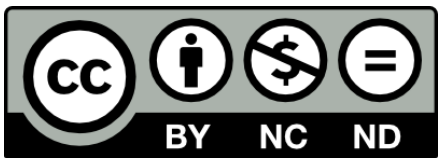
# Álgebra II


**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
Arturo Olivares Martos

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 $H$. Este será abeliano si y solo si $G$ y $H$ lo son.

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:

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

**Notación.** En grupos aditivos $(G, +, 0)$, en lugar de $x^n$ escribiremos $n \cdot x$, que se define de igual forma pero en el caso $n > 0$, en lugar de escribir $\prod$, escribiremos $\sum$.

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

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

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.

[4]Excluimos $n = 0$ ya que en la definición de grupo exigimos que $G \neq \emptyset$.

**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 $x_i x_j$.

**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: $O(x) = +\infty$.

[5]Entendiendo que en este caso hacemos uso de la notación multiplicativa.
[6]Podremos encontrarnos cualquiera de las dos notaciones.

**Notación.** Si consideramos un grupo con notación aditiva, $(G, +, 0)$, interpretando la anterior definición con esta notación diremos que $x \in G$ tendrá orden $n \in \mathbb{N} \setminus \{0\}$ si $n$ es el menor natural no negativo de forma que verifica $n \cdot x = \sum_{i=1}^{n} x = 0$.

**Proposición 1.8.** *Sea $G$ un grupo, $x \in G$ con $O(x) = n$ y sea $m \in \mathbb{N} \setminus \{0\}$:*

$$x^m = 1 \iff n \mid m$$

*Demostración.* Demostramos las dos implicaciones:

$\Longrightarrow$) 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 $O(x) = r$.

$\Longleftarrow$) Si $n \mid m$, entonces $\exists q \in \mathbb{N}$ de forma que $m = qn$, luego:

$$x^m = x^{qn} = (x^n)^q = 1^q = 1$$

□

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

1. *$O(x) = 1 \iff x = 1$.*
2. *$O(x) = O(x^{-1})$ $\forall x \in G$.*
3. *Si $O(x) = +\infty$ para cierto $x \in G$, entonces todas las potencias de $x$ son elementos distintos de $G$.*
4. *Si $G$ es finito, entonces $O(x) \neq +\infty$ para todo $x \in G$.*
5. *Si $O(x) = n \in \mathbb{N} \setminus \{0\}$ para cierto $x \in G$, entonces $x$ tiene $n$ potencias distintas. Más aún, sean $p, q \in \mathbb{N}$ de forma que $x^p = x^q$ con $q > p$, entonces:*

$$x^{q-p} = 1 \iff n \mid (q - p)$$

*Demostración.* Demostramos todas las 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. Distinguimos dos casos:

   - 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 $(x^{-1})^n = 1$:

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

     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:

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

   - Si tenemos que $O(x) = +\infty$, por reducción al absurdo, supongamos que $\exists n \in \mathbb{N} \setminus \{0\}$ de forma que $O(x^{-1}) = n$.
     Que $O(x) = +\infty$ significa que $\nexists m \in \mathbb{N} \setminus \{0\}$ de forma que $x^m = 1$.
     Como $O(x^{-1}) = n$, tenemos que:

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

     De donde llegamos a que:

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

     Contradicción, puesto que $O(x) = +\infty$. Deducimos que si $O(x) = +\infty$, entonces ha de ser $O(x^{-1}) = +\infty$.

3. Por reducción al absurdo, supongamos que existen $p, q \in \mathbb{N}$ con $p < q$ de forma que $x^p = x^q$, luego:

   $$x^{q-p} = 1$$

   De donde deducimos que $O(x) < +\infty$, contradicción, luego $x^p \neq x^q$ para todo $p, q \in \mathbb{N}$ con $p \neq q$.

4. Por reducción al absurdo, supongamos que $\exists x \in G$ con $O(x) = +\infty$. En este caso, podemos construir una aplicación $\phi : \mathbb{N} \to G$ dada por $\phi(n) = x^n$ $\forall n \in \mathbb{N}$. Esta aplicación es inyectiva gracias al punto 3, lo que contradice que $G$ sea un grupo finito. Concluimos que $O(x) = n \in \mathbb{N} \setminus \{0\}$ para todo $x \in G$.

5. Si $O(x) = n$, consideramos la sucesión:

   $$x, x^2, x^3, \ldots, x^{n-1}, x^n = 1$$

   Si seguimos calculando potencias, está claro que se repetirá este patrón, por lo que tratamos de ver que todos los elementos de la sucesión son distintos

entre sí. Por reducción al absurdo, supuesto que existen $p, q \in \mathbb{N}$ de forma que $p < q \leqslant n$ con $x^p = x^q$, entonces $x^{q-p} = 1$ con $q - p \leqslant n$, lo que contradice que $O(x) = n$.

Para ver que si $p, q \in \mathbb{N}$ con $x^p = x^q$, entonces:

$$x^{q-p} = 1 \iff n \mid (q - p)$$

Basta aplicar la Proposición 1.8 con $m = q - p$.

□

**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 $\mathbb{Z}_9$, $O\left(\overline{6}\right) = 3$:
$$\overline{6} \neq \overline{0}$$
$$\overline{6+6} = \overline{12} = \overline{3} \neq \overline{0}$$
$$\overline{6+6+6} = \overline{18} = \overline{0}$$
4. En $\mathbb{Z}_7^* = \mathcal{U}(\mathbb{Z}_7)$ :
   - $O\left(\overline{2}\right) = 3$:
   $$\overline{2} \neq \overline{1}$$
   $$\overline{2 \cdot 2} = \overline{4} \neq \overline{1}$$
   $$\overline{2 \cdot 2 \cdot 2} = \overline{8} = \overline{1}$$
   - $O\left(\overline{3}\right) = 6$.
   $$\overline{3} \neq \overline{1}$$
   $$\overline{3 \cdot 3} = \overline{9} = \overline{2} \neq \overline{1}$$
   $$\overline{3 \cdot 3 \cdot 3} = \overline{27} = \overline{6} \neq \overline{1}$$
   $$\overline{3 \cdot 3 \cdot 3 \cdot 3} = \overline{81} = \overline{3} \neq \overline{1}$$
   $$\overline{3 \cdot 3 \cdot 3 \cdot 3 \cdot 3} = \overline{243} = \overline{5} \neq \overline{1}$$
   $$\overline{3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3} = \overline{729} = \overline{1}$$

## 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.

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

### 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.

**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.

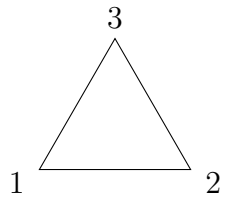



Figura 1.1: Triángulo equilátero con centro en el origen de coordenadas.

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 $2\pi$.

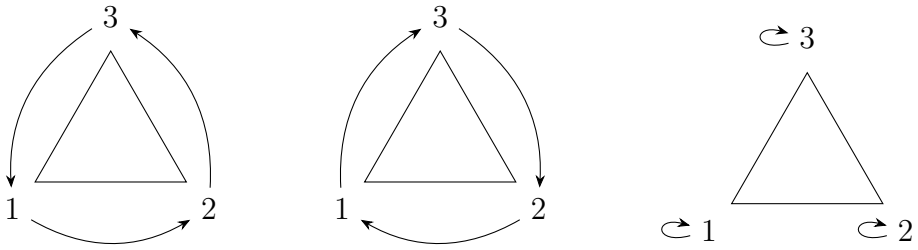



Figura 1.2: Todos los giros que dejan invariánte al triángulo.

**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.

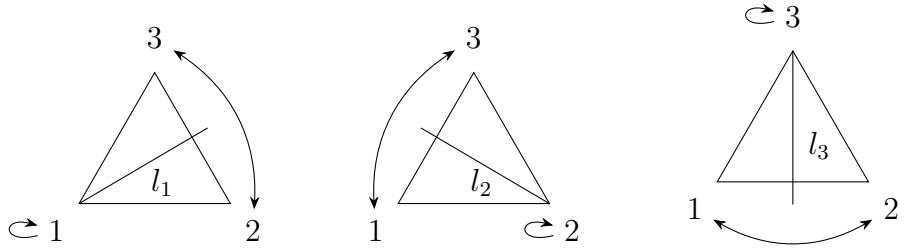



Figura 1.3: Todas las reflexiones que dejan invariante al triángulo.

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 $\sigma$ por:

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

*Observación.* Notemos que podemos notar a un ciclo de longitud $m$, $\sigma$, de $m$ formas distintas:

$$\sigma = (a_1 \ a_2 \ \ldots \ a_m) = (a_2 \ \ldots \ a_m \ a_1) = \ldots = (a_m \ a_1 \ a_2 \ \ldots \ a_{m-1})$$

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 $\sigma$ a $\{1, 2, 3, 4, 5\}$ definiendo:

$$\sigma(5) = 5$$

Entonces, la notación para $\sigma$ 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 $2\pi$ es $r^3$.
- La simetría respecto a la recta $l_2$ es $sr^2$.

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

- La simetría respecto a la recta $l_3$ es $sr$.

Notemos que el giro de ángulo $2\pi$ 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.

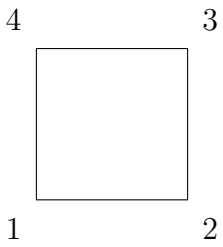



Figura 1.4: Cuadrado con centro en el origen de coordenadas.

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

- Los giros de ángulos $\frac{\pi}{2}$, $\pi$, $\frac{3\pi}{2}$ y $2\pi$.
- 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 $\pi$ es (1 3)(2 4).
- El giro de ángulo $\frac{3\pi}{2}$ es (1 4 3 2).

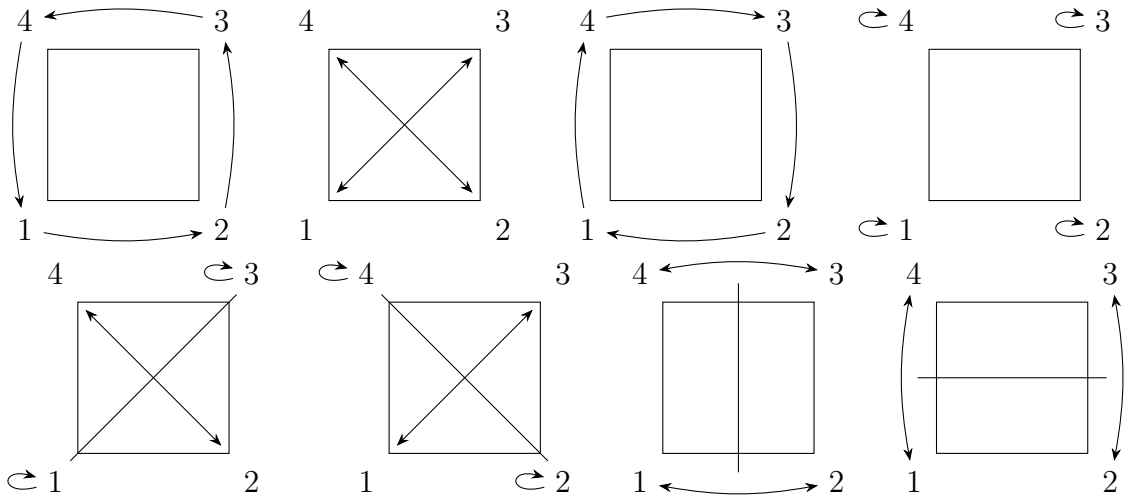



Figura 1.5: Giros y simetrías que dejan invariante al cuadrado

- El giro de ángulo $2\pi$ es la identidad, (1).
- 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 4)(2 3).
- $sr^2$ es (1 3).
- $sr^3$ es (1 2)(3 4).

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:

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

Y diremos que $G$ es finitamente generado.
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 $V^{\text{abs}}$, con $(xy)^{-1} = yx$. Vemos que no hay más elementos que puedan estar en $V^{\text{abs}}$, 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 $V^{\text{abs}}$ y $D_2$ o entre $Q_2^{\text{abs}}$ y $D_4$ las formalizaremos con ayuda de un concepto algebraico que luego definiremos, pero merece la pena destacar ahora una similaritud entre $Q_2^{\text{abs}}$, 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

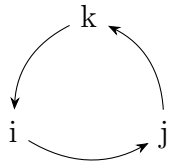



Figura 1.6: Dirección en la que se multiplican los cuaternios de forma positiva.

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

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

Si pensamos en relacionar los elementos de la Tabla 1.1.

| $Q_2^{\text{abs}}$ | 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 $\sigma$ 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 $\sigma$.

**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 $\sigma$ y $\tau$ 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 $\sigma \in S_n$, existe $m \in \mathbb{N}$ de forma que $\sigma^{m+1}(x) = x$, $\forall x \in X = \{1, \ldots, n\}$.*
2. *Todo ciclo es una permutación.*
3. *El orden de un ciclo de longitud $m$ es $m$.*
4. *Si $\sigma = (x_1\ x_2\ \ldots\ x_{m-1}\ x_m)$, entonces: $\sigma^{-1} = (x_m\ x_{m-1}\ \ldots\ x_2\ x_1)$.*

*Demostración.* Demostramos cada propiedad:

1. Por la Proposición 1.9, como $S_n$ es un grupo finito, sabemos que $\exists n \in \mathbb{N} \setminus \{0\}$ de forma que $O(\sigma) = n$. Tomando $m = n - 1$, tenemos que:
$$\sigma^{m+1}(x) = \sigma^n(x) = x \qquad \forall x \in X$$
2. Se tiene directamente por la definición de ciclo.
3. Sea $\sigma \in S_n$ un ciclo de longitud $m$:
$$\sigma = (x_1\ x_2\ \ldots\ x_m) \qquad x_1, x_2, \ldots, x_m \in X$$
Queremos ver que $O(\sigma) = m$. Para ello:
   - En primer lugar, veamos que $\sigma^m = 1$:
     - Si $x \in X$ con $x \neq x_i$ para todo $i \in \{1, \ldots, m\}$, entonces $\sigma(x) = x$, luego:
$$\sigma^m(x) = \sigma^{m-1}(\sigma(x)) = \sigma^{m-1}(x) = \sigma^{m-2}(\sigma(x)) = \ldots = x$$
     - Si ahora consideramos $x_i$ con $i \in \{1, \ldots, m\}$, tendremos que:
$$x_i \underbrace{\overset{\sigma}{\longmapsto} x_{i+1} \overset{\sigma}{\longmapsto} \ldots \overset{\sigma}{\longmapsto} x_{m-1} \overset{\sigma}{\longmapsto}}_{\sigma^{m-i}} x_m \underbrace{\overset{\sigma}{\longmapsto} x_1 \overset{\sigma}{\longmapsto} \ldots \overset{\sigma}{\longmapsto} x_{i-1} \overset{\sigma}{\longmapsto}}_{\sigma^{i}} x_i$$
     Luego: $1 = \sigma^{m-i}\sigma^i = \sigma^{m-i+i} = \sigma^m$
   - Supongamos ahora que existe $k < m$ de forma que $\sigma^k = 1$, esto significaría que $\sigma^k(x_1) = x_1$, pero como $\sigma$ es un ciclo de longitud $m$, se tiene que $\sigma^k(x_1) = x_k$ y $x_k \neq x_1$, contradicción, con lo que $k \geqslant m$.
4. Recordamos por la definción de ciclo que si $\sigma = (a_1\ a_2\ \ldots\ a_{m-1}\ a_m)$, entonces se ha de cumplir que:
$$\begin{aligned} \sigma(x) &= x \qquad x \neq x_i, \quad i \in \{1, \ldots, m\} \\ \sigma(x_i) &= x_{i+1} \qquad i \in \{1, \ldots, m-1\} \\ \sigma(x_m) &= x_1 \end{aligned}$$
   Si vemos $\sigma$ como aplicación y tratamos de buscarle su aplicación inversa $\sigma^{-1}$, esta ha de cumplir que:
$$\begin{aligned} \sigma^{-1}(x) &= x \qquad x \neq x_i, \quad i \in \{1, \ldots, m\} \\ \sigma^{-1}(x_{i+1}) &= x_i \qquad i \in \{1, \ldots, m-1\} \\ \sigma^{-1}(x_1) &= x_m \end{aligned}$$
   Sin embargo, vemos que entonces $\sigma^{-1}$ también es un ciclo:
$$\sigma^{-1} = (x_m\ x_{m-1}\ \ldots\ x_2\ x_1)$$

□

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 $\gamma_i$ 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 $\gamma_x$.

1. Sean $\overline{i}, \overline{j} \in X/R$ con $\overline{i} \neq \overline{j}$, entonces los elementos que se mueven en $\gamma_i$ son los elementos de $C_i$, mientras los elementos que se mueven en $\gamma_j$ 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 $\gamma_i$ y $\gamma_j$ 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 $\tau$ los ciclos de longitud menor que 2, la permutación $\sigma$ no cambia y tenemos que $\sigma$ 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 $\sigma$ como el producto de todas esas notaciones.

Como acabamos de decir, a partir del Teorema 1.12, podremos notar a las permutaciones como su descomposición en ciclos disjuntos. Sin embargo, merece la pena preguntarse sobre el orden de los ciclos en esta descomposición, pregunta a la que contestamos con la siguiente proposición:

**Proposición 1.13.** *Se verifican:*

1. *Si $\gamma_1, \gamma_2 \in S_n$ son dos ciclos disjuntos, entonces:*

$$\gamma_1\gamma_2 = \gamma_2\gamma_1$$

*Es decir, el producto de ciclos disjuntos es conmutativo.*

2. *Sea $\sigma \in S_n$ una permutación, si consideramos su descompoisición en ciclos disjuntos:*

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

*Entonces, se tiene que:*

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

*Demostración.* Demostramos cada uno de los resultados:

1. Supongamos que:

$$\gamma_1 = (x_1\ x_2\ \dots\ x_n), \qquad \gamma_2 = (y_1\ y_2\ \dots\ y_m)$$
$$x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m \in X \text{ todos ellos distintos}$$

Tenemos entonces que:

- Si $x \neq x_i, x \neq y_j$ para $i \in \{1, \dots, n\}, j \in \{1, \dots, m\}$:

$$\gamma_1(\gamma_2(x)) = \gamma_1(x) = x = \gamma_2(x) = \gamma_2(\gamma_1(x))$$

- Si consideramos $i \in \{1, \dots, n-1\}$:

$$\gamma_1(\gamma_2(x_i)) = \gamma_1(x_i) = x_{i+1} = \gamma_2(x_{i+1}) = \gamma_2(\gamma_1(x_i))$$

Donde hemos usado que $x_i \neq y_j$ para todo $j \in \{1, \dots, m\}$.

