

Extraordinaria Estructuras Algebraicas

Antonio Cabrera Landín

6 de junio de 2025

Índice

1. Teoremas	3
1.1. Teorema (Propiedad cancelativa)	3
1.2. Teorema	3
1.3. Teorema	3
1.4. Teorema	3
1.5. Teorema	3
1.6. Teorema	3
1.7. Lema	3
1.8. Teorema	4
1.9. Teorema (Teorema de Caley)	4
1.10. Teorema	4
1.11. Teorema	4
1.12. Lema	5
1.13. Teorema	5
1.14. Teorema (Teorema de Lagrange)	5
1.15. Colorario	5
1.16. Teorema	5
1.17. Teorema	5
1.18. Teorema	6
1.19. Teorema	6
1.20. Teorema	6
1.21. Teorema	7
1.22. Teorema	7
1.23. Teorema	7
1.24. Teorema (Pimer teorema de isomorfía)	7
2. Problemas	8
2.1. Buscar el orden de algunos elementos del grupo	8
2.2. Averiguar si algún conjunto es semigrupo, monoide o grupo.	8
2.3. Determinar si algún subconjunto es subgrupo. Determinar si un subgrupo es normal.	10
2.4. Buscar los subgrupos normales. Determinar a qué grupos son isomorfos los grupos cocientes correspondientes.	10
2.5. Buscar los subgrupos, hallar el retículo de los subgrupos.	10
2.6. Calcular operaciones en los grupos (diédrico, simétrico, etc.). Hallar el conmutador y el conjugado de dos elementos.	10
2.7. Hallar el orden y la signatura de un elemento de un grupo simétrico.	10
2.8. Hallar el centro y el conmutador de un grupo dado.	10
2.9. Comprobar el isomorfismo entre dos o más grupos o demostrar que no pueden ser isomorfos.	10
2.10. Comprobar el isomorfismo/comprobar que una función lo define. Buscar Ker, Im de un homomorfismo.	10
2.11. Calcular la cantidad de homomorfismos o isomorfismos de grupos.	10
2.12. Comprobar que un grupo es soluble o demostrar que no lo es.	10
2.13. Buscar las clases izquierdas o derechas. Hallar el grupo cociente.	10

2.14. Encontrar el subgrupo de un grupo simétrico isomorfo a un grupo dado.	10
---	----

1. Teoremas

Teorema 1.1 (Propiedad cancelativa). *Para todo grupo $G = \{X, \cdot\}$ se cumple*

$$a \cdot c = b \cdot c \implies a = b \quad (1)$$

$$c \cdot a = c \cdot b \implies a = b \quad (2)$$

Demostración.

$$a \cdot c = b \cdot c \iff a \cdot c \cdot c^{-1} = b \cdot c \cdot c^{-1} \iff a \cdot e = b \cdot e \iff a = b \quad (3)$$

$$c \cdot a = c \cdot b \iff c^{-1} \cdot c \cdot a = c^{-1} \cdot c \cdot b \iff e \cdot a = e \cdot b \iff a = b \quad (4)$$

□

Teorema 1.2. *En cada grupo solo puede existir un elemento neutro.*

Demostración. Sea el grupo $G = \{X, \cdot\}$ asumamos que tenga dos elementos neutros e_1 y e_2 , entonces

$$\begin{cases} x \cdot e_1 = x \\ x \cdot e_2 = x \end{cases} \implies x \cdot e_1 = x \cdot e_2 \iff x^{-1} \cdot x \cdot e_1 = x^{-1} \cdot x \cdot e_2 \iff e \cdot e_1 = e \cdot e_2 \iff e_1 = e_2 \quad (5)$$

□

Teorema 1.3. *Dado un grupo $G = \{X, \cdot\}$, si para cualquier elemento $a \in G$ se cumple que $a \cdot a = e$, entonces G es abeliano.*

$$\forall a \in G : a \cdot a = e \implies \forall a, b \in G : a \cdot b = b \cdot a \quad (6)$$

