

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	16
1.1.1. Motivación	16
1.1.2. Definición y primeras propiedades	21
1.2. Generadores de un grupo	23
1.3. Grupos Simétricos S_n	25
1.4. Grupos: generalidades y ejemplos	29

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 $\mathcal{P}(X)$.

Definición 1.2 (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 (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 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 .

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.

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:

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

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 .

11. Si X es un conjunto no vacío y consideramos

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

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:

$$S_n = S(X)$$

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 $+$:

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

- 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 $+$:

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

□

²Concepto que luego formalizaremos.

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 1.1. *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 $f * x = x \quad \forall x \in G$, entonces:

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

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

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 1.2. *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 1.3. *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 1.4. *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: $\exists c, d \in G \mid ac = b \wedge da = b$.

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

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 1.5 (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 $0 < m < n$.

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 $0 < m < n + 1$:

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

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

□

Definición 1.3 (Potencia). Sea (G, \cdot, e) un grupo, dado $x \in G$ y $n \in \mathbb{Z}$, podemos definir:

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

Proposición 1.6. 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) $m \geq 0$:

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

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 1.4 (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.

Definición 1.5 (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
0	0	1
1	1	0

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

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

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

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

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

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 1.4 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 1.6 (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: $O(x) = +\infty$.

Proposición 1.7. 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 1.8. Sea G un grupo, se verifica que:

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

Demostración. Demostramos las dos propiedades:

⁶Podremos encontrarnos cualquiera de las dos notaciones.

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

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

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

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

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

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

□

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

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

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

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

$$\blacksquare O(\bar{2}) = 3:$$

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

$$\blacksquare O(\bar{3}) = 6.$$

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

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.

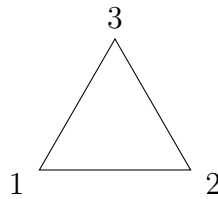


Figura 1.1: Triángulo equilátero con centro en el origen de coordenadas.

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:

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 $\frac{2\pi}{3}$.

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

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

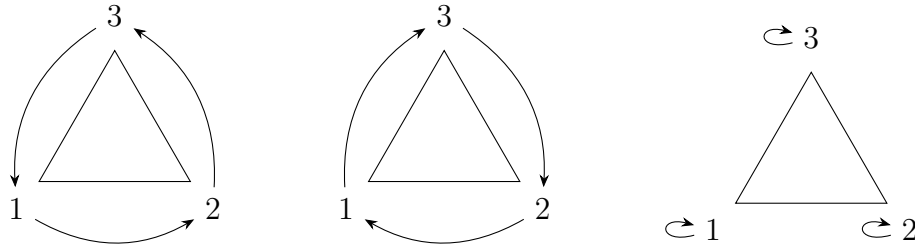


Figura 1.2: Todos los giros que dejan invariante al triángulo.

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.

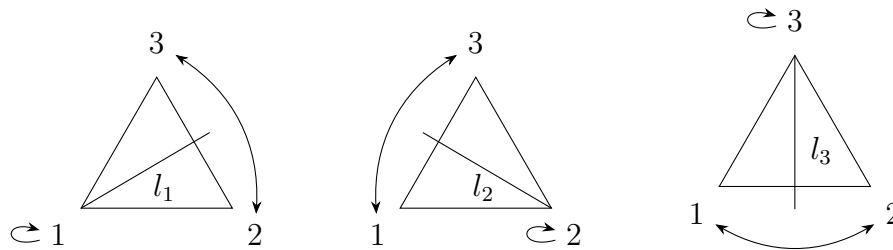


Figura 1.3: Todas las reflexiones que dejan invariante al triángulo.

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

Definición 1.7 (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 1.8 (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:

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

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 por:

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

Aprovechando la notación para los ciclos previamente definida.

Si por ejemplo extendemos σ a $\{1, 2, 3, 4, 5\}$ definiendo:

$$\sigma(5) = 5$$

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

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

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

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

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

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

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

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

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

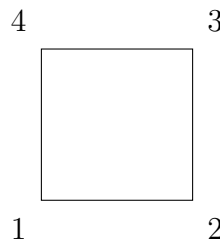


Figura 1.4: Cuadrado con centro en el origen de coordenadas.