- Si consideramos ahora $j \in \{1, \dots, m-1\}$:

$$\gamma_1(\gamma_2(y_j)) = \gamma_1(y_{j+1}) = y_{j+1} = \gamma_2(y_j) = \gamma_2(\gamma_1(y_j))$$

Donde hemos usado que $y_j \neq x_j$ para todo $i \in \{1, \dots, n\}$.

- Faltan los casos de $x_n$ y $y_m$, que son análogos:

$$\gamma_1(\gamma_2(x_n)) = \gamma_1(x_n) = x_1 = \gamma_2(x_1) = \gamma_2(\gamma_1(x_n))$$
$$\gamma_1(\gamma_2(y_m)) = \gamma_1(y_1) = y_1 = \gamma_2(y_m) = \gamma_2(\gamma_1(y_m))$$

Como hemos visto que $\gamma_1(\gamma_2(x)) = \gamma_2(\gamma_1(x))$ para todo $x \in X$, concluimos que $\gamma_1\gamma_2 = \gamma_2\gamma_1$.

2. Dado $\sigma = \gamma_1\gamma_2 \dots \gamma_k$, buscamos una permutación $\tau \in S_n$ que verifique que:

$$\sigma\tau = \gamma_1\gamma_2 \dots \gamma_{k-1}\gamma_k\tau = 1$$

Observamos que como $\tau$ podemos tomar:

$$\tau = \gamma_k^{-1}\gamma_{k-1}^{-1} \dots \gamma_2^{-1}\gamma_1^{-1}$$

sin embargo, como los $\gamma_i$ con $i \in \{1, \ldots, k\}$ eran ciclos disjuntos, por la Proposición 1.11, sabemos que los $\gamma_i^{-1}$ también seguirán siendo ciclos disjuntos y por 1 sabemos que su producto es conmutativo, por lo que podemos escribir:

$$\tau = \gamma_1^{-1}\gamma_2^{-1} \ldots \gamma_k^{-1}$$

Como $\sigma\tau = 1$, concluimos que $\tau = \sigma^{-1}$.

□

**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, sabemos que para calcular la permutación inversa basta calcular la inversa de cada uno de los ciclos:

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

Del Teorema 1.12 deducimos el siguiente corolario:

**Corolario 1.13.1.** *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 $\sigma$ se descompone de la forma:

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

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

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

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

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

Donde en $(*)$ hemos usado la Proposición 1.8. Concluimos que $m$ es el mínimo común múltiplo de los órdenes de los ciclos, que por la Proposición 1.11, 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** (Elementos conjugados)**.** Sea $G$ un grupo y $a, c \in G$, decimos que son conjugados si $\exists b \in G$ de forma que $a = bcb^{-1}$.

**Proposición 1.14.** *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 $\gamma$ 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 $\alpha$ 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 $\alpha$ 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 1.15.** *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 la conjugación de ciclos aplicando las Proposiciones 1.14 y 1.15, 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 $\tau\sigma\tau^{-1}$. Para ello, sabemos por la Proposición 1.15 que si[9] $\sigma = \gamma_1\gamma_2\gamma_3\gamma_4$, entonces basta calcular:

$$\tau\gamma_1\tau^{-1}, \quad \tau\gamma_2\tau^{-1}, \quad \tau\gamma_3\tau^{-1}, \quad \tau\gamma_4\tau^{-1}$$

Por la Proposición 1.14, sabemos que:

$$\begin{aligned}
\tau\gamma_1\tau^{-1} &= (\tau(1)\ \tau(12)\ \tau(8)\ \tau(10)\ \tau(4)) = (1\ 7\ 12\ 10\ 8)\\
\tau\gamma_2\tau^{-1} &= (\tau(2)\ \tau(13)) = (2\ 13)\\
\tau\gamma_3\tau^{-1} &= (\tau(5)\ \tau(11)\ \tau(7)) = (9\ 11\ 5)\\
\tau\gamma_4\tau^{-1} &= (\tau(6)\ \tau(9)) = (6\ 4)
\end{aligned}$$

Si lo escribimos todo junto:

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

**Proposición 1.16.** *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:

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

[9] Observar la descomposición hecha ya de $\sigma$.

Para verlo, observemos qué hace la aplicación de la derecha con cada elemento (léase la descomposición de derecha a izquierda):

$$\begin{aligned}
&x_1 \longmapsto x_2\\
&x_2 \longmapsto x_1 \longmapsto x_3\\
&x_3 \longmapsto x_1 \longmapsto x_4\\
&\vdots\\
&x_i \longmapsto x_1 \longmapsto x_{i+1}\\
&\vdots\\
&x_m \longmapsto x_1
\end{aligned}$$

O también podemos escribir:

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

Para verlo:

$$\begin{aligned}
&x_1 \longmapsto x_2\\
&x_2 \longmapsto x_3\\
&x_3 \longmapsto x_4\\
&\vdots\\
&x_i \longmapsto x_{i+1}\\
&\vdots\\
&x_m \longmapsto x_{m-1} \longmapsto x_{m-2} \longmapsto \ldots \longmapsto x_3 \longmapsto x_2 \longmapsto x_1
\end{aligned}$$

□

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

$$\sigma = t_1 t_2 t_3 t_4$$

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 $\gamma = t_1 t_2 t_3 t_4$ y veamos que coincide con la de $\sigma$:

$$\left.\begin{array}{l}
1 \overset{t_4}{\longmapsto} 2 \overset{t_3}{\longmapsto} 2 \overset{t_2}{\longmapsto} 2 \overset{t_1}{\longmapsto} 2\\
2 \longmapsto 1 \longmapsto 3 \longmapsto 3 \longmapsto 3\\
3 \longmapsto 3 \longmapsto 1 \longmapsto 4 \longmapsto 4\\
4 \longmapsto 4 \longmapsto 4 \longmapsto 1 \longmapsto 5\\
5 \longmapsto 5 \longmapsto 5 \longmapsto 5 \longmapsto 1
\end{array}\right\} \Longrightarrow \left\{\begin{array}{l}
1 \overset{\gamma}{\longmapsto} 2\\
2 \longmapsto 3\\
3 \longmapsto 4\\
4 \longmapsto 5\\
5 \longmapsto 1
\end{array}\right.$$

De esta forma:

$$\gamma = t_1 t_2 t_3 t_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5\\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} = (1\ 2\ 3\ 4\ 5) = \sigma$$

Si ahora consideramos la descomposición de la forma:

$$\sigma = r_1 r_2 r_3 r_4$$

Con $r_1 = (1\ 2)$, $r_2 = (2\ 3)$, $r_3 = (3\ 4)$, $r_4 = (4\ 5)$, escribimos ahora la imagen de $X$ mediante la permutación $\tau = r_1 r_2 r_3 r_4$:

$$\left.\begin{array}{l} 1 \overset{r_4}{\longmapsto} 1 \overset{r_3}{\longmapsto} 1 \overset{r_2}{\longmapsto} 1 \overset{r_1}{\longmapsto} 2 \\ 2 \longmapsto 2 \longmapsto 2 \longmapsto 3 \longmapsto 3 \\ 3 \longmapsto 3 \longmapsto 4 \longmapsto 4 \longmapsto 4 \\ 4 \longmapsto 5 \longmapsto 5 \longmapsto 5 \longmapsto 5 \\ 5 \longmapsto 4 \longmapsto 3 \longmapsto 2 \longmapsto 1 \end{array}\right\} \Longrightarrow \left\{\begin{array}{l} 1 \overset{\gamma}{\longmapsto} 2 \\ 2 \longmapsto 3 \\ 3 \longmapsto 4 \\ 4 \longmapsto 5 \\ 5 \longmapsto 1 \end{array}\right.$$

Vemos igual que antes que $\tau = \sigma$.

**Proposición 1.17.** *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:

$$\varepsilon(\sigma) = \left\{\begin{array}{ll} 1 & \text{si } \sigma(\Delta) = \Delta \\ -1 & \text{si } \sigma(\Delta) = -\Delta \end{array}\right.$$

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

**Proposición 1.18.** *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 $\sigma$ es par:
    - Si $\tau$ es par, se tendrá $\sigma(\tau(\Delta)) = \sigma(\Delta) = \Delta$, con lo que $\sigma\tau$ es par.
    - Si $\tau$ es impar, se tendrá $\sigma(\tau(\Delta)) = \sigma(-\Delta) = -\sigma(\Delta) = -\Delta$, con lo que $\sigma\tau$ es impar.
  - Si $\sigma$ es impar:
    - Si $\tau$ es par, se tendrá $\sigma(\tau(\Delta)) = \sigma(\Delta) = -\Delta$, con lo que $\sigma\tau$ es impar.
    - Si $\tau$ 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.

□

**Proposición 1.19.** *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 $\sigma$ 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 $\sigma$, 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 $\Delta$, ya que al aplicar $\sigma$:

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

  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 $\Delta$:

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

- 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 $\Delta$ al aplicar $\sigma$.

Concluimos que al aplicar $\sigma = (i\ j)$ sobre $\Delta$, 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 $\sigma$ 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 1.18, 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 $\tau$ un ciclo de longitud $m \geqslant 3$, en la Proposición 1.16 vimos que $\tau$ 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 $\tau$ es impar.
- Si $m$ es impar, entonces $m-1$ es par, con lo que $\tau$ 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 1.18, tenemos que:

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

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

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

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

□

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

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

Como tiene 2 ciclos de longitud par (un número par), $\sigma$ 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 $\sigma^{-1}$ 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 $n = 4$:

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

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

**Proposición 1.20.** *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 (por la Proposición 1.16):

$$S_n = \langle (i\ j) \mid i, j \in \{1, \ldots, n\},\ i < j \rangle$$

Supuesto que $i < j$, vemos que:

$$(i\ j) = (i\ i{+}1)(i{+}1\ i{+}2)\ldots(j{-}2\ j{-}1)(j{-}1\ j)(j{-}1\ j{-}2)\ldots(i{+}2\ i{+}1)(i{+}1\ i)$$

(b) Por el apartado anterior, basta obtener cualquier transposición de la forma $(i\ i+1)$ con $i \in \{1, \dots, n-1\}$ a partir de $\sigma = (1\ 2\ \dots\ n)$ y $(1\ 2)$. Para ello, como se tiene que:

$$\sigma^{i-1}(1) = i \qquad \sigma^{i-1}(2) = i+1$$

Podemos considerar el conjugado de $(1\ 2)$ mediante $\sigma^{i-1}$:

$$\sigma^{i-1}(1\ 2)(\sigma^{i-1})^{-1} = \sigma^{i-1}(1\ 2)\sigma^{1-i} = (\sigma^{i-1}(1)\ \sigma^{i-1}(2)) = (i\ i+1)$$

(c) Basta ver que $(1\ 2\ \dots\ n)$ se puede obtener por composición de transposiciones de la forma $(1\ j)$ con $j \in \{2, \dots, n\}$, lo que ya se hizo en la Proposición 1.16:

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

(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, por lo que basta expresar estos productos en función de ciclos de la forma $(x_1\ x_2\ x_3)$.

- Si hay elementos comunes, escribiremos:

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

- 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) Usando el apartado anterior, 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.** Usando la Proposición 1.20, veamos distintos conjuntos generadores para varios grupos:

(a) Destacamos:

- $S_3 = \langle (1\ 2), (2\ 3) \rangle$ y buscamos expresar la última transposición como producto de estas:

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

- En $S_4 = \langle (1\ 2)(2\ 3)(3\ 4) \rangle$ mostramos por ejemplo que:

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

(b) Ahora:

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

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

- 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) Recordamos los elementos de $A_4$:

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

Tenemos que:

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

Por ejemplo, podemos escribir:

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

(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, aunque estaremos interesados en ver el conjunto $\mathcal{M}_n(\mathbb{F})$ como un grupo en su forma más interesante, es decir, como grupo con notación multiplicativa.

### 1.4.1. Grupo lineal $\mathrm{GL}_n(\mathbb{F})$

**Definición 1.18** (Grupo lineal $\mathrm{GL}_n(\mathbb{F})$)**.** Sea $\mathbb{F}$ un cuerpo finito, en $\mathcal{M}_n(\mathbb{F})$ consideramos el conjunto:

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

Se verifica que $(\mathrm{GL}_n(\mathbb{F}), \cdot, I)$ es un grupo:

- La asociatividad de $\cdot$ viene heredada de la de $\cdot$ en $\mathcal{M}_n(\mathbb{F})$.
- $\det(I) = 1 \neq 0$ y se tiene que $I$ es el elemento neutro para $\cdot$.
- Como consideramos las matrices con determinante no nulo, sabemos que todas estas tienen inversa.

A $\mathrm{GL}_n(\mathbb{F})$ lo llamamos el grupo lineal de orden $n$.

**Proposición 1.21.** *Sea $n \in \mathbb{N}$, si $|\mathbb{F}| = q$, entonces se verifica que:*

$$|\operatorname{GL}_n(\mathbb{F})| = (q^n - 1)(q^n - q)\dots(q^n - q^{n-1}) = \prod_{k=1}^{n} \left(q^n - q^{k-1}\right)$$

*Demostración.* Como $A \in \mathrm{GL}_n(\mathbb{F}) \iff A$ es regular $\iff$ sus filas son vectores linealmente independientes, basta contar de cuántas formas podemos elegir $n$ vectores linealmente independientes con $n$ entradas en $\mathbb{F}$ (que recordamos tenía $q$ elementos). Para ello:

- Para elegir el primer vector $v_1 \in \mathbb{F}^n$, podemos elegir cualquiera, luego el problema es elegir $n$ números de entre $q$ posibilidades, $q^n$ posibles elecciones.

  Sin embargo, como queremos que $v_1$ sea linealmente independiente con el resto de vectores que forman las filas de una matriz, hemos de exigir $v_1 \neq 0$, con lo que tenemos $q^n - 1$ posibilidades para $v_1$.

- Una vez elegido $v_1$, para elegir $v_2$ no podemos elegir un vector de $\mathcal{L}(v_1) \cong \mathbb{F}$, por lo que tenemos $q$ vectores que no podemos elegir; elegimos un vector de los $q^n - q$ restantes.

- Repitiendo el proceso, una vez elegido $v_{k-1}$, para elegir $v_k$ (con $k \in \{2, \dots, n\}$), no podemos elegir ningún vector de $\mathcal{L}(v_1, \dots, v_{k-1}) \cong \mathbb{F}^{k-1}$, por lo que tenemos $q^{k-1}$ vectores que no podemos elegir y elegimos entre los $q^n - q^{k-1}$ restantes.

Este proceso ilusta que las posibles elecciones totales de vectores para las filas de una matriz de $\mathrm{GL}_n(\mathbb{F})$ son:

$$\prod_{k=1}^{n} \left(q^n - q^{k-1}\right)$$

Por lo que este debe ser el cardinal de $|\operatorname{GL}_n(\mathbb{F})|$. □

**Ejemplo.** Veamos:

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

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

  Podemos escribirlos sin que se nos olvide ninguna pensando en que tenemos que escribir todas las matrices de forma que los vectores formados por las columnas sean linealmente independientes entre sí (para así conseguir un determinante no nulo).

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

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

### 1.4.2. Grupo lineal especial $\mathrm{SL}_n(\mathbb{F})$

**Definición 1.19** (Grupo lineal especial $\mathrm{SL}_n(\mathbb{F})$)**.** Sea $\mathbb{F}$ un cuerpo finito, en $\mathcal{M}_n(\mathbb{F})$ consideramos el conjunto:

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

Se verifica que $(\mathrm{SL}_n(\mathbb{F}), \cdot, I)$ es un grupo:

- La asociatividad de $\cdot$ viene heredada de la de $\cdot$ en $\mathcal{M}_n(\mathbb{F})$.
- $\det(I) = 1$ y se tiene que $I$ es el elemento neutro para $\cdot$.
- Como consideramos las matrices con determinante $1 \neq 0$, sabemos que todas estas tienen inversa.

A $\mathrm{SL}_n(\mathbb{F})$ lo llamamos el grupo lineal especial de orden $n$.

**Proposición 1.22.** *Sea $n \in \mathbb{N}$, si $|\mathbb{F}| = q$, entonces se verifica que:*

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

*Demostración.* Sea $A \in \mathrm{GL}_n(\mathbb{F})$, observemos que $\det(A)$ puede[10] tomar $q$ valores distintos, uno por cada elemento de $\mathbb{F}$. De esta forma, si dado $k \in \mathbb{F}^* = \mathbb{F} \setminus \{0\}$ definimos:

$$D_k = \{A \in \mathrm{GL}_n(\mathbb{F}) : \det(A) = k\}$$

Es claro que estos conjuntos forman una partición de $\mathrm{GL}_n(\mathbb{F})$:

$$\mathrm{GL}_n(\mathbb{F}) = \biguplus_{k \in \mathbb{F}^*} D_k$$

Veamos que $|D_k| = |D_1|$ para todo $k \in \mathbb{F}^*$. Para ello, sea $k \in \mathbb{F}^*$, definimos la aplicación $\varphi_k : \mathrm{GL}_n(\mathbb{F}) \to \mathrm{GL}_n(\mathbb{F})$ dada por:

$$\varphi_k(A) = \varphi_k((a_{ij})_{i,j}) = (\overline{a_{ij}})_{i,j} \qquad \forall A = (a_{ij})_{i,j} \in \mathrm{GL}_n(\mathbb{F})$$

Donde:

$$\overline{a_{ij}} = \begin{cases} ka_{ij} & \text{si } i = 1 \\ a_{ij} & \text{si } i \neq 1 \end{cases}$$

Es decir, $\varphi_k$ multiplica la primera fila de una matriz por $k$. De esta forma, las propiedades de los determinantes nos dicen que si $A \in D_1$, entonces:

$$\det(\varphi_k(A)) = k \cdot \det(A) = k$$

Por lo que $\varphi_k(A) \in D_k$ para todo $k \in \mathbb{F}^*$. Por tanto, podemos definir la aplicación $\psi_k : D_1 \to D_k$ de forma que $\psi_k = \varphi_{k_{|D_1}}$. Veamos que $\psi_k$ es biyectiva para terminar el razonamiento. Para ello, dada $\psi_k$ para un cierto $k \in \mathbb{F}$, consideramos $\psi_{k^{-1}}$. Como:

$$kk^{-1}a_{ij} = k^{-1}ka_{ij} = a_{ij} \qquad \forall a_{ij} \in \mathbb{F}$$

[10] De hecho los toma, es fácil comprobar que $\det : \mathrm{GL}_n(\mathbb{F}) \to \mathbb{F}$ es una aplicación sobreyectiva.

