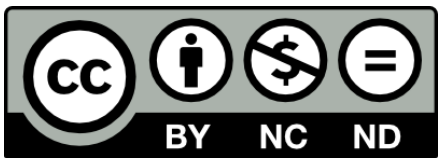
Álgebra II

Los Del DGIIM, losdeldgiim.github.io

Doble Grado en Ingeniería Informática y Matemáticas
Universidad de Granada



Álgebra II

Los Del DGIIM, `losdeldgiim.github.io`

José Juan Urrutia Milán

Granada, 2025

Índice general

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

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

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

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

[1]La operación cumplirá ciertas propiedades deseables.

1. Grupos: definición, generalidades y ejemplos

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

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

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

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

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

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 $*$:

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

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

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

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 $*$:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

11. Si X es un conjunto no vacío y consideramos

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

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

$$S_n = S(X)$$

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

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

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

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

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

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

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

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

Casos a destacar son:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

□

[2]Concepto 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) $x * x' = e \ \forall x \in G$.

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

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

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

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

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

Demostración. Demostramos cada una a partir de la anterior:

i) En primer lugar, observemos que:

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

Ahora:

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

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

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

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

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

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

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

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

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

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

□

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

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

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

Proposición 1.2. *En un grupo G se verifica la propiedad cancelativa (tanto a la izquierda como a la derecha):*

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

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

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

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

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

□

Proposición 1.3. *Sea G un grupo, entones:*

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

Demostración. Cada caso se demuestra observando sencillamante que:

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

□

Proposición 1.4. *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 ecuaciones[3]:

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

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

[3]Donde 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:

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

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

□

Proposición 1.5 (Ley asociativa general)**.** *Sea G un grupo, dados $n, m \in \mathbb{N}$ con $n > m > 0$, se tiene que:*

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

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 $m = 1$):

$$\left(\prod_{i=1}^{m} x_i\right)\left(\prod_{i=m+1}^{n} x_i\right) = x_1x_2 = \prod_{i=1}^{n} x_i \qquad \forall x_1, x_2 \in G$$

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

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

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

□

Definición 1.3 (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:*

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

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

1. $\underline{n > 0}$:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

   $$x^{n+m} \overset{(*)}{=} x^{m+n} = x^m \cdot x^n = x^n \cdot x^m$$

   donde en $(*)$ hemos usado la propiedad conmutativa de la suma en $\mathbb{Z}$.

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

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

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

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

□

Definición 1.4 (Grupos finitos e infinitos)**.** Sea G un grupo, si G como conjunto tiene[4] $n \in \mathbb{N} \setminus \{0\}$ elementos, diremos que es un grupo finito. En dicho caso, diremos que n es el "orden del grupo", notado por: $|G| = n$.
Si G no fuera finito, decimos que es un grupo infinito

Definición 1.5 (Tabla de Cayley)**.** En un grupo finito $G = \{x_1, x_2, \ldots, x_n\}$, se llama tabla de Cayley (o de multiplicar[5]) a la matriz $n \times n$ de forma que su entrada (i, j) es $x_i x_j$.

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

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

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

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

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

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

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

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

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

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

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

- Si consideramos un grupo abeliano, su tabla de Cayley será una matriz simétrica.
- Todos los elementos del grupo aparecen en todas las filas o columnas de la tabla de Cayley, ya que en la Proposición 1.4 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, notaremos[6]: $O(x) = ord(x) = n$.
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 $m \geqslant n$. En cuyo caso, $\exists q, r \in \mathbb{N}$ de forma que:

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

Pero entonces:

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

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

Proposición 1.8. *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:

[6]Podremos encontrarnos cualquiera de las dos notaciones.

1. Por doble implicación:

   $\Longleftarrow$) Trivial.

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

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

□

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

1. Si cogemos $x \neq 1$ en $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ con la multiplicación: $O(x) = +\infty$.

