Una introducción a la Teoría de Grupos

Héctor Barrantes González
Reiman Acuña Chacón
Bolívar Ramírez Santamaría

Primera Edición 2025

Revista digital Matemática Educación e Internet (https://tecdigital.tec.ac.cr/servicios/revistamatematica/).
Correo Electrónico: reiacuna@itcr.ac.cr
Escuela de Matemática
Instituto Tecnológico de Costa Rica
Apdo. 159-7050, Cartago
Teléfono (506) 25502225.

Barrantes González, H., AAcuña Chacón, R., Ramírez Santamaría, B.
Una introducción a la Teoría de Grupos. 1ra ed.
– Escuela de Matemática,Instituto Tecnológico de Costa Rica. 2026.
399 pp.
ISBN Obra Independiente: 978-9930-617-90-8
1. El conjunto de los números enteros.
2. Teoría de Grupos.
3. Aplicaciones.

Revista digital
Matemática, Educación e Internet.
https://tecdigital.tec.ac.cr/servicios/revistamatematica/.

Citar como:

Barrantes, H., Acuña, R., & Ramírez, B. (2025). *Introducción a la teoría de grupos* (1.ª ed.) [E-book]. Revista Digital Matemática, Educación e Internet. Disponible en https://tecdigital.tec.ac.cr/servicios/revistamatematica/material_didactico/libros/. ISBN 978-9930-617-90-8

Índice general

Capítulo 1

El conjunto de los números enteros

Dios hizo los números enteros, el resto es obra del hombre

Leopold Kronecker

El Álgebra, como disciplina matemática, se presenta, en cierto sentido, como una generalización de los números enteros y sus propiedades fundamentales, brindando un marco conceptual aplicable a diversos contextos matemáticos. Este capítulo se centra en el examen de propiedades significativas de los números enteros y de la aritmética modular. Estas propiedades, detalladas en este contexto, se revelan como herramientas esenciales que se emplearán de manera recurrente en los temas subsecuentes, contribuyendo así a la comprensión y resolución de problemas matemáticos más avanzados.

1.1 Propiedades básicas

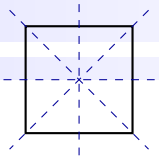
Las definiciones y teoremas recordados en este apartado acera del conjunto de los números enteros, principio de buena ordenación, divisibilidad, entre otros, serán fundamentales para el tema de Grupos.

Definición 1.1.1:

Se llama **Conjunto de los números enteros** al conjunto

$$\mathbb{Z} := \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

Observación 1.1.1.



Sobre la definición 1.1 anterior, es importante considerar los siguientes aspectos:

1. Se pueden definir el conjunto de los números enteros negativos como

$$\mathbb{Z}^- := \{\ldots, -4, -3, -2, -1\}$$

y el conjunto de los números enteros positivos como

$$\mathbb{Z}^+ := \{1, 2, 3, 4, \ldots\}.$$

2. De acuerdo con los puntos anteriores,

$$\mathbb{Z} = \mathbb{Z}^- \cup \{0\} \cup \mathbb{Z}^+.$$

3. Cuando se indica el conjunto de los números enteros **no negativos**, corresponde al conjunto formado por

$$\{0\} \cup \mathbb{Z}^+ = \{0, 1, 2, 3, 4, \ldots\}.$$

4. Aunque no se ha definido el conjunto de los números naturales, denotado por $\mathbb{N}$, este corresponde al conjunto de los números enteros positivos, es decir,

$$\mathbb{N} := \{1, 2, 3, 4, \ldots\}.$$

5. A partir de lo puntos anteriores, se deducen las siguientes relaciones de inclusión:

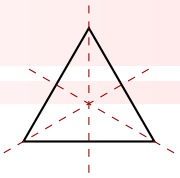
   a) $\mathbb{Z}^- \subseteq \mathbb{Z}$. *b*) $\mathbb{Z}^+ \subseteq \mathbb{Z}$. *c*) $\mathbb{N} \subseteq \mathbb{Z}$.

6. En el conjunto de los números enteros se tienen dos operaciones, llamadas suma y multiplicación, que satisfacen las propiedades mostradas a continuación.

Axioma 1.1.1:

Sea $a, b, c \in \mathbb{Z}$, entonces se cumple que:

1. $(a + b) + c = a + (b + c)$.
2. $a + b = b + a$.
3. Existe $0 \in \mathbb{Z}$ tal que $a + 0 = 0 + a$.



4. Existe $-a \in \mathbb{Z}$ tal que $a + (-a) = 0$.
5. $(ab)c = a(bc)$.
6. $ab = ba$.
7. $1 \cdot a = a$.
8. $a(b + c) = ab + ac$.
9. $ab = 0$ si y sólo si $a = 0$ o $b = 0$.

Teorema 1.1.1: Principio de la buena ordenación.

Todo subconjunto no vacío de enteros no negativos, tiene un elemento mínimo.

Ejemplo 1.1.1.

El elemento mínimo del conjunto de los números naturales $\mathbb{N}$, es el 1.

Definición 1.1.2:

Se dice que $a \in \mathbb{Z}$ **divide** a $b \in \mathbb{Z}$, si existe $q \in \mathbb{Z}$ tal que $b = aq$. Si a divide a b se escribe $a \mid b$.

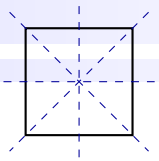
Ejemplo 1.1.2.

El entero $a = 4$ divide a $b = 20$, pues existe $q = 5$ tal que $20 = 4 \cdot 5$. De acuerdo con la definición anterior, se escribe $4 \mid 20$.

Teorema 1.1.2:

Para cualesquiera $m, n, a, b, c \in \mathbb{Z}$ se cumplen las siguientes propiedades:

1. $a|a$.
2. Si $a|b$ y $b|c$ entonces $a|c$.
3. Si $a|b$ y $b|a$ entonces $|a| = |b|$.
4. Si $a|n$ y $a|m$ entonces $a|bn + cm$.
5. Si $a|b$ entonces $am|bm$.
6. Si $ab|ac$ y $a \neq 0$, entonces $b|c$.



7. $1|m$.
8. $m|0$.
9. Si $0|m$ entonces $m = 0$.
10. Si $a|b$ y $b \neq 0$, entonces $|a| \leq |b|$.

Teorema 1.1.3: Algoritmo de la división (Euclides)

Sean $a, b \in \mathbb{Z}$ dos enteros con $b > 0$, entonces existen únicos $q, r \in \mathbb{Z}$ tales que

$$a = b \cdot q + r, \qquad \text{con} \;\; 0 \leq r < b. \tag{1.1}$$

Demostración. Considere los números $a, b \in \mathbb{Z}$ con $b > 0$. Se debe probar tanto la existencia como la unicidad de los números enteros q, r que satisfacen la ecuación (1.1). Para mostrar la **existencia:**, defina el conjunto

$$S := \{a - mb \;:\; m \in \mathbb{Z},\, a - bm \geq 0\}.$$

Note que $S \subseteq \mathbb{Z}$ y que $S \neq \emptyset$ pues S tiene al menos un elemento no negativo. Para ver esto, usando el hecho de que $b > 0$, basta tomar un entero negativo m_0 tal que $a \geq bm_0$, es decir $a - bm_0 \geq 0$, por lo que $a - bm_0 \in S$. Teniendo claro que $S \neq \emptyset$, se analiza los casos en que $0 \in S$ o bien $0 \notin S$.

- Si $0 \in S$ entonces, por la forma que tienen los elementos de S, existe $q \in \mathbb{Z}$ tal que $a - qb = 0$, es decir, $a = qb$, que a su vez se puede escribir $a = qb + 0$, siendo en este caso $r = 0$.

- Si $0 \notin S$, entonces todos los elementos de S son positivos y por el principio del buen orden, S tiene un elemento mínimo positivo. Denote por r ese elemento mínimo. Luego, por la definición de S se tiene que

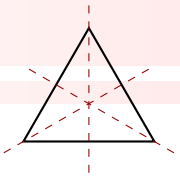
  $$r = a - bq \quad \text{para algún} \;\; q \in \mathbb{Z},$$

  es decir,

  $$a = bq + r, \quad 0 < r. \tag{1.2}$$

  Falta probar que $r < b$. Para ello suponga por contradicción que $r \geq b$. Entonces $r - b \geq 0$, pero, como $r = a - bq$, entonces

  $$a - bq - b \geq 0,$$



lo cual equivale a

$$a - b(q+1) \geq 0,$$

por lo que $a - b(q+1) \in S$. Sin embargo, como b es positivo se tiene

$$a - b(q+1) = a - bq - b < a - bq = r,$$

lo cual contradice que r es el menor elemento de S, de aquí $0 < r < b$ como se deseaba.

Con el fin de probar la **unicidad**, suponga que existen q, r, q' y r' en $\mathbb{Z}$ tales que

$$\begin{aligned} a &= bq + r \quad \text{con} \quad 0 \leq r < b \\ a &= bq' + r' \quad \text{con} \quad 0 \leq r' < b \end{aligned} \tag{1.3}$$

Se debe llegar a concluir que $q = q'$ y $r = r'$. Ahora, de las igualdades en (1.3) se tiene que

$$a - a = qb + r - (q'b + r'),$$

lo cual es equivalente a

$$0 = (q - q')b + r - r',$$

o bien

$$r - r' = (q' - q)b.$$

Esto significa que b divide a $r - r'$, es decir,

$$b|(r - r') \tag{1.4}$$

Por otro lado, de las desigualdades en (1.3) se tiene que

$$0 \leq r < b \quad \text{y} \quad -b < -r' \leq 0,$$

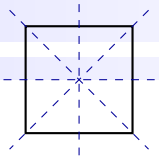
entonces

$$-b < r - r' < b,$$

lo que es lo mismo que

$$|r - r'| < |b| = b, \quad \text{pues} \quad b > 0. \tag{1.5}$$

De las expresiones (1.4) y (1.5) se tiene que $r - r' = 0$, pues si $r \neq r'$ se contradice la parte 10 del teorema



1.1.2. Por lo tanto $r = r'$. Ahora, sustituyendo $r = r'$ en (1.3) se tiene

$$a = bq + r \text{ con } 0 \leq r < b$$

$$a = bq' + r \text{ con } 0 \leq r < b,$$

se resta ambas expresiones se tiene que

$$0 = (q - q')b \text{ con } 0 < b$$

de donde es inmediato que $q = q'$. □

Definición 1.1.3:

Sean a, b dos números enteros. Un número $d \in \mathbb{Z}$ se llama *máximo común divisor* de a y b si se cumplen las siguientes condiciones:

1. $d|a$ y $d|b$.
2. Si c es un número entero tal que $c|a$ y $c|b$ entonces $c|d$.

El máximo común divisor de a y b se denota (a, b) y básicamente es el mayor número que divide tanto a a como a b.

Ejemplo 1.1.3.

El máximo común divisor entre 84 y 120 es 12. Note que 12 divide a 84 y 120 y además no existe otro número mayor de 12 que divida a ambos. Por lo tanto $(84, 120) = 12$.

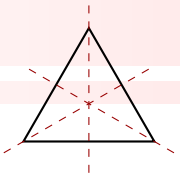
Teorema 1.1.4:

Para cualesquiera $a, b \in \mathbb{Z}$, existen $s, t \in \mathbb{Z}$ tales que $(a, b) = sa + tb$.

Demostración. Considere el conjunto

$$S := \{sa + tb \ : \ s, t \in \mathbb{Z}\}.$$

Tomando $s = a$ y $t = b$, entonces $a^2 + b^2 \in S$, por lo que S contiene enteros positivos y por el principio del buen orden existe un entero positivo más pequeño. Denote por d ese elemento. Como $d \in S$ entonces, por la definición de S, existen $s, t \in \mathbb{Z}$ tales que $d = as + bt$. Se va a probar que $d = (a, b)$, es decir, que d es el máximo común divisor de a y b. Para ello, se prueba primero que $d|a$ y $d|b$. En este sentido, y por



el algoritmo de la división (Teorema 1.1.3) existen $q, r \in \mathbb{Z}$ tales que

$$a = qd + r \quad \text{con} \quad 0 \leq r < d. \tag{1.6}$$

Despejando r de la ecuación anterior y usando el hecho de que $d = as + bt$, se tiene que

$$\begin{aligned} r &= a - qd \\ &= a - q(as + bt) \\ &= a - qas - qbt \\ &= (1 - qs)a + (-qt)b \end{aligned}$$

Esto significa que $r \in S$. Pero, por la desigualdad en (1.6) se cumple que $r < d$ y dado que d es entero positivo más pequeño de S, se tiene necesariamente que $r = 0$. Luego, sustituyendo $r = 0$ en la igualdad en (1.6) se tiene que

$$a = qd$$

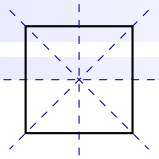
Esto prueba que $d|a$. De modo similar se muestra que $d|b$.
Ahora se debe demostrar que d es el máximo común divisor de a y b, es decir, probar que cualquier entero c que divide a a y b también divide a d. Con este fin, considere $c \in \mathbb{Z}$ tal que $c|b$ y $c|b$, entonces por la parte 4 del Teorema 1.1.2

$$c|(as + bt)$$

y como $d = as + bt$ se sigue que $c|d$. Por lo tanto $d = sa + tb$ es el máximo común divisor de a y b como se afirmaba. □

1.2 Aritmética modular

En el ámbito de las matemáticas, la aritmética modular surge como una herramienta fundamental para el análisis de patrones y relaciones numéricas. De manera objetiva, la aritmética modular proporciona un marco conceptual que se centra en las propiedades cíclicas de los números bajo ciertas operaciones aritméticas. Su utilidad subyace en el estudio de congruencias y su aplicación extendida en la teoría de números, criptografía y diversas ramas de la informática.



Definición 1.2.1:

Sean $a, b \in \mathbb{Z}$. Decimos que a **es congruente con** b **módulo** n si

$$n|(a-b).$$

Si a es congruente con b módulo n, se escribe

$$a \equiv b(mod\ n). \tag{1.7}$$

Observación 1.2.1.

1. La relación "$\equiv$" define una relación de equivalencia en $\mathbb{Z}$. La prueba de esta afirmación queda como ejercicio.

2. De acuerdo con la definición anterior, $a \equiv b(mod\ n)$ si y sólo $n|(a-b)$. Y esto sucede si existe $k \in \mathbb{Z}$ tal que $a - b = kn$. Es decir, $a = b + kn$. Por lo tanto, se puede escribir que

$$a \equiv b(mod\ n) \quad \text{si y sólo si existe} \quad k \in \mathbb{Z} \quad \text{tal que} \quad a = b + kn. \tag{1.8}$$

Ejemplo 1.2.1.

Considere los enteros $a = 15$ y $b = 7$. Como $15 = 2 \cdot 7 + 1$, es decir $15 - 1 = 2 \cdot 7$, entonces $2|(15-1)$ por lo que $15 \equiv 1(mod\ 2)$. También observe que $7|(15-1)$, entonces $15 \equiv 1(mod\ 7)$.

Definición 1.2.2:

Sea $a \in \mathbb{Z}$. Se define la **clase de congruencia módulo** n **de** a por

$$[a] := \left\{ b \in \mathbb{Z} \ : \ b \equiv a(mod\ n) \right\}$$

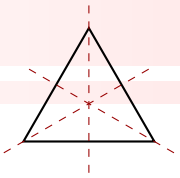
Observación 1.2.2.

Dado $n \in \mathbb{Z}$, el **conjunto de todas las clases módulo** n es el conjunto

$$\mathbb{Z}_n := \left\{ [0], [1], [2], [3], \ldots, [n-1] \right\}.$$

De esta forma se "divide" $\mathbb{Z}$ en subconjuntos (disjuntos) o clases de equivalencia.

Ejemplo 1.2.2.



La clase del 0 módulo 4 es el conjunto

$$\begin{aligned}[0] &= \{b \in \mathbb{Z} \ : \ b \equiv 0(mod\ 4)\} \\ &= \{0+4k \ : k \in \mathbb{Z}\} \quad \text{por} \quad (1{,}8) \\ &= \{4k \ : k \in \mathbb{Z}\} \\ &= \{\ldots, -8, -4, 0, 4, 8, \ldots\}\end{aligned}$$

La clase del 1, módulo 4, es el conjunto

$$\begin{aligned}[1] &= \{b \in \mathbb{Z} \ : \ b \equiv 1\ (mod\ 4)\} \\ &= \{1+4k \ : k \in \mathbb{Z}\} \quad \text{por} \quad (1{,}8) \\ &= \{\ldots, -7, -3, 1, 5, 9, \ldots\}\end{aligned}$$

La clase del 2, módulo 4, es el conjunto

$$\begin{aligned}[2] &= \{b \in \mathbb{Z} \ : \ b \equiv 2\ (mod\ 4)\} \\ &= \{2+4k \ : k \in \mathbb{Z}\} \quad \text{por} \quad (1{,}8) \\ &= \{\ldots, -6, -2, 0, 6, 10, \ldots\}\end{aligned}$$

La clase del 3, módulo 4, es el conjunto

$$\begin{aligned}[3] &= \{b \in \mathbb{Z} \ : \ b \equiv 3\ (mod\ 4)\} \\ &= \{3+4k \ : k \in \mathbb{Z}\} \quad \text{por} \quad (1{,}8) \\ &= \{\ldots, -5, -1, 3, 7, 11, \ldots\}\end{aligned}$$

Si se construye la clase del 4, módulo 4, se observa que es igual a [0]. De forma similar, módulo 4, se tiene que [5] = [1], [6] = [2], [7] = [3], [8] = [0], etcétera. Por lo tanto,

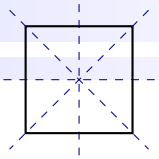
$$\mathbb{Z}_4 = \{[0], [1], [2], [3]\},$$

donde

$$[0] = \{\ldots, -8, -4, 0, 4, 8, \ldots\},$$

$$[1] = \{\ldots, -7, -3, 1, 5, 9, \ldots\},$$

$$[2] = \{\ldots, -6, -2, 0, 6, 10, \ldots\},$$



$$[3] = \{\ldots, -5, -1, 3, 7, 11, \ldots\}.$$

Definición 1.2.3:

Dados $a, b \in \mathbb{Z}$, se definen, la *suma de clases módulo n* y *el producto de clases módulo n*, respectivamente, por

1. $[a] + [b] := [a + b]$
2. $[a][b] := [ab]$

Ejemplo 1.2.3.

Considere el conjunto de clases $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$. Algunas sumas en $\mathbb{Z}_4$, utilizando la definición anterior, corresponde a:

$$\begin{aligned} [0] + [1] &= [0 + 1] = [1] \\ [2] + [1] &= [2 + 1] = [3] \\ [3] + [2] &= [3 + 2] = [5] = [1] \\ [2] + [2] &= [2 + 2] = [4] = [0] \end{aligned}$$

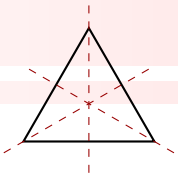
De hecho, la siguiente tabla resume todas las posibles sumas en $\mathbb{Z}_4$.

+	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

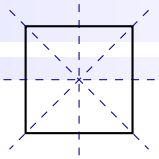
De forma similar, algunos productos en $\mathbb{Z}_4$ son:

$$\begin{aligned} [0][1] &= [0 \cdot 1] = [0] \\ [2][1] &= [2 \cdot 1] = [2] \\ [3][2] &= [3 \cdot 2] = [6] = [2] \\ [2][2] &= [2 \cdot 2] = [4] = [0] \end{aligned}$$

Además, la siguiente tabla resume todos los posibles productos en $\mathbb{Z}_4$.



$\cdot$	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]



1.3 Ejercicios

R/ p.246

● Ejercicio 1.3.1 (Divisibilidad)

Sean $a, b \in \mathbb{Z}$ tales que $a|b$, muestre que

$-a|b$.

$a|(-b)$.

$(-a)|(-b)$.

R/ p.246

● Ejercicio 1.3.2 (Divisibilidad)

Dados enteros a, b, c, d, verifique lo siguiente

Si $a|b$ entonces $a|bc$.

Si $a|b$ y $a|c$ entonces $a^2|bc$

R/ p.246

● Ejercicio 1.3.3 (Divisibilidad)

Muestre que $3|\left(n^3+2n\right)$ para todo $n \in \mathbb{N}$.

R/ p.247

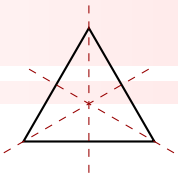
● Ejercicio 1.3.4 (Divisibilidad)

Sean $a, b \in \mathbb{N}$ números impares, con $a > b$. Muestre que $8|(a^2-b^2)$.

R/ p.247

● Ejercicio 1.3.5 (Residuo)

Muestre que, cuando el cuadrado de un número impar se divide por 8, el residuo es 1.



● Ejercicio 1.3.6 (Divisibilidad) R/ p.247

Sean $a, b, d \in \mathbb{Z}$ con $d \neq 0$, $d|a$ y $d|b$. Muestre que $a|b$ si y sólo si $\frac{a}{d} \Big| \frac{b}{d}$

● Ejercicio 1.3.7 (Divisibilidad) R/ p.248

Muestre que si a es impar, entonces $12| \left(a^2 + (a+2)^2 + (a+4)^2 + 1\right)$

● Ejercicio 1.3.8 (Divisibilidad) R/ p.248

Muestre que si $a \in \mathbb{Z}$ entonces $2|a(a+1)$.

● Ejercicio 1.3.9 (Algoritmo de la división) R/ p.248

Muestre que si $a, b \in \mathbb{Z}$ con $b > 0$, entonces, existen únicos enteros q, r tales que

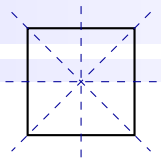
$$a = qb + r, \quad \text{con} \quad 2b \leq r < 3b$$

● Ejercicio 1.3.10 (Divisibilidad) R/ p.249

Sean $a, b \in \mathbb{Z}$ con $b \neq 0$. Muestre que $b|a$ si y sólo si el residuo de dividir a por b es igual a cero.

● Ejercicio 1.3.11 (Divisibilidad) R/ p.250

Muestre que cualquier número entero de la forma $6k + 5$ es también de la forma $3m + 2$. Muestre también que lo contrario no sucede.



R/ p.251 ● **Ejercicio 1.3.12 (Divisibilidad)**

Muestre que el cuadrado de cualquier número entero tiene una de las formas $3k$ o $3k+1$.

R/ p.252 ● **Ejercicio 1.3.13 (Divisibilidad)**

Muestre que no existen enteros a, b tales que $a+b=100$ y $(a,b)=3$.

R/ p.252 ● **Ejercicio 1.3.14 (Divisibilidad)**

Muestre que si $(a,b)=1$, entonces $(2a+b, a+2b)=1$ o $(2a+b, a+2b)=3$

R/ p.253 ● **Ejercicio 1.3.15 (Divisibilidad)**

Muestre que si $(a,b)=1$, entonces $(a+b, ab)=1$

R/ p.254 ● **Ejercicio 1.3.16 (Divisibilidad)**

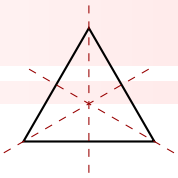
Use el algoritmo de la división para hallar el máximo común divisor de las siguientes parejas de números

2456, -1234

5096, 7098

12321, 8658

156, 1740



● Ejercicio 1.3.17 (Divisibilidad) R/ p.255

Use el algoritmo de la división para hallar $s, t \in \mathbb{Z}$ tales que

$(56, 72) = 56s + 72t$

$(24, 138) = 24s + 138t$

$(119, 272) = 119s + 272t$

● Ejercicio 1.3.18 (Divisibilidad) R/ p.257

Sean $a, b \in \mathbb{Z}$ y p un primo.

Muestre que si $ab \equiv 0 (\text{mod } p)$, entonces $[a] = [0]$ o $[b] = [0]$.

Muestre que si $ab \equiv ac (\text{mod } p)$ con $[a] \neq [0]$, entonces $[b] = [c]$.

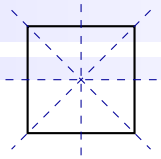
Muestre que si $a^2 \equiv b^2 (\text{mod } p)$, entonces $[a] = [b]$ o $[a] = -[b]$.

● Ejercicio 1.3.19 (Divisibilidad) R/ p.259

Sean $a, b \in \mathbb{Z}$. Muestre que si $c > 0$ y $a \equiv b \ (\text{mod } n)$, entonces $ca \equiv cb \ (\text{mod } cn)$.

● Ejercicio 1.3.20 (Divisibilidad) R/ p.259

Sean $a, b, n \in \mathbb{Z}$ divisibles por $d \in \mathbb{N}$. Muestre que si $a \equiv b \ (\text{mod } n)$, entonces $\frac{a}{d} \equiv \frac{b}{d} \ (\text{mod } \frac{n}{d})$.



R/ p.260

● **Ejercicio 1.3.21 (Divisibilidad)**

De un ejemplo para mostrar que $a^2 \equiv b^2 \pmod{n}$ no implica que $a \equiv b \pmod{n}$.

R/ p.260

● **Ejercicio 1.3.22 (Divisibilidad)**

Si $a \equiv b \pmod{n}$, muestre que $(a, n) = (b, n)$.

Capítulo 2

Teoría de Grupos

¡Trinidad grandiosa! ¡Triángulo luminoso! ¡El que no os ha conocido es un insensato!

Teorema de Jordan-Hölder

En este capítulo, se aborda la Teoría de Grupos, una rama matemática esencial para comprender las propiedades algebraicas de conjuntos bajo operaciones específicas. Su origen en el siglo XIX, propuesto por Évariste Galois[1], estableció las bases para el análisis sistemático de estructuras algebraicas que capturan conceptos fundamentales como la simetría y la transformación. Se explorarán definiciones clave, como la cerradura bajo operaciones binarias, junto con propiedades inherentes, incluyendo la existencia de un elemento neutro y la presencia de inversos, para proporcionar una comprensión profunda de cómo los grupos modelan fenómenos matemáticos y físicos.

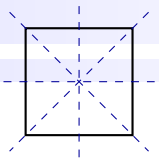
A lo largo de este estudio, se presentarán ejemplos concretos y se desarrollará la teoría necesaria. Este enfoque impersonal permitirá a los lectores familiarizarse con los principios esenciales que subyacen en

[1]La vida de Évariste Galois, un matemático francés del siglo XIX, estuvo marcada por su pasión y genialidad, así como por las adversidades personales y políticas de la época. Nació el 25 de octubre de 1811 en Bourg-la-Reine, Francia.

Galois destacó desde temprana edad en matemáticas, y a los 16 años ya había desarrollado gran parte de la teoría de grupos y la teoría de Galois, que más tarde sería fundamental en el álgebra abstracta. Sus contribuciones revolucionaron la teoría de ecuaciones algebraicas y proporcionaron un enfoque estructurado para comprender las soluciones de estas ecuaciones.

A pesar de su brillantez matemática, Galois enfrentó desafíos en su vida personal y política. Estuvo involucrado en actividades políticas durante la Revolución de 1830 en Francia, y su participación le llevó a ser arrestado y encarcelado brevemente. También enfrentó tensiones personales y rivalidades académicas.

Trágicamente, Évariste Galois murió en un duelo a la edad de 20 años, el 31 de mayo de 1832. Su legado, sin embargo, ha perdurado a lo largo de los años. La teoría de Galois se convirtió en una herramienta esencial en la resolución de ecuaciones algebraicas y sentó las bases para el desarrollo posterior del álgebra abstracta. Su impacto en las matemáticas es reconocido como fundamental, y la teoría de Galois sigue siendo una parte integral del currículo matemático hasta el día de hoy. Consultar en Goldenberg (2024)



la estructura algebraica de los grupos, preparándolos para abordar problemas matemáticos y científicos más avanzados.

2.1 Definición y ejemplos de grupos.

Dentro del vasto campo de las Matemáticas, los grupos emergen como estructuras algebraicas fundamentales que capturan esencialmente la noción de simetría y transformación. En dicho sentido, los grupos proporcionan un marco conceptual que permite analizar y comprender las propiedades fundamentales de conjuntos bajo operaciones específicas.

Definición 2.1.1: Grupo.

Un **grupo** es un par $(G, *)$, donde G es un conjunto y $*$ es una operación en G que cumple los siguientes axiomas:

1. La operación "$*$" es *cerrada* en G. Es decir, para cualesquiera dos elementos $g_1, g_2 \in G$, se tiene que $g_1 * g_2 \in G$.

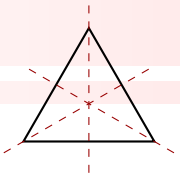
2. La operación "$*$"es *asociativa*. Es decir, para cualesquiera tres elementos $g_1, g_2, g_3 \in G$, se tiene que
$$(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3).$$

3. Existe un elemento $e \in G$ tal que para todo $g \in G$
$$g * e = g = e * g.$$
El elemento e se llama el **elemento identidad o elemento neutro** de la operación $*$. Más adelante se probará que este elemento es único.

4. Para cada elemento $g \in G$, existe un elemento $g' \in G$ tal que
$$g * g' = e = g' * g.$$
El elemento g' se llama el **inverso** de g. El inverso de un elemento se denota por g^{-1} o bien por $-g$.

Observación 2.1.1.

De manera similar a la definición 2.1.1 anterior, se consideran los siguientes puntos:



1. Si $(G, *)$ sólo cumple la cerradura y la asociatividad, entonces $(G,)$ se llama semigrupo.
2. Si $(G, *)$ sólo cumple la cerradura, la asociatividad y la existencia del elemento neutro, entonces $(G, *)$ se llama monoide.
3. Para probar que un conjunto G, junto con una operación $*$, es un grupo, hay que verificar que la operación $*$ satisface las cuatro condiciones de la definición (2.1.1).
4. Cuando se prueba la existencia del elemento neutro se debe mostrar que $x * e = x$ (existencia del elemento neutro por la derecha) y que $e * x = x$ (existencia del elemento neutro por la izquierda).
5. Cuando se prueba la existencia de los elementos inversos, de igual forma se debe probar tanto por la derecha como por la izquierda.

Ejemplo 2.1.1.

El par $(\mathbb{Z}, +)$, donde $+$ es la suma usual de números enteros, es un grupo.

Demostración. Se verifica que $+$ satisface las condiciones de la definición 2.1.1, según se detalla a continuación:

1. *Cerradura:* note que si $x, y \in \mathbb{Z}$ entonces, $x + y$ también está en $\mathbb{Z}$.
2. *Asociatividad:* sean $x, y, z \in \mathbb{Z}$. Dado que la suma es asociativa en $\mathbb{R}$, entonces también lo es en $\mathbb{Z}$, es decir se cumple $(x + y) + z = x + (y + z)$.
3. *Existencia de un elemento neutro:* el elemento identidad de la suma usual es $0 \in \mathbb{Z}$.
4. *Existencia de inversos:* Para cada $x \in \mathbb{Z}$, el inverso es $-x \in \mathbb{Z}$.

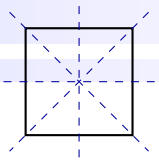
Así que todos los axiomas de grupo se cumplen. Por lo tanto $(\mathbb{Z}, +)$ es un grupo. □

Ejemplo 2.1.2.

De manera similar el caso anterior, los pares $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R} - \{0\}, \cdot)$, $(\mathbb{Q} - \{0\}, \cdot)$, donde $+$ y $\cdot$ denotan la suma y el producto de números reales, son grupos.

Ejemplo 2.1.3.

El par $(\mathbb{Z} - \{0\}, \cdot)$, donde $\cdot$ es la multiplicación usual, no es grupo porque dado un elemento $a \neq 1$, su inverso es $a' = \frac{1}{a}$, el cual no es un elemento de $\mathbb{Z} - \{0\}$. Sin embargo, si cumple con la cerradura, la asociatividad y el elemento neutro que es $e = 1$, por lo tanto es un monoide.



Ejemplo 2.1.4.

Sea $G := \mathbb{R} - \{x, y \in \mathbb{R} : xy = 1\}$. En G considere la operación

$$x * y = \frac{x + y}{1 - xy}.$$

El par $(G, *)$ es un grupo.

Demostración. Se debe verificar que la operación $*$ satisface las condiciones de la definición 2.1.1, esto es:

1. *Cerradura:* para mostrar la propiedad de cerradura observe que $xy \neq 1$, entonces $1 - xy \neq 0$, con lo cual $x * y$ está bien definida y su resultado es un elemento de $\mathbb{R}$, es decir,

$$x * y = \frac{x + y}{1 - xy} \in \mathbb{R}.$$

2. *Asociatividad:* para probar la propiedad asociativa considere x, y y z números reales, entonces:

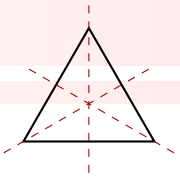
$$\begin{aligned}
(x * y) * z &= \frac{x + y}{1 - xy} * z \\
&= \frac{\frac{x+y}{1-xy} + z}{1 - \left(\frac{x+y}{1-xy}\right) z} \\
&= \frac{\frac{x+y+z-xyz}{1-xy}}{\frac{1-xy-xz-yz}{1-xy}} \\
&= \frac{x + y + z - xyz}{1 - xy - xz - yz}.
\end{aligned}$$

   De forma similar se comprueba la igualdad

$$x * (y * z) = \frac{x + y + z - xyz}{1 - xy - xz - yz}.$$

   Con estos resultados se concluye que $(x * y) * z = x * (y * z)$.

