

Álgebra II

FACULTAD
DE
CIENCIAS
UNIVERSIDAD DE GRANADA



Los Del DGIIM, losdeldgiim.github.io

Doble Grado en Ingeniería Informática y Matemáticas
Universidad de Granada



Esta obra está bajo una Licencia Creative Commons Atribución-NoComercial-SinDerivadas 4.0 Internacional (CC BY-NC-ND 4.0).

Eres libre de compartir y redistribuir el contenido de esta obra en cualquier medio o formato, siempre y cuando des el crédito adecuado a los autores originales y no persigas fines comerciales.

Álgebra II

Los Del DGIIM, `losdeldgiim.github.io`

José Juan Urrutia Milán

Granada, 2025

Índice general

1. Grupos: definición, generalidades y ejemplos	5
1.1. Grupos diédricos D_n	17
1.1.1. Motivación	17
1.1.2. Definición y primeras propiedades	22
1.2. Generadores de un grupo	24
1.3. Grupos Simétricos S_n	26
1.3.1. Signatura	36
1.3.2. Grupos Alternados A_n	40
1.4. Grupos de matrices	42
1.4.1. Grupo lineal $GL_n(\mathbb{F})$	43
1.4.2. Grupo lineal especial $SL_n(\mathbb{F})$	43
1.5. Homomorfismos de grupos	44
2. Subgrupos, Generadores, Retículos y Grupos cíclicos	51
2.1. Grupos: generalidades y ejemplos	54

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 “buena¹”. Por tanto, los grupos serán estructuras menos restrictivas que los anillos conmutativos, aunque su estudio no será menos interesante.

¹La 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

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

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 $*$:

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

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

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

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 $*$:

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

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

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

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 $*$:

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

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:

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

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 heredado¹ 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 $n \geq 1$, consideramos:

$$\begin{aligned} \mu_n &= \{\text{raíces complejas de } x^n - 1\} = \left\{ \xi_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n} : k \in \{0, \dots, n-1\} \right\} \\ &= \left\{ 1, \xi, \xi^2, \dots, \xi^{n-1} : \xi = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n} \right\} \end{aligned}$$

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 $*$: $(G \times H) \times (G \times H) \rightarrow G \times H$ dada por:

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

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

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

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: $X = \{x_1, x_2, \dots, x_n\}$, notaremos:

$$S_n = S(X)$$

¹Será 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:

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

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

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

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

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

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

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

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 $*$: $X \times X \rightarrow X$ dada por:

$$e * e = e \quad e \in X$$

A este grupo (independientemente de cual sea el conjunto X , ya que todos tendrán la misma² estructura) lo llamaremos grupo trivial.

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

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

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 $+$:

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

²Concepto 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 $*$:

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

- 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 $-x - 2 \in \mathbb{Z}$:

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

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

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

□

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:*

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

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

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

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

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:

$$x' * (x * x') = (x' * x) * x' = e * x' = x' \quad (1.1)$$

Ahora:

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

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

ii) Usando i) en (*):

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

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

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

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:

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

Donde en (*) hemos usado i).

□

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

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

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):*

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

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, entonces:*

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 sencillamente 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 ecuaciones³:

$$aX = b \quad Xa = b$$

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:

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

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:

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

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

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

³Donde 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 $m = 1$):

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

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

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

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:

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

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

1. $n > 0$:

- a) $m > 0$:

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

- b) $m = 0$:

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

- c) $m < 0$:

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

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

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

2) $n + m = 0$: Entonces, $n = -m$. Tenemos:

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

3) $n + m < 0$: Entonces, $n < -m$. Tenemos:

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

2. $n = 0$:

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

3. $n < 0$:

a) $m > 0$:

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

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) $m = 0$:

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

c) $m < 0$:

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

□

Definición 1.5 (Grupos finitos e infinitos). Sea G un grupo, si G como conjunto tiene⁴ $n \in \mathbb{N} \setminus \{0\}$ 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.

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

Definición 1.6 (Tabla de Cayley). En un grupo finito $G = \{x_1, x_2, \dots, x_n\}$, se llama tabla de Cayley (o de multiplicar⁵) 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	$*_2$	0	1
0	0	1	0	1	0
1	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	1	2	3
0	0	1	2	3	0	0	1	2	3
1	1	2	3	0	1	1	0	3	2
2	2	3	0	1	2	2	3	0	1
3	3	0	1	2	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, notaremos⁶: $O(x) = \text{ord}(x) = n$.

Si para un elemento $x \in G$ dicho n no existe, se dice que su orden es infinito: $O(x) = +\infty$.

⁵Entendiendo que en este caso hacemos uso de la notación multiplicativa.

⁶Podremos 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, $x \in G$ y sea $m \in \mathbb{N} \setminus \{0\}$ de forma que $x^m = 1$ con $O(x) = n$, entonces $n|m$.

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

$$m = nq + r \quad \text{con } 0 \leq r < n$$

Pero entonces:

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

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

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 G es finito, entonces $O(x) \neq +\infty$ para todo $x \in G$.

Demostración. Demostramos las dos propiedades:

1. Por doble implicación:

\Leftarrow) Trivial.

\Rightarrow) 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 $O(x^{-1}) \leq n$. Para ello, vemos que $(x^{-1})^n = 1$:

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

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

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

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

$$n \leq O(x^{-1}) \leq n \implies O(x^{-1}) = n$$

- 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:

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

De donde llegamos a que:

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

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

3. Para ello, consideramos la sucesión de elementos $\{x^n\}$:

$$x, x^2, x^3, \dots$$

Como $x^n \in G$ para todo $n \in \mathbb{N}$ y G es un conjunto finito, tarde o temprano ha de repetirse algún valor en la sucesión, es decir, existen $k > j \geq 0$ de forma que:

$$x^k = x^j$$

Si ahora tomamos $n = k - j$, tenemos que:

$$x^k = x^{j+n} = x^j$$

Si multiplicamos por x^{-j} a ambos lados, llegamos a que:

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

Por lo que no puede ser $O(x) = +\infty$.

□

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 , $O(\bar{6}) = 3$:

$$\begin{aligned} \bar{6} &\neq \bar{0} \\ \bar{6} + \bar{6} &= \bar{12} = \bar{3} \neq \bar{0} \\ \bar{6} + \bar{6} + \bar{6} &= \bar{18} = \bar{0} \end{aligned}$$

4. En $\mathbb{Z}_7^* = \mathcal{U}(\mathbb{Z}_7)$:

■ $O(\bar{2}) = 3$:

$$\begin{aligned}\bar{2} &\neq \bar{1} \\ \overline{2 \cdot 2} &= \bar{4} \neq \bar{1} \\ \overline{2 \cdot 2 \cdot 2} &= \bar{8} = \bar{1}\end{aligned}$$

■ $O(\bar{3}) = 6$.

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

1.1. Grupos diédricos D_n

A continuación, estaremos interesados en el estudio de una familia⁷ de grupos conocida como los “grupos diédricos”, cuyo estudio se desarrollará a lo largo de la asignatura.

1.1.1. Motivación

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

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.

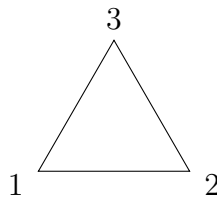


Figura 1.1: Triángulo equilátero con centro en el origen de coordenadas.

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:

⁷Donde con “familia” hacemos referencia a un conjunto de grupos que guardan cierta similitud entre ellos.

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

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

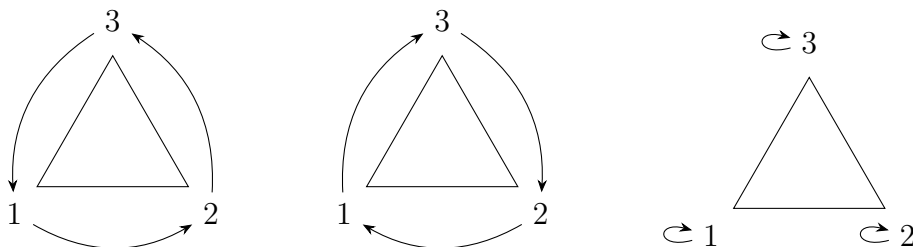


Figura 1.2: Todos los giros que dejan invariante al triángulo.

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.

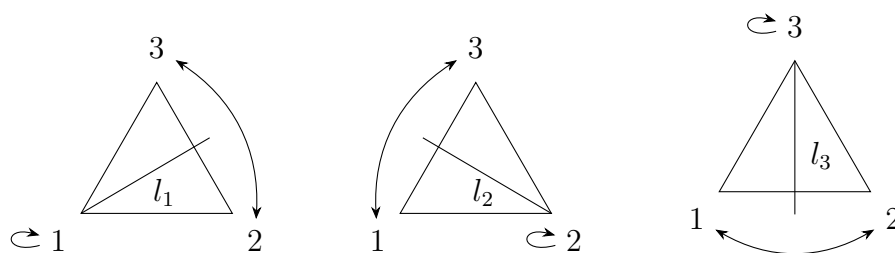


Figura 1.3: Todas las reflexiones que dejan invariante al triángulo.

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 $f : X \rightarrow X$.

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

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

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

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

En dicho caso, representaremos a σ por:

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

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

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

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

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

A los 2-ciclos los llamaremos transposiciones.

Ejemplo. Para familiarizarnos con los ciclos, observamos que:

- En S_3 , los ciclos de longitud 2 que podemos considerar son: $(1 \ 2)$, $(1 \ 3)$ y $(2 \ 3)$. Estos se interpretan respectivamente como:
 - Mantener el 3 fijo e intercambiar el 1 con el 2.
 - Mantener el 2 fijo e intercambiar el 1 con el 3.
 - Mantener el 1 fijo e intercambiar el 2 con el 3.
- En S_3 , los únicos ciclos de longitud 3 que podemos considerar son: $(1 \ 2 \ 3)$ y $(3 \ 2 \ 1)$, cuya definición debe estar clara.

Notación. Es claro que no toda permutación es un ciclo, basta considerar la aplicación identidad. Sin embargo, hay ciertas permutaciones como por ejemplo la aplicación $\sigma : \{1, 2, 3, 4\} \rightarrow \{1, 2, 3, 4\}$ 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 por⁸:

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

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

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

$$\sigma(5) = 5$$

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

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

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

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

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

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

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

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

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

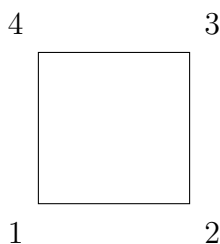


Figura 1.4: Cuadrado con centro en el origen de coordenadas.

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

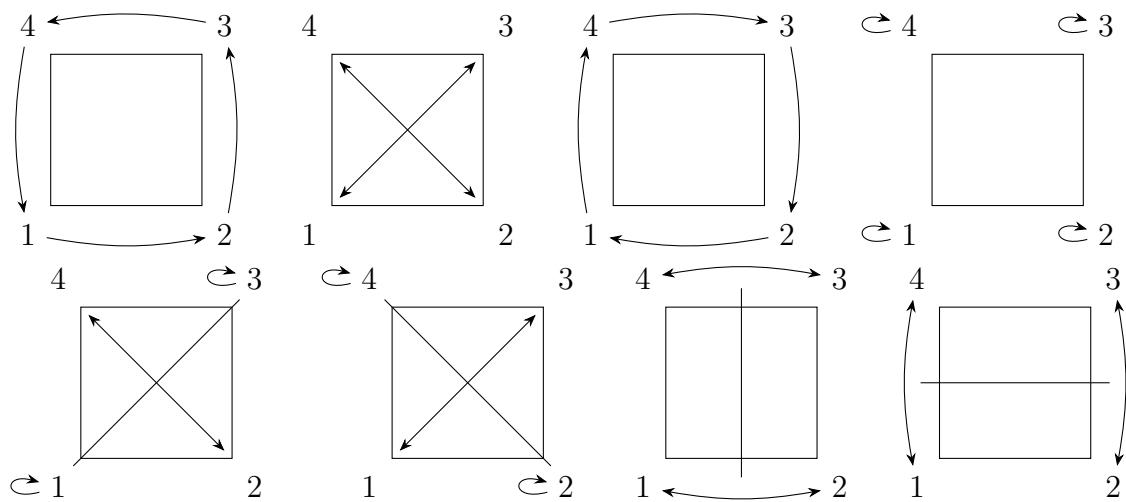


Figura 1.5: Giros y simetrías que dejan invariante al cuadrado

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

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

- El giro de ángulo $\frac{\pi}{2}$ es $(1\ 2\ 3\ 4)$.
- El giro de ángulo π es $(1\ 3)(2\ 4)$.
- El giro de ángulo $\frac{3\pi}{2}$ es $(1\ 4\ 3\ 2)$.
- El giro de ángulo 2π es la identidad, (1) .
- 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 algebraico) con la composición de r y s :

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

De esta forma, si consideramos el conjunto:

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

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

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

1.1.2. Definición y primeras propiedades

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

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

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

- n rotaciones de ángulo $\frac{2k\pi}{n}$, con $k \in \{1, \dots, n\}$.
- n simetrías axiales:
 - Si n es par, tenemos:

- $n/2$ simetrías respecto a las mediatrices.
- $n/2$ simetrías respecto a unir vértices opuestos.
- Si n es impar, tenemos n simetrías respecto a las mediatrices.