2. Si consideramos $\mathbb{C}$ con su multiplicación: $O(i) = 4$, ya que $i^4 = 1$.

3. En $\mathbb{Z}_9$, $O\left(\overline{6}\right) = 3$:

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

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

   - $O\left(\overline{2}\right) = 4$:

$$\begin{gathered} \overline{2} \neq \overline{1} \\ \overline{2+2} = \overline{4} \neq \overline{1} \\ \overline{2+2+2} = \overline{6} \neq \overline{1} \\ \overline{2+2+2+2} = \overline{8} = \overline{1} \end{gathered}$$

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

1.1. Grupos diédricos

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

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

1.1.1. Motivación

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

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

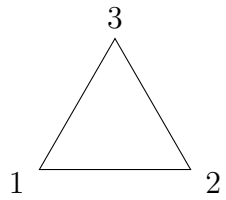


Figura 1.1: Triángulo equilátero con centro en el origen de coordenadas.

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

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

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

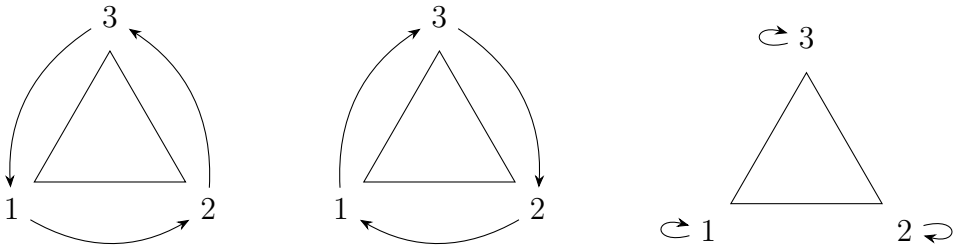


Figura 1.2: Todos los giros que dejan invariánte al triángulo.

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

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

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

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

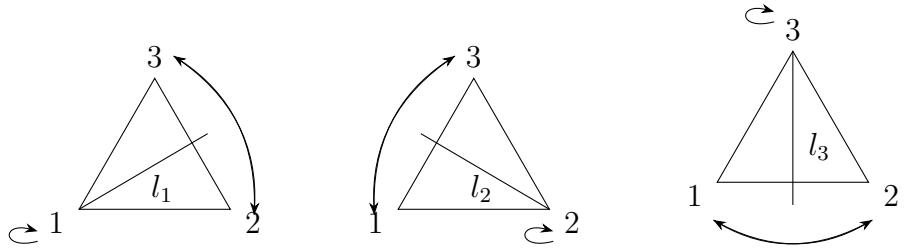


Figura 1.3: Todas las reflexiones que dejan invariante al triángulo.

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

Definición 1.7 (Permutación)**.** Sea X un conjunto, una permutación del mismo es cualquier aplicación biyectiva $f : X \to X$.

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

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

Definición 1.8 (Ciclo)**.** Sea $\{a_1, a_2, \ldots, a_m\} \subseteq \{1, 2, \ldots, n\}$, un ciclo de longitud $m \leqslant n$ es una permutación $\sigma \in S_n$ de forma que:

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

En dicho caso, representaremos a σ por:

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

Ejemplo. Para familiarizarnos con los ciclos, observamos que:

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

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

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

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

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

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.
- La simetría respecto a la recta l_3 es sr^2.

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.

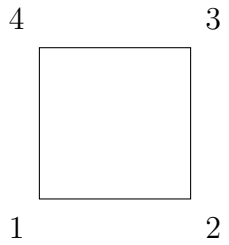


Figura 1.4: Cuadrado con centro en el origen de coordenadas.

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.

