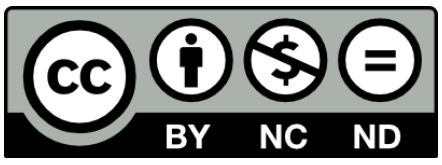
Álgebra II

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

1. Grupos: definición, generalidades y ejemplos

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 son:

1. La suma y el producto de números en $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, ...
2. Dado un conjunto X, consideramos las operaciones $\bigcup$, $\bigcap$ sobre $\mathcal{P}(X)$.

Definición 1.2 (Monoide)**.** Un monoide es un conjunto G no vacío junto con una operación binaria $*$ que verifica:

i) Asociatividad: $(x * y) * z = x * (y * z)\ \forall x, y, z \in G$.

ii) Existencia de elemento neutro: $\exists e \in G \mid e * x = x\ \forall x \in G$

Observación. En un monoide, el elemento neutro es único.

Demostración. □

Notación. Si X es un monoide con una operación binaria $*$ y un elemento neutro $e \in X$, será común hacer referencia al monoide por la tripleta:

$$(X, *, e)$$

Ejemplo. Ejemplos de monoides son (notando):

1. $(\mathbb{N}, +, 0)$, $(\mathbb{N}, \cdot, 1)$
2. $(\mathcal{P}(X), \cap, X)$, $(\mathcal{P}(X), \cup, \emptyset)$

Definición 1.3 (grupo)**.** Un grupo es un conjunto G no vacío junto con una operación binaria $*$ que verifica:

i) Asociatividad: $(x * y) * z = x * (y * z)\ \forall x, y, z \in G$.

ii) Existencia de elemento neutro: $\exists e \in G \mid e * x = x\ \forall x \in G$.

iii) Existencia de elemento simétrico[1]: $\forall x \in G\ \exists x' \in G \mid x' * x = e$.

[1] Al que luego llamaremos inverso en algunos casos.

Si además se cumple que:

iv) La propiedad conmutativa de $*$: $x * y = y * x \ \forall x, y \in G$.

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

Notación. Nos permitimos los siguientes abusos del lenguaje:

1. Por abuso de lenguaje, admitimos escribir G en lugar de $(G, *, e)$, en los casos en los que $*$ y e estén claros por el contexto.

2. Usaremos una notación multiplicativa usualmente, es decir, sustituiremos $*$ por $\cdot$ o por la yuxtaposición:

$$x * y = x \cdot y = xy$$

   Con esta notación, notaremos $e = 1$ y al elemento simétrico de x lo notaremos por x^{-1}.

3. En los casos con notación aditiva, escribiremos como operación $*$ el símbolo $+$, $\forall x \in G$.

   En estos casos, notaremos $e = 0$ y al elemento simétrico de x lo notaremos por $-x$, $\forall x \in G$.

Ejemplo. Consideramos los siguientes ejemplos:

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.

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

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

5. $GL_2(\mathbb{R})$, el grupo lineal[2] de orden 2 (con coeficientes en $\mathbb{R}$) con el producto de matrices es un grupo que no es abeliano.

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

7. $U(\mathbb{Z}_n) = \{[a] \in \mathbb{Z}_n \mid mcd(a, n) = 1\}$ con el producto es un grupo abeliano, $\forall n \in \mathbb{N}$.

8. Dado $n \geqslant 1$, $\mu_n = \{\text{raíces complejas de } x^n - 1\} = \{\xi_n = \cos\frac{2k\pi}{2} + i \operatorname{sen}\frac{2k\pi}{2} \mid k \in \mathbb{N}\}$ es un grupo abeliano con el proudcto.

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

9. El grupo lineal especial de orden 2 sobre el cuerpo $\mathbb{K}$:

$$SL_2(\mathbb{K}) = \{\text{matrices con determinante } 1\}$$

   siendo $\mathbb{K}$ un cuerpo con el producto de matrices es un grupo no abeliano.

[2]Es decir, el conjunto formado por todas las matrices regulares.

10. Sean G y H dos grupos, $G \times H$ es un grupo, considerando la operación binaria $* : (G \times H) \times (G \times H) \to G \times H$.

$$(x, y) * (x', y') = (xx', yy')$$

A $G \times H$ lo llamaremos grupo directo de G y H.

11. Si X es un conjunto no vacío y consideramos

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

será un grupo (no abeliano[3]) con la operación de composición $\circ$.

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

$$S_n = S(X)$$

12. Sea G un grupo y X un conjunto, consideramos el conjunto:

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

junto con la operación binaria de multiplicación de aplicaciones:

$$(f * g)(x) = f(x)g(x) \qquad \forall x \in X$$

De forma que la aplicación simétrica la calculamos de la forma[4]:

$$f'(x) = (f(x))'$$

Es un grupo. 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 conjunto $\{1\}$ con cualquier operación binaria es un grupo conmutativo, al que llamaremos grupo trivial.

