*)}{=} x'' * (x * x') = (x'' * x) * x' = e * x' = x'$$

Donde en $(*)$ hemos usado *i*).

□

Notación. A partir de ahora, dado un grupo $(G, *, e)$, comenzaremos a usar (por comodidad) la notacion multiplicativa de los grupos:

$$xy = x * y \qquad \forall x, y \in G$$

Y denotando a x' (el elemento simétrico de x) por x^{-1}.

Proposición 1.3. *En un grupo G se verifica la propiedad cancelativa (tanto a la izquierda como a la derecha):*

$$\forall x, y, z \in G : \begin{cases} xy = xz \Longrightarrow y = z \\ xy = zy \Longrightarrow x = z \end{cases}$$

Demostración. Para la primera, supongamos que $xy = xz$:

$$y = ey = (x^{-1}x)y = x^{-1}(xy) = x^{-1}(xz) = (x^{-1}x)z = ez = z$$

Ahora, para la segunda, supongamos que $xy = zy$ y la demostración es la misma que la anterior pero en el otro sentido y tomando $e = yy^{-1}$.

$$x = xe = x(yy^{-1}) = (xy)y^{-1} = (zy)y^{-1} = z(yy^{-1}) = z$$

□

Proposición 1.4. *Sea G un grupo, entones:*

1. $e^{-1} = e$.
2. $(x^{-1})^{-1} = x$, $\forall x \in G$.
3. $(xy)^{-1} = y^{-1}x^{-1}$, $\forall x, y \in G$.

Demostración. Cada caso se demuestra observando sencillamante que:

1. $ee = e$.
2. $xx^{-1} = e$.
3. $(y^{-1}x^{-1})(xy) = y^{-1}x^{-1}xy = y^{-1}ey = e$.

□

Proposición 1.5. *Sea G un conjunto no vacío con una operación binaria $*$ asociativa, son equivalentes:*

i) G es un grupo.

ii) Para cada par de elementos $a, b \in G$, las ecuaciones[3]:

$$aX = b \qquad Xa = b$$

Tienen solución en G, es decir: $\exists c, d \in G \mid ac = b \wedge da = b$.

Demostración. Demostramos las dos implicaciones:

i) $\Rightarrow$ *ii)* Tomando $c = a^{-1}b, d = ba^{-1} \in G$ se tiene.

ii) $\Rightarrow$ *i)* Basta demostrar que $\exists e \in G$ con $ex = x \ \forall x \in G$ y que fijado $x \in G$, entonces $\exists x' \in G$ con $x'x = e$:

1. Dado $a \in G$, sabemos que la ecuación $Xa = a$ tiene solución, por lo que existe $e \in G$ de forma que $ea = a$.

   Veamos que no depende de la elección de a; es decir, que es un elemento neutro para cualquier elemento de G. Para ello, dado cualquier $b \in G$, sabemos que la ecuación $aX = b$ tiene solución, por lo que existirá un $x_b \in G$ de forma que $ax_b = b$. Finalmente:

   $$eb = e(ax_b) = (ea)x_b = ax_b = b \qquad \forall b \in G$$

2. Fijado $x \in G$, sabemos que la ecuación $Xx = e$ tiene solución, por lo que existe $x' \in G$ de forma que $x'x = e$, para cualquier $x \in G$.

□

Proposición 1.6 (Ley asociativa general)**.** *Sea G un grupo, dados $n, m \in \mathbb{N}$ con $n > m > 0$, se tiene que:*

$$\left(\prod_{i=1}^{m} x_i\right)\left(\prod_{i=m+1}^{n} x_i\right) = \prod_{i=1}^{n} x_i \qquad \forall x_i \in G, \quad i \in \{1, \ldots, n\}$$

Demostración. Por inducción sobre $n \in \mathbb{N}$:

- Para $n = 0, n = 1$: No hay nada que probar: $\nexists m \in \mathbb{N}$ con $0 < m < n$.

[3]Donde hemos usado X para denotar la incógnita y que no se confunda con un elemento de G.

- Para $n = 2$: Dado $m \in \mathbb{N}$ con $0 < m < n$ (entonces $m = 1$):

$$\left(\prod_{i=1}^{m} x_i\right)\left(\prod_{i=m+1}^{n} x_i\right) = x_1 x_2 = \prod_{i=1}^{n} x_i \qquad \forall x_1, x_2 \in G$$

- Supuesto para n, veámoslo para $n+1$: Dado $m \in \mathbb{N}$ con $0 < m < n+1$:

$$\begin{aligned}\left(\prod_{i=1}^{m} x_i\right)\left(\prod_{i=m+1}^{n+1} x_i\right) &= \left[x_1\left(\prod_{i=2}^{m} x_i\right)\right]\left[\left(\prod_{i=m+1}^{n} x_i\right) x_{n+1}\right] \\ &= x_1\left(\prod_{i=2}^{m} x_i \prod_{i=m+1}^{n} x_i\right) x_{n+1} \overset{(*)}{=} x_1\left(\prod_{i=2}^{n} x_i\right) x_{n+1} = \prod_{i=1}^{n+1} x_i \\ &\forall x_i \in G, \quad i \in \{1, \dots, n+1\}\end{aligned}$$

  Donde en $(*)$ hemos usado la hipótesis de inducción, ya que $0 < m - 1 < n$.

□

Definición 1.4 (Potencia)**.** Sea $(G, \cdot, e)$ un grupo, dado $x \in G$ y $n \in \mathbb{Z}$, podemos definir:

$$x^n = \begin{cases} \prod_{i=1}^{n} x & \text{si } n > 0 \\ e & \text{si } n = 0 \\ (x^{-1})^{-n} & \text{si } n < 0 \end{cases}$$

Proposición 1.7. *Sea G un grupo, se verifica que:*

$$x^{n+m} = x^n \cdot x^m \qquad \forall x \in G, \quad n, m \in \mathbb{Z}$$

Demostración. Aunque la demostración es sencilla, hemos de distinguir bastantes casos, pues hemos de asegurarnos de que el límite superior de cada producto sea siempre un número positivo. Fijado $x \in G$, distinguimos en función de los valores de $n, m \in \mathbb{Z}$:

1. $n > 0$:

   a) $m > 0$:

$$x^{n+m} = \prod_{i=1}^{n+m} x = \left(\prod_{i=1}^{n} x\right) \cdot \left(\prod_{i=n+1}^{n+m} x\right) = \left(\prod_{i=1}^{n} x\right) \cdot \left(\prod_{i=1}^{m} x\right) = x^n \cdot x^m$$

   b) $m = 0$:

$$x^{n+0} = x^n = x^n \cdot e = x^n \cdot x^0$$

   c) $m < 0$:

   En este caso, no sabemos el signo de $n+m$. Por tanto, hemos de distinguir casos:

   1) $n + m > 0$: Entonces, $n > -m$. Tenemos:

$$x^n \cdot x^m = \left(\prod_{i=1}^{n} x\right) \cdot (x^{-1})^{-m} = \left(\prod_{i=1}^{n} x\right) \cdot \left(\prod_{i=1}^{-m} x^{-1}\right) = \prod_{i=1}^{n-(-m)} x = \prod_{i=1}^{n+m} x = x^{n+m}$$

2) $\underline{n+m=0}$: Entonces, $n=-m$. Tenemos:

$$x^{n+m}=x^0=e=\left(\prod_{i=1}^{n}x\right)\cdot\left(\prod_{i=1}^{n}x^{-1}\right)=x^n\cdot\left(\prod_{i=1}^{-m}x^{-1}\right)=x^n\cdot\left(x^{-1}\right)^{-m}=x^n\cdot x^m$$

3) $\underline{n+m<0}$: Entonces, $n<-m$. Tenemos:

$$x^n\cdot x^m=\left(\prod_{i=1}^{n}x\right)\cdot\left(x^{-1}\right)^{-m}=\left(\prod_{i=1}^{n}x\right)\cdot\left(\prod_{i=1}^{-m}x^{-1}\right)=\prod_{i=1}^{-m-n}x^{-1}=$$
$$=\prod_{i=1}^{-(n+m)}x^{-1}=\left(x^{-1}\right)^{-(n+m)}=x^{n+m}$$

2. $\underline{n=0}$:

$$x^{0+m}=x^m=e\cdot x^m=x^0\cdot x^m$$

3. $\underline{n<0}$:

a) $\underline{m>0}$:

$$x^{n+m}=x^{m+n}=x^m\cdot x^n=\prod_{i=1}^{m}x\cdot\prod_{i=1}^{-n}x^{-1}=x^n\cdot x^m$$

donde en la primera igualdad hemos usado la propiedad conmutativa de la suma en $\mathbb{Z}$, en la segunda hemos empleado el caso anteriormente demostrado, y en la última igualdad hemos empleado que $xx^{-1}=e=x^{-1}x$.

b) $\underline{m=0}$:

$$x^{n+0}=x^n=x^n\cdot e=x^n\cdot x^0$$

c) $\underline{m<0}$:

$$x^n\cdot x^m=\left(x^{-1}\right)^{-n}\cdot\left(x^{-1}\right)^{-m}=\left(\prod_{i=1}^{-n}x^{-1}\right)\cdot\left(\prod_{i=-1}^{-m}x^{-1}\right)=$$
$$=\prod_{i=1}^{-n-m}x^{-1}=\left(x^{-1}\right)^{-(n+m)}=x^{n+m}$$

□

Definición 1.5 (Grupos finitos e infinitos)**.** Sea G un grupo, si G como conjunto tiene[4] $n\in\mathbb{N}\setminus\{0\}$ elementos, diremos que es un grupo finito. En dicho caso, diremos que n es el "orden del grupo", notado por: $|G|=n$.
Si G no fuera finito, decimos que es un grupo infinito.

Definición 1.6 (Tabla de Cayley)**.** En un grupo finito $G=\{x_1,x_2,\ldots,x_n\}$, se llama tabla de Cayley (o de multiplicar[5]) a la matriz $n\times n$ de forma que su entrada (i,j) es x_ix_j.

[4]Excluimos $n=0$ ya que en la definición de grupo exigimos que $G\neq\emptyset$.
[5]Entendiendo que en este caso hacemos uso de la notación multiplicativa.