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

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

De esta forma, todos los elementos de D_n son:

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

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

Demostración. Demostramos cada una de las propiedades:

1. La primera parte es competencia 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, $S = \{x_1, x_2, \dots, x_n\} \subseteq G$, podemos escribir:

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

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

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

- i) S es un conjunto de generadores de G .
- ii) Dado $x \in G$, $\exists x_1, x_2, \dots, x_p \in S$ de forma que:

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

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:

$$x = \underbrace{1 + 1 + \dots + 1}_{x \text{ veces}}$$

- Si $x < 0$, entonces (-1 es el simétrico de 1):

$$x = \underbrace{-1 - 1 - \dots - 1}_{x \text{ veces}}$$

- 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, \dots, 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:

$$G = \langle S \mid R_1, R_2, \dots, R_m \rangle$$

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: $C_n = \{1, x, x^2, x^3, \dots, x^{n-1}\}$

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 $xy \in V^{\text{abs}}$ y que:

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

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

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

Observamos que el grupo nos recuerda a D_2 .

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

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

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

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

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

Observamos también que el grupo nos recuerda a D_4 .

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

$$\begin{aligned} i^2 &= j^2 = k^2 = -1 \\ ij &= k & jk &= i & ki &= j \\ ji &= -k & kj &= -i & ik &= -j \end{aligned}$$

Productos que pueden recordarse observando la Figura 1.6

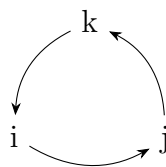


Figura 1.6: Dirección en la que se multiplican los cuaternios de forma positiva.

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

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

Si pensamos en relacionar los elementos de la Tabla 1.1.

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

Tabla 1.1: Elementos que se relacionan.

1.3. Grupos Simétricos S_n

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

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

Definición 1.13 (Grupos Simétricos S_n). Dado $n \in \mathbb{N}$, consideramos $X = \{1, 2, \dots, n\}$ 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 $id : X \rightarrow X$ es el elemento neutro.
- Como las permutaciones son biyecciones, cada una tiene su elemento simétrico.

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

$$|S_n| = n!$$

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

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

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

Observemos que, conocida la matriz anterior, conocemos σ .

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

1. Si consideramos S_0 , son todas las permutaciones del \emptyset en el \emptyset , que solo hay una: $\sigma : \emptyset \rightarrow \emptyset$.
2. Si consideramos S_1 , solo hay una permutación: $id : \{1\} \rightarrow \{1\}$.
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:

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

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 $n \geq 3$ no es abeliano, ya que si estamos en S_n , podemos considerar las extensiones de σ y τ a S_n :

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

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

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

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

Se pide calcular $s_1 s_2$, $s_2 s_1$ y s_2^2 .

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

Proposición 1.11. *Se verifica que:*

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

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:

$$\sigma^{m+1}(x) = \sigma^n(x) = x \quad \forall x \in X$$

2. Se tiene directamente por la definición de ciclo.
3. Sea $\sigma \in S_n$ un ciclo de longitud m :

$$\sigma = (x_1 \ x_2 \ \dots \ x_m) \quad x_1, x_2, \dots, x_m \in X$$

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 $i \in \{1, \dots, m\}$, entonces $\sigma(x) = x$, luego:

$$\sigma^m(x) = \sigma^{m-1}(\sigma(x)) = \sigma^{m-1}(x) = \sigma^{m-2}(\sigma(x)) = \dots = x$$

- Si ahora consideramos x_i con $i \in \{1, \dots, m\}$, tendremos que:

$$x_1 \xrightarrow{\sigma} x_{i+1} \xrightarrow{\sigma} \dots \xrightarrow{\sigma} x_m \xrightarrow{\sigma} x_1 \xrightarrow{\sigma} x_2 \dots \xrightarrow{\sigma} x_{i-1} \xrightarrow{\sigma} x_i$$

$\underbrace{\hspace{10em}}_{\sigma^{m-i+1}} \qquad \underbrace{\hspace{10em}}_{\sigma^{i-1}}$

$$\text{Y } \sigma^{m-i+1} \sigma^{i-1} = \sigma^{m-i+1+i-1} = \sigma^m$$

- Supongamos ahora que existe $k < m$ de forma que $\sigma^k = 1$, esto significaría que $\sigma^k(x_1) = x_1$, pero como σ 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 $k \geq m$.
- 4. Recordamos por la definición de ciclo que si $\sigma = (a_1 \ a_2 \ \dots \ a_{m-1} \ a_m)$, entonces se ha de cumplir que:

$$\begin{aligned}\sigma(x) &= x & x \neq x_i, \quad i \in \{1, \dots, m\} \\ \sigma(x_i) &= x_{i+1} & i \in \{1, \dots, m-1\} \\ \sigma(x_m) &= x_1\end{aligned}$$

Si vemos σ como aplicación y tratamos de buscarle su aplicación inversa σ^{-1} , esta ha de cumplir que:

$$\begin{aligned}\sigma^{-1}(x) &= x & x \neq x_i, \quad i \in \{1, \dots, m\} \\ \sigma^{-1}(x_{i+1}) &= x_i & i \in \{1, \dots, m-1\} \\ \sigma^{-1}(x_1) &= x_m\end{aligned}$$

Sin embargo, vemos que entonces σ^{-1} también es un ciclo:

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

□

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 $i \in X = \{1, 2, \dots, n\}$ 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:

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

siendo los γ_i con $i \in \{1, \dots, k\}$ 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 $X = \{1, 2, \dots, n\}$, 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:

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

- 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:

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

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

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

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:

$$C_x = \bar{x} = \{x, \sigma(x), \sigma^2(x), \dots, \sigma^m(x)\}$$

Si consideramos ahora el ciclo:

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

Tenemos que:

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

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

1. Sean $\bar{i}, \bar{j} \in X/R$ con $\bar{i} \neq \bar{j}$, entonces los elementos que se mueven en γ_i son los elementos de C_i , mientras los elementos que se mueven en γ_j son los de C_j . Como se tiene que $C_i \cap C_j = \emptyset$ por ser C_i y C_j clases de equivalencia distintas, llegamos a que γ_i y γ_j son ciclos disjuntos, para $\bar{i} \neq \bar{j}$.
2. Sea $\tau = \gamma_1 \gamma_2 \dots \gamma_n$, sea $y \in X$, entonces:

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

Ya que anteriormente vimos que:

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

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

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:

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

Teníamos una notación estandar para cada ciclo. Ahora podemos notar σ 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 descomposición 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:

$$\gamma_1 = (x_1 \ x_2 \ \dots \ x_n), \quad \gamma_2 = (y_1 \ y_2 \ \dots \ y_m)$$

$$x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m \in X \text{ todos ellos distintos}$$

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 $y_j \neq x_i$ para todo $i \in \{1, \dots, n\}$.

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

$$\begin{aligned}\gamma_1(\gamma_2(x_n)) &= \gamma_1(x_n) = x_1 = \gamma_2(x_1) = \gamma_2(\gamma_1(x_n)) \\ \gamma_1(\gamma_2(y_m)) &= \gamma_1(y_1) = y_1 = \gamma_2(y_m) = \gamma_2(\gamma_1(y_m))\end{aligned}$$

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 τ podemos tomar:

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

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

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

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 permutación 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 σ se descompone de la forma:

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

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

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

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

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

Donde en $(*)$ hemos usado la Proposición 1.8. Concluimos que m es el mínimo común múltiplo de los órdenes de los ciclos, que por la Proposición 1.11, coincide con el mínimo común múltiplo de las longitudes de los ciclos. \square

Ejemplo. Para familiarizarnos 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 γ es un ciclo, entonces $\tau\gamma\tau^{-1}$ es un ciclo de longitud m .

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

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

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

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

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

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

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

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

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

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 $\alpha = \tau\gamma\tau^{-1}$:

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

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

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

Proposición 1.15. 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:

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

calcular $\tau\sigma\tau^{-1}$. Para ello, sabemos por la Proposición 1.15 que si⁹ $\sigma = \gamma_1\gamma_2\gamma_3\gamma_4$, 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:

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

⁹Observar la descomposición hecha ya de σ .

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:

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

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

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

O también podemos escribir:

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

Para verlo:

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

□

Ejemplo. Sea $\sigma = (1 \ 2 \ 3 \ 4 \ 5)$, veamos que σ 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 σ :

$$\left. \begin{aligned} 1 &\xrightarrow{t_4} 2 \xrightarrow{t_3} 2 \xrightarrow{t_2} 2 \xrightarrow{t_1} 2 \\ 2 &\mapsto 1 \mapsto 3 \mapsto 3 \mapsto 3 \\ 3 &\mapsto 3 \mapsto 1 \mapsto 4 \mapsto 4 \\ 4 &\mapsto 4 \mapsto 4 \mapsto 1 \mapsto 5 \\ 5 &\mapsto 5 \mapsto 5 \mapsto 5 \mapsto 1 \end{aligned} \right\} \implies \left\{ \begin{aligned} 1 &\xrightarrow{\gamma} 2 \\ 2 &\mapsto 3 \\ 3 &\mapsto 4 \\ 4 &\mapsto 5 \\ 5 &\mapsto 1 \end{aligned} \right.$$

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 $\tau = r_1 r_2 r_3 r_4$:

$$\left. \begin{array}{l} 1 \xrightarrow{r_4} 1 \xrightarrow{r_3} 1 \xrightarrow{r_2} 1 \xrightarrow{r_1} 2 \\ 2 \mapsto 2 \mapsto 2 \mapsto 3 \mapsto 3 \\ 3 \mapsto 3 \mapsto 4 \mapsto 4 \mapsto 4 \\ 4 \mapsto 5 \mapsto 5 \mapsto 5 \mapsto 5 \\ 5 \mapsto 4 \mapsto 3 \mapsto 2 \mapsto 1 \end{array} \right\} \implies \left\{ \begin{array}{l} 1 \xrightarrow{\gamma} 2 \\ 2 \mapsto 3 \\ 3 \mapsto 4 \\ 4 \mapsto 5 \\ 5 \mapsto 1 \end{array} \right.$$

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:

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

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

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

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

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

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

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

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

$$\Delta = \prod_{1 \leq i < j \leq 4} (x_i - x_j) = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4)$$

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

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

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

Proposición 1.18. *La aplicación signatura verifica que:*

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

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

Demostración. Por inducción sobre m :

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

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

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

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

- Supuesto para m :

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

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 $m \geq 2$ 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 $1 \leq i < j \leq n$), estudiemos qué sucede con $\sigma(\Delta)$:

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

$$\begin{aligned}(x_a - x_i) &\xrightarrow{\sigma} (x_a - x_j) \\ (x_a - x_j) &\xrightarrow{\sigma} (x_a - x_i)\end{aligned}$$

Tenemos que un factor va al otro, por lo que no alteran el signo.