Propiedades

Proposición 1.1. *En un grupo G, el neutro y el simétrico de cada elemento son únicos.*

Demostración. □

Proposición 1.2. *Sea G un grupo, entonces:*

i) $xx^{-1} = e \ \forall x \in G$

ii) $xe = x \ \forall x \in G$

Demostración. Veamos cada una de las propiedades:

[3]Compruébese

[4]En cada punto, la aplicacion simétrica es el simétrico del elemento $f(x)$.

i) Usando la unicidad del neutro $e \in G$:

$$x^{-1}(xx^{-1}) = (x^{-1}x)x^{-1} = ex^{-1} = x^{-1} \Longrightarrow xx^{-1} = e$$

ii)

$$xe = x(x^{-1}x) = (xx^{-1})x = ex = x$$

□

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

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

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

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

□

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

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

Demostración. Cada caso se demuestra observando sencillamante:

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

□

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

i) G es un grupo.

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

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

Tienen solución en G ($\exists c, d \in G \mid ac = b \wedge da = b$).

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

i) $\Rightarrow$ *ii)*

□

2. Relaciones de Ejercicios

2.1. Grupos: generalidades y ejemplos

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

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

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

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

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

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

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

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

Ejercicio 2.1.8. Demostrar que si en un grupo G, $x, y \in G$ verifican que $xy = yx$ entonces, para todo $n \geqslant 1$, se tiene que $(xy)^n = x^n y^n$.

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

Ejercicio 2.1.10.

1. Demostrar que $|\operatorname{GL}_2(\mathbb{Z}_2)| = 6$, describiendo explícitamente todos los elementos que forman este grupo.
2. Sea $\alpha = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ y $\beta = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Demostrar que
$$\operatorname{GL}_2(\mathbb{Z}_2) = \{1, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta\}.$$
3. Escribir, utilizando la representación anterior, la tabla de multiplicar de $\operatorname{GL}_2(\mathbb{Z}_2)$.

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

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

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

1. Demostrar que para todo $i = 0, \ldots, m-1$ se verifica $b^i a = ab^{ik}$.
2. Demostrar que para todo $j = 0, \ldots, n-1$ se verifica $ba^j = a^j b^{k^j}$.
3. Demostrar que para todo $i = 0, \ldots, m-1$ y todo $j = 0, \ldots, n-1$ se verifica $b^i a^j = a^j b^{ikj}$.
4. Demostrar que todo elemento de $\langle a, b\rangle$ puede escribirse como $a^r b^s$ con $0 \leqslant r < n$, $0 \leqslant s < m$.

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

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

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

Ejercicio 2.1.15. Dadas las permutaciones

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

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

Ejercicio 2.1.16. 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 $\{1, \ldots, 9\}$ que deja fijos a los elementos 8 y 9.

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

1. Calcular el orden de la permutación producto $s_1 s_2$. ¿Coincide dicho orden con el producto de los órdenes de s_1 y s_2?
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 2.1.18. Sean s_1, s_2, p_1 y p_2 las permutaciones dadas anteriormente. Sean también $s_3 = (2\ 4\ 6)$ y $s_4 = (1\ 2\ 7)(2\ 4\ 6\ 1)(5\ 3)$. ¿Cuál es la paridad de las permutaciones s_1, $s_4p_1p_2$ y p_2s_3?

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

1. Demostrar que
$$S_3 = \{1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}.$$
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 2.1.20. Describir los diferentes ciclos del grupo S_4. Expresar todos los elementos de S_4 como producto de ciclos disjuntos.

Ejercicio 2.1.21. Demostrar que el conjunto de transposiciones
$$\{(1,2),(2,3),\ldots,(n-1,n)\}$$
genera al grupo simétrico S_n.

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

Ejercicio 2.1.23. 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 2.1.24. Demostrar que si $(x_1x_2\cdots x_r) \in S_n$ es un ciclo de longitud r, entonces
$$s(x_1x_2\cdots x_r) = (-1)^{r-1}.$$

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

Ejercicio 2.1.26.

1. Demostrar que la aplicación
$$1 \mapsto 1, \qquad -1 \mapsto 4, \qquad i \mapsto 2, \qquad -i \mapsto 3,$$
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 2.1.27. Encontrar un isomorfismo $\mu_2 \times \mu_2 \cong \mathbb{Z}_8^\times$.

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

Ejercicio 2.1.29. Sea K un cuerpo y considérese la operación binaria

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

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

Ejercicio 2.1.30.

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 2.1.31. 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 2.1.32. Demostrar que un grupo generado por dos elementos distintos de orden dos, que conmutan entre sí, consiste del 1, de esos elementos y de su producto y es isomorfo al grupo de Klein.

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

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

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

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

1. $f(x^n) = f(x)^n\ \forall n \in \mathbb{Z}$.
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 2.1.36.

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

Ejercicio 2.1.37. Sea G un grupo. Demostrar:

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

2. G es abeliano $\iff$ la aplicación $f : G \to G$ dada por $f(x) = x^2$ es un homomorfismo de grupos.

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

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