Concluimos que $\psi_k^{-1} = \psi_{k^{-1}}$ y además vemos que $\varphi_{k^{-1}}(D_k) \subseteq D_1$. Llegamos a que $\psi_k$ es biyectiva, por lo que $|D_k| = |D_1|$ para todo $k \in \mathbb{F}^*$.

Sea ahora $\phi : \{1, \dots, q-1\} \to \mathbb{F}^*$ cualquier biyección de forma que $\phi(1) = 1$, como los $D_k$ formaban una partición finita de $\mathrm{GL}_n(\mathbb{F})$, tenemos que:

$$|\mathrm{GL}_n(\mathbb{F})| = \sum_{k=1}^{q-1} |D_{\phi(k)}| = \sum_{k=1}^{q-1} |D_1| = (q-1)|D_1| = (q-1)|\mathrm{SL}_n(\mathbb{F})|$$

De donde deducimos que:

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

□

**Ejemplo.** Tenemos:

- $|\mathrm{SL}_3(\mathbb{Z}_3)| = 24$.
- $\mathrm{SL}_n(\mathbb{Z}_2) = \mathrm{GL}_n(\mathbb{Z}_2)\ \forall n \in \mathbb{N}$

## 1.5. Homomorfismos de grupos

**Definición 1.20** (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 1.23.** *Si $f : G \to H$ es un homomorfismo de grupos, entonces:*

1. $f(1) = 1$
2. $f(x^{-1}) = (f(x))^{-1}$
3. $f(x^n) = (f(x))^n\ \forall n \in \mathbb{N}$

*Demostración.* Veamos cada una:

1. $f(1) = f(1 \cdot 1) = f(1)f(1) \Longrightarrow f(1) = 1$
2. $1 = f(1) = f(xx^{-1}) = f(x)f(x^{-1}) \Longrightarrow f(x^{-1}) = (f(x))^{-1}$
3. $f(x^n) = f(\underbrace{x \cdot \ldots \cdot x}_{n \text{ veces}}) = \underbrace{f(x) \cdot \ldots \cdot f(x)}_{n \text{ veces}} = (f(x))^n$

□

**Definición 1.21.** 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. Dado $G$ un grupo, $id : G \to G$.
2. Dados $G, H$ grupos, consideramos el siguiente homomorfismo, denominado *homomorfismo trivial*:
$$\begin{array}{rccc} f: & G & \longrightarrow & H \\ & x & \longmapsto & 1 \end{array}$$
3. La exponencial es también un homomorfismo:
$$\begin{array}{rccc} \exp: & (\mathbb{R},+) & \longrightarrow & (\mathbb{R}^+,\cdot) \\ & x & \longmapsto & e^x \end{array}$$
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:
$$\begin{array}{rccc} \varepsilon: & S_n & \longrightarrow & \mathcal{U}(\mathbb{Z}) = \{-1,1\} \\ & \sigma & \longmapsto & \varepsilon(\sigma) \end{array}$$

**Proposición 1.24.** *Sean $f : G \to H$ y $g : H \to T$ dos homomorfismos de grupos, entonces la aplicación $g \circ f : G \to T$ es un homomorfismo de grupos.*

*Demostración.* Sean $x, y \in G$, entonces:

$$(g \circ f)(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = (g \circ f)(x)(g \circ f)(y)$$

□

**Definición 1.22.** 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 1.25.** *Sea $f : G \to H$ un homomorfismo de grupos, entonces:*

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

*ii)* *$f$ es isomorfismo $\iff f^{-1}$ es un isomorfismo.*

*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:

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

Concluimos que $f$ es inyectiva.

*ii*) Demostramos las dos implicaciones:

$\Longrightarrow$) Si $f$ es un isomorfismo, entonces es biyectiva, por lo que tendrá una aplicación inversa $f^{-1}$, que por lo pronto ya sabemos que es biyectiva. Basta ver que esta aplicación es un homomorfismo. Para ello, sean $y, y' \in H$, por ser $f$ un biyectiva, existirán $x, x' \in G$ de forma que $f(x) = y$ y $f(x') = y'$, luego $x = f^{-1}(y)$ y $x' = f^{-1}(y')$. Por tanto:

$$f^{-1}(yy') = f^{-1}(f(x)f(x')) = f^{-1}(f(xx')) = xx' = f^{-1}(y)f^{-1}(y')$$

Lo que demuestra que $f^{-1}$ es un homomorfismo biyectivo, luego isomorfismo.

$\Longleftarrow$) Si $f^{-1}$ es un isomorfismo, entonces por la implicación que acabamos de demostrar, $(f^{-1})^{-1} = f$ también es un isomorfismo. □

**Definición 1.23** (Grupos isomorfos)**.** Sean $G$ y $H$ dos grupos, decimos que son isomorfos si existe un isomorfismo entre ellos, que se denotará por $G \cong H$.

**Proposición 1.26.** *La propiedad de ser isomorfo es una relación de equivalencia.*

*Demostración.* Demostramos cada una de las propiedades:

- Propiedad reflexiva. Sea $G$ un grupo, como $id : G \to G$ es un homomorfismo, tenemos que $G \cong G$.
- Propiedad simétrica. Sean $G$ y $H$ dos grupos de forma que $G \cong H$, entonces existe un isomorfismo $f : G \to H$. Por la Proposición 1.25, $f^{-1} : H \to G$ también será un isomorfismo, por lo que $H \cong G$.
- Propiedad transitiva. Sean $G$, $H$ y $T$ tres grupos de forma que $G \cong H$ y $H \cong T$, entonces existen dos isomorfismos: $f : G \to H$ y $g : H \to T$. Si consideramos $g \circ f : G \to T$, tenemos por la Proposición 1.24 que $g \circ f$ es un isomorfismo de $G$ en $T$, por lo que $G \cong T$.

□

**Proposición 1.27.** *Se verifican:*

*i*) *Si $f : X \to Y$ es una aplicación biyectiva, se tiene que la aplicación siguiente es un isomorfismo de grupos:*

$$\begin{array}{rccc} \varphi : & \mathrm{Perm}(X) & \longrightarrow & \mathrm{Perm}(Y) \\ & \sigma & \longmapsto & f\sigma f^{-1} \end{array}$$

*ii)* *$Aut(G) = \{f : G \to G \mid f$ automorfismo$\}$ con la composición forman un grupo.*

*iii)* *Si $f : G \to H$ es un isomorfismo, entonces $|G| = |H|$.*

*iv)* *Si $G$ y $H$ son isomorfos, entonces $G$ es abeliano $\iff H$ es abeliano.*

*v)* *Si $f : G \to H$ es un isomorfismo, entonces se mantiene el orden:*

$$O(x) = O(f(x)) \qquad \forall x \in G$$

*vi)* *Si $f : G \to H$ es un epimorfismo y $S = \{s_1, \ldots, s_n\} \subseteq G$ cumple que $G = \langle S \rangle$, entonces $H = \langle f(S) \rangle$.*

*Demostración.* Veamos cada una:

*i)* Hemos de ver que $\varphi$ es un homomorfismo biyectivo:

- Sean $\sigma, \tau \in \mathrm{Perm}(X)$, entonces:

$$\varphi(\sigma\tau) = f\sigma\tau f^{-1} \overset{(*)}{=} f\sigma f^{-1} f\tau f^{-1} = \varphi(\sigma)\varphi(\tau)$$

  Donde podemos ver $(*)$ descomponiendo en ciclos disjuntos tanto $\sigma$ como $\tau$ y aplicando la Proposición 1.15.

- Definimos la siguiente aplicación:

$$\begin{array}{rccc} \psi: & \mathrm{Perm}(Y) & \longrightarrow & \mathrm{Perm}(X) \\ & \tau & \longmapsto & f^{-1}\tau f \end{array}$$

  Veamos que $\psi$ es la inversa de $\varphi$:

$$\psi(\varphi(\sigma)) = \psi(f\sigma f^{-1}) = f^{-1}f\sigma f^{-1}f = \sigma$$
$$\varphi(\psi(\tau)) = \varphi(f^{-1}\tau f) = f(f^{-1}\tau f)f^{-1} = \tau$$

  Por tanto, $\varphi$ es biyectiva.

Como $\varphi$ es un homomorfismo biyectivo, es un isomorfismo.

*ii)* La asociatividad viene heredada de la asociatividad de funciones, el neutro del grupo es $id : G \to G$ y como son automorfismos, son aplicaciones biyectivas, con lo que cada una tiene inversa.

*iii)* Por ser $f$ biyectiva, se tiene $|G| = |H|$.

*iv)* Veamos las dos implicaciones:

$\Longrightarrow$) Sean $x, y \in H$:

$$xy = f(f^{-1}(xy)) = f(f^{-1}(x)f^{-1}(y)) = f(f^{-1}(y)f(f^{-1}(x)) = f(f^{-1}(yx)) = yx$$

$\Longleftarrow$) Como $G \cong H \iff H \cong G$, por la propiedad simétrica se tiene la otra implicación.

*v)* Si $O(x) = n$, entonces:

$$(f(x))^n = f(x^n) = f(1) = 1$$

Por tanto, tenemos que $O(f(x)) \leqslant n$. Si suponemos ahora que $\exists m \in \mathbb{N}$ tal que $(f(x))^m = 1$, entonces $f(x^m) = 1 = f(1)$ y por inyectividad tenemos que $x^m = 1$, luego $n \leqslant m$. De todo esto deducimos que $O(f(x)) = n$.

Si $O(x) = +\infty$, basta observar que $f(x^n) = (f(x))^n$ para todo $n \in \mathbb{N} \setminus \{0\}$, para concluir que $O(f(x)) = +\infty$. Si $O(f(x)) = +\infty$, basta usar $f^{-1}$.

*vi)* Sea $y \in H$, buscamos una descomposición de $y$ en función de los elementos $f(s_i)$. Para ello, como $f$ es sobreyectiva, existirá $x \in G$ de forma que $y = f(x)$. Como $G = \langle S \rangle$, tendremos que existen $\gamma_1, \ldots, \gamma_k \in \mathbb{Z}$ de forma que:

$$x = s_1^{\gamma_1} s_2^{\gamma_2} \ldots s_k^{\gamma_k}$$

Luego:

$$y = f(x) = f(s_1^{\gamma_1} s_2^{\gamma_2} \ldots s_k^{\gamma_k}) = f(s_1)^{\gamma_1} f(s_2)^{\gamma_2} \ldots f(s_k)^{\gamma_k}$$

Por lo que $H = \langle f(s_1), f(s_2), \ldots, f(s_n) \rangle = \langle f(S) \rangle$.

□

**Teorema 1.28** (de Dyck)**.** *Sea $G$ un grupo finito con una presentación*

$$G = \langle S \mid R_1, R_2, \ldots, R_k \rangle \qquad S = \{s_1, \ldots, s_m\}$$

*Sea $H$ otro grupo finito con $\{r_1, \ldots, r_m\} \subseteq H$, y supongamos que cualquier relación satisfecha en $G$ por los $s_i$ con $i \in \{1, \ldots, m\}$ es también satisfecha en $H$ para los $r_i$ con $i \in \{1, \ldots, m\}$. Entonces existe un único homomorfismo de grupos $f : G \to H$ de forma que:*

$$f(s_i) = r_i \qquad i \in \{1, \ldots, n\}$$

- *Si además $\{r_1, \ldots, r_m\}$ son un conjunto de generadores de $H$, entonces $f$ es un epimorfismo.*
- *Más aún, si $|G| = |H|$, entonces $f$ es un isomorfismo.*

**Ejemplo.** Usando el Teorema 1.28, podemos dar muchos ejemplos de grupos isomorfos:

1. Si consideramos el grupo cíclico de orden $n$: $C_n = \langle x \mid x^n = 1 \rangle$.

   Observamos que en $\mathbb{Z}_n$ el elemento $\overline{1}$ también verifica la propiedad $x^n = 1$, ya que:

   $$n \cdot \overline{1} = \underbrace{\overline{1} + \ldots + \overline{1}}_{n \text{ veces}} = 0$$

   De esta forma, por el Teorema 1.28, sabemos que existe un homomorfismo $f : C_n \to \mathbb{Z}_n$, de forma que $f(x) = 1$.

   Más aún, como $\mathbb{Z}_n = \langle \overline{1} \rangle$ y $|C_n| = n = |\mathbb{Z}_n|$, tenemos que $f$ es un isomorfismo de grupos, por lo que $C_n \cong \mathbb{Z}_n$.

2. Si ahora consideramos el grupo de Klein abstracto:

$$V^{\text{abs}} = \langle x, y \mid x^2 = y^2 = 1, xy = yx \rangle$$

Podemos intentar relacionarlo con el grupo directo $\mathbb{Z}_2 \times \mathbb{Z}_2$, ya que los elementos $(0,1)$ y $(1,0)$ cumplen las relaciones enunciadas:

$$\begin{aligned} 2 \cdot (0,1) &= (0,1) + (0,1) = (0,0) \\ 2 \cdot (1,0) &= (1,0) + (1,0) = (0,0) \\ (0,1) + (1,0) &= (1,1) = (1,0) + (0,1) \end{aligned}$$

Por lo que existirá un homomorfismo $f : V^{\text{abs}} \to \mathbb{Z}_2 \times \mathbb{Z}_2$ de forma que $f(x) = (0,1)$ y $f(y) = (1,0)$.

Más aún, como $\mathbb{Z}_2 \times \mathbb{Z}_2 = \langle (0,1), (1,0) \rangle$ y es claro que $|\mathbb{Z}_2 \times \mathbb{Z}_2| = 4 = |V^{\text{abs}}|$, tenemos que $f$ es un isomorfismo, por lo que $V^{\text{abs}} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

3. Si tratamos ahora de relacionar el grupo de Klein abstracto (visto en el ejemplo anterior) con el grupo de Klein:

$$V = \langle (1\ 2)(3\ 4), (1\ 3)(2\ 4) \rangle = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

Como $(1\ 2)(3\ 4)$ y $(1\ 3)(2\ 4)$ verifican que:

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

Por el Teorema de Dyck, existe un homomorfismo $g : V^{\text{abs}} \to V$ de forma que $g(x) = (1\ 2)(3\ 4)$ y $g(y) = (1\ 3)(2\ 4)$.

Como hemos visto ya que $V = \langle g(x), g(y) \rangle$ y que $|V^{\text{abs}}| = 4 = |V|$, $g$ es un isomorfismo. Tenemos que $V^{\text{abs}} \cong V$.

Como vimos que $\cong$ es una relación de equivalencia, también tendremos que $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

4. Consideramos ahora el grupo diédrico de orden 3:

$$D_3 = \langle r, s \mid r^3 = 1, s^2 = 1, sr = r^2 s \rangle$$

Que vamos a intentar relacionar con $S_3$. Como $(1\ 2)$ y $(1\ 2\ 3)$ verifican que:

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

Tenemos que existe un homomorfismo $f : D_3 \to S_3$ de forma que $f(r) = (1\ 2\ 3)$ y $f(s) = (1\ 2)$. Como además tenemos que[11] $S_3 = \langle (1\ 2)(1\ 2\ 3) \rangle$ y que $|D_3| = 2 \cdot 3 = 6 = 3! = |S_3|$, concluimos que $f$ es un isomorfismo, por lo que $D_3 \cong S_3$.

[11] Esto se vio en la Proposición 1.20.

5. Si consideramos el grupo lineal de orden 2 sobre $\mathbb{Z}_2$:

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

Y tratamos de relacionarlo con $S_3 = \langle r, s \mid r^3 = 1, s^2 = 1, sr = r^2 s \rangle$, como tenemos que:

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^2 \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Entonces, existe un homomorfismo $f : S_3 \to \mathrm{GL}_2(\mathbb{Z}_2)$ de forma que:

$$f(r) = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \qquad f(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Además, como (ver el Ejercicio **??**):

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

Y ambos tienen el mismo número de elementos, $f$ es un isomorfismo.

6. Fijado $n \in \mathbb{N} \setminus \{0, 3\}$, si ahora consideramos el grupo simétrico de orden $n$, $S_n$ y el grupo diédrico de orden $n$, $D_n$, como $|D_n| = 2n \neq n! = |S_n|$ no vamos a tener un isomorfismo de grupos. Sin embargo, los elementos:

$$(1\ 2\ \ldots\ n), \begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ 1 & n & n-1 & \ldots & 3 & 2 \end{pmatrix} \in S_n$$

Verifican todas las propiedades de la presentación de $D_n$, por lo que existirá un homomorfismo $f : D_n \to S_n$ de forma que

$$f(r) = (1\ 2\ \ldots\ n)$$
$$f(s) = \begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ 1 & n & n-1 & \ldots & 3 & 2 \end{pmatrix}$$

7. Si consideramos ahora:

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

Y pensamos en relacionarlo con $Q_2 = \{\pm 1, \pm i, \pm j, \pm k\}$, como tenemos que:

$$i^4 = 1$$
$$j^2 = -1 = i^2$$
$$ji(-j) = j(-k) = -i$$

Sabemos que existe un homomorfismo $f : Q_2^{\mathrm{abs}} \to Q_2$ de forma que $f(x) = i$ y $f(y) = j$. Además, como $Q_2 = \langle i, j \rangle$ y $|Q_2^{\mathrm{abs}}| = 4 = |Q_2|$, tenemos que $f$ es un isomorfismo, por lo que $Q_2^{\mathrm{abs}} \cong Q_2$.

8. Como último ejemplo, si consideramos $k, n \in \mathbb{N}$, $k \geqslant 3$ con $k \mid n$ y consideramos los grupos diédricos:

$$D_n = \langle r, s \mid r^n = 1, s^2 = 1, sr = r^{-1}s \rangle$$
$$D_k = \langle r_1, s_1 \mid r_1^k = 1, s_1^2 = 1, s_1 r_1 = r_1^{-1} s_1 \rangle$$

Y tratamos de relacionarlos, como $k \mid n$, existirá $p \in \mathbb{N}$ de forma que $n = kp$.