- De forma análoga, los factores de la forma $(x_y - x_b)$ con $y \in \{i, j\}$ y $b > j$ tampoco alteran el signo de Δ :

$$\begin{aligned}(x_i - x_b) &\xrightarrow{\sigma} (x_j - x_b) \\ (x_j - x_b) &\xrightarrow{\sigma} (x_i - x_b)\end{aligned}$$

- 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:

$$\begin{aligned}(x_i - x_a) &\xrightarrow{\sigma} (x_j - x_a) = -(x_a - x_j) \\ (x_a - x_j) &\xrightarrow{\sigma} (x_a - x_i) = -(x_i - x_a)\end{aligned}$$

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

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

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

y llegamos a que σ es impar.

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

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

Usando la Proposición 1.18, 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 τ un ciclo de longitud $m \geq 3$, en la Proposición 1.16 vimos que τ se podía descomponer como producto de $m - 1$ transposiciones:

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

Por tanto, y aplicando 2, tenemos que:

- Si m es par, entonces $m - 1$ es impar, con lo que τ es impar.
 - Si m es impar, entonces $m - 1$ es par, con lo que τ es par.
4. Sea $\sigma \in S_n$, esta se puede descomponer como producto de k ciclos disjuntos de longitud mayor o igual que 2:

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

Usando la Proposición 1.18, tenemos que:

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

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

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

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

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

Por tanto:

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

□

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

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

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

1.3.2. Grupos Alternados A_n

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

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

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

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

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

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

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

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

1. Para $n = 3$:

$$\begin{aligned} S_3 &= \{1, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\} \\ A_3 &= \{1, (1\ 2\ 3), (1\ 3\ 2)\} \end{aligned}$$

2. Para $n = 4$:

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

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

Proposición 1.20. *Se tiene que:*

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

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

$$(d) A_n = \langle (x_1\ x_2\ x_3) \rangle \text{ con } n \geq 3$$

$$(e) A_n = \langle (1\ x\ y) \rangle \text{ con } n \geq 3$$

Demostración. Veamos cada uno de los enunciados:

(a) Sabemos que (por la Proposición 1.16):

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

Supuesto que $i < j$, vemos que:

$$(i\ j) = (i\ i+1)(i+1\ i+2) \dots (j-2\ j-1)(j-1\ j)(j-1\ j-2) \dots (i+2\ i+1)(i+1\ i)$$

(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:

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

Podemos considerar el conjugado de $(1\ 2)$ mediante σ^{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 $\text{GL}_n(\mathbb{F})$

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

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

Se verifica que $(\text{GL}_n(\mathbb{F}), \cdot, I)$ 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 $\text{GL}_n(\mathbb{F})$ lo llamamos el grupo lineal de orden n . Si $|\mathbb{F}| = q$, este verifica:

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

Ejemplo. Veamos:

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

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

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 $|\text{GL}_3(\mathbb{Z}_2)| = 168$. Se deja como ejercicio escribir todas las matrices.
- Tenemos $|\text{GL}_2(\mathbb{Z}_3)| = 48$.

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

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

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

Se verifica que $(\text{SL}_n(\mathbb{F}), \cdot, I)$ 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 $\text{SL}_n(\mathbb{F})$ lo llamamos el grupo lineal especial de orden n . Si $|\mathbb{F}| = q$, este verifica:

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

Ejemplo. Tenemos:

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

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 $f : G \rightarrow H$ que verifica:

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

Proposición 1.21. Si $f : G \rightarrow H$ es un homomorfismo de grupos, entonces:

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

Demostración. Veamos cada una:

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

□

Definición 1.21. Sea $f : G \rightarrow H$ un homomorfismo de grupos, distinguimos:

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

Ejemplo. Ejemplos de homomorfismos de grupos son:

1. Dado G un grupo, $\text{id} : G \rightarrow G$.
2. Dados G, H grupos, consideramos el siguiente homomorfismo, denominado *homomorfismo trivial*:

$$\begin{aligned} f : G &\longrightarrow H \\ x &\longmapsto 1 \end{aligned}$$

3. La exponencial es también un homomorfismo:

$$\begin{aligned} \exp : (\mathbb{R}, +) &\longrightarrow (\mathbb{R}^+, \cdot) \\ x &\longmapsto e^x \end{aligned}$$

4. La aplicación determinante de matrices con determinante no nulo:

$$\begin{aligned} \det : \text{GL}_n(\mathbb{F}) &\longrightarrow \mathbb{F}^* \\ A &\longmapsto \det(A) \end{aligned}$$

5. La aplicación signatura:

$$\begin{aligned} \varepsilon : S_n &\longrightarrow \mathcal{U}(\mathbb{Z}) = \{-1, 1\} \\ \sigma &\longmapsto \varepsilon(\sigma) \end{aligned}$$

Proposición 1.22. Sean $f : G \rightarrow H$ y $g : H \rightarrow T$ dos homomorfismos de grupos, entonces la aplicación $g \circ f : G \rightarrow T$ 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 $f : G \rightarrow H$ 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 1.23. Sea $f : G \rightarrow H$ 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:

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

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

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

Concluimos que f es inyectiva.

ii) Demostramos las dos implicaciones:

\implies) 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.

\impliedby) 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 1.24. *La propiedad de ser isomorfo es una relación de equivalencia.*

Demostración. Demostramos cada una de las propiedades:

- Propiedad reflexiva. Sea G un grupo, como $id : G \rightarrow G$ 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 $f : G \rightarrow H$. Por la Proposición 1.23, $f^{-1} : H \rightarrow G$ 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: $f : G \rightarrow H$ y $g : H \rightarrow T$. Si consideramos $g \circ f : G \rightarrow T$, tenemos por la Proposición 1.22 que $g \circ f$ es un isomorfismo de G en T , por lo que $G \cong T$.

□

Proposición 1.25. *Se verifican:*

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

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

- ii) $\text{Aut}(G) = \{f : G \rightarrow G \mid f \text{ automorfismo}\}$ con la composición forman un grupo.
- iii) Si $f : G \rightarrow H$ es un isomorfismo, entonces $|G| = |H|$.
- iv) Si G y H son isomorfos, entonces G es abeliano $\iff H$ es abeliano.
- v) Si $f : G \rightarrow H$ es un isomorfismo, entonces se mantiene el orden:

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

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

Demostración. Veamos cada una:

- i) Hemos de ver que φ es un homomorfismo biyectivo:

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

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

Donde podemos ver $(*)$ descomponiendo en ciclos disjuntos tanto σ como τ y aplicando la Proposición 1.15.

- Definimos la siguiente aplicación:

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

Veamos que ψ es la inversa de φ :

$$\begin{aligned} \psi(\varphi(\sigma)) &= \psi(f\sigma f^{-1}) = f^{-1}f\sigma f^{-1}f = \sigma \\ \varphi(\psi(\tau)) &= \varphi(f^{-1}\tau f) = f(f^{-1}\tau f)f^{-1} = \tau \end{aligned}$$

Por tanto, φ es biyectiva.

Como φ es un homomorfismo biyectivo, es un isomorfismo.

ii) La asociatividad viene heredada de la asociatividad de funciones, el neutro del grupo es $id : G \rightarrow G$ 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:

\implies) 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 $O(f(x)) \leq n$. 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 $n \leq m$. 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 $\gamma_1, \dots, \gamma_k \in \mathbb{Z}$ de forma que:

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

Luego:

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

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

□

Teorema 1.26 (de Dyck). *Sea G un grupo finito con una presentación*

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

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

$$f(s_i) = r_i \quad i \in \{1, \dots, m\}$$

- *Si además $\{r_1, \dots, r_m\}$ 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 1.26, 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 $\bar{1}$ también verifica la propiedad $x^n = 1$, ya que:

$$n \cdot \bar{1} = \underbrace{\bar{1} + \dots + \bar{1}}_{n \text{ veces}} = 0$$

De esta forma, por el Teorema 1.26, sabemos que existe un homomorfismo $f : C_n \rightarrow \mathbb{Z}_n$, de forma que $f(x) = 1$.

Más aún, como $\mathbb{Z}_n = \langle \bar{1} \rangle$ 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 $f : V^{\text{abs}} \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$ 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 $g : V^{\text{abs}} \rightarrow V$ 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:

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

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 $f : D_3 \rightarrow S_3$ de forma que $f(r) = (1\ 2\ 3)$ y $f(s) = (1\ 2)$. Como además tenemos que¹⁰ $S_3 = \langle (1\ 2)(1\ 2\ 3) \rangle$ y que $|D_3| = 2 \cdot 3 = 6 = 3! = |S_3|$, concluimos que f es un isomorfismo, por lo que $D_3 \cong S_3$.

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

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

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

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

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

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

¹⁰Esto se vio en la Proposición 1.20.

Además, como (ver el Ejercicio 2.1.18):

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

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:

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

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

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

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:

$$\begin{aligned} i^4 &= 1 \\ j^2 &= -1 = i^2 \\ ji(-j) &= j(-k) = -i \end{aligned}$$

Sabemos que existe un homomorfismo $f : Q_2^{\mathrm{abs}} \rightarrow Q_2$ 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 $k, n \in \mathbb{N}$, $k \geq 3$ con $k \mid n$ y consideramos los grupos diédricos:

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

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:

$$\begin{aligned} r_1^n &= r_1^{kp} = (r_1^k)^p = 1^p = 1 \\ s_1^2 &= 1 \\ s_1 r_1 &= r_1^{-1} s_1 \end{aligned}$$

Tenemos por el Teorema 1.26 que existe un homomorfismo $f : D_n \rightarrow D_k$ de forma que $f(r) = r_1$ y $f(s) = s_1$.

2. Subgrupos, Generadores, Retículos y Grupos cíclicos

Definición 2.1 (Subgrupo). Dados dos grupos G y H , se dice que H es un subgrupo de G , denotado por $H < G$ si $H \subseteq G$ y la aplicación de inclusión¹ $i : H \rightarrow G$ es un homomorfismo de grupos.

Observación. Dado un grupo $(G, *, e)$, este tendrá siempre dos subgrupos: $(G, *, e)$ y $(\{e\}, *, e)$, que llamaremos subgrupos impropios. Si $H \subseteq G$ es un subgrupo de G que no es ninguno de esos, diremos que es un subgrupo propio.

Ejemplo. Vemos claramente que:

1. $(\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +)$
2. $\{r^k \mid k \leq n, r \in D_n\} < D_n$
3. $n\mathbb{Z} < \mathbb{Z}$
4. $\text{SL}_n(\mathbb{F}) < \text{GL}_n(\mathbb{F})$
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 $j : G \rightarrow H$ y $k : H \rightarrow T$ son homomorfismos, tendremos que $i = k \circ j : G \rightarrow T$ es un homomorfismo. \square

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 $x^{-1} \in H$.

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

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

Demostración. Veamos las implicaciones de forma cíclica:

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

ii) \implies iii) Si $x, y \in H$, entonces (por (c)) $y^{-1} \in H$, por lo que (por (a)) tendremos que $xy^{-1} \in H$.

iii) \implies i) Como $\emptyset \neq H$, existirá al menos un $x \in H$, por lo que $xx^{-1} = 1 \in H$.