Ejemplo. A continuación, mostramos ejemplos de posibles tablas de Cayley para ciertas operaciones sobre determinados grupos. Como podemos ver, la finalidad de la tabla es mostrar en cada caso cómo se comporta la operación binaria cuando se aplica a distintos elementos del grupo.

1. Si $G = \{0, 1\}$, podemos considerar sobre G las operaciones $*_1$ y $*_2$, cuya definición puede obtenerse a partir de sus tablas de Cayley:

$*_1$	0	1
0	0	1
1	1	0

$*_2$	0	1
0	1	0
1	0	1

2. Si $G = \{0, 1, 2\}$, podemos considerar sobre G la siguiente operación binaria:

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

3. Si $G = \{0, 1, 2, 3\}$, podemos considerar sobre G las siguientes operaciones binarias:

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

A partir de la definición de la tabla de Cayley para la operación binaria de un grupo pueden deducirse ciertas propiedades que estas tienen, las cuales no demostraremos, entendiendo que pueden deducirse de fórmula fácil a partir de la definición de grupo:

- Si consideramos un grupo abeliano, su tabla de Cayley será una matriz simétrica.
- Todos los elementos del grupo aparecen en todas las filas o columnas de la tabla de Cayley, ya que en la Proposición 1.5 vimos que las ecuaciones $aX = b$ y $Xa = b$ tenían que tener solución $\forall a, b \in G$, para que G fuese un grupo.
- Como para que G sea un grupo tiene que haber un elemento que actúe de neutro, esto se refleja en la tabla con un elemento que mantiene igual los encabezados en una fila y en una columna.

Definición 1.7 (Orden de un elemento)**.** Sea $(G, \cdot, 1)$ un grupo, el orden de un elemento $x \in G$ es el menor $n \in \mathbb{N} \setminus \{0\}$ (en caso de existir) que verifica: $x^n = 1$. En cuyo caso, notaremos[6]: $O(x) = \text{ord}(x) = n$.
Si para un elemento $x \in G$ dicho n no existe, se dice que su orden es infinito: $O(x) = +\infty$.

[6]Podremos encontrarnos cualquiera de las dos notaciones.

Proposición 1.8. *Sea G un grupo, $x \in G$ y sea $m \in \mathbb{N} \setminus \{0\}$ de forma que $x^m = 1$ con $O(x) = n$, entonces $n|m$.*

Demostración. Si $O(x) = n$, entonces no puede ser $m < n$, ya que si no el orden de x no sería n sino m, por lo que $m \geqslant n$. En cuyo caso, $\exists q, r \in \mathbb{N}$ de forma que:

$$m = nq + r \qquad \text{con } 0 \leqslant r < n$$

Pero entonces:

$$1 = x^m = x^{nq+r} = x^{nq}x^r = x^r \overset{(*)}{\Longrightarrow} r = 0$$

Donde en $(*)$ hemos usado que $r < n$, ya que si r no fuese 0, tendríamos que $O(x) = r$. □

Proposición 1.9. *Sea G un grupo, se verifica que:*

1. $O(x) = 1 \Longleftrightarrow x = 1$.
2. $O(x) = O(x^{-1})\ \forall x \in G$.

Demostración. Demostramos las dos propiedades:

1. Por doble implicación:

   $\Longleftarrow$) Trivial.

   $\Longrightarrow$) Si aplicamos la definición de $O(x)$ y de x^1:

   $$1 = x^1 = \prod_{i=1}^{1} x = x$$

2. Fijado $x \in G$ con $O(x) = n$, entonces $x^n = 1$, por lo que:

   $$x^{-1} = x^{n-1}$$

   Veamos en primer lugar que $O(x^{-1}) \leqslant n$. Para ello, vemos que $(x^{-1})^n = 1$:

   $$\left(x^{-1}\right)^n = \left(x^{n-1}\right)^n = x^{n(n-1)} = 1$$

   Veamos ahora que $O(x^{-1}) \geqslant n$. Supongamos ahora que $O(x^{-1}) = k$, entonces:

   $$(x^{-1})^k = 1 \Longrightarrow x^{(n-1)k} = 1 \Longrightarrow n \mid (n-1)k$$

   Por tanto, como $n \nmid (n-1)$ y $\text{mcd}(n, n-1) = 1$, entonces $n \mid k$, por lo que $n \leqslant k = O(x^{-1})$. Por tanto, tenemos que:

   $$n \leqslant O(x^{-1}) \leqslant n \Longrightarrow O(x^{-1}) = n$$

□

Ejemplo. Mostramos ahora ejemplos de órdenes de ciertos elementos en distintos grupos, entendiendo que cuando consideramos conjuntos susceptibles de ser anillos (conjuntos con suma y multiplicación), si dejamos el 0 en el conjunto consideramos el grupo con su suma ($e = 0$) y que cuando quitamos el 0 del conjunto consideramos el grupo con su multiplicación ($e = 1$).

1. Si cogemos $x \neq 1$ en $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ con la multiplicación: $O(x) = +\infty$.
2. Si consideramos $\mathbb{C}$ con su multiplicación: $O(i) = 4$, ya que $i^4 = 1$.
3. En $\mathbb{Z}_9$, $O\left(\overline{6}\right) = 3$:

$$\begin{gathered}\overline{6} \neq \overline{0} \\ \overline{6+6} = \overline{12} = \overline{3} \neq \overline{0} \\ \overline{6+6+6} = \overline{18} = \overline{0}\end{gathered}$$

4. En $\mathbb{Z}_7^* = \mathcal{U}(\mathbb{Z}_7)$:
   - $O\left(\overline{2}\right) = 3$:

$$\begin{gathered}\overline{2} \neq \overline{1} \\ \overline{2 \cdot 2} = \overline{4} \neq \overline{1} \\ \overline{2 \cdot 2 \cdot 2} = \overline{8} = \overline{1}\end{gathered}$$

   - $O\left(\overline{3}\right) = 6$.

$$\begin{gathered}\overline{3} \neq \overline{1} \\ \overline{3 \cdot 3} = \overline{9} = \overline{2} \neq \overline{1} \\ \overline{3 \cdot 3 \cdot 3} = \overline{27} = \overline{6} \neq \overline{1} \\ \overline{3 \cdot 3 \cdot 3 \cdot 3} = \overline{81} = \overline{3} \neq \overline{1} \\ \overline{3 \cdot 3 \cdot 3 \cdot 3 \cdot 3} = \overline{243} = \overline{5} \neq \overline{1} \\ \overline{3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3} = \overline{729} = \overline{1}\end{gathered}$$

1.1. Grupos diédricos D_n

A continuación, estaremos interesados en el estudio de una familia[7] de grupos conocida como los "grupos diédricos", cuyo estudio se desarrollará a lo largo de la asignatura.

1.1.1. Motivación

Para entender estos grupos, conviene destacar la forma en la que surgieron ciertos objetos geométricos que luego fueron interesantes desde el punto de vista algebraico, por formar un grupo.

[7]Donde con "familia" hacemos referencia a un conjunto de grupos que guardan cierta similitud entre ellos.

Ejemplo. Si pensamos en un triángulo rectángulo (el menor polígono regular) sobre el plano centrado en el origen como el de la Figura 1.1, donde hemos numerado los vértices del mismo, es interesante preguntarnos sobre las isometrías del plano en el plano que dejan invariante al mismo.

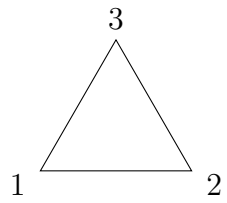


Figura 1.1: Triángulo equilátero con centro en el origen de coordenadas.

En Geometría II se vio que las únicas isometrías que podemos considerar en el plano son los giros y las simetrías axiales o centrales, por lo que procedemos a distinguir casos:

Giros. Como vemos en la Figura 1.2, de forma intuitiva vemos que giros (pensando que todos son en sentido antihorario) que dejan el triángulo invariante solo hay 3:

- El giro de ángulo $\frac{2\pi}{3}$.
- El giro de ángulo $\frac{4\pi}{3}$.
- El giro de ángulo 2π.

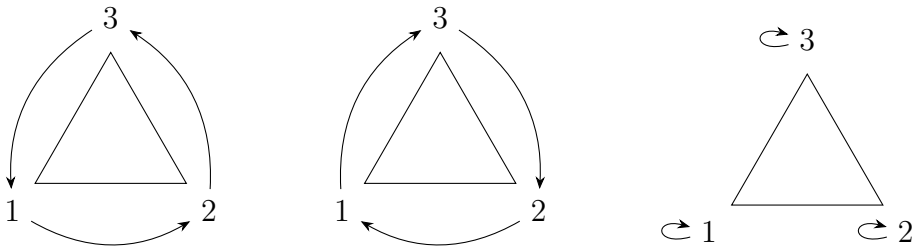


Figura 1.2: Todos los giros que dejan invariánte al triángulo.

Simetrías. Como vemos en la Figura 1.3, de forma intuitiva vemos que hay 3 simetrías axiales que dejan invariante al triángulo y que no hay ninguna simetría central que lo deje invariante:

- La simetría respecto a la mediatriz del segmento 2, 3.
- La simetría respecto a la mediatriz del segmento 3, 1.
- La simetría respecto a la mediatriz del segmento 1, 2.

Notemos la forma en la que hemos nombrado las rectas respecto a las cuales se hace la simetría: la recta l_i contiene al vértice i-ésimo.

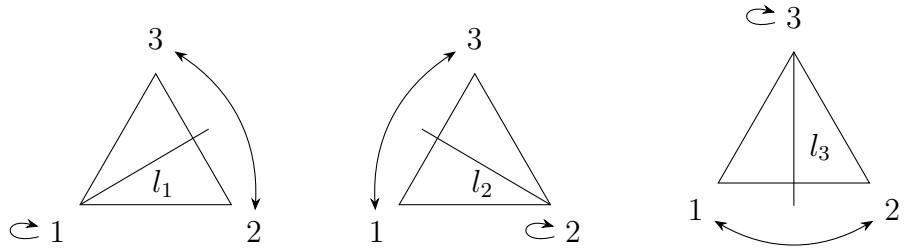


Figura 1.3: Todas las reflexiones que dejan invariante al triángulo.