3. *Existencia de un elemento neutro:* se debe encontrar un elemento $e \in G$ tal que $x * e = x = e * x$.



Para ello, note que si $x * e = x$ implica que

$$\begin{aligned} & \frac{x+e}{1-xe} = x \\ \Rightarrow \quad & x+e = x - x^2e \\ \Rightarrow \quad & e + x^2e = 0 \\ \Rightarrow \quad & e(1+x^2) = 0, \quad \text{donde} \quad 1+x^2 \neq 0, \\ \Rightarrow \quad & e = 0. \end{aligned}$$

De forma análoga se prueba que existe el elemento neutro por la izquierda; para ello suponga que $e * x = x$ y se concluye que $e = 0$. Finalmente, con los resultados obtenidos se verifica la existencia del elemento neutro.

4. *Existencia de inversos:* para probar la existencia de elementos inversos considere un elemento x en G; se debe encontrar un x' en G tal que $x * x' = 0 = x' * x$, puesto que $e = 0$ es el elemento neutro por el punto anterior. Note que $x * x' = 0$ equivale a $\frac{x+x'}{1-xx'} = 0$, de acá se despeja x' de forma sencilla y se concluye que $x' = -x$. De forma análoga se llega a que si $x' * x = 0$, entonces $x' = -x$. Por lo tanto, si x está en G, su elemento inverso bajo la operación $*$ es $-x$.

De esta forma se concluye que $(G, *)$ es un grupo. □

Ejemplo 2.1.5.

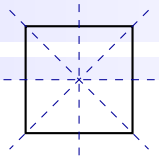
En $\mathbb{R} - \{0\}$ defina la operación $x * y = 4xy$. Entonces $(\mathbb{R} - \{0\}, *)$ es un grupo.

Demostración. Se debe verificar que la operación $*$ satisface las condiciones de la definición 2.1.1, esto es:

1. *Cerradura:* visualice que si x, y están en $\mathbb{R} - \{0\}$, entonces $4xy$ también es un elemento de $\mathbb{R} - \{0\}$. Así se verifica que $x * y = 4xy$ es una operación cerrada.

2. *Asociatividad:* sean x, y y z elementos de $\mathbb{R} - \{0\}$, entonces

$$\begin{aligned} (x * y) * z &= (4xy) * z \\ &= 4(4xy)z \\ &= 16xyz \\ &= 4x(4yz) \\ &= x * (4yz) \\ &= x * (y * z). \end{aligned}$$



Por lo tanto, la operación $*$ es asociativa.

3. *Existe un elemento neutro:* primero se busca en elemento neutro por la derecha. Para ello sea x un elemento de $\mathbb{R}-\{0\}$ tal que $x * e = x$, esto implica que $4xe = x$ y puesto que $x \neq 0$, se obtiene que $e = \frac{1}{4}$. De forma análoga se resuelve que si $e * x = x$, entonces $e = \frac{1}{4}$, por lo tanto este sería en elemento neutro.

4. *Existencia de inversos:* sea x un elemento de $\mathbb{R}-\{0\}$, se debe encontrar un elemento x' en $\mathbb{R}-\{0\}$ tal que $x * x' = \frac{1}{4}$, lo cual implica que $4xx' = \frac{1}{4}$, de donde se obtiene que $x' = \frac{1}{16x}$, donde $x \neq 0$. Además, se llega a la misma conclusión si $x' * x = \frac{1}{4}$. Entonces, el elemento inverso de $x \neq 0$ corresponde a $x' = \frac{1}{16x}$.

De acuerdo con lo anterior, se concluye que $(\mathbb{R}-\{0\}, *)$ es un grupo. □

Ejemplo 2.1.6.

Considere el conjunto de los números complejos

$$\mathbb{C} := \{a + bi \ : \ a, b \in \mathbb{R},\ i^2 = -1\}.$$

Se define en $\mathbb{C}$ la operación suma por

$$(a + bi) + (c + di) = (a + c) + (b + d)i.$$

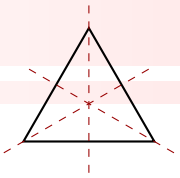
Con esta operación, $\mathbb{C}$ es un grupo.

Demostración. A continuación se verifica que la suma en $\mathbb{C}$ satisface las condiciones de la definición 2.1.1:

1. *Cerradura:* sean $z_1, z_2 \in \mathbb{C}$, $z_1 = a+bi$, $z_2 = c+di$ con $a, b, c, d \in \mathbb{R}$. Como $a+c \in \mathbb{R}$ y $b+d \in \mathbb{R}$, entonces

$$z_1 + z_2 = (a + bi) + (c + di) = (a + c) + (b + d)i \in \mathbb{C}.$$

Esto prueba que $z_1 + z_2$ también está en $\mathbb{C}$.



2. *Asociatividad:* sean $z_1, z_2, z_3 \in \mathbb{C}$, $z_1 = a + bi$, $z_2 = c + di$ y $z_3 = e + if$ con $a, b, c, d, e, f \in \mathbb{R}$. Usando el hecho de que la suma es asociativa en $\mathbb{R}$ se tiene:

$$\begin{aligned}(z_1 + z_2) + z_3 &= (a + bi + c + di) + e + fi \\ &= (a + c) + (b + d)i + e + fi \\ &= (a + c) + e + ((b + d) + f)i \\ &= a + (c + e) + (b + (d + f))i \\ &= a + bi + ((c + e) + (d + f)i) \\ &= a + bi + (c + di + e + fi) \\ &= z_1 + (z_2 + z_3).\end{aligned}$$

3. *Existencia de un elemento neutro:* el elemento identidad de la suma usual es $0 := 0 + 0i \in \mathbb{C}$. En efecto, para cada $z = a + bi \in \mathbb{C}$ se tiene

$$z + 0 = a + bi + 0 + 0i = (a + 0) + (b + 0)i = a + bi = z.$$

   Similarmente se prueba que $0 + z = z$.

4. *Existencia de inversos:* para cada $z = a + bi \in \mathbb{C}$, el inverso es $-z := -a + -bi \in \mathbb{C}$. En efecto

$$z + -z = a + bi + -a + -bi = (a + -a) + (b + -b)i = 0 + 0i = 0.$$

   Lo mismo ocurre si $-z + z = 0$.

Por lo tanto $(\mathbb{C}, +)$ es un grupo. □

Ejemplo 2.1.7.

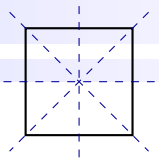
El conjunto de números pares definido por

$$2\mathbb{Z} := \{\cdots, -4, -2, 0, 2, 4, \cdots\} = \{2n : n \in \mathbb{Z}\},$$

con la suma usual + de números enteros, es un grupo.

Demostración. A continuación se prueba los axiomas respectivos:

1. *Cerradura:* sean $x, y \in 2\mathbb{Z}$, $x = 2a$ y $y = 2b$ para algunos $a, b \in \mathbb{Z}$. Entonces $x + y = 2a + 2b = 2(a + b)$, el cual es un número par y por tanto está en $2\mathbb{Z}$.



2. *Asociatividad:* sean x, y y z elementos de $2\mathbb{Z}$, $x = 2a$, $y = 2b$ y $z = 2c$ para $a, b, c \in \mathbb{Z}$, entonces

$$\begin{aligned}(x + y) + z &= (2a + 2b) + z \\ &= (2a + 2b) + 2c \\ &= 2a + (2b + 2c) \\ &= 2a + (y + z) \\ &= x + (y + z).\end{aligned}$$

3. *Existencia de un elemento neutro:* es claro que el elemento neutro es el cero.

4. *Existencia de inversos:* si x es un elemento de $2\mathbb{Z}$, $x = 2a$ con $a \in \mathbb{Z}$, no es difícil comprobar que $x' = -2a$ es su inverso.

Se concluye que $(2\mathbb{Z}, +)$ es un grupo. □

Ejemplo 2.1.8.

Considere la operación $*$ definida sobre $(\mathbb{R} - \{0\}) \times \mathbb{R}$ por:

$$(a, b) * (c, d) = (2ac, b + d + 4).$$

Entonces $(\mathbb{R} - \{0\}) \times \mathbb{R}, *)$ es un grupo.

Demostración. De forma similar a los ejemplos anteriores, se muestra los siguientes axiomas:

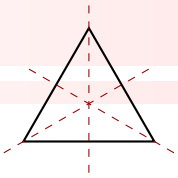
1. *Cerradura:* sean (a, b) y (c, d) elementos de $\mathbb{R} - \{0\} \times \mathbb{R}$. Note que $a, c \in \mathbb{R} - \{0\}$, por lo tanto $2ac \in \mathbb{R} - \{0\}$. Además, es claro que $b + d + 4 \in \mathbb{R}$, por lo tanto $(a, b) * (c, d) = (2ac, b + d + 4)$ es un elemento de $(\mathbb{R} - \{0\}) \times \mathbb{R}$.

2. *Asociatividad:* la operación es asociativa pues dados (a, b), (c, d) y (e, f) elementos de $(\mathbb{R}-\{0\})\times\mathbb{R}$, entonces

$$\begin{aligned}[(a, b) * (c, d)] * (e, f) &= (2ac, b + d + 4) * (e, f) \\ &= (2(2ac)e, (b + d + 4) + f + 4) \\ &= (4ac, b + d + f + 8).\end{aligned}$$

   De manera similar se prueba que

$$(a, b) * [(c, d) * (e, f)] = (4ac, b + d + f + 8),$$



lo cual permite verificar que $[(a,b)*(c,d)]*(e,f)=(a,b)*[(c,d)*(e,f)]$.

3. *Existencia de un elemento neutro:* sea (a,b) un elemento de $(\mathbb{R}-\{0\})\times\mathbb{R}$. Se debe encontrar un elemento (e_1,e_2) de $(\mathbb{R}-\{0\})\times\mathbb{R}$ tal que

$$(a,b)*(e_1,e_2)=(a,b)=(e_1,e_2)*(a,b).$$

Primero se encuentra el elemento neutro por la derecha, esto es:

$$\begin{array}{rrcl} & (a,b)*(e_1,e_2) & = & (a,b) \\ \Rightarrow & (2ae_1,b+e_2+4) & = & (a,b) \\ \Rightarrow & 2ae_1=a & \text{y} & b+e_2+4=b \\ \Rightarrow & e_1=\frac{1}{2} & \text{y} & e_2=-4. \end{array}$$

Así, el elemento neutro por la derecha es $\left(\frac{1}{2},-4\right)$. De forma análoga se comprueba que también es el elemento neutro por la izquierda.

4. *Existencia de inversos:* sea (a,b) un elemento de $(\mathbb{R}-\{0\})\times\mathbb{R}$, entoncesse busca un elemento (a',b') de $(\mathbb{R}-\{0\})\times\mathbb{R}$ tal que

$$(a,b)*(a',b')=\left(\frac{1}{2},-4\right)=(a',b')*(a,b).$$

Para el inverso por la derecha note que

$$\begin{array}{rrcl} & (a,b)*(a',b') & = & \left(\frac{1}{2},-4\right) \\ \Rightarrow & (2aa',b+b'+4) & = & \left(\frac{1}{2},-4\right) \\ \Rightarrow & 2aa'=\frac{1}{2} & \text{y} & b+b'+4=-4 \\ \Rightarrow & a'=\frac{1}{4a},a\neq 0 & \text{y} & b'=b-8. \end{array}$$

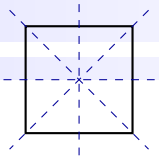
Con ello, el elemento inverso de (a,b) es $\left(\frac{1}{4a},b-8\right)$ que también es un elemento de $(\mathbb{R}-\{0\})\times\mathbb{R}$. De forma análoga se muestra que es el mismo elemento inverso por la izquierda.

Con los anterior probado, se tiene certeza que $((\mathbb{R}-\{0\})\times\mathbb{R},*)$ es un grupo. □

Ejemplo 2.1.9.

Sea $\mathbb{S}^1:=\{(x,y)\in\mathbb{R}^2\mid x^2+y^2=1\}$. Considere la operación $*$ definida sobre $\mathbb{S}^1$ como sigue

$$(x_1,y_1)*(x_2,y_2):=(x_1x_2-y_1y_2,x_1y_2+y_1x_2)$$



Entonces $(\mathbb{S}^1, *)$ es un grupo.

Demostración. Note que $\mathbb{S}^1$ es el conjunto de puntos que se encuentran en el círculo de radio uno. Con esto claro, en los siguientes pasos se prueban los axiomas respectivos:

1. *Cerradura:* Sean (x_1, y_1) y , (x_2, y_2) dos elementos en $\mathbb{S}^1$, entonces se cumple que

$$x_1^1 + y_1^2 = 1 \quad \text{y} \quad x_2^2 + y_2^2 = 1. \tag{2.1}$$

Para comprobar que $(x_1, y_1) * (x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + y_1x_2)$ es cerrada, se debe mostrar que $(x_1x_2 - y_1y_2, x_1y_2 + y_1x_2)$ es un elemento de $\mathbb{S}^1$, es decir, se debe verificar la igualdad

$$(x_1x_2 - y_1y_2)^2 + (x_1y_2 + y_1x_2)^2 = 1.$$

En efecto,

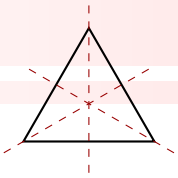
$$\begin{aligned}
(x_1x_2 - y_1y_2)^2 + (x_1y_2 + y_1x_2)^2 &= x_1^2x_2^2 - 2x_1x_2y_1y_2 + y_1^2y_2^2 + x_1^2y_2^2 + 2x_1y_2y_1x_2 + y_1^2x_2^2 \\
&= x_1^2x_2^2 + y_1^2y_2^2 + x_1^2y_2^2 + y_1^2x_2^2 \\
&= (x_1^2x_2^2 + y_1^2x_2^2) + (y_1^2y_2^2 + x_1^2y_2^2) \\
&= x_2^2(x_1^2 + y_1^2) + y_2^2(y_1^2 + x_1^2) \\
&= x_2^2 + y_2^2 \quad \text{por la primera igualdad dada en 2.1,} \\
&= 1 \quad \text{por la segunda igualdad dada en 2.1.}
\end{aligned}$$

2. *Asociatividad:* sean (x_1, y_1), (x_2, y_2) y (x_3, y_3) elementos de $\mathbb{S}^1$, se debe verificar que

$$[(x_1, y_1) * (x_2, y_2)] * (x_3, y_3) = (x_1, y_1) * [(x_2, y_2) * (x_3, y_3)].$$

Con este fin se desarrolla primero la expresión de la izquierda:

$$\begin{aligned}
[(x_1, y_1) * (x_2, y_2)] * (x_3, y_3) &= (x_1x_2 - y_1y_2, x_1y_2 + y_1x_2) * (x_3, y_3) \\
&= \big((x_1x_2 - y_1y_2)x_3 - (x_1y_2 + y_1x_2)y_3, \\
&\quad (x_1x_2 - y_1y_2)y_3 + (x_1y_2 + y_1x_2)x_3\big) \\
&= \big(x_1x_2x_3 - y_1y_2x_3 - x_1y_2y_3 - y_1x_2y_3, \\
&\quad x_1x_2y_3 - y_1y_2y_3 + x_1y_2x_3 + y_1x_2x_3\big).
\end{aligned}$$



De forma similar:

$$\begin{aligned}(x_1, y_1) * [(x_2, y_2) * (x_3, y_3)] &= (x_1, y_1) * (x_2x_3 - y_2y_3, x_2y_3 + y_2x_3) \\ &= \big(x_1(x_2x_3 - y_2y_3) - y_1(x_2y_3 + y_2x_3), \\ &\quad x_1(x_2y_3 + y_2x_3) + y_1(x_2x_3 - y_2y_3)\big) \\ &= \big(x_1x_2x_3 - x_1y_2y_3 - y_1x_2y_3 - y_1y_2x_3, \\ &\quad x_1x_2y_3 + x_1y_2x_3 + y_1x_2x_3 - y_1y_2y_3)\big).\end{aligned}$$

Puesto que ambas expresiones tienen el mismo resultado, se verifica la propiedad asociativa.

3. *Existe un elemento neutro:* sea (x_1, y_1) un elemento de $\mathbb{S}^1$, se debe encontrar un elemento (e_1, e_2) en $\mathbb{S}^1$ tal que

$$(x_1, y_1) * (e_1, e_2) = (x_1, y_1) \quad \text{(Elemento neutro por la derecha).}$$

Esta igualdad se cumple si y sólo si

$$(x_1e_1 - y_1e_2, x_1e_2 + y_1e_1) = (x_1, y_1),$$

de donde se forma el siguiente sistema de ecuaciones:

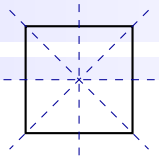
$$\begin{cases} x_1e_1 - y_1e_2 &= x_1 \\ x_1e_2 + y_1e_1 &= y_1 \end{cases}$$

De la primera ecuación se obtiene que

$$e_2 = \frac{x_1e_1 - x_1}{y_1}$$

y de la segunda ecuación

$$e_2 = \frac{y_1 - y_1e_1}{x_1}.$$



Ambos resultados se igualan y se despeja e_1, esto es:

$$\begin{aligned} \frac{x_1e_1 - x_1}{y_1} &= \frac{y_1 - y_1e_1}{x_1} \\ \Rightarrow \quad x_1^2e_1 - x_1^2 &= y_1^2 - y_1^2e_1 \\ \Rightarrow \quad x_1^2e_1 + y_1^2e_1 &= x_1^2 + y_1^2 \\ \Rightarrow \quad (x_1^2 + y_1^2)e_1 &= x_1^2 + y_1^2 \\ \Rightarrow \quad e_1 &= 1. \end{aligned}$$

También se pudo haber usado el hecho que (x_1, y_1) es un elemento en $\mathbb{S}^1$, por lo tanto $x_1^2 + y_1^2 = 1$, entonces en el paso tres de la ecuación anterior se concluye de inmediato que $e_1 = 1$. Ahora, recuerde que $e_2 = \dfrac{x_1e_1 - x_1}{y_1}$, o bien $e_2 = \dfrac{y_1 - y_1e_1}{x_1}$, en cualquiera de los dos casos se cambia el valor obtenido de $e_1 = 1$ y se obtiene que $e_2 = 0$. Con esta información, el elemento neutro por la derecha corresponde a $(1, 0)$. No es difícil verificar que también es el elemento neutro por la izquierda. Además, es claro que $(1, 0)$ es un elemento de $\mathbb{S}^1$.

4. *Existencia de inversos:* sea (x_1, y_1) un elemento de $\mathbb{S}^1$, se debe encontrar un elemento (x_1', y_1') en $\mathbb{S}^1$ tal que

$$(x_1, y_1) * (x_1', y_1') = (1, 0) \quad \text{(Elemento inverso por la derecha).}$$

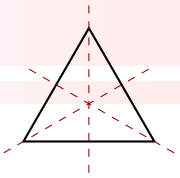
De acá se infiere que $(x_1x_1' - y_1y_1', x_1y_1' + y_1x_1') = (1, 0)$, de donde se forma el siguiente sistema de ecuaciones:

$$\begin{cases} x_1x_1' - y_1y_1' &= 1 \\ x_1y_1' + y_1x_1' &= 0 \end{cases}$$

De la primera ecuación se obtiene que $y_1' = \dfrac{x_1x_1' - 1}{y_1}$ y de la segunda ecuación $y_1' = \dfrac{-y_1x_1'}{x_1}$. Estos resultados se igualan y se despeja x_1', esto es:

$$\begin{aligned} \frac{x_1x_1' - 1}{y_1} &= \frac{-y_1x_1'}{x_1} \\ \Rightarrow \quad x_1^2x_1' - x_1 &= -y_1^2x_1' \\ \Rightarrow \quad x_1^2x_1' + y_1^2x_1' &= x_1 \\ \Rightarrow \quad (x_1^2 + y_1^2)x_1' &= x_1 \\ \Rightarrow \quad x_1' &= x_1 \quad \text{puesto que} \quad x_1^2 + y_1^2 = 1. \end{aligned}$$

Recuerde que $y_1' = \dfrac{x_1x_1' - 1}{y_1}$, o bien $y_1' = \dfrac{-y_1x_1'}{x_1}$, en cualquiera de los dos casos se cambia $x_1' = x_1$ y se obtiene que $y_1' = -y_1$. Entonces, el elemento inverso de (x_1, y_1) por la derecha corresponde a



$(x_1, -y_1)$. No es difícil verificar que también es el elemento inverso por la izquierda. Asimismo, es claro que $(x_1, -y_1)$ es un elemento de $\mathbb{S}^1$.

Finalmente, con los axiomas verificados se establece que $(\mathbb{S}^1, *)$ es un grupo. □

Ejemplo 2.1.10.

Considere un conjunto $G := \{e, a\}$ con la operación " $*$"definida por la siguiente tabla:

$*$	e	a
e	e	a
a	a	e

El par $(G, *)$ es un grupo.

Demostración. A partir de la tabla dada es claro que la operación " $*$" es cerrada y asociativa. El neutro para la operación " $*$" es e ya que $e * a = a * e = a$. En cuanto a los elementos inversos de e es e y el de a es a mismo. Por lo tanto, se cumplen todas las propiedades de la definición (2.1.1) y se concluye que $(G, *)$ es un grupo. □

Ejemplo 2.1.11.

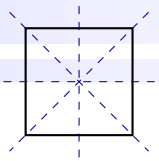
El conjunto $G := \{1, -1, -i, i\}$, donde $i^2 = -1$, con la multiplicación de los números complejos, es un grupo. La tabla de este grupo se muestra a continuación:

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Demostración. A partir de la tabla anterior es claro que la operación es cerrada. La asociatividad se hereda de la multiplicación de los números complejos. El elemento neutro es 1. El elemento inverso de -1 es él mismo, el inverso de i es $-i$ y el de $-i$ es i. Por lo tanto $(G, \cdot)$ es un grupo. □

Observación 2.1.2.

Para probar que un par $(G, *)$ no es grupo, es suficiente verificar que una de las condiciones de la definición 2.1.1 no se satisface.



Ejemplo 2.1.12.

El par $(2\mathbb{Z}, \cdot)$, donde $\cdot$ es la multiplicación usual de números reales, no es un grupo.

Demostración. Es suficiente probar que no hay un elemento neutro. Considere un elemento $x \in 2\mathbb{Z} - \{0\}$. Este elemento es de la forma $x = 2n$, para algún $n \in \mathbb{Z}$. Si existiera un elemento neutro e, se tendría

$$e \cdot (2n) = 2n,$$

es decir, $e = 1$, sin embargo, $1 \notin 2\mathbb{Z}$, entonces la ecuación anterior no tiene solución en $2\mathbb{Z}$. Por lo tanto $(2\mathbb{Z}, \cdot)$ no es grupo. □

Ejemplo 2.1.13.

El conjunto $2\mathbb{Z} + 1 := \{2n + 1 \mid n \in \mathbb{Z}\}$ con la suma usual de suma de los números enteros, no es un grupo.

Demostración. En particular tome los números 3 y 5, ambos son impares y por lo tanto pertenecen al conjunto $2\mathbb{Z}+1$. Observe que $3+5 = 8$, pero $8 \notin 2\mathbb{Z}+1$, es decir, la suma no es cerrada en este conjunto. Así, $(2\mathbb{Z} + 1, +)$ no es un grupo. □

Ejemplo 2.1.14.

El par $(\mathbb{R}, *)$ donde $a * b := a + (b - 3)(b - 2)$, no es un grupo.

Demostración. En este caso, y en particular, para cada $a \in \mathbb{R}$ se cumple que $a * 2 = a$, es decir, el número 2 es el elemento neutro por la derecha con respecto a $*$. Sin embargo, note que

$$2 * a = 2 + (a - 3)(a - 2) = a^2 - 5a + 8 \neq a,$$

excepto para $a = 2$ o $a = 4$. Sin embargo, el elemento neutro debe ser el mismo para para cada a y no para ciertos valores.

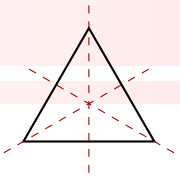
□

Ejemplo 2.1.15.

Sean $(G_1, \cdot)$ y $(G_2, *)$ dos grupos cualesquiera. Se define en $G_1 \times G_2$ la operación

$$(g_1, g_2) \otimes (h_1, h_2) := (g_1 \cdot h_1, g_2 * h_2)$$

para cualesquiera $g_1, h_1 \in G_1$, $g_2, h_2 \in G_2$.Con esta operación $G_1 \times G_2$ es un grupo. De hecho, el par $(G_1 \times G_2, \otimes)$ se llama **producto directo** de G_1 y G_2.



Demostración. De forma similar a los ejemplos anteriores, se muestra que se cumplen los axiomas de la definición de grupo según se aprecia a continuación:

1. *Cerradura:* sean (a, b) y (c, d). Usando el hecho de que las operaciones $\cdot$ y $*$ son cerradas, se tiene que
$$(a, b) \otimes (c, d) = (a \cdot c, b * d) \in G_1 \times G_2.$$
Esto prueba que la operación $\otimes$ es cerrada.

2. *Asociatividad:* sean (a, b), (c, d) (e, f) elementos de $G_1 \times G_2$. Dado que las operaciones $\cdot$ y $*$ son asociativas, se tiene
$$\begin{aligned}\Big((a, b) \otimes (c, d)\Big) \otimes (e, f) &= \Big((a \cdot c, b * d)\Big) \otimes (e, f) \\ &= ((a \cdot c) \cdot e, (b * d) * f) \\ &= (a \cdot (c \cdot e), b * (d * f)) \\ &= (a, b) \otimes \Big((c \cdot e), (d * f)\Big) \\ &= (a, b) \otimes \Big((c, d) \otimes (e, f)\Big)\end{aligned}$$
Esto prueba que la operación $\otimes$ es asociativa.

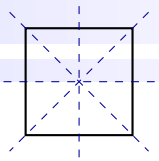
3. *Existencia del elemento neutro:* el elemento neutro en $G_1 \times G_2$ es $(e_1, e_2) \in G_1 \times G_2$, donde e_1 es el elemento neutro en G_1 y e_2 es el elemento neutro en G_2.

4. *Existencia de inversos:* sea $(a, b) \in G_1 \times G_2$. Como $a \in G_1$ y $b \in G_2$, existen sus elementos inversos $a^{-1} \in G_1$ y $b^{-1} \in G_2$. Entonces, el inverso de (a, b) es el elemento $(a^{-1}, b^{-1}) \in G_1 \times G_2$.

Esto concluye la prueba de que $(G_1 \times G_2, \otimes)$ es grupo. □

Observación 2.1.3.

De manera análoga, en el caso de grupos aditivos $(G_1, +_1)$ y $(G_2, +_2)$, se define la **suma directa** sobre $G_1 \times G_2$ por
$$(g_1, g_2) \oplus (h_1, h_2) := (g_1 +_1 h_1, g_2 +_2 h_2).$$



2.1.1. EL grupo de Klein

En teoría de grupos, el o grupo de cuatro de Klein, es un grupo formado por cuatro elementos, donde cada uno de ellos es inverso de sí mismo. Se le llama así en honor al matemático alemán Felix Klein[2], y se denota generalmente con la letra V, por el vocablo alemán Vierergruppe, que significa *grupo de cuatro*.

Ejemplo 2.1.16.

Un forma de entender la naturaleza de este grupo es mediante su interpretación como el grupo de movimientos rígidos o simetrías de un rectángulo. Considere un rectángulo con vértices A, B, C y D como se muestra en la figura

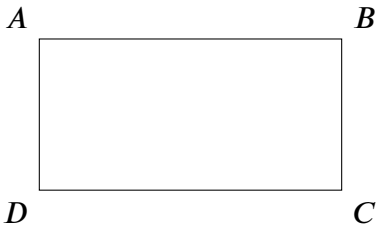


Figura 2.1: Rectángulo R
Fuente: Elaboración propia

A partir de este, se pueden definir las siguientes transformaciones que preservan la forma y el tamaño de dicho rectángulo:

- **Identidad** (e): no se hace ningún cambio, el rectángulo permanece en su posición original. También se puede considerar como una rotación de 360 grados.

[2]Felix Christian Klein (Düsseldorf, 25 de abril de 1849 - Gotinga, 22 de junio de 1925) fue un destacado matemático alemán cuyas contribuciones revolucionaron la comprensión de las geometrías métricas, tanto euclidianas como no euclidianas. En 1871, presentó un influyente marco teórico conocido como el "programa de Erlangen", donde llevó a cabo una notable clasificación de las geometrías. Este programa marcó el fin de la división entre la geometría pura y la geometría analítica al establecer que ambas son casos particulares de la geometría proyectiva. En su clasificación, introdujo el concepto de grupo, otorgándole un papel central al convertir el objeto de estudio de cada geometría en el análisis del grupo de transformaciones que la caracteriza. La influencia duradera de Klein se evidencia en su impacto significativo en la teoría de grupos y en la unificación de distintas ramas de la geometría. Consultar Klein (1892–1893)

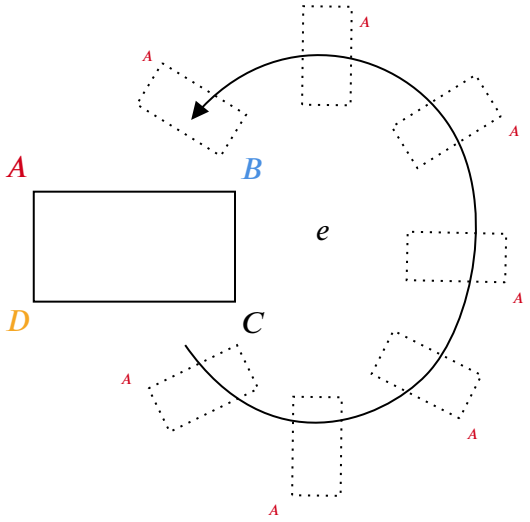


Figura 2.2: Transformación e
Fuente: Elaboración propia

- **Reflexión horizontal** (h): se refleja el rectángulo en relación con la recta horizontal que pasa por el centro del rectángulo.

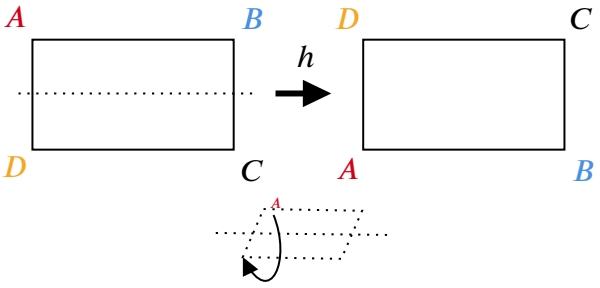


Figura 2.3: Transformación h
Fuente: Elaboración propia

- **Reflexión vertical** (v): se refleja el rectángulo en relación con la recta vertical que pasa por el centro del rectángulo.

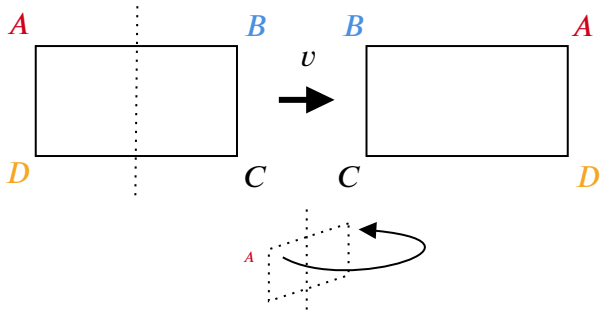


Figura 2.4: Transformación v
Fuente: Elaboración propia

- **Rotación de** 180° (r): se rota el rectángulo 180 grados en torno al punto medio de su base.

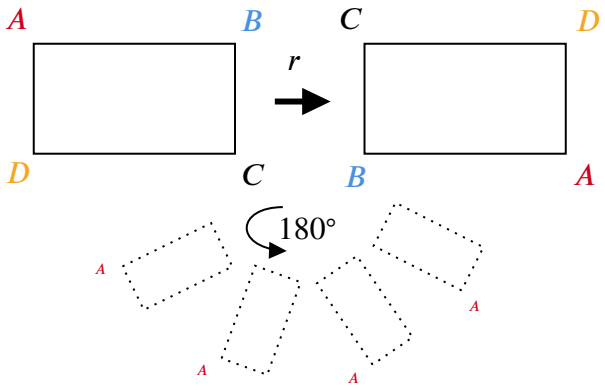
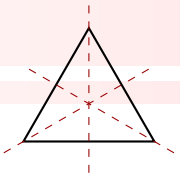


Figura 2.5: Transformación r
Fuente: Elaboración propia

Ahora, por ejemplo, si se aplica v y luego h, se obtiene una rotación de 180 grados, es decir, se obtiene r. Esto se puede escribir como $v \circ h = r$. Otro ejemplo podría ser si se aplica h y luego de nuevo h, se mantiene el rectángulo original, es decir, se obtiene e, lo cual se puede denotar como $h \circ h = e$, y así de forma sucesiva. En general, el grupo de Klein se define como el conjunto $V := \{e, h, r, v\}$ con la operación "$\circ$", que tiene una relación directa con la composición de funciones. La siguiente tabla muestra



todas las posibles operaciones que se pueden realizar:

$\circ$	e	h	r	v
e	e	h	r	v
h	h	e	v	r
r	r	v	e	h
v	v	r	h	e

Note que la operación es cerrada y asociativa. Además, el elemento neutro es e y el elemento inverso de un elemento es el mismo elemento, cumpliendo así con los axiomas de la definición de grupo 2.1.1.