□

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:

ii) \implies i) Como G es finito, para todo $x \in G$, existirá $n > 0$ de forma que $x^n = 1$, por lo que $x^{-1} = x^{n-1}$

□

Ejemplo. Veamos que:

1. $A_n < S_n$
2. Si $n > 0$, $n\mathbb{Z} < \mathbb{Z}$ Todo subgrupo de \mathbb{Z} es así.
3. $V < S_4$
4. Si $n \mid m$, entonces $D_n < D_m$

Definición 2.2. Sea G un grupo y f una aplicación, llamamos imagen directa de G por f a:

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

Respectivamente, imagen inversa a:

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

Proposición 2.3. Sea $f : G \rightarrow G'$ un homomorfismo de grupos:

i) Si $H < G$, entonces $f_*(H) = \{f(x) \mid x \in H\} < G'$

ii) Si $H' < G'$, entonces $f^*(H') = \{x \in G \mid f(x) \in H'\} < G$

$$\text{Im}(f) = f_*(G) \subseteq G' \quad \ker(f) = f^*(1) < G$$

Proposición 2.4. Sea $\{H_i\}_{i \in I}$ una familia de subgrupos de G , entonces:

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

Demostración. Si $1 \in H_i$ para todo $i \in I$, entonces:

$$1 \in \bigcap_{i \in I} H_i \neq \emptyset$$

Si ahora $x, y \in \bigcap_{i \in I} H_i$, entonces $x, y \in H_i$ para todo $i \in I$, por lo que $xy^{-1} \in H_i$ para todo $i \in I$, por lo que:

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

□

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

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

Definición 2.3. Sea G un grupo y $S \subseteq G$, el subgrupo generado por S , $\langle S \rangle$ es la intersección todos los subgrupos de G que contienen a S .

Es decir, $\langle S \rangle$ es el menor subgrupo de G que contiene a S .

Proposición 2.5. Sea G un grupo, $S \subseteq G$, $\langle S \rangle$, entonces:

- Si $S = \emptyset$, entonces $\langle S \rangle = \{e\}$, el grupo trivial.
- Si $S \neq \emptyset$, entonces $\langle S \rangle = \{x_1^{\gamma_1} x_2^{\gamma_2} \dots x_m^{\gamma_m} \mid m \geq 1, x_i \in S, \gamma_i \in \mathbb{Z}\}$
- Si G es finito y $\emptyset \neq S$, entonces $\langle S \rangle = \{\text{productos finitos de elementos de } S\}$

Ejemplo. Veamos:

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 $S = \left\{ i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\} \subseteq \text{GL}_2(\mathbb{C})$, entonces $\langle i, j \rangle < \text{GL}_2(\mathbb{C})$.

Proposición 2.6. Si $S \subseteq G$ de forma que $\langle S \rangle = G$, entonces S es un sistema de generadores de G .

En el caso en el que S sea finito, diremos que G es finitamente generado.

2.1. Grupos: generalidades y ejemplos

Ejercicio 2.1.1. Describir explícitamente la tabla de multiplicar de los grupos \mathbb{Z}_n^\times para $n = 4$, $n = 6$ y $n = 8$, donde por \mathbb{Z}_n^\times denotamos al grupo de las unidades del anillo \mathbb{Z}_n .

Sabemos que, fijado $n \in \mathbb{N}$, las unidades del anillo \mathbb{Z}_n son:

$$\mathcal{U}(\mathbb{Z}_n) = \mathbb{Z}_n^\times = \{a \in \mathbb{Z}_n \mid \text{mcd}(a, n) = 1\}$$

Describimos entonces a continuación las tablas de multiplicar de los grupos \mathbb{Z}_4^\times , \mathbb{Z}_6^\times y \mathbb{Z}_8^\times .

- Para $n = 4$:

\cdot	1	3
1	1	3
3	3	1

- Para $n = 6$:

\cdot	1	5
1	1	5
5	5	1

- Para $n = 8$:

\cdot	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Ejercicio 2.1.2. Describir explícitamente la tabla de multiplicar de los grupos \mathbb{Z}_p^\times para $p = 2$, $p = 3$, $p = 5$ y $p = 7$.

- Para $p = 2$:

\cdot	1
1	1

- Para $p = 3$:

\cdot	1	2
1	1	2
2	2	1

- Para $p = 5$:

\cdot	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

- Para $p = 7$:

\cdot	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Ejercicio 2.1.3. Calcular el inverso de 7 en los grupos \mathbb{Z}_{11}^\times y \mathbb{Z}_{37}^\times .

Para calcular el inverso de un elemento a en un grupo \mathbb{Z}_n^\times , basta con encontrar un elemento b tal que $ab = 1$ en \mathbb{Z}_n .

- Para \mathbb{Z}_{11}^\times :

$$7 \cdot 8 = 56 = 1 \implies 7^{-1} = 8$$

- Para \mathbb{Z}_{37}^\times :

$$7 \cdot 16 = 112 = 1 \implies 7^{-1} = 16$$

Ejercicio 2.1.4. Describir explícitamente los grupos μ_n (de raíces n -ésimas de la unidad) para $n = 3$, $n = 4$ y $n = 8$, dando su tabla de multiplicar.

- Para $n = 3$:

$$\begin{aligned} \mu_3 &= \left\{ 1, \xi_3, \xi_3^2 \mid \xi_3 = \cos\left(\frac{2\pi}{3}\right) + i \sin\left(\frac{2\pi}{3}\right) \right\} = \\ &= \left\{ 1, -\frac{1}{2} + i\frac{\sqrt{3}}{2}, -\frac{1}{2} - i\frac{\sqrt{3}}{2} \right\} \end{aligned}$$

\cdot	1	ξ_3	ξ_3^2
1	1	ξ_3	ξ_3^2
ξ_3	ξ_3	ξ_3^2	1
ξ_3^2	ξ_3^2	1	ξ_3

- Para $n = 4$:

$$\begin{aligned} \mu_4 &= \left\{ 1, \xi_4, \xi_4^2, \xi_4^3 \mid \xi_4 = \cos\left(\frac{\pi}{2}\right) + i \sin\left(\frac{\pi}{2}\right) \right\} = \\ &= \{1, \xi_4, \xi_4^2, \xi_4^3 \mid \xi_4 = i\} = \{1, i, -1, -i\} \end{aligned}$$

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

■ Para $n = 8$:

$$\begin{aligned}\mu_8 &= \left\{ 1, \xi_8, \xi_8^2, \xi_8^3, \xi_8^4, \xi_8^5, \xi_8^6, \xi_8^7 \mid \xi_8 = \cos\left(\frac{\pi}{4}\right) + i \operatorname{sen}\left(\frac{\pi}{4}\right) \right\} = \\ &= \left\{ 1, \xi_8, \xi_8^2, \xi_8^3, \xi_8^4, \xi_8^5, \xi_8^6, \xi_8^7 \mid \xi_8 = \frac{1}{\sqrt{2}} + i \frac{1}{\sqrt{2}} \right\} = \\ &= \left\{ 1, \frac{1}{\sqrt{2}} + i \frac{1}{\sqrt{2}}, i, -\frac{1}{\sqrt{2}} + i \frac{1}{\sqrt{2}}, -1, -\frac{1}{\sqrt{2}} - i \frac{1}{\sqrt{2}}, -i, \frac{1}{\sqrt{2}} - i \frac{1}{\sqrt{2}} \right\}\end{aligned}$$

\cdot	1	ξ_8	ξ_8^2	ξ_8^3	ξ_8^4	ξ_8^5	ξ_8^6	ξ_8^7
1	1	ξ_8	i	ξ_8^3	-1	ξ_8^5	-i	ξ_8^7
ξ_8	ξ_8	i	ξ_8^3	-1	ξ_8^5	-i	ξ_8^7	1
ξ_8^2	i	ξ_8^3	-1	ξ_8^5	-i	ξ_8^7	1	ξ_8
ξ_8^3	ξ_8^3	-1	ξ_8^5	-i	ξ_8^7	1	ξ_8	i
ξ_8^4	-1	ξ_8^5	-i	ξ_8^7	1	ξ_8	i	ξ_8^3
ξ_8^5	ξ_8^5	-i	ξ_8^7	1	ξ_8	i	ξ_8^3	-1
ξ_8^6	-i	ξ_8^7	1	ξ_8	i	ξ_8^3	-1	ξ_8^5
ξ_8^7	ξ_8^7	1	ξ_8	i	ξ_8^3	-1	ξ_8^5	-i

Ejercicio 2.1.5. En el conjunto $\mathbb{Q}^\times := \{q \in \mathbb{Q} \mid q \neq 0\}$ de los números racionales no nulos, se considera la operación de división, dada por $(x, y) \mapsto x/y = xy^{-1}$. ¿Nos da esta operación una estructura de grupo en \mathbb{Q}^\times ?

Veamos qué condiciones han de cumplirse para que se tenga la propiedad asociativa. Sean $a, b, c \in \mathbb{Q}^\times$, entonces:

$$\frac{a/b}{c} = \frac{a}{b/c} \iff \frac{a}{bc} = \frac{ac}{b} \iff ab = abc^2 \iff 1 = c^2$$

Por tanto, tomando por ejemplo $2, 3, 4 \in \mathbb{Q}^\times$ no se tiene la propiedad asociativa, por lo que no se tiene un grupo.

Ejercicio 2.1.6. Sea G un grupo en el que $x^2 = 1$ para todo $x \in G$. Demostrar que el grupo G es abeliano.

Dados $x, y \in G$, se tiene que:

$$\begin{aligned}(xy)(xy) &= (xy)^2 = 1 \implies (xy)^{-1} = xy \\ xy &= (xy)^{-1} = y^{-1}x^{-1} = yx\end{aligned}$$

Por tanto, $xy = yx$ para todo $x, y \in G$, por lo que G es abeliano.

Ejercicio 2.1.7. Sea G un grupo. Demostrar que son equivalentes:

1. G es abeliano.
2. $\forall x, y \in G$ se verifica que $(xy)^2 = x^2y^2$.
3. $\forall x, y \in G$ se verifica que $(xy)^{-1} = x^{-1}y^{-1}$.

Demostración.

$1 \implies 2$) Dados $x, y \in G$, se tiene que:

$$(xy)^2 = xyxy \stackrel{(*)}{=} x^2y^2$$

donde en $(*)$ se ha usado que G es abeliano.

$2 \implies 1$) Dados $x, y \in G$, se tiene que:

$$\begin{aligned} (xy)^2 &= (xy)(xy) = xyxy \\ &\stackrel{(*)}{=} x^2y^2 \end{aligned}$$

donde en $(*)$ se ha usado la hipótesis. Por la propiedad cancelativa, se tiene que:

$$xyxy = x^2y^2 \implies xy = yx$$

Como se tiene para todo $x, y \in G$, entonces G es abeliano.

$1 \implies 3$) Dados $x, y \in G$, se tiene que:

$$(xy)^{-1} = y^{-1}x^{-1} \stackrel{(*)}{=} x^{-1}y^{-1}$$

donde en $(*)$ se ha usado que G es abeliano.

$3 \implies 1$) Dados $x, y \in G$, tenemos que:

$$(xy)^{-1} \stackrel{(*)}{=} x^{-1}y^{-1} = (yx)^{-1} \implies ((xy)^{-1})^{-1} = ((yx)^{-1})^{-1} \implies xy = yx$$

donde en $(*)$ se ha usado la hipótesis. Por tanto, como se tiene para todo $x, y \in G$, entonces G es abeliano.

□

Ejercicio 2.1.8. Demostrar que si en un grupo G , $x, y \in G$ verifican que $xy = yx$ entonces, para todo $n \in \mathbb{N} \setminus \{0\}$, se tiene que $(xy)^n = x^n y^n$.

Demostramos por inducción sobre n .

■ Caso base: $n = 1$.

$$(xy)^1 = xy = yx = x^1 y^1$$

■ Paso inductivo: Supuesto cierto para n , veamos que se cumple para $n + 1$.

$$\begin{aligned} (xy)^{n+1} &= (xy)^n(xy) = x^n y^n xy \\ &= x^n xy^n x = x^{n+1} y^{n+1} \end{aligned}$$

Por tanto, por inducción, se tiene que $(xy)^n = x^n y^n$ para todo $n \in \mathbb{N} \setminus \{0\}$.

Ejercicio 2.1.9. Demostrar que el conjunto de las aplicaciones $f : \mathbb{R} \rightarrow \mathbb{R}$, tales que $f(x) = ax + b$ para algún $a, b \in \mathbb{R}$, $a \neq 0$, es un grupo con la composición como ley de composición.