Con el fin de estudiar las isometrías que mantienen polígonos regulares en el plano, conviene introducir las siguientes definiciones y notaciones:

Definición 1.8 (Permutación)**.** Sea X un conjunto, una permutación del mismo es cualquier aplicación biyectiva $f : X \to X$.

Si X es el conjunto $\{1, 2, \ldots, n\}$, es usual notar:

$$S_n = \text{Perm}(X) = \{f : X \to X \mid f \text{ es una permutación}\}$$

Definición 1.9 (Ciclo)**.** Sea $\{a_1, a_2, \ldots, a_m\} \subseteq \{1, 2, \ldots, n\}$, un ciclo de longitud $m \leqslant n$ es una permutación $\sigma \in S_n$ de forma que:

1. $\sigma(a_i) = a_{i+1}$ para todo $i \in \{1, \ldots, m-1\}$.
2. $\sigma(a_m) = a_1$.
3. $\sigma(a_j) = a_j$ para todo $a_j \notin \{a_1, a_2, \ldots, a_m\}$.

En dicho caso, representaremos a σ por:

$$\sigma = (a_1\ a_2\ \ldots\ a_m)$$

Observación. Notemos que podemos notar a un ciclo de longitud m, σ, de m formas distintas:

$$\sigma = (a_1\ a_2\ \ldots\ a_m) = (a_2\ \ldots\ a_m\ a_1) = \ldots = (a_m\ \ldots\ a_1\ a_2)$$

De esta forma, el número de ciclos de longitud m son todas las posibles combinaciones de los m elementos entre n, pero como cada vez aparecen m:

$$\frac{V_m^n}{m}$$

A los 2−ciclos los llamaremos transposiciones.

Ejemplo. Para familiarizarnos con los ciclos, observamos que:

- En S_3, los ciclos de longitud 2 que podemos considerar son: (1 2), (1 3) y (2 3). Estos se interpretan respectivamente como:
  - Mantener el 3 fijo e intercambiar el 1 con el 2.

  - Mantener el 2 fijo e intercambiar el 1 con el 3.
  - Mantener el 1 fijo e intercambiar el 2 con el 3.

- En S_3, los únicos ciclos de longitud 3 que podemos considerar son: (1 2 3) y (3 2 1), cuya definición debe estar clara.

Notación. Es claro que no toda permutación es un ciclo, basta considerar la aplicación identidad. Sin embargo, hay ciertas permutaciones como por ejemplo la aplicación $\sigma : \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$ dada por:

$$\begin{aligned}\sigma(1) &= 2\\ \sigma(2) &= 1\\ \sigma(3) &= 4\\ \sigma(4) &= 3\end{aligned}$$

Que restringida a $\{1, 2\}$ da el ciclo (1 2) y que restringida al $\{3, 4\}$ da el ciclo (3 4). Será usual denotar permutaciones como esta por[8]:

$$\sigma = (1\ 2)(3\ 4)$$

Aprovechando la notación para los ciclos previamente definida, si por ejemplo extendemos σ a $\{1, 2, 3, 4, 5\}$ definiendo:

$$\sigma(5) = 5$$

Entonces, la notación para σ será la misma: (1 2)(3 4), ya que el 5 "no se mueve".

Ejemplo. Volviendo al ejemplo anterior del triángulo y de las isometrías que lo dejan invariante, si notamos por:

- r al giro de ángulo $\frac{2\pi}{3}$.
- s a la simetría axial cuya recta pasa por el vértice 1.

Puede comprobarse de forma geométrica que a partir de composiciones de r y de s obtenemos los otros 4 movimientos restantes (notaremos la composición de aplicaciones por yuxtaposición, ya que estamos buscando un grupo con estas aplicaciones):

- El giro de ángulo $\frac{4\pi}{3}$ es $r^2 = rr$.
- El giro de ángulo 2π es r^3.
- La simetría respecto a la recta l_2 es sr^2.
- La simetría respecto a la recta l_3 es sr.

[8]Más adelante formalizaremos bien esta notación, aunque por ahora empecemos a usarla desde un punto de vista más intuitivo.

Notemos que el giro de ángulo 2π es la identidad, que es el elemento neutro para la composición, por lo que el elemento neutro del futuro grupo que definamos será r^3, que podemos denotar por 1. Además, la composición de aplicaciones es una operación asociativa y se deja como ejercicio demostrar que cada elemento del conjunto:

$$D_3 = \{1, r, r^2, s, sr, sr^2\}$$

Tiene un elemento simétrico respecto de la composición. Podemos ver que $(D_3, \circ, 1)$ es un grupo.

Ejemplo. Continuando con la motivación para los grupos diédricos, nos preguntamos ahora qué pasa si en vez de considerar las isometrías que mantienen invariante a un triángulo equilátero, consideramos las isometrías del plano que mantienen invariantes los vértices de un cuadrado sobre el plano; un cuadrado como el de la Figura 1.4.

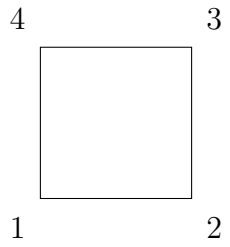


Figura 1.4: Cuadrado con centro en el origen de coordenadas.

Es fácil ver que las únicas isometrías que dejan invariante al cuadrado son (Véase la Figura 1.5):

- Los giros de ángulos $\frac{\pi}{2}$, π, $\frac{3\pi}{2}$ y 2π.
- Las simetrías axiales respecto a las rectas:
  - La recta que une los vértices 1 y 3.
  - La recta que une los vértices 2 y 4.
  - La recta que es mediatriz del segmento 1, 2.
  - La recta que es mediatriz del segmento 2, 3.

Todos estos movimientos pueden verse como aplicaciones lineales $f : \mathbb{R}^2 \to \mathbb{R}^2$ tal y como se hace en geometría o aprovecharnos de que todas ellas mantienen el cuadrado invariante, por lo que podemos pensar en ellas como si fueran permutaciones del conjunto $\{1, 2, 3, 4\}$. Aprovechando esta dualidad, vemos que:

- El giro de ángulo $\frac{\pi}{2}$ es (1 2 3 4).
- El giro de ángulo π es (1 3)(2 4).
- El giro de ángulo $\frac{3\pi}{2}$ es (1 4 3 2).
- El giro de ángulo 2π es la identidad, (1).

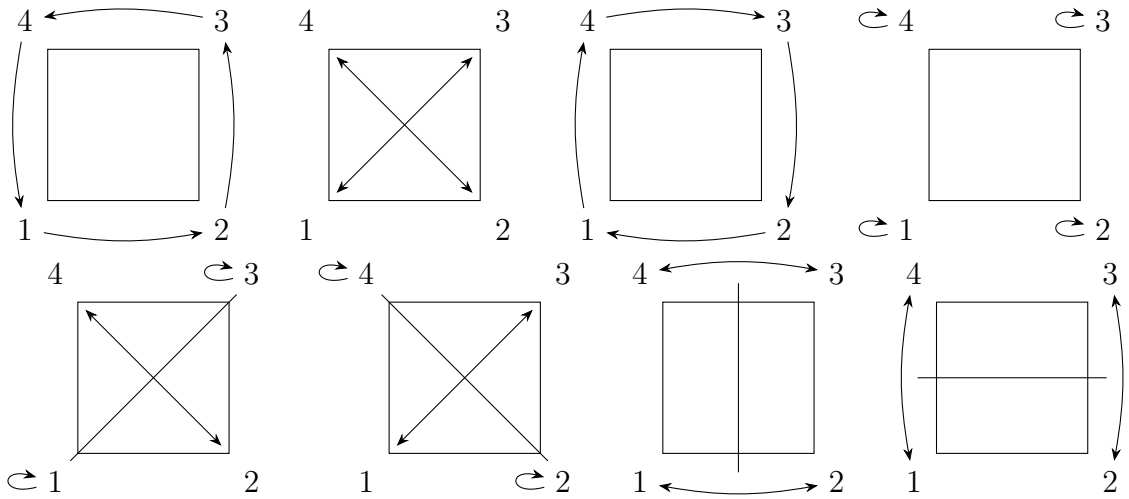


Figura 1.5: Giros y simetrías que dejan invariante al cuadrado

- La simetría respecto a la recta que une 1 y 3 es (2 4).
- La simetría respecto a la recta que une 2 y 4 es (1 3).
- La simetría respecto a la mediatriz de 1 y 2 es (1 2)(3 4).
- La simetría respecto a la mediatriz de 2 y 3 es (1 4)(2 3).

Dejamos como ejercicio hacer esta correspondencia (notar las isometrías como su correspondiente permutación) con los movimientos que teníamos en el triángulo. Si ahora hacemos como hicimos anteriormente con el triángulo y notamos por:

- r al giro de ángulo $\frac{\pi}{2}$.
- s a la reflexión respecto a la recta que pasa por el vértice 1.

Podemos obtener los otros 6 movimientos (o permutaciones desde el punto de vista algebráico) con la composición de r y s:

- r^2 es (1 3)(2 4).
- r^3 es (1 4 3 2).
- r^4 es 1 (la aplicación identidad).
- sr es (1 2)(3 4).
- sr^2 es (1 3).
- sr^3 es (1 4)(2 3).

De esta forma, si consideramos el conjunto:

$$D_4 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$$

Tenemos que $(D_4, \circ, 1)$ es un grupo. Más aún, podemos completar su tabla de Cayley para observar cómo se comporta $\circ$ dentro de D_4:

$\circ$	1	r	r^2	r^3	s	sr	sr^2	sr^3
1	1	r	r^2	r^3	s	sr	sr^2	sr^3
r	r	r^2	r^3	1	sr^3	s	sr	sr^2
r^2	r^2	r^3	1	r	sr^2	sr^3	s	sr
r^3	r^3	1	r	r^2	sr	sr^2	sr^3	s
s	s	sr	sr^2	sr^3	1	r	r^2	r^3
sr	sr	sr^2	sr^3	s	r^3	1	r	r^2
sr^2	sr^2	sr^3	s	sr	r^2	r^3	1	r
sr^3	sr^3	s	sr	sr^2	r	r^2	r^3	1

1.1.2. Definición y primeras propiedades

Una vez comprendida la motivación de los grupos diédricos, estamos preparados para dar su definición. No demostraremos que, dado $n \in \mathbb{N}$, el conjunto de isometrías que dejan invariante al polígono regular de n lados forma un grupo si consideramos sobre dicho conjunto la composición de aplicaciones, ya que no es interesante para esta asignatura.