Algunos ejemplos gráficos son los siguientes:

1. $(h \circ r)(R) = v(R)$

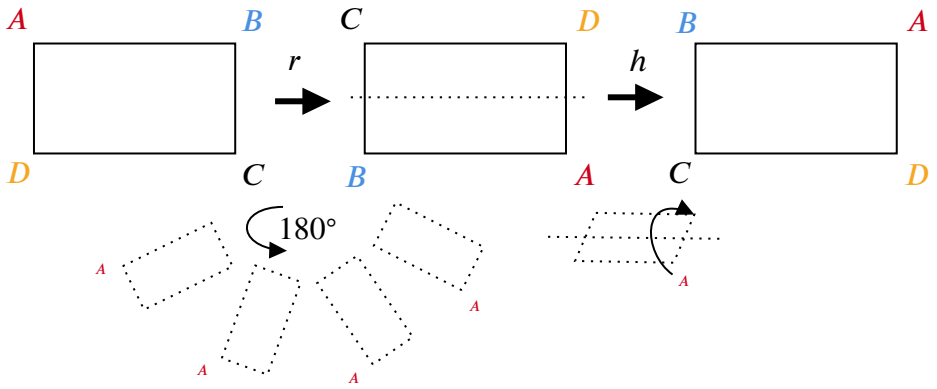
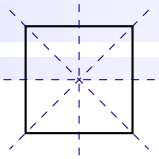


Figura 2.6: Operación $(h \circ r)(R)$
Fuente: Elaboración propia

2. $(v \circ v)(R) = e(R)$



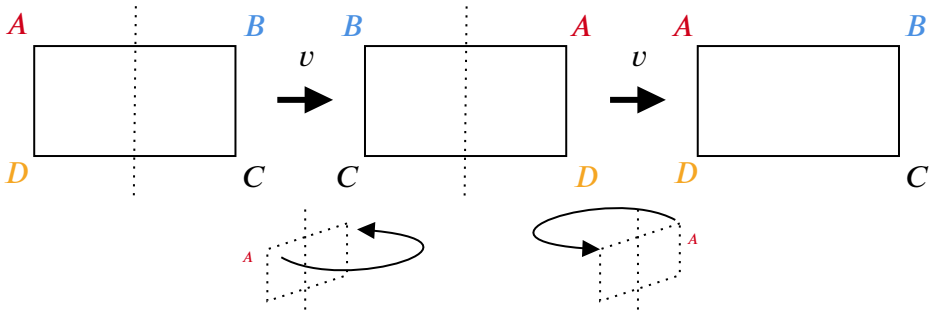


Figura 2.7: Operación $(v \circ v)(R)$

Fuente: Elaboración propia

3. $(v \circ h)(R) = r(R)$

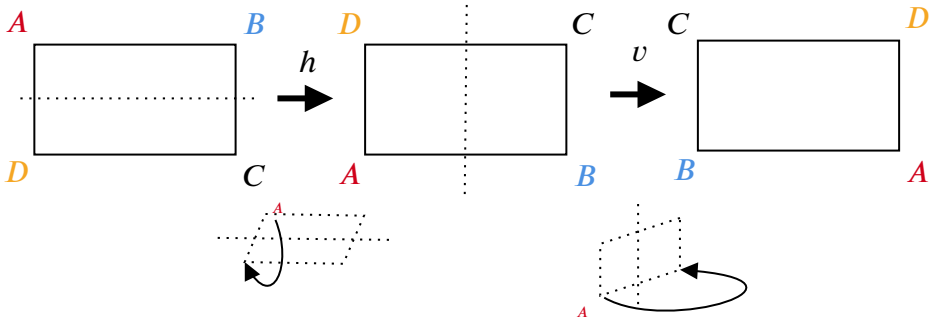


Figura 2.8: Operación $(v \circ h)(R)$

Fuente: Elaboración propia

4. $(h \circ h)(R) = e(R)$

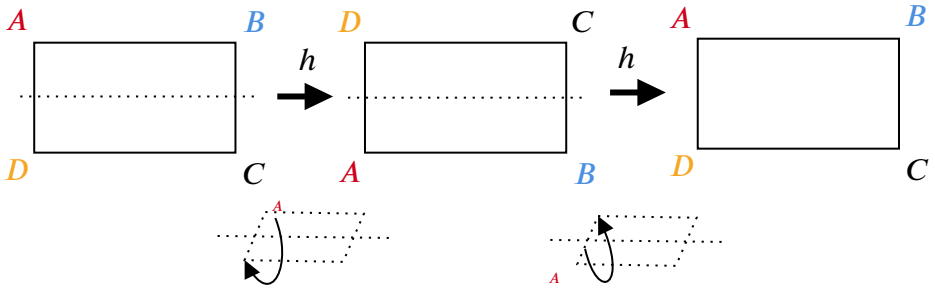
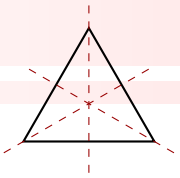


Figura 2.9: Operación $(h \circ h)(R)$

Fuente: Elaboración propia



5. $(r \circ v)(R) = h(R)$

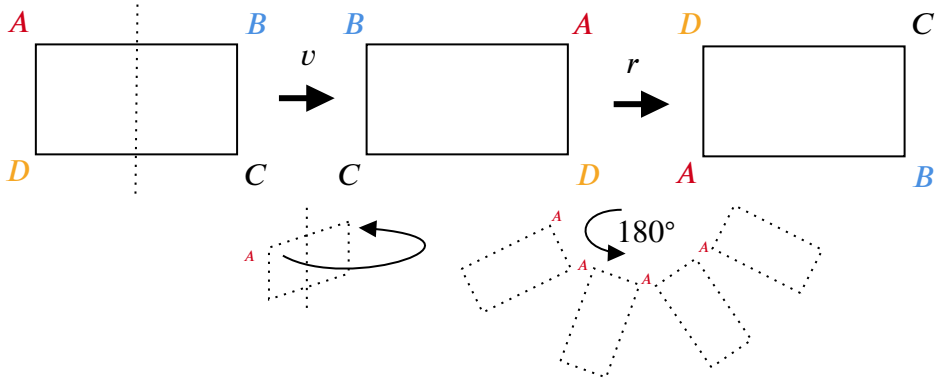


Figura 2.10: Operación $(r \circ v)(R)$
Fuente: Elaboración Propia

2.1.2. El grupo $(\mathbb{Z}_n, +)$

Teorema 2.1.1:

Para cualquier $n \in \mathbb{N}$, el conjunto $\mathbb{Z}_n$ es un grupo con la suma de clases de la definición 1.2.3.

$$[a] + [b] := [a + b]$$

para cualesquiera $[a], [b] \in \mathbb{Z}_n$.

Demostración. Se debe probar que $(\mathbb{Z}_n, +)$ satisface las condiciones de la definición de grupo (2.1.1).

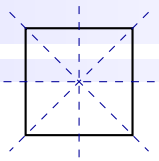
1. *Cerradura:* Sean $[x], [y] \in \mathbb{Z}_n$. Por el algoritmo de la división (1.1.3) existen $q, r \in \mathbb{Z}$ tales que

$$x + y = qn + r \quad \text{con} \quad 0 \leq r < n$$

Como $0 \leq r < n$, entonces $[r] \in \mathbb{Z}_n$. Ahora, tomando las clases módulo n y usando el hecho de que $[n] = [0]$, se tiene que

$$[x + y] = [qn + r] = [qn] + [r] = [q][n] + [r] = [r] \in \mathbb{Z}_n$$

Por lo tanto la suma de clases es cerrada sobre $\mathbb{Z}_n$.



2. *Asociatividad:* Sean $[x], [y], [z] \in \mathbb{Z}_n$. Entonces

$$\begin{aligned}
([x]+[y])+[z] &= [x+y]+[z] && \text{por la Definición 1.2.3 de suma en } \mathbb{Z}_n.\\
&= [(x+y)+z] && \text{por la Definición 1.2.3 de suma en } \mathbb{Z}_n.\\
&= [x+(y+z)] && \text{por la asociatividad en } \mathbb{Z}.\\
&= [x]+[y+z]\\
&= [x]+([y]+[z]).
\end{aligned}$$

3. *Existencia de elemento neutro:* en este caso el elemento neutro para la suma de clases es [0]. Esto se verifica fácilmente, pues sí $[x] \in \mathbb{Z}_n$, entonces

$$[x]+[0]=[x+0]=[x] \text{ y } [0]+[x]=[0+x]=[x].$$

4. *Existencia de inversos:* sea $[x] \in \mathbb{Z}_n$. Se puede suponer que $1 \leq x \leq n-1$. Entonces, por la observación (1.2.2) el inverso de $[x]$ es $[n-x] \in \mathbb{Z}_n$, pues

$$[x]+[n-x]=[x+(n-x)]=[n]=[0].$$

De igual forma se concluye que $[n-x]+[x]=[0]$. Con la información anterior se concluye que $(\mathbb{Z}_n, +)$ es un grupo.

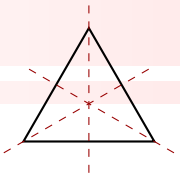
□

Ejemplo 2.1.17.

Por el teorema anterior, $(\mathbb{Z}_4, +)$ es grupo. Esto puede verificarse también mediante la siguiente tabla que contiene todas las operaciones posibles entre los elementos de $\mathbb{Z}_4$ bajo la operación $+$.

+	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

En efecto, note que [0] es el elemento neutro, la operación es asociativa y el inverso de [1] es [3], el inverso de [2] es él mismo y el inverso de [3] es [1].



2.1.3. El grupo $(\mathbb{Z}_p^*, \cdot)$, con p primo.

El teorema anterior señala que $(\mathbb{Z}_n, +)$ es un grupo con la suma de clases módulo n, para cualquier $n \in \mathbb{N}$. ¿Será cierto que $(\mathbb{Z}_n, \cdot)$ es un grupo con el producto de clases, para cualquier $n \in \mathbb{N}$? La respuesta es no, a menos que n sea primo. Observe los siguientes ejemplos:

Ejemplo 2.1.18.

El par $(\mathbb{Z}_4, \cdot)$, donde $\cdot$ es el producto de clases módulo 4, no es grupo. La tabla correspondiente a $(\mathbb{Z}_4, \cdot)$ se muestra a continuación.

$\cdot$	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

De acuerdo con la tabla anterior, en particular, note que [1] y [3] no tienen elemento inverso. Por lo tanto, $(\mathbb{Z}_4, \cdot)$ no es un grupo.

Ejemplo 2.1.19.

Sea $\mathbb{Z}_5^* = \mathbb{Z}_5 - \{[0]\}$. Contrario de lo que sucede en el ejemplo anterior, el par $(\mathbb{Z}_5^*, \cdot)$ sí es grupo, Para verificarlo, observe la siguiente tabla:

$\cdot$	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]
[2]	[2]	[4]	[1]	[3]
[3]	[3]	[1]	[4]	[2]
[4]	[4]	[3]	[2]	[1]

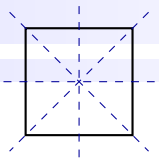
Note que la operación es cerrada y asociativa. Además, el elemento neutro es [1] y el elemento inverso de [1] es él mismo, el elemento inverso de [2] es [3], el inverso de [3] es [2] y el inverso de [4] es él mismo.

Definición 2.1.2:

Sea $p \in \mathbb{N}$. Se define

$$\mathbb{Z}_p^* := \{[1], [2], \ldots, [p-1]\} .$$

Ejemplo 2.1.20.



Para $p = 2$, $p = 3$, $p = 4$ y $p = 5$ tenemos los siguientes conjuntos de clases

$$\begin{aligned}
\mathbb{Z}_2^* &:= \{[1]\} \\
\mathbb{Z}_3^* &:= \{[1], [2]\} \\
\mathbb{Z}_4^* &:= \{[1], [2], [3]\} \\
\mathbb{Z}_5^* &:= \{[1], [2], [3], [4]\}\,.
\end{aligned}$$

Teorema 2.1.2:

Sea $p \in \mathbb{Z}$. El par $\left(\mathbb{Z}_p{}^*, \cdot\right)$ es un grupo si y solo si p es primo.

Demostración.

("⇒") Suponga que $(\mathbb{Z}_p{}^*, \cdot)$ es grupo y por contradicción suponga que p no es primo. Entonces, existen $a, b \in \mathbb{N}$ tales que $p = ab$. En particular, $[a], [b] \in \mathbb{Z}_p^*$. En módulo p se tiene que

$$[p] = [ab] = [a][b],$$

pero $[p] = [0]$ módulo p, por lo que

$$[0] = [a][b].$$

Esto significa que $[a][b] \notin \mathbb{Z}_p^*$ lo cual contradice la hipótesis de que $(\mathbb{Z}_p{}^*, \cdot)$ es grupo, en particular, contradice la cerradura de la operación "$\cdot$". Por lo tanto p es primo.

("⇐") Suponga ahora que p es primo. Se debe probar que $\mathbb{Z}_p{}^*$ es grupo.

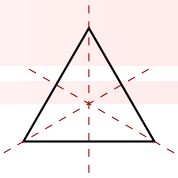
1. *Cerradura:* sean $[a], [b] \in \mathbb{Z}_p{}^*$. Sin pérdida de generalidad suponga que a, b son positivos. Por el algoritmo de la división (Teorema 1.1.3) existen $q, r \in \mathbb{Z}$, tales que

$$ab = pq + r \quad \text{con } 0 \leq r < p, \tag{2.2}$$

entonces, módulo p se tiene que

$$[ab] = [pq + r] = [p][q] + [r] = [r].$$

Ahora se debe probar que $[r] \in \mathbb{Z}_p^*$. Para ello se verifica que $0 < r < p$. Sin embargo, ya se tiene que $r < p$, falta probar que $0 < r$.



Si $r = 0$ entonces de la igualdad en (2.2) se tiene

$$ab = pq,$$

lo cual implica

$$[a][b] = [0] \text{ módulo } p.$$

Esto es equivalente a

$$ab \equiv 0(mod\ p),$$

es decir $p|ab$. Como p es primo, entonces

$$p|a \quad \text{o} \quad p|b$$

Esto es lo mismo que $[a] = [0]$ o $[b] = [0]$, lo cual contradice $[a], [b] \in \mathbb{Z}_p^*$. Así que $0 < r < p$, por lo que que $[a][b] = [r] \in \mathbb{Z}_p{}^*$.

2. *Asociatividad:* se hereda de la asociatividad del producto en $\mathbb{Z}$.

3. *Existencia de elemento neutro:* el neutro para el producto de clases es la clase $[1]$.

4. *Elementos inversos:* Sea $[x] \in \mathbb{Z}_p^*$. Como p es primo por hipótesis, el máximo común divisor de x y p es 1, es decir $(x, p) = 1$. Por el Teorema 1.1.4, existen $s, t \in \mathbb{Z}$ tales que

$$1 = ps + tx,$$

tomando módulo p se tiene

$$[1] = [t][x]. \tag{2.3}$$

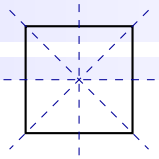
Note que $[t]$ es el posible inverso de $[x]$. Falta probar que $[t] \in \mathbb{Z}_p^*$. Por el algoritmo de la división (Teorema 1.1.3) existen $q, r \in \mathbb{Z}$ tales que

$$t = qp + r \quad \text{con} \quad 0 \leq r < p.$$

Si $r = 0$ entonces $t = pq$, esto significa que, módulo p

$$[t] = [pq] = [p][q] = [0][q] = [0]$$

pero $[1] = [t][x]$, por lo que $[1] = [0]$, lo cual es una contradicción. De lo anterior, necesariamente



$0 < r < p$. Esto implica que $[r] \in \mathbb{Z}_p^*$ y además

$$t = qp + r \quad \text{con} \quad 0 < r < p.$$

Restando r tomando módulo p en la igualdad anterior se tiene

$$[t - r] = [qp] = [q][p] = [0],$$

es decir,

$$[t] = [r] \in \mathbb{Z}_p^*.$$

Luego, por la ecuación (2.3) y el hecho de que $[t] \in \mathbb{Z}_p^*$, se concluye que existe un inverso para $[x]$.

Por lo tanto, $\mathbb{Z}_p{}^*$ con el producto de clases módulo p, es un grupo, siempre y cuando p se un número primo. □

2.1.4. El grupo $(U_n, \cdot)$

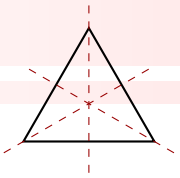
El objetivo es construir un grupo de elementos de $\mathbb{Z}_n$ de modo que la operación de producto se trabaje de forma similar que en $\mathbb{Z}$ con algunas diferencias importantes. Por ejemplo, en $\mathbb{Z} \subset \mathbb{Q}$, la ecuación $xy = 0$ implica $x = 0$ o $y = 0$,co cual no necesariamente sucede en $\mathbb{Z}_n$. Es decir, puede haber elementos $[x], [y] \in \mathbb{Z}_n$ con $[x] \neq [0], [y] \neq [0]$ tales que $[x][y] = [0]$. Por ejemplo en $\mathbb{Z}_6$ se tiene que $[2] \neq [0], [3] \neq [0]$, pero $[2][3] = [6] = [0]$.

Además, en $\mathbb{Z} \subset \mathbb{Q}$, es posible resolver la ecuación $3x = 0$ dividiendo por 3 y se tiene que la única solución es $x = 0$. En $\mathbb{Z}_6$, si se tiene la ecuación $[3]x = [0]$, las soluciones podrían ser $x = [0]$ o $x = [2]$.

Otra diferencia importante es que en $\mathbb{Z}$ los únicos elementos invertibles bajo la multiplicación, son 1 y -1. En $\mathbb{Z}_n$, con el producto de clases módulo n, pueden haber muchos elementos invertibles, como se vio en el apartado anterior. Por ejemplo, en $\mathbb{Z}_5$ se tiene que

$$[1][1] = [1], \quad [2][3] = [1], \quad [4][4] = [1]$$

Por lo tanto, los elementos [1], [2], [3], [4] son invertibles. No obstante, aún con estas diferencias, se puede rescatar una porción apropiada de $\mathbb{Z}_n$, que sí forma un grupo respecto al producto. .



Definición 2.1.3:

Sea $n \in \mathbb{N}$ y $[a] \in \mathbb{Z}_n$, $[a] \neq [0]$.

1. $[a]$ se llama un **divisor de cero** si existe $[b] \in \mathbb{Z}_n$, $[b] \neq [0]$, tal que $[a][b] = [0]$.
2. $[a]$ se llama una **unidad** o **invertible**, si existe $[b] \in \mathbb{Z}_n$ tal que $[a][b] = [1]$. En este caso $[b]$ se llama **inverso** de $[a]$ y se denota por $[a]^{-1}$.

Ejemplo 2.1.21.

1. En $\mathbb{Z}_6$, $[2] \neq [0], [3] \neq [0]$ y $[2][3] = [0]$. Entonces $[2]$ y $[3]$ son divisores de cero. Además, note que $[2]$ y $[3]$ no son una unidad, es decir, no son invertibles.
2. En $\mathbb{Z}_5$,
$$[1][1] = [1], \quad [2][3] = [1], \quad [4][4] = [1]$$
Entonces $[1], [2], [3]$ Y $[4]$ son unidades (o invertibles). En este caso $[1]^{-1} = [1]$, $[2]^{-1} = [3]$, $[3]^{-1} = [2]$ y $[4]^{-1} = [4]$. Además, note que $[1], [2], [3]$ Y $[4]$ no son divisores de cero.

Observación 2.1.4.

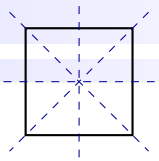
1. En $\mathbb{Z}_n$, si $[a] \neq [0]$ es un divisor de cero, entonces no es una unidad, es decir, no es invertible.
2. En $\mathbb{Z}_n$, si $[a] \neq [0]$ es una unidad, es decir, es invertible, entonces no es un divisor de cero.
3. El siguiente teorema proporciona un criterio para hallar todos los divisores de cero y unidades de $\mathbb{Z}_n$, con $n \in \mathbb{N}$. Es importante recordar que dados $a, b \in \mathbb{Z}$, el par (a, b) denota al máximo común divisor de a y b.

Teorema 2.1.3:

Sea $n \in \mathbb{Z}$ y $[a] \in \mathbb{Z}_n$.

1. $[a] = [0]$ si y sólo si $(a, n) = n$.
2. $[a]$ es un divisor de cero si y sólo si $1 < (a, n) < n$.
3. $[a]$ es una unidad si y sólo si $(a, n) = 1$.

Demostración.



1. ($\Rightarrow$) Suponga que $[a] = [0]$ módulo n. Se debe probar que $(a, n) = n$. Como $[a] = [0]$, entonces $a \equiv 0(mod\ n)$. Por definición de congruencia módulo n esto significa $n|a$, lo cual implica $(a, n) = n$. ($\Leftarrow$) Suponga ahora que $n = (a, n)$. Entonces n es un divisor de a, es decir $a = kn$ para algún $k \in \mathbb{Z}$. Entonces, en módulo n se tiene que

$$[a] = [kn] = [k][n] = [k][0] = [k \cdot 0] = [0]$$

2. ($\Rightarrow$) Suponga que $[a]$ es un divisor de cero. Se debe probar que $1 < (a, n) < n$. Para ello, denote $d = (a, n)$. Como $[a]$ es un divisor de cero, por definición $[a] \neq [0]$. Entonces, por la parte uno de este teorema, que ya se demostró, se tiene que $d < n$. Falta probar que $1 < d$. Con este fin, por contradicción suponga que $d = 1$. Por el Teorema 1.1.4 existen $s, t \in \mathbb{Z}$, tales que

$$1 = sa + tn$$

Entonces, en módulo n

$$[1] = [s][a] + [t][n] = [s][a], \quad \text{es decir,} \quad [1] = [s][a]. \tag{2.4}$$

Note que $[s] \neq [0]$, pues de lo contrario se tendría que $[1] = [0]$ en la ecuación anterior. Entonces $[s] \in \mathbb{Z}_n - \{0\}$. Luego, por la demostración del Teorema 2.1.2, específicamente donde se demostró la existencia de inversos, se infiere que $[a]$ es una unidad (o es invertible). Por otro lado, por hipótesis se tiene que $[a]$ es un divisor de cero. Es decir, existe $[b] \in \mathbb{Z}_n$, $[b] \neq [0]$, tal que

$$[a][b] = [0].$$

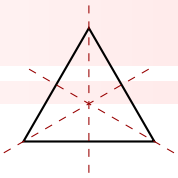
Multiplicando por $[b]$ en la ecuación (2.4) se tiene que

$$[b] = [1 \cdot b] = [1][b] = \big([s][a]\big)\,[b] = [s]\,\big([a][b]\big) = [s][0] = [s \cdot 0] = [0],$$

lo cual es una contradicción. Se sigue que el supuesto $d = 1$ no puede ser verdadera. Por lo tanto $1 < (a, n) < n$.

($\Leftarrow$) Suponga ahora que $1 < (a, n) < n$ y denote $d = (a, n)$. Se debe probar que $[a]$ es un divisor de cero. Como $d = (a, n)$, por definición de máximo común divisor $d|a$ y $d|n$. Entonces, existen $p, q \in \mathbb{Z}$ tales que

$$a = pd \quad \text{y} \quad n = qd.$$



Como $1 < d$ por hipótesis, entonces multiplicando por q se tiene que

$$q < qd = n,$$

esto implica que, en módulo n,

$$[q] \neq [n] = [0].$$

Luego,

$$[a][q] = [aq] = [(pd)q] = [p(dq)] = [pn] = [p][n] = [p][0] = [p \cdot 0] = [0],$$

y como $[q] \neq [0]$, se concluye que $[a]$ es un divisor de cero.

3. ($\Rightarrow$) Suponga que $[a]$ es una unidad y denote $d = (a, n)$. Se debe probar que $d = 1$. Para ello suponga por contradicción que $1 < d$. Como $d = (a, n)$, por definición de máximo común divisor $d|a$ y $d|n$. Entonces, existen $p, q \in \mathbb{Z}$ tales que

$$a = pd \quad \text{y} \quad n = qd.$$

Como $1 < d$, entonces multiplicando por q se tiene que

$$q < qd = n,$$

esto implica que, en módulo n,

$$[q] \neq [n] = [0].$$

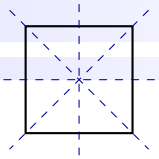
Luego,

$$[a][q] = [aq] = [(pd)q] = [p(dq)] = [pn] = [p][n] = [p][0] = [p \cdot 0] = [0]$$

y como $[q] \neq [0]$, se obtiene que $[a]$ es un divisor de cero, lo cual contradice la hipótesis de que $[a]$ es una unidad. Por lo tanto $d = 1$.

($\Leftarrow$) Suponga ahora que $d = (a, b) = 1$. Se debe probar que $[a]$ es una unidad, es decir, que es invertible. Por el Teorema 1.1.4 existen s, t tales que

$$1 = sa + tn.$$



Puesto que $[n] = [0]$ en módulo n, entonces

$$[1] = [s][a]. \tag{2.5}$$

Note que $[s]$ es el posible inverso de $[a]$. Falta probar que $[s]$ es un elemento de $\mathbb{Z}_n$. Para ello, por el algoritmo de la división (Teorema 1.1.3) existen $q, r \in \mathbb{Z}$ tales que

$$s = qn + r \quad \text{con} \quad 0 \leq r < n.$$

Si $r = 0$ entonces $s = nq$. En módulo n esto significa

$$[s] = [nq] = [n][q] = [0][q] = [0],$$

pero $[1] = [s][a]$, y por la igualdad anterior $[1] = [0]$, lo cual es una contradicción. De lo anterior, necesariamente $0 < r < n$. En particular $[r] \in \mathbb{Z}_n^*$ y

$$s = qn + r \quad \text{con} \quad 0 < r < n$$

esto implica que, en módulo n,

$$[s - r] = [qn] = [q][n] = [0],$$

es decir

$$[s] = [r] \in \mathbb{Z}_n^*.$$

Luego, por la ecuación (2.5) y el hecho de que $[s] \in \mathbb{Z}_n^*$, se concluye que existe un inverso para $[a]$.

□

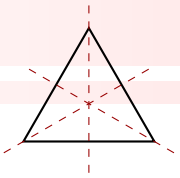
Definición 2.1.4:

Se define el conjunto de unidades de $\mathbb{Z}_n$ por

$$U_n := \left\{ [a] \in \mathbb{Z}_n : \ [a] \text{ es una unidad} \right\}.$$

Observación 2.1.5.

Puesto que $[a] \in \mathbb{Z}_n$ es una unidad si y sólo si $(a, n) = 1$, resultado mostrado en la parte tres del teorema



2.1.3, entonces también se puede escribir

$$U_n := \left\{ [a] \in \mathbb{Z}_n \,:\, (a,n) = 1 \right\}.$$

Ejemplo 2.1.22.

El conjunto de unidades U_5, está formado por todos los $[a] \in \mathbb{Z}_5$ tales que $(a,5) = 1$. Es decir, U_5 está formado por las clases módulo 5, de los primos relativos con 5, menores que 5. En otra palabras, para hallar los elementos de U_5, basta buscar los primos relativos con 5. En este caso los números 1, 2, 3 y 4 son primos relativos con 5, entonces las clases $[1], [2], [3], [4]$ están en U_5. De esta forma

$$U_5 = \{[1], [2], [3], [4]\}.$$

Ejemplo 2.1.23.

El conjunto U_6 es el conjunto de todas las unidades de $\mathbb{Z}_6$. Como los únicos primos relativos con 6, menores que 6, son 1 y 5, entonces

$$U_6 = \{[1], [5]\}.$$

Ejemplo 2.1.24.

El conjunto U_9 es el conjunto de todas las unidades de $\mathbb{Z}_9$. Los primos relativos con 9, menores que 9, son 1,2,4,5 y 7, entonces

$$U_9 = \{[1], [2], [4], [5], [7], [8]\}.$$

Teorema 2.1.4:

Sea $n \in \mathbb{N}$. El conjunto U_n es un grupo con el producto de clases módulo n.

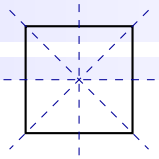
Demostración.

1. *Cerradura:* sean $[a], [b] \in U_n$. Se debe probar probar que $[ab] \in U_n$. Como $[a]$ y $[b]$ son unidades, existen $[a]^{-1}, [b]^{-1} \in U_n$ tales que

   $$[a][a]^{-1} = [1] \quad \text{y} \quad [b][b]^{-1} = [1].$$

   Entonces

   $$[a][b][b]^{-1}[a]^{-1} = [a][1][a]^{-1} = [a][a]^{-1} = [1],$$



de lo cual se obtiene que el inverso de $[ab]$ es

$$[ab]^{-1} = [b]^{-1}[a]^{-1}.$$

Por lo tanto $[ab]$ es una unidad y debe estar en U_n.

2. *Asociatividad:* se hereda de la asociatividad del producto en $\mathbb{Z}_n$.

3. *Elemento identidad:* el elemento identidad en U_n es $[1] \in U_n$.

4. *Inversos:* por la definición de U_n, si $[a] \in U_n$, existe $[a]^{-1} \in U_n$ tal que $[a][a]^{-1} = [1]$ y $[a]^{-1}[a] = [1]$.

Por lo tanto $(U_n, \cdot)$ es un grupo. □

Ejemplo 2.1.25.

El conjunto U_8 corresponde a $U_8 = \{a \in \mathbb{Z}_8 : (a, 8) = 1\} = \{[1], [3], [5], [7]\}$. La tabla del grupo $(U_8, \cdot)$ es

$\cdot$	[1]	[3]	[5]	[7]
[1]	[1]	[3]	[5]	[7]
[3]	[3]	[1]	[7]	[5]
[5]	[5]	[7]	[1]	[3]
[7]	[7]	[5]	[3]	[1]

Entonces U_8 con el producto de clases módulo 8, es un grupo.

2.1.5. Grupos de funciones

Ejemplo 2.1.26.

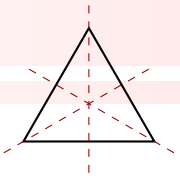
Sea A un subconbjunto de $\mathbb{R}$ y considere el conjunto

$$\mathcal{F} := \{f : A \to \mathbb{R} \ : \ f \text{ es una función}\}.$$

En $\mathcal{F}$ se define la suma de funciones como

$$(f + g)(x) := f(x) + g(x),$$

para cualesquiera $f, g \in \mathcal{F}$ y para todo $x \in A$. Con esta operación $\mathcal{F}$ es un grupo ya que cumple con los axiomas de la definición 2.1.1.



Demostración.

1. *Cerradura:* si f, g son funciones de $\mathcal{F}$, note que $f+g : A \to \mathbb{R}$, entonces $f+g$ pertenece a $\mathcal{F}$.

2. *Asociatividad:* sean f, g y h funciones de $\mathcal{F}$, entonces

$$\begin{aligned}((f+g)+h)(x) &= (f+g)(x)+h(x)\\ &= (f(x)+g(x))+h(x)\\ &= f(x)+(g(x)+h(x))\\ &= f(x)+(g+h)(x)\\ &= (f+(g+h))(x)\end{aligned}$$

3. *Elemento neutro:* el elemento neutro es la función constante nula $0 : A \to \mathbb{R}$ tal que $0(x) = 0$.

4. *Existencia de elementos inversos:* el elemento inverso de una función f en $\mathcal{F}$ en es la función $-f : A \to \mathbb{R}$ tal que $(-f)(x) = -f(x)$.

□

Ejemplo 2.1.27.

Sea A un subconbjunto de $\mathbb{R}$. Considere el conjunto

$$C(A,\mathbb{R}) := \{f : A \to \mathbb{R} \mid : f \quad \text{es una función continua}\}.$$

$C(A,\mathbb{R})$ es un grupo, con la misma operación definida en el ejemplo anterior. En este caso, para la cerradura recuerde que la suma de funciones continuas genera otra función continua. Los demás axiomas son idénticos al ejemplo anterior.

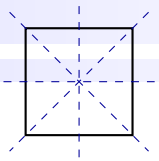
Ejemplo 2.1.28.

Considere el conjunto

$$G := \{f : A \subset \mathbb{R} \to A \mid : f \quad \text{es una función biyectiva}\}.$$

G con la composición de funciones usual, es un grupo.