Demostración.

$$a \cdot b \in G \implies (ab)^2 = ab \cdot ab = e \quad (7)$$

$$\begin{aligned} aabb = e \cdot e = e = (ab)^2 &\implies a^{-1}(aabb) = a^{-1}(abab) \iff \\ abb = bab &\iff (abb)b^{-1} = (bab)b^{-1} \iff ab = ba \end{aligned} \quad (8)$$

□

Teorema 1.4. *Dado un grupo $G = \{X, \cdot\}$, si para todo $a, b \in G$ se cumple que $(a \cdot b)^2 = a^2 \cdot b^2$, entonces G es abeliano*

$$\forall a, b \in G : (a \cdot b)^2 = a^2 \cdot b^2 \implies \forall a, b \in G : a \cdot b = b \cdot a \quad (9)$$

Demostración.

$$\begin{aligned} (a \cdot b)^2 = a^2 \cdot b^2 &\implies abab = aabb \iff a^{-1}(abab) = a^{-1}(aabb) \iff \\ bab = abb &\iff (bab)b^{-1} = (abb)b^{-1} \iff ba = ab \end{aligned} \quad (10)$$

□

Teorema 1.5. \mathbb{Z}_n tiene $\varphi(n)$ generadores

Teorema 1.6. *Dado un grupo $G = \{X, \cdot\}$, para todos sus elementos $a \in G$ el inverso del inverso de a es a .*

$$\forall a \in G : (a^{-1})^{-1} = a \quad (11)$$

Demostración.

$$(a^{-1})^{-1} \cdot a^{-1} = e \iff (a^{-1})^{-1} \cdot a^{-1} \cdot a = e \cdot a \iff (a^{-1})^{-1} = a \quad (12)$$

□

Lema 1.7. *Dado un grupo $G = \{X, \cdot\}$, para cada pareja $a, b \in G$ se cumple que $(a \cdot b)^{-1} = b^{-1}a^{-1}$*

Demostración.

$$\begin{aligned}
(a \cdot b)^{-1}(a \cdot b) = e &\iff (a \cdot b)^{-1}(a \cdot b) \cdot b^{-1} = e \cdot b^{-1} \iff \\
(a \cdot b)^{-1}a = b^{-1} &\iff (a \cdot b)^{-1}a \cdot a^{-1} = b^{-1}a^{-1} \iff \\
(a \cdot b)^{-1} &= b^{-1}a^{-1}
\end{aligned} \tag{13}$$

□

Teorema 1.8. *Dado un grupo $G = \{X, \cdot\}$, para cada pareja $a, b \in G$ el orden de ab es el mismo que el de ba*

$$\forall a, b \in G : (a \cdot b)^k = e \iff (b \cdot a)^k = e \tag{14}$$

Demostración.

$$\begin{aligned}
(ab)^k &= ab \cdot ab \cdots ab = a \cdot (ba \cdots ba) \cdot b = a \cdot (ba)^{k-1} \cdot b = e \iff \\
a^{-1} \cdot a \cdot (ba)^{k-1} \cdot b &= a^{-1} \iff (ba)^{k-1} \cdot b = a^{-1} \iff \\
(ba)^{k-1} \cdot b \cdot b^{-1} &= a^{-1}b^{-1} \iff (ba)^{k-1} = a^{-1}b^{-1} \stackrel{\text{lema 1.7}}{\downarrow} (ba)^{-1} \iff \\
(ba)^{k-1}(ba) &= (ba)^{-1}(ba) \iff (ba)^k = e
\end{aligned} \tag{15}$$

□

Teorema 1.9 (Teorema de Caley). *Todo grupo G es isomorfo a un subgrupo de las biyecciones de G , $B(G)$, que es el grupo simétrico.*