Sin embargo, aceptaremos la definición como válida (animamos al lector a investigar más sobre los grupos diédricos y su definición) y procedemos a destacar las propiedades algebraicas de estos grupos, que es lo que nos interesa.

Definición 1.10 (Grupos diédricos D_n)**.** Sea D_n el conjunto de isometrías que dejan invariante al polígono regular de n lados. Sabemos que D_n tiene $2n$ elementos:

- n rotaciones de ángulo $\frac{2k\pi}{n}$, con $k \in \{1, \dots, n\}$.
- n simetrías axiales:
  - Si n es par, tenemos:
    - $n/2$ simetrías respecto a las mediatrices.
    - $n/2$ simetrías respecto a unir vértices opuestos.
  - Si n es impar, tenemos n simetrías respecto a las mediatrices.

Se verifica que $(D_n, \circ, 1)$ es un grupo. Además, destacamos dos elementos suyos:

- r, la rotación de ángulo $\frac{2\pi}{n}$.
- s, la simetría axial respecto a la recta que pasa por el origen de coordenadas y el vértice nombrado 1.

De esta forma, todos los elementos de D_n son:

$$D_n = \left\{1, r, r^2, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\right\}$$

Proposición 1.10. *Dado $n \in \mathbb{N}$, en D_n se cumple que:*

1. *$1, r, r^2, \dots, r^{n-1}$ son todos distintos y $r^n = 1$, es decir, $O(r) = n$.*

2. $s^2 = 1$.
3. $s \neq r^i$, $\forall\ 0 \leqslant i \leqslant n-1$.
4. sr^i *con* $0 \leqslant i \leqslant n-1$ *son simetrías.*
5. $sr^i \neq sr^j$ *para todo* $i \neq j$, *con* $i, j \in \{1, \ldots, n-1\}$.
6. $sr = r^{-1}s$.
7. $sr^i = r^{-i}s$.

Demostración. Demostramos cada una de las propiedades:

1. La primera parte es compentencia de Geometría. Para la segunda, basta ver que r^n es componer n veces el giro de ángulo $\frac{2\pi}{n}$, que es lo mismo que considerar el giro de ángulo $n \cdot \frac{2\pi}{n} = 2\pi$, que es la identidad.
2. Es competencia de Geometría.
3. Es competencia de Geometría, que puede probarse de distintas formas:
   - Viendo que s tiene puntos fijos y r^i no.
   - Viendo que s es un movimiento inverso y que r^i es directo.
4. Es competencia de Geometría.
5. Basta aplicar 1.

6, 7. Son competencia de Geometría.

□

Usaremos los resultados de la Proposición 1.10 con frecuencia, como las propiedades básicas de los grupos diédricos. Notemos que a partir de estas puede construirse la tabla de Cayley para cualquier grupo diédrico D_n.

Ejercicio. Construya la tabla de Cayley para D_4 y D_5 usando los resultados de la Proposición 1.10.

1.2. Generadores de un grupo

Definición 1.11 (Conjunto de generadores de un grupo)**.** Sea G un grupo, diremos que $S \subseteq G$ es un conjunto de generadores de G si todo elemento $x \in G$ puede escribirse como producto finito de elementos de S y de sus inversos. En dicho caso, notaremos: $G = \langle S \rangle$.
Si S es un conjunto finito, $S = \{x_1, x_2, \ldots, x_n\} \subseteq G$, podemos escribir:

$$G = \langle x_1, x_2, \ldots, x_n \rangle$$

Si S está formado solo por un elemento, diremos que G es un grupo cíclico.

Observación. Sea G un grupo y $S \subseteq G$, equivalen:

i) S es un conjunto de generadores de G.

ii) Dado $x \in G$, $\exists x_1, x_2, \ldots, x_p \in S$ de forma que:

$$x = x_1^{\gamma_1} x_2^{\gamma_2} \ldots x_p^{\gamma_p} \qquad \gamma_i \in \mathbb{Z}, \quad i \in \{1, \ldots, p\}$$

Ejemplo. Como ejemplos a destacar, vemos que:

1. $\mathbb{Z} = \langle 1 \rangle$ si pensamos en $(\mathbb{Z}, +, 0)$, ya que dado $x \in \mathbb{Z}$:
   - Si $x > 0$, entonces:
   $$x = \underbrace{1 + 1 + \ldots + 1}_{x \text{ veces}}$$
   - Si $x < 0$, entonces (-1 es el simétrico de 1):
   $$x = \underbrace{-1 - 1 - \ldots - 1}_{x \text{ veces}}$$
   - Si $x = 0$, consideramos la suma de 0 elementos.
2. $D_n = \langle r, s \rangle$.

Definición 1.12 (Presentación de un grupo)**.** Sea G un grupo y $S \subseteq G$, si $G = \langle S \rangle$ y existe un conjunto de relaciones $R_1, R_2, \ldots, R_m$ (igualdades entre elementos de S, $\{1\}$ y los elementos simétricos de S) tal que cualquier relación entre los elementos de S puede deducirse de estas, entonces, decimos que estos generadores y relaciones constituyen una presentación de G, notado:

$$G = \langle S \mid R_1, R_2, \ldots, R_n \rangle$$

Ejemplo. Veamos algunos ejemplos de presentaciones, observando que dar una presentación es equivalente a dar la definición del propio grupo, ya que a partir de la presentación pueden deducirse todos los elementos del grupo y las relaciones que estos guardan entre sí.

1. En el diédrico D_n, tenemos que:
   $$D_n = \langle r, s \mid rs = sr^{-1}, r^n = 1, s^2 = 1 \rangle$$
2. $D_1 := \langle s \mid s^2 = 1 \rangle$.
   En este caso, vemos que $D_1 = \{s\}$.
3. $D_2 := \langle r, s \mid r^2 = s^2 = 1, sr = rs \rangle$.
   Ahora, tenemos: $D_2 = \{1, r, s, rs\}$.
4. $C_n = \langle x \mid x^n = 1 \rangle$ es un grupo cíclico de orden n.
   Vemos que: $C_n = \{1, x, x^2, x^3, \ldots, x^{n-1}\}$

5. $V^{\text{abs}} = \langle x, y \mid x^2 = 1, y^2 = 1, (xy)^2 = 1 \rangle$ es el grupo de Klein abstracto.

   En primer lugar, sabemos que $\{1, x, y\} \subseteq V^{\text{abs}}$. Como x e y son de orden 2, sabemos que $x^{-1} = x$ y que $y^{-1} = y$. Además, vemos que $xy \in V^{\text{abas}}$ y que:

   $$(xy)^2 = 1 \iff xyxy = 1 \iff xy = yx$$

   Por lo que xy también está en V^{abs}, con $(xy)^{-1} = yx$. Vemos que no hay más elementos que puedan estar en V^{abs}, con lo que:

   $$V^{\text{abs}} = \{1, x, y, xy\}$$

   Observamos que el grupo nos recuerda a D_2.

6. $Q_2^{\text{abs}} = \langle x, y \mid x^4 = 1, y^2 = x^2, yxy^{-1} = x^{-1} \rangle$.

   Inicialmente, $\{1, x, y\} \subseteq Q_2^{\text{abs}}$. De la primera relación vemos que también tenemos $\{x^2, x^3\} \subseteq Q_2^{\text{abs}}$. Reescribimos la última relación, para buscar más elementos de forma cómoda:

   $$yxy^{-1} = x^{-1} \iff yx = x^{-1}y$$

   Como yx no guarda ninguna relación con x e y, sabemos que también está en el grupo, junto con yx^2 y yx^3. De esta forma:

   $$Q_2^{\text{abs}} = \{1, x, x^2, x^3, y, yx, yx^2, yx^3\}$$

   Observamos también que el grupo nos recuerda a D_4.

Ejemplo. Las similitudes que hemos encontrado entre distintos grupos como entre V^{abs} y D_2 o entre Q_2^{abs} y D_4 las formalizaremos con ayuda de un concepto algebraico que luego definiremos, pero merece la pena destacar ahora una similaritud entre Q_2^{abs}, el grupo de los cuaternios $Q_2 = \{\pm 1, \pm i, \pm j, \pm k\}$ y unos elementos del grupo $\mathrm{SL}_2(\mathbb{C})$. Para familiarizarnos con los cuaternios, estos cumplen que:

$$i^2 = j^2 = k^2 = -1$$

$$\begin{array}{ccc} ij = k & jk = i & ki = j \\ ji = -k & kj = -i & ik = -j \end{array}$$

Productos que pueden recordarse observando la Figura 1.6

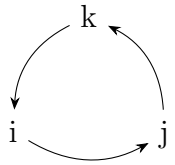


Figura 1.6: Dirección en la que se multiplican los cuaternios de forma positiva.

Se deja como ejercicio ver en qué forma podemos entender que los grupos Q_2, Q_2^{abs} y el subconjunto de matrices de $\mathrm{SL}_2(\mathbb{C})$ con la operación heredada del mismo:

$$C = \left\{ \begin{array}{cccc} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, & \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, & \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, & \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \\ \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, & \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}, & \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, & \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \end{array} \right\} \subseteq \mathrm{SL}_2(\mathbb{C})$$

Si pensamos en relacionar los elementos de la Tabla 1.1.

Q_2^{abs}	C	Q_2
1	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	1
x	$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$	i
y	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	j
x^2	$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$	-1
x^3	$\begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$	$-i$
xy	$\begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$	k
x^2y	$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$	$-j$
x^3y	$\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$	$-k$

Tabla 1.1: Elementos que se relacionan.