Definimos el conjunto siguiente:

$$G = \{f : \mathbb{R} \rightarrow \mathbb{R} \mid \exists a, b \in \mathbb{R}, a \neq 0 \text{ tales que } f(x) = ax + b \forall x \in \mathbb{R}\}$$

En primer lugar, hemos de comprobar que G es cerrado bajo la composición de funciones, algo que tendremos gracias a ser \mathbb{R} cerrado para el producto y la suma. Dados $f, g \in G$, entonces existen $a, b, c, d \in \mathbb{R}$, $a, c \neq 0$ tales que:

$$f(x) = ax + b, \quad g(x) = cx + d$$

Entonces, se tiene que:

$$\begin{aligned} (f \circ g)(x) &= f(g(x)) = a(cx + d) + b = acx + ad + b \in G \\ (g \circ f)(x) &= g(f(x)) = c(ax + b) + d = acx + cb + d \in G \end{aligned}$$

Por tanto, G es cerrado bajo la composición de funciones. Ahora, tomando $a = 1$ y $b = 0$, se tiene que $\text{Id}_{\mathbb{R}} \in G$. Veamos que $(G, \circ, \text{Id}_{\mathbb{R}})$ es un grupo.

- A asociatividad: Se tiene de forma directa por serlo la composición de funciones.
- Elemento neutro: Se tiene de forma directa.
- Elemento inverso: Dado $f \in G$, entonces existen $a, b \in \mathbb{R}$, $a \neq 0$ tales que $f(x) = ax + b$. Entonces, definimos su elemento inverso como:

$$f^{-1}(z) = a^{-1}(z - b) \in G$$

Comprobémoslo (notemos que tan solo hace falta comprobar que $f \circ f^{-1} = \text{Id}_{\mathbb{R}}$, puesto que en la definición no se impone $f^{-1} \circ f = \text{Id}_{\mathbb{R}}$):

$$(f \circ f^{-1})(z) = a(a^{-1}(z - b)) + b = z \quad \forall z \in \mathbb{R}$$

Por tanto, para todo $f \in G$, existe $f^{-1} \in G$ tal que $f \circ f^{-1} = \text{Id}_{\mathbb{R}}$.

Ejercicio 2.1.10.

1. Demostrar que $|\text{GL}_2(\mathbb{Z}_2)| = 6$, describiendo explícitamente todos los elementos que forman este grupo.

Sea $A \in \text{GL}_2(\mathbb{Z}_2)$:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \implies |A| = ad - bc \neq 0 \implies ad \neq bc$$

Por tanto, los elementos de $\text{GL}_2(\mathbb{Z}_2)$ son:

$$\begin{aligned} A_1 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, & A_2 &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, & A_3 &= \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \\ A_4 &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, & A_5 &= \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, & A_6 &= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \end{aligned}$$

2. Sea $\alpha = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ y $\beta = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Demostrar que

$$\text{GL}_2(\mathbb{Z}_2) = \{1, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta\}.$$

Tenemos que:

$$1 = A_1, \quad \alpha = A_5, \quad \alpha^2 = A_6, \quad \beta = A_4, \quad \alpha\beta = A_3, \quad \alpha^2\beta = A_2$$

3. Escribir, utilizando la representación anterior, la tabla de multiplicar de $\text{GL}_2(\mathbb{Z}_2)$.

\cdot	1	α	α^2	β	$\alpha\beta$	$\alpha^2\beta$
1	1	α	α^2	β	$\alpha\beta$	$\alpha^2\beta$
α	α	α^2	1	$\alpha\beta$	$\alpha^2\beta$	β
α^2	α^2	1	α	$\alpha^2\beta$	β	$\alpha\beta$
β	β	$\alpha^2\beta$	$\alpha\beta$	1	α^2	α
$\alpha\beta$	$\alpha\beta$	β	$\alpha^2\beta$	α	1	α^2
$\alpha^2\beta$	$\alpha^2\beta$	$\alpha\beta$	β	α^2	α	1

Ejercicio 2.1.11. Dar las tablas de grupo para los grupos D_3 , D_4 , D_5 y D_6 .

Recordamos que:

$$D_n = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$$

■ Para D_3 :

\cdot	1	r	r^2	s	sr	sr^2
1	1	r	r^2	s	sr	sr^2
r	r	r^2	1	sr^2	s	sr
r^2	r^2	1	r	sr	sr^2	s
s	s	sr	sr^2	1	r	r^2
sr	sr	sr^2	s	r^2	1	r
sr^2	sr^2	s	sr	r	r^2	1

■ Para D_4 :

\cdot	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

■ Para D_5 :

\cdot	1	r	r^2	r^3	r^4	s	sr	sr^2	sr^3	sr^4
1	1	r	r^2	r^3	r^4	s	sr	sr^2	sr^3	sr^4
r	r	r^2	r^3	r^4	1	sr^4	s	sr	sr^2	sr^3
r^2	r^2	r^3	r^4	1	r	sr^3	sr^4	s	sr	sr^2
r^3	r^3	r^4	1	r	r^2	sr^2	sr^3	sr^4	s	sr
r^4	r^4	1	r	r^2	r^3	sr	sr^2	sr^3	sr^4	s
s	s	sr	sr^2	sr^3	sr^4	1	r	r^2	r^3	r^4
sr	sr	sr^2	sr^3	sr^4	s	r^4	1	r	r^2	r^3
sr^2	sr^2	sr^3	sr^4	s	sr	r^3	r^4	1	r	r^2
sr^3	sr^3	sr^4	s	sr	sr^2	r^2	r^3	r^4	1	r
sr^4	sr^4	s	sr	sr^2	sr^3	r	r^2	r^3	r^4	1

■ Para D_6 :

\cdot	1	r	r^2	r^3	r^4	r^5	s	sr	sr^2	sr^3	sr^4	sr^5
1	1	r	r^2	r^3	r^4	r^5	s	sr	sr^2	sr^3	sr^4	sr^5
r	r	r^2	r^3	r^4	r^5	1	sr^5	s	sr	sr^2	sr^3	sr^4
r^2	r^2	r^3	r^4	r^5	1	r	sr^4	sr^5	s	sr	sr^2	sr^3
r^3	r^3	r^4	r^5	1	r	r^2	sr^3	sr^4	sr^5	s	sr	sr^2
r^4	r^4	r^5	1	r	r^2	r^3	sr^2	sr^3	sr^4	sr^5	s	sr
r^5	r^5	1	r	r^2	r^3	r^4	sr	sr^2	sr^3	sr^4	sr^5	s
s	s	sr	sr^2	sr^3	sr^4	sr^5	1	r	r^2	r^3	r^4	r^5
sr	sr	sr^2	sr^3	sr^4	sr^5	s	r^5	1	r	r^2	r^3	r^4
sr^2	sr^2	sr^3	sr^4	sr^5	s	sr	r^4	r^5	1	r	r^2	r^3
sr^3	sr^3	sr^4	sr^5	s	sr	sr^2	r^3	r^4	r^5	1	r	r^2
sr^4	sr^4	sr^5	s	sr	sr^2	sr^3	r^2	r^3	r^4	r^5	1	r
sr^5	sr^5	s	sr	sr^2	sr^3	sr^4	r	r^2	r^3	r^4	r^5	1

Ejercicio 2.1.12. Demostrar que el conjunto de rotaciones respecto al origen del plano euclídeo junto con el conjunto de simetrías respecto a las rectas que pasan por el origen, es un grupo.

Denotamos por G al conjunto de rotaciones respecto al origen del plano euclídeo junto con el conjunto de simetrías respecto a las rectas que pasan por el origen. Notemos que no se trata de ningún grupo diédrico:

$$D_n \subsetneq G \quad \forall n \in \mathbb{N}$$

En primer lugar, sería necesario demostrar que es cerrado por la composición, algo que dejamos como ejercicio al lector por ser competencia de Geometría II.

Además, $\text{Id}_{\mathbb{R}^2} \in G$. Veamos que $(G, \circ, \text{Id}_{\mathbb{R}^2})$ es un grupo.

- Asociatividad: Se tiene de forma directa por serlo la composición de funciones.
- Elemento neutro: Se tiene de forma directa.
- Elemento inverso: Dado $f \in G$, veamos que existe $f^{-1} \in G$ tal que se tiene $f \circ f^{-1} = \text{Id}_{\mathbb{R}^2}$.

- Si f es una rotación de ángulo θ respecto al origen, entonces f^{-1} es la rotación de ángulo $-\theta$ respecto al origen.
- Si f es una simetría respecto a una recta que pasa por el origen, entonces f^{-1} es la misma simetría.

En ambos casos, se tiene que $f \circ f^{-1} = \text{Id}_{\mathbb{R}^2}$.

Por tanto, $(G, \circ, \text{Id}_{\mathbb{R}^2})$ es un grupo.

Ejercicio 2.1.13. Sea G un grupo y sean $a, b \in G$ tales que $ba = ab^k$, $a^n = 1 = b^m$ con $n, m > 0$.

1. Demostrar que para todo $i = 0, \dots, m-1$ se verifica $b^i a = ab^{ik}$.

Demostramos para todo $i \in \mathbb{N}$ por inducción sobre i .

- Caso base: $i = 0$.

$$b^0 a = a = ab^0$$

- Caso base: $i = 1$.

$$b^1 a = ba = ab^k = ab^{1 \cdot k}$$

- Paso inductivo: Supuesto cierto para i , veamos que se cumple para $i+1$.

$$b^{i+1} a = b b^i a = b a b^{ik} = a b^k b^{ik} = a b^{k(i+1)}$$

2. Demostrar que para todo $j = 0, \dots, n-1$ se verifica $ba^j = a^j b^{k^j}$.

Demostramos para todo $j \in \mathbb{N}$ por inducción sobre j .

- Caso base: $j = 0$.

$$ba^0 = b = a^0 b^{k^0}$$

- Caso base: $j = 1$.

$$ba = ab^k = a^1 b^{k^1}$$

- Paso inductivo: Supuesto cierto para j , veamos que se cumple para $j+1$.

$$ba^{j+1} = ba^j a = a^j b^{k^j} a \stackrel{(*)}{=} a^j a b^{k^j k} = a^{j+1} b^{k^{j+1}}$$

donde en $(*)$ se ha usado el apartado anterior.

3. Demostrar que para todo $i = 0, \dots, m-1$ y todo $j = 0, \dots, n-1$ se verifica $b^i a^j = a^j b^{ik^j}$.

Fijado $i \in \mathbb{N}$, demostramos por inducción sobre j .

- Caso base: $j = 0$.

$$b^i a^0 = b^i = a^0 b^{ik^0}$$

- Caso base: $j = 1$.

$$b^i a = ab^{ik} = a^1 b^{ik^1}$$

- Paso inductivo: Supuesto cierto para j , veamos que se cumple para $j+1$.

$$b^i a^{j+1} = b^i a^j a = a^j b^{ik^j} a \stackrel{(*)}{=} a^j a b^{ik^j} k = a^{j+1} b^{ik^{j+1}}$$

donde en $(*)$ se ha usado el apartado anterior.

Por tanto, se tiene para todo $i, j \in \mathbb{N}$.

4. Demostrar que todo elemento de $\langle a, b \rangle$ puede escribirse como $a^r b^s$ cumpliendo $0 \leq r < n$, $0 \leq s < m$.

Dado $x \in \langle a, b \rangle$, entonces x es producto de elementos de $\{a, b, a^{-1}, b^{-1}\}$. Como $a^n = 1 = b^m$, entonces $a^{-1} = a^{n-1}$ y $b^{-1} = b^{m-1}$. Por tanto, se tiene que x es producto de elementos de $\{a, b\}$. Usando el apartado anterior, podemos “llevar” los a ’s a la izquierda y los b ’s a la derecha, obteniendo lo siguiente:

$$x = a^{r'} b^{s'} \quad r', s' \in \mathbb{N} \cup \{0\}$$

Supuesto $r' \geq n$, sea $r = r' \text{ mód } n$ ($r' = nk + r$) y se tiene que:

$$a^{r'} = a^{nk+r} = (a^n)^k \cdot a^r = a^r$$

Además, se cumple que $0 \leq r < n$. Análogamente, supuesto $s' \geq m$, sea $s = s' \text{ mód } m$ ($s' = mk + s$) y se tiene que:

$$b^{s'} = b^{mk+s} = (b^m)^k \cdot b^s = b^s$$

Además, se cumple que $0 \leq s < m$. Por tanto:

$$x = a^{r'} b^{s'} = a^r b^s \quad 0 \leq r < n, \quad 0 \leq s < m$$

Observación. Notemos que D_n es un caso particular de este grupo, donde:

$$a = r, \quad b = s, \quad k = n - 1, \quad m = 2, \quad n = n$$

Ejercicio 2.1.14. Sean $s_1, s_2 \in S_7$ las permutaciones dadas por

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

Calcular los productos $s_1 s_2$, $s_2 s_1$ y s_2^2 , y su representación como producto de ciclos disjuntos.