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

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

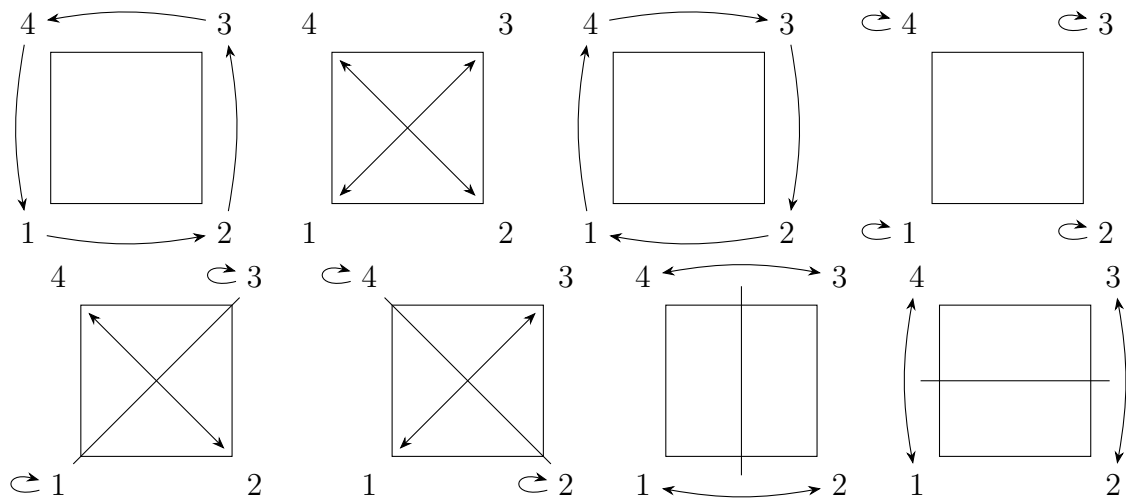


Figura 1.5: Giros y simetrías que dejan invariante al cuadrado

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 1.9 (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 1.9. *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 uno 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 1.9 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 1.9.

1.2. Generadores de un grupo

Definición 1.10 (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 $x = 0$, consideremos el producto de 0 elementos.

2. $D_n = \langle r, s \rangle$.

Definición 1.11 (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, que además nos podrán ayudar para definir grupos:

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. $D_1 := \langle s \mid s^2 = 1 \rangle$.

3. $D_2 := \langle r, s \mid r^2 = s^2 = 1, sr = rs \rangle$.

4. $C_n = \langle x \mid x^n = 1 \rangle$ es un grupo cíclico de orden n .

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

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

Ejercicio. Pensar cómo se relaciona Q_2^{abs} con el grupo de los cuaternios:

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

A partir de la presentación de Q_2^{abs} , somos capaces de describir todos sus elementos:

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

Es un grupo de orden 8 y vamos a fijarnos en los órdenes de sus elementos:

$$O(1) = 1$$

$$O(x^2) = 2$$

$$O(a) = 4 \quad \forall a \in Q_2^{\text{abs}} \setminus \{1, x^2\}$$

Esto podemos identificarlo dentro del grupo especial lineal $\text{SL}_2(\mathbb{C})$, mediante la identificación:

$$\begin{aligned} 1 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, x = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \\ x^2 &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, x^3 = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, xy = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \\ x^2y &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, x^3y = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \end{aligned}$$

En los cuaternios:

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

con:

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

$$ij = k$$

$$jk = i$$

$$ki = j$$

$$ji = -k$$

$$kj = -i$$

$$ik = -j$$

En positivo: $k \rightarrow i \rightarrow j \rightarrow k$. En negativo: $k \rightarrow j \rightarrow i \rightarrow k$.

Identificaremos:

$$\begin{aligned} 1 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \\ -1 &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, -i = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, k = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \\ -j &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, -k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \end{aligned}$$

1.3. Grupos Simétricos S_n

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

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

Consideraremos el caso en el que X sea finito, es decir, el caso $X = \{1, 2, \dots, n\}$, donde notaremos $S_n = S(X)$ y diremos que es el n -ésimo grupo simétrico, considerando la operación de composición. Se tiene que:

$$|S_n| = n!$$

Notación. Una forma de representar este grupo es mediante la representación matricial, que recoge la imagen de cada elemento. Sea $\sigma \in S_n$:

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

Ejemplo. Con este ejemplo vemos que S_5 no es un grupo abeliano (sin embargo, S_0 , S_1 y S_2 sí son abelianos, aunque a partir de S_3 no lo sea, $(1\ 2)$ y $(1\ 3)$):

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$$

Tenemos que:

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 1 & 3 \end{pmatrix} \neq \tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 2 & 3 \end{pmatrix}$$

Notación. Otra forma de notar σ es mediante la notación similar a los ciclos, la notación en ciclos disjuntos. En el ejemplo anterior:

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

Notación. Sea $\sigma \in S_n$ una permutación de forma que desplaza de forma circular el conjunto $\{a_1, a_2, \dots, a_m\} \subseteq X$, entonces llamaremos a σ ciclo de longitud m .