1.3. Grupos Simétricos S_n

Recordamos que dado un conjunto X, podemos considerar el conjunto de todas sus permutaciones:

$$S(X) = \{f : X \to X \mid f \text{ biyectiva}\}$$

Definición 1.13 (Grupos Simétricos S_n)**.** Dado $n \in \mathbb{N}$, consideramos $X = \{1, 2, \ldots, n\}$ y definimos $S_n = S(X)$, el conjunto de todas las permutaciones de X. Se verifica que S_n junto con la operación de composición de aplicaciones es un grupo:

- La composición de aplicaciones es asociativa.
- La aplicación $id : X \to X$ es el elemento neutro.
- Como las permutaciones son biyecciones, cada una tiene su elemento simétrico.

Llamaremos a $(S_n, \circ, id)$ el $n-$ésimo grupo simétrico, que recordamos tiene orden:

$$|S_n| = n!$$

Notación. Estaremos interesados en ver cómo se comportan de forma algebraica las permutaciones de conjuntos de n elementos, por lo que tendremos que conocer en cada caso cuáles son las aplicaciones con las que estamos trabajando.

Para abreviar, en muchos casos usaremos la notación matricial de las permutaciones. Sea $\sigma \in S_n$, sabemos que dar σ es equivalente a dar $\sigma(a)$ para cualquier $a \in X$. De esta forma, podemos dar una matriz $2 \times n$ de la forma:

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$$

Observemos que, conocida la matriz anterior, conocemos σ.

Ejemplo. En este ejemplo, vemos los grupos simétricos más pequeños:

1. Si consideramos S_0, son todas las permutaciones del $\emptyset$ en el $\emptyset$, que solo hay una: $\sigma : \emptyset \to \emptyset$.

2. Si consideramos S_1, solo hay una permutación: $id : \{1\} \to \{1\}$.

3. En S_2, tenemos $S_2 = \{\sigma_1, \sigma_2\}$, con:

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

   Hasta ahora, todos estos grupos son abelianos.

4. En S_3, tenemos:

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$$

   Que ya es un ejemplo de grupo simétrico no abeliano, ya que si tomamos:

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

   Vemos que $\sigma\tau \neq \tau\sigma$:

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

   De esta forma, acabamos de probar que S_n con $n \geqslant 3$ no es abeliano, ya que si estamos en S_n, podemos considerar las extensiones de σ y τ a S_n:

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

   Y tendremos que $\sigma\tau \neq \tau\sigma$.

Ejemplo. Sean $s_1, s_2 \in S_7$ dadas por:

$$s_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 6 & 2 & 1 & 4 & 3 \end{pmatrix}, \quad s_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 4 & 5 & 1 & 7 & 6 \end{pmatrix}$$

Se pide calcular s_1s_2, s_2s_1 y s_2^2.

$$s_1s_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 6 & 7 & 2 & 3 & 5 & 4 \end{pmatrix}$$

$$s_2s_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 7 & 2 & 1 & 5 & 3 & 4 \end{pmatrix}$$

$$s_2^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 4 & 7 & 5 & 2 & 6 \end{pmatrix}$$

Proposición 1.11. *Se verifica que:*

1. *Dado $\sigma \in S_n$ y $x \in \{1, 2, \ldots, n\}$, existe $m \in \mathbb{N}$ de forma que $\sigma^{m+1}(x) = x$.*
2. *Todo ciclo es una permutación.*
3. *El orden de un ciclo de longitud m es m.*
4. *Si $\sigma = (a_1\ a_2\ \ldots\ a_{m-1}\ a_m)$, entonces: $\sigma^{-1} = (a_m\ a_{m-1}\ \ldots\ a_2\ a_1)$.*

Con el siguiente teorema veremos que los ciclos son una parte interesante de los grupos simétricos, tanto que cualquier permutación pueda expresarse como una composición de ciertos ciclos de longitud mayor o igual que 2. Para ello, será necesario primero realizar una definición:

Definición 1.14 (Ciclos disjuntos)**.** Sean $\sigma_1, \sigma_2 \in S_n$ ciclos, decimos que son disjuntos si no existe $i \in X = \{1, 2, \ldots, n\}$ de forma que:

$$\sigma_1(i) = j, \quad \sigma_2(i) = k \quad \text{con } j, k \in X, i \neq j \neq k \neq i$$

Es decir, si no hay ningún elemento que se mueva en ambos ciclos.

Ejemplo. Ejemplos de ciclos disjuntos son:

$$\sigma_1 = (1\ 3\ 5), \quad \sigma_2 = (2\ 4\ 6), \quad \sigma_3 = (7\ 8)$$

Un ejemplo de dos ciclos que no son disjuntos son:

$$\tau_1 = (1\ 3\ 5\ 8), \quad \tau_2 = (2\ 4\ 5\ 9)$$

Ya que $\tau_1(5) = 8$ y $\tau_2(5) = 9$, con $5 \neq 8 \neq 9 \neq 5$. Es decir, el 5 se mueve en ambos ciclos.

Teorema 1.12. *Toda permutación $\sigma \in S_n$ con $\sigma \neq 1$ se expresa en la forma:*

$$\sigma = \gamma_1 \gamma_2 \ldots \gamma_k$$

siendo los γ_i con $i \in \{1, \ldots, k\}$ ciclos disjuntos de longitud mayor o igual que 2. Además, dicha descomposición es única, salvo el orden de los factores.

Demostración. Supuesto que estamos trabajando con permutaciones sobre el conjunto $X = \{1, 2, \ldots, n\}$, sea $\sigma \in S_n$ con $\sigma \neq 1$, definimos la relación:

$$yRx \iff \exists m \in \mathbb{Z} \mid y = \sigma^m(x)$$

Que es una relación de equivalencia:

- Propiedad reflexiva. Se tiene gracias a la Proposición 1.11.
- Propiedad simétrica. Sean $x, y \in X$ de forma que yRx, tenemos que $\exists m \in \mathbb{Z}$ de forma que $y = \sigma^m(x)$, pero entonces:

$$\sigma^{-m}(y) = \sigma^{-m}(\sigma^m(x)) = x \Longrightarrow xRy$$

- Propiedad transitiva. Sean $x, y, z \in X$ de forma que yRx y que zRx, entonces: $\exists p, q \in \mathbb{Z}$ de forma que:

$$\left.\begin{array}{l} y = \sigma^p(x) \\ z = \sigma^q(y) \end{array}\right\} \Longrightarrow z = \sigma^q(\sigma^p(x)) = \sigma^{p+q}(x) \Longrightarrow zRx$$

De esta forma, dado $x \in X$, podemos considerar su clase de equivalencia:

$$\overline{x} = \{\sigma^m(x) \mid m \in \mathbb{Z}\} \in X/R$$

Que es un conjunto finito, ya que gracias a la Proposición 1.11, existe $m \in \mathbb{N}$ de forma que $\sigma^{m+1}(x) = x$, con lo que:

$$C_x = \overline{x} = \{x, \sigma(x), \sigma^2(x), \ldots, \sigma^m(x)\}$$

Si consideramos ahora el ciclo:

$$\gamma_x = (x\ \sigma(x)\ \sigma^2(x)\ \cdots\ \sigma^m(x)) \in S_n$$

Tenemos que:

$$\gamma_x(y) = \begin{cases} \sigma(y) & \text{si } y \in C_x \\ y & \text{si } y \notin C_x \end{cases}$$

De esta forma, tenemos una partición de X en clases de equivalencia, cada una de las C_x con $x \in X$, que llevan asociado un ciclo γ_x.

1. Sean $\overline{i}, \overline{j} \in X/R$ con $\overline{i} \neq \overline{j}$, entonces los elementos que se mueven en γ_i son los elementos de C_i, mientras los elementos que se mueven en γ_j son los de C_j. Como se tiene que $C_i \cap C_j = \emptyset$ por ser C_i y C_j clases de equivalencia distintas, llegamos a que γ_i y γ_j son ciclos disjuntos, para $\overline{i} \neq \overline{j}$.

2. Sea $\tau = \gamma_1\gamma_2 \ldots \gamma_n$, sea $y \in X$, entonces:

   $$\tau(y) = \gamma_1\gamma_2 \ldots \gamma_n(y) = \gamma_1\gamma_2 \ldots \gamma_y(y) = \gamma_1\gamma_2 \ldots \gamma_{y-1}(\sigma(y)) = \gamma_1(\sigma(y)) = \sigma(y)$$

   Ya que anteriormente vimos que:

   $$\gamma_j(y) = \begin{cases} \sigma(y) & \text{si } y \in C_j \\ y & \text{si } y \notin C_j \end{cases} \qquad \forall j \in X$$

   Y se verifica que $y, \sigma(y) \in C_y$. Por tanto, tenemos que $\tau = \sigma$. Si ahora despreciamos de la expresión de τ los ciclos de longitud menor que 2, la permutación σ no cambia y tenemos que σ se expresa como producto de ciclos disjuntos (por el apartado 1) de longitud mayor o igual que 2.

□

Notación. A partir del Teorema 1.12, podemos introducir una nueva notación basada en los ciclos disjuntos. Dado $\sigma \in S_n$, como existe una única descomposición en ciclos disjuntos:

$$\sigma = \gamma_1\gamma_2 \ldots \gamma_k$$

Teníamos una notación estandar para cada ciclo. Ahora podemos notar σ como el producto de todas esas notaciones.