Demostración. Recuerde que si f, g están en G, entonces se define la composición de funciones como $f \circ g : A \subset \mathbb{R} \to A$ tal que $(f \circ g)(x) = f(g(x))$, para todo $x \in A$.



1. *Cerradura:* se cumple de forma inmediata a partir de la definición de composición de funciones.

2. *Asociatividad:* sean f, g y h funciones de G y sea $x \in A$, entonces

$$\begin{aligned}((f\circ g)\circ h)(x) &= (f\circ g)(h(x))\\ &= f(g(h(x)))\\ &= f((g\circ h)(x))\\ &= (f\circ(g\circ h))(x)\end{aligned}$$

   Esto prueba que la igualdad $((f\circ g)\circ h)(x) = (f\circ(g\circ h))(x)$ se cumple para todo $x \in A$, por lo tanto $(f\circ g)\circ h = f\circ(g\circ h)$

3. *Elemento neutro:* el elemento neutro es la función identidad $i : A \subset \mathbb{R} \to A$ tal que $i(x) = x$. De hecho, si $f \in G$, note que $(f\circ i)(x) = f(i(x)) = f(x)$. De forma análoga $(i\circ f)(x) = f(x)$.

4. *Existencia de elementos inversos:* sea f una función de G, entonces f es biyectiva, por lo tanto existe una función inversa definida por $f^{-1} : A \subset \mathbb{R} \to A$ tal que

$$(f\circ f^{-1})(x) = f(f^{-1}(x)) = x = i(x).$$

   De igual forma se concluye que $(f^{-1}\circ f)(x) = i(x)$.

□

Ejemplo 2.1.29.

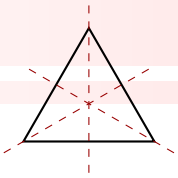
El conjunto de rectas

$$G := \{y : \mathbb{R} \to \mathbb{R} \ : \ y(x) = mx + b, \ \ m, b \in \mathbb{R}, \ m > 0\},$$

junto con la operación composición de funciones, es un grupo.

Demostración. Dado que en G se define la composición de funciones, entonces la cerradura, la asociatividad, la existencia del elemento neutro y la existencia de elementos inversos, son heredadas del ejemplo anterior. Sin embargo, a continuación se especifica su prueba, excepto la asociatividad porque es la misma.

1. *Cerradura:* sean y_1, y_2 en G, entonces $y_1(x) = m_1x + b_1$ y $y_2(x) = m_2x + b_2$, donde m_1, m_2, b_1, b_2



son números reales y m_1 y m_2 son positivos. Ahora, note que

$$\begin{aligned}(y_1 \circ y_2)(x) &= y_1(y_2(x)) \\ &= y_1(m_2x + b_2) \\ &= m_1(m_2x + b_2) + b_1 \\ &= m_1m_2x + m_1b_2 + b_1.\end{aligned}$$

Visualice que $m_1m_2 > 0$. Así, $(y_1 \circ y_2)(x) = m_1m_2x + m_1b_2 + b_1$ es una recta con pendiente positiva, de donde se induce que $y_1 \circ y_2 \in G$.

2. *Elemento neutro:* el elemento neutro es la recta identidad $i : \mathbb{R} \to \mathbb{R}$ tal que $i(x) = 1x + 0 = x$. Es claro que esta recta pertenece a G.

3. *Existencia de elementos inversos:* sea $y : \mathbb{R} \to \mathbb{R}$ una recta de G, $y = mx + b$, con $m, b \in \mathbb{R}$ y $m > 0$. Esta recta es biyectiva, por tanto tiene inversa, la cual está dada por $y^{-1} : \mathbb{R} \to \mathbb{R}$ tal que $y^{-1}(x) = \frac{1}{m}x - \frac{b}{m}$. Como $m > 0$ es inmediato que $\frac{1}{m} > 0$, entonces y^{-1} es una recta de G. Además, no es difícil comprobar que

$$(y \circ y^{-1})(x) = x = (y^{-1} \circ y)(x).$$

□

2.1.6. El grupo simétrico S_n

Definición 2.1.5:

Se define el conjunto S_n, con $n \in \mathbb{N}$, por

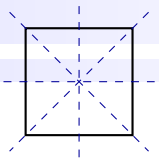
$$S_n := \left\{ \sigma : \{1, 2, 3, \dots, n\} \to \{1, 2, 3, \dots, n\} \;\middle|\; \sigma \text{ es biyectiva} \right\}.$$

Es decir, S_n consiste en todas las posibles permutaciones de n elementos ya que es el conjunto de todas las biyecciones del conjunto $\{1, 2, 3, \dots, n\}$ en sí mismo. Los elementos de S_n se llaman *permutaciones*.

Definición 2.1.6:

Se define el conjunto S_n, con $n \in \mathbb{N}$, por

$$S_n := \left\{ \sigma \in \mathbb{M}_{2\times n}(\mathbb{R}) \mid \sigma \text{ es una matriz de permutación} \right\}.$$



Es decir, S_n consiste en todas las matrices de permutación de tamaño $2 \times n$, donde en cada fila existe una permutación del conjunto $\{1, 2, 3, \ldots, n\}$. Aquí σ es biyectiva y se representa por:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ 1 & 2 & 3 & \ldots & n \end{pmatrix}.$$

Observación 2.1.6.

En la teoría de grupos, especialmente en el estudio de grupos simétricos, es usual utilizar matrices debido a que proporcionan un lenguaje y una estructura muy poderosa para describir, analizar y manipular simetrías y transformaciones, lo que las hace esenciales en el estudio de los grupos simétricos. Particularmente, una **matriz de permutación** es una matriz que representa una permutación de elementos en un conjunto finito. Esto facilita el estudio algebraico y computacional de las permutaciones.

Ejemplo 2.1.30.

Considere el conjunto $X = \{1, 2, 3\}$. De acuerdo con la definición anterior el conjunto S_3 es

$$S_3 := \{\sigma : X \to X \mid \sigma \text{ es una función biyectiva } \}$$

Observe que el conjunto S_3 tiene $3! = 6$ elementos o permutaciones. Explícitamente, estas permutaciones son:

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

$$\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

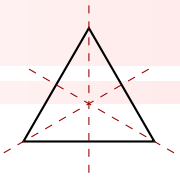
Definición 2.1.7:

Se define en S_n, la operación composición "$\circ$" por

$$\sigma_1\sigma_2 := \sigma_1 \circ \sigma_2,$$

para cualesquiera $\sigma_1, \sigma_2 \in S_n$.

Ejemplo 2.1.31.



Continuando con el ejemplo 2.1.30 sobre el conjunto S_3 y considerando la operación composición de funciones, se tendría en particular que $\sigma_3 \circ \sigma_4$ es la función definida por:

$$\begin{aligned}(\sigma_3\circ\sigma_4)(1) &= \sigma_3(\sigma_4(1)) = \sigma_3(2) = 3,\\ (\sigma_3\circ\sigma_4)(2) &= \sigma_3(\sigma_4(2)) = \sigma_3(3) = 2,\\ (\sigma_3\circ\sigma_4)(3) &= \sigma_3(\sigma_4(3)) = \sigma_4(1) = 1.\end{aligned}$$

Así que $\sigma_3 \circ \sigma_4 = \sigma_6$. De forma análoga, se puede comprobar que

$$\sigma_1\circ\sigma_2 = \sigma_2, \qquad \sigma_2\circ\sigma_3 = \sigma_4, \quad , \quad \sigma_3\circ\sigma_5 = \sigma_2.$$

$$\sigma_4\circ\sigma_6 = \sigma_3, \qquad \sigma_5\circ\sigma_4 = \sigma_1, \qquad \sigma_6\circ\sigma_1 = \sigma_6.$$

Similarmente se construyen todas las demás combinaciones y se obtiene la tabla siguiente:

$\circ$	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_1	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_2	σ_2	σ_1	σ_4	σ_3	σ_6	σ_5
σ_3	σ_3	σ_5	σ_1	σ_6	σ_2	σ_4
σ_4	σ_4	σ_6	σ_2	σ_5	σ_1	σ_3
σ_5	σ_5	σ_3	σ_6	σ_1	σ_4	σ_2
σ_6	σ_6	σ_4	σ_5	σ_2	σ_3	σ_1

En particular, note que si se considera el par $(S_3, \circ)$, entonces la composición es una operación cerrada según se visualiza en la tabla, la composición de funciones biyectivas es asociativa como se demostró en los ejemplos de grupo de funciones, la función σ_1 es el elemento neutro, los elementos inversos de σ_2, σ_3 y σ_6 son ellos mismos, el inverso de σ_4 es σ_5 y el inverso de σ_5 es σ_4. Por lo tanto, el par $(S_3, \circ)$ es un grupo. De hecho, el teorema a continuación generaliza este resultado.

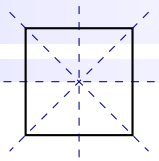
Teorema 2.1.5:

El conjunto S_n, con $n \in \mathbb{N}$, es un grupo con la operación definida por

$$\sigma_1\sigma_2 := \sigma_1\circ\sigma_2,$$

para cualesquiera $\sigma_1, \sigma_2 \in S_n$, donde "$\circ$" es la composición de funciones

Demostración. Se debe mostrar los axiomas de la definición 2.1.1, esto es:



1. **Cerradura:** tome dos elementos arbitrarios σ_1 y σ_2 de S_n, se debe demostrar que la composición $\sigma_1 \circ \sigma_2$ es un elemento de S_n. Ahora, dado que σ_1 y σ_2 son biyecciones de $\{1, 2, 3, \ldots, n\}$ en sí mismos, entonces la composición $\sigma_1 \circ \sigma_2$ debe ser una biyección de $\{1, 2, 3, \ldots, n\}$ en sí misma, es decir, $\sigma_1 \circ \sigma_2 \in S_n$.

2. *Asociatividad:* la asociatividad se hereda de la composición de funciones biyectivas (ver ejemplo 2.1.28).

3. *Elemento neutro:* sea σ_1 la función de S_n que deja todos los elementos inalterados, es decir

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ 1 & 2 & 3 & \ldots & n \end{pmatrix}.$$

   Note que para cualquier $\sigma \in S_n$ se cumple que $\sigma \circ \sigma_1 = \sigma = \sigma_1 \circ \sigma$. Entonces, σ_1 actúa como el elemento neutro de $(S_n, \circ)$.

4. *Existencia de elementos inversos:* sea σ un elemento de S_n, σ diferente del elemento neutro σ_1, entonces necesariamente debe existir una permutación que deshace la reorganización realizada por σ. Denote esta permutación σ^{-1}. Entonces

$$\sigma \circ \sigma^{-1} = \sigma_1 = \sigma^{-1} \sigma.$$

□

Por lo tanto $(S_n, \circ)$ es un grupo.

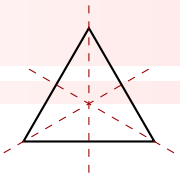
2.1.7. Grupos de Matrices

Ejemplo 2.1.32.

Denote por $M(m, n, \mathbb{R})$ al conjunto de matrices de tamaño $m \times n$ con entradas en $\mathbb{R}$. Este conjunto, con la suma usual de matrices, es un grupo.

Demostración.

1. *Cerradura*: Sean $A = (a_{ij})_{m \times n}$ y $B = (b_{ij})_{m \times n}$ dos matrices en $M(m, n, \mathbb{R})$. Se debe probar que



$A + B \in M(m, n, \mathbb{R})$. Para ello, receurde que la suma de matrices se define como

$$A + B = (a_{ij})_{m\times n} + (b_{ij})_{m\times n} = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \cdots & a_{1n} + b_{1n} \\ a_{21} + b_{21} & a_{22} + b_{22} & \cdots & a_{2n} + b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} + b_{m1} & a_{m2} + b_{m2} & \cdots & a_{mn} + b_{mn} \end{pmatrix}$$

Esta nueva matriz es de tamaño $m \times n$, por lo que $A + B \in M(m, n, \mathbb{R})$.

2. *Asociatividad*: considere las matrices $A = (a_{ij})_{m\times n}$, $B = (b_{ij})_{m\times n}$, $C = (c_{ij})_{m\times n}$, entonces

$$\begin{aligned} (A + B) + C &= \Big((a_{ij})_{m\times n} + (b_{ij})_{m\times n}\Big) + (c_{ij})_{m\times n} \\ &= \Big((a_{ij} + b_{ij})_{m\times n}\Big) + (c_{ij})_{m\times n} \\ &= \Big((a_{ij} + b_{ij}) + c_{ij}\Big)_{m\times n} \quad \text{por definición de suma de matrices.} \\ &= \Big(a_{ij} + (b_{ij} + c_{ij})\Big)_{m\times n} \quad \text{por la asociatividad de la suma en } \mathbb{R}. \\ &= (a_{ij})_{m\times n} + \Big(b_{ij} + c_{ij}\Big)_{m\times n} \quad \text{por definición de suma de matrices.} \\ &= (a_{ij})_{m\times n} + \Big((b_{ij})_{m\times n} + (c_{ij})_{m\times n}\Big) \\ &= A + (B + C). \end{aligned}$$

Por lo tanto $(A + B) + C = A + (B + C)$.

3. *Elemento neutro*: el elemento neutro para la suma de matrices, es la matriz nula de tamaño $m \times n$, la cual se escribe como $0_{m\times n} \in M(m, n, \mathbb{R})$.

4. *Existencia de inversos*: Para cualquier matriz $A \in M(m, n, \mathbb{R})$ la inversa de A (con respecto a la suma) es $-A \in M(m, n, \mathbb{R})$.

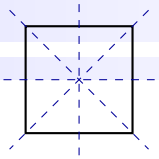
Por lo tanto $M(n, m, \mathbb{R})$ es un grupo con la suma de matrices. □

Ejemplo 2.1.33.

Denote por $GL(n, \mathbb{R})$ al conjunto de matrices invertibles de orden n con entradas en $\mathbb{R}$, definido por

$$GL(n, \mathbb{R}) := \{A \in M(n, \mathbb{R}) : \det A \neq 0\}. \tag{2.6}$$

El par $(GL(n, \mathbb{R}), \cdot)$, donde $\cdot$ es el producto usual de matrices, es un grupo. Este grupo es llamado **Grupo General Lineal (real)**.



Demostración.

1. *Cerradura*: sean A, B matrices en $GL(n,\mathbb{R})$, se debe probar que $AB \in GL(n,\mathbb{R})$. Como A y B están en $GL(n,\mathbb{R})$, entonces $\det A \neq 0$ y $\det B \neq 0$. Por las propiedades del determinante se tiene que
$$\det(AB) = \det(A)\det(B) \neq 0.$$
Esto implica que el AB es invertible. Por lo tanto $AB \in GL(n,\mathbb{R})$.

2. *Asociatividad*: sean A, B, C matrices en $GL(n,\mathbb{R})$. Puesto que estas matrices son cuadradas del mismo orden, entonces los productos BC y $A(BC)$ están definidos. Por lo tanto
$$A(BC) = (AB)C.$$

3. *Elemento neutro*: el elemento neutro para la multiplicación de matrices es la matriz identidad $I_n \in GL(n,\mathbb{R})$. Recuerde que $\det I_n = 1$.

4. *Existencia de inversos*: por la definición de $GL(n,\mathbb{R})$, para cualquier matriz $A \in GL(n,\mathbb{R})$ existe una inversa $A^{-1} \in GL(n,\mathbb{R})$ tal que $AA^{-1} = A^{-1}A = I_n$.

Por lo tanto $GL(n,\mathbb{R})$ es un grupo con el producto de matrices. □

Ejemplo 2.1.34.

Análogamente se define $GL(n,\mathbb{C})$ como el conjunto de matrices invertibles con entradas en $\mathbb{C}$.

$$GL(n,\mathbb{C}) := \{A \in M(n,\mathbb{C}) : \det(A) \neq 0\}. \tag{2.7}$$

El par $(GL(n,\mathbb{C}),\cdot)$ es un grupo llamado **Grupo General Lineal (complejo)**.

Demostración. La prueba es análoga a la del ejemplo anterior. □

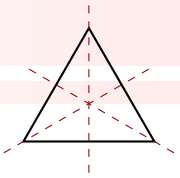
Ejemplo 2.1.35.

El conjunto de matrices $n \times n$ ortogonales definido por

$$O(n) := \{A \in M(n,\mathbb{R}) \ : \ A^tA = AA^t = I_n\}$$

es un grupo junto con la multiplicación usual de matrices. Este grupo es llamado **Grupo Ortogonal**.

Demostración.



1. *Cerradura*: sean A, B matrices en $O(n)$, se debe probar que $AB \in O(n)$. Como A y B están en $O(n)$, entonces $A^tA = I_n$ y $B^tB = I_n$. Recuerde que $(AB)^t = B^tA^t$. Con ello, note que

$$(AB)^t(AB) = B^t(A^tA)B = (B^tI_n)B = B^tB = I_n.$$

   Entonces AB está en $O(n)$.

2. *Asociatividad*: se hereda del grupo $GL(n, \mathbb{R})$.

3. *Elemento neutro*: es la matriz identidad I_n. Además, note que $I_n \in O(n)$ porque $I_n^tI_n = I_n$.

4. *Existencia de inversos*: por la definición de $O(n)$, se cumple que $A^{-1} = A^t$.

Por lo tanto $O(n)$ es un grupo con el producto de matrices. □

Ejemplo 2.1.36.

El conjunto de matrices $n \times n$ definido por

$$SO(n) := \{A \in O(n) \ : \ \det A = 1\},$$

es un grupo junto con la multiplicación usual de matrices. Este grupo es llamado **Grupo Ortogonal Especial**.

Demostración. La asociatividad y la existencia de elementos inversos se heredan del grupo $GL(n, \mathbb{R})$.

1. *Cerradura*: sean A, B matrices en $SO(n)$, se debe probar que $AB \in SO(n)$. Como A y B están en $SO(n)$, entonces $\det A = 1$ y $\det B = 1$. Entonces

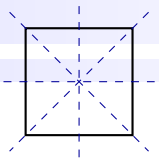
$$\det(AB) = \det(A)\det(B) = 1.$$

   Así, AB está en $SO(n)$.

2. *Elemento neutro*: es la matriz identidad I_n. De hecho, observe que $I_n \in SO(n)$ porque $\det I_n = 1$.

Por lo tanto $SO(n)$ es un grupo con el producto de matrices. □

Ejemplo 2.1.37.



Considere el conjunto definido por

$$G := \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{R} \right\}$$

Este conjunto con el producto usual de matrices, es un grupo. Este grupo se llama el **grupo de Heisenberg** de dimensión 3.

Demostración. Note que si $A \in G$, entonces $\det A = 1$, por lo tanto $A \in SO(n)$. Esto implica que las propiedad de cerradura, asociatividad, elemento neutro y existencia de elementos inversos las hereda de este grupo $SO(n)$. En particular, a continuación se prueba la cerradura: sean A y B matrices en G, entonces

$$A = \begin{pmatrix} 1 & a_1 & b_1 \\ 0 & 1 & c_1 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{y} \quad B = \begin{pmatrix} 1 & a_2 & b_2 \\ 0 & 1 & c_2 \\ 0 & 0 & 1 \end{pmatrix}.$$

Ahora, note que

$$AB = \begin{pmatrix} 1 & a_1 & b_1 \\ 0 & 1 & c_1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a_2 & b_2 \\ 0 & 1 & c_2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a_1 + a_2 & b_2 + a_1 c_2 + b_1 \\ 0 & 1 & c_1 + c_2 \\ 0 & 0 & 1 \end{pmatrix}.$$

Es claro que esta última matriz está en G. □

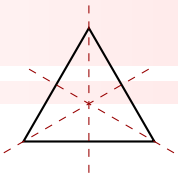
2.2 Teoremas y resultados importantes sobre grupos

En lo que sigue, si no hay ambigüedad, se omite la operación del grupo a la hora de operar elementos. Es decir, dado un grupo $(G, *)$ y elementos $a, b \in G$, se escribe ab en lugar de $a * b$. Además, siempre y cuando no se genere confusión, en vez de escribir el par $(G, *)$ es un grupo, solamente se escribe G es un grupo.

Teorema 2.2.1:

Si G es un grupo, entonces el elemento neutro es único.

Demostración. Suponga que existen dos elementos neutros e_1 y e_2 en G. Se debe probar que $e_1 = e_2$.



Ahora, como e_1 es elemento neutro, entonces

$$e_1 e_2 = e_2.$$

Similarmente, como e_2 es elemento neutro, entonces

$$e_1 e_2 = e_1.$$

De estas dos ecuaciones se obtiene que

$$e_2 = e_1 e_2 = e_1,$$

por lo tanto el elemento neutro es único. □

Teorema 2.2.2:

Sea G un grupo. Para cada elemento $a \in G$ existe un único elemento inverso en G.

Demostración. Sea a un elemento cualquiera de G. Como G es grupo, por definición existe un elemento inverso de a, por lo que solo falta probar que este inverso es único. Para ello, suponga que a_1 y a_2 son dos inversos de a. Se va a probar que necesariamente $a_1 = a_2$. Con este fin, y como a_1 y a_2 son inversos de a, se cumple que

$$aa_1 = e \quad \text{y} \quad aa_2 = e,$$

donde e es el neutro en G. Entonces

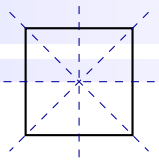
$$\begin{aligned} a_1 &= a_1 e \\ &= a_1(aa_2) \\ &= (a_1 a)a_2 \\ &= ea_2 \\ &= a_2. \end{aligned}$$

Por lo tanto, el inverso de a es único. □

Teorema 2.2.3:

Sea G un grupo. Para cada $a \in G$ se cumple que

$$\left(a^{-1}\right)^{-1} = a.$$



Demostración. Como G es un grupo, entonces cualquier elemento de G tiene un único inverso. Ahora, si $a \in G$ entonces, su inverso $a^{-1} \in G$. Pero, si $a^{-1} \in G$, también tiene un inverso denotado por $(a^{-1})^{-1} \in G$ tal que

$$(a^{-1})^{-1}a^{-1} = e = a^{-1}(a^{-1})^{-1}.$$

Además, es claro que se cumple

$$aa^{-1} = e = a^{-1}a,$$

lo cual también se puede interpretar que g es el inverso de a^{-1}. Es decir, a^{-1} posee dos elementos inversos, siendo estos a y $(a^{-1})^{-1}$. Sin embargo, por el teorema anterior se sabe que el inverso es único, por lo tanto

$$(a^{-1})^{-1} = a.$$

□

Teorema 2.2.4:

Sea G un grupo y sean a y b elementos cualquiera de G. Entonces

$$(ab)^{-1} = b^{-1}a^{-1}.$$

Demostración. Nótese que

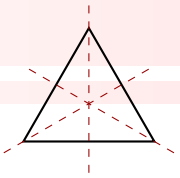
$$\begin{aligned}(ab)(b^{-1}a^{-1}) &= a(b(b^{-1}a^{-1}))\\ &= a((bb^{-1})a^{-1})\\ &= a(ea^{-1})\\ &= aa^{-1}\\ &= e.\end{aligned}$$

Similarmente se muestra que $(b^{-1}a^{-1})(ab) = e$. De esta forma se tiene que $b^{-1}a^{-1}$ es el inverso de ab, pero el inverso de ab es $(ab)^{-1}$ y como el inverso de ab es único, necesariamente $b^{-1}a^{-1} = (ab)^{-1}$. □

Definición 2.2.1:

Sea G un grupo. Sea $n \in \mathbb{N}$ y $a \in G$. Se define

1. $a^0 := e$, donde e es el elemento neutro en G.
2. $a^n := \underbrace{aaa \ldots a}_{n-veces}$.
3. $a^{-n} := \left(a^{-1}\right)^n$.



Ejemplo 2.2.1.

Considere el grupo $(U_8, \cdot)$, algunas potencias en U_8 son:

$$[3]^4 = [3] \cdot [3] \cdot [3] \cdot [3] = [1].$$

$$[5]^3 = [5] \cdot [5] \cdot [5] = [1].$$

$$[7]^{-3} = ([7]^{-1})^3 = [7]^3 = [7] \cdot [7] \cdot [7] = [1].$$

Ejemplo 2.2.2.

Considere el grupo $(S_3, \circ)$, algunas potencias en S_3 son:

$$\sigma_4^2 = \sigma_4 \circ \sigma_4 = \sigma_5.$$

$$\sigma_6^2 = \sigma_4 \circ \sigma_4 = \sigma_1.$$

$$\sigma_5^{-2} = (\sigma_5^{-1})^5 = \sigma_4^2 = \sigma_4 \circ \sigma_4 = \sigma_5.$$

Ejemplo 2.2.3. *2.1.4*

Considere el grupo del ejemplo 2.1.4, el cual se define sobre $\mathbb{R} - \{x, y : xy = 1\}$ con la operación $x * y = \dfrac{x+y}{1-xy}$.

$$4^2 = 4 * 4 = -\frac{8}{15}.$$

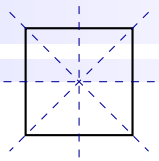
$$2^3 = 2 * 2 * 2 = \frac{2}{11}.$$

$$3^{-2} = (3^{-1})^2 = (-3)^2 = -3 * -3 = \frac{3}{4}.$$

Observación 2.2.1.

En el caso de grupos aditivos $(G, +)$, las condiciones de la definición 2.2.1 se escriben, respectivamente, como:

1. $0a := 0$ donde 0 es el elemento neutro en G.
2. $na := \underbrace{a + a + \ldots + a}_{n-veces}$.
3. $-na := n(-a)$.



Ejemplo 2.2.4.

Considere el grupo $(\mathbb{Z}_6, +)$, entonces:

$$5[4] = [4] + [4] + [4] + [4] + [4] = 5[4] = [2].$$

$$3[2] = [2] + [2] + [2] = [0].$$

Se deja como ejercicio para el lector desarrollar la expresión

$$-3[4]$$

Teorema 2.2.5:

Sea G un grupo y sea $a \in G$. Entonces:

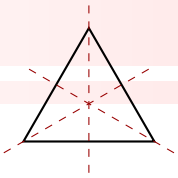
1. $a^n = a^{n-1}a$, para todo $n \in \mathbb{Z}$.
2. $a^{-n} = \left(a^n\right)^{-1}$, para todo $n \in \mathbb{Z}$.
3. $a^m a^n = a^{m+n}$, para todos $m, n \in \mathbb{Z}$.
4. $\left(a^n\right)^m = a^{nm}$, para todos $m, n \in \mathbb{Z}$.

Demostración.

1. Note que $a^n = \underbrace{aaa\ldots a}_{n-veces}$ para todo $n \in \mathbb{N}$. Usando el mismo hecho se tiene que

$$a^{n-1}a = \underbrace{aaa\ldots a}_{(n-1)-veces}\, a = \underbrace{aaa\ldots a}_{n-veces}.$$

Entonces se concluye que $a^n = a^{n-1}a$ para todo $n \in \mathbb{N}$. Sin embargo, la demostración se debe realizar para todo $n \in \mathbb{Z}$. En este sentido, existen dos casos que faltan: si $n = 0$ y si n es un número negativo. Para el primer caso, por la parte uno de la definición 2.2.1 el resultado es inmediato. Para



el segundo caso, asuma que $n \in \mathbb{Z}^-$ y sea $n = -k$, $k \in \mathbb{N}$, entonces:

$$\begin{aligned}
a^n &= a^{-k} \\
&= (a^{-1})^k \quad \text{por la parte tres de la definición 2.2.1.} \\
&= (a^{-1})^k e \quad \text{donde} \quad e \quad \text{es el elemento neutro.} \\
&= (a^{-1})^k (a^{-1}a) \\
&= ((a^{-1})^k a^{-1})a \\
&= (a^{-1})^{k+1} a \quad \text{por la parte dos de la definición 2.2.1.} \\
&= (a^{-(k+1)})a \quad \text{por la parte tres de la definición 2.2.1.} \\
&= a^{-k-1}a \\
&= a^{n-1}a.
\end{aligned}$$

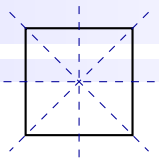
2. Primero se prueba que $a^{-n} = \left(a^n\right)^{-1}$ para todo $n \in \mathbb{N}$ mediante inducción sobre n. Para ello, note que si $n = 1$ entonces $a^{-1} = \left(a^1\right)^{-1}$, verificando que el teorema es verdadero para $n = 1$. Ahora, suponga que el teorema se cumple para n (*hipótesis de inducción*), es decir, suponga que se cumple

$$a^{-n} = \left(a^n\right)^{-1}.$$

Se debe probar que también se cumple para $n + 1$. En efecto, observe que:

$$\begin{aligned}
a^{-(n+1)} &= (a^{-1})^{n+1} \quad \text{por la parte tres de la definición 2.2.1.} \\
&= (a^{-1})^n a^{-1} \quad \text{por la parte dos de la definición 2.2.1.} \\
&= a^{-n}a^{-1} \quad \text{por la parte tres de la definición 2.2.1.} \\
&= (a^n)^{-1}a^{-1} \quad \text{por la hipótesis de inducción.} \\
&= (aa^n)^{-1} \quad \text{por el Teorema 2.2.4.} \\
&= (a^{1+n})^{-1} \\
&= (a^{n+1})^{-1},
\end{aligned}$$

por lo tanto $a^{-n} = \left(a^n\right)^{-1}$ para todo $n \in \mathbb{N}$. Falta verificar el resultado para todo $n \in \mathbb{Z}$. Entonces existen dos casos que faltan: si $n = 0$ y n es un número negativo. Para el primer caso, por la parte uno de la definición 2.2.1 el resultado es inmediato. Para el segundo caso, asuma que $n \in \mathbb{Z}^-$ y sea



$n = -k$, $k \in \mathbb{N}$, así:

$$\begin{aligned}
(a^n)^{-1} &= (a^{-k})^{-1} \\
&= ((a^{-1})^k)^{-1} \quad \text{por la parte 3 de la definición 2.2.1.} \\
&= (a^{-1})^{-k} \quad \text{porque} \quad a^{-n} = \left(a^n\right)^{-1}, n \in \mathbb{N}. \\
&= ((a^{-1})^{-1})^k \quad \text{por la parte 3 de la definición 2.2.1.} \\
&= a^k \quad \text{por el Teorema 2.2.3.} \\
&= a^{-n}.
\end{aligned}$$

Por lo tanto $a^{-n} = \left(a^n\right)^{-1}$ para todo $n \in \mathbb{Z}$.

3. Primero se va demostrar que $a^m a^n = a^{m+n}$, para todos $m, n \in \mathbb{N}$. Por la parte dos de la definición 2.2.1 se tiene que

$$a^m a^n = \underbrace{aaa\ldots a}_{m-veces}\underbrace{aaa\ldots a}_{n-veces} = \underbrace{aaa\ldots a}_{(m+n)-veces} = a^{m+n}.$$

Falta verificar el resultado para todo $m, n \in \mathbb{Z}$. A diferencia de las dos demostraciones anteriores, se están manipulando dos números m, n, lo genera más casos: el primer caso es $m = 0$ o $n = 0$, el segundo caso es $m, n \in \mathbb{Z}^-$, el tercer caso es $m \in \mathbb{Z}^+$ y $n \in \mathbb{Z}^-$ y el cuarto caso es $m \in \mathbb{Z}^-$ y $n \in \mathbb{Z}^+$.

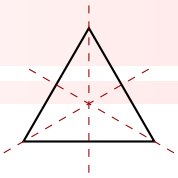
- Caso en que $m = 0$ o $n = 0$: si se supone que $m = 0$, entonces:

$$a^m a^n = a^0 a^n = ea^n = a^n = a^{0+n} = a^{m+n}.$$

  Si $n = 0$ se hace de forma idéntica.

- Caso en que $m, n \in \mathbb{Z}^-$: sean $m = -k_1$ y $n = -k_2$, donde k_1, k_2 están en $\mathbb{N}$, entonces:

$$\begin{aligned}
a^m a^n &= a^{-k_1} a^{-k_2} \\
&= (a^{-1})^{k_1} (a^{-1})^{k_2} \quad \text{por la parte tres de la definición 2.2.1.} \\
&= (a^{-1})^{k_1+k_2} \quad \text{puesto que } a^m a^n = a^{m+n} \text{ si } m, n \in \mathbb{N}. \\
&= a^{-(k_1+k_2)} \quad \text{por la parte tres de la definición 2.2.1.} \\
&= a^{-k_1-k_2)} \\
&= a^{m+n}.
\end{aligned}$$



- Caso en que $m \in \mathbb{Z}^+$ y $n \in \mathbb{Z}^-$: suponga que $n = -k$, con $k \in \mathbb{Z}^+$. Tanto m y k son números enteros positivos y puede suceder que $k \geq m$ o bien $k < m$. Ahora, si se supone que $k \geq m$ se tiene que:

$$\begin{aligned}
a^m a^n &= a^m a^{-k} \\
&= a^m (a^k)^{-1} \quad \text{por la parte dos de este teorema.} \\
&= a^m (a^{k-m+m})^{-1} \quad \text{siendo } k \geq m, \text{ entonces } k - m \geq 0. \\
&= a^m (a^{k-m} a^m)^{-1} \quad \text{siendo válido para } m \in \mathbb{Z}^+ \text{ y para } k - m \geq 0. \\
&= a^m (a^m)^{-1} (a^{k-m})^{-1} \quad \text{por el teorema 2.2.3.} \\
&= e(a^{k-m})^{-1} \quad \text{donde } e \text{ es el elemento neutro del grupo.} \\
&= a^{-(k-m)} \quad \text{por la parte tres de la definición 2.2.1.} \\
&= a^{m-k} \\
&= a^{m+n}.
\end{aligned}$$

En cambio, si se supone que $k < m$, entonces:

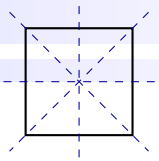
$$\begin{aligned}
a^m a^n &= a^{m-k+k} a^{-k} \\
&= a^{m-k} a^k a^{-k} \quad \text{siendo } k < m, \text{ entonces } m - k > 0. \\
&= a^{m-k} a^k (a^k)^{-1} \quad \text{por la parte dos de este teorema.} \\
&= a^{m-k} e \\
&= a^{m-k} \\
&= a^{m+n}.
\end{aligned}$$

- Caso en que $m \in \mathbb{Z}^-$ y $n \in \mathbb{Z}^+$: es análogo al anterior.