En cuyo caso, podemos representar a σ de m formas distintas:

$$\sigma = (a_1\ a_2\ \dots\ a_m) = (a_2\ a_3\ \dots\ a_m\ a_1) = \dots = (a_m\ \dots\ a_1\ a_2)$$

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.

Proposición 1.10. *Se verifica que:*

1. El orden de un ciclo de longitud m es m .

2. Si $\sigma = (a_1 \ a_2 \ \dots \ a_{m-1} \ a_m)$, entonces: $\sigma^{-1} = (a_m \ a_{m-1} \ \dots \ a_2 \ a_1)$.

Notación. Podemos descomponer una permutación σ en ciclos disjuntos:

$$\sigma = (a_1 \ a_2 \ \dots \ a_{m_1})(a_{m_1+1} \ \dots \ a_m) \dots (a_{m_k+1} \ \dots \ a_{m_{k+1}})$$

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:

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

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

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

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 .

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

En forma de ciclos disjuntos:

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

Teorema 1.11. 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 $i \in \{1, \dots, k\}$ son ciclos disjuntos de longitud mayor o igual que 2. Además, dicha descomposición es única, salvo el orden de los factores.

Demostración. Supuesto que trabajamos sobre $X = \{1, 2, \dots, n\}$, sea $\sigma \in S_n$ con $\sigma \neq 1$, definimos la relación:

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

Se verifica que R es una relación de equivalencia. De esta forma, dado $x \in X$:

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

Que es un conjunto finito (ya que $\sigma^{m+1}(x) = x$):

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

Si consideramos el ciclo:

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

Tenemos que:

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

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 .

Como γ_i no deja fijos a los elementos de C_i y γ_j no deja fijos a los elementos de C_j y $C_i \neq C_j$ para $i \neq j$, tenemos que los ciclos γ_i y γ_j son disjuntos.

Si ahora tomamos:

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

Entonces (si $y \in C_i$), se mantiene fijo y llega un momento en el que pasa a σ , donde luego se mantiene fijo.

$$\sigma(y) = \gamma_1 \gamma_2 \dots \gamma_i(y) = \gamma_1 \gamma_2 \dots \gamma_{i-1}(\sigma(y))$$

Para la unicidad: Supongamos que hay otra descomposición en ciclos y se llega a que en realidad es una reenumeración de las anteriores porque se llega a que las C s son las mismas viendo las imágenes. \square

Corolario 1.11.1. *Para σ un ciclo:*

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

Corolario 1.11.2. *El orden de una permutación $\sigma \in S_n$ es el mcm de las longitudes de los ciclos disjuntos en los que se descompone.*

Demostración. Supongamos que σ se descompone de la forma:

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

con $\gamma_i \gamma_j = \gamma_j \gamma_i$, tenemos que $\forall m \in \mathbb{N}$:

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

Si $m = O(x)$, entonces:

$$\sigma^m = 1 \iff \gamma_i^m = 1 \implies O(\gamma_i) \mid m \quad \forall i \implies \text{mcm} = m$$

\square

Ejemplo. Veamos los grupos S_n (recordando que $|S_n| = n!$):

1. En S_2 : tenemos $X = \{1, 2\}$ y tenemos las permutaciones:

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

2. En S_3 : tenemos $X = \{1, 2, 3\}$ y:

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

3. En S_4 : tenemos $X = \{1, 2, 3, 4\}$ y:

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

1.4. Grupos: generalidades y ejemplos

Ejercicio 1.4.1. 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 1.4.2. 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 1.4.3. 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 1.4.4. 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 $n = 3$:

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

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

- Para $n = 4$:

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

\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 1.4.5. 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 1.4.6. 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:

$$\begin{aligned} (xy)(xy) &= (xy)^2 = 1 \implies (xy)^{-1} = xy \\ (xy)(yx) &= x(yy)x = xy^2x = x1x = xx = x^2 = 1 \implies (xy)^{-1} = yx \end{aligned}$$

Por tanto, como en un grupo se tiene la unicidad del inverso, se tiene que $xy = yx$ para todo $x, y \in G$, por lo que G es abeliano.

Ejercicio 1.4.7. 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 1.4.8. 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 1.4.9. 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, 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.

- 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:

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

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 1.4.10.