En notación matricial, se tiene que:

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

Descomponiendo en ciclos disjuntos, se tiene que:

$$\begin{aligned}s_2 &= (1\ 5)(2\ 7\ 3\ 6\ 4) \\ s_1 &= (1\ 3\ 4\ 5)(6\ 7) \\ s_1 s_2 &= (2\ 6\ 5\ 3\ 7\ 4) \\ s_2 s_1 &= (1\ 6\ 3\ 2\ 7\ 4) \\ s_2^2 &= (2\ 3\ 4\ 7\ 6)\end{aligned}$$

Ejercicio 2.1.15. Dadas las permutaciones

$$p_1 = (1\ 3\ 2\ 8\ 5\ 9)(2\ 6\ 3), \quad p_2 = (1\ 3\ 6)(2\ 5\ 3)(1\ 9\ 2\ 8\ 5),$$

hallar la descomposición de la permutación producto $p_1 p_2$ como producto de ciclos disjuntos.

Usando la notación matricial, se tiene que:

$$p_1 p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 6 & 4 & 8 & 3 & 7 & 2 & 9 \end{pmatrix}$$

Descomponiendo en ciclos disjuntos, se tiene que:

$$p_1 p_2 = (2\ 5\ 8)(3\ 6)$$

Ejercicio 2.1.16. Sean s_1, s_2, p_1 y p_2 las permutaciones dadas en los ejercicios anteriores.

Observación. Aquí tratamos a S_7 como un subgrupo de S_9 , donde consideramos cada permutación del conjunto $\{1, 2, 3, 4, 5, 6, 7\}$ como una permutación del conjunto $\{1, \dots, 9\}$ que deja fijos a los elementos 8 y 9.

1. Descomponer la permutación $s_1 s_2 s_1 s_2$ como producto de ciclos disjuntos.

$$\begin{aligned}s_1 s_2 s_1 s_2 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 4 & 6 & 7 & 3 & 2 & 8 & 9 \end{pmatrix} \\ &= (2\ 5\ 7)(3\ 4\ 6)\end{aligned}$$

2. Expresar matricialmente la permutación $p_3 = p_2 p_1 p_2$ y obtener su descomposición como ciclos disjuntos.

$$\begin{aligned}p_3 = p_2 p_1 p_2 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 3 & 1 & 4 & 6 & 2 & 7 & 8 & 5 \end{pmatrix} \\ &= (1\ 9\ 5\ 6\ 2\ 3)\end{aligned}$$

3. Descomponer la permutación $s_2 p_2$ como producto de ciclos disjuntos y expresarla matricialmente.

$$\begin{aligned}s_2 p_2 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 8 & 7 & 2 & 6 & 5 & 3 & 4 & 1 \end{pmatrix} \\ &= (1\ 9)(2\ 8\ 4)(3\ 7)(5\ 6)\end{aligned}$$

Ejercicio 2.1.17. Sean s_1, s_2, p_1 y p_2 las permutaciones dadas en los ejercicios anteriores.

1. Calcular el orden de la permutación producto $s_1 s_2$. ¿Coincide dicho orden con el producto de los órdenes de s_1 y s_2 ?

$$\begin{aligned}s_1 s_2 &= (2\ 6\ 5\ 3\ 7\ 4) \\ s_1 &= (1\ 3\ 4\ 5)(6\ 7) \\ s_2 &= (1\ 5)(2\ 7\ 3\ 6\ 4)\end{aligned}$$

Por el Corolario 1.13.1, se tiene que:

$$\begin{aligned}O(s_1 s_2) &= 6 \\ O(s_1) &= \text{mcm}(4, 2) = 4 \\ O(s_2) &= \text{mcm}(2, 5) = 10\end{aligned}$$

Por tanto, $O(s_1 s_2) \neq O(s_1)O(s_2)$.

2. Calcular el orden de $s_1(s_2)^{-1}(s_1)^{-1}$.

$$\begin{aligned}s_1(s_2)^{-1}(s_1)^{-1} &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 1 & 6 & 7 & 2 & 4 \end{pmatrix} = \\ &= (1\ 3)(2\ 5\ 7\ 4\ 6)O(s_1(s_2)^{-1}(s_1)^{-1}) = \text{mcm}(2, 5) = 10\end{aligned}$$

3. Calcular la permutación $(s_1)^{-1}$, y expresarla como producto de ciclos disjuntos.

$$\begin{aligned}s_1 &= (1\ 3\ 4\ 5)(6\ 7) \\ (s_1)^{-1} &= (5\ 4\ 3\ 1)(7\ 6)\end{aligned}$$

4. Calcular la permutación $(p_1)^{-1}$ y expresarla matricialmente.

$$\begin{aligned}p_1^{-1} &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 6 & 1 & 4 & 8 & 2 & 7 & 3 & 5 \end{pmatrix} = \\ &= (1\ 9\ 5\ 8\ 3)(2\ 6)\end{aligned}$$

5. Calcular la permutación $p_2(s_2)^2(p_1)^{-1}$. ¿Cuál es su orden?

$$\begin{aligned}p_2 &= (1\ 3\ 6)(2\ 5\ 3)(1\ 9\ 2\ 8\ 5) \\ (s_2)^2 &= (2\ 3\ 4\ 7\ 6) \\ (p_1)^{-1} &= (1\ 9\ 5\ 8\ 3)(2\ 6) \\ p_2(s_2)^2(p_1)^{-1} &= (1\ 3\ 6)(2\ 5\ 3)(1\ 9\ 2\ 8\ 5)(2\ 3\ 4\ 7\ 6)(1\ 9\ 5\ 8\ 3)(2\ 6) \\ &= (1\ 5\ 6\ 2\ 8\ 4\ 7)(3\ 9) \\ O(p_2(s_2)^2(p_1)^{-1}) &= \text{mcm}(7, 2) = 14\end{aligned}$$

Ejercicio 2.1.18. Sean s_1, s_2, p_1 y p_2 las permutaciones dadas anteriormente. Sean también $s_3 = (2\ 4\ 6)$ y $s_4 = (1\ 2\ 7)(2\ 4\ 6\ 1)(5\ 3)$. ¿Cuál es la paridad de las permutaciones $s_1, s_4p_1p_2$ y p_2s_3 ?

$$\begin{aligned}s_1 &= (1\ 3\ 4\ 5)(6\ 7) \\ s_4p_1p_2 &= (1\ 7)(2\ 3)(4\ 6\ 5\ 8) \\ p_2s_3 &= (1\ 9\ 5\ 3\ 2\ 4)(6\ 8)\end{aligned}$$

Por tanto:

$$\begin{aligned}\varepsilon(s_1) &= 1 \\ \varepsilon(s_4p_1p_2) &= -1 \\ \varepsilon(p_2s_3) &= 1\end{aligned}$$

Ejercicio 2.1.19. En el grupo S_3 , se consideran las permutaciones $\sigma = (1\ 2\ 3)$ y $\tau = (1\ 2)$.

1. Demostrar que

$$S_3 = \{1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}.$$

Sabemos que $|S_3| = 3! = 6$. Dividimos S_3 en dos conjuntos, uno con las permutaciones pares (P) y otro con las impares (I).

$$\begin{aligned}P &= \{1, \sigma, \sigma^2\} \\ I &= \{\tau, \sigma\tau, \sigma^2\tau\}\end{aligned}$$

Como $O(\sigma) = 3$, tenemos que las tres permutaciones pares son distintas. Supongamos ahora que dos permutaciones impares son iguales. Entonces, componiendo por la derecha con τ^{-1} , obtenemos que dos permutaciones pares serían iguales, algo que hemos descartado. Por tanto, las tres permutaciones impares son distintas.

$$|P| = |I| = 3$$

Como una permutación par no puede ser igual a una impar, tenemos que $P \cap I = \emptyset$. Por tanto:

$$\left. \begin{array}{l} |P \cup I| = |P| + |I| = 6 = |S_3| \\ \wedge \\ P \cup I \subset S_3 \end{array} \right\} \Rightarrow S_3 = P \cup I$$

Por tanto, $S_3 = \{1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$.

2. Reescribir la tabla de multiplicar de S_3 empleando la anterior expresión de los elementos de S_3 .

\cdot	1	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
1	1	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
σ	σ	σ^2	1	$\sigma\tau$	$\sigma^2\tau$	τ
σ^2	σ^2	1	σ	$\sigma^2\tau$	τ	$\sigma\tau$
τ	τ	$\sigma^2\tau$	$\sigma\tau$	1	σ^2	σ
$\sigma\tau$	$\sigma\tau$	τ	$\sigma^2\tau$	σ	1	σ^2
$\sigma^2\tau$	$\sigma^2\tau$	$\sigma\tau$	τ	σ^2	σ	1

3. Probar que

$$\sigma^3 = 1, \quad \tau^2 = 1, \quad \tau\sigma = \sigma^2\tau.$$

Como $O(\sigma) = 3$, tenemos que $\sigma^3 = 1$. Por otro lado, como $O(\tau) = 2$, tenemos que $\tau^2 = 1$. El último caso hay que calcularlo, y se ha visto ya en la tabla de multiplicar.

4. Observar que es posible escribir toda la tabla de multiplicar de S_3 usando simplemente la descripción anterior y las relaciones anteriores.

Ejercicio 2.1.20. Describir los diferentes ciclos del grupo S_4 . Expresar todos los elementos de S_4 como producto de ciclos disjuntos.

Veamos cuántos ciclos de longitud m hay en un S_n . Cada una de las elecciones es una variación de n elementos tomados de m en m . Como además un mismo ciclo de longitud m puede empezar en m posiciones distintas, tenemos que el número de ciclos de longitud m es:

$$\frac{V_n^m}{m} = \frac{n!}{m(n-m)!}$$

Por tanto, los ciclos son:

l	Nº	Ciclos
1	1	id
2	6	$(1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4)$
3	8	$(1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 2), (1\ 3\ 4), (1\ 4\ 2), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3)$
4	6	$(1\ 2\ 3\ 4), (1\ 2\ 4\ 3), (1\ 3\ 2\ 4), (1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2)$

Tenemos ahora que $|S_4| = 4! = 24$. Como ya hemos dado 21 elementos, nos faltan 3. Estos son los elementos que no son ciclos, y son los siguientes:

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

Ejercicio 2.1.21. Demostrar que el conjunto de transposiciones

$$\{(1, 2), (2, 3), \dots, (n-1, n)\}$$

genera al grupo simétrico S_n .

Demostramos por doble inclusión que:

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

⊂) Dado $\sigma \in \langle (1, 2), (2, 3), \dots, (n-1, n) \rangle$, entonces como S_n es cerrado por producto, se tiene que $\sigma \in S_n$.

⊃) Dado $\sigma \in S_n$, veamos que $\sigma \in \langle (1, 2), (2, 3), \dots, (n-1, n) \rangle$. Por ser una permutación, tenemos que σ es producto de transposiciones. Por tanto, basta con demostrar que cualquier transposición se puede escribir como producto de elementos de $\{(1, 2), (2, 3), \dots, (n-1, n)\}$.

Sea una transposición (i, j) , y sin pérdida de generalidad, supongamos que $i < j$. Entonces, se tiene que:

$$(i, j) = (i, i+1)(i+1, i+2) \cdots (j-2, j-1)(j-1, j)(j-2, j-1) \cdots (i+1, i+2)(i, i+1)$$

Por tanto, $\sigma \in \langle (1, 2), (2, 3), \dots, (n-1, n) \rangle$.

