

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
---	---

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. El grupo lineal de orden 2 con coeficientes en \mathbb{R} :

$$GL_2(\mathbb{R}) = \{M \in \mathcal{M}_2(\mathbb{R}) : \det(M) \neq 0\}$$

con el producto heredado de $\mathcal{M}_2(\mathbb{R})$ es un grupo abeliano.

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

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:

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

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:

$$SL_2(\mathbb{K}) = \{M \in \mathcal{M}_2(\mathbb{K}) : \det(M) = 1\}$$

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

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

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:

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

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.

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

²Concepto que luego formalizaremos.

iv) Dado $x \in G$, sea $x'' \in G$ de forma que $x'' * x = x$, 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: $\exists c, d \in G \mid ac = b \wedge da = b$.

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 $ea = a$.

Por otra parte, 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 $x \in G$.

□

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