Como $r_1, s_1 \in D_k$ verifican que:

$$r_1^n = r_1^{kp} = (r_1^k)^p = 1^p = 1$$
$$s_1^2 = 1$$
$$s_1 r_1 = r_1^{-1} s_1$$

Tenemos por el Teorema 1.28 que existe un homomorfismo $f : D_n \to D_k$ de forma que $f(r) = r_1$ y $f(s) = s_1$.

## 1.6. Resumen de grupos

Para finalizar este capítulo, haremos un breve repaso de los grupos vistos hasta el momento, ya que los usaremos de forma constante a lo largo de la asignatura, por lo que conviene tenerlos siempre presentes.

**Grupo Trivial.** $(\{e\}, *, e)$.

**Grupos de los enteros módulo $n$.** $(\mathbb{Z}_n, +)$, $(\mathcal{U}(\mathbb{Z}_n), \cdot)$.

**Grupo de raíces $n-$ésimas de la unidad.**

$$\mu_n = \left\{ 1, \xi, \xi^2, \ldots, \xi^{n-1} \mid \xi = \cos\left(\frac{2\pi}{n}\right) + i \operatorname{sen}\left(\frac{2\pi}{n}\right) \right\} \subseteq \mathbb{C}$$

**Grupo lineal de orden $n$.** Sea $\mathbb{F}$ un cuerpo:

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

**Grupo lineal especial de orden $n$.** Sea $\mathbb{F}$ un cuerpo:

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

**Potencias de grupos.** Sea $G$ un grupo y $X$ un conjunto:

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

**$n-$ésimo grupo diédrico.** Sea $n \in \mathbb{N}$:

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

**$n-$ésimo grupo simétrico.** Sea $X$ un conjunto con $|X| = n \in \mathbb{N}$:

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

**$n-$ésimo grupo alternado.** Sea $n \in \mathbb{N}$:

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

**Grupo cíclico de orden $n$.** Sea $n \in \mathbb{N}$:

$$C_n = \langle x \mid x^n = 1\rangle = \{1, x, x^2, x^3, \ldots, x^{n-1}\}$$

**Grupo de los cuaternios.**

$$Q_2 = \{\pm 1, \pm i, \pm j, \pm k\}$$

**Grupo abstracto $Q_2^{\text{abs}}$.**

$$\begin{aligned} Q_2^{\text{abs}} &= \langle x, y \mid x^4 = 1, y^2 = x^2, yxy^{-1} = x^{-1}\rangle \\ &= \{1, x, x^2, x^3, y, yx, yx^2, yx^3\} \end{aligned}$$

**Grupo de Klein.** Sea $n \in \mathbb{N}$ con $n \geqslant 4$:

$$V = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \subseteq S_n$$

**Grupo de Klein abstracto.**

$$V^{\text{abs}} = \langle x, y \mid x^2 = y^2 = 1, xy = yx\rangle = \{1, x, y, xy\}$$

# 2. Subgrupos, Generadores, Retículos y Grupos cíclicos

**Definición 2.1** (Subgrupo)**.** Dados dos grupos $G$ y $H$, decimos que $H$ es un subgrupo de $G$, denotado por $H < G$ si $H \subseteq G$ y la aplicación de inclusión[1] $i : H \to G$ es un homomorfismo de grupos.

*Observación.* Dado un grupo $(G, *, e)$, este tendrá siempre dos subgrupos:

- $(\{e\}, *, e)$, al que llamaremos subgrupo trivial.
- El propio $(G, *, e)$

**Definición 2.2.** Sea $H$ un subgrupo de otro $G$, diremos que $H$ es un subgrupo impropio de $G$ si $H$ es el grupo trivial o el propio $G$. En otro caso, diremos que $H$ es un subgrupo propio de $G$.

**Notación.** Recordamos la notación que ya usábamos en Álgebra I para, fijado $n \in \mathbb{N} \setminus \{0\}$, denotar a todos los múltiplos de $n$ en $\mathbb{Z}$:

$$n\mathbb{Z} = \{nm \mid m \in \mathbb{Z}\}$$

**Ejemplo.** Vemos claramente que:

1. $(\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +)$
2. $\{r^k \mid k \leqslant n, r \in D_n\} < D_n$
3. $n\mathbb{Z} < \mathbb{Z}$ para todo $n \in \mathbb{N}$.
4. $\mathrm{SL}_n(\mathbb{F}) < \mathrm{GL}_n(\mathbb{F})$
5. $(\mathbb{Q}^*, \cdot) \not< (\mathbb{R}, +)$ No es un subgrupo, ya que $i(1) = 1 \neq 0$.
6. $(\mathbb{Z}^+, +) \not< (\mathbb{Z}, +)$, ya que $(\mathbb{Z}^+, +)$ no es un grupo.
7. $D_6 \not< D_8$, ya que $D_6 \not\subseteq D_8$.

*Observación.* Si $G$, $H$ y $T$ son grupos de forma que $G < H < T$, entonces $G < T$.

*Demostración.* La transitividad de $\subseteq$ nos da que $G \subseteq H \subseteq T$. Por otra parte, como las inclusiones $j : G \to H$ y $k : H \to T$ son homomorfismos, tendremos que $i = k \circ j : G \to T$ es un homomorfismo. □

[1] Viene dada por $i(x) = x$, para todo $x \in H$.

**Proposición 2.1.** *Sea $G$ un grupo y $\emptyset \neq H \subseteq G$, entonces son equivalentes:*

*i)* $H < G$

*ii) Se verifican:*

*(a) Si $x, y \in H$ entonces $xy \in H$.*

*(b) $1 \in H$.*

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

*iii) Si $x, y \in H$, entonces $xy^{-1} \in H$.*

*Demostración.* Veamos las implicaciones de forma cíclica:

*i)* $\Longrightarrow$ *ii)* Como $H$ es un grupo, por su definición se han de cumplir $(a)$, $(b)$ y $(c)$.

*ii)* $\Longrightarrow$ *iii)* Si $x, y \in H$, entonces $y^{-1} \in H$, por lo que tendremos que $xy^{-1} \in H$.

*iii)* $\Longrightarrow$ *i)* Como $\emptyset \neq H$, existirá al menos un $x \in H$, por lo que $xx^{-1} = 1 \in H$. Además, si $x \in H$ también tendremos que $1x^{-1} = x^{-1} \in H$. Para ver que $H$ es un grupo, tan solo nos falta ver que su operación interna está bien definida; es decir, que si $x, y \in H$, entonces $xy \in H$. Dados $x, y \in H$, tendremos que $y^{-1} \in H$, por lo que:

$$xy = x(y^{-1})^{-1} \in H$$

Con esto tenemos ya que $H$ es un grupo. Al considerar en $H$ la misma operación que en $G$, tenemos directamente que $i : H \to G$ es un homomorfismo, ya que $id : H \to H$ es un homomorfismo y al extender el codominio para considerar la aplicación inclusión $i$, seguirá siendo un homomorfismo[2].

□

**Proposición 2.2.** *Sea $G$ un grupo finito y $\emptyset \neq H \subseteq G$, entonces son equivalentes:*

*i)* $H < G$

*ii) Si $x, y \in H$, entonces $xy \in H$*

*Demostración.* Veamos las dos implicaciones:

*i)* $\Longrightarrow$ *ii)* Se verifica por ser $H$ un grupo.

*ii)* $\Longrightarrow$ *i)* Como $G$ es finito, por la Proposición 1.9, para todo $x \in G$ existirá $n > 0$ de forma que $x^n = 1$, por lo que $x^{-1} = x^{n-1}$. De esto deducimos que $x^{-1} \in H$ y que $1 = xx^{-1} \in H$. Por la Proposición 2.1, $H < G$.

□

**Ejemplo.** Se deja como ejercicio comprobar que:

1. $A_n < S_n$

[2]Notemos que si en $H$ tenemos una operación distinta que en $G$ esto no siempre será cierto y habrá que comprobar que $i : H \to G$ es un homomorfismo.

2. Todo subgrupo de $\mathbb{Z}$ es de la forma $n\mathbb{Z}$ con $n \in \mathbb{N}$.
3. $V < S_4$
4. Si $n \mid m$, entonces $D_n < D_m$

**Definición 2.3.** Sea $G$ un grupo, $f : G \to G'$ una aplicación, y $H \subseteq G$, $H' \subseteq G'$, definimos:

- El conjunto imagen directa de $H$ por $f$ como el conjunto:

$$f_*(H) = \{f(x) \mid x \in H\} \subseteq G'$$

- El conjunto imagen inversa de $H'$ por $f$ como el conjunto:

$$f^*(H') = \{x \in G \mid f(x) \in H'\} \subseteq G$$

**Proposición 2.3.** *Sea $f : G \to G'$ un homomorfismo de grupos, entonces:*

*i) Si $H < G$, entonces $f_*(H) < G'$*

*ii) Si $H' < G'$, entonces $f^*(H') < G$*

*Demostración.* Demostramos las dos implicaciones:

*i)* Sean $x, y \in f_*(H)$, entonces $\exists a, b \in H$ de forma que $x = f(a), y = f(b)$. Como $H$ es un subgrupo de $G$, tendremos que $ab^{-1} \in H$, por lo que:

$$f(ab^{-1}) = f(a)f(b)^{-1} = xy^{-1} \in f_*(H)$$

Concluimos que $f_*(H)$ es un subgrupo de $G'$.

*ii)* Sean $x, y \in f^*(H')$, entonces $a = f(x), b = f(y) \in H'$. Por ser $H'$ un subgrupo de $G'$, tendremos que

$$ab^{-1} = f(x)f(y)^{-1} = f(xy^{-1}) \in H'$$

Por tanto, $xy^{-1} \in f^*(H')$. Concluimos que $f^*(H')$ es un subgrupo de $G$.

□

**Proposición 2.4.** *Sea $\{H_i\}_{i \in I}$ una familia de subgrupos de $G$, entonces la intersección de todo ellos sigue siendo un subgrupo de $G$:*

$$\bigcap_{i \in I} H_i < G$$

*Demostración.* En primer lugar, como $H_i < G$ para todo $i \in I$, se ha de verificar que $1 \in H_i \ \forall i \in I$, por lo que $1 \in \bigcap_{i \in I} H_i \neq \emptyset$. Como la intersección es no vacía, podemos pensar en aplicar el tercer punto de la Proposición 2.1 para comprobar que es un subgrupo de $G$.

Para ello, sean $x, y \in \bigcap_{i\in I} H_i$, entonces $x, y \in H_i$ para todo $i \in I$, por lo que por ser $H_i < G$, tendremos que $xy^{-1} \in H_i \ \forall i \in I$, luego:

$$xy^{-1} \in \bigcap_{i\in I} H_i$$

Concluimos que $\bigcap_{i\in I} H_i$ es un subgrupo de $G$. □

**Ejemplo.** En general, la unión de subgrupos no es un subgrupo:

$$2\mathbb{Z} \cup 3\mathbb{Z} \not< \mathbb{Z}$$

Ya que $2, 3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$ y $2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$.

## 2.1. Generadores de subgrupos

**Definición 2.4** (Subgrupo generado)**.** Sea $G$ un grupo y $S \subseteq G$, definimos el subgrupo generado por $S$ como el menor subgrupo de $G$ que contiene a $S$, es decir:

$$\langle S\rangle = \bigcap\{H < G \mid S \subseteq H\}$$

*Observación.* Notemos que, gracias a la Proposición 2.4, $\langle S\rangle$ efectivamente es un subgrupo de $G$.

**Proposición 2.5.** *Sea $(G, \cdot, e)$ un grupo, $S \subseteq G$, entonces:*

- *Si $S = \emptyset$, entonces $\langle S\rangle = \{e\}$, el grupo trivial.*
- *Si $S \neq \emptyset$, entonces $\langle S\rangle = \{x_1^{\gamma_1} x_2^{\gamma_2} \dots x_m^{\gamma_m} \mid m \geqslant 1, x_i \in S, \gamma_i \in \mathbb{Z}\}$*

*Demostración.* Distinguimos casos:

- Si $S = \emptyset$, entonces $\{e\} < G$ con $S \subseteq \{e\}$. Como $\{e\}$ solo tiene un elemento y todo subgrupo de $G$ contiene a $e$, concluimos que:

$$\langle S\rangle = \bigcap\{H < G \mid S \subseteq H\} = \{e\}$$

- Si $S \neq \emptyset$, si notamos $\mathcal{S} = \bigcap\{H < G \mid S \subseteq H\}$, queremos ver que:

$$\mathcal{S} = \{x_1^{\gamma_1} x_2^{\gamma_2} \dots x_m^{\gamma_m} \mid m \geqslant 1, x_i \in S, \gamma_i \in \mathbb{Z}\}$$

  $\supseteq$) Como $S \subseteq \mathcal{S}$ y $\mathcal{S}$ es un grupo, tendremos que:

$$x_1^{\gamma_1} x_2^{\gamma_2} \dots x_m^{\gamma_m} \in \mathcal{S} \qquad x_i \in S, \gamma_i \in \mathbb{Z} \quad \forall 1 \leqslant i \leqslant m$$

  $\subseteq$) Si llamamos $A$ al conjunto de la derecha, $A$ es un grupo, ya que si tomamos $a, b \in A$, existirán $x_1, \dots, x_p$ y $y_1, \dots, y_q$ en $S$ y $\gamma_1, \dots, \gamma_p, \alpha_1, \dots, \alpha_q \in \mathbb{Z}$ de forma que:

$$a = x_1^{\gamma_1} \dots x_p^{\gamma_p} \qquad b = y_1^{\alpha_1} \dots y_q^{\alpha_q}$$

  Por lo que

$$ab^{-1} = x_1^{\gamma_1} \dots x_p^{\gamma_p} y_q^{-\alpha_q} \dots y_1^{-\alpha_1} \in A$$

  Lo que demuestra que $A$ es un subgrupo de $G$. Además, como es claro que $S \subseteq A$, tenemos un grupo del que $S$ es subconjunto, por lo que por ser $\mathcal{S}$ el menor subgrupo que contiene a $S$, está claro que $\mathcal{S} \subseteq A$. □

**Corolario 2.5.1.** *Si $S \subseteq G$ de forma que $\langle S \rangle = G$, entonces $S$ es un conjunto de generadores de $G$.*

*Demostración.* Por la Proposición 2.5, sabemos que si $\langle S \rangle = G$, entonces cualquier elemento $x \in G$ se puede expresar de la forma:

$$x = x_1^{\gamma_1} x_2^{\gamma_2} \dots x_m^{\gamma_m} \qquad x_i \in S, \gamma_i \in \mathbb{Z}, \quad \forall 1 \leqslant i \leqslant m$$

Por lo que $S$ es un conjunto de generadores de $G$. □

**Ejemplo.** Ejemplos interesantes de subgrupos generados por ciertos conjuntos son:

1. Si $S = \{r\} \subseteq D_n$, entonces $\langle S \rangle = \{1, r, r^2, \dots, r^{n-1}\}$
2. Si $S = \{s\} \subseteq D_n$, entonces $\langle S \rangle = \{1, s\}$
3. Si $S = \{(1\ 2)(3\ 4), (1\ 3)(2\ 4)\} \subseteq S_4$, entonces $\langle S \rangle = V$
4. Si $S = \{(x_1\ x_2\ x_3) \mid x_1 < x_2 < x_3\} \subseteq S_n$, entonces $\langle S \rangle = A_n$
5. Si $S = \left\{ \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\} \subseteq \mathrm{GL}_2(\mathbb{C})$, entonces $\langle S \rangle < \mathrm{GL}_2(\mathbb{C})$.

En la Proposición 2.4 vimos que la intersección de una familia arbitraria de subgrupos era un subgrupo, mientras que con el ejemplo de $2\mathbb{Z} \cup 3\mathbb{Z} \subseteq \mathbb{Z}$, vimos que, en general, la unión de dos subgrupos no es un subgrupo. Sin embargo, cabe preguntarse de qué forma podemos hacer una operación parecida con subgrupos para sí obtener un subgrupo. De esto nace la siguiente definición.

**Definición 2.5** (Compuesto)**.** Sea $\{H_i\}_{i \in I}$ una familia de subgrupos de un grupo $G$, llamamos compuesto de los subgrupos $H_i$, denotado por $\bigvee\limits_{i \in I} H_i$, al subgrupo:

$$\bigvee_{i \in I} H_i = \left\langle \bigcup_{i \in I} H_i \right\rangle$$

Cuando tengamos un número finito de subgrupos $\{H_1, H_2, \dots, H_n\}$, notaremos:

$$H_1 \vee H_2 \vee \dots \vee H_n$$

Notemos que es natural la definición, ya que como la unión de subgrupos no es en general un subgrupo, buscamos el menor subgrupo que contenga a la unión de subgrupos, que por definición es el compuesto de la familia de subgrupos que queríamos unir.

## 2.2. Retículo de subgrupos de un grupo

Introduciremos ahora el concepto de retículo[3], estructura algebraica de gran interés que usaremos brevemente para trabajar de forma cómoda con el conjunto de todos los subgrupos de un grupo.

[3]Que en el contexto de teoría de conjuntos o del orden puede tener otra definición.

**Definición 2.6** (Retículo)**.** Un retículo es una tripleta $(L, \vee, \wedge)$ donde:

- $L$ es un conjunto no vacío.
- $\wedge$ y $\vee$ son dos operaciones[4] binarias en $L$ que verifican las leyes:

  *i*) Conmutativa:
  $$a \vee b = b \vee a \qquad a \wedge b = b \wedge a$$

  *ii*) Asociativa:
  $$a \vee (b \vee c) = (a \vee b) \vee c \qquad a \wedge (b \wedge c) = (a \wedge b) \wedge c$$

  *iii*) de Absorción:
  $$a \vee (a \wedge b) = a \qquad a \wedge (a \vee b) = a$$

  *iv*) de Idempotencia:
  $$a \vee a = a \qquad a \wedge a = a$$

En el caso de que $(L, \vee, \wedge)$ sea un retículo, es común definir una relación binaria notada por "$\leqslant$" y definida por:

$$a \leqslant b \iff a \vee b = b \iff a \wedge b = a$$

donde para la segunda equivalencia hemos empleado la conmutatividad y la propiedad de absorción.