4. Primero se va probar que $\left(a^n\right)^m = a^{nm}$, para todos $m, n \in \mathbb{N}$. Para este fin, por la parte dos de la definición 2.2.1 se tiene que

$$\left(a^n\right)^m = \underbrace{a^n a^n a^n \ldots a^n}_{m-veces} = \underbrace{\underbrace{(aaa \ldots a)}_{n-veces}\underbrace{(aaa \ldots a)}_{n-veces} \ldots \underbrace{(aaa \ldots a)}_{n-veces}}_{m-veces} = a^{nm}.$$

Al igual que la parte anterior, falta verificar el resultado para todo $m, n \in \mathbb{Z}$, lo genera tres casos: el primer caso es $m = 0$ o $n = 0$, el segundo caso es $m, n \in \mathbb{Z}^-$, el tercer caso es $m \in \mathbb{Z}^+$ y $n \in \mathbb{Z}^-$



y el cuarto caso es $m \in \mathbb{Z}^-$ y $n \in \mathbb{Z}^+$.

- Caso en que $m = 0$ o $n = 0$: si $m = 0$, sea e el elemento neutro del grupo, entonces, por la parte uno de la definición 2.2.1 se tiene que:

$$(a^n)^m = (a^n)^0 = e = a^0 = a^{0n} = a^{mn}.$$

  De forma similar, si $n = 0$ entonces

$$(a^n)^m = (a^0)^m = e^m = \underbrace{eee \ldots e}_{m-veces} = e = a^0 = a^{m0} = a^{mn}.$$

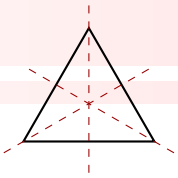
- Caso en que $m, n \in \mathbb{Z}^-$: sean $m = -k_1$ y $n = -k_2$, donde k_1, k_2 están en $\mathbb{N}$, entonces:

$$\begin{aligned}
(a^n)^m &= (a^{-k_2})^{-k_1} \\
&= ((a^{-k_2})^{-1})^{k_1} \quad \text{por la parte tres de la definición 2.2.1.} \\
&= (((a^{k_2})^{-1})^{-1})^{k_1} \quad \text{por la parte dos de este teorema.} \\
&= (a^{k_2})^{k_1} \quad \text{por el teorema 2.2.3.} \\
&= a^{k_2 k_1} \quad \text{porque } (a^n)^m = a^{nm} \text{ para } n, m \in \mathbb{N}. \\
&= a^{mn} \quad \text{porque } m = -k_1 \text{ y } n = -k_2. \\
&= a^{nm}.
\end{aligned}$$

- Caso en que $m \in \mathbb{Z}^+$ y $n \in \mathbb{Z}^-$: suponga que $n = -k$, con $k \in \mathbb{Z}^+$. Tanto m y k son números enteros positivos, entonces se tiene que:

$$\begin{aligned}
(a^n)^m &= (a^{-k})^m \\
&= ((a^{-1})^k)^m \quad \text{por la parte tres de la definición 2.2.1.} \\
&= (a^{-1})^{km} \quad \text{porque } (a^n)^m = a^{nm} \text{ para } n, m \in \mathbb{N}. \\
&= (a^{-(km)} \quad \text{por la parte tres de la definición 2.2.1.} \\
&= a^{-km} \\
&= a^{nm}.
\end{aligned}$$

- Caso en que $m \in \mathbb{Z}^-$ y $n \in \mathbb{Z}^+$: suponga que $m = -k$, con $k \in \mathbb{Z}^+$. Tanto n y k son números



enteros positivos, entonces se tiene que:

$$\begin{aligned}
(a^n)^m &= (a^n)^{-k} \\
&= ((a^n)^k)^{-1} \quad \text{por la parte dos de este teorema.} \\
&= (a^{nk})^{-1} \quad \text{porque } (a^n)^m = a^{nm} \text{ para } n, m \in \mathbb{N}. \\
&= a^{-(nk)} \quad \text{por la parte dos de este teorema.} \\
&= a^{n\cdot(-k)} \\
&= a^{nm}.
\end{aligned}$$

□

Ejemplo 2.2.5.

Sea G un grupo, muestre que $x^n = e$ si y sólo sí $(y^{-1}xy)^n = e$.

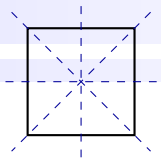
Demostración. Primero se prueba la sugerencia, para ello note que

$$\left(y^{-1}xy\right)^n = \underbrace{(y^{-1}xy)(y^{-1}xy)(y^{-1}xy)\dots(y^{-1}xy)}_{n-veces}.$$

De esta forma

$$\begin{aligned}
\left(y^{-1}xy\right)^n &= y^{-1}x(yy^{-1})x(yy^{-1})x(yy^{-1})\dots xy \\
&= y^{-1}(xe)(xe)\dots xy \\
&= y^{-1}\underbrace{xx\cdots x}_{n \text{ veces}}y \\
&= y^{-1}x^n y
\end{aligned}$$

Con esto claro, se procede con la demostración de lo solicitado.



1. ($\Rightarrow$) Suponga que $x^n = e$, se debe verificar que $(y^{-1}ey)^n = e$. Para ello, note que:

$$\begin{aligned}(y^{-1}ey)^n &= y^{-1}e^n y \quad \text{por la sugerencia.}\\ &= y^{-1}ey \quad \text{porque} \quad e^n = e.\\ &= y^{-1}(ey) \quad \text{por asociatividad.}\\ &= y^{-1}y\\ &= e.\end{aligned}$$

2. ($\Leftarrow$) Suponga que $\left(y^{-1}xy\right)^n = e$, se debe probar que $x^n = e$. Para ello, considere que

$$yy^{-1} = e = y^{-1}y.$$

Luego:

$$\begin{aligned}x^n &= ex^ne\\ &= yy^{-1}x^nyy^{-1}\\ &= y(y^{-1}x^ny)y^{-1} \quad \text{por asociatividad.}\\ &= y(y^{-1}xy)^ny^{-1} \quad \text{por la sugerencia.}\\ &= yey^{-1} \quad \text{porque } (y^{-1} * x * y)^n = e.\\ &= yy^{-1}\\ &= e.\end{aligned}$$

□

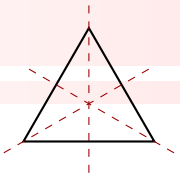
2.3 Ejercicios

R/ p.262

● Ejercicio 2.3.1 (Grupo)

Sobre $\mathbb{R}$, defina la operación $a * b = \pi ab$, para cualesquiera $a, b \in \mathbb{R}$, donde el producto de números reales es cerrado en $\mathbb{R}$.

Determine si $(\mathbb{R}, *)$ es un grupo.



Calcule

$$3^3 * \left[7 * \left(2 * \frac{1}{4}\right)^{-1}\right]^4.$$

● Ejercicio 2.3.2 (Grupo) R/ p.263

Pruebe que $A :=]0, 1]$ no es un grupo con la multiplicación de números reales.

● Ejercicio 2.3.3 (Grupo) R/ p.263

Considere $\mathbb{R}^* := \mathbb{R} - \{0\}$. En el conjunto $\mathbb{R} \times \mathbb{R}^*$ se define la operación

$$(a, b) \cdot (c, d) = (a + c - 4, 2bd)$$

Pruebe que $(\mathbb{R} \times \mathbb{R}^*, \cdot)$ es un grupo.

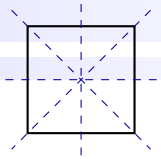
Calcule $(2, -1)^3 \cdot \left[\left(0, \frac{1}{3}\right) \cdot (1, -1)^{-1}\right]^2$.

● Ejercicio 2.3.4 (Grupo) R/ p.264

Sea $G :=]0, +\infty[- \{1\}$. Considere la operación $*$ definida por

$$x * y := x^{\ln y}, \quad \forall x, y \in G.$$

Determine si $(G, *)$ es un grupo.



R/ p.265 ● **Ejercicio 2.3.5 (Grupo)**

Dado un conjunto U, se denota por $P(U)$ al conjunto de partes de U. Muestre que $P(U)$ es un grupo con la operación de conjuntos definida por

$$A \vartriangle B = (A - B) \cup (B - A), \quad \forall A, B \in P(U).$$

R/ p.266 ● **Ejercicio 2.3.6 (Grupo)**

Sea $G := \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a^2 + b^2, \neq 0,\ a, b \in \mathbb{R} \right\}$. Muestre que $G\}$ es un grupo con la multiplicación usual de matrices.

R/ p.267 ● **Ejercicio 2.3.7 (Grupo)**

En el conjunto $\mathbb{Z} \times \mathbb{Z}$ se define la operación

$$(a, b) * (c, d) = (a + c, (-1)^c b + d).$$

Muestre que $(\mathbb{Z} \times \mathbb{Z}, *)$ es un grupo.

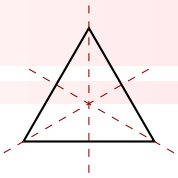
$$SL(n, \mathbb{R}) = \{A \in GL(n, \mathbb{R}) \mid \det(A) = 1\}$$

R/ p.268 ● **Ejercicio 2.3.8 (Grupo)**

Sea $A := \{a \in \mathbb{Z} : a \equiv 0 \pmod 3\}$. Pruebe que A es un grupo con la suma usual de números enteros.

R/ p.268 ● **Ejercicio 2.3.9 (Grupo)**

Sea $B := \{a \in \mathbb{Z} : a \equiv 1 \pmod 3\}$. Pruebe que B no es un grupo con la suma usual de números enteros.



● Ejercicio 2.3.10 (Grupo) R/ p.269

Muestre que el conjunto $Sym(n, \mathbb{R})$, de matrices simétricas, de tamaño $n \times n$ con entradas en $\mathbb{R}$, es un grupo con la suma usual de Matrices. ¿Es $Sym(n, \mathbb{R})$ un grupo con la multiplicación de matrices? (Recuerde que una matriz cuadrada A es simétrica si $A = A^t$).

● Ejercicio 2.3.11 (Grupo) R/ p.270

Sea $G := \{x \in \mathbb{R} : x \neq -1\}$. En G se define la operación $a * b = a + b + ab$, $\forall a, b \in G$.

Muestre que $(G, *)$ es un grupo.

Halle la solución de la ecuación $5 * x * 2 = 8$.

● Ejercicio 2.3.12 (Grupo) R/ p.272

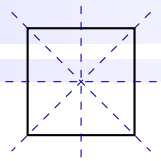
Sea G un grupo. Para cada $g \in G$, definimos la función $L_g : G \to G$ por

$$L_g(x) := gx, \qquad \forall x \in G.$$

Sea $\overline{G} = \{L_g : g \in G\}$. Demuestre que $\overline{G}$ es un grupo con la composición de funciones.

● Ejercicio 2.3.13 (Grupo) R/ p.273

Para cada $a, b \in \mathbb{R}$, $a \neq 0$, considere la función $T_{a,b} : \mathbb{R} \to \mathbb{R}$ definida por $T_{a,b}(x) = ax + b$. Sea $G := \{T_{a,b} : a, b \in \mathbb{R}, a \neq 0\}$. Muestre que G es un grupo con la composición de funciones.



R/ p.274

● **Ejercicio 2.3.14 (Grupo)**

Sean $(G_1, *)$ y $(G_2, \cdot)$ dos grupos cualesquiera. Sea $\varphi : G_1 \to G_2$ una función tal que

$$\varphi(g * h) = \varphi(g) \cdot \varphi(h) \qquad \forall g, h \in G_1$$

Denote por $\overline{e}$ al elemento neutro en G_2 y considere los conjuntos

$$K := \left\{ g \in G_1 : \varphi(g) = \overline{e} \right\}, \qquad R := \left\{ h \in G_2 : \varphi(g) = h, \text{ para algún } g \in G_1 \right\}$$

Demuestre que

$(K, *)$ es un grupo.

$(R, \cdot)$ es un grupo.

R/ p.277

● **Ejercicio 2.3.15 (Grupo)**

Sea $\mathcal{F}(\mathbb{R})$ el conjunto de todas las funciones de $\mathbb{R}$ en $\mathbb{R}$. Para $f, g \in \mathcal{F}(\mathbb{R})$, defina las operaciones $f + g$ y $f \cdot g$ por

$$(f + g)(x) := f(x) + g(x), \quad (f \cdot g)(x) := f(x)g(x), \quad x \in \mathbb{R}$$

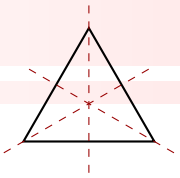
Muestre que $(\mathcal{F}(\mathbb{R}), +)$ es un grupo.

Muestre que $(\mathcal{F}(\mathbb{R}), \cdot)$ no es un grupo.

Sea $C^0(\mathbb{R}) = \{f \in \mathcal{F}(\mathbb{R}) : \ f \text{ es continua}\}$. Muestre que $(C^0(\mathbb{R}), +)$ es un grupo.

Sea $F^I(\mathbb{R}) = \{f \in \mathcal{F}(\mathbb{R}) : \ f(-x) = -f(x)\}$. Muestre que $(F^I(\mathbb{R}), +)$ es un grupo.

Sea $F^+(\mathbb{R}) = \{f \in \mathcal{F}(\mathbb{R}) : \ f(x) > 0, \forall x \in \mathbb{R}\}$. Muestre que $(F^+(\mathbb{R}), \cdot)$ es un grupo y que $(F^+(\mathbb{R}), +)$ no es grupo.



● Ejercicio 2.3.16 (Grupo) R/ p.281

(Grupo de cuaterniones) Defina los símbolos $\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}$ mediante

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

Usando multiplicación de matrices muestre que $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$, $\mathbf{ij} = -\mathbf{ji} = \mathbf{k}$, $\mathbf{jk} = -\mathbf{kj} = \mathbf{i}$ y $\mathbf{ki} = -\mathbf{ik} = \mathbf{j}$.

Muestre que el conjunto $Q_8 := \{-\mathbf{1}, -\mathbf{i}, -\mathbf{j}, -\mathbf{k}, \mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ es un grupo con la multiplicación de matrices (que satisface las propiedades del ítem anterior).

● Ejercicio 2.3.17 (Grupo) R/ p.282

Escriba las tablas de los grupos $(\mathbb{Z}_5, +)$, $(\mathbb{Z}_5{}^*, \cdot)$, $(U_5, \cdot)$ y $(\mathbb{Z}_6, +)$.

● Ejercicio 2.3.18 (Grupo) R/ p.283

Sea G un grupo. Muestre que si $x, y, z \in G$ satisfacen $xz = yz$, entonces $x = y$.

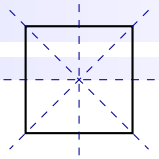
● Ejercicio 2.3.19 (Grupo) R/ p.284

Sea G un grupo. Si se cumple que $a^5 = e$, $b^4 = e$, $ab = ba^3$, muestre que $a^2b = ba$ y $ab^3 = b^3a^2$.

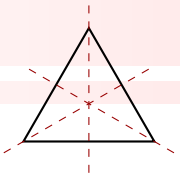
● Ejercicio 2.3.20 (Grupo) R/ p.285

Sea G e un grupo.

Muestre que $a \cdot b = c \cdot b$ si y solo si $a = c$.



Muestre que $b \cdot a = b \cdot c$ si y solo si $a = c$.



2.4 Grupos Abelianos

En el marco de la Teoría de Grupos, los grupos abelianos ocupan una posición de particular relevancia. Definidos por la propiedad conmutativa de su operación binaria, estos grupos ofrecen un terreno fértil para la exploración algebraica.

Niels Abel[3], a través de sus contribuciones a la teoría de ecuaciones algebraicas, desempeñó un papel fundamental en la conceptualización y comprensión de los grupos abelianos. El término "grupo abeliano"se popularizó más tarde en el siglo XIX, en honor a Abel.

Definición 2.4.1:

Un grupo G se llama **abeliano** si para cualesquiera $a, b \in G$ se tiene

$$ab = ba.$$

Es decir, G es abeliano si la operación definida sobre G es conmutativa.

Ejemplo 2.4.1.

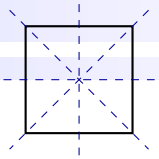
Los grupos $(\mathbb{R}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{R} - \{0\}, \cdot)$, $(\mathbb{Q} - \{0\}, \cdot)$, son abelianos.

Ejemplo 2.4.2.

En el ejemplo 2.1.4 se probó que el par $(G, *)$ tal que $x * y = \dfrac{x + y}{1 - xy}$ donde $G := \mathbb{R} - \{x, y : xy = 1\}$, es un grupo. Más aún, este par es un grupo abeliano.

Demostración. Para probar que es un grupo abeliano, falta mostrar que $x * y = y * x$. En efecto, usando

[3]Niels Henrik Abel, un destacado matemático noruego del siglo XIX, nació el 5 de agosto de 1802 en la ciudad de Finneidfjord, en Noruega. Aunque su vida fue corta, su impacto en las matemáticas fue extraordinario.
Abel mostró habilidades matemáticas excepcionales desde joven. A pesar de las dificultades económicas de su familia, continuó su educación en la Universidad de Oslo, donde comenzó a destacar en el ámbito matemático. A los 19 años, ya había resuelto una de las cuestiones más antiguas e importantes en la teoría de ecuaciones: demostrar la imposibilidad de resolver ecuaciones algebraicas generales de quinto grado mediante radicales.
A lo largo de su carrera, Abel trabajó en diversas áreas de las matemáticas, incluyendo ecuaciones diferenciales, teoría de números y funciones elípticas. Sus contribuciones fundamentales a la teoría de funciones elípticas le otorgaron un lugar destacado en la historia de las matemáticas. Abel también sufrió desafíos económicos y tuvo dificultades para obtener reconocimiento académico debido a la falta de apoyo institucional en Noruega en ese momento.
Trágicamente, la salud de Abel se vio afectada por las condiciones adversas y murió a la temprana edad de 26 años el 6 de abril de 1829. A pesar de su corta vida, sus contribuciones a las Matemáticas le valieron reconocimiento póstumo y su nombre quedó inmortalizado en la teoría de grupos abelianos, la función elíptica de Abel y otros conceptos matemáticos cruciales. Su legado perdura como un testimonio de su genio y dedicación a la disciplina matemática. Consultar HistoriaUniversal (2024)



el hecho que la suma y producto usual de números reales son conmutativos, note que:

$$x * y = \frac{x+y}{1-xy} = \frac{y+x}{1-yx} = y * x.$$

□

Ejemplo 2.4.3.

En el ejemplo 2.1.6 se probó que el conjunto de los números complejos $\mathbb{C}$ con la operación suma definida por

$$(a+bi)+(c+di) = (a+c)+(b+d)i,$$

es un grupo. Se va probar que $(\mathbb{C}, +)$ es un grupo abeliano.

Demostración. Sean $z_1 := a+bi$ y $z_2 := c+di$. Entonces, usando la conmutatividad de la suma en $\mathbb{R}$ se tiene que

$$\begin{aligned} z_1 + z_2 &= (a+bi)+(c+di) \\ &= (a+c)+(b+d)i \\ &= (c+a)+(d+b)i \\ &= c+di+a+bi \\ &= z_2 + z_1 \end{aligned}$$

por lo tanto, $(\mathbb{C}, +)$ es un grupo abeliano. □

Ejemplo 2.4.4.

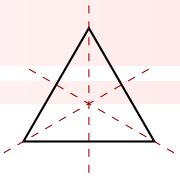
En el ejemplo 2.1.8 se probó que $(\mathbb{R}-\{0\})\times\mathbb{R}$ con la operación

$$(a,b) * (c,d) = (2ac, b+d+4).$$

para cualesquiera $(a,b),(c,d) \in (\mathbb{R}-\{0\})\times\mathbb{R}$ es un grupo. Sin embargo, también tiene la propiedad de ser un grupo abeliano.

Demostración. Usando el hecho que la suma y producto usual en $\mathbb{R}$ son conmutativos, observe que:

$$\begin{aligned} (a,b) * (c,d) &= (2ac, b+d+4) \\ &= (2ca, d+b+4) \\ &= (c,d) * (a,b) \end{aligned}$$



con lo cual se concluye que $(\mathbb{R} - \{0\} \times \mathbb{R})$ es un grupo abeliano. □

Ejemplo 2.4.5.

En el ejemplo 2.1.9 se definió el conjunto $\mathbb{S}^1 := \{(x, y) \in \mathbb{R}^2 \ : \ x^2 + y^2 = 1\}$ Sobre $\mathbb{S}^1$ se define la operación

$$(x_1, y_1) * (x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + y_1x_2)$$

Entonces $(\mathbb{S}^1, *)$ es un grupo abeliano.

Demostración. Ya se había probado que en efecto es un grupo, falta mostrar que la operación $*$ es conmutativa. Para ello, observe que:

$$\begin{aligned}(x_1, y_1) * (x_2, y_2) &= (x_1x_2 - y_1y_2, x_1y_2 + y_1x_2)\\ &= (x_2x_1 - y_2y_1, y_2x_1 + x_2y_1)\\ &= (x_2x_1 - y_2y_1, x_2y_1 + y_2x_1)\\ &= (x_2, y_2) * (x_1, y_1).\end{aligned}$$

□

Ejemplo 2.4.6.

No es difícil verificar que el grupo de Klein, estudiado en el ejemplo 2.1.16, es un grupo abeliano.

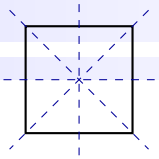
Demostración. Las operaciones de los elementos del grupo de Klein, denotado por $(V, \circ)$, se resumen en al siguiente tabla:

$\circ$	e	h	r	v
e	e	h	r	v
h	h	e	v	r
r	r	v	e	h
v	v	r	h	e

A partir de esta tabla, observe que todos los elementos de V conmutan entre ellos mediante la operación $\circ$. Por ejemplo, en particular, $h \circ r = v = r \circ h$. Así se comprueba con el resto de elementos y se concluye que $(V, \circ)$ es un grupo abeliano. □

Ejemplo 2.4.7.

El grupo $(\mathbb{Z}_n, +)$ del Teorema 2.1.1, es un grupo abeliano.



Demostración. Sean $[x], [y] \in \mathbb{Z}_n$. Entonces

$$\begin{aligned} [x]+[y] &= [x+y] \quad \text{por la definición de suma de clases.} \\ &= [y+x] \quad \text{por la conmutatividad de la suma en } \mathbb{Z}. \\ &= [y]+[x] \quad \text{nuevamente, por la definición de suma de clases.} \end{aligned}$$

De esta manera $(\mathbb{Z}_n, +)$ es un grupo abeliano. □

Ejemplo 2.4.8.

El grupo $\left(\mathbb{Z}_p^*, \cdot\right)$ del Teorema 2.1.2 es un grupo abeliano.

Demostración. Sean $[x], [y] \in \mathbb{Z}_p^*$. Entonces,

$$\begin{aligned} [x][y] &= [xy] \quad \text{por la definición de producto de clases.} \\ &= [yx] \quad \text{por la conmutatividad del producto en } \mathbb{Z}. \\ &= [y][x] \quad \text{nuevamente, por la definición de producto de clases.} \end{aligned}$$

Por lo tanto $\left(\mathbb{Z}_p{}^*, \cdot\right)$ es un grupo abeliano. □

Ejemplo 2.4.9.

EL grupo $(U_n, \cdot)$ estudiando en el Teorema 2.1.4, es un grupo abeliano.

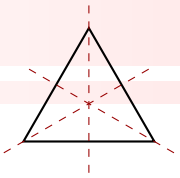
Demostración. La demostración se basa en la conmutatividad de la multiplicación de clases de la definición 1.2.3 y es análoga a la del ejemplo anterior. □

Ejemplo 2.4.10.

El grupo $(S_3, \circ)$ del ejemplo 2.1.30 es un grupo **no** abeliano.

Demostración. Todas las combinaciones de los elementos de S_3 con la operación $\circ$ están en la tabla siguiente:

$\circ$	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_1	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_2	σ_2	σ_1	σ_4	σ_3	σ_6	σ_5
σ_3	σ_3	σ_5	σ_1	σ_6	σ_2	σ_4
σ_4	σ_4	σ_6	σ_2	σ_5	σ_1	σ_3
σ_5	σ_5	σ_3	σ_6	σ_1	σ_4	σ_2
σ_6	σ_6	σ_4	σ_5	σ_2	σ_3	σ_1



En particular, note que $\sigma_4 \circ \sigma_6 = \sigma_3$ y que $\sigma_6 \circ \sigma_4 = \sigma_2$, es decir, $\sigma_4 \circ \sigma_6 = \sigma_3 \neq \sigma_6 \circ \sigma_4 = \sigma_2$. Con esto basta para verificar que $(S_3, \circ)$ es un grupo **no** abeliano. □

Ejemplo 2.4.11.

El grupo general lineal $GL(n, \mathbb{R})$ del ejemplo 2.1.33, definido por

$$GL(n, \mathbb{R}) := \{A \in M(n, \mathbb{R}) : \det A \neq 0\} \tag{2.8}$$

con la multiplicación de matrices, es un grupo no abeliano.

Demostración. Es suficiente observar que el producto de matrices en $GL(n, \mathbb{R})$ no es conmutativo. En particular, considere $n = 3$ y las matrices

$$A = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{y} \quad B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

Observe que A y B están $GL(3, \mathbb{R})$ porque ambas matrices tienen el determinante diferente de cero. Además, note que

$$AB = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Ahora se calcula $B \cdot A$:

$$BA = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

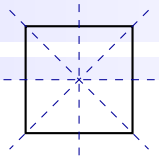
Por lo tanto $AB \neq BA$, lo que indica que el producto no es conmutativo y así $GL(n, \mathbb{R})$ es un grupo no abeliano. □

Ejemplo 2.4.12.

El conjunto de matrices ortogonales del ejemplo 2.1.35, definido por

$$O(n) = \{A \in GL(n, \mathbb{R}) \ : \ A^t A = I_n\}$$

junto con la multiplicación usual de matrices, es un grupo no abeliano.



Demostración. De manera similar al ejemplo anterior, es suficiente observar que el producto de matrices en $O(n, \mathbb{R})$ no es conmutativo. □

Ejemplo 2.4.13.

Sea G un grupo, muestre que si todo elemento de G es su propio inverso, entonces G es un grupo abeliano.

Demostración. Suponga que a es un elemento de G, entonces $aa = e$ por hipótesis, donde e es el elemento neutro. Se debe probar que $ab = ba$ para cada $a, b \in G$. En efecto, note que:

$$\begin{aligned} ab &= eabe \\ &= bb(ab)aa \quad \text{por hipótesis.} \\ &= b(ba)(ba)a \quad \text{por asociatividad.} \\ &= bea \quad \text{por hipótesis se tiene que} \quad (ba)(ba) = e. \\ &= ba. \end{aligned}$$

□

Teorema 2.4.1:

Un grupo G es abeliano si y sólo sí para cualesquiera $a, b \in G$ se tiene

$$(ab)^{-1} = a^{-1}b^{-1}.$$

Demostración.
($\Rightarrow$) Suponga que G es abeliano. Por el teorema 2.2.4 se tiene que

$$(ab)^{-1} = b^{-1}a^{-1}$$

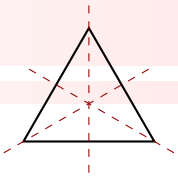
y por hipótesis

$$b^{-1}a^{-1} = a^{-1}b^{-1}.$$

Por lo que $(ab)^{-1} = a^{-1}b^{-1}$, siendo esto lo que se quería probar.

($\Leftarrow$) Suponga ahora que para cualesquiera $a, b \in G$ se cumple la igualdad

$$(ab)^{-1} = a^{-1}b^{-1}.$$



Se debe probar que G es abeliano, es decir, probar que $ab = ba$ para cualesquiera $a, b \in G$. Con este fin, sean $a, b \in G$, entonces, por hipótesis se cumple que

$$(ab)^{-1} = a^{-1}b^{-1}.$$

Se toman inversos a ambos lados, esto es

$$((ab)^{-1})^{-1} = (a^{-1}b^{-1})^{-1},$$

Aplicando los teoremas 2.2.3 y 2.2.4 se obtiene que

$$ab = (b^{-1})^{-1}(a^{-1})^{-1}.$$

De nuevo aplicando el teorema 2.2.3 se tiene que

$$ab = ba.$$

Por lo tanto G es un grupo abeliano. □

2.5 Orden de un grupo.

En la Teoría de Grupos, el concepto de orden de un grupo se erige como una medida fundamental que caracteriza la magnitud de su estructura algebraica. De manera objetiva, el orden de un grupo se define como la cantidad de elementos únicos en dicho grupo, revelando así la complejidad y extensión de sus simetrías y transformaciones.

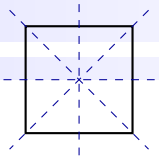
Definición 2.5.1: Orden de un grupo.

Se dice que un grupo G es **finito** si G tiene un número finito de elementos. A este número se le llama el **orden** de G y se denota $|G|$. En otro caso se dice que G tiene **orden infinito** y se escribe $|G| = \infty$.

Ejemplo 2.5.1.

Considere el ejemplo 2.1.11, donde el conjunto $G := \{1, -1, -i, i\}$ con la multiplicación de los números complejos es un grupo. Más aún, note que $(G, \cdot)$ es un grupo finito de orden $|G| = 4$.

Ejemplo 2.5.2.



No es difícil comprobar que el conjunto $G := \{-1, 1\}$, con la multiplicación de números reales, es un grupo finito de orden $|G| = 2$. La tabla de este grupo se muestra a continuación:

$\cdot$	1	-1
1	1	-1
-1	-1	1

Ejemplo 2.5.3.

El grupo de Klein $(V, \circ)$ del ejemplo 2.1.16 es un grupo finito de orden $|K| = 4$.

Ejemplo 2.5.4.

El grupo $(\mathbb{Z}_n, +)$ del teorema 2.1.1 es un grupo finito de orden $|\mathbb{Z}_n| = n$.

Ejemplo 2.5.5.

El grupo $(\mathbb{Z}_p^*, \cdot)$ estudiando en el teorema 2.1.2 es un grupo finito de orden $|\mathbb{Z}_p^*| = p - 1$.

Ejemplo 2.5.6.

El grupo simétrico $(S_n, \circ)$ estudiado en el teorema 2.1.5, es un grupo finito de orden $|S_n| = n!$. De hecho, en el ejemplo 2.1.30 se particularizó para S_3 y en efecto hay $3! = 6$ elementos.

Ejemplo 2.5.7.

Los grupo $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R} - \{0\}, \cdot)$, $(\mathbb{Q} - \{0\}, \cdot)$, vistos en los ejemplos 2.1.1 y 2.1.2, son grupos de orden infinito o simplemente grupos infinitos. .

Ejemplo 2.5.8.

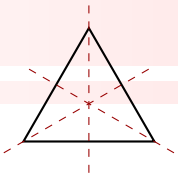
El grupo general lineal real $(GL(n, \mathbb{R}), \cdot)$ estudiado en el ejemplo 2.1.33, es un grupo infinito.

Teorema 2.5.1:

Sea G un grupo finito y sea $a \in G$.Para cada elemento a de G existe un $n \in \mathbb{N}$ tal que $a^n = e$, donde e es el elemento identidad del grupo G.

Demostración. Se puede abordar la demostración en dos casos, esto es:

1. Si $a = e$ se tiene el resultado



2. Si $a \neq e$, entonces se puede afirmar que

$$a, a^2, a^3, a^4 \ldots$$

son elementos de G, es decir, $a^n \in G$ para cualquier $n \in \mathbb{Z}^+$. Por otro lado, dado que G es finito, existen enteros positivos r, s con $r > s > 0$, tales que $a^r = a^s$. Esto se debe a que si hay más potencias que elementos distintos en G, algunas de estas potencias deben ser iguales[4]. Entonces

$$a^r = a^s$$

operando por $(a^s)^{-1}$ a ambos lados se tiene

$$\begin{aligned} & a^r(a^s)^{-1} = a^s(a^s)^{-1} \\ \Rightarrow \quad & a^r a^{-s} = e \\ \Rightarrow \quad & a^{r-s} = e. \end{aligned}$$

Ahora, como $r > s > 0$ se puede tomar $n = r - s \in \mathbb{N}$ y así $a^n = e$.