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 1.4.11. 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 1.4.12. 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:

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

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 $f \circ f^{-1} = \text{Id}_{\mathbb{R}^2}$.
 - 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 1.4.13. 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 $r = r' \bmod n$ ($r' = nk + r$) 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 $s = s' \bmod m$ ($s' = mk + s$) 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 1.4.14. 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 1.4.15. 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.

Ejercicio 1.4.16. Sean s_1, s_2, p_1 y p_2 las permutaciones dadas en los ejercicios anteriores.

1. Descomponer la permutación $s_1 s_2 s_1 s_2$ como producto de ciclos disjuntos.
2. Expresar matricialmente la permutación $p_3 = p_2 p_1 p_2$ y obtener su descomposición como ciclos disjuntos.
3. Descomponer la permutación $s_2 p_2$ como producto de ciclos disjuntos y expresarla matricialmente.

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.

Ejercicio 1.4.17. 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 ?
2. Calcular el orden de $s_1(s_2)^{-1}(s_1)^{-1}$.
3. Calcular la permutación $(s_1)^{-1}$, y expresarla como producto de ciclos disjuntos.
4. Calcular la permutación $(p_1)^{-1}$ y expresarla matricialmente.
5. Calcular la permutación $p_2(s_2)^2(p_1)^{-1}$. ¿Cuál es su orden?

Ejercicio 1.4.18. 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 $s_1, s_4 p_1 p_2$ y $p_2 s_3$?

Ejercicio 1.4.19. En el grupo S_3 , se consideran las permutaciones $\sigma = (1\ 2\ 3)$ y $\tau = (1\ 2)$.

1. Demostrar que

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

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

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

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

Ejercicio 1.4.20. Describir los diferentes ciclos del grupo S_4 . Expresar todos los elementos de S_4 como producto de ciclos disjuntos.

Ejercicio 1.4.21. Demostrar que el conjunto de transposiciones

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

genera al grupo simétrico S_n .

Ejercicio 1.4.22. Demostrar que el conjunto $\{(1, 2, \dots, n), (1, 2)\}$ genera al grupo simétrico S_n .

Ejercicio 1.4.23. Demostrar que para cualquier permutación $\alpha \in S_n$ se verifica que $s(\alpha) = s(\alpha^{-1})$, donde s denota la signatura, o paridad, de una permutación.

Ejercicio 1.4.24. Demostrar que si $(x_1 x_2 \cdots x_r) \in S_n$ es un ciclo de longitud r , entonces

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

Ejercicio 1.4.25. Encontrar un isomorfismo $\mu_2 \cong \mathbb{Z}_3^\times$.

Ejercicio 1.4.26.

1. Demostrar que la aplicación

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

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 .

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

Ejercicio 1.4.27. Encontrar un isomorfismo $\mu_2 \times \mu_2 \cong \mathbb{Z}_8^\times$.

Ejercicio 1.4.28. Demostrar, haciendo uso de las representaciones conocidas, que $D_3 \cong S_3 \cong \text{GL}_2(\mathbb{Z}_2)$.

Ejercicio 1.4.29. Sea K un cuerpo y considérese la operación binaria

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

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

Ejercicio 1.4.30.

1. Probar que si $f : G \cong G'$ es un isomorfismo de grupos, entonces $o(a) = o(f(a))$, para todo elemento $a \in G$.
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.

Ejercicio 1.4.31. Calcular el orden de:

1. la permutación $\sigma = (1 \ 8 \ 10 \ 4 \ 5 \ 9)(2 \ 6 \ 3) \in S_{15}$.
2. cada elemento del grupo \mathbb{Z}_{11}^\times .

Ejercicio 1.4.32. 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.

Ejercicio 1.4.33. 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).
2. Demostrar que $o(ba) = o(ab)$.

Ejercicio 1.4.34. 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 $o(b) = 5$.

Ejercicio 1.4.35. Sea $f : G \rightarrow H$ un homomorfismo de grupos.

1. $f(x^n) = f(x)^n \quad \forall n \in \mathbb{Z}$.
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?
3. Si f es un isomorfismo entonces G es abeliano $\Leftrightarrow H$ es abeliano.

Ejercicio 1.4.36.

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

Ejercicio 1.4.37. Sea G un grupo. Demostrar:

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

Ejercicio 1.4.38. Si G es un grupo cíclico demostrar que cualquier homomorfismo de grupos $f : G \rightarrow H$ está determinado por la imagen del generador.

Ejercicio 1.4.39. Demostrar que no existe ningún cuerpo K tal que sus grupos aditivo $(K, +)$ y (K^*, \cdot) sean isomorfos.