Teorema 1.10. *El centro de un grupo es un subgrupo y es normal.*

Demostración. El centro $Z(G)$ es un subgrupo de G

1. El centro $Z(G)$, al mantener la operación de G , seguirá cumpliendo la propiedad asociativa.
2. El centro mantiene el neutro:

$$\forall x \in G : e \cdot x = x \cdot e \implies e \in Z(G) \tag{16}$$

3. Si x está en el centro entonces su inverso x^{-1} también:

$$\begin{aligned}
x \in Z(G) &\implies \forall g \in G : g \cdot x^{-1} = x \cdot x^{-1} \cdot g \cdot x^{-1} = \\
x^{-1} \cdot g \cdot x \cdot x^{-1} &= x^{-1} \implies x^{-1} \in Z(G)
\end{aligned} \tag{17}$$

□

Demostración. El centro $Z(G)$ es un subgrupo normal

$$\begin{aligned}
\forall h \in Z(G), g \in G : g \cdot h \cdot g^{-1} &= g \cdot g^{-1} \cdot h = h \implies \\
gHg^{-1} &= H \implies Z(G) \text{ subgrupo normal}
\end{aligned} \tag{18}$$

□

Teorema 1.11. *Todos los subgrupos de índice 2 son normales*

Demostración. Si un subgrupo tiene índice 2, significa que solo tiene dos clases laterales izquierdas y 2 clases laterales derechas.

Tendremos dos clases laterales izquierdas, aH y bH . Como e estará en una de las dos, podemos hablar de H y xH . Lo mismo ocurre con las clases laterales derechas, tendremos H y Hx

$$\begin{cases} H \cup xH = G \\ H \cup Hx = G \end{cases} \implies xH = Hx \implies H \text{ es normal} \tag{19}$$

□

Lema 1.12. Si $a \in xH$ entonces $xH = aH$

Demostración.

$$a \in xH \implies \exists h \in H : a = xh \iff aH = xhH \implies aH = xH \quad (20)$$

□

Teorema 1.13. Las clases laterales izquierdas o coinciden o no tienen intersección.

Demostración. Dado un grupo $G = \{X, \cdot\}$ con un subgrupo $H \subseteq G$. Supongamos que $\exists a \in xH$ que además $a \in yH$, entonces:

$$\begin{cases} a \in xH \implies \exists h_1 \in H : a = xh_1 \\ a \in yH \implies \exists h_2 \in H : a = yh_2 \end{cases} \implies xh_1 = yh_2 \iff xh_1 \cdot h_1^{-1} = yh_2h_1^{-1} \iff x = yh_2h_1^{-1} = yh_3, h_3 \in H \implies x \in yH \quad (21)$$

Utilizando el lema 1, sabemos que $x \in yH \implies xH = yH$.

□

Teorema 1.14 (Teorema de Lagrange). El orden del grupo es múltiplo del orden del subgrupo

$$H \subseteq G \implies |G| = |H| \cdot n \quad n \in \mathbb{N} \quad (22)$$

Demostración. Dado un grupo G con un subgrupo H y con clases laterales x_iH , por el teorema 1.13 sabemos que las clases laterales no tienen intersección. Como tienen que abarcar a todo el grupo G y no tienen intersección, entonces necesariamente el orden de G será múltiplo del orden de las clases laterales.

$$\sum_{i=1}^{\text{índice}} |x_iH| = |G| \implies |G| = |x_iH| \cdot n \quad n \in \mathbb{N} \quad (23)$$

Las clases laterales x_iH tienen el mismo orden que H , ya que se construyen operando x_i con los elementos de H , entonces el orden de G es múltiplo del orden de H .