Ejercicio 2.1.22. Demostrar que el conjunto $\{(1, 2, \dots, n), (1, 2)\}$ genera al grupo simétrico S_n .

Demostramos por doble inclusión que:

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

⊂) Dado $\sigma \in \langle (1, 2, \dots, n), (1, 2) \rangle$, entonces como S_n es cerrado por producto, se tiene que $\sigma \in S_n$.

⊃) Dado $\sigma \in S_n$, veamos que $\sigma \in \langle (1, 2, \dots, n), (1, 2) \rangle$. En primer lugar, definimos $\tau = (1, 2, \dots, n)$. Entonces, se tiene que:

$$\tau^k(j) = j + k \quad \forall k, j \in \{1, \dots, n\}, \quad k + j \leq n$$

Además, por las propiedades de los conjugados, tenemos que:

$$\tau^{(k-1)}(1, 2)\tau^{-(k-1)} = (\tau^{k-1}(1), \tau^{k-1}(2)) = (k, k+1) \quad \forall k \in \mathbb{N}, \quad k < n$$

Entonces, tenemos que:

$$\{(1, 2), (2, 3), \dots, (n-1, n)\} \subset \langle (1, 2, \dots, n), (1, 2) \rangle$$

Por tanto:

$$\sigma \in S_n = \langle (1, 2), (2, 3), \dots, (n-1, n) \rangle \subset \langle (1, 2, \dots, n), (1, 2) \rangle$$

Ejercicio 2.1.23. Demostrar que para cualquier permutación $\alpha \in S_n$ se verifica que $\varepsilon(\alpha) = \varepsilon(\alpha^{-1})$, donde ε denota la signatura, o paridad, de una permutación.

Sabemos que la paridad depende del número de ciclos de longitud par que tiene una permutación en su descomposición en ciclos disjuntos. Como este valor es el mismo para una permutación y su inversa, se tiene que $\varepsilon(\alpha) = \varepsilon(\alpha^{-1})$.

Ejercicio 2.1.24. Demostrar que si $(x_1 x_2 \cdots x_r) \in S_n$ es un ciclo de longitud r , entonces

$$\varepsilon(x_1 x_2 \cdots x_r) = (-1)^{r-1}.$$

- Si r es par, entonces hay un solo ciclo de longitud par, y por tanto $\varepsilon(x_1 x_2 \cdots x_r) = -1$. Como además $r-1$ es impar, se tiene que $(-1)^{r-1} = -1$.
- Si r es impar, entonces hay un solo ciclo de longitud impar, y 0 ciclos de longitud par. Por tanto, $\varepsilon(x_1 x_2 \cdots x_r) = 1$. Como además $r-1$ es par, se tiene que $(-1)^{r-1} = 1$.

Ejercicio 2.1.25. Encontrar un isomorfismo $\mu_2 \cong \mathbb{Z}_3^\times$.

Definimos la aplicación $f : \mu_2 \rightarrow \mathbb{Z}_3^\times$ dada por:

$$\begin{aligned} 1 &\mapsto 1 \\ -1 &\mapsto 2 \end{aligned}$$

Vemos de forma directa que es biyectiva. Veamos además que se trata de un homomorfismo. Para ello, a priori deberíamos de comprobar que, para todas las parejas $x, y \in \mu_2$, se cumple que $f(xy) = f(x)f(y)$. Sin embargo, por tratarse de grupos conmutativos, podemos ahorrarnos la comprobación de algunas de ellas. Además, en todas las parejas en las que aparezca el elemento neutro, puesto que $f(1) = 1$, se tiene que:

$$f(x) = f(1 \cdot x) = f(1) \cdot f(x) = 1 \cdot f(x) = f(x) \quad \forall x \in \mu_2$$

Por tanto, todas estas también se tienen ya comprobadas (idea que repetiremos en ejercicios posteriores). Comprobamos las restantes:

$$1 = f(1) = f((-1) \cdot (-1)) = f(-1) \cdot f(-1) = 2 \cdot 2 = 4 = 1$$

Por tanto, f es un isomorfismo entre ambos grupos.

Ejercicio 2.1.26.

1. Demostrar que la aplicación $f : \mu_4 \rightarrow \mathbb{Z}_5^\times$ dada por:

$$1 \mapsto 1, \quad -1 \mapsto 4, \quad i \mapsto 2, \quad -i \mapsto 3,$$

da un isomorfismo entre el grupo μ_4 de las raíces cuárticas de la unidad y el grupo \mathbb{Z}_5^\times de las unidades en \mathbb{Z}_5 .

De forma directa, vemos que es biyectiva. Para ver que es un homomorfismo, tendremos que comprobar que se da la condición para las 16 posibles parejas. Por tratarse de grupos conmutativos, podremos ahorrarnos la comprobación de algunas de ellas.

$$\begin{aligned} 1 &= f(1) = f((-1) \cdot (-1)) = f(-1) \cdot f(-1) = 4 \cdot 4 = 16 = 1 \\ 4 &= f(-1) = f(i \cdot i) = f(i) \cdot f(i) = 2 \cdot 2 = 4 \\ 4 &= f(-1) = f((-i) \cdot (-i)) = f(-i) \cdot f(-i) = 3 \cdot 3 = 9 = 4 \\ 3 &= f(-i) = f((-1) \cdot i) = f(-1) \cdot f(i) = 4 \cdot 2 = 8 = 3 \\ 2 &= f(i) = f((-1) \cdot (-i)) = f(-1) \cdot f(-i) = 4 \cdot 3 = 12 = 2 \\ 1 &= f(1) = f(i \cdot (-i)) = f(i) \cdot f(-i) = 2 \cdot 3 = 6 = 1 \end{aligned}$$

Por tanto, f es un isomorfismo entre ambos grupos.

2. Encontrar otro isomorfismo entre estos dos grupos que sea distinto del anterior.

Sea $g : \mu_4 \rightarrow \mathbb{Z}_5^\times$ otra aplicación que a continuación definiremos de forma que sea un isomorfismo. En primer lugar, hemos de imponer que $g(1) = 1$, por ser este el elemento neutro en ambos grupos. Por otro lado, en \mathbb{Z}_5^\times tenemos que:

$$O(2) = O(3) = 4 \quad O(4) = 2$$

Como en μ_2 tenemos que $O(-1) = 2$ y sabemos que el orden se conserva en un isomorfismo, tenemos que ha de ser $g(-1) = 4$. Por tanto, solo nos quedan dos opciones para i y $-i$ de forma que g sea biyectiva. Una de ellas opciones nos daría f , por lo que consideramos la otra alternativa. Definimos g entonces como sigue:

$$1 \mapsto 1, \quad -1 \mapsto 4, \quad i \mapsto 3, \quad -i \mapsto 2,$$

La biyección la tenemos de forma directa, y hemos de comprobar que se trata de un homomorfismo. Comprobamos tan solo los pares en los que intervienen los elementos i o $-i$:

$$\begin{aligned} 4 &= g(-1) = g(i \cdot i) = g(i) \cdot g(i) = 3 \cdot 3 = 9 = 4 \\ 4 &= g(-1) = g((-i) \cdot (-i)) = g(-i) \cdot g(-i) = 2 \cdot 2 = 4 \\ 3 &= g(i) = g((-1) \cdot (-i)) = g(-1) \cdot g(-i) = 4 \cdot 2 = 8 = 3 \\ 2 &= g(-i) = g((-1) \cdot i) = g(-1) \cdot g(i) = 4 \cdot 3 = 12 = 2 \\ 1 &= g(1) = g(i \cdot (-i)) = g(i) \cdot g(-i) = 3 \cdot 2 = 6 = 1 \end{aligned}$$

Ejercicio 2.1.27. Encontrar un isomorfismo $\mu_2 \times \mu_2 \cong \mathbb{Z}_8^\times$.

Sea $f : \mu_2 \times \mu_2 \rightarrow \mathbb{Z}_8^\times$ la aplicación definida por:

$$\begin{aligned} (1, 1) &\mapsto 1 \\ (1, -1) &\mapsto 3 \\ (-1, 1) &\mapsto 5 \\ (-1, -1) &\mapsto 7 \end{aligned}$$

Comprobamos que es biyectiva de forma directa. Veamos ahora que es un homomorfismo:

$$\begin{aligned} 1 &= f(1, 1) = f[(1, -1)(1, -1)] = f(1, -1)f(1, -1) = 3 \cdot 3 = 9 = 1 \\ 1 &= f(1, 1) = f[(-1, 1)(-1, 1)] = f(-1, 1)f(-1, 1) = 5 \cdot 5 = 25 = 1 \\ 1 &= f(1, 1) = f[(-1, -1)(-1, -1)] = f(-1, -1)f(-1, -1) = 7 \cdot 7 = 49 = 1 \\ 7 &= f(-1, -1) = f[(1, -1)(-1, 1)] = f(1, -1)f(-1, 1) = 3 \cdot 5 = 15 = 7 \\ 5 &= f(-1, 1) = f[(1, -1)(-1, -1)] = f(1, -1)f(-1, -1) = 3 \cdot 7 = 21 = 5 \\ 3 &= f(1, -1) = f[(-1, 1)(-1, -1)] = f(-1, 1)f(-1, -1) = 5 \cdot 7 = 35 = 3 \end{aligned}$$

Por tanto, f es un isomorfismo entre ambos grupos.

Ejercicio 2.1.28. Demostrar, haciendo uso de las representaciones conocidas, que $D_3 \cong S_3 \cong \text{GL}_2(\mathbb{Z}_2)$.

En primer lugar, tenemos que:

$$\begin{aligned} |D_3| &= 2 \cdot 3 = 6 \\ |S_3| &= 3! = 6 \\ |\text{GL}_2(\mathbb{Z}_2)| &= (2^2 - 1)(2^2 - 2) = 6 \end{aligned}$$

Ahora, damos generadores para cada grupo. El generador de S_3 se ha visto en el Ejercicio 2.1.22, mientras que el generador de $\text{GL}_2(\mathbb{Z}_2)$ se ha visto en el Ejercicio 2.1.10.

$$\begin{aligned} D_3 &= \langle r, s \mid r^3 = 1, s^2 = 1, sr = r^{-1}s \rangle \\ S_3 &= \langle (1\ 2\ 3), (1\ 2) \rangle \\ \text{GL}_2(\mathbb{Z}_2) &= \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \end{aligned}$$

Comprobemos en primer lugar que el generador de S_3 cumple las relaciones de D_3 .

- Como $O((1\ 2\ 3)) = 3$, se tiene que $(1\ 2\ 3)^3 = 1$.
- Como $O((1\ 2)) = 2$, se tiene que $(1\ 2)^2 = 1$.
- Comprobemos que $(1\ 2)(1\ 2\ 3) = (3\ 2\ 1)(1\ 2)$.

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

Por tanto, por el Teorema de Dyck (Teorema 1.26), se tiene que existe un único homomorfismo f de D_3 en S_3 dado por:

$$\begin{aligned} r &\mapsto (1\ 2\ 3) \\ s &\mapsto (1\ 2) \end{aligned}$$

Como además $\{f(r), f(s)\}$ son un generador de S_3 , tenemos que se trata de un epimorfismo, y como además $|D_3| = |S_3|$, se trata de un isomorfismo. Por tanto, $D_3 \cong S_3$.

Comprobemos ahora que el generador de $\text{GL}_2(\mathbb{Z}_2)$ cumple las relaciones de D_3 .

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

Entonces, existe un único homomorfismo $g : S_3 \rightarrow \text{GL}_2(\mathbb{Z}_2)$ de forma que:

$$g(r) = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \quad g(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Como además $\{g(r), g(s)\}$ son un generador de $\text{GL}_2(\mathbb{Z}_2)$, tenemos que se trata de un epimorfismo, y como además $|S_3| = |\text{GL}_2(\mathbb{Z}_2)|$, se trata de un isomorfismo. Por tanto, $S_3 \cong \text{GL}_2(\mathbb{Z}_2)$.