**Proposición 2.6.** *Todo retículo $(L, \vee, \wedge)$ junto con la relación de orden $\leqslant$ que se define a partir de sus operaciones es un conjunto parcialmente ordenado.*

*Demostración.* Hemos de probar las propiedades:

- Reflexiva. Por la propiedad de idempotencia, dado $a \in L$, tenemos que:
  $$a \vee a = a \Longrightarrow a \leqslant a$$

- Antisimétrica. Sean $a, b \in L$ de forma que $a \leqslant b$ y $b \leqslant a$. Por definición de $\leqslant$, tenemos que:
  $$a \vee b = b \qquad b \vee a = a$$
  Y aplicando la conmutatividad de $\vee$ llegamos a que:
  $$a = a \vee b = b \vee a = b$$

- Transitiva. Sean $a, b, c \in L$ de forma que $a \leqslant b$ y $b \leqslant c$, es decir, $a \vee b = b$ y $b \vee c = c$, entonces:
  $$a \vee c = a \vee (b \vee c) = (a \vee b) \vee c = b \vee c = c$$
  De donde deducimos que $a \leqslant c$.

□

[4]Es común referirse a $\vee$ por "supremo" y a $\wedge$ por "ínfimo".

**Ejemplo.** Ejemplos de retículos son:

1. El retículo endoplasmático rugoso.
2. Dado un número $n \in \mathbb{N}$, el conjunto de divisores de $n$:

$$D(n) = \{m \in \mathbb{N} : m \text{ divide a } n\}$$

   Junto con las operaciones de:

$$a \vee b = \text{mcm}(a, b)$$
$$a \wedge b = \text{mcd}(a, b)$$

   forma un retículo[5]. En este, la relación de orden que obtenemos es la de "ser divisor de"; es decir, si $a, b \in D(n)$, entonces:

$$a \leqslant b \iff a \mid b$$

3. En la asignatura LMD vimos que los álgebras de Boole eran retículos.

**Lema 2.7.** *Sea $G$ un grupo y $T, U < G$, entonces:*

$$\langle \langle T \rangle \cup U \rangle = \langle T \cup U \rangle$$

*Demostración.* Haǵamoslo por doble inclusión:

$\supseteq$) Basta ver que:

$$T \subseteq \langle T \rangle \Longrightarrow T \cup U \subseteq \langle T \rangle \cup U \Longrightarrow \langle T \cup U \rangle \subseteq \langle \langle T \rangle \cup U \rangle$$

$\subseteq$) Sea $x \in \langle \langle T \rangle \cup U \rangle$, entonces existirán $\alpha_1, \ldots, \alpha_n \in \langle T \rangle$, $u_1, \ldots, u_m \in U$ y $\gamma_1, \ldots, \gamma_{n+m} \in \mathbb{Z}$ de forma que:

$$x = \alpha_1^{\gamma_1} \ldots \alpha_n^{\gamma_n} u_1^{\gamma_{n+1}} \ldots u_m^{\gamma_{n+m}}$$

Pero por ser $\alpha_1, \ldots, \alpha_n \in \langle T \rangle$, podemos encontrar $t_{ij} \in T$ y $\delta_{ij} \in \mathbb{Z}$ de forma que:

$$\alpha_1 = t_{11}^{\delta_{11}} \ldots t_{1n_1}^{\delta_{1n_1}}$$
$$\vdots$$
$$\alpha_n = t_{n1}^{\delta_{n1}} \ldots t_{nn_n}^{\delta_{nn_n}}$$

Por lo que:

$$x = t_{11}^{\delta_{11}} \ldots t_{1n_1}^{\delta_{1n_1}} \ldots t_{nn_n}^{\delta_{nn_n}} u_1^{\gamma_{n+1}} \ldots u_m^{\gamma_{n+m}} \in \langle T \cup U \rangle$$

□

[5]Es un buen ejercicio comprobarlo.

**Proposición 2.8.** *Sea $G$ un grupo, si definimos el conjunto de subgrupos de $G$:*

$$\Lambda = \{H \subseteq G \mid H < G\}$$

*Se verifica que $\Lambda$ es un retículo, junto con las operaciones:*

$$T \vee U = \langle T \cup U \rangle$$
$$T \wedge U = T \cap U$$

*Demostración.* De Álgebra I ya sabemos que la intersección de conjuntos es conmutativa, asociativa y que tiene la propiedad de idempotencia. Veamos estas para el compuesto de dos subgrupos, que se deducen a partir de las propiedades conmutativa, asociativa y de idempotencia para la unión de dos conjuntos:

- Conmutativa. Sean $T, U \in \Lambda$:

$$T \vee U = \langle T \cup U \rangle = \langle U \cup T \rangle = U \vee T$$

- Asociativa. Sean $T, U, V \in \Lambda$:

$$T \vee (U \vee V) = T \vee \langle U \cup V \rangle = \langle T \cup \langle U \cup V \rangle \rangle \overset{(*)}{=} \langle T \cup U \cup V \rangle$$
$$\overset{(*)}{=} \langle \langle T \cup U \rangle \cup V \rangle = \langle T \cup U \rangle \vee V = (T \vee U) \vee V$$

  Donde en $(*)$ hemos aplicado el Lema anterior.

- Idempotencia. Sea $T \in \Lambda$:

$$T \vee T = \langle T \cup T \rangle = \langle T \rangle \overset{(*)}{=} T$$

  Donde en $(*)$ hemos usado que $T$ es un grupo, por ser subgrupo de $G$.

Finalmente, nos queda comprobar las propiedades de absorción. Para ello, sean $T, U \in \Lambda$:

$$T \vee (T \cap U) = \langle T \cup (T \cap U) \rangle = \langle (T \cup T) \cap (T \cup U) \rangle = \langle T \cap (T \cup U) \rangle = \langle T \rangle = T$$
$$T \cap (T \vee U) = T \cap \langle T \cup U \rangle = T$$

□

Al trabajar con retículos, una estructura que surge de forma natural son los diagramas de Hasse, que nos permiten comprender mucho mejor la estructura de un retículo concreto.

**Definición 2.7** (Diagrama de Hasse)**.** Sea $(L, \leqslant)$ un conjunto finito parcialmente ordenado, definimos su diagrama de Hasse como el grafo dirigido $(V, E)$ donde:

- Los vértices son cada uno de los elementos de $L$, es decir: $V = L$.

- Dados dos vértices $a, b \in V$ con $a \neq b$, tendremos una arista de $a$ a $b$ ($a \to b$) si $a \leqslant b$ y no existe ningún elemento $c \in V$ con $a \neq c \neq b$ de forma que $a \leqslant c \leqslant b$.

  Es decir, escribiremos $a \to b$ en el caso en el que $a \leqslant b$, obviando los ciclos (ya que $\leqslant$ es una relación simétrica) y las relaciones que puedan deducirse de la transitividad de $\leqslant$: si $a \leqslant b$ y $b \leqslant c$, no consideraremos la arista $a \to c$.

**Notación.** Por comodidad y claridad a la hora de dibujar los diagramas de Hasse, no dibujaremos grafos dirigidos, sino que lo que haremos será ordenar los vértices por "niveles": colocaremos abajo del todo los vértices que son menores o iguales que todos los demás (colocando en un mismo nivel aquellos elementos que no son comparables entre sí[6]). En el nivel inmediatamente superior a este, colocaremos los elementos que son menores o iguales a todos los demás salvo a estos últimos. Repetiremos el proceso de forma sucesiva, hasta colocar en el último nivel aquellos elementos que son mayores o iguales que todos los demás.

De esta forma, tendremos el diagrama de Hasse ordenado por niveles, donde podremos ver "qué tan grande" es cada elemento. Además, no necesitaremos dibujar las aristas dirigidas, ya que dibujaremos aristas no dirigidas pensando que todas las aristas están dirigidas hacia arriba.

### 2.2.1. Ejemplos

**Ejemplo.** Diagramas de Hasse para ciertos retículos[7] son:

1. Para $D(30) = \{1, 2, 3, 5, 6, 10, 15, 30\}$:

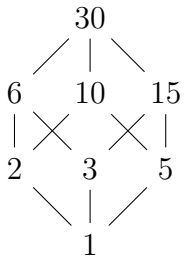



Figura 2.1: Diagragama de Hasse para $D(30)$.

2. Para $\mathcal{B}^3$, el álgebra de Boole con 3 elementos, tenemos:

[6] Ya que no tenemos por qué tener un orden total.

[7] Notemos que cualquier retículo es un conjunto parcialmente ordenado.

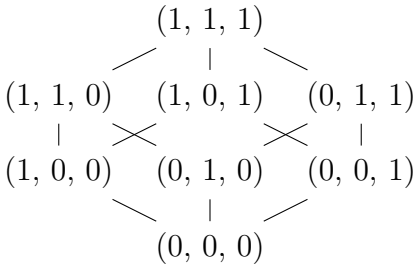



Figura 2.2: Diagragama de Hasse para $\mathcal{B}^3$.

Centrándonos ya en los retículos que nos interesan, daremos a continuación varios ejemplos de retículos de los retículos formados por los subgrupos de un grupo dado, que representaremos mediante sus diagramas de Hasse (en estos aparecerán las aristas etiquetadas con números, que por ahora ignoraremos, pero que luego señalaremos lo que significan).

**Ejemplo.** Veamos varios ejemplos con grupos de la forma $\mathbb{Z}_n$:

1. Para calcular el retículo de subgrupos de $\mathbb{Z}_4$, hemos de pensar primero en todos los subgrupos posibles de $\mathbb{Z}_4$. Para ello, vemos que:

$$\begin{aligned}\langle 0\rangle &= \{0\}\\ \langle 1\rangle &= \mathbb{Z}_4\\ \langle 2\rangle &= \{0,2\}\\ \langle 3\rangle &= \mathbb{Z}_4\end{aligned}$$

   Concluimos que $\Lambda_{\mathbb{Z}_4} = \{\{0\}, \{0,2\}, \mathbb{Z}_4\}$. Pasamos ahora a ver cómo se relacionan mediante su diagrama de Hasse.

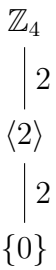



Figura 2.3: Diagrama de Hasse para los subgrupos de $\mathbb{Z}_4$.

2. En $\mathbb{Z}_6$ tenemos que[8]:

$$\begin{aligned}\langle 1\rangle = \langle 5\rangle &= \mathbb{Z}_6\\ \langle 2\rangle = \langle 4\rangle &= \{0,2,4\}\\ \langle 3\rangle &= \{0,3\}\end{aligned}$$

[8]Hemos escrito directamente los subgrupos de $\mathbb{Z}_6$, pero lo que hemos hecho para buscarlos todos es pensar en todos los posibles conjuntos de generadores.

Y podemos dibujar su diagrama de Hasse:

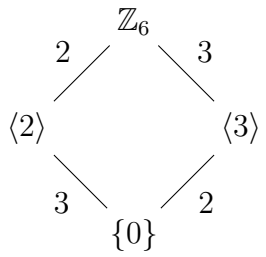



Figura 2.4: Diagrama de Hasse para los subgrupos de $\mathbb{Z}_6$.

3. En $\mathbb{Z}_8$, tenemos que:

$$\begin{aligned} \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle &= \mathbb{Z}_8 \\ \langle 2 \rangle = \langle 6 \rangle &= \{0, 2, 4, 6\} \\ \langle 4 \rangle &= \{0, 4\} \end{aligned}$$

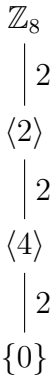



Figura 2.5: Diagrama de Hasse para los subgrupos de $\mathbb{Z}_8$.

4. En $\mathbb{Z}_{12}$, tenemos:

$$\begin{aligned} \langle 1 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 11 \rangle &= \mathbb{Z}_{12} \\ \langle 2 \rangle = \langle 10 \rangle &= \{0, 2, 4, 6, 8, 10\} \\ \langle 3 \rangle = \langle 9 \rangle &= \{0, 3, 6, 9\} \\ \langle 4 \rangle = \langle 8 \rangle &= \{0, 4, 8\} \\ \langle 6 \rangle &= \{0, 6\} \end{aligned}$$

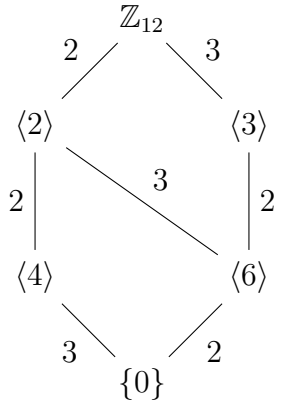



Figura 2.6: Diagrama de Hasse para los subgrupos de $\mathbb{Z}_{12}$.

**Ejemplo.** Si trabajamos ahora con otro tipo de grupos:

1. Si consideramos el grupo de Klein:

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

Todos sus subgrupos posibles son:

$$V, \langle (1\ 2)(3\ 4)\rangle, \langle (1\ 3)(2\ 4)\rangle, \langle (1\ 4)(2\ 3)\rangle, \{1\}$$

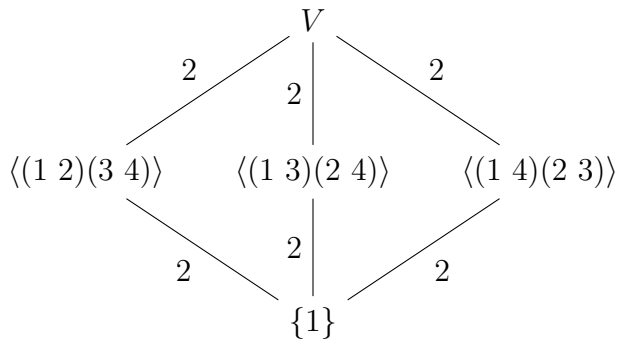



Figura 2.7: Diagrama de Hasse para los subgrupos del grupo de Klein.

2. En el grupo de los cuaternios:

$$Q_2 = \{\pm 1, \pm i, \pm j, \pm k\}$$

Los subgrupos posibles son:

$$Q_2, \langle i\rangle, \langle j\rangle, \langle k\rangle, \langle -1\rangle, \{1\}$$

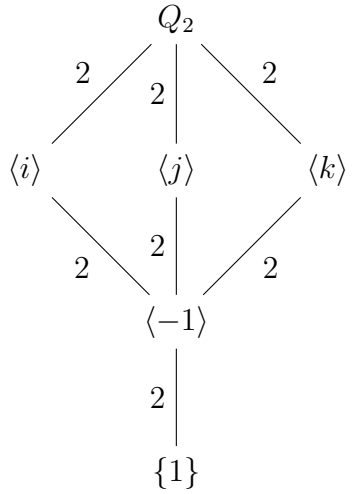



Figura 2.8: Diagrama de Hasse para los subgrupos del grupo de los cuaternios.

3. En $S_3 = \{1, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$, los posibles subgrupos son:

$$S_3, \langle(1\ 2\ 3)\rangle, \langle(1\ 2)\rangle, \langle(1\ 3)\rangle, \langle(2\ 3)\rangle, \{1\}$$

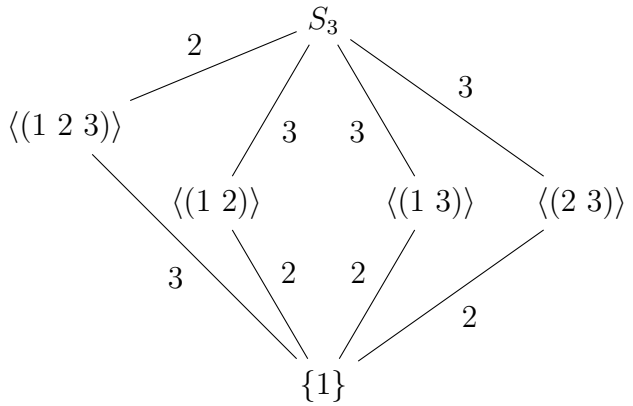



Figura 2.9: Diagrama de Hasse para los subgrupos de $S_3$.

4. En $D_4 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$, los posibles subgrupos son:

$$\begin{aligned}
\langle r\rangle = \langle r^3\rangle &= \{1, r, r^2, r^3\}\\
\langle r^2\rangle &= \{1, r^2\}\\
\langle s\rangle &= \{1, s\}\\
\langle sr\rangle &= \{1, sr\}\\
\langle sr^2\rangle &= \{1, sr^2\}\\
\langle sr^3\rangle &= \{1, sr^3\}\\
\langle r^2, s\rangle &= \{1, r^2, s, sr^2\}\\
\langle r^2, sr\rangle &= \{1, r^2, sr, sr^3\}
\end{aligned}$$

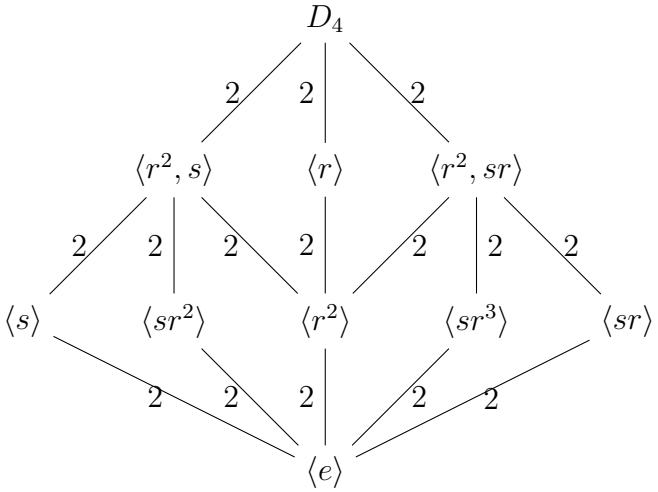



Figura 2.10: Diagrama de Hasse para los subgrupos de $D_4$.

**Ejemplo.** Obtenemos un ejemplo interesante al considerar los grupos:

$$G = \langle x, y \mid x^8 = y^2 = 1, xy = yx\rangle$$
$$H = \langle u, v \mid u^2 = v^8 = 1, vu = uv^5\rangle$$

Donde $H$ recibe el nombre de "grupo modular de orden 16", notemos que ambos grupos tienen orden 16. Además, como $G$ es conmutativo y $H$ no, sabemos que no pueden ser isomorfos. Sin embargo, sucede algo particular cuando consideramos sus diagramas de Hasse. Antes de ello, debemos calcular todos los subgrupos de cada uno, cosa que no vamos a detallar pero sí daremos aquellos subgrupos más grandes:

- $G$ tiene 3 subgrupos de orden 8: $\langle x^2, y\rangle$, $\langle x\rangle$, $\langle xy\rangle$.
- $H$ tiene 3 subgrupos de orden 8: $\langle u, v^2\rangle$, $\langle u\rangle$, $\langle uv\rangle$.