$$|x_iH| = |H| \implies |G| = |H| \cdot n \quad n \in \mathbb{N} \quad (24)$$

□

Colorario 1.15. El orden del grupo es múltiplo del orden de un elemento

$$x \in G : x^k = e \implies |G| = k \cdot n \quad n \in \mathbb{N} \quad (25)$$

Teorema 1.16. Cualquier grupo de orden primo es cíclico

$$|G| = p \text{ primo} \implies \exists x \in G : x^p = e \quad (26)$$

Demostración. Por el colorario 1.15 sabemos que el orden del grupo tiene que ser múltiplo del orden de los elementos. Como el orden del grupo es primo, los elementos solo pueden tener orden 1 u orden p . Por el teorema 1.2, el único elemento de orden 1 es el neutro, entonces el resto de elementos del grupo tienen orden p . Como existe al menos un elemento de orden p , el grupo es cíclico. □

Teorema 1.17. Si $H \subset G$ es un subgrupo, entonces gHg^{-1} , con $g \in G$, también lo es.

$$H \subset G \implies gHg^{-1} \subset G \quad g \in G \quad (27)$$

Demostración. gHg^{-1} cumple con las tres propiedades de los subgrupos:

1. gHg^{-1} seguirá manteniendo la propiedad asociativa ya que solo hemos operado los elementos de H con elementos de G .

2. El elemento neutro $e \in G$ está en gHg^{-1} :

$$e \in H \implies g \cdot e \cdot g^{-1} = g \cdot g^{-1} = e \implies e \in gHg^{-1} \quad (28)$$

3. Cada elemento $x = ghg^{-1} \in gHg^{-1}$ tiene inverso x^{-1} :

$$ghg^{-1} \cdot g(h^{-1})g^{-1} = gh(h^{-1})g^{-1} \cdot g^{-1} = gg^{-1} = e \implies g(h^{-1})g = x^{-1} \in gHg^{-1} \quad (29)$$

□

Teorema 1.18. Para todo grupo $G = \{X, \cdot\}$ con un subgrupo $H \subset G$:

$$gHg^{-1} = H \quad g \in G \iff xH = Hx \quad (30)$$

Demostración. \implies

$$gHg^{-1} = H \iff gHg^{-1} \cdot g = Hg \iff gH = Hg \quad h \in G \quad (31)$$

□

Demostración. \Leftarrow

$$xH = Hx \implies xH \cdot x^{-1} = Hx \cdot x^{-1} \iff xHx^{-1} = H \quad x \in G \quad (32)$$

□

Teorema 1.19. Las clases laterales izquierdas x_iH de un subgrupo H normal, forman un grupo.

Demostración. Las clases laterales izquierdas de un subgrupo H cumplen con las tres propiedades de los grupos:

1. La operación no se sale del conjunto y por tanto conserva la propiedad asociativa:

$$xH = Hx \implies \forall a \in xH : xH \cdot yH = xyHH = xyH \implies ab \in xyH \quad (33)$$

2. El neutro pertenece a la clase lateral izquierda eH .

3. Todo elemento $a \in xH$ tiene inverso $a^{-1} \in (x^{-1})H$:

$$\forall a = xh_1 \in xH \exists a^{-1} = (x^{-1})h_2 \in (x^{-1})H : h_1x \cdot (x^{-1})h_2 = h_1h_2 \in eH \quad h_1, h_2 \in H \quad (34)$$

□

Teorema 1.20. El conmutador es un subgrupo y es normal.

Demostración. El conmutador $G' = \{<[a, b]> : a, b \in G\}$ es un subgrupo.

1. Como estamos operando elementos de G con la misma operación, se seguirá conservando la propiedad asociativa.

2. El elemento neutro $[a, e] = e$ pertenece a C :

$$[a, e] = a \cdot e \cdot a^{-1} \cdot e^{-1} = a \cdot e \cdot a^{-1} \cdot e = a \cdot a^{-1} = e \implies e \in C \quad a, b \in G \quad (35)$$