□

2.6 Orden de un elemento.

La noción de orden de un elemento constituye un concepto esencial que arroja luz sobre las propiedades algebraicas de los grupos. De manera objetiva, el orden de un elemento en un grupo refleja la cantidad mínima de veces que debe operarse ese elemento consigo mismo para obtener el elemento neutro del grupo.

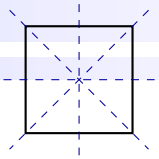
Definición 2.6.1: Orden de un elemento.

Sea $(G, \cdot)$ un grupo con elemento neutro e y sea $a \in G$.

1. Se dice que a es de **orden finito** si existe $m \in \mathbb{N}$ tal que $a^m = e$.

2. Si a es de orden finito, el *número natural más pequeño* n tal que $a^n = e$ se llama **orden** de a

[4]Esto también se puede explicar mediante el principio del palomar, que es un concepto en combinatoria y teoría de conjuntos. Este principio establece una propiedad básica relacionada con la distribución de elementos en conjuntos. La formulación típica es la siguiente: si n objetos se distribuyen en m contenedores y $n > m$, entonces al menos uno de los contenedores debe contener más de un objeto. La analogía aquí es pensar en los "objetos"como "palomas" y los "contenedores" como "cajones". Si tienes más palomas que cajones, entonces al menos un cajón debe contener más de una paloma. Esto es una consecuencia directa del hecho de que no puedes distribuir más elementos en contenedores que la cantidad total de contenedores que se tiene.



y se denota $|a| = n$. Con esta notación se tiene $a^{|a|} = e$. También se usa la notación $o(a) = n$.

3. Si no existe $m \in \mathbb{N}$ tal que $a^m = e$, se dice que a es de **orden infinito**.

Observación 2.6.1.

En el caso del elemento neutro e, se tiene que $e^1 = e$, por lo que $|e| = 1$.

Observación 2.6.2.

Si se utiliza la notación de grupos aditivos $(G, +)$, la definición anterior se escribe de la siguiente manera: sea $(G, +)$ un grupo con elemento neutro 0 y sea $a \in G$.

1. Se dice que a es de **orden finito** si existe $m \in \mathbb{N}$ tal que $ma = 0$.
2. Si a es de orden finito, el *número natural más pequeño* n tal que $na = 0$ se llama **orden** de a y se denota $|a| = n$. Con esta notación se tiene $|a|a = 0$.
3. Si no existe $m \in \mathbb{N}$ tal que $ma = 0$, se dice que a es de **orden infinito**.

Bajo esta premisa, en el caso del elemento neutro 0, se tiene que $1 \cdot 0 = 0$, por lo que $|0| = 1$.

Ejemplo 2.6.1.

Considere el grupo de Klein $(V, \circ)$, y su tabla

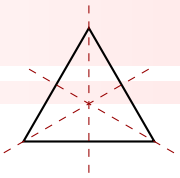
$\circ$	e	h	r	v
e	e	h	r	v
h	h	e	v	r
r	r	v	e	h
v	v	r	h	e

Note que $h^2 = h \circ h = e$, entonces el orden de h es $|h| = 2$. De forma análoga se concluye que $|r| = 2$ y $|v| = 2$.

Ejemplo 2.6.2.

De la definición 2.1.2 recuerde que $\mathbb{Z}_5^* := \{[1], [2], [3], [4]\}$. Se quiere determinar los órdenes de cada elemento del grupo $(\mathbb{Z}_5^*, \cdot)$, esto es:

- Como [1] es el elemento neutro en $\mathbb{Z}_5^*$, se tiene que el orden de [1] es $\left|[1]\right| = 1$.



- Para hallar el orden de [2], se debe *multiplicar* [2] por sí mismo hasta obtener el elemento neutro del grupo, en este caso, hasta obtener [1]. Así, multiplique [2] por sí mismo, usando la definición 2.2.1, aumentando la cantidad de veces, y recalcando que se usa "en módulo 5":

$$\begin{aligned}
[2]^1 &= [2] \\
[2]^2 &= [2][2] = [4] \\
[2]^3 &= [2][2][2] = [8] = [3] \\
[2]^4 &= [2][2][2][2] = [16] = [1] \\
[2]^5 &= [2][2][2][2][2] = [32] = [2] \\
[2]^6 &= [2][2][2][2][2][2] = [64] = [4] \\
[2]^7 &= [2][2][2][2][2][2][2] = [128] = [3] \\
[2]^8 &= [2][2][2][2][2][2][2][2] = [256] = [1]
\end{aligned}$$

  Si se continúa multiplicando de esta manera, se obtienen todas las clases en módulo 5. Además, observe que el menor número natural n tal que $[2]^n = 1$ es $n = 4$. Por lo tanto, el orden de [2] es $\left|[2]\right| = 4$.

- De forma similar, en el caso de $[3] \in \mathbb{Z}_5^*$, se cumple que:

$$\begin{aligned}
[3]^1 &= [3] \\
[3]^2 &= [3][3] = [9] = [4] \\
[3]^3 &= [3][3][3] = [27] = [2] \\
[3]^4 &= [3][3][3][3] = [81] = [1]
\end{aligned}$$

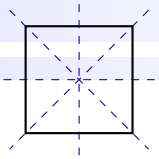
  Por lo que $\left|[3]\right| = 4$.

- En el caso de $[4] \in \mathbb{Z}_5^*$, se tiene que:

$$\begin{aligned}
[4]^1 &= [4] \\
[4]^2 &= [4][4] = [16] = [1]
\end{aligned}$$

  Entonces $\left|[4]\right| = 2$.

Ejemplo 2.6.3.



Se van a hallar los órdenes de cada elemento del grupo aditivo $(\mathbb{Z}_6, +)$, donde

$$\mathbb{Z}_6 := \{[0], [1], [2], [3], [4], [5]\}.$$

- Como $[0]$ es el elemento neutro en $\mathbb{Z}_6$, se tiene que el orden de $[0]$ es $\left|[0]\right| = 1$.

- Para hallar el orden de $[1]$, se debe *sumar* $[1]$ consigo mismo, usando la definición 2.2.1 y la observación 2.2.1, hasta obtener el elemento neutro del grupo, en este caso, hasta obtener $[0]$. Sume entonces $[0]$ por sí mismo, aumentando la cantidad de veces, recordando nuevamente que la suma es "en módulo 6":

$$\begin{aligned}
1[1] &= [1] \\
2[1] &= [1] + [1] = [2] \\
3[1] &= [1] + [1] + [1] = [3] \\
4[1] &= [1] + [1] + [1] + [1] = [4] \\
5[1] &= [1] + [1] + [1] + [1] + [1] = [5] \\
6[1] &= [1] + [1] + [1] + [1] + [1] + [1] = [6] = [0]
\end{aligned}$$

  Como $6[1] = [0]$, entonces $\left|[1]\right| = 6$.

- Se calcula ahora el orden de $[2]$:

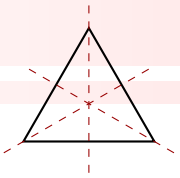
$$\begin{aligned}
1[2] &= [2] \\
2[2] &= [2] + [2] = [4] \\
3[2] &= [2] + [2] + [2] = [6] = [0]
\end{aligned}$$

  Como $3[2] = [0]$, entonces $\left|[2]\right| = 3$.

- Similarmente, en el caso de $[3]$:

$$\begin{aligned}
1[3] &= [3] \\
2[3] &= [3] + [3] = [6] = [0]
\end{aligned}$$

  Como $2[3] = [0]$, entonces $\left|[3]\right| = 2$.



- En el caso de $[4] \in \mathbb{Z}_6^*$, se tiene que:

$$\begin{aligned} [4] &= [4] \\ 2[4] &= [4]+[4] = [8] = [2] \\ 3[4] &= [4]+[4]+[4] = [12] = [0] \end{aligned}$$

  Como $3[4] = [0]$, entonces $\left|[4]\right| = \infty$.

- En el caso de $[5]$ se cumple que:

$$\begin{aligned} 1[5] &= [5] \\ 2[5] &= [5]+[5] = [10] = [4] \\ 3[5] &= [5]+[5]+[5] = [15] = [3] \\ 4[5] &= [5]+[5]+[5]+[5] = [20] = [2] \\ 5[5] &= [5]+[5]+[5]+[5]+[5] = [25] = [1] \\ 6[5] &= [5]+[5]+[5]+[5]+[5]+[5] = [30] = [0] \end{aligned}$$

  Como $6[5] = [0]$, entonces $\left|[5]\right| = 6$.

Teorema 2.6.1:

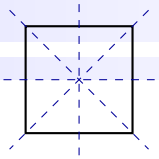
Sea G un grupo con elemento neutro e y sea $a \in G$ un elemento de orden finito $|a| = n$. Entonces:

1. $a^m = e$ si y sólo si $n \mid m$.
2. $a^m = a^k$ si y sólo si $m \equiv k \pmod{n}$
3. Si G es finito tal que $|G| = m$, entonces $n \leq m$.

Demostración. Las tres partes de este teorema se prueban a continuación:

1. ($\Rightarrow$) Suponga que a tiene orden finito $|a| = n$, así $a^n = e$. Se debe probar que $n \mid m$. Por el algoritmo de la división (teorema 1.1.3), existen $q, r \in \mathbb{Z}$ tales que

$$m = qn + r, \quad \text{con} \quad 0 \leq r < n.$$



Entonces

$$\begin{aligned} a^m &= a^{qn+r} \\ &= a^{qn}a^r \\ &= (a^n)^q a^r \\ &= e^q a^r \text{ pues } n \text{ es el orden de } a. \\ &= a^r. \end{aligned}$$

Así, $a^m = a^r$, pero por hipótesis $a^m = e$, lo cual implica que $a^r = e$. Sin embargo, por la definición 2.6.1, n es el menor número natural tal que $a^n = e$ y como $r < n$, se tiene que necesariamente $r = 0$. Por lo tanto,

$$m = qn,$$

es decir, n divide a m, lo cual había que probar.

($\Leftarrow$) Suponga que a tiene orden finito $|a| = n$ y que $n \mid m$. Se debe probar que $a^m = e$. Como n divide a m, entonces $m = nk$ para algún $k \in \mathbb{Z}$. Así, se cumple que:

$$a^m = a^{nk} = (a^n)^k = e^k = e. \tag{2.9}$$

2. ($\Rightarrow$) Suponga que a tiene orden finito $|a| = n$ y que $a^n = a^k$. se debe probar que $m \equiv k(\text{mod } n)$. Luego, como $a^n = a^k$, entonces multiplicando por el inverso $(a^k)^{-1} = a^{-k}$ de a^k (ver teorema 2.2.5), se tiene que

$$a^{m-k} = e.$$

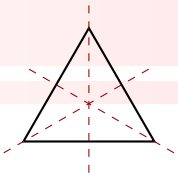
Ahora bien, por la parte uno de este teorema que se acaba de demostrar, la ecuación anterior implica que n divide a $m - k$, o equivalentemente por definición de congruencia modular

$$m \equiv k(\text{mod } n).$$

($\Leftarrow$) Suponga ahora que a tiene orden finito $|a| = n$ y que $m \equiv k(\text{mod } n)$. Se debe probar que $a^n = a^k$.

Por definición de congruencia modular,

$$m \equiv k(\text{mod } n) \text{ si y sólo si } n \mid m - k,$$



y esto sucede si y sólo si

$$m - k = nl \quad \text{para algún} \quad l \in \mathbb{Z}.$$

Entonces

$$a^{m-k} = a^{nl} = (a^n)^l = e^l = e,$$

lo anterior implica que

$$a^m a^{-k} = e,$$

equivalentemente a

$$a^m = a^k.$$

3. Suponga que a tiene orden finito $|a| = n$ y que G es finito tal que $|G| = m$. Se debe probar que $n \leq m$. Para ello considere el conjunto definido por

$$A := \{a, a^2, a^3, \ldots, a^{m+1}\}$$

Como $|G| = m$, entonces A no puede contener $m + 1$ elementos distintos, por lo que A tiene al menos dos elementos iguales. Es decir, existen $n_1, n_2 \in \mathbb{N}$ con $1 \leq n_1 < n_2 \leq m + 1$, tales que

$$a^{n_1} = a^{n_2},$$

equivalentemente

$$a^{n_2 - n_1} = e.$$

Ahora, como

$$1 \leq n_1 < n_2 \leq m + 1,$$

entonces

$$1 - n_1 \leq 0 < n_2 - n_1 \leq m + 1 - n_1 \leq m, \quad \text{pues} \quad 1 \leq n_1.$$

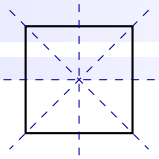
Dado que por hipótesis $|a| = n$ y además $a^{n_2 - n_1} = e$, entonces, por la parte uno de este teorema, n divide a $n_2 - n_1$. Esto, junto con las desigualdades anteriores, implica

$$n \leq n_2 - n_1 \leq m$$

es decir, $n \leq m$ o bien, $|a| \leq |G|$.

□

Ejemplo 2.6.4.



Sea G un grupo, mostrar que si a tiene orden finito, entonces $|a| = |a^{-1}|$, es decir, el orden de un elemento es el mismo orden de su inverso.

Demostración. Sea $a \in G$ tal que $|a| = n$ y $|a^{-1}| = m$. Se debe probar que $n = m$. Para ello, note que

$$(a^{-1})^n = a^{-n} = (a^n)^{-1} = e^{-1} = e.$$

Pero m el menor número natural tal que $(a^{-1})^m = e$, por lo tanto $m \leq n$. De forma similar

$$a^m = ((a^m)^{-1})^{-1} = ((a^{-1})^m)^{-1} = e^{-1} = e,$$

pero n es el menor número natural tal que $a^n = e$, entonces $n \leq m$. Finalmente, con estos resultados se concluye que $n = m$. □

2.7 Subgrupos

En el contexto de la Teoría de Grupos, la noción de subgrupo se presenta como un concepto fundamental que enriquece la comprensión sobre la estructura algebraica de un grupo. De manera objetiva, un subgrupo es un conjunto contenido dentro de otro grupo, cerrado bajo la misma operación del grupo y que, en sí mismo, forma un grupo con respecto a dicha operación.

Definición 2.7.1: Subgrupo

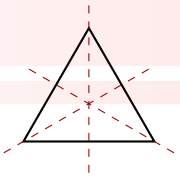
Sea un grupo $(G, \cdot)$ y sea H un subconjunto de G. Se dice que H es un **subgrupo** de G, si H con la misma operación "$\cdot$" de G, es un grupo. Si $(H, \cdot)$ es un subgrupo de $(G, \cdot)$, se escribe $H \leq G$.

Observación 2.7.1.

1. En lo que sigue, y siempre y cuando no exista ambiguedad alguna sobre la operación usada, en vez de escribir $(G, \cdot)$ se escribe solo G y en vez de escribir $(H, \cdot)$ se escribe solo H.
2. Si G es un grupo existe al menos dos subgrupos de G: G mismo y $\{e\}$. Estos son llamados **subgrupos triviales** de G.
3. Si $H \leq G$ con $H \neq G$ y $H \neq \{e\}$, entonces H se denomina subgrupo propio de G.

Ejemplo 2.7.1.

1. Bajo la suma usual de números reales se cumple que $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$. Se pueden considerar como subgrupos aditivos.



2. Bajo la multiplicación usual de números reales se tiene que $\mathbb{Q}^* \leq \mathbb{R}^* \leq \mathbb{C}^*$. Se pueden considerar como subgrupos multiplicativos.

Ejemplo 2.7.2.

No es difícil verificar con tablas que el grupo de klein posee tres subgrupos propios, estos son:

$$V_1 := \{e, h\}, V_2 := \{e, r\} \quad \text{y} \quad V_3 := \{e, v\}.$$

De hecho, respectivamente las tablas corresponden a:

$\circ$	e	h
e	e	h
h	h	e

$\circ$	e	r
e	e	r
r	r	e

$\circ$	e	v
e	e	v
v	v	e

Ejemplo 2.7.3.

Considere el conjunto $2\mathbb{Z} := \{2n : n \in \mathbb{Z}\}$ estudiado en el ejemplo 2.1.7. Como $2\mathbb{Z} \subset \mathbb{Z}$ y $2\mathbb{Z}$ es un grupo con la suma usual de enteros, entonces $2\mathbb{Z}$ es un subgrupo propio de $\mathbb{Z}$ con la suma. Es decir $2\mathbb{Z} < \mathbb{Z}$.

Ejemplo 2.7.4.

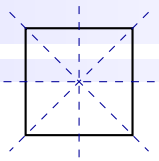
El conjunto $2\mathbb{Z}+1 := \{2n+1 : n \in \mathbb{Z}\}$ no es un subgrupo de $(\mathbb{Z}, +)$, ya que $(2\mathbb{Z}+1, +)$ no es un grupo, pues la suma $+$ no es una operación cerrada en $2\mathbb{Z}+1$ (ver ejemplo 2.1.13).

Ejemplo 2.7.5.

Considere el grupo $(\mathbb{Z}_6, +)$ cuya tabla es la siguiente

$+$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

El conjunto $H := \{[0], [2], [4]\}$ es un subgrupo de $(\mathbb{Z}_6, +)$, pues H está contenido en $\mathbb{Z}_6$ y es un grupo en sí mismo con la suma de clases en módulo 6. Para verificar esto, a continuación se presenta una tabla



para los elementos de H:

$+$	[0]	[2]	[4]
[0]	[0]	[2]	[4]
[2]	[2]	[4]	[0]
[4]	[4]	[0]	[2]

Observe que la tabla anterior muestra que $(H,+)$ es cerrado, la asociatividad se hereda de $(\mathbb{Z}_6,+)$, el elemento identidad corresponde a [0] y [2] y [4] son inversos de forma mutua. Por lo tanto H es un subgrupo propio de $\mathbb{Z}_6$ bajo la suma de clases en módulo 6.

Ejemplo 2.7.6.

Considere el grupo $(\mathbb{Z}_{13}^*,\cdot)$ y defina $H := \{[1],[5],[8],[12]\}$. Note que $H \subseteq \mathbb{Z}_{13}^*$ y además $(H,\cdot)$ es un grupo por sí mismo. Para ver esto, considere la tabla de H, recordando que es el producto en módulo 13.

$\cdot$	[1]	[5]	[8]	[12]
[1]	[1]	[5]	[8]	[12]
[5]	[5]	[12]	[1]	[8]
[8]	[8]	[1]	[12]	[5]
[12]	[12]	[8]	[5]	[1]

Note que la tabla anterior muestra que $(H,\cdot)$ es cerrado, la asociatividad se hereda de $(\mathbb{Z}_{13}^*,\cdot)$, el elemento identidad corresponde a [1] y [5] y [8] son inversos de forma mutua y [12] es inverso de sí mismo. Por lo tanto H es un subgrupo propio de $\mathbb{Z}_{13}^*$ bajo el producto de clases en módulo 13.

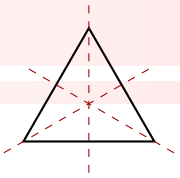
Ejemplo 2.7.7.

En el grupo $(S_3,\circ)$ estudiado en el ejemplo 2.1.30, todos los elementos, excepto σ_4,σ_5, son su propio inverso. De esta forma, no es difícil verificar que los subgrupos (triviales y propios) de este grupo son:

$$\{\sigma_1\},\ \{\sigma_1,\sigma_3\},\ \{\sigma_1,\sigma_6\},\ \{\sigma_1,\sigma_2\},\ \{\sigma_1,\sigma_4,\sigma_5\},\ S_3.$$

Ejemplo 2.7.8.

El grupo ortogonal $O(n)$ estudiado en el ejemplo 2.1.35 es un subgrupo de $GL(n,\mathbb{R})$ bajo el producto usual de matrices, pues $O(n) \subseteq GL(n,\mathbb{R})$ y además $O(n)$ es un grupo con la misma operación de $GL(n,\mathbb{R})$.



Teorema 2.7.1:

Sea $(G, \cdot)$ un grupo y sea $H \subseteq G$ un subconjunto no vacío de G. Entonces H es un subgrupo de G si y solo si para cualesquiera $x, y \in H$ se tiene $xy^{-1} \in H$.

Demostración. Se procede a probar para ambos sentidos:
($\Rightarrow$) Suponga que H es un subgrupo de G, se debe probar que si $x, y \in H$, entonces $xy^{-1} \in H$. Para tal efecto, como $y \in H$ y H es un grupo, existe $y^{-1} \in H$. Además, por ser H un grupo, H es cerrado con respecto a la operación definida, lo cual implica que $xy^{-1} \in H$.

($\Leftarrow$) Suponga ahora que para cualesquiera $x, y \in H$ se tiene $xy^{-1} \in H$. Se debe probar que H es un grupo. Para ello se verifican los axiomas de la definición 2.1.1, pero por conveniencia, se empieza probando la asociatividad:

1. *Asociatividad:* se hereda de G. Es decir, dados $x, y, z \in H$ entonces $x, y, z \in G$ pues $H \subseteq G$ y dado que la operación definida en G es asociativa, se cumple que

$$(xy)z = x(yz).$$

2. *Existencia del elemento neutro*: denote por e el elemento neutro de G. Se debe probar que e también está en H. Por hipótesis se tiene que $xy^{-1} \in H$ para cualesquiera $x, y \in H$ entonces, tomado $y = x$ se tiene $xx^{-1} \in H$, es decir, $e \in H$ puesto que $xx^{-1} = e$.

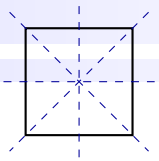
3. *Existencia de elementos inversos*: sea $x \in H$ y como $e \in H$ por el punto anterior, entonces $ex^{-1} \in H$ por hipótesis, pero $ex^{-1} = x^{-1}$, por lo tanto $x^{-1} \in H$.

4. *Cerradura:* sean $x, y \in H$, se debe probar que $xy \in H$. En el punto anterior se probó que para cada elemento de H, existe un inverso en H, entonces, si $y \in H$ también $y^{-1} \in H$, y esto, a su vez, implica que $(y^{-1})^{-1} \in H$. De esta forma, y por hipótesis, se debe cumplir que $x(y^{-1})^{-1} \in H$, pero $(y^{-1})^{-1} = y$, por lo que $xy \in H$.

Por lo tanto H es un subgrupo de G. □

Observación 2.7.2.

Sobre el teorema 2.7.1 anterior se resaltan los siguientes puntos:



1. Este teorema permite demostrar que un subconjunto H de un grupo G, es un subgrupo de G, sin la necesidad de probar que H cumple las cuatro condiciones de la definición de grupo. Esto se debe a que solo basta probar que $H \neq \emptyset$ y que dados dos elementos x, y de H, el producto xy^{-1} también está en H.

2. En algunos textos también suelen escribir que si H es un subconjunto de un grupo G, $H \neq \emptyset$, entonces $H \leq G$ si y solo si se cumple que:

   a) Si $x, y \in H$, entonces $xy \in H$.

   b) Si $x \in H$, entonces $x^{-1} \in H$.

   Es decir, solo basta con que la operación sea cerrada en H y que existan los elementos inversos en H. La demostración de esto es análoga a la demostración del teorema 2.7.1 y queda como ejercicio para el lector.

3. En notación de grupos aditivos $(G, +)$, el teorema anterior dice lo siguiente: Sea $(G, +)$ un grupo y sea $H \subseteq G$ un subconjunto no vacío de G. Entonces H es un subgrupo de G si y solo si para cualesquiera $x, y \in H$ se tiene $x + -y \in H$.

Ejemplo 2.7.9.

Se va utilizar el teorema 2.7.1 para probar que $2\mathbb{Z}$ es un subgrupo $\mathbb{Z}$ con la suma usual de enteros.

Demostración. Sean $x, y \in 2\mathbb{Z}$. Por la definición de $2\mathbb{Z}$, x, y son de la forma $x = 2n, y = 2m$, para algunos $m, n \in \mathbb{Z}$. En este caso el inverso de $y = 2m$ es $-y = -2m$. Entonces

$$x + -y = 2n + -2m = 2(n - m) \in 2\mathbb{Z}.$$

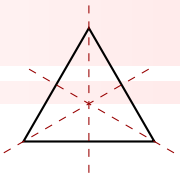
Luego, por el teorema 2.7.1, se concluye que $2\mathbb{Z} < \mathbb{Z}$. □

Ejemplo 2.7.10.

Se va probar que el subconjunto de $\mathbb{Z}$ definido por

$$m\mathbb{Z} := \{mk : k \in \mathbb{Z}\}$$

es un subgrupo de $(\mathbb{Z}, +)$.



Demostración. Utilizando el teorema 2.7.1, sean x, y elementos de $m\mathbb{Z}$, entonces $x = mk_1$ y $y = mk_2$, donde k_1, k_2 son números enteros. Luego, note que:

$$x + -y = mk_1 + -mk_2 = mk_1 - mk_2 = m(k_1 - k_2),$$

es decir, $x + -y$ posee la misma estructura de los elementos de $m\mathbb{Z}$, por lo tanto $x + -y \in m\mathbb{Z}$. Con ello $m\mathbb{Z} \leq \mathbb{Z}$. □

Observación 2.7.3.

El teorema 2.7.2 expuesto y demostrado más adelante establece que cualquier subgrupo de $(Z, +)$ debe tener la forma mZ.

Ejemplo 2.7.11.

Considere el grupo $(\mathbb{R}^2, +)$, donde $+$ es la suma usual en $\mathbb{R}^2$ definida por

$$(a, b) + (c, d) = (a + c, b + d),$$

para cualesquiera $(a, b), (c, d) \in \mathbb{R}^2$. Sea

$$H := \{(x, y) \in \mathbb{R}^2 \ : \ y = 2x \}.$$

Muestre que $H < \mathbb{R}^2$.

Demostración. Observe primero que $(x, y) \in H$ si y solo si $y = 2x$. Entonces, cada elemento de H es de la forma $(x, 2x)$ con $x \in \mathbb{R}$. Es decir,

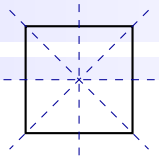
$$H := \{(x, 2x) \ : \ x \in \mathbb{R} \}.$$

Ahora, sean $(a, 2a), (b, 2b) \in H$, con $a, b \in \mathbb{R}$. El inverso (aditivo) de $(b, 2b)$ es $(-b, -2b)$. Entonces

$$\begin{aligned} (a, 2a) + (-b, -2b) &= (a + -b, 2a + -2b) \\ &= (a - b, 2(a - b)) \end{aligned}$$

De lo anterior se concluye que $(a, 2a)+(-b, -2b) \in H$. Por lo tanto $(H, +)$ es un subgrupo de $(\mathbb{R}^2, +)$. □

Ejemplo 2.7.12.



Considere el grupo $GL(n,\mathbb{R})$ bajo la multiplicación usual de matrices estudiado en el ejemplo 2.1.33, el cual es el conjunto de matrices invertibles de orden n con entradas en $\mathbb{R}$, definido por

$$GL(n,\mathbb{R}) := \{A \in M(n,\mathbb{R}) : \det A \neq 0\}$$

Defina el subconjunto de $GL(n,\mathbb{R})$ por

$$H(2,\mathbb{R}) := \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in \mathbb{R} \right\}.$$

Entonces $H(2,\mathbb{R}) < GL(n,\mathbb{R})$.

Demostración. Sean $A, B \in H(2,\mathbb{R})$ tales que

$$A = \begin{pmatrix} 1 & x_1 \\ 0 & 1 \end{pmatrix} \quad \text{y} \quad B = \begin{pmatrix} 1 & x_2 \\ 0 & 1 \end{pmatrix} \quad \text{con} \quad x_1, x_2 \in \mathbb{R}.$$

Se debe mostrar que $AB^{-1} \in H(2,\mathbb{R})$. En efecto, observe que $B^{-1} = \begin{pmatrix} 1 & -x_2 \\ 0 & 1 \end{pmatrix}$, entonces

$$AB^{-1} = \begin{pmatrix} 1 & x_1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -x_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x_1 - x_2 \\ 0 & 1 \end{pmatrix}.$$

Es claro que la matriz resultante posee la misma estructura que los elementos de $H(2,\mathbb{R})$, es decir, $AB^{-1} \in H(2,\mathbb{R})$. Con ello se concluye que $H(2,\mathbb{R}) \leq GL(n,\mathbb{R})$. □

Ejemplo 2.7.13.

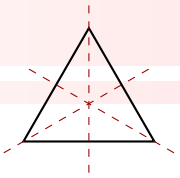
El grupo ortogonal especial $SO(n,\mathbb{R})$ analizado en el ejemplo 2.1.36 es un subgrupo de $GL(n,\mathbb{R})$.

Demostración. Sean A, B dos matrices en $SO(n,\mathbb{R})$. Entonces, por la definición de $SO(n,\mathbb{R})$ estas matrices cumplen que $\det A = 1$ y $\det B = 1$. Se debe probar que $AB^{-1} \in SO(n,\mathbb{R})$, es decir, probar que $\det(AB^{-1}) = 1$, esto es:

$$\det(AB^{-1}) = \det(A)\det(B^{-1}) = \det(A)\frac{1}{\det(B)} = 1.$$

Entonces $SO(n,\mathbb{R}) < GL(n,\mathbb{R})$. □

Ejemplo 2.7.14.



Sea G un grupo y sea a un elemento fijo de G. Considere el subconjunto de G dado por

$$H := \left\{ x \in G : xax^{-1} = a \right\}.$$

Entonces H es un subgrupo de G.

Demostración. Se utilizará el punto dos de la observación 2.7.2, es decir, se va demostrar la cerradura y la existencia de inversos.

1. Para la cerradura, considere dos elementos $x, y \in H$, entonces

   $$xax^{-1} = a \quad \text{y} \quad yay^{-1} = a,$$

   Se debe probar que $xy \in H$, es decir, probar que

   $$(xy)a(xy)^{-1} = a.$$

   Para este fin, note que

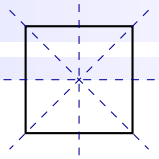
   $$\begin{aligned} (xy)a(xy)^{-1} &= (xy)a(y^{-1}x^{-1}) && \text{por el teorema 2.2.4.} \\ &= x(yay^{-1})x^{-1} && \text{por asociatividad y dados que } a, x, y \in G. \\ &= xax^{-1} && \text{por hipótesis.} \\ &= a && \text{por hipótesis.} \end{aligned}$$

2. Para la existencia de inversos, considere $x \in H$. Se debe probar que $x^{-1} \in H$, es decir, se debe probar que $x^{-1}a(x^{-1})^{-1} = a$, o lo que es equivalente, $x^{-1}ax = a$, esto por el teorema 2.2.3.

   Por hipótesis, si $x \in H$, entonces

   $$\begin{aligned} & xax^{-1} = a \\ \Rightarrow \quad & x^{-1}(xax^{-1})x = x^{-1}ax \\ \Rightarrow \quad & (x^{-1}x)a(x^{-1}x) = x^{-1}ax \\ \Rightarrow \quad & eae = x^{-1}ax \\ \Rightarrow \quad & a = x^{-1}ax \end{aligned}$$

   Así, $x^{-1}ax = a$, permitiendo concluir que $x^{-1} \in H$.



Finalmente se cumple que $H < G$. □

Ejemplo 2.7.15.

Defina $HK := \{hk : h \in H \text{ y } k \in K\}$. Sea G un grupo y sean $H < G$, $K < G$. Muestre que $HK < G$ si y solo si $KH = HK$.

Demostración.
($\Rightarrow$) Suponga que G es un grupo, $H < G$, $K < G$, $HK < G$, se debe probar que $KH = HK$. Para tal efecto, se probará que $KH \subseteq HK$ y que $KH \supseteq HK$.

- ($\subseteq$) Sea $x \in KH$, entonces existen un $k \in K$ y un $h \in H$ tales que $x = kh$. Con ello se tiene que:

$$\begin{aligned} & x = kh \\ \Rightarrow\ & x^{-1} = (kh)^{-1} \\ \Rightarrow\ & x^{-1} = h^{-1}k^{-1} \quad \text{por el teorema 2.2.4.} \end{aligned}$$

  Ahora, como H y K son subgrupos, entonces $h^{-1} \in H$ y $k^{-1} \in K$, más aún, $h^{-1}k^{-1} \in HK$, es decir, $x^{-1} \in HK$. Pero HK es un subgrupo, lo cual implica que $x \in HK$. Así, $KH \subseteq HK$.

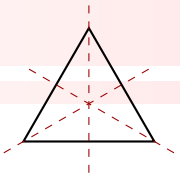
- ($\supseteq$) Sea $x \in HK$ y como HK es un subgrupo, entonces $x^{-1} \in HK$, es decir, existen un $h \in H$ y un $k \in K$ tales que $x^{-1} = hk$. Usando un proceso idéntico al pasado se concluye que $x = k^{-1}h^{-1}$, y como K y H son subgrupos, entonces $k^{-1} \in K$ y $h^{-1} \in H$, así $x \in KH$. Con ello $HK \subseteq KH$.