Por ser \cong una relación de equivalencia, tenemos que:

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

Ejercicio 2.1.29. Sea \mathbb{K} un cuerpo y considérese la operación binaria

$$\begin{aligned}\otimes : \mathbb{K} \times \mathbb{K} &\longrightarrow \mathbb{K} \\ (a, b) &\longmapsto a \otimes b = a + b - ab.\end{aligned}$$

Demostrar que $(\mathbb{K} \setminus \{1\}, \otimes)$ es un grupo isomorfo al grupo multiplicativo \mathbb{K}^* .

En primer lugar, hemos de ver que es cerrado para el producto así definido. Dados $a, b \in \mathbb{K} \setminus \{1\}$, veamos que $a \otimes b \neq 1$. Tenemos que:

$$a \otimes b = 1 \iff a + b - ab = 1 \iff a(1 - b) = 1 - b \iff a = 1$$

donde, en la última implicación, hemos usado que \mathbb{K} es un cuerpo y $b \neq 1$, por lo que $1 - b \neq 0$ y por tanto tiene inverso. Por tanto, se tiene que $a \otimes b \neq 1$ y por tanto es cerrado para dicho producto. Veamos ahora que se trata de un grupo (donde hemos de tener en cuenta que no tenemos garantizada la conmutatividad de la suma):

1. **Asociatividad:** Dados $a, b, c \in \mathbb{K} \setminus \{1\}$, hemos de comprobar que se da la igualdad $(a \otimes b) \otimes c = a \otimes (b \otimes c)$. Tenemos que:

$$\begin{aligned}(a \otimes b) \otimes c &= (a + b - ab) \otimes c = a + b - ab + c - (a + b - ab)c \\ a \otimes (b \otimes c) &= a \otimes (b + c - bc) = a + b + c - bc - a(b + c - bc)\end{aligned}$$

Por tanto, tenemos que:

$$(a \otimes b) \otimes c = a \otimes (b \otimes c) \iff -ab - ac - bc - abc = -bc - ab - ac - abc$$

Por tanto, se tiene que la asociatividad se cumple.

2. **Elemento neutro:** Hemos de encontrar un elemento neutro $e \in \mathbb{K} \setminus \{1\}$ tal que $a \otimes e = a$ para todo $a \in \mathbb{K} \setminus \{1\}$. Tenemos que:

$$a \otimes e = a \iff a + e - ae = a \iff e = ae \iff e = 0$$

Por tanto, el elemento neutro es el elemento neutro para la suma en \mathbb{K} , $e = 0$.

3. **Elemento inverso:** Dado $a \in \mathbb{K} \setminus \{1\}$, hemos de encontrar un elemento inverso $a^{-1} \in \mathbb{K} \setminus \{1\}$ tal que $a \otimes a^{-1} = e$. Tenemos que:

$$a \otimes a^{-1} = 0 \iff a + a^{-1} - aa^{-1} = 0 \iff a = a^{-1}(-1 + a) \iff a^{-1} = a(-1 + a)^{-1}$$

donde hemos usado que $a \neq 1$ y por tanto $-1 + a \neq 0$, por lo que podemos considerar su inverso en \mathbb{K} .

Ejercicio 2.1.30.

1. Probar que si $f : G \cong G'$ es un isomorfismo de grupos, entonces se mantiene el orden; es decir, $O(a) = O(f(a))$ para todo elemento $a \in G$.

Probado en la Proposición 1.25.

2. Listar los órdenes de los diferentes elementos del grupo Q_2 y del grupo D_4 y concluir que D_4 y Q_2 no son isomorfos.

En primer lugar, tenemos que:

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

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

Calculamos los órdenes de D_4 :

$$O(1) = 1 \quad O(r) = O(r^3) = 4$$

$$O(r^2) = O(s) = O(sr) = O(sr^2) = O(sr^3) = 2$$

Por otro lado, calculamos los órdenes de Q_2 :

$$O(1) = 1 \quad O(-1) = 2$$

$$O(\pm i) = O(\pm j) = O(\pm k) = 4$$

Por tanto no es posible establecer un isomorfismo $f : D_4 \rightarrow Q_2$ de forma que cumpla

$$O(x) = O(f(x)) \quad \forall x \in D_4$$

Por tanto, D_4 y Q_2 no son isomorfos.

Ejercicio 2.1.31. Calcular el orden de:

1. La permutación $\sigma = (1 \ 8 \ 10 \ 4)(2 \ 8)(5 \ 1 \ 4 \ 8) \in S_{15}$.

$$\sigma = (2 \ 10 \ 4)(5 \ 8)$$

$$O(\sigma) = \text{mcm}(3, 2) = 6$$

2. Cada elemento del grupo \mathbb{Z}_{11}^\times .

$$O(1) = 1$$

$$O(3) = O(4) = O(5) = O(9) = 5$$

$$O(2) = O(6) = O(7) = O(8) = 10$$

$$O(10) = 2$$

Ejercicio 2.1.32. Demostrar que un grupo generado por dos elementos distintos de orden dos, que conmutan entre sí, consiste del 1, de esos elementos y de su producto y es isomorfo al grupo de Klein.

Sea $G = \langle a, b \mid a^2 = b^2 = 1, ab = ba \rangle$. Entonces, por el Ejercicio 2.1.13 tenemos:

$$G = \{1, a, b, ab\}$$

Sea ahora el grupo de Klein el siguiente:

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

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

Por tanto, hemos de encontrar un isomorfismo entre ambos grupos. Comprueba-
mos que los elementos generadores de V cumplen las relaciones de G :

$$\begin{aligned} O((1\ 2)(3\ 4)) &= \text{mcm}(2, 2) = 2 \implies [(1\ 2)(3\ 4)]^2 = 1 \\ O((1\ 3)(2\ 4)) &= \text{mcm}(2, 2) = 2 \implies [(1\ 3)(2\ 4)]^2 = 1 \\ (1\ 2)(3\ 4) (1\ 3)(2\ 4) &= (1\ 4)(2\ 3) \\ (1\ 3)(2\ 4) (1\ 2)(3\ 4) &= (1\ 4)(2\ 3) \end{aligned}$$

Por tanto, por el Teorema de Dyck (Teorema 1.26), se tiene que existe un único homomorfismo $f : G \rightarrow V$ cumpliendo:

$$\begin{aligned} a &\mapsto (1\ 2)(3\ 4) \\ b &\mapsto (1\ 3)(2\ 4) \end{aligned}$$

Como además $\{f(a), f(b)\}$ son un generador de V , tenemos que se trata de un epimorfismo, y como además $|G| = |V|$, se trata de un isomorfismo. Por tanto, $G \cong V$.

Ejercicio 2.1.33. Sea G un grupo y sean $a, b \in G$.

1. Demostrar que $O(b) = O(aba^{-1})$ (un elemento y su conjugado tienen el mismo orden).

Para todo $n \in \mathbb{N}$, se tiene que:

$$1 = (aba^{-1})^n = ab^n a^{-1} \iff a^{-1} = b^n a^{-1} \iff 1 = b^n$$

Comprobemos ahora que $O(b) = O(aba^{-1})$:

- Si $O(b) = \infty$, supongamos por reducción al absurdo que $\exists n \in \mathbb{N}$ tal que $(aba^{-1})^n = 1$. Entonces, se tiene que $b^n = 1$, lo que contradice que $O(b) = \infty$.
- Si $O(b) = n$, entonces se tiene que $b^n = 1$, por lo que $(aba^{-1})^n = 1$ y por tanto $O(aba^{-1}) \leq n$. Por otro lado, supongamos que $\exists m \in \mathbb{N}$, con $m < n$, tal que $(aba^{-1})^m = 1$. Entonces, se tiene que $b^m = 1$, lo que contradice que $O(b) = n$. Por tanto, $O(aba^{-1}) = n$.

En cualquier caso, se tiene que $O(b) = O(aba^{-1})$.

2. Demostrar que $O(ba) = O(ab)$.

Por el apartado anterior, considerando ahora $ba \in G$, se tiene:

$$O(ba) = O(a\ ba\ a^{-1}) = O(ab)$$

Ejercicio 2.1.34. Sea G un grupo y sean $a, b \in G$, $a \neq 1 \neq b$, tales que $a^2 = 1$ y $ab^2 = b^3a$. Demostrar que $O(a) = 2$ y que $O(b) = 5$.

Comprobemos en primer lugar que $O(a) = 2$. Por hipótesis, tenemos que $a^2 = 1$, por lo que $O(a) \mid 2$. Por tanto, $O(a) = 1$ o $O(a) = 2$. Como $a \neq 1$, se tiene que $O(a) = 2$. Veamos ahora que $O(b) = 5$. Tenemos que:

$$\begin{aligned}
 ab^2 = b^3a &\implies b^2 = ab^3a \implies \\
 &\implies b^4 = (ab^3a)(ab^3a) = ab^6a = a(ab^3a)(ab^3a)a = b^9 \implies 1 = b^5
 \end{aligned}$$

Por tanto, $O(b) \mid 5$. Por tanto, $O(b) = 1$ o $O(b) = 5$. Como $b \neq 1$, se tiene que $O(b) = 5$.

Ejercicio 2.1.35. Sea $f : G \rightarrow H$ un homomorfismo de grupos.

$$1. f(x^n) = f(x)^n \quad \forall n \in \mathbb{Z}.$$

Por inducción, se tiene que:

■ Caso base: $n = 1$.

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

■ Paso inductivo: Supongamos que se cumple para n , y veamos que se cumple para $n + 1$.

$$f(x^{n+1}) = f(x^n x) = f(x^n) f(x) = f(x)^n f(x) = f(x)^{n+1}$$

Por tanto, se tiene que $f(x^n) = f(x)^n \quad \forall n \in \mathbb{Z}$.

2. Si f es un isomorfismo entonces G y H tienen el mismo número de elementos de orden n . ¿Es cierto el resultado si f es sólo un homomorfismo?

Consideramos la aplicación inclusión dada por:

$$\begin{aligned}
 i : \mathbb{R}^* &\longrightarrow \mathbb{C}^* \\
 x &\longmapsto x
 \end{aligned}$$

Comprobemos que se trata de un homomorfismo:

$$i(x \cdot y) = x \cdot y = i(x) \cdot i(y) \quad \forall x, y \in \mathbb{R}^*$$

No obstante, tenemos que en \mathbb{C}^* hay elementos de orden 4 ($O(i) = 4$), mientras que en \mathbb{R}^* no los hay. Por tanto, no se cumple el resultado si f es solo un homomorfismo.

3. Si f es un isomorfismo entonces G es abeliano $\Leftrightarrow H$ es abeliano.

Probado en la Proposición 1.25.

Ejercicio 2.1.36.

1. Demostrar que los grupos multiplicativos \mathbb{R}^* (de los reales no nulos) y \mathbb{C}^* (de los complejos no nulos) no son isomorfos.

En \mathbb{R}^* , tenemos que:

$$O(x) = \infty \quad \forall x \in \mathbb{R}^* \setminus \{1\}$$

No obstante, en \mathbb{C}^* , tenemos que $O(i) = 4$. Por tanto, no pueden ser isomorfos.

2. Demostrar que los grupos aditivos \mathbb{Z} y \mathbb{Q} no son isomorfos.

Ejercicio 2.1.37. Sea G un grupo. Demostrar:

1. G es abeliano \iff la aplicación $f : G \rightarrow G$ dada por $f(x) = x^{-1}$ es un homomorfismo de grupos.
2. G es abeliano \iff la aplicación $f : G \rightarrow G$ dada por $f(x) = x^2$ es un homomorfismo de grupos.

Ejercicio 2.1.38. Si G es un grupo cíclico demostrar que cualquier homomorfismo de grupos $f : G \rightarrow H$ está determinado por la imagen del generador.

Ejercicio 2.1.39. Demostrar que no existe ningún cuerpo K tal que sus grupos aditivo $(K, +)$ y (K^*, \cdot) sean isomorfos.