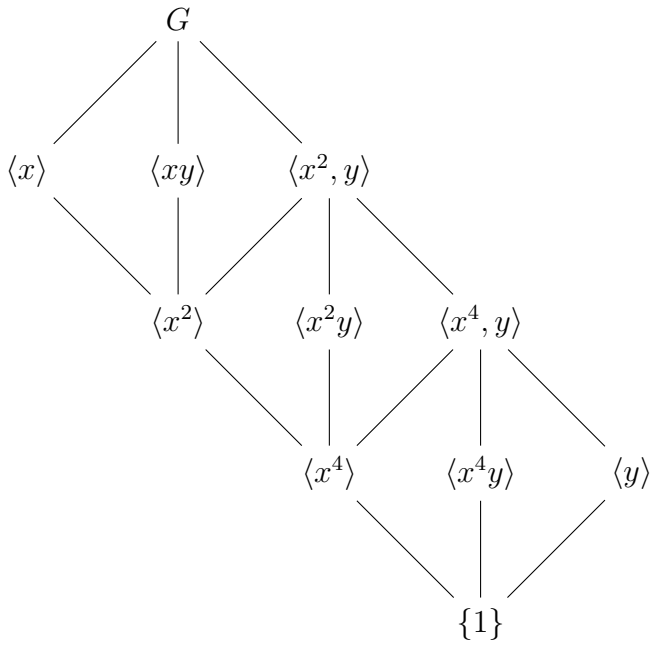



Figura 2.11: Diagrama de Hasse para los subgrupos de $G$.

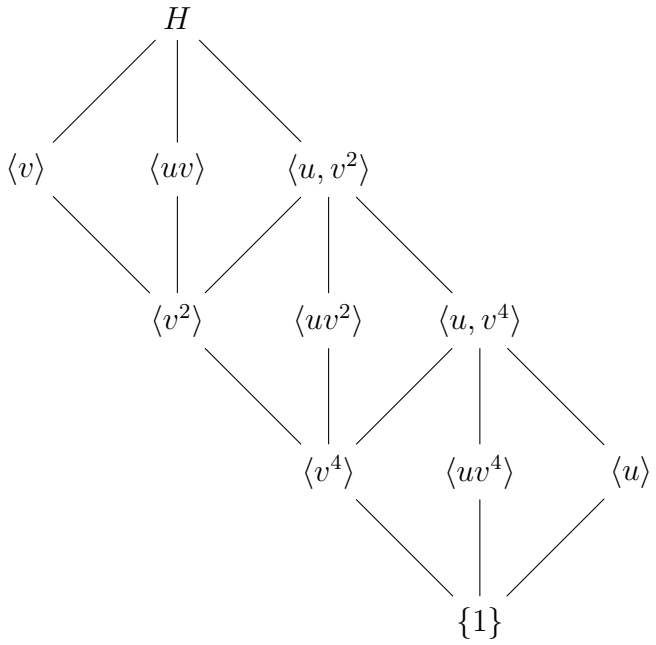



Figura 2.12: Diagrama de Hasse para los subgrupos de $H$.

A lo largo de todos estos ejemplos hemos debido darnos cuenta de una particularidad, que se pone de manifiesto especialmente en el ejemplo de los $\mathbb{Z}_n$. Resulta que los órdenes de los subgrupos que hemos ido obteniendo dividían al orden del grupo, resultado que luego demostraremos en general. Sin embargo, estamos ya en condiciones de demostrar que el contrarrecíproco no es cierto en general, es decir, no todos los divisores del orden de un grupo se corresponden con el orden de algún subgrupo suyo.

**Proposición 2.9.** *El orden del subgrupo divide al orden del grupo, pero no todos los divisores del orden del grupo se corresponden con el orden de algún subgrupo suyo.*

Veremos que el orden de todo subgrupo divide al orden del grupo (en caso de ser el grupo finito) en el Teorema de Lagrange (Teorema 2.13).

**Ejemplo.** Para ver que el recíproco no se cumple, consideramos:

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

Que recordamos tiene de orden:

$$|A_4| = \frac{4!}{2} = 4 \cdot 3 = 12$$

Y todos los posibles divisores de 12 son:

$$D(12) = \{1, 2, 3, 4, 6, 12\}$$

Sin embargo, $A_4$ tiene:

- Un subgrupo de orden 1, $\{1\}$.

- Cuatro subgrupos de orden 3.
- Un subgrupo de orden 4, $V < A_4$.
- Tres subgrupos de orden 2.
- Un subgrupo de orden 12, $A_4$.

Más aún, veamos que es imposible que tenga un subgrupo de orden 6.

*Demostración.* Supongamos que existe $H < A_4$ de forma que $|H| = 6$. En dicho caso, viendo todos los elementos de $A_4$, concluimos que $H$ debe contener al menos un 3−ciclo:

$$(x_1\ x_2\ x_3) \in H$$

En dicho caso, por ser $H$ un subgrupo de $A_4$, también debe estar su elemento inverso:

$$(x_1\ x_3\ x_2) \in H$$

Ahora, distingamos casos:

- Si $H$ no tiene más 3−ciclos, la única posibilidad (observando nuevamente todos los elementos de $A_4$) es que $H$ sea de la forma:

  $$H = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (x_1\ x_2\ x_3), (x_1\ x_3\ x_2)\}$$

  En cuyo caso, observemos que $V < H$. Sin embargo, $|V| = 4 \nmid 6 = |H|$, contradicción.

- Si $H$ tiene otro 3−ciclo, por ejemplo $(x_1\ x_2\ x_4)$, también ha de contener a su inverso, por lo que:

  $$\{(x_1\ x_2\ x_3), (x_1\ x_3\ x_2), (x_1\ x_2\ x_4), (x_1\ x_4\ x_2)\} \subseteq H$$

  Sin embargo, como:

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

  Concluimos que también $(x_1\ x_4\ x_3)$ y su inverso: $(x_1\ x_3\ x_4)$ deben estar en $H$, luego $H$ es un subgrupo formado por 6 3−ciclos, contradicción, ya que $H$ debe también contener al 1.

Concluimos que no puede existir un subgrupo de $A_4$ con 6 elementos. □

## 2.3. Índice y Teorema de Lagrange

**Definición 2.8.** Sea $G$ un grupo, $H, K < G$, definimos:

$$HK = \{hk \mid h \in H, k \in K\}$$

**Proposición 2.10.** *Sea $G$ un grupo, $H, K < G$, tenemos que $HK$ es un subgrupo de $G$ si y solo si $HK = KH$. En cuyo caso, tendremos que:*

$$HK = H \vee K$$

*Demostración.* Por doble implicación:

$\Longrightarrow$) Veamos que $KH = HK$ por doble inclusión:

$\subseteq$) Sean $k \in K, h \in H$, tenemos que:

$$kh = (h^{-1}k^{-1})^{-1} \in HK \Longrightarrow KH \subseteq HK$$

$\supseteq$) Observemos que la única hipótesis que tenemos es que $HK$ es un subgrupo de $G$ (nada tenemos sobre $KH$). Sean $h \in H, k \in K$:

$$hk = (k^{-1}h^{-1})^{-1} \in HK$$

Por lo que $k^{-1}h^{-1} \in HK$, luego existirán $h_1 \in H$, $k_1 \in K$ de forma que:

$$k^{-1}h^{-1} = h_1k_1$$

Finalmente:

$$hk = (k^{-1}h^{-1})^{-1} = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH$$

$\Longleftarrow$) Sean $hk, h_1k_1 \in HK$, queremos ver qué pasa con $hk(h_1k_1)^{-1}$:

$$hk(h_1k_1)^{-1} = hkk_1^{-1}h_1^{-1} \overset{(*)}{=} hk_2h_2 \overset{(**)}{=} hh_3k_3 \in HK$$

Donde:

- En $(*)$ hemos aplicado que $K$ es un grupo, ya que si $k, k_1 \in K$, entonces $kk_1^{-1} \in K$, por lo que existirá $k_2 = kk_1^{-1} \in K$.
  De forma análoga, como $h_1 \in H$, tenemos que $h_1^{-1} \in H$, por lo que existirá $h_2 = h_1^{-1} \in H$.
- En $(**)$ hemos aplicado que $k_2h_2 \in KH = HK$, por lo que existirán $h_3 \in H$, $k_3 \in K$ de forma que $k_2h_2 = h_3k_3$.

Falta ver que si $HK < G$ con $HK = KH$ (que ya sabemos que son equivalentes), entonces:

$$HK = H \vee K$$

$\subseteq$) Sea $x \in HK$, entonces $\exists h \in H, k \in K$ de forma que $x = hk \in \langle H \cup K \rangle = H \vee K$.

$\supseteq$) Sea $x \in H \vee K$, entonces sabemos que existen $\alpha_1, \ldots, \alpha_n \in H \cup K$ y $\gamma_1, \ldots, \gamma_n \in \mathbb{Z}$ de forma que:

$$x = \alpha_1^{\gamma_1} \ldots \alpha_n^{\gamma_n}$$

Como $HK = KH$, tras varias conmutaciones de términos, existirán $h_1, \ldots, h_p \in H$, $k_{p+1}, \ldots, k_n \in K$ y $\delta_1, \ldots, \delta_n \in \mathbb{Z}$ de forma que:

$$x = h_1^{\delta_1} \ldots h_p^{\delta_p} k_{p+1}^{\delta_{p+1}} \ldots k_n^{\delta_n}$$

Y por ser $H$ y $K$ grupos, tendremos que existen $h \in H$ y $k \in K$ de forma que:

$$h = h_1^{\delta_1} \ldots h_p^{\delta_p}$$
$$k = k_{p+1}^{\delta_{p+1}} \ldots k_n^{\delta_n}$$

Por lo que $x = hk \in HK$. $\square$

**Definición 2.9.** Sea $G$ un grupo y $H < G$, definimos dos relaciones binarias en $G$:

- La relación ${}_H\sim$ definida por:

$$y \,{}_H\!\sim\, x \iff x^{-1}y \in H$$

- La relación $\sim_H$ definida por:

$$y \sim_H x \iff yx^{-1} \in H$$

**Proposición 2.11.** *Sea $G$ un grupo y $H < G$, se verifica que ${}_H\sim$ y $\sim_H$ son relaciones de equivalencia en $G$. Además, dado $x \in G$, se tiene que sus clases de equivalencia*[9] *son de la forma:*

$$ {}_H[x] = \{xh \mid h \in H\}$$
$$ [x]_H = \{hx \mid h \in H\}$$

*Demostración.* Comprobemos primero que ${}_H\sim$ y $\sim_H$ son relaciones de equivalencia:

- Propiedad reflexiva. Como $H$ es un grupo, $1 \in H$, por lo que dado $x \in G$:

$$xx^{-1} = x^{-1}x = 1 \in H$$

  De donde deducimos que $x \sim_H x$ y $x \,{}_H\!\sim\, x$, de forma respectiva.

- Propiedad simétrica. Sean $x, y \in G$:

  - Si $x \,{}_H\!\sim\, y$, entonces $y^{-1}x \in H$, pero por ser $H$ un grupo, también tendremos:
$$(y^{-1}x)^{-1} = x^{-1}y \in H$$
    De donde deducimos que $y \,{}_H\!\sim\, x$.
  - Si $x \sim_H y$, entonces $xy^{-1} \in H$, y por ser $H$ un grupo:
$$(xy^{-1})^{-1} = yx^{-1} \in H$$
    De donde deducimos que $y \sim_H x$.

- Propiedad transitiva. Sean $x, y, z \in G$:

  - Si $x \,{}_H\!\sim\, y$ y $y \,{}_H\!\sim\, z$, entonces: $y^{-1}x, z^{-1}y \in H$ y por ser $H$ un grupo, deducimos que:
$$(z^{-1}y)(y^{-1}x) = z^{-1}x \in H$$
    De donde $x \,{}_H\!\sim\, z$.
  - Si $x \sim_H y$ y $y \sim_H z$, entonces $xy^{-1}, yz^{-1} \in H$ y por ser $H$ un grupo:
$$(xy^{-1})(yz^{-1}) = xz^{-1} \in H$$
    De donde $x \sim_H z$.

[9] Que denotaremos por ${}_H[x]$ y por $[x]_H$ respectivamente.

Concluimos que ${}_H\sim$ y $\sim_H$ son relaciones de equivalencia en $G$. Falta comprobar las igualdades:

$$ {}_H[x] \overset{(1)}{=} \{xh \mid h \in H\} $$
$$ [x]_H \overset{(2)}{=} \{hx \mid h \in H\} $$

1. Sean $x, y \in G$, tenemos que:

$$ x \, {}_H\sim y \iff y^{-1}x \in H \iff \exists h \in H \text{ con } y^{-1}x = h \iff \exists h \in H \text{ con } y^{-1} = hx^{-1} $$
$$ \iff \exists h \in H \text{ con } y = xh^{-1} \iff \exists h' \in H \text{ con } y = xh' $$

   Concluimos que se cumple (1).

2. Sean $x, y \in G$:

$$ x \sim_H y \iff xy^{-1} \in H \iff \exists h \in H \text{ con } xy^{-1} = h \iff \exists h \in H \text{ con } y = h^{-1}x $$
$$ \iff \exists h' \in H \text{ con } y = hx $$

   Concluimos que también se cumple (2).

□

**Definición 2.10.** Sea $G$ un grupo y $H < G$:

- Si consideramos la relación ${}_H\sim$, dado $x \in G$, definimos la clase lateral por la izquierda de $G$ en $H$ definida por $x$ a la clase de equivalencia de $x$ por la relación de equivalencia ${}_H\sim$, que denotamos por:

$$ xH = \{xh \mid h \in H\} $$

  De esta forma, tendremos que el conjunto cociente dado por la relación es de la forma:

$$ G/{}_H\sim \; = \{xH \mid x \in G\} $$

- Si consideramos ahora la relación $\sim_H$, dado $x \in G$, definimos la clase lateral por la derecha de $G$ en $H$ definida por $x$ a la clase de equivalencia de $x$ por la relación de equivalencia $\sim_H$, denotada por:

$$ Hx = \{hx \mid h \in H\} $$

  Y consideraremos el conjunto cociente:

$$ G/\sim_H = \{Hx \mid x \in G\} $$

**Ejemplo.** En $S_3 = \{1, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$, si consideramos como $H$:

$$ H = \langle (1\ 2) \rangle = \{1, (1\ 2)\} $$

Podemos calcular todas las clases laterales por la izquierda de $G$ en $H$ si consideramos la relación ${}_H\sim$:

$$\begin{aligned}
1H &= \{1\cdot 1, 1(1\ 2)\} = \{1, (1\ 2)\} = H\\
(1\ 2)H &= \{(1\ 2)1, (1\ 2)(1\ 2)\} = \{(1\ 2), 1\} = H\\
(1\ 3)H &= \{(1\ 3)1, (1\ 3)(1\ 2)\} = \{(1\ 3), (1\ 2\ 3)\}\\
(2\ 3)H &= \{(2\ 3)1, (2\ 3)(1\ 2)\} = \{(2\ 3), (1\ 3\ 2)\}\\
(1\ 2\ 3)H &= \{(1\ 2\ 3)1, (1\ 2\ 3)(1\ 2)\} = \{(1\ 2\ 3), (1\ 3)\} = (1\ 3)H\\
(1\ 3\ 2)H &= \{(1\ 3\ 2)1, (1\ 3\ 2)(1\ 2)\} = \{(1\ 3\ 2), (2\ 3)\} = (2\ 3)H
\end{aligned}$$

Por lo que el conjunto cociente $G/{}_H\sim$ vendrá dado por:

$$G/{}_H\sim = \{H, (1\ 3)H, (2\ 3)H\}$$

Si ahora calculamos todas las clases laterales por la derecha de $G$ en $H$, considerando la relación $\sim_H$, entonces:

$$\begin{aligned}
H1 &= \{1\cdot 1, (1\ 2)1\} = \{1, (1\ 2)\} = H\\
H(1\ 2) &= \{1(1\ 2), (1\ 2)(1\ 2)\} = \{(1\ 2), 1\} = H\\
H(1\ 3) &= \{1(1\ 3), (1\ 2)(1\ 3)\} = \{(1\ 3), (1\ 3\ 2)\}\\
H(2\ 3) &= \{1(2\ 3), (1\ 2)(2\ 3)\} = \{(2\ 3), (1\ 2\ 3)\}\\
H(1\ 2\ 3) &= \{1(1\ 2\ 3), (1\ 2)(1\ 2\ 3)\} = \{(1\ 2\ 3), (2\ 3)\} = H(2\ 3)\\
H(1\ 3\ 2) &= \{1(1\ 3\ 2), (1\ 2)(1\ 3\ 2)\} = \{(1\ 3\ 2), (1\ 3)\} = H(1\ 3)
\end{aligned}$$

Por lo que el conjunto cociente $G/\sim_H$ vendrá dado por:

$$G/\sim_H = \{H, H(1\ 3), H(2\ 3)\}$$

**Proposición 2.12.** *Sea $G$ un grupo, $H < G$ y $x \in G$, entonces:*

*i)* $x \in xH$ *y* $x \in Hx$.

*ii)* *Los conjuntos $H$, $xH$ y $Hx$ son biyectivos.*

*iii)* *Los conjuntos cocientes $G/{}_H\sim$ y $G/\sim_H$ son biyectivos.*

*Demostración.* Veamos cada una de ellas:

*i)* Como $H$ es un grupo, tendremos que $1 \in H$, por lo que:

$$x = x\cdot 1 \in xH \qquad x = 1\cdot x \in Hx$$

*ii)* Sean $f : xH \longrightarrow H$, $g : H \longrightarrow Hx$ dadas por:

$$\begin{aligned}
f(xh) &= h \qquad \forall xh \in xH\\
g(h) &= hx \qquad \forall h \in H
\end{aligned}$$

Es fácil comprobar que $f$ y $g$ son biyectivas, por lo que $xH$ es biyectivo con $H$ y $H$ es biyectivo con $Hx$. Basta considerar $g \circ f$ para obtener una biyección de $xH$ con $Hx$.