De esta forma $KH = HK$.

($\Leftarrow$) Sea G un grupo y sean $H < G$, $K < G$. Además se cumple que $KH = HK$, hay que mostrar que $HK < G$. Para tal efecto se usará el teorema 2.7.1, esto es, sean $x, y \in HK$, se debe probar que $xy^{-1} \in HK$. Ahora, si $x, y \in HK$, entonces existen $h_1, h_2 \in H$ y $k_1, k_2 \in K$ tales que $x = h_1k_1$ y $y = h_2k_2$. Con esto se tendría que

$$\begin{aligned} xy^{-1} &= h_1k_1(h_2k_2)^{-1} \\ &= h_1k_1k_2^{-1}h_2^{-1} \quad \text{por el teorema 2.2.4.} \end{aligned}$$

Puesto que K es subgrupo, entonces $k_1k_2^{-1} \in K$, por lo tanto $k_1k_2^{-1}h_2^{-1} \in KH = HK$ por hipótesis. Se podría establecer que existen un $h \in H$ y un $k \in K$ tales que $k_1k_2^{-1}h_2^{-1} = hk$. Con esto se tendría que $xy^{-1} = h_1hk$, sin embargo, como H es subgrupo, entonces $h_1h \in H$, así $xy^{-1} = h_1hk \in HK$, que era lo que se quería probar. Finalmente se concluye que $HK < G$. □



Teorema 2.7.2:

Todo subgrupo de $(\mathbb{Z}, +)$, tiene la forma

$$m\mathbb{Z} = \{mk : k \in \mathbb{Z}\}.$$

Demostración. En el ejemplo 2.7.10 se probó que $m\mathbb{Z}$ es un subgrupo aditivo de $\mathbb{Z}$. Lo que se debe demostrar es que si H es otro subgrupo aditivo de $\mathbb{Z}$, entonces $H = m\mathbb{Z}$. Para ello, si $H = \{0\}$, entonces tome $m = 0$ y así $\{0\} = m\mathbb{Z} = 0\mathbb{Z}$. De esta forma, suponga que $H \neq \{0\}$, entonces existe un elemento $x \in H$ con $x \neq 0$. Dado que H es un subgrupo de $\mathbb{Z}$, entonces $-x \in H$. De lo anterior se puede suponer, sin pérdida de generalidad, que $x > 0$, así H contiene enteros positivos y por el principio del buen orden, H tiene un menor elemento positivo. Sea $m \in H$ ese elemento. A partir de ahora se va a demostrar que $H = m\mathbb{Z}$, para lo cual se verificará que $m\mathbb{Z} \subseteq H$ y $m\mathbb{Z} \supseteq H$.

- ($\subseteq$). Como $m \in H$ y H es cerrado con la suma, se cumple que

  $$m, 2m, 3m, 4m, 5m, \ldots \in H.$$

  Por esta misma razón

  $$\ldots - 3m, -2m, -m, \in H,$$

  y como $-m, m \in H$ entonces, por la cerradura de H, se tiene que $0 = -m + m \in H$. Lo anterior significa que

  $$\{\ldots - 3m, -2m, -m, 0, m, 2m, 3m, 4m, 5m, \cdots\} \subseteq H,$$

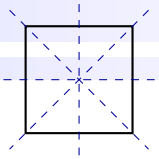
  es decir, $m\mathbb{Z} \subseteq H$.

- ($\supseteq$) Como m es el menor entero positivo en H, entonces $m \geq 1$. De aquí se tienen dos posibles situaciones: si $m = 1$, entonces $m\mathbb{Z} = \mathbb{Z}$ y así $H = \mathbb{Z} = 1\mathbb{Z}$. Si $m > 1$, sea $x \in H$ un elemento cualquiera de H. Aplicando el algoritmo de la división a x y m, existen enteros q y r tales que

  $$x = qm + r, \quad \text{con} \quad 0 \leq r < m$$

  Como $qm \in H$ entonces $-qm \in H$, por lo que $r = x - qm \in H$, es decir, $r \in H$, lo cual contradice que m sea el menor entero positivo que pertenece a H. Por lo tanto $r = 0$ y así $x = qm$, es decir que $x \in m\mathbb{Z}$. En resumen, si $x \in H$, entonces $x \in m\mathbb{Z}$, con lo cual $m\mathbb{Z} \supseteq H$.

Finalmente $H = m\mathbb{Z}$, que es lo que se quería probar. □



Teorema 2.7.3:

Sea G un grupo finito y $H \subseteq G$, $H \neq \emptyset$. Entonces $H < G$ si y solo si para cada $x, y \in H$ se cumple que $xy \in H$

Demostración. Se procede a probar las dos implicaciones del teorema:
($\Rightarrow$) Es trivial porque la operación definida H es cerrada por ser un subgrupo.

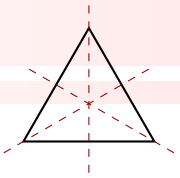
($\Leftarrow$) Suponga que si $x, y \in H$ se cumple que $xy \in H$. Por el punto dos de la observación 2.7.2 solo se debe probar la existencia de inversos. Para ello, suponga que $x \in H$, entonces, por la hipótesis $xx \in H$, es decir, $x^2 \in H$. Sin embargo, aplicando la mis analogía, se cumple que $x^2x \in H$, es decir, $x^3 \in H$. De esta forma, se podría concluir que $x^n \in H$ para $n \in \mathbb{N}$. Con esto presente, note que H debe ser finito por ser un subconjunto de un conjunto finito, entonces existen enteros positivos, r y s, $r > s$, tales que $x^r = a^s$, esto a su vez implica que $x^{r-s} = e$. Pero, como $r > s$, entonces $r - s > 0$, así $x^{r-s} = e$ debe ser un elemento de H, con lo cual $e \in H$, es decir, $x^0 \in H$. Por otro lado note que si $r - s > 0$, entonces $r - s - 1 \geq 0$, y como $x^0 \in H$, se puede concluir que también $x^{r-s-1} \in H$. Ahora, observe que

$$\begin{aligned} x^{r-s-1} &= x^{r-s}x^{-1} \\ &= ex^{-1} \\ &= x^{-1}. \end{aligned}$$

Por lo tanto, $x^{-1} \in H$ y se concluye que $H \leq G$. □

Observación 2.7.4.

El teorema anterior establece que si H es un subconjunto no vacío de un grupo finito, solo basta verificar que la operación sea cerrada en H para concluir que H es un subgrupo de G. Tome como referencia el ejemplo 2.7.2 de los subgrupos del grupo de Klein, el ejemplo 2.7.5 sobre un subgrupo de $(\mathbb{Z}_6.+)$, el ejemplo 2.7.6 sobre un subgrupo de $(\mathbb{Z}_{13}^*, \cdot)$ y el ejemplo 2.7.7 sobre los subgrupos de S_3.



2.8 Ejercicios

● Ejercicio 2.8.1 (Grupo Abeliano) R/ p.288

Muestre que el grupo de matrices $\big(M(m,n,\mathbb{R}),+\big)$ es un grupo Abeliano.

● Ejercicio 2.8.2 (Grupo Abeliano) R/ p.288

Determine si el grupo

$$G=\{y:\ \mathbb{R}\to\mathbb{R}\ :\ y(x)=ax+b,\ \ a,b\in\mathbb{R},\ a>0\},$$

con la operación composición de funciones, es un grupo Abeliano.

● Ejercicio 2.8.3 (Grupo Abeliano) R/ p.289

Considere el conjunto $(\mathbb{Q}^+,*)$, donde $*$ es la operación definida por

$$p*q=\frac{pq}{2}$$

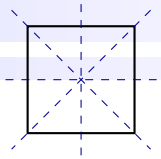
para cualesquiera $p,q\in\mathbb{Q}^+$. Muestre que $(\mathbb{Q}^+,*)$ es un grupo Abeliano.

● Ejercicio 2.8.4 (Grupo Abeliano) R/ p.290

Muestre que G es un grupo abeliano si y sólo si, para cualesquiera $a,b\in G$ se cumple $(ab)^2=a^2b^2$.

● Ejercicio 2.8.5 (Grupo Abeliano) R/ p.291

Muestre que si en un grupo G se cumple $x^2=e$, para todo elemento x de G, entonces el grupo es abeliano.



R/ p.291

● **Ejercicio 2.8.6 (Grupo Abeliano)**

Sea $(G, \cdot)$ un grupo tal que $|G| = 3$. Pruebe que G es un grupo abeliano. Como G es de orden 3 implica que $a^3 = e$ y $b^3 = e$. Ahora se puede usar una Tabla de Cayley para representar a G, esto es:

R/ p.292

● **Ejercicio 2.8.7 (Subgrupo)**

Sea S un subgrupo de un grupo.

Pruebe que si $h \in S$, entonces $hS = S = Sh$.

Pruebe que $x^{-1}y \in S$ si y solo si $xS = Sy$.

R/ p.294

● **Ejercicio 2.8.8 (Grupo y subgrupo)**

Considere el conjunto $\mathbb{Z}\times\mathbb{Z}$ con la operación $(a, b)+(c, d) = (a+c, b+d)$, para cualesquiera $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}$.

Muestre que $\mathbb{Z} \times \mathbb{Z}$ es un grupo con la suma con definida anteriormente.

Considere el conjunto $H := \{(m, n) : 2m-3n = 0\} \subset \mathbb{Z}\times\mathbb{Z}$. Muestre que es un subgrupo de $\mathbb{Z} \times \mathbb{Z}$.

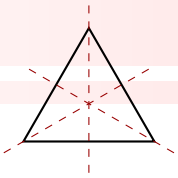
R/ p.296

● **Ejercicio 2.8.9 (Subgrupo)**

Sea $\mathbb{Q}^* = \mathbb{Q} - \{0\}$ y considere el grupo $(\mathbb{Q}^*, \cdot)$. Defina el conjunto

$$H := \left\{1, 2, \frac{1}{2}, 2^2, \frac{1}{2^2}, \ldots, 2^n, \frac{1}{2^n}, \ldots\right\}$$

Muestre que $H < \mathbb{Q}^*$.



● Ejercicio 2.8.10 (Subgrupo) R/ p.297

Considere el grupo de Klein $(V, \circ)$, donde $V := \{e, h, v, r\}$ y sea $H := \{e, r\}$. Muestre que $H < V$.

● Ejercicio 2.8.11 (Subgrupo) R/ p.298

Muestre que $SO(n, \mathbb{R})$ es subgrupo de $GL(n, \mathbb{R})$, con la multiplicación usual de matrices.

● Ejercicio 2.8.12 (Grupo y subgrupo) R/ p.299

Se denota $\mathbb{R}^* = \mathbb{R} - \{0\}$. Considere $(\mathbb{R}^* \times \mathbb{R}, *)$, donde

$$(a, b) * (c, d) := (4ac, b + d + 3)$$

Pruebe que $(\mathbb{R}^* \times \mathbb{R}, *)$ es un grupo.

Sea $H = \{(x, -3) : x \in \mathbb{R}^*\}$. Verifique que $H < \mathbb{R}^* \times \mathbb{R}$.

● Ejercicio 2.8.13 (Subgrupo) R/ p.302

Sea $(G, \cdot)$ un grupo Abeliano con elemento neutro e y sea n un entero positivo. Considere el subconjunto de G,

$$H := \{x \in G : x^n = e\}.$$

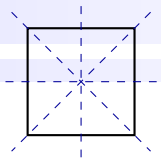
Muestre que $H < G$.

● Ejercicio 2.8.14 (Subgrupo) R/ p.304

Sea $(G, \cdot)$ un grupo y sean $H_1, H_2, \ldots, H_n$ subgrupos de G. Demuestre que

$$H := \bigcap_{i=1}^{n} H_i$$

es subgrupo de G.



R/ p.305 ● **Ejercicio 2.8.15 (Subgrupo)**

Sea $H_1 \subset H_2 \subset H_3 \subset \cdots$ una sucesión de subgrupos de un grupo G. Muestre que

$$H := \bigcup_{n\in\mathbb{N}} H_n$$

es un subgrupo de G.

R/ p.305 ● **Ejercicio 2.8.16 (Subgrupo)**

Sea $(G,\cdot)$ un grupo. Pruebe que si $K < H$ y $H < G$, entonces $K < G$.

R/ p.306 ● **Ejercicio 2.8.17 (Subgrupo)**

Sea $(G,\cdot)$ un grupo y sean H y K subgrupos de G. Muestre que $H \cup K < G$ sí y solo si $H \subset K$ ó $K \subset H$.

R/ p.307 ● **Ejercicio 2.8.18 (Subgrupo)**

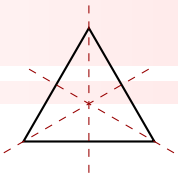
Se define

$$HK := \{hk \ : \ h \in H,\ k \in K\}$$

Sea $(G,\cdot)$ un grupo abeliano, demuestre que si $H < G$ y $K < G$ entonces $HK < G$.

R/ p.308 ● **Ejercicio 2.8.19 (Subgrupo)**

Sea $(G,\cdot)$ un grupo y $H < G$, $K < G$. Muestre que $HK < G$ si y sólo si $HK = KH$.



● Ejercicio 2.8.20 (Centralizador y Subgrupo) R/ p.311

Sea $(G, \cdot)$ un grupo. Se define el **centro** $Z(G)$ de G por

$$Z(G) := \{g \in G \ : \ gx = xg, \forall x \in G\}.$$

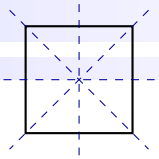
Demuestre que $Z(G)$ es un subgrupo de G.

● Ejercicio 2.8.21 (Centralizador y Subgrupo) R/ p.312

Sea $(G, \cdot)$ un grupo y $A \subset G$. Se define el **centralizador** $C_G(A)$ de A en G por

$$C_G(A) := \{g \in G \ : \ ga = ag, \forall a \in A\}.$$

Muestre que $C_G(A)$ es un subgrupo de G.



2.9 Clases laterales

En el marco de la Teoría de Grupos, el concepto de clases laterales emerge como una herramienta fundamental para explorar las relaciones entre los elementos de un grupo y entender su estructura algebraica. De manera objetiva, las clases laterales ofrecen una perspectiva clara sobre la partición de un grupo en conjuntos que comparten propiedades fundamentales bajo la operación del grupo.

Aunque las clases laterales en su forma moderna se formalizaron principalmente en la primera mitad del siglo XX, el estudio de particiones de conjuntos y simetrías dentro de los grupos se remonta a los trabajos pioneros de matemáticos como Évariste Galois en el siglo XIX.

Durante el siglo XX, con el auge de la Teoría de Grupos y su aplicación en diversas ramas de las matemáticas, incluyendo la teoría de números y la geometría, los conceptos relacionados con las clases laterales adquirieron una importancia considerable. Los matemáticos desarrollaron métodos sistemáticos para comprender la estructura interna de los grupos y la relación entre sus elementos a través de las clases laterales.

En particular, los trabajos de destacados matemáticos como Emmy Noether[5] y Claude Chevalley[6] propor-

[5]Emmy Noether fue una destacada matemática alemana que dejó una profunda huella en el desarrollo de la teoría algebraica y la física teórica en el siglo XX. Nació el 23 de marzo de 1882 en Erlangen, Alemania. A pesar de las barreras sociales y de género que enfrentó en esa época, Noether demostró su excepcional talento matemático desde joven.

Obtuvo su doctorado en matemáticas en 1907 y, a lo largo de su carrera, realizó importantes contribuciones a la teoría de números, la teoría de invariantes, y especialmente, a la teoría de grupos y álgebras. Su teorema fundamental, conocido como el Teorema de Noether, establece la relación entre simetrías y leyes de conservación en física, y se ha convertido en un pilar fundamental de la física teórica.

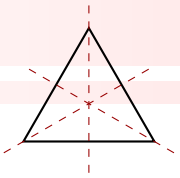
A pesar de que Noether no tuvo acceso a cargos académicos oficiales debido a su género y ascendió en una época en la que las mujeres tenían limitado reconocimiento en la academia, logró influir profundamente en la comunidad matemática y científica. Dio clases en la Universidad de Gotinga bajo la supervisión de David Hilbert y, más tarde, se trasladó a los Estados Unidos para enseñar en la Universidad de Bryn Mawr.

Emmy Noether falleció el 14 de abril de 1935, pero su legado perdura. Su trabajo ha influido en diversas áreas de las matemáticas y la física, y su impacto se refleja en la actualidad con el reconocimiento de la importancia de su contribución a la ciencia. Además, su valentía y perseverancia han inspirado a generaciones posteriores de mujeres en el campo STEM (ciencia, tecnología, ingeniería y matemáticas). Consultar O'Connor (2024a)

[6]Claude Chevalley fue un destacado matemático francés nacido el 11 de febrero de 1909 en París y fallecido el 28 de junio de 1984 en París. Fue conocido por sus contribuciones significativas en álgebra, teoría de números y geometría algebraica.

Chevalley desempeñó un papel crucial en el desarrollo de la teoría de grupos y álgebras, y su trabajo en teoría de números algebraicos fue influyente. Contribuyó al estudio de estructuras algebraicas y formuló la teoría de Chevalley sobre grupos algebraicos lineales, que tuvo un impacto duradero en la teoría de grupos y la geometría algebraica.

Además de su destacada carrera académica, Claude Chevalley también fue profesor en instituciones prominentes como la Universidad de Princeton y la Universidad de París. Su enfoque riguroso y sus ideas innovadoras han dejado una marca duradera en la matemática del siglo XX. Chevalley también jugó un papel importante en la creación del grupo Bourbaki, una colaboración matemática que ha tenido un impacto significativo en la investigación matemática contemporánea. Su legado como matemático y educador continúa siendo reconocido y apreciado en la comunidad matemática.Encyclopedia.com (s.f.)



cionaron contribuciones fundamentales al entendimiento de las clases laterales y su aplicación en álgebras abstractas. Estos avances han influido significativamente en la forma en que se abordan y enseñan los conceptos de la Teoría de Grupos en la actualidad.

Definición 2.9.1:

Sea G un grupo y sea H un subgrupo de G.

1. Se llama **clase izquierda** de H en G, determinada por $g \in G$, al conjunto

$$gH := \{gh : h \in H\}.$$

2. Se llama **clase derecha** de H en G, determinada por $g \in G$, al conjunto

$$Hg := \{hg : h \in H\}.$$

Observación 2.9.1.

Si se utiliza la notación de grupo aditivo $(G, +)$, entonces las clases izquierda y derecha de H en G, determinadas por $g \in G$, son respectivamente

$$g + H := \{g + h : h \in H\}$$

$$H + g := \{h + g : h \in H\}$$

En lo que sigue de, se trabajará con clases laterales izquierdas, ya que todos los resultados son análogos para las clases derechas.

Definición 2.9.2:

Sea G un grupo y sea H un subgrupo de G. Se llama **conjunto cociente** de H en G, al conjunto

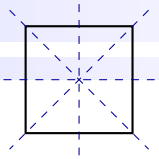
$$G/H := \{gH : g \in G\}.$$

En otras palabras, el conjunto cociente de H en G es el *conjunto formado por todas las clases laterales* izquierdas de de H en G.

Observación 2.9.2.

Si se usa la notación de grupo aditivo $(G, +)$, el conjunto cociente de H en G se escribe como

$$G/H := \{g + H : g \in G\}$$



Ejemplo 2.9.1.

Considere el grupo de Klein $(V, \circ)$ estudiado en el ejemplo 2.1.16, donde $V := \{e, h, r, v\}$ y $\circ$ es la composición de funciones. Sea $H := \{e, h\}$. Usando el teorema 2.7.3 es fácil verificar que H es subgrupo de V. Además. recuerde que la tabla del grupo de Klein es la siguiente:

$\circ$	e	h	r	v
e	e	h	r	v
h	h	e	v	r
r	r	v	e	h
v	v	r	h	e

Para hallar las clases izquierdas de H en V se usa la definición 2.9.1. Así, la clase izquierda de H en V, determinada por e, es

$$eH = \{e\circ e, e\circ h\} = \{e, h\} = H.$$

Similarmente, la clase izquierda de H en V, determinada por h, es

$$hH = \{h\circ e, h\circ h\} = \{h, e\} = H.$$

La clase izquierda de H en V, determinada por r, es

$$rH = \{r\circ e, r\circ h\} = \{r, v\}.$$

Finalmente, la clase izquierda de H en V, determinada por v, es

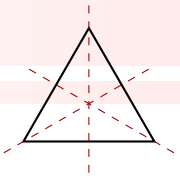
$$vH = \{v\circ e, v\circ h\} = \{v, r\}.$$

Observe que sólo hay dos clases izquierdas: H y $\{v, r\}$. Por lo tanto, el conjunto cociente formado por todas las clases izquierdas es

$$V/H = \{H, \{v, r\}\}.$$

Ejemplo 2.9.2.

Considere el grupo simétrico $S_3 = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$ del ejemplo 2.1.30. Recuerde que la tabla de S_3



con la operación composición usual de funciones es

$\circ$	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_1	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_2	σ_2	σ_1	σ_4	σ_3	σ_6	σ_5
σ_3	σ_3	σ_5	σ_1	σ_6	σ_2	σ_4
σ_4	σ_4	σ_6	σ_2	σ_5	σ_1	σ_3
σ_5	σ_5	σ_3	σ_6	σ_1	σ_4	σ_2
σ_6	σ_6	σ_4	σ_5	σ_2	σ_3	σ_1

Sea $H := \{\sigma_1, \sigma_4, \sigma_5\}$. Usando el teorema 2.7.3 no es difícil verificar que $H < S_3$. Ahora, las clases izquierdas son

$$\begin{aligned}
\sigma_1 H &= \{\sigma_1\circ\sigma_1, \sigma_1\circ\sigma_4, \sigma_1\circ\sigma_5\} = \{\sigma_1, \sigma_4, \sigma_5\} = H \\
\sigma_2 H &= \{\sigma_2\circ\sigma_1, \sigma_2\circ\sigma_4, \sigma_2\circ\sigma_5\} = \{\sigma_2, \sigma_3, \sigma_6\} \\
\sigma_3 H &= \{\sigma_3\circ\sigma_1, \sigma_3\circ\sigma_4, \sigma_3\circ\sigma_5\} = \{\sigma_3, \sigma_6, \sigma_2\} \\
\sigma_4 H &= \{\sigma_4\circ\sigma_1, \sigma_4\circ\sigma_4, \sigma_4\circ\sigma_5\} = \{\sigma_4, \sigma_5, \sigma_1\} = H \\
\sigma_5 H &= \{\sigma_5\circ\sigma_1, \sigma_5\circ\sigma_4, \sigma_5\circ\sigma_5\} = \{\sigma_5, \sigma_1, \sigma_4\} = H \\
\sigma_6 H &= \{\sigma_6\circ\sigma_1, \sigma_6\circ\sigma_4, \sigma_6\circ\sigma_5\} = \{\sigma_6, \sigma_2, \sigma_3\}
\end{aligned}$$

Por lo tanto, el conjunto cociente de H en S_3 es

$$S_3/H = \left\{H, \{\sigma_2, \sigma_3, \sigma_6\}\right\}.$$

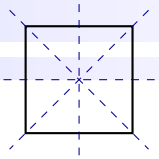
Ejemplo 2.9.3.

Considere el subconjunto $H = 2\mathbb{Z}$. Observe que H es un subgrupo de $\mathbb{R}$ con la suma usual de números reales. Por ejemplo, la clase izquierda de $2\mathbb{Z}$ en $\mathbb{R}$ determinada por el número $3 \in \mathbb{R}$, es

$$3 + 2\mathbb{Z} = \{3 + 2n \ : \ n \in \mathbb{Z}\}.$$

En general, para cualquier $x \in \mathbb{R}$, la clase izquierda de $2\mathbb{Z}$ en $\mathbb{R}$ determinada por $x \in \mathbb{R}$, es

$$x + 2\mathbb{Z} = \{x + 2n \ : \ n \in \mathbb{Z}\}.$$



Por lo tanto, el conjunto cociente, formado por todas las clases izquierdas, es

$$\mathbb{R}/2\mathbb{Z} = \{x + 2\mathbb{Z} : x \in \mathbb{R}\}.$$

Ejemplo 2.9.4.

Sea $x \in \mathbb{Z}_5$ y observe que si $[x] \in \mathbb{Z}_5$, entonces

$$\begin{aligned}
[x] &:= \left\{ y \in \mathbb{Z} : y \equiv x (\text{mod } 5) \right\} \\
&= \left\{ y \in \mathbb{Z} : 5|(y - x) \right\} \\
&= \left\{ y \in \mathbb{Z} : y - x = 5k,\ k \in \mathbb{Z} \right\} \\
&= \left\{ y \in \mathbb{Z} : y = x + 5k,\ k \in \mathbb{Z} \right\} \\
&= x + 5\mathbb{Z}.
\end{aligned}$$

Ahora, si se considera el subgrupo $(5\mathbb{Z}, +)$ de $(\mathbb{Z}, +)$, se puede inferir que la clase $[x]$ módulo 5 es igual a la clase izquierda de x en $5\mathbb{Z}$. Es decir

$$[x] = x + 5\mathbb{Z}.$$

Entonces, el conjunto de clases izquierdas de $5\mathbb{Z}$ en $\mathbb{Z}$ es

$$\begin{aligned}
\mathbb{Z}/5\mathbb{Z} &= \left\{ x + 5\mathbb{Z} : x \in \mathbb{Z} \right\} \\
&= \left\{ [x] \quad \text{módulo } 5 : x \in \mathbb{Z} \right\} \\
&= \mathbb{Z}_5
\end{aligned}$$

Observación 2.9.3.

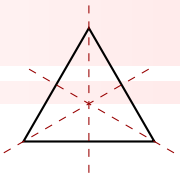
En general, de manera análoga al ejemplo anterior, si n es un número entero se cumple que

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n.$$

Teorema 2.9.1:

Sea G un grupo y sea $H < G$. Para cada $g \in G$ se tiene que

$$\left|gH\right| = \left|H\right| = \left|Hg\right|$$



Demostración. Se va probar que $\left|gH\right| = \left|H\right|$. Para esto, es suficiente encontrar una función biyectiva de H en gH. Sea $g \in G$ y defina la aplicación $\varphi : H \to gH$ tal que

$$\varphi(h) = gh$$

para todo $h \in H$. Se debe probar que esta función es inyectiva y sobreyectiva.

- Para la inyectividad[7], considere h_1, h_2 elementos de H y suponga que

  $$\varphi(h_1) = \varphi(h_2),$$

  esto implica que

  $$gh_1 = gH_2.$$

  Operando g^{-1} por la izquierda de la igualdad tiene

  $$g^{-1}gh_1 = gg^{-1}h_2.$$

  Luego

  $$h_1 = h_2.$$

  Así, la función φ es inyectiva.

- Para la sobreyectividad[8], considere $y \in gH$, entonces existe $h \in H$ tal que $y = gh$. Luego, observe que $\varphi(h) = gh$, es decir, la preimagen de y es h. Así, la función φ es sobreyectiva.

Finalmente la función φ es biyectiva y se concluye que $\left|gH\right| = \left|H\right|$.

La prueba de que $|H| = |HG|$ es análoga. □

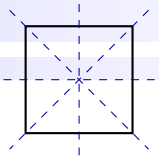
Teorema 2.9.2:

Sea G un grupo y $H < G$, entonces para cualquier par de elementos a, b de G se tiene que:

1. H es en sí mismo una clase de H en G.
2. $a \in aH$.
3. $b \in aH$ si y solo si $a \in bH$.

[7]Recuerde que una función $f : A \to B$ es inyectiva si y solo si para cada $a, b \in A$ se cumple que si $a \neq b$ entonces $f(a) \neq f(b)$. O su contrapositiva, para cada $a, b \in A$ se cumple que si $f(a) = f(b)$ entonces $a = b$.

[8]Recuerde que una función $f : A \to B$ es sobreyectiva si solo si para cada $b \in B$ existe $a \in A$ tal que $f(a) = b$.



4. $b \in aH$ si y solo si $bH = aH$

5. Si $aH \cap bH \neq \emptyset$ entonces $aH = bH$.

Demostración. Se procede a demostrar los cuatro puntos del teorema anterior:

1. Considere el elemento neutro $e \in G$, entonces

$$eH = \{eh : h \in H\} = \{h : h \in H\} = H,$$

es decir, H es una clase en sí mismo de H en G.

2. Como $H < G$ entonces $e \in H$. Luego, $a = ae \in aH$, es decir, $a \in aH$.

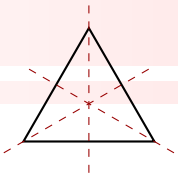
3. ($\Rightarrow$) Suponga que $b \in aH$, se debe probar que $a \in bH$. Ahora, como $b \in aH$, entonces existe un $h \in H$ tal que $b = ah$. Como H es un subgrupo de G, entonces existe el elemento inverso de h denotado por $h^{-1} \in H$, el cual se opera en la igualdad $b = ah$ resultando $bh^{-1} = a$. Es decir, a se obtiene de operar b con un elemento de H, entonces $a \in bH$.
($\Leftarrow$) Es análoga al anterior.

4. ($\Rightarrow$) Suponga que $b \in aH$, se debe probar que $bH = aH$. Para tal efecto, primero se probará que $bH \subseteq aH$ y luego que $aH \subseteq bH$.

   - ($\subseteq$) Sea $x \in bH$, entonces $x = bh_1$ para algún $h_1 \in H$. Además, por hipótesis $b \in aH$, entonces $b = ah_2$ para algún $h_2 \in H$. De estos dos resultados se obtiene que $x = ah_2h_1$, pero h_2h_1 debe estar en H pues H es un subgrupo de G, por lo tanto $x \in aH$. Así se cumple que $bH \subseteq aH$.
   - ($\supseteq$) Sea $x \in aH$, entonces $x = ah_1$ para algún $h_1 \in H$. Asimismo, por hipótesis $b \in aH$, entonces $b = ah_2$ para algún $h_2 \in H$. Ahora, como H es un subgrupo de G, existe h_2^{-1}, el cual se opera en la igualdad $b = ah_2$ de la forma $bh_2^{-1} = ah_2h_2^{-1}$, obteniendo $bh_2^{-1} = a$. Este resultado se cambia en $x = ah_1$ obteniendo $x = bh_2^{-1}h_1$, donde $h_2^{-1}h_1$ es un elemento de H, por lo tanto $x = bh_2^{-1}h_1$ es un elemento de bH, es decir, $x \in bH$. Por lo tanto $aH \subseteq bH$.

   Finalmente $bH = aH$.

5. Suponga que $aH \cap bH \neq \emptyset$, hay que demostrar que $aH = bH$. Ahora, como $aH \cap bH \neq \emptyset$, existe al menos un elemento $x \in aH \cap bH$, es decir, $x \in aH$ y $x \in bH$, es decir, existen $h_1, h_2 \in H$



tales que

$$x = ah_1 = bh_2.$$

Ahora, se va demostrar que $aH \subseteq bH$. y $bH \subseteq aH$.

- ($\subseteq$) Sea $y \in aH$, entonces existe $h_3 \in H$ tal que $y = ah_3$. Además, como $x = ah_1$ fácilmente se infiere que $xh_1^{-1} = a$, y como $x = bh_2$, entonces $bh_2h_1^{-1} = a$. Con este último dato note que

$$y = ah_3 = bh_2h_1^{-1}h_3,$$

  donde $h_2h_1^{-1}h_3$ es un elemento de H porque este es un subgrupo. Así, $y \in bH$ y $aH \subseteq bH$.

- ($\supseteq$) Sea $y \in bH$, entonces existe $h_4 \in H$ tal que $y = bh_4$. El resto de la demostración es análoga, solo que esa vez debe concluir que

$$y = ah_1h_2^{-1}h_4,$$

  donde $h_1h_2^{-1}h_4$ es un elemento de H porque este es un subgrupo. Así, $y \in aH$ y $bH \subseteq aH$.

Por último $aH = bH$.

□

Observación 2.9.4.

Dado un grupo G y $H < G$, entonces, del teorema anterior se puede notar lo siguiente:

1. Dos clases laterales de H en G o bien son disjuntas o bien son la misma clase. En otras palabras, dos clases diferentes no pueden compartir elementos en común, de lo contrario, son la misma clase.

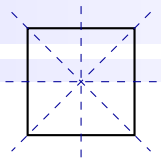
2. Cada elemento de G está exactamente en una sola clase.

Teorema 2.9.3:

Sea G un grupo y $H < G$, $H \neq \emptyset$, entonces G es la unión de clases distintas de H en G, es decir,

$$G = \bigcup_{a \in G} aH$$

Demostración. Para probar la igualdad anterior Se probarán utilizando las dos relaciones de inclusión $G \subseteq \cup_{a \in G} aH$ y $\cup_{a \in G} aH \subseteq G$.