3. Todo elemento $x = [a, b]$ tiene inverso $x^{-1} = [b, a]$

$$\begin{aligned} \forall x = [a, b] &= aba^{-1}b^{-1} \in C \exists x^{-1} = [b, a] = bab^{-1}a^{-1} \in C : x \cdot x^{-1} = \\ &= aba^{-1}b^{-1} \cdot bab^{-1}a^{-1} = aba^{-1}ab^{-1}a^{-1} = abb^{-1}a^{-1} = aa^{-1} = e \end{aligned} \quad (36)$$

□

Demostración. El conmutador $C = \langle [a, b] \rangle$ es un subgrupo normal.

$$\forall h \in G' : aha^{-1} = aha^{-1}h^{-1}h = [a, h] \cdot h \in G' \implies g(G')g = G' \quad (37)$$

□

Teorema 1.21. *El núcleo de un homomorfismo es un subgrupo y es normal.*

Teorema 1.22. *La imagen de un homomorfismo es un subgrupo.*

Teorema 1.23. *La aplicación $G \rightarrow G/H : \pi(g) = gH$ es un homomorfismo suprayectivo.*

Teorema 1.24 (Primer teorema de isomorfía).

2. Problemas

2.1. Buscar el orden de algunos elementos del grupo

2.2. Averiguar si algún conjunto es semigrupo, monoide o grupo.

1. El conjunto de cadenas de símbolos ("*string*") con la concatenación como operación binaria.

a) Cumple con la propiedad asociativa:

$$("a" + "b") + "c" = "a" + ("b" + "c") = "abc" \quad (38)$$

b) El elemento neutro es la cadena vacía (""):

$$"a" + "" = "a" \quad (39)$$

c) No existe elemento inverso

Por lo tanto, se trata de un monoide.

2. El conjunto {Hija, Madre, Abuela} con la operación "*La mayor de las dos*".

a) Cumple con la propiedad asociativa, ya que el resultado siempre será el mayor de todos:

$$\begin{aligned} \text{Hija} * (\text{Madre} * \text{Abuela}) &= \text{Hija} * \text{Abuela} = \text{Abuela} = \\ (\text{Hija} * \text{Madre}) * \text{Abuela} &= \text{Madre} * \text{Abuela} = \text{Abuela} \end{aligned} \quad (40)$$

b) El elemento neutro es $e = \text{Hija}$:

$$\text{Hija} * \text{Hija} = \text{Hija} \quad \text{Madre} * \text{Hija} = \text{Madre} \quad \text{Abuela} * \text{Hija} = \text{Abuela} \quad (41)$$

c) No existe el elemento inverso.

Por lo tanto, se trata de un monoide.

3. El conjunto {Giro de 0° , Giro de 120° , Giro de 240° } con la composición de giros.

a) Cumple con la propiedad asociativa, ya que no importa que giro aplicar primero, al final saldrán los mismo grados.

$$(0^\circ * 120^\circ) * 240^\circ = 120^\circ * 240^\circ = 0^\circ = 0^\circ * (120^\circ * 240^\circ) = 0^\circ * 0^\circ = 0^\circ \quad (42)$$

b) El elemento neutro es el giro de 0 grados $e = 0^\circ$

c) Cada elemento tiene un inverso:

$$\begin{aligned} 0^\circ * 0^\circ &= 0^\circ \implies (0^\circ)^{-1} = 0^\circ \\ 120^\circ * 240^\circ &= 0^\circ \implies (120^\circ)^{-1} = 240^\circ \\ 240^\circ * 120^\circ &= 0^\circ \implies (240^\circ)^{-1} = 120^\circ \end{aligned} \quad (43)$$

Por lo tanto, se trata de un grupo.

4. Los enteros positivos pares con la operación suma.

a) Al tratarse de la suma de enteros, cumple la propiedad asociativa.

b) El neutro 0, no pertenece al conjunto, por lo tanto no existe un neutro.

Se trata de un semigrupo.

5. Los enteros positivos pares más el cero con la operación suma.

- a) Al tratarse de la suma de enteros, cumple la propiedad asociativa.
- b) El neutro es el 0, ya que se trata de la suma.
- c) Al no tener negativos, el único elemento con inverso es el 0.