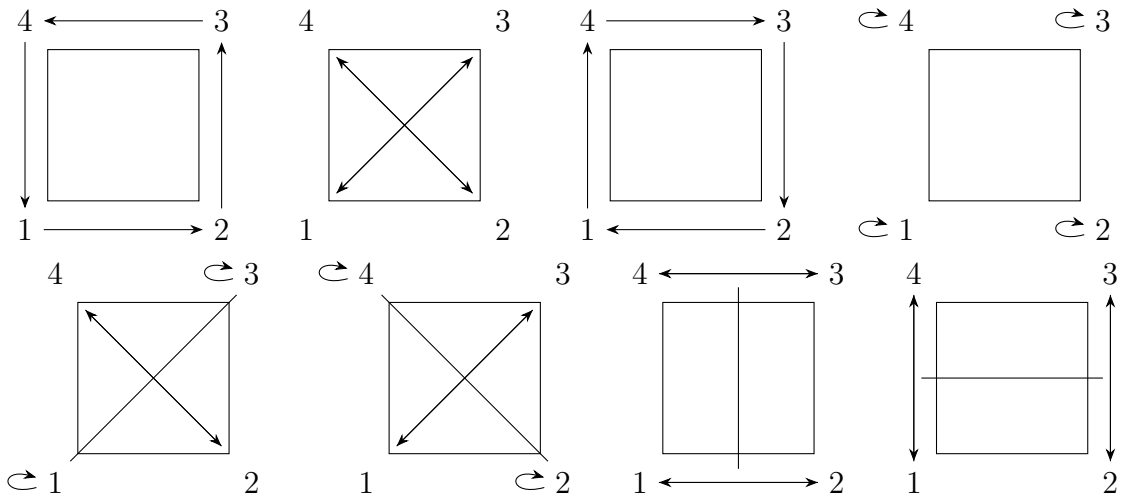


Figura 1.5: Giros y simetrías que dejan invariante al cuadrado

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

- El giro de ángulo $\frac{\pi}{2}$ es (1 2 3 4).
- El giro de ángulo π es (1 3) (2 4).
- El giro de ángulo $\frac{3\pi}{2}$ es (1 4 3 2).
- El giro de ángulo 2π es la identidad, (1).
- La simetría respecto a la recta que une 1 y 3 es (2 4).
- La simetría respecto a la recta que une 2 y 4 es (1 3).
- La simetría respecto a la mediatriz de 1 y 2 es (1 2) (3 4).
- La simetría respecto a la mediatriz de 2 y 3 es (1 4) (2 3).

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

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

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

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

De esta forma, si consideramos el conjunto:

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

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

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

1.1.2. Definición y primeras propiedades

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

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

Definición 1.9 (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:

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

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

Demostración. Demostramos cada uno de las propiedades:

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

6, 7. Son competencia de Geometría.

□

Usaremos los resultados de la Proposición 1.9 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, $S = \{x_1, x_2, \ldots, x_n\} \subseteq G$, podemos escribir:

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

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

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

i) S es un conjunto de generadores de G.

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

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

Ejemplo. Como ejemplos a destacar, vemos que:

1. $\mathbb{Z} = \langle 1 \rangle$ si pensamos en $(\mathbb{Z}, +, 0)$, ya que dado $x \in \mathbb{Z}$:
   - Si $x > 0$, entonces:
   $$x = \underbrace{1 + 1 + \ldots + 1}_{x \text{ veces}}$$

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

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

- Si $x = 0$, considermos 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 $R_1, R_2, \ldots, R_m$ (igualdades entre elementos de S, $\{1\}$ y los elementos simétricos de S) tal que cualquier relación entre los elementos de S puede deducirse de estas, entonces, decimos que estos generadores y relaciones constituyen una presentación de G, notado:

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

Ejemplo. Veamos que:

- En el diédrico D_n, tenemos que:

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

- $D_1 = \langle s, s^2 = 1 \rangle$.
- $D_2 = \langle r, s / r^2 = s^2 = 1, sr = rs \rangle$.
- $C_n = \langle x / x^n = 1 \rangle$ es un grupo cíclico de orden n.
- $V^{\text{abs}} = \langle x, y / x^2 = 1, y^2 = 1, (xy)^2 = 1 \rangle$ es el grupo de Klein abstracto.
- $Q_2^{\text{abs}} = \langle x, y / x^4 = 1, y^2 = x^2, yxy^{-1} = x \rangle$.

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

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