*iii*) Sea $f : G/_{H}\sim \longrightarrow G/\sim_H$ dada por:

$$f(xH) = Hx^{-1} \qquad \forall xH \in G/_{H}\sim$$

En primer lugar, hemos de ver que $f$ está bien definida. Para ello, sean $x, y \in G$ de forma que $xH = yH$, entonces $x \,{}_{H}\!\sim y$, luego $y^{-1}x \in H$, pero por ser $H$ un grupo:

$$(y^{-1}x)^{-1} = x^{-1}y \in H \Longrightarrow x^{-1} \sim_H y^{-1}$$

Por lo que $Hx^{-1} = Hy^{-1}$, luego $f$ está bien definida. Finalmente, es fácil ver que $f$ es biyectiva. □

**Definición 2.11** (Índice de un grupo en un subgrupo)**.** Sea $G$ un grupo y $H < G$, en la Proposición 2.12, vimos que:

$$|G/_{H}\sim| = |G/\sim_H|$$

Los cardinales de estos conjuntos recibirán el nombre de índice de $G$ en $H$, y los denotaremos por $[G : H]$.

**Ejemplo.** En los diagramas de Hasse de las Figuras 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9 y 2.10, los números que dibujábamos en las aristas de los diagramas de Hasse eran los índices de los grupos en los respectivos subgrupos marcados por la arista. Por ejemplo, en la Figura 2.9, observamos que $[S_3 : \langle(1\ 2)\rangle] = 3$.

Otro ejemplo puede ser el anterior, donde considerábamos en $S_3$ el conjunto:

$$H = \langle(1\ 2)\rangle = \{1, (1\ 2)\}$$

En esta situación, teníamos que $[S_3 : H] = |G/\sim_H| = |G/_{H}\sim| = 3$.

**Teorema 2.13** (de Lagrange)**.** *Sea $G$ un grupo finito y $H < G$, entonces:*

$$|G| = [G : H]|H|$$

*Observemos que a partir de esta igualdad deducimos que $|H|$ divide a $|G|$.*

*Demostración.* Como $_{H}\sim$ es una relación de equivalencia, tenemos una partición de $G$ a partir de las clases de equivalencia dadas por esta relación:

$$G = \bigcup_{x\in G} xH$$

Como $G$ es finito, habrá un número finito de clases de equivalencia. Si elegimos un elemento en cada una de estas, tendremos un conjunto con cada uno de los representantes de las clases $\{x_1, x_2, \ldots, x_n\}$, con lo que:

$$|G| = |x_1H| + |x_2H| + \ldots + |x_nH| \overset{(*)}{=} n|H|$$

Donde en $(*)$ hemos usado la Proposición 2.12, ya que como $xH$ es biyectivo con $H$ para cualquier $x \in G$, concluimos que $|x_iH| = |x_1H|$ para todo $i \in \{1, \ldots, n\}$. Sin embargo, $n$ es el número de clases de equivalencia distintas del conjunto cociente, es decir, $n = [G : H]$, con lo que:

$$|G| = [G : H]|H|$$

□

*Observación.* Notemos que a partir del Teorema de Lagrange podemos deducir resultados ya vistos y demostrados, como por ejemplo, la Proposición 1.22, donde deducíamos el orden de los grupos $|\operatorname{SL}_n(\mathbb{F})|$, pero resulta que $[\operatorname{GL}_n(\mathbb{F}) : \operatorname{SL}_n(\mathbb{F})] = q-1$ si $|\mathbb{F}| = q$, por lo que:

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

**Corolario 2.13.1.** *Sea $G$ un grupo finito, el orden de cualquier elemento de $G$ divide a $|G|$.*

*Demostración.* Sea $x \in G$, basta ver que $O(x) = |\langle x \rangle|$. Sin embargo, por la Proposición 1.9, ya vimos que por ser $G$ un grupo finito, entonces $\exists n \in \mathbb{N} \setminus \{0\}$ de forma que $O(x) = n$. En esta misma Proposición vimos que entonces $x$ tenía $n$ potencias distintas, por lo que:

$$\langle x \rangle = \{1, x, x^2, \ldots, x^{n-1}\} \Longrightarrow |\langle x \rangle| = n$$

Basta aplicar el Teorema de Lagrange, puesto que $\langle x \rangle < G$. □

**Corolario 2.13.2.** *Sea $G$ un grupo finito y $K < H < G$, entonces:*

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

*Demostración.* Por el Teorema de Lagrange, sabemos que:

$$\left.\begin{aligned} |G| &= [G : K]|K| \\ |G| = [G : H]|H| &= [G : H][H : K]|K| \end{aligned}\right\} \Longrightarrow [G : K] = [G : H][H : K]$$

□

## 2.4. Propiedades de grupos cíclicos

Terminaremos este capítulo repasando varias propiedades de los grupos cíclicos que debemos conocer, no sin antes recordar la definición de un grupo cíclico. Decimos que un grupo $G$ es cíclico si $\exists a \in G$ de forma que $G = \langle a \rangle$. En cuyo caso, todos los elementos de $G$ serán potencias de $a$: si $x \in G$, existirá $n \in \mathbb{N}$ de forma que $x = a^n$.

Antes de continuar, recordamos una propiedad de los grupos cíclicos: sea $G = \langle a \rangle$ un grupo cíclico, entonces:

$$|G| = O(a)$$

**Proposición 2.14.** *Si $G$ es un grupo con $|G| = p$ primo, entonces $G$ es cíclico.*

*Demostración.* Sea $a \in G$, $a \neq 1$ (como $p$ es primo, $p \geqslant 2$), observamos que:

$$\{1\} \neq \langle a \rangle < G$$

Por el Teorema de Lagrange, $1 \neq |\langle a \rangle|$ divide a $|G|$, pero $p$ es primo, por lo que $|\langle a \rangle| = p$ y ha de ser $\langle a \rangle = G$. □

**Lema 2.15.** *Sea $G$ un grupo, $a \in G$, existe un homomorfismo de grupos*

$$\varphi_a : \mathbb{Z} \to G$$

*De forma que $\varphi_a(1) = a$ y $Im(\varphi_a) = \{a^n \mid n \in \mathbb{Z}\} = \langle a \rangle$.*

*Demostración.* Definimos $\varphi_a$ como la aplicación:

$$\varphi_a(n) = a^n \qquad \forall n \in \mathbb{Z}$$

Es claro que $\varphi_a(1) = a$ y que $Im(\varphi_a) = \{a^n \mid n \in \mathbb{Z}\} = \langle a \rangle$. Falta ver que $\varphi_a$ es un homomorfismo. Para ello:

$$\varphi_a(n+m) = a^{n+m} = a^n a^m = \varphi_a(n)\varphi_a(m) \qquad \forall n, m \in \mathbb{Z}$$

□

**Teorema 2.16.** *Sea $G$ un grupo cíclico, entonces:*

- *Si $G$ es infinito, $G \cong \mathbb{Z}$.*
- *Si $|G| = n$, $G \cong \mathbb{Z}_n$.*

*Demostración.* Como $G$ es cíclico, existirá $a \in G$ de forma que $\langle a \rangle = G$. El Lema anterior nos da una aplicación $\varphi_a : \mathbb{Z} \to G$ sobreyectiva, veamos cómo conseguir la inyectividad:

- Si $G$ es infinito, entonces ha de ser $O(a) = +\infty$, por lo que $\nexists n \in \mathbb{N} \setminus \{0\}$ de forma que $\varphi_a(n) = a^n = 1$, por lo que:

  $$\ker(\varphi_a) = \{0\} \Longrightarrow \varphi_a \text{ inyectiva}$$

  Concluimos que $G \cong \mathbb{Z}$.

- Si $G$ es finito y tiene cardinal $n \in \mathbb{N} \setminus \{0\}$, entonces tendremos que $O(a) = n$, por lo que $\varphi_a(n) = a^n = 1$ y $\varphi_a$ no será inyectiva por ser $\{0, n\} \subseteq \ker(\varphi_a)$. Sin embargo, podemos definir la aplicación $\psi_a : \mathbb{Z}_n \to G$ dada por $\psi_a(\overline{r}) = a^r$ para todo $\overline{r} \in \mathbb{Z}_n$:

  - $\psi_a$ está bien definida, ya que si $\overline{r}, \overline{s} \in \mathbb{Z}_n$ de forma que $\overline{r} = \overline{s}$, entonces:

    $$r - s \in n\mathbb{Z} \Longrightarrow \exists t \in \mathbb{Z} \text{ con } a^{r-s} = a^{nt} = (a^n)^t = 1 \Longrightarrow a^r = a^s$$

  - $\psi_a$ es un homomorfismo:

    $$\psi_a(\overline{r} + \overline{s}) = a^{r+s} = a^r a^s = \psi_a(\overline{r})\psi_a(\overline{s}) \qquad \forall \overline{r}, \overline{s} \in \mathbb{Z}_n$$

  - $\psi_a$ es inyectiva, ya que si $\overline{r} \in \mathbb{Z}_n$ con $\psi_a(\overline{r}) = a^r = 1$, entonces $n \mid r$, luego $\overline{r} = \overline{0}$ y se tiene que:

    $$\ker(\psi_a) = \{\overline{0}\}$$

  - Como $\langle a \rangle = G$ y $|G| = n = O(a)$, está claro que $\psi_a$ es sobreyectiva.

  Por todo esto, concluimos que $\psi_a$ es un isomorfismo, luego $G \cong \mathbb{Z}_n$.

□

**Proposición 2.17.** *Sea $G = \langle a \rangle$ un grupo cíclico con $O(a) = n$, entonces para cada divisor $m$ de $n$, existe un único subgrupo de $G$ de orden $m$, el subgrupo cíclico $\langle a^{\frac{n}{m}} \rangle$. Además, estos son los únicos subgrupos de $G$.*

*Demostración.* Sea $m$ un divisor de $n$, veamos que $\langle a^{\frac{n}{m}} \rangle$ es un grupo cíclico de orden $m$. Para ello, veamos que $O\left(a^{\frac{n}{m}}\right) = m$:

- En primer lugar, tenemos que:

$$(a^{\frac{n}{m}})^m = a^n = 1$$

- Sea $t \in \mathbb{N} \setminus \{0\}$ de forma que:

$$(a^{\frac{n}{m}})^t = 1 \Longrightarrow n \mid \frac{nt}{m}$$

  En cuyo caso, existe $r \in \mathbb{N}$ de forma que:

$$\frac{nt}{m} = rn \Longrightarrow t = rm \Longrightarrow m \mid t$$

Concluimos que $O(a^{\frac{n}{m}}) = m$. Ahora, si $H < G$, nos gustaría probar que si $|H| = m$, entonces:

$$H = \langle a^{\frac{n}{m}} \rangle$$

En primer lugar, observemos que si $H < G$, por el Teorema de Lagrange tenemos que $m \mid n$. Para ver la igualdad, sea:

$$k = \text{mín}\{t \in \mathbb{N} \setminus \{0\} \mid a^t \in H\}$$

Veamos que $H = \langle a^k \rangle$:

$\supseteq$) Se tiene por la definición de $k$.

$\subseteq$) Sea $b \in H < G = \langle a \rangle$, entonces $\exists s \in \mathbb{N}$ de forma que $b = a^s$. Si dividimos $s$ entre $k$, tenemos que $\exists q, r \in \mathbb{N}$ de forma que:

$$s = kq + r \qquad 0 \leqslant r < k$$

Y por ser $a^s, a^k \in H$, vemos que:

$$a^r = a^s a^{-kq} \in H$$

Por esto, concluimos que $r = 0$, ya que $k$ era el menor que cumplía esta propiedad, por lo que $s = kq$ y:

$$b = (a^k)^q \in \langle a^k \rangle$$

Falta ahora ver que $k = {}^n\!/_m$. Como $H$ es un grupo, tenemos que $a^n = 1 \in H$, por lo que $k \mid n$ por la Proposición 1.8. De aquí deducimos que:

$$m = |H| = O(a^k) = \frac{n}{k} \Longrightarrow k = \frac{n}{m}$$

□

*Observación.* De la Proposición anterior, deducimos que dado $G$ un grupo cíclico con $|G| = n$, entonces la aplicación $\phi : Div(n) \to \Lambda_G$ con:

$$\Lambda_G = \{H \subseteq G \mid H < G\}$$

dada por:

$$\phi(m) = \left\langle a^{\frac{n}{m}} \right\rangle \qquad \forall m \in Div(n)$$

Es una biyección.

**Ejemplo.** A partir de esta última observación, es muy fácil calcular todos los subgrupos de cualquier grupo cíclico, ya que el problema se reduce a estudiar todos los divisores del orden del grupo. Ilustramos el procedimiento con el grupo cíclico de orden 12:

$$C_{12} = \langle x \mid x^{12} = 1 \rangle$$

Tenemos que:

$$Div(12) = \{1, 2, 3, 4, 6, 12\}$$

Y usando nuestra aplicación $\phi$, podemos listar todos los subgrupos de $C_{12}$:

$$\begin{aligned}
1 &\overset{\phi}{\longmapsto} \left\langle x^{\frac{12}{1}} \right\rangle = \langle x^{12} \rangle = \langle 1 \rangle = \{1\} \\
2 &\longmapsto \left\langle x^{\frac{12}{2}} \right\rangle = \langle x^6 \rangle = \{1, x^6\} \\
3 &\longmapsto \left\langle x^{\frac{12}{3}} \right\rangle = \langle x^4 \rangle = \{1, x^4, x^8\} \\
4 &\longmapsto \left\langle x^{\frac{12}{4}} \right\rangle = \langle x^3 \rangle = \{1, x^3, x^6, x^9\} \\
6 &\longmapsto \left\langle x^{\frac{12}{6}} \right\rangle = \langle x^2 \rangle = \{1, x^2, x^4, x^6, x^8, x^{10}\} \\
12 &\longmapsto \left\langle x^{\frac{12}{12}} \right\rangle = \langle x \rangle = C_{12}
\end{aligned}$$

Por lo que su diagrama de Hasse será de la forma:

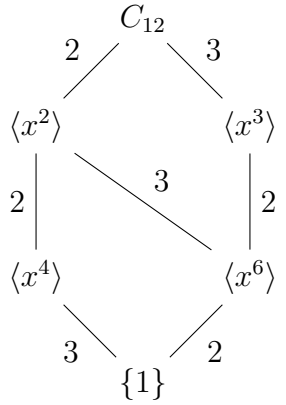



Figura 2.13: Diagrama de Hasse para los subgrupos de $C_{12}$.

**Corolario 2.17.1.** *Si tenemos un grupo cíclico de orden $p^n$ con $p$ primo, entonces todos sus subgrupos serán cíclicos y de orden $p^r$, con $0 \leqslant r \leqslant n$.*

**Proposición 2.18.** *Sea $G$ un grupo, $a \in G$ con $O(a) = n$ y $k \in \mathbb{N} \setminus \{0\}$, entonces:*

$$\langle a^k \rangle = \langle a^d \rangle \qquad \text{siendo } d = \text{mcd}(n, k)$$

*En cuyo caso, $O(a^k) = \dfrac{n}{d}$.*

*Demostración.* Por doble inclusión:

$\subseteq$) Como $d \mid k$, tenemos que $k = dt$ para cierto $t$, luego $a^k = a^{dt} \in \langle a^d \rangle$.

$\supseteq$) Como $d = \text{mcd}(n, k)$, entonces la ecuación:

$$nX + kY = d$$

tiene solución[10], por lo que existen $u, v \in \mathbb{N}$ de forma que $nu + kv = d$, luego:

$$a^d = a^{nu} a^{kv} = \cancel{(a^n)^u}^{1} (a^k)^v \in \langle a^k \rangle$$

Para ver que $O(a^k) = {}^n\!/_d$, como $\langle a^k \rangle = \langle a^d \rangle$, tenemos que $O(a^k) = O(a^d)$ y como:

- Tenemos que:
$$(a^d)^{\frac{n}{d}} = a^n = 1$$
- Si $t \in \mathbb{N}$ de forma que:
$$(a^d)^t = 1 \Longrightarrow n \mid dt \Longrightarrow \frac{n}{d} \mid t$$

Concluimos que $O(a^k) = O(a^d) = {}^n\!/_d$. □

**Ejemplo.** Por ejemplo, ¿por qué en $\mathbb{Z}_{12}$ el subgrupo generado por el 8 coincide con el generado por el 4? Porque $4 = \text{mcd}(8, 12)$.

**Corolario 2.18.1.** *Sea $G$ un grupo y $a \in G$ con $O(a) = n$, entonces:*

$$\langle a^p \rangle = \langle a^q \rangle \Longleftrightarrow \text{mcd}(n, p) = \text{mcd}(n, q)$$

**Corolario 2.18.2.** *Sea $G = \langle a \rangle$ un grupo cíclico con $O(a) = n$, entonces:*

$$G = \langle a^k \rangle \Longleftrightarrow \text{mcd}(k, n) = 1$$

*Es decir, el número de generadores de $G$ es $\varphi(n)$, siendo $\varphi$ la función de Euler:*

$$\varphi(n) = \{k \in \mathbb{N} \mid \text{mcd}(k, n) = 1\}$$

**Ejemplo.** En $\mathbb{Z}_{12}$:

$$\mathbb{Z}_{12} = \langle \overline{1} \rangle = \langle \overline{5} \rangle = \langle \overline{7} \rangle = \langle \overline{11} \rangle$$

[10] Se vió en Álgebra I, se trata de la Identidad de Bezout.

# 3. Relaciones de Ejercicios

# 3.1. Subgrupos, Generadores, Retículos y Grupos cíclicos

**Ejercicio 3.1.1.** Describir todos los elementos de los grupos alternados $A_n$, consistentes en las permutaciones pares del $S_n$ correspondiente, para:

1. $n = 2$.

$$S_2 = \{1, (1\ 2)\}$$
$$A_2 = \{1\}$$

2. $n = 3$.

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

3. $n = 4$.

$$\begin{aligned} S_4 = \{&1, (1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4), (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 2), (1\ 3\ 4),\\ &(1\ 4\ 2), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3), (1\ 2\ 3\ 4), (1\ 2\ 4\ 3), (1\ 3\ 2\ 4),\\ &(1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}\\ A_4 = \{&1, (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 2), (1\ 3\ 4), (1\ 4\ 2), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3),\\ &(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \end{aligned}$$

**Ejercicio 3.1.2.** Sea $D_n$ el grupo diédrico. Demostrar que el subgrupo de $D_n$ generado por los elementos $\{r^j s, r^k s\}$ es todo el grupo $D_n$ siempre que $0 \leqslant j < k < n$ y $\text{mcd}(k - j, n) = 1$.

Haciendo uso de que $D_n = \langle r, s\rangle$, veamos que:

$$\langle r^j s, r^k s\rangle = D_n$$

$\subseteq$) Como $r, s \in D_n$, entonces $r^j s, r^k s \in D_n$. Por ser $D_n$ un grupo, en particular es cerrado para el producto y para inversos, por lo que $\langle r^j s, r^k s\rangle \subseteq D_n$.