Por lo tanto, se trata de un monoide.

6. \mathbb{Q} con la suma.

- a) Al tratarse de la suma de racionales, cumple la propiedad asociativa.
- b) El neutro es $0 \in \mathbb{Q}$, ya que se trata de la suma.
- c) Cada elemento $a \in \mathbb{Q}$ tiene inverso $-a \in \mathbb{Q}$

Por lo tanto, se trata de un grupo.

7. \mathbb{Q} con la multiplicación.

- a) Al tratarse del producto de racionales, cumple la propiedad asociativa.
- b) El 1 es el elemento neutro.
- c) Todos los elementos tienen inverso excepto el 0.

Por lo tanto, se trata de un monoide. Para que fuese un grupo, habría que eliminar al 0 del conjunto.

8. $\mathbb{R} \setminus \{0\}$ con la división.

- a) La división no cumple con la propiedad asociativa.

Por lo tanto, no es ni semigrupo, ni monoide, ni grupo.

9. \mathbb{Z} con la suma.

- a) Al tratarse de la suma de enteros, cumple con la propiedad asociativa.
- b) El 0 es el elemento neutro.
- c) Cada elemento $a \in \mathbb{Z}$ tiene inverso $-a \in \mathbb{Z}$.

Por lo tanto, se trata de un grupo.

10. $\mathbb{R} \setminus \{0\}$ con la operación $a \cdot b = 3ab$

- a) Como en la operación solo intervienen productos, cumple con la propiedad asociativa.
- b) El elemento inverso es $e = \frac{1}{3}$:

$$a \cdot \frac{1}{3} = 3a \cdot \frac{1}{3} = a \quad (44)$$

- c) El inverso de a es $a^{-1} = \frac{1}{9a}$:

$$a \cdot \frac{1}{9a} = 3a \cdot \frac{1}{9a} = \frac{1}{3} = e \quad (45)$$

Por lo tanto, es un grupo.

11. $\mathbb{R} \setminus \{-1\}$ con la operación $a \cdot b = a + b + ab$

- a) Como en la operación solo intervienen sumas y productos, cumple con la propiedad asociativa.
- b) El elemento neutro es el 0:

$$a \cdot 0 = a + 0 + a \cdot 0 = a \quad (46)$$

- c) El inverso de a es $a^{-1} = -\frac{a}{1+a}$:

$$a + a^{-1} + aa^{-1} = 0 \iff a^{-1}(1+a) + a = 0 \iff a^{-1} = -\frac{a}{1+a} \quad (47)$$

Por lo tanto, se trata de un grupo.

- 2.3. Determinar si algún subconjunto es subgrupo. Determinar si un subgrupo es normal.
- 2.4. Buscar los subgrupos normales. Determinar a qué grupos son isomorfos los grupos cocientes correspondientes.
- 2.5. Buscar los subgrupos, hallar el retículo de los subgrupos.
- 2.6. Calcular operaciones en los grupos (diédrico, simétrico, etc.). Hallar el conmutador y el conjugado de dos elementos.
- 2.7. Hallar el orden y la signatura de un elemento de un grupo simétrico.
- 2.8. Hallar el centro y el conmutador de un grupo dado.
- 2.9. Comprobar el isomorfismo entre dos o más grupos o demostrar que no pueden ser isomorfos.
- 2.10. Comprobar el isomorfismo/comprobar que una función lo define. Buscar Ker , Im de un homomorfismo.
- 2.11. Calcular la cantidad de homomorfismos o isomorfismos de grupos.
- 2.12. Comprobar que un grupo es soluble o demostrar que no lo es.
- 2.13. Buscar las clases izquierdas o derechas. Hallar el grupo cociente.
- 2.14. Encontrar el subgrupo de un grupo simétrico isomorfo a un grupo dado.