Ejemplo. En S_{13}, consideramos:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 12 & 13 & 3 & 1 & 11 & 9 & 5 & 10 & 6 & 4 & 7 & 8 & 2 \end{pmatrix}$$

De forma por ciclos disjuntos, podemos notar:

$$\sigma = (1\ 12\ 8\ 10\ 4)(2\ 13)(5\ 11\ 7)(6\ 9)$$

Dada una permutacion en notación de ciclos disjuntos, para calcular la permutación inversa basta calcular la inversa de cada uno de los ciclos:

$$\sigma^{-1} = (4\ 10\ 8\ 12\ 1)(2\ 13)(5\ 11\ 7)(6\ 9)$$

Del Teorema 1.12 deducimos los siguientes corolarios:

Corolario 1.12.1. *Para σ un ciclo, su orden coincide con su longitud.*

$$O(\sigma) = l(\sigma)$$

Corolario 1.12.2. *El orden de una permutación $\sigma \in S_n$ es el mínimo común múltiplo de las longitudes de los ciclos disjuntos en los que se descompone.*

Demostración. Supongamos que σ se descompone de la forma:

$$\sigma = \gamma_1\gamma_2 \dots \gamma_k$$

como $\gamma_i\gamma_j = \gamma_j\gamma_i$ para $i, j \in \{1, \dots, k\}$, tenemos que $\forall m \in \mathbb{N}$:

$$\sigma^m = \gamma_1^m\gamma_2^m \dots \gamma_k^m$$

Si $m = O(\sigma)$, entonces:

$$\sigma^m = 1 \iff \gamma_i^m = 1 \overset{(*)}{\Longrightarrow} O(\gamma_i)|m \quad \forall i \in \{1, \dots, k\}$$

Donde en $(*)$ hemos usado la Proposición 1.8. Concluimos que m es el mínimo común múltiplo de los órdenes de los ciclos, que por el Corolario 1.12.1, coincide con el mínimo común múltiplo de las longitudes de los ciclos. □

Ejemplo. Para familizarnos con la notación de permutaciones por ciclos disjuntos, vamos a enumerar todos los elementos de S_n para $n = 2, 3, 4$:

1. Para $n = 2$, tenemos $X = \{1, 2\}$ y por tanto:

$$S_2 = \{id, (1\ 2)\}$$

2. Para $n = 3$, tenemos $X = \{1, 2, 3\}$ y:

$$S_3 = \{id, (1\ 2\ 3), (1\ 3\ 2), (1\ 2), (1\ 3), (2, 3)\}$$

3. Para $n = 4$, tenemos $X = \{1, 2, 3, 4\}$ y:

$$\begin{aligned} S_4 = \{&id, (1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4), (1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), \\ &(1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3), (1\ 2\ 3\ 4), (1\ 3\ 2\ 4), (1\ 2\ 4\ 3), \\ &(1\ 3\ 2\ 4), (1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \end{aligned}$$

Definición 1.15. Sean $\alpha, \gamma \in S_n$, decimos que son conjugados si $\exists \tau \in S_n$ de forma que $\alpha = \tau\gamma\tau^{-1}$.

Proposición 1.13. *Si $\gamma \in S_n$ es un ciclo de longitud m, también lo será cualquier conjugado suyo. Es decir, si $\tau \in S_n$ y γ es un ciclo, entonces $\tau\gamma\tau^{-1}$ es un ciclo de longitud m.*

Demostración. Si $\gamma = (x_1\ x_2\ \dots\ x_m)$, sea $\tau \in S_n$, entonces veamos que:

$$\alpha = \tau\gamma\tau^{-1} = (\tau(x_1)\ \tau(x_2)\ \dots\ \tau(x_m))$$

Luego α será un ciclo de longitud m. Para ello, sea $y \in \{1, \dots, n\}$:

- Si $\tau^{-1}(y) = x_i \Longrightarrow y = \tau(x_i)$ con $i \in \{1, \dots, m-1\}$:

$$y \overset{\tau^{-1}}{\longmapsto} x_i \overset{\gamma}{\longmapsto} x_{i+1} \overset{\tau}{\longmapsto} \tau(x_{i+1}) = \alpha(\tau(x_i))$$

- Si $\tau^{-1}(y) = x_m \Longrightarrow y = \tau(x_m)$:

$$y \overset{\tau^{-1}}{\longmapsto} x_m \overset{\gamma}{\longmapsto} x_1 \overset{\tau}{\longmapsto} \tau(x_1) = \alpha(\tau(x_m))$$

- Si $\tau^{-1}(y) = x \Longrightarrow y = \tau(x)$ con $x \neq x_i$ para todo $i \in \{1, \dots, m\}$:

$$y \overset{\tau^{-1}}{\longmapsto} x \overset{\gamma}{\longmapsto} x \overset{\tau}{\longmapsto} \tau(x) = \alpha(\tau(x))$$

Concluimos que $\alpha = (\tau(x_1)\ \tau(x_2)\ \dots\ \tau(x_m))$. □

Ejemplo. Veamos la última Proposición en un caso práctico. Si consideramos:

$$\tau = (1\ 3\ 4), \quad \gamma = (2\ 4\ 5\ 3), \quad \tau^{-1} = (4\ 3\ 1)$$

Y tratamos de estudiar la imagen de $X = \{1, 2, 3, 4, 5\}$ bajo $\alpha = \tau\gamma\tau^{-1}$:

$$\begin{aligned}
1 &\overset{\tau^{-1}}{\longmapsto} 4 \overset{\sigma}{\longmapsto} 5 \overset{\tau}{\longmapsto} 5 \\
2 &\longmapsto 2 \longmapsto 4 \longmapsto 1 \\
3 &\longmapsto 1 \longmapsto 1 \longmapsto 3 \\
4 &\longmapsto 3 \longmapsto 2 \longmapsto 2 \\
5 &\longmapsto 5 \longmapsto 3 \longmapsto 4
\end{aligned}$$

Tenemos entonces que α es también un ciclo de longitud 4:

$$\alpha = \tau\gamma\tau^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix} = (1\ 5\ 4\ 2)$$

Proposición 1.14. *Sea $\sigma \in S_n$ una permutación de forma que se descompone en ciclos disjuntos de la forma:*

$$\sigma = \gamma_1 \dots \gamma_k$$

Entonces, podemos calcular su conjugado mediante $\tau \in S_n$ componiendo el conjugado de cada uno de los ciclos disjuntos en los que se descompone:

$$\tau\sigma\tau^{-1} = \tau\gamma_1\tau^{-1} \dots \tau\gamma_k\tau^{-1}$$

Demostración.

$$\tau\sigma\tau^{-1} = \tau\gamma_1 \dots \gamma_k\tau^{-1} = \tau\gamma_1 id\gamma_2 id \dots id\gamma_k\tau^{-1} = \tau\gamma_1\tau^{-1}\tau\gamma_2\tau^{-1} \dots \tau\gamma_k\tau^{-1}$$

□

Ejemplo. Para practicar con la Proposición anterior, se plantea dados:

$$\sigma = (1\ 12\ 8\ 10\ 4)(2\ 13)(5\ 11\ 7)(6\ 9), \qquad \tau = (4\ 8\ 12\ 7\ 5\ 9)$$

calcular $\tau\sigma\tau^{-1}$, cuya expresión vemos a continuación:

$$(1\ 7\ 12\ 10\ 8)(2\ 13)(5\ 9\ 11)(4\ 6)$$

Proposición 1.15. *Toda permutación es un producto de transposiciones.*

Demostración. Dada $\sigma \in S_n$, esta tiene su descomposición en ciclos disjuntos:

$$\sigma = \gamma_1 \dots \gamma_k$$

Basta demostrar que todo ciclo es producto de transposiciones.
En efecto, sea $\gamma = (x_1\ x_2\ \dots\ x_m)$, podemos escribir:

$$(x_1\ x_2\ \dots\ x_m) = (x_1\ x_m)(x_1\ x_{m-1}) \dots (x_1x_3)(x_1x_2)$$

O también podemos escribir:

$$(x_1\ x_2\ \dots\ x_m) = (x_1\ x_2)(x_2\ x_3) \dots (x_{m-1}\ x_m)$$

□

Ejemplo. Sea $\sigma = (1\ 2\ 3\ 4\ 5)$, veamos que σ se puede descomponer en transposiciones de la forma:

$$\sigma = t_1t_2t_3t_4$$

Con $t_1 = (1\ 5),\ t_2 = (1\ 4),\ t_3 = (1\ 3),\ t_4 = (1\ 2)$.
Para ello, escribamos la imagen de $X = \{1, 2, 3, 4, 5\}$ mediante la permutación resultante de componer las 4 transposiciones $\gamma = t_1t_2t_3t_4$ y veamos que coincide con la de σ:

$$\begin{aligned} 1 &\overset{\gamma}{\longmapsto} 2 \\ 2 &\longmapsto 3 \\ 3 &\longmapsto 4 \\ 4 &\longmapsto 5 \\ 5 &\longmapsto 1 \end{aligned}$$

De esta forma:

$$t_1t_2t_3t_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} = (1\ 2\ 3\ 4\ 5) = \sigma$$

Proposición 1.16. *Una permutación admite varias descomposiciones en productos de transposiciones, pero todas ellas coinciden en la paridad del número de transposiciones.*

1.3.1. Signatura

Definición 1.16 (Signatura)**.** Consideraremos el siguiente polinomio de n variables:

$$\Delta = \prod_{1 \leqslant i < j \leqslant n} (x_i - x_j) \in \mathbb{Z}[x_1, \ldots, x_n]$$

Y definimos para cada $\sigma \in S_n$:

$$\sigma(\Delta) = \prod_{1 \leqslant i < j \leqslant n} (x_{\sigma(i)} - x_{\sigma(j)})$$

Podemos ahora definir la aplicación signatura $\varepsilon : S_n \longrightarrow \{-1, 1\}$ dada por:

$$\varepsilon(\sigma) = \begin{cases} 1 & \text{si } \sigma(\Delta) = \Delta \\ -1 & \text{si } \sigma(\Delta) = -\Delta \end{cases}$$

- Si $\varepsilon(\sigma) = 1$, diremos que σ es una permutación par.
- Si $\varepsilon(\sigma) = -1$, diremos que σ es una permutación impar.

Observación. A partir de la definición anterior, tenemos que $\sigma(\Delta) = \varepsilon(\sigma)\Delta$.

Ejemplo. Sea $n = 4$, estaremos interesados en el polinomio:

$$\Delta = \prod_{1 \leqslant i < j \leqslant n} (x_i - x_j) = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4)$$

Si consideramos $\sigma = (1\ 2\ 3\ 4)$, queremos comprobar cual es la signatura de σ. Como:

$$\sigma(\Delta) = (x_2 - x_3)(x_2 - x_4)(x_2 - x_1)(x_3 - x_4)(x_3 - x_1)(x_4 - x_1) = -\Delta$$

Deducimos que $\varepsilon(\sigma) = -1$, es decir, σ es una permutación impar.