$\supseteq$) Veamos en primer lugar que $r \in \langle r^j s, r^k s\rangle$. Sabemos que:

$$(r^j s)^{-1} = s r^{-j} \in \langle r^j s, r^k s\rangle$$

Por tanto, como $r^k s \in \langle r^j s, r^k s\rangle$, entonces:

$$r^k s (r^j s)^{-1} = r^k s s r^{-j} = r^{k-j} \in \langle r^j s, r^k s\rangle$$

Como $\text{mcd}(k - j, n) = 1$, entonces existe $m \in \mathbb{Z}$, con $0 \leqslant m < n$, tal que $m(k - j) = qn + 1$ para algún $q \in \mathbb{Z}$. Por tanto:

$$(r^{k-j})^m = r^{m(k-j)} = r^{qn+1} = r \in \langle r^j s, r^k s\rangle$$

Por último, veamos que $s \in \langle r^j s, r^k s\rangle$. Como $r \in \langle r^j s, r^k s\rangle$, entonces:

$$r^{n-j} r^j s = r^{n-j+j} s = s \in \langle r^j s, r^k s\rangle$$

Por tanto, $r, s \in \langle r^j s, r^k s\rangle$, y por ser $D_n = \langle r, s\rangle$, entonces $D_n \subset \langle r^j s, r^k s\rangle$.

**Ejercicio 3.1.3.**

1. Demostrar que el subgrupo de $\mathrm{SL}_2(\mathbb{Z}_3)$ generado por los elementos

$$i = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad j = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

es isomorfo al grupo cuaternio $Q_2$.

Por la propiedad transitiva de la isomorfia, basta con encontrar un isomorfismo entre $\mathrm{SL}_2(\mathbb{Z}_3)$ y:

$$Q_2^{abs} = \langle x, y \mid x^4 = 1,\ y^2 = x^2,\ yx = x^{-1}y \rangle$$

Comprobamos que $i, j$ cumplen las relaciones de $Q_2^{abs}$:

$$\begin{aligned} i^2 &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \\ j^2 &= \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \\ ji &= \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} \\ i^3 j &= \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} \end{aligned}$$

Por tanto, $i, j$ cumplen las relaciones de $Q_2^{abs}$. Por el Teorema de Teorema de Dyck, existe un único homomorfismo $f : Q_2^{abs} \to \langle i, j \rangle$ tal que $f(x) = i$ y $f(y) = j$.

- Como $i, j \in \langle i, j \rangle$ son un generador de $\langle i, j \rangle$, entonces se trata de un epimorfismo.
- Para terminar de ver que es un isomorfismo, basta con comprobar que $|Q_2^{abs}| = |\langle i, j \rangle|$. Sabemos que:

$$\begin{aligned} \langle i, j \rangle &= \{1, i, i^2, i^3, j, ij, i^2 j, i^3 j\} \\ |Q_2^{abs}| &= 8 = |\langle i, j \rangle| \end{aligned}$$

  Por tanto, $f$ es un isomorfismo.

Por tanto, $\langle i, j \rangle \cong Q_2^{abs} \cong Q_2$.

2. Demostrar que $\mathrm{SL}_2(\mathbb{Z}_3)$ y $S_4$ son dos grupos de orden 24 que no son isomorfos.

*Observación.* Demostrar que $S_4$ no puede contener a ningún subgrupo isomorfo a $Q_2$.

Tenemos que:

$$Q_2 = \{\pm 1, \pm i, \pm j, \pm k\}$$

Los órdenes de los elementos de $Q_2$ son:

$$O(\pm i) = O(\pm j) = O(\pm k) = 4 \qquad O(-1) = 2$$

Supongamos ahora $\exists H \leqslant S_4$ tal que $H \cong Q_2$. Por lo pronto, sabemos que $1 \in H$ y $|H| = 8$. Además, como los isomorfismos mantienen los órdenes, sabemos que en $H$ habrá 6 elementos distintos de orden 4 y 1 de orden 2. Como en $S_4$ tan solo hay 6 elementos de orden 4, entonces $H$ ha de contener a todos los elementos de orden 4 de $S_4$; es decir:

$$\{1, (1\ 2\ 3\ 4), (1\ 2\ 4\ 3), (1\ 3\ 2\ 4), (1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2)\} \subseteq H$$

Por tanto, ya tenemos 7 elementos de $H$, y sabemos que el restante es de orden 2 (no sabemos si es una transposición o un producto de dos transposición disjuntas). Por ser $H$ un grupo, tenemos que es cerrado para productos, por lo que:

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

No obstante, hemos encontrado un elemento de orden 3 perteneciente a $H$, lo cual es una contradicción. Por tanto, no puede existir un subgrupo de $S_4$ isomorfo a $Q_2$.

Para demostrar lo pedido, supongamos que $\exists f : \mathrm{SL}_2(\mathbb{Z}_3) \to S_4$ un isomorfismo, y consideramos la restricción a $Q = \langle i, j \rangle \cong Q_2$. Sabemos que la siguiente aplicación es un isomorfismo:

$$\begin{array}{rccc} f_{\big|_Q}: & Q & \longrightarrow & f_*(Q) \\ & x & \longmapsto & f(M) \end{array}$$

Por tanto, $Q_2 \cong Q \cong f_*(Q)$. Además, como $f_*$ es un homomorfismo y se tiene $Q < \mathrm{SL}_2(\mathbb{Z}_3)$, entonces $f_*(Q) < S_4$. Por tanto, hemos encontrado un subgrupo de $S_4$ isomorfo a $Q_2$, lo cual es una contradicción por lo que hemos demostrado anteriormente. Por tanto, $\mathrm{SL}_2(\mathbb{Z}_3) \ncong S_4$.

**Ejercicio 3.1.4.** Razonar que un subconjunto no vacío $X \subseteq G$ de un grupo $G$ es un subgrupo de $G$ si, y sólo si, $X = \langle X \rangle$.

$\Longrightarrow$) Supongamos que $X$ es un subgrupo de $G$, y veamos que $X = \langle X \rangle$.

$\subseteq$) Por definición de subgrupo generado por un conjunto, $X \subseteq \langle X \rangle$.

$\supseteq$) Veamos que $\langle X \rangle \subseteq X$. Dado $x \in \langle X \rangle$, entonces $x$ es una combinación de elementos de $X$ mediante el producto y el inverso. Por ser $X$ un subgrupo, en particular es un grupo, por lo que es cerrado para el producto y para inversos. Por tanto, $x \in X$.

Por tanto, $X = \langle X \rangle$.

$\Longleftarrow$) Supongamos que $X = \langle X \rangle$, y veamos que $X$ es un subgrupo de $G$. Por definición, $\langle X \rangle$ es el menor subgrupo de $G$ que contiene a $X$. Por tanto, $X$ es un subgrupo de $G$.

**Ejercicio 3.1.5.** Sean $a, b \in G$ dos elementos de un grupo que conmutan entre sí, esto es, para los que $ab = ba$, y de manera que sus órdenes son primos relativos, esto es, $\text{mcd}(O(a), O(b)) = 1$.

1. Razonar que $\langle a \rangle \cap \langle b \rangle = \{1\}$.

   Puesto que la intersección de dos subgrupos es un subgrupo, sabemos que $\langle a \rangle \cap \langle b \rangle$ es un subgrupo de $G$, y por tanto $1 \in \langle a \rangle \cap \langle b \rangle \neq \emptyset$. Por tanto, podemos considerar $x \in \langle a \rangle \cap \langle b \rangle$.

   Como menciona el $\text{mcd}(O(a), O(b))$, podemos considerar que ambos órdenes son finitos. Por el Teorema de Lagrange, sabemos que:

   $$|\langle a \rangle \cap \langle b \rangle| \mid |\langle a \rangle| = O(a)$$
   $$|\langle a \rangle \cap \langle b \rangle| \mid |\langle b \rangle| = O(b)$$

   Por tanto, $|\langle a \rangle \cap \langle b \rangle|$ es divisor común de $O(a)$ y $O(b)$, y por ser $\text{mcd}(O(a), O(b)) = 1$, entonces $|\langle a \rangle \cap \langle b \rangle| = 1$. Por tanto, $\langle a \rangle \cap \langle b \rangle = \{1\}$.

2. Demostrar que $O(ab) = O(a)O(b)$.

   Puesto que conmutan, tenemos que:

   $$(ab)^k = a^k b^k \qquad \forall k \in \mathbb{Z}$$

   Por comodidad, sean $O(a) = n$ y $O(b) = m$.

   $$(ab)^{nm} = a^{nm} b^{nm} = (a^n)^m (b^m)^n = 1$$

   Supongamos ahora $t \in \mathbb{N}$ tal que $(ab)^t = 1$.

$$1 = (ab)^t = a^t b^t \implies a^t = b^{-t} \in \langle a \rangle \cap \langle b \rangle = \{1\} \implies \left\{ \begin{array}{l} a^t = 1 \Longrightarrow n \mid t \\ a^t = 1 \Longrightarrow m \mid t \end{array} \right\} \overset{(*)}{\Longrightarrow} nm \mid t$$

   donde en $(*)$ hemos usado que $\text{mcd}(n, m) = 1$. Por tanto:

   $$O(ab) = nm = O(a)O(b)$$

**Ejercicio 3.1.6.** Encontrar un grupo $G$ y elementos $a, b \in G$ tales que sus órdenes sean primos relativos, pero para los que no se verifique la igualdad $O(ab) = O(a)O(b)$ del ejercicio anterior.

En primer lugar, hemos de tener que no conmuten. Por tanto, consideremos el grupo $S_3$ y los elementos:

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

Tenemos que $O(a) = 2$ y $O(b) = 3$, y por tanto $\text{mcd}(O(a), O(b)) = 1$. Además, $O(a)O(b) = 6$. Supongamos que $\exists \sigma \in S_3$ tal que $O(\sigma) = 6$. Por tanto, el mínimo común múltiplo de los ciclos disjuntos que la descomponen debe ser 6. Sin embargo, esto no es posible, porque en $S_3$ tan solo hay elementos de orden 1, 2 y 3. Por tanto, $O(ab) \neq O(a)O(b)$.

**Ejercicio 3.1.7.** Sea $G$ un grupo y $a, b \in G$ dos elementos de orden finito. ¿Es $ab$ necesariamente de orden finito?

*Observación.* Considerar el grupo $\mathrm{GL}_2(\mathbb{Q})$ y los elementos

$$a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad b = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}.$$

Calculemos el orden de $a$ y $b$:

$$a^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I_2 \implies O(a) = 4$$
$$b^2 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$$
$$b^3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I_2 \implies O(b) = 6$$

Calculamos ahora el orden de $ab$. Por inducción, demostraremos que:

$$(ab)^n = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$$

- Caso base: $n = 1$.

$$(ab)^1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$$

- Supuesto cierto para $n$, demostramos para $n+1$:

$$(ab)^{n+1} = (ab)^n(ab) = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -(n+1) \\ 0 & 1 \end{pmatrix}$$

Por tanto, como en $(ab)^n \neq I_2$ para todo $n \in \mathbb{N}$, entonces $O(ab) = \infty$.

**Ejercicio 3.1.8.** En el grupo $S_3$ se considera el conjunto

$$H = \{1, (1\ 2\ 3), (1\ 3\ 2)\}.$$

1. Demostrar que $H$ es un subgrupo de $S_3$.

   Por ser $S_3$ finito, tan solo hemos de comprobar que $H$ es cerrado para el producto. Como vimos, no es necesario comprobar si uno de los elementos es el neutro.

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

   Por tanto, $H < S_3$.

2. Describir las diferentes clases de $S_3$ módulo $H$.

   Por el Teorema de Lagrange, sabemos que:

$$|S_3| = [S_3 : H] \cdot |H| \Longrightarrow [S_3 : H] = \frac{6}{3} = 2 \Longrightarrow |S_3/_H\!\sim| = |S_3/\sim_H| = 2$$

   Calculamos ahora las clases de equivalencia de $S_3/_H\!\sim$:

$$1H = \{1x \mid x \in H\} = \{1, (1\ 2\ 3), (1\ 3\ 2)\} = H$$
$$(1\ 2)H = \{(1\ 2)x \mid x \in H\} = \{(1\ 2), (1\ 2)(1\ 2\ 3), (1\ 2)(1\ 3\ 2)\} = \{(1\ 2), (2\ 3), (1\ 3)\} \neq H$$

   Como ya hemos encontrado dos clases de equivalencia distintas, entonces hemos encontrado todas las posibles.

$$S_3/_H\!\sim = \{H, (1\ 2)H\}$$

   Calculamos ahora las clases de equivalencia de $S_3/\sim_H$:

$$H1 = \{x1 \mid x \in H\} = \{1, (1\ 2\ 3), (1\ 3\ 2)\} = H$$
$$H(1\ 2) = \{x(1\ 2) \mid x \in H\} = \{(1\ 2), (1\ 2\ 3)(1\ 2), (1\ 3\ 2)(1\ 2)\} = \{(1\ 2), (1\ 3), (2\ 3)\} \neq H$$

   Por tanto, hemos encontrado todas las clases de equivalencia de $S_3/\sim_H$.

$$S_3/\sim_H = \{H, H(1\ 2)\}$$

**Ejercicio 3.1.9.** Sea $G$ un grupo finito.

1. Demostrar que si $H \leqslant G$ es un subgrupo, entonces $[G : H] = |G|$ si, y sólo si, $H = \{1\}$, mientras que $[G : H] = 1$ si, y sólo si, $H = G$.

   Demostremos en primer lugar que $[G : H] = |G| \iff H = \{1\}$. Por el Teorma de Lagrange, sabemos que $|G| = [G : H] \cdot |H|$. Por tanto:

$$[G : H] = \frac{|G|}{|H|} = |G| \iff |G| = |G|\,|H| \iff |H| = 1 \iff H = \{1\}$$

   donde, desde el inicio, hemos usado que $|G|, |H| \neq 0$.

   De nuevo, por el Teorema de Lagrange, sabemos que $|G| = [G : H] \cdot |H|$. Por tanto:

$$[G : H] = \frac{|G|}{|H|} = 1 \iff |G| = |H|$$

   Como además $H \subset G$ por ser subgrupo, tenemos que $[G : H] = 1$ si y solo si $H = G$.

2. Demostrar que si se tienen subgrupos $G_2 \leqslant G_1 \leqslant G$, entonces

$$[G : G_2] = [G : G_1][G_1 : G_2],$$

$$\begin{array}{c} G \\ | \\ \{1\} \end{array}$$

Figura 3.1: Retículo de subgrupos de para el Ejercicio 3.1.13.

3. Demostrar que si se tiene una cadena descendente de subgrupos de la forma

$$G = G_0 \geqslant G_1 \geqslant \cdots \geqslant G_{r-1} \geqslant G_r,$$

entonces

$$[G : G_r] = \prod_{i=0}^{r-1} [G_i : G_{i+1}].$$

4. Demostrar que si se tiene una cadena descendente de subgrupos de la forma

$$G = G_0 \geqslant G_1 \geqslant \cdots \geqslant G_{r-1} \geqslant G_r = \{1\},$$

entonces

$$|G| = \prod_{i=0}^{r-1} [G_i : G_{i+1}].$$

**Ejercicio 3.1.10.**

1. Demostrar que si $G$ es un grupo de orden 4, entonces se tiene que o bien $G$ es cíclico, o bien es isomorfo al grupo de Klein.
2. Demostrar que si $G$ es un grupo de orden 6, entonces se tiene que o bien $G$ es cíclico, o bien es isomorfo al grupo diédrico $D_3$.

**Ejercicio 3.1.11.** Describir los retículos de subgrupos de los siguientes grupos:

1. El grupo $V$ de Klein.
2. El grupo simétrico $S_3$.
3. El grupo diédrico $D_4$.
4. El grupo cuaternio $Q_2$.
5. El grupo alternado $A_4$.

**Ejercicio 3.1.12.** Fijado un número primo $p$, describe el retículo de subgrupos del grupo cíclico $C_{p^n}$. En particular, describe el retículo de subgrupos del grupo cíclico $C_8$.

**Ejercicio 3.1.13.** Demostrar que un grupo finito $G \neq \{1\}$ carece de subgrupos propios, esto es, que su retículo de subgrupos es el de la Figura 3.1 si, y sólo si, $G = C_p$ es un grupo cíclico de orden primo.

**Ejercicio 3.1.14.** Describir los retículos de subgrupos de los grupos cíclicos siguentes:

1. $C_6$.
2. $C_{12}$.

**Ejercicio 3.1.15.** Se considera el grupo cíclico $C_{136}$ de orden 136, con generador $t$. ¿Qué relación hay entre los subgrupos $H_1 = \langle t^{48}, t^{72} \rangle$ y $H_2 = \langle t^{46} \rangle$?

**Ejercicio 3.1.16.** Demostrar que el grupo de unidades $\mathbb{Z}_7^\times$ es un grupo cíclico.

**Ejercicio 3.1.17.** Sea $G$ un grupo y sea $C_n$ el grupo cíclico de orden $n$ generado por $x$. Demostrar que:

1. Si $\theta : C_n \to G$ es un homomorfismo de grupos, entonces:
$$O(\theta(x)) \mid n, \quad \text{y} \quad \theta(x^k) = \theta(x)^k \quad \forall k \in \{0, \ldots, n-1\}.$$
2. Para cada $g \in G$ tal que $O(g) \mid n$, existe un único homomorfismo de grupos $\theta_g : C_n \to G$ tal que $\theta_g(x) = g$.
3. Si $g \in G$ es tal que $O(g) \mid n$, entonces el morfismo $\theta_g$ es monomorfismo si, y sólo si, $O(g) = n$.
4. Existe un isomorfismo de grupos
$$U(\mathbb{Z}_n) \cong \mathrm{Aut}(C_n),$$
dado por $r \mapsto f_r$ para cada $r = 1, \ldots, n$ con $\mathrm{mcd}(r, n) = 1$, donde el automorfismo $f_r$ se define mediante $f_r(x) = x^r$.
En particular, $\mathrm{Aut}(C_n)$ es un grupo abeliano de orden $\varphi(n)$.

**Ejercicio 3.1.18.**

1. Describir explícitamente el grupo de automorfismos $\mathrm{Aut}(C_8)$.
2. Demostrar que $\mathrm{Aut}(C_8)$ es isomorfo al grupo de Klein.