Proposición 1.17. *La aplicación signatura verifica que:*

$$\varepsilon\left(\prod_{i=1}^{m} \sigma_i\right) = \prod_{i=1}^{m} \varepsilon(\sigma_i)$$

Con $\sigma_1, \sigma_2, \ldots, \sigma_m \in S_n$.

Demostración. Por inducción sobre m:

- Para $m = 2$: Queremos ver que dadas $\sigma, \tau \in S_n$, entonces:

  $$\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$$

  Para ello, si vemos que $(\sigma\tau)(\Delta) = \sigma(\tau(\Delta))$ y que $\sigma(-\Delta) = -\sigma(\Delta)$, basta distinguir casos:

  - Si σ es par:
    - Si τ es par, se tendrá $\sigma(\tau(\Delta)) = \sigma(\Delta) = \Delta$, con lo que $\sigma\tau$ es par.

- Si τ es impar, se tendrá $\sigma(\tau(\Delta)) = \sigma(-\Delta) = -\sigma(\Delta) = -\Delta$, con lo que $\sigma\tau$ es impar.

- Si σ es impar:
  - Si τ es par, se tendrá $\sigma(\tau(\Delta)) = \sigma(\Delta) = -\Delta$, con lo que $\sigma\tau$ es impar.
  - Si τ es impar, se tendrá $\sigma(\tau(\Delta)) = \sigma(-\Delta) = -\sigma(\Delta) = \Delta$, con lo que $\sigma\tau$ es par.

- Supuesto para m:

$$\varepsilon\left(\prod_{i=1}^{m}\sigma_1\right) = \varepsilon\left(\left(\prod_{i=1}^{m-1}\sigma_i\right)\sigma_m\right) = \varepsilon\left(\prod_{i=1}^{m-1}\sigma_i\right)\varepsilon(\sigma_m) \overset{(*)}{=} \prod_{i=1}^{m-1}\left(\varepsilon(\sigma_i)\right)\varepsilon(\sigma_m) = \prod_{i=1}^{m}\varepsilon(\sigma_i)$$

Donde en $(*)$ hemos usado la hipótesis de inducción.

□

Corolario 1.17.1. *Se verifican los siguientes resultados:*

1. *Las transposiciones son permutaciones impares.*
2. *Una permutación es par si y solo si se descompone en el producto de un número par de transposiciones.*
3. *Un ciclo de longitud $m \geqslant 2$ es par si y solo si m es impar.*
4. *Una permutación es par si y solo si el número de ciclos de longitud par en su descomposición en ciclos disjuntos es par.*

Demostración. Demostramos cada uno de los resultados:

1. Sea $\sigma = (i\ j)$ una transposición (con $1 \leqslant i < j \leqslant n$), estudiemos qué sucede con $\sigma(\Delta)$:

   - Por una parte, está claro que hay un cambio de signo tras aplicar σ al factor $(x_i - x_j)$, ya que este pasa a ser $(x_j - x_i)$.
   - Está claro que los factores de la forma $(x_a - x_b)$ con $a, b \notin \{i, j\}$ se mantienen invariantes ante σ, por lo que no hay cambio de signo en estos.
   - Además, los factores de la forma $(x_a - x_y)$ con $y \in \{i, j\}$ y $a < i$ tampoco alteran el signo de Δ, ya que al aplicar σ:

     $$(x_a - x_i) \overset{\sigma}{\longmapsto} (x_a - x_j)$$
     $$(x_a - x_j) \longmapsto (x_a - x_i)$$

     Tenemos que un factor va al otro, por lo que no alteran el signo.
   - De forma análoga, los factores de la forma $(x_y - x_b)$ con $y \in \{i, j\}$ y $b > j$ tampoco alteran el signo de Δ:

     $$(x_i - x_b) \overset{\sigma}{\longmapsto} (x_j - x_b)$$
     $$(x_j - x_b) \longmapsto (x_i - x_b)$$

- Finalmente, los únicos factores que nos quedan por considerar son los de la forma $(x_i - x_a)$ y $(x_a - x_j)$, con $i < a < j$. En este caso:

$$(x_i - x_a) \overset{\sigma}{\longmapsto} (x_j - x_a) = -(x_a - x_j)$$
$$(x_a - x_j) \longmapsto (x_a - x_i) = -(x_i - x_a)$$

Fijado a con $i < a < j$, tanto el factor $(x_i - x_a)$ como el $(x_a - x_j)$ cambian de signo, por lo que el doble cambio de signo se compensa, luego estos factores no alteran el signo de Δ al aplicar σ.

Concluimos que al aplicar $\sigma = (i\ j)$ sobre Δ, el signo obtenido es el mismo salvo por el factor $(x_i - x_j)$, que cambia de signo, por lo que:

$$\sigma(\Delta) = -\Delta$$

y llegamos a que σ es impar.

2. Sea $\sigma \in S_n$ una permutación, sabemos que puede descomponerse en k transposiciones:

$$\sigma = \gamma_1\gamma_2 \dots \gamma_k$$

Usando la Proposición 1.17, tenemos que:

$$\varepsilon(\sigma) = \prod_{i=1}^{k} \varepsilon(\gamma_i)$$

Por lo que:

- Si k es par, entonces $\varepsilon(\sigma) = 1$.
- Si k es impar, entonces $\varepsilon(\sigma) = -1$.

3. Para $m = 2$, un ciclo de longitud m es una transposición, que ya sabemos que es impar. Sea τ un ciclo de longitud $m \geqslant 3$, en la Proposición 1.15 vimos que τ se podía descomponer como producto de $m - 1$ transposiciones:

$$\tau = \gamma_1\gamma_2 \dots \gamma_{m-1}$$

Por tanto, y aplicando 2, tenemos que:

- Si m es par, entonces $m - 1$ es impar, con lo que τ es impar.
- Si m es impar, entonces $m - 1$ es par, con lo que τ es par.

4. Sea $\sigma \in S_n$, esta se puede descomponer como producto de k ciclos disjuntos de longitud mayor o igual que 2:

$$\sigma = \gamma_1\gamma_2 \dots \gamma_k$$

Usando la Proposición 1.17, tenemos que:

$$\varepsilon(\sigma) = \prod_{i=1}^{k} \varepsilon(\gamma_i)$$

Si consideramos la siguiente partición de $\{1, \ldots, k\}$:

$$A = \{i \in \{1, \ldots, k\} \mid \gamma_i \text{ tiene longitud impar}\}$$
$$B = \{i \in \{1, \ldots, k\} \mid \gamma_i \text{ tiene longitud par}\}$$

Por 3 tenemos que $\varepsilon(\gamma_i) = 1$ para todo $i \in A$ y que $\varepsilon(\gamma_j) = -1$ para todo $j \in B$. De esta forma:

$$\varepsilon(\sigma) = \left(\prod_{i \in A} \varepsilon(\gamma_i)\right)\left(\prod_{i \in B} \varepsilon(\gamma_i)\right) = \left(\prod_{i \in A} 1\right)\left(\prod_{i \in B} -1\right) = \prod_{i \in B} -1$$

Por tanto:

- Si $|B|$ es par, tenemos que σ es par.
- Si $|B|$ es impar, tenemos que σ es impar.

□

Ejemplo. Ahora, es fácil determinar la signatura de cualquier permutación. Por ejemplo, si consideramos:

$$\sigma = (1\ 12\ 8\ 10\ 4)(2\ 13)(5\ 11\ 7)(69)$$

Como tiene 2 ciclos de longitud par (un número par), σ es una permutación par.

1.3.2. Grupos Alternados A_n

Definición 1.17 (Grupos Alternados A_n)**.** En S_n consideramos el conjunto:

$$A_n = \{\sigma \in S_n \mid \sigma \text{ es par}\}$$

Se verifica que $(A_n, \circ, 1)$ es un grupo:

- La asociatividad de $\circ$ es heredada de la de $\circ$ en S_n.
- El producto de dos permutaciones pares es par, luego está bien definido el grupo.
- La identidad es una permutación par, que es el neutro de la operación binaria.
- Dado $\sigma \in A_n$, escribimos su descomposición en ciclos disjuntos e invertimos cada ciclo. La longitud de los ciclos no cambia, luego la paridad del ciclo inverso tampoco, por lo que σ^{-1} sigue siendo una permutación par.

Al grupo A_n lo llamamos el grupo alternado de grado n, que verifica:

$$|A_n| = \frac{n!}{2}$$

Observación. Notemos que si definimos $B_n = \{\sigma \in S_n \mid \sigma \text{ es impar}\}$, entonces sobre B_n no podemos tener una estructura de grupo con la operación $\circ$, ya que el neutro para $\circ$ de S_n no está en B_n, sino en A_n.

Ejemplo. Listar todos los elementos de los grupos alternados es fácil si previamente listamos todos los elementos de su grupo simétrico correspondiente:

1. Para $n = 3$:

$$S_3 = \{1, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$$
$$A_3 = \{1, (1\ 2\ 3), (1\ 3\ 2)\}$$

2. Para $n = 4$:

$$S_4 = \{1, (1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4), (1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4),$$
$$(1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3), (1\ 2\ 3\ 4), (1\ 3\ 2\ 4), (1\ 2\ 4\ 3),$$
$$(1\ 3\ 2\ 4), (1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

$$A_4 = \{1, (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 2), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3),$$
$$(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

Proposición 1.18. *Se tiene que:*

(a) $S_n = \langle (1\ 2), (2\ 3), \ldots, (n-1, n)\rangle$

(b) $S_n = \langle (1\ 2), (1\ 2\ \ldots\ n)\rangle$

(c) $S_n = \langle (1\ 2), (1\ 3), \ldots, (1\ n)\rangle$

(d) $A_n = \langle (x_1\ x_2\ x_3)\rangle$ *con* $n \geqslant 3$

(e) $A_n = \langle (1\ x\ y)\rangle$ *con* $n \geqslant 3$

Demostración. Veamos cada uno de los enunciados:

(a) Sabemos que:
$$S_n = \langle (i\ j) \mid i, j \in \{1, \ldots, n\},\ i < j\rangle$$
Supuesto que $i < j$, vemos que:
$$(i\ j) = (i\ i+1)(i+1\ i+2)\ldots(j-2\ j-1)(j-1\ j)(j-1\ j-2)\ldots(i+1\ i)$$

(b) Basta obtener $\sigma = (1\ 2\ \ldots\ n)$ a partir de las trasposiciones, para $i, j \in \{1, \ldots, n\}$:
$$\sigma^{i-1}(1) = i$$
$$\sigma^{i-1}(2) = i+1$$
De esta forma:
$$\sigma^{i-1}(1\ 2)\sigma^{1-i} = (i\ i+1)$$
Que se ve porque:
$$\sigma^{i-1}(1\ 2)\sigma^{1-i}(i) = i+1$$
$$\sigma^{i-1}(1\ 2)\sigma^{1-i}(i+1) = i$$
$$\sigma^{i-1}(1\ 2)\sigma^{1-i}(j) = j \qquad j \neq i, i+1$$

(c) Basta ver (se hizo anteriormente):

$$(1\ 2\ \ldots\ n) = (1\ n)(1\ n-1)\ldots(1\ 3)(1\ 2)$$

(d) Podemos suponer que $x_1 < x_2 < x_3$, ya que:

$$(x_1\ x_3\ x_2) = (x_1\ x_2\ x_3)^2$$

Sabemos que si $\sigma \in A_n$, entonces será producto de un número par de transposiciones.

- Si hay elementos comunes:

$$(x_1\ x_2)(x_2\ x_3) = (x_1\ x_2\ x_3)^2$$

- Si no hay elementos comunes (tenemos dos transposiciones disjuntas), entonces:

$$(x_1\ x_2)(x_3\ x_4) = (x_1\ x_2\ x_3)(x_2\ x_3\ x_4)$$

(e) Tenemos que cualquier terna ordenada $(x_1\ x_2\ x_3)$ podemos escribirla de la forma:

$$(x_1\ x_2\ x_3) = (1\ x_3\ x_2)(1\ x_1\ x_2)(1\ x_1\ x_3)$$

□

Ejemplo. (a) Destacamos:

- $S_3 = \langle (1\ 2), (2\ 3)\rangle$ y tenemos:

$$(1\ 3) = (1\ 2)(2\ 3)(2\ 1)$$

- En $S_4 = \langle (1\ 2)(2\ 3)(3\ 4)\rangle$ tenemos:

$$(1\ 4) = (1\ 2)(2\ 3)(3\ 4)(3\ 2)(2\ 1)$$

(b) Ahora:

- En $S_3 = \langle (1\ 2), (1\ 2\ 3)\rangle$:

$$(2\ 3) = (1\ 2\ 3)^2(1\ 2)(1\ 2\ 3)^{-2}$$

- En $S_4 = \langle (1\ 2), (1\ 2\ 3\ 4)\rangle$:

$$(2\ 3) = (1\ 2\ 3\ 4)(1\ 2)(1\ 2\ 3\ 4)^{-1}$$
$$(3\ 4) = (1\ 2\ 3\ 4)^2(1\ 2)(1\ 2\ 3\ 4)^{-2}$$

(d) Veamos: $A_4 = \{1, (1\,2\,3), (1\,3\,2), (1\,2\,4), (1\,4\,2), (1\,3\,4), (1\,4\,3), (2\,3\,4), (2\,4\,3), (1\,2)(3\,4), (1\,3)(2\,4$
Tenemos que:

$$A_4 = \langle (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 4), (2\ 3\ 4)\rangle$$

Ya que:

$$(1\ 2)(3\ 4) = (1\ 2\ 3)(2\ 3\ 4)$$

(e) Tenemos:

$$A_4 = \langle (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 4)\rangle$$

1.4. Grupos de matrices

Sea $\mathbb{F}$ un cuerpo, las matrices cuadradas de orden n sobre $\mathbb{F}$ las denotaremos por:

$$\mathcal{M}_n(\mathbb{F})$$

Sabemos que $(\mathcal{M}_n(\mathbb{F}), +, \cdot)$ es un anillo, de donde nos quedaremos con el grupo lineal general con notación multiplicativa $\mathrm{GL}_n(\mathbb{F})$:

$$\mathrm{GL}_n(\mathbb{F}) = U(\mathcal{M}_n(\mathbb{F})) = \{A \in \mathcal{M}_n(\mathbb{F}) \mid A \text{ tiene inversa}\} = \{A \in \mathcal{M}_n(\mathbb{F}) \mid \det(A) \neq 0\}$$

Recordamos que esto sucede si y solo si $\det(A) \neq 0$, es decir, si las columnas de A son linealmente independientes.

Este grupo es importante porque nos va a pasar de grupos concretos a grupos abstractos.

Suponiendo que $\mathbb{F}$ es finito y tiene q elementos, tendremos:

$$|\,\mathrm{GL}_n(\mathbb{F})| = (q^n - 1)(q^n - q)\dots(q^n - q^{n-1})$$

Ya que vectores de n componentes con q valores no nulos que podemos generar son $q^n - 1$. Fijada esta columna, podemos elegir $q^n - q$ valores distintos para la siguiente columna ($-q$ porque necesitamos que sea linealmente independiente con la anterior).

Ejemplo. Veamos:

- En $|\,\mathrm{GL}_2(\mathbb{Z}_2)| = (2^2 - 1)(2^2 - 2) = 6$:

  $$\mathrm{GL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}$$

  Podemos escribirlos a partir de cómo se calcula el cardinal.

- Tenemos $|\,\mathrm{GL}_3(\mathbb{Z}_2)| = 168$. Se deja como ejercicio escribir todas las matrices.

- Tenemos $|\,\mathrm{GL}_2(\mathbb{Z}_3)| = 48$.

Si ahora consideramos el grupo lineal especial de orden n:

$$\mathrm{SL}_n(\mathbb{F}) = \{A \in \mathcal{M}_n(\mathbb{F}) \mid \det(A) = 1\}$$

Tenemos:

$$|\,\mathrm{SL}_n(\mathbb{F})| = \frac{|\,\mathrm{GL}_n(\mathbb{F})|}{q - 1}$$

Ejemplo. Tenemos:

- $\mathrm{SL}_2(\mathbb{Z}_2) = \mathrm{GL}_2(\mathbb{Z}_2)$.

- $|\,\mathrm{SL}_3(\mathbb{Z}_3)| = 24$.

1.5. Homomorfismos de grupos

Definición 1.18 (Homomorfismo)**.** Dados dos grupos G y H, un homomorfismo de grupos de G en H es una aplicación $f : G \to H$ que verifica:

$$f(xy) = f(x)f(y) \qquad \forall x, y \in G$$

Proposición 1.19. *Si $f : G \to H$ es un homomorfismo de grupos, entonces:*

1. $f(1) = 1$
2. $f(x^{-1}) = (f(x))^{-1}$

Demostración. Veamos cada una:

1. $f(1) = f(1 \cdot 1) = f(1)f(1) \Longrightarrow f(1) = 1$
2. $1 = f(1) = f(xx^{-1}) = f(x)f(x^{-1}) \Longrightarrow f(x^{-1}) = (f(x))^{-1}$

□

Definición 1.19. Sea $f : G \to H$ un homomorfismo de grupos, distinguimos:

- $\ker f = \{x \in G \mid f(x) = 1\}$
- $Imf = \{f(x) \mid x \in G\}$

Ejemplo. Ejemplos de homomorfismos de grupos son:

1. $id : G \to G$
2. $f : G \to H$ de forma que $f(x) = 1 \ \forall x \in G$, el homomorfismo trivial.
3. $exp : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$, dada por $exp(x) = e^x \ \forall x \in \mathbb{R}$
4. La aplicación determinante de matrices con determinante no nulo:

$$\begin{array}{rccc} \det: & \mathrm{GL}_n(\mathbb{F}) & \longrightarrow & \mathbb{F} \\ & A & \longmapsto & \det(A) \end{array}$$

5. La aplicación signatura:

$$\begin{array}{rccc} \varepsilon: & S_n & \longrightarrow & U(\mathbb{Z}) \\ & \sigma & \longmapsto & \varepsilon(\sigma) \end{array}$$

6. Si $f : G \to H$ y $g : H \to T$ son homomorfismos de grupos, entonces $g \circ f : G \to T$ es un homomorfismo de grupos.

Definición 1.20. Dado $f : G \to H$ un homomorfismo de grupos, decimos que:

- f es un monomorfismo si es inyectiva.
- f es un epimorfismo si es sobreyectiva.
- f es un isomorfismo si es biyectiva.

- Si $G = H$, diremos que f es un endomorfismo.
- Si f es un endomorfismo biyectivo, diremos que es un automorfismo.

Proposición 1.20. *Sea $f : G \to H$ un homomorfismo de grupos, entonces:*

i) *f es monomorfismo* $\iff \ker(f) = \{1\}$

ii) *f es isomorfismo* $\iff$ *f tiene inversa*

Demostración. Veamos los dos resultados:

i) Para el primero, demostramos las dos implicaciones:

$\Longrightarrow$) $x \in \ker(f) \Longrightarrow f(x) = 1 = f(1)$, pero como f es inyectiva, tenemos que $x = 1$.

$\Longleftarrow$) Sean $x, y \in G$ de forma que $f(x) = f(y)$, entonces:

$$f(x)(f(y))^{-1} = 1 \Longrightarrow f(xy^{-1}) = 1 \Longrightarrow xy^{-1} = q \Longrightarrow x = y$$

Concluimos que f es inyectiva.

ii) Trivial.

□

Definición 1.21 (Grupos isomorfos)**.** Sean G y H dos grupos, decimos que son isomorfos si existe un isomorfismo entre ellos.

Proposición 1.21. *La propiedad de ser isomorfo es una relación de equivalencia.*

Demostración. □

Teorema 1.22 (de clasificación)**.**

Cualquier grupo no abeliano de orden 6 es isomorfo a S_3.

Ejemplo. Tenemos:

$$S_3 \cong D_3 \cong \mathrm{GL}_2(\mathbb{Z}_2) \cong \mathrm{SL}_2(\mathbb{Z}_2)$$