($\subseteq$) Sea $x \in G$ y sea e el elemento neutro de G. Como $H < G$ entonces $e \in H$. Ahora, note que $x = xe \in xH$, es decir, x pertenece al menos a una clase lateral izquierda de H en G. Por lo tanto $x \in \bigcup_{a \in G} aH$.
($\supseteq$) Sea $x \in \bigcup_{a \in G} aH$. Por definición de unión de conjuntos

$$x \in aH, \quad \text{para algún } a \in G,$$

entonces

$$x = ah, \quad \text{para algún } h \in H \quad \text{y para algún } a \in G,$$

y como G es cerrado, $ah \in G$. Por lo tanto $x \in G$. □

Ejemplo 2.9.5.

En el ejemplo 2.9.1 se hallaron las clases izquierdas del subgrupo $H := \{e, h\}$ del grupo de Klein. Estas clases son H y $\{v, r\}$. Luego, note que la unión de estas clases equivale a:

$$H \cup \{v, r\} = \{e, h, v, r\} = G,$$

lo cual verifica el resultado del teorema 2.9.3 anterior.

Ejemplo 2.9.6.

En el ejemplo 2.9.2 se consideró el grupo simétrico $S_3 = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$ y se hallaron las clases izquierdas del subgrupo $H := \{\sigma_1, \sigma_4, \sigma_5\}$, las cuales son H y $\{\sigma_2, \sigma_3, \sigma_6\}$. Note que la unión de estas clases forma precisamente el grupo S_3.

Ejemplo 2.9.7.

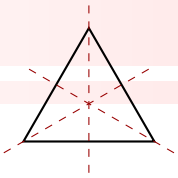
Considere el grupo $(\mathbb{Z}, +)$ y su subgrupo $(3\mathbb{Z}, +)$ (ver teorema 2.7.2). Ahora, las clases izquierdas de $3\mathbb{Z}$ en $\mathbb{Z}$ bajo la suma son de la forma $[x] = x + 3\mathbb{Z}$ (tome como referencia el ejemplo 2.9.4), es decir:

$$[0] = 0 + 3\mathbb{Z} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\} = 3\mathbb{Z}.$$

$$[1] = 1 + 3\mathbb{Z} = \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\}.$$

$$[2] = 2 + 3\mathbb{Z} = \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\}.$$

Note que $3\mathbb{Z} \cup 1 + 3\mathbb{Z} \cup 2 + 3\mathbb{Z} = \mathbb{Z}$, verificando lo expuesto en el teorema 2.9.3.



2.9.1. El Teorema de Lagrange.

En la Teoría de Grupos, el Teorema de Lagrange se presenta como un resultado fundamental que aborda la estructura de los subgrupos dentro de un grupo finito. De manera objetiva, este teorema, formulado por Joseph-Louis Lagrange[9] en el siglo XVIII, establece una relación crucial entre el orden de un grupo y el orden de sus subgrupos. Esta breve introducción busca proporcionar una visión sobria del Teorema de Lagrange, resaltando su importancia en el análisis de la estructura algebraica de los grupos finitos.

Definición 2.9.3:

Sea G un grupo y sea H un subgrupo de G. Se llama **índice** de H en G, al número

$$\big[G : H\big] := \Big|G/H\Big|$$

Es decir, el índice de H en G es el número de clases izquierdas (derechas) de H en G, el cual es la cardinalidad del conjunto cociente

$$G/H := \{gH \ : g \in G\}$$

de la definición 2.9.2.

Ejemplo 2.9.8.

Considere el ejemplo 2.9.2 sobre el grupo simétrico S_3 y de su subgrupo

$$H := \{\sigma_1, \sigma_4, \sigma_5\},$$

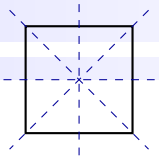
[9]Joseph-Louis Lagrange, nacido Giuseppe Lodovico Lagrangia el 25 de enero de 1736 en Turín, Italia, y fallecido el 10 de abril de 1813 en París, fue un matemático y físico italo-francés que realizó contribuciones fundamentales en diversos campos de las matemáticas y la física.

Lagrange fue un prodigio matemático desde joven y, a la edad de 19 años, ya había realizado contribuciones significativas a la teoría de números. Trabajó en la teoría de ecuaciones, desarrollando el método de Lagrange para resolver ecuaciones polinómicas generales.

En el ámbito de la mecánica analítica, Lagrange formuló las ecuaciones de movimiento conocidas como las ecuaciones de Lagrange, que son fundamentales en la descripción de sistemas dinámicos. Su enfoque elegante y sistemático en la mecánica analítica influyó en el desarrollo posterior de la física teórica.

Lagrange también desempeñó un papel crucial en la teoría de números, la teoría de funciones analíticas y la teoría de grupos. Fue un miembro destacado de la Academia de Ciencias de París y contribuyó al establecimiento de la notación matemática moderna.

Su vida transcurrió en varios centros académicos europeos, incluyendo Turín, Berlín y París. Lagrange fue nombrado conde por Napoleón Bonaparte y se convirtió en senador. Su legado perdura en los numerosos teoremas y conceptos que llevan su nombre, destacando la influencia duradera de sus contribuciones en las matemáticas y la física. Consultar Fernandez (2004)



El conjunto cociente de H en S_3 es

$$S_3/H = \Big\{ H, \{\sigma_2, \sigma_3, \sigma_6\} \Big\},$$

entonces, el índice de H en S_3 es $\big[S_3 : H\big] = \Big|S_3/H\Big| = \Big|\Big\{ H, \{\sigma_2, \sigma_3, \sigma_6\} \Big\}\Big| = 2.$

Ejemplo 2.9.9.

Considere el grupo $(\mathbb{Z}, +)$ y el subgrupo $5\mathbb{Z} < \mathbb{Z}$. Por el ejemplo 2.9.4, el conjunto cociente de $\mathbb{Z}$ en $5\mathbb{Z}$ es

$$\mathbb{Z}/5\mathbb{Z} = \mathbb{Z}_5.$$

Entonces, el índice de $5\mathbb{Z}$ en $\mathbb{Z}$ es

$$\big[\mathbb{Z} : 5\mathbb{Z}\big] = \Big|\mathbb{Z}/5\mathbb{Z}\Big| = \Big|\mathbb{Z}_5\Big| = 5.$$

Ejemplo 2.9.10.

De forma análoga al ejemplo anterior, en general, si $n \in \mathbb{N}$, el índice de $n\mathbb{Z}$ en $\mathbb{Z}$ es

$$\big[\mathbb{Z} : n\mathbb{Z}\big] = \Big|\mathbb{Z}/n\mathbb{Z}\Big| = n.$$

Teorema 2.9.4:

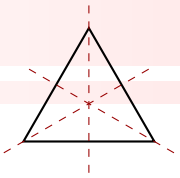
Sea G un grupo finito y sea $H < G$. Entonces

$$\Big|G/H\Big| = \frac{|G|}{|H|}.$$

Es decir, si G es de orden finito, el orden de cualquier subgrupo divide al orden del grupo.

Demostración. Como G es finito, el conjunto cociente G/H debe ser finito. Entonces se puede escribir

$$G/H = \{a_1H, a_2H, \ldots, a_nH\}$$



donde $a_iH \cap a_jH = \emptyset$ si $i \neq j$. Además, note que $|G/H| = n$. Por otro lado observe que:

$$\begin{aligned} |G| &= \left|\bigcup_{i\in\mathbb{N}}^{n} a_iH\right| \quad \text{por el teorema 2.9.3.} \\ &= |a_1H| + |a_2H| + |a_3H| + \cdots + |a_nH| \\ &= |H| + |H| + \cdots + |H| \\ &= n|H| \\ &= |G/H||H|. \end{aligned}$$

□

Observación 2.9.5.

El teorema 2.9.4 se llama Teorema de Lagrange. Básicamente, éste establece que dado un grupo finito G y si $H < G$, entonces el orden de H divide al orden de G, es decir

$$|H|\Big||G|.$$

Ejemplo 2.9.11.

Considere el grupo $(\mathbb{Z}_6, +)$. Como $|\mathbb{Z}_6| = 6$, el cual es divisible por 1, 2, 3 o 6,es entonces $\mathbb{Z}_6$ sólo puede tener subgrupos de órdenes 1, 2, 3 o 6. Es importante recalcar que los subgrupos de orden 1 y orden 6 deben ser los triviales.

Ejemplo 2.9.12.

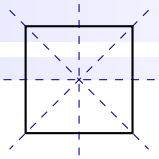
Considere el grupo $(\mathbb{Z}_5, +)$. Como $|\mathbb{Z}_5| = 5$ y solo es divisible por 1 y por 5, entonces $\mathbb{Z}_5$ sólo puede tener subgrupos de órdenes 1 o 5. De hecho, tienen que ser los dos subgrupos triviales, es decir, el subgrupo de orden 1 es $\{[0]\}$ y el de orden 5 es el mismo $\mathbb{Z}_5$.

Ejemplo 2.9.13.

Considere el grupo de $(\mathbb{Z}_5^*, \cdot)$. Se sabe que $|\mathbb{Z}_5^*| = 4$, entonces los posibles órdenes de sus subgrupos $1, 2$ o 4. De hecho, los subgrupos de $(\mathbb{Z}_5^*, \cdot)$ son:

$$\{[1]\}, \quad \{[1],[3]\}, \quad \{[1],[4]\} \quad \text{y} \quad \mathbb{Z}_5^*.$$

Ejemplo 2.9.14.



Como $|S_3| = 3! = 6$, entonces por el Teorema de Lagrange los subgrupos de S_3 son de orden $1, 2, 3$ o 6. En efecto, por el ejemplo 2.7.7 los subgrupos de S_3 son

$$\{\sigma_1\},\ \{\sigma_1, \sigma_3\},\ \{\sigma_1, \sigma_6\},\ \{\sigma_1, \sigma_2\},\ \{\sigma_1, \sigma_4, \sigma_5\},\ S_3.$$

2.10 Grupos Cíclicos

En el ámbito de la Teoría de Grupos, los Grupos Cíclicos se destacan como entidades algebraicas notables que han capturado la atención de los matemáticos a lo largo del tiempo. Un Grupo Cíclico, definido por su capacidad para ser generado por un solo elemento, revela propiedades únicas y estructuras fundamentales bajo la operación de composición del grupo.

Definición 2.10.1: Grupo Cíclico.

Sea G un grupo y sea $g \in G$. Se llama **conjunto generado** por g al conjunto

$$\langle g \rangle := \{g^n \ : n \in \mathbb{Z}\} = \{\ldots, g^{-3}, g^{-2}, g^{-1}, e, g, g^2, g^3, \ldots\},$$

Observación 2.10.1.

Con la notación de grupos aditivos $(G, +)$, el conjunto generado por $g \in G$ es el conjunto

$$\langle g \rangle := \{ng \ : n \in \mathbb{Z}\} = \{\cdots, -3g, -2g, -g, e, g, 2g, 3g, \cdots\}.$$

Teorema 2.10.1:

Sea G un grupo y sea $g \in G$. Entonces $\langle g \rangle$ es un subgrupo de G.

Demostración. Sea $g \in G$ y sean $x, y \in \langle g \rangle$. Entonces

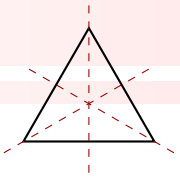
$$x = g^n, \quad y = g^m \quad \text{para algunos} \quad n, m \in \mathbb{Z}.$$

Por el teorema 2.2.5 el inverso de y es

$$y^{-1} = (g^m)^{-1} = g^{-m},$$

lo cual implica que

$$xy^{-1} = g^n g^{-m} = g^{n-m}$$



Como $n-m \in \mathbb{Z}$, entonces $g^{n-m} \in \langle g \rangle$, es decir $xy^{-1} \in \langle g \rangle$ y por el teorema 2.7.1 se tiene que $\langle g \rangle$ es un subgrupo de G. □

Observación 2.10.2.

Dado un grupo G, note que $e^n = e$ para cualquier $n \in \mathbb{Z}$, entonces el subgrupo generado por el elemento neutro e es $\{e\}$, es decir, el subgrupo trivial $\{e\}$. Por lo tanto

$$\langle e \rangle = \{e\}.$$

Ejemplo 2.10.1.

Considere el grupo de Klein $(V, \circ)$ estudiado en el ejemplo 2.1.16, donde $V := \{e, h, r, v\}$. Recuerde que la tabla del grupo de Klein es la siguiente:

$\circ$	e	h	r	v
e	e	h	r	v
h	h	e	v	r
r	r	v	e	h
v	v	r	h	e

Se va hallar el subgrupo generado por h. Para ello se opera h consigo mismo reiteradamente, esto es:

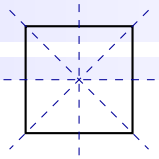
$$\begin{aligned} h &= h \\ h^2 = h \circ h &= e \\ h^3 = h \circ h \circ h &= h \\ h^4 = h \circ h \circ h \circ h &= e \end{aligned}$$

Si se continúa operando h consigo mismo, siempre se obtiene los elementos e y h. Por lo que el subgrupo generado por h es

$$\langle h \rangle = \{e, h\}.$$

Similarmente, el subgrupo generado por r es

$$\langle r \rangle = \{e, r\}$$



y el subgrupo generado por v es

$$\langle v \rangle = \{e, v\}.$$

Ejemplo 2.10.2.

Considere el grupo $(\mathbb{Z}_5^*, \cdot)$ y en particular tome el elemento [2], se va hallar el subgrupo generado por dicho elemento. Para ello note que:

$$\begin{aligned} [2] &= [2] \\ ([2])^2 &= [4] \\ ([2])^3 &= [3] \\ ([2])^4 &= [1] \end{aligned}$$

Observe que el subgrupo generado por [2] es el conjunto formado por cada elemento de $\mathbb{Z}_5^*$, es decir,

$$\langle [2] \rangle = \mathbb{Z}_5^*.$$

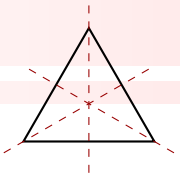
Ejemplo 2.10.3.

Considere el grupo $(\mathbb{Z}_6, +)$ y en particular tome el elemento [4], se va hallar el subgrupo generado por dicho elemento, recordando que al ser un grupo aditivo se escribe $n[x]$ en lugar de $[x]^n$ para $n \in \mathbb{Z}$, entonces:

$$\begin{aligned} [4] &= [4] \\ 2[4] &= [2] \\ 3[4] &= [0] \\ 4[4] &= [4] \\ 5[4] &= [2] \\ 6[4] &= [0] \end{aligned}$$

Así, el subgrupo generado por [4] en el grupo $(\mathbb{Z}_6, +)$ corresponde a

$$\langle [4] \rangle = \{[0], [2], [4]\}.$$



Definición 2.10.2:

Se dice que un grupo G es un **grupo cíclico** si existe $g \in G$ tal que

$$G = \langle g \rangle$$

En tal caso, se dice que g es un **generador** de G.

Observación 2.10.3.

Básicamente, G es un grupo cíclico generado por g si para cada elemento $a \in G$ existe un $n \in \mathbb{Z}$ tal que $a = g^n$.

Ejemplo 2.10.4.

Tome como referencia el ejemplo 2.10.2 donde se determinó que $\langle [2] \rangle = \mathbb{Z}_5^*$ bajo el producto de clases en módulo 5, es decir $(\mathbb{Z}_5^*, \cdot)$ es generado por [2] y así $(\mathbb{Z}_5^*, \cdot)$ se considera como un grupo cíclico.

Ejemplo 2.10.5.

Recuerde que el conjunto de unidades U_5 está formado por todos los $[a] \in \mathbb{Z}_5$ tales que $(a, 5) = 1$, según se estudió en el ejemplo 2.1.22. Es decir,

$$U_5 = \{[1], [2], [3], [4]\}.$$

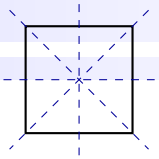
De hecho y con fundamento en el ejemplo anterior, $(U_5, \cdot)$ también es un grupo cíclico generado por [2].

Ejemplo 2.10.6.

Considere el grupo $(\mathbb{Z}_4, +)$ y en particular tome el elemento [3], observe que:

$$\begin{aligned} [3] &= [3] \\ 2[3] &= [2] \\ 3[3] &= [1] \\ 4[3] &= [0] \end{aligned}$$

Note que [3] genera a cada elemento de $\mathbb{Z}_4$ bajo la suma de clases en módulo 4, entonces $(\mathbb{Z}_4, +)$ es un grupo cíclico porque $\langle [3] \rangle = \mathbb{Z}_4$.



Teorema 2.10.2:

Si G es un grupo cíclico, entonces G es un grupo abeliano.

Demostración. Suponga que G es generado por el elemento g, es decir $G = \langle g \rangle$. Luego, sean $a, b \in G$, entonces existen $m, n \in \mathbb{Z}$ tales que $a = g^m$ y $b = g^n$. De esta forma se tiene que

$$\begin{aligned} ab &= a^m b^n \\ &= g^{m+n} \quad \text{por la parte tres del teorema 2.2.5.} \\ &= g^{n+m} \\ &= g^n g^m \\ &= ba. \end{aligned}$$

Por lo tanto $ab = ba$, lo cual implica que $G = \langle g \rangle$ es un grupo abeliano. □

Observación 2.10.4.

Si un grupo fuera abeliano, esto no implica de forma necesaria que sea un grupo cíclico. Para comprender esto, considere el ejemplo 2.10.1 sobre el grupo de Klein, el cual es un grupo abeliano pero no es cíclico, ya que

$$\langle h \rangle = \{e, h\}, \quad \langle r \rangle = \{e, r\}, \quad \langle v \rangle = \{e, v\}.$$

Además, no es difícil verificar que $\langle e \rangle = \{e\}$. Por lo tanto, el grupo V no es generado por ninguno de sus elementos, concluyendo así que V no es cíclico.

Ejemplo 2.10.7.

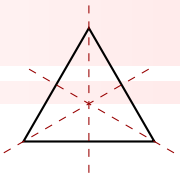
Sea G un grupo cíclico generado por $g \in G$, entonces G también es generado por su inverso g^{-1}.

Demostración. Sea $a \in G$, entonces existe $n \in \mathbb{Z}$ tal que $a = g^n$ puesto que $\langle g \rangle = G$. Luego, usando la parte tres de la definición 2.2.1 se cumple que

$$a = g^n = g^{-(-n)} = (g^{-1})^{-n},$$

y como $-n \in \mathbb{Z}$, entonces G es generado por g^{-1}. □

Ejemplo 2.10.8.



Considere el grupo $(G,\cdot)$, donde $G := \{1,-1,-i,i\}$, $i^2=-1$, y "$\cdot$" es la multiplicación de los números complejos, estudiado en el ejemplo 2.1.11. Note que

$$\begin{aligned} i^1 &= i \\ i^2 &= -1 \\ i^3 &= -i \\ i^4 &= 1 \\ i^5 &= i \end{aligned}$$

Como las potencias de i generan todos los elementos de G, se concluye que G es cíclico y que i es un generador de G, es decir, $\langle i\rangle = G$. Además, como $-i$ es el inverso de i y por el resultado del ejemplo 2.10.7, se cumple que $\langle -i\rangle = G$.

Ejemplo 2.10.9.

Considere el grupo $(\mathbb{Z}_3,+)$ y el elemento $[1]$, observe que

$$\begin{aligned} 1[1] &= [1], \\ 2[1] &= [2] \\ 3[1] &= [0] \end{aligned}$$

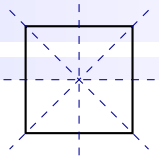
Esto significa que $[1]$ genera $\mathbb{Z}_3$ y por lo tanto $\mathbb{Z}_3 = \langle[1]\rangle$, así $(\mathbb{Z}_3,+)$ es ungrupo cíclico. También, como $[2]$ es el inverso de $[1]$ y por el resultado del ejemplo 2.10.7, se tiene que $\langle[2]\rangle = G$. De hecho, note que Similarmente, en el caso de $[2]$ tenemos

$$\begin{aligned} 1[2] &= [2], \\ 2[2] &= [1] \\ 3[2] &= [0] \end{aligned}$$

Ejemplo 2.10.10.

En el ejemplo 2.10.6 se probó que $(\mathbb{Z}_4,+)$ es un grupo cíclico tal que $\langle[3]\rangle = \mathbb{Z}_4$. Entonces se tendría que $\langle[1]\rangle = \mathbb{Z}_4$ puesto que $[1]$ es el inverso de $[3]$.

Ejemplo 2.10.11.



En general, para cualquier $n \in \mathbb{N}$, el grupo $(\mathbb{Z}_n, +)$ es cíclico con generador $[1]$, pues

$$\begin{aligned} 1[1] &= [1], \\ 2[1] &= [2] \\ 3[1] &= [3] \\ &\vdots \\ (n-1)[1] &= [n-1] \\ n[1] &= [n] = [0] \end{aligned}$$

Asimismo, como $[n-1]$ es el inverso de $[1]$ y por el resultado del ejemplo 2.10.7, se tiene que $(\mathbb{Z}_n, +)$ también es generado por $[n-1]$, esto es $\langle [n-1] \rangle = (\mathbb{Z}_n, +)$.

Ejemplo 2.10.12.

Muestre que el grupo $(\mathbb{Q}, +)$ no es cíclico.

Demostración. Suponga por contradicción que $(\mathbb{Q}, +)$ es cíclico. Entonces existe $q \in \mathbb{Q}$ tal que $\langle q \rangle = \mathbb{Q}$. Como q es un número racional, entonces q es de la forma $q = \frac{a}{b}$, donde $a, b \in \mathbb{Z} - \{0\}$. Entonces

$$\langle q \rangle = \left\langle \frac{a}{b} \right\rangle = \mathbb{Q}.$$

Considere ahora el número $\frac{1}{2b} \in \mathbb{Q}$. Como q genera todos los elementos de $\mathbb{Q}$, entonces

$$\frac{1}{2b} = kq = k\frac{a}{b}, \quad \text{para algún} \quad k \in \mathbb{Z},$$

esto implica

$$ka = \frac{1}{2},$$

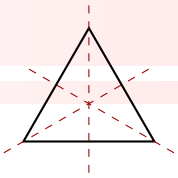
lo cual no puede suceder, pues $a, b \in \mathbb{Z}$. Por lo tanto, se sigue que no existe $q \in \mathbb{Q}$ tal que $\langle q \rangle = \mathbb{Q}$ y así $\mathbb{Q}$ no es cíclico. □

Teorema 2.10.3:

Sea G un grupo y sea $g \in G$. Entonces $\langle g \rangle$ es la intersección de todos los subgrupos de G que contienen a g. Es decir

$$\langle g \rangle = \bigcap_{i \in I} H_i$$

donde $g \in H_i < G$, para todo $i \in I$.



Demostración. Se va utilizar la relación de inclusión para probar la igualdad $\langle g\rangle = \bigcap_{i\in I} H_i$.

- ($\subseteq$) Sea $x \in \langle g\rangle$, entonces x es de la forma g^n para algún $n \in \mathbb{Z}$. Como $g \in H_i$ para todo $i \in I$ y H_i es cerrado por ser subgrupo de G, se cumple que $g^n \in H_i$ para todo $i \in I$, es decir $x \in H_i$ para todo $i \in I$. Esto, a su vez, implica que $x \in \bigcap_{i\in I} H_i$.

- ($\supseteq$) Sea $x \in \bigcap_{i\in I} H_i$. Entonces $x \in H_i$ para todo $i \in I$. Observe que $\langle g\rangle$ es un subgrupo de G que contiene a g. Esto significa que $\langle g\rangle$ es uno de los H_i, lo cual implica que $x \in \langle g\rangle$.

Por lo tanto $\langle g\rangle = \bigcap_{i\in I} H_i$, $g \in H_i < G$, para todo $i \in I$. □

Teorema 2.10.4:

Sea G un grupo y sea $g \in G$ un elemento de orden $|g| = n$. Entonces

$$\langle g\rangle = \left\{e, g, g^2, \dots, g^{n-1}\right\},$$

donde todos los elementos son distintos dos a dos.

Demostración. Se utilizará la relación de inclusión para probar la igualdad. Para ello considere el conjunto

$$A := \left\{e, g, g^2, \dots, g^{n-1}\right\}$$

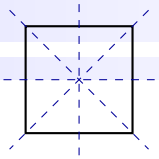
Se probará primero que $\langle g\rangle \subseteq A$ y luego que $\langle g\rangle \supseteq A$.

- ($\subseteq$) Sea $x \in \langle g\rangle$. Entonces x es de la forma

$$x = g^m \quad \text{para algún } m \in \mathbb{Z}.$$

Por el Algoritmo de la División (teorema 1.1.3), existen $q, r \in \mathbb{Z}$ tales que

$$m = qn + r, \quad \text{con } 0 \leq r < n.$$



Entonces,

$$\begin{aligned} g^m &= g^{qn+r} \\ &= g^{qn}g^r, \\ &= (g^n)^q g^r, \\ &= e^q g^r, \quad \text{pues } |g| = n \\ &= eg^r, \\ &= g^r. \end{aligned}$$

Como $0 \leq r < n$, entonces $g^r \in A$ lo cual implica que $g^m \in A$. Por lo tanto $\langle g \rangle \subseteq A$.

- ($\subseteq$) Sea $x \in A$, entonces, en particular, debe existir un $n = 0, 1, 2, 3, \ldots$ tal que $x = g^n$, así $x \in \langle g \rangle$ y por lo tanto $A \subseteq \langle g \rangle$.

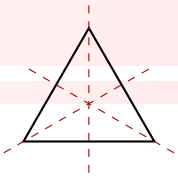
Se debe probar ahora que los elementos del conjunto A son todos distintos dos a dos. Para ello suponga por contradicción que existen dos elementos iguales de este conjunto, es decir,

$$g^k = g^l \quad \text{donde} \quad 0 < k < l \leq n - 1.$$

Entonces,

$$\begin{aligned} g^{l-k} &= g^l g^{-k}, \\ &= g^l (g^k)^{-1}, \quad (g^k = g^l) \\ &= g^l (g^l)^{-1}, \\ &= g^l g^{-l}, \\ &= g^{l-l}, \\ &= g^0, \\ &= e. \end{aligned}$$

Pero como $0 < l - k < n$, esto contradice el hecho de que n es el entero positivo más pequeño tal que $g^n = e$. Por lo tanto $g^{l-k} \neq e$, esto significa que $g^l \neq g^k$ si $l \neq k$ y así todos los elementos de este conjunto son distintos dos a dos. □



Corolario 2.10.1:

Sea G un grupo y sea $g \in G$. Si $|g| = n$, entonces $\left|\langle g \rangle\right| = n$.

Demostración. Por el teorema 2.10.4 anterior se tiene que si $|g| = n$ entonces

$$\langle g \rangle = \left\{ e, g, g^2, \ldots, g^{n-1} \right\}.$$

Note $\langle g \rangle$ tiene n elementos, es decir $\left|\langle g \rangle\right| = n = |g|$. □

Corolario 2.10.2:

Sea G un grupo finito con elemento neutro e. Para cada $g \in G$ se cumple

1. $|g| \Big| |G|$.
2. $g^{|G|} = e$.

Demostración.

1. Por el teorema 2.10.1 se sabe que $\langle g \rangle$ es un subgrupo de G. Luego, por el Teorema de Lagrange (teorema 2.9.4) el orden de $\langle g \rangle$ divide al orden de G. Además, por el corolario anterior, $|\langle g \rangle| = |g|$, por lo tanto $|g| \Big| |G|$.
2. Como $|g| \Big| |G|$, entonces $|G| = k|g|$ para algún $k \in \mathbb{Z}$. Luego

$$g^{|G|} = g^{k|g|} = \left(g^{|g|}\right)^k = e^k = e.$$

□

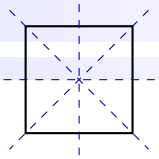
Teorema 2.10.5:

Todo subgrupo de un grupo cíclico, es cíclico.

Demostración. Sea G un grupo cíclico y sea $H < G$, se debe probar que H es cíclico.

Como G es cíclico, G tiene un elemento generador $g \in G$, es decir, $G = \langle g \rangle$. En este punto existen varios casos:

1. Si $H = \{e\}$, entonces $H = \langle e \rangle$ y es inmediato que H es cíclico.
2. Si $H = G$ entonces $H = \langle g \rangle$ y por lo tanto H es cíclico.



3. Si $H \neq \{e\}$ y $H \neq G$. Entonces existe $k \in \mathbb{Z}$ tal que $g^k \in H$ y además $g^k \neq e$. Ahora como $H < G$, H es cerrado, entonces

$$(g^k)^1, (g^k)^2, (g^k)^3, \ldots \in H.$$

De forma similar

$$(g^k)^{-1}, (g^k)^{-2}, (g^k)^{-3}, \ldots \in H.$$

Sea m el menor entero positivo para el cual $g^m \in H$. Se va a probar que $\langle g^m \rangle = H$ mediante la relación de inclusión.
($\subseteq$) Sea $x \in \langle g^m \rangle$, entonces x es de la forma $x = (g^m)^n$ para algún $n \in \mathbb{Z}$. Como $g^m \in H$ y H es cerrado, entonces $(g^m)^n \in H$, es decir $x \in H$ y por lo tanto $\langle g^m \rangle \subseteq H$.
($\supseteq$) Sea $y \in H$. Como $H < G = \langle g \rangle$, entonces y es de la forma $y = g^n$, para algún $n \in \mathbb{Z}$. Por el algoritmo de la división existen $q, r \in \mathbb{Z}$ tales que

$$n = qm + r, \quad \text{con} \;\; 0 \leq r < m. \tag{2.10}$$

Entonces

$$\begin{aligned} g^n &= g^{qm+r}, \\ &= g^{qm} g^r, \end{aligned}$$

así

$$g^r = g^n g^{-qm}$$

Como $g^n \in H$ y $g^{-qm} \in H$, entonces $g^n g^{-qm} \in H$ pues H es cerrrado y por lo tanto $g^r \in H$. Pero, por la desigualdad en (2.10) y el hecho de que m es el menor entero positivo tal que $g^m \in H$, se tiene que necesariamente $r = 0$, lo cual implica, de la igualdad en (2.10), que $n = qm$, entonces

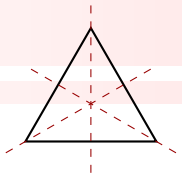
$$g^n = (g^m)^q.$$

De esta forma se cumple que $g^n \in \langle g^m \rangle$, por lo tanto $H \subseteq \langle g^m \rangle$. Finalmente se concluye que $H = \langle g^m \rangle$ y así H es cíclico.

□

Ejemplo 2.10.13.

Considere el grupo $(\mathbb{Z}, +)$. Este es un grupo cíclico con generador 1, es decir $\langle 1 \rangle = \mathbb{Z}$. Por el Teorema



2.7.2, todo subgrupo de $\mathbb{Z}$ es de la forma $m\mathbb{Z}$, entonces, por el teorema anterior $(m\mathbb{Z},+)$ es cíclico. Más aún, observe que $\langle m\rangle = m\mathbb{Z}$, es decir, m es un generador de $m\mathbb{Z}$.

Teorema 2.10.6:

Sea G un grupo finito y cíclico, generado por un elemento $g \in G$ de orden $|g| = n$. Sea $k \in \mathbb{N}$ tal que $(n,k) = 1$, entonces $\left\langle g^k \right\rangle = G$.

Demostración. Como $|g| = n$, entonces, por el corolario 2.10.1, $|\langle g\rangle| = n$ y dado que, por hipótesis $G = \langle g\rangle$, entonces

$$|G| = n \tag{2.11}$$

Por otro lado, como G es finito y $\left\langle g^k \right\rangle$ es subgrupo de G, entonces $\left\langle g^k \right\rangle$ también es finito. Sea m el orden de $\left\langle g^k \right\rangle$, es decir $\left|\left\langle g^k \right\rangle\right| = m$. Para probar que $\left\langle g^k \right\rangle = G$ basta mostrar que que $m = n$, es decir, $\left|\left\langle g^k \right\rangle\right| = |G|$. Por la parte dos del corolario 2.10.2, se tiene

$$e = \left(g^k\right)^{|\langle g^k\rangle|} = \left(g^k\right)^m.$$

Por otro lado, como $|g| = n$ y $g^{km} = (g^k)^m = e$, entonces, por la parte uno del teorema 2.6.1, n divide a km y dado que por hipótesis $(k,n) = 1$, se cumple que

$$n|m. \tag{2.12}$$

Similarmente, como $\left|g^k\right| = m$ y $\left(g^k\right)^n = (g^n)^k = e^k = e$, entonces

$$m|n \tag{2.13}$$

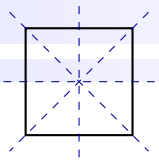
Luego, de las ecuaciones (2.12) y (2.13) se deduce que $m = n$. Lo anterior implica que $\left|\left\langle g^k \right\rangle\right| = n$ y por la igualdad 2.11 se tiene que $\left|\left\langle g^k \right\rangle\right| = |G|$. Esto significa que $\left\langle g^k \right\rangle$ tiene la misma cantidad de elementos que G y como $\left\langle g^k \right\rangle < G$, entonces necesariamente, $\left\langle g^k \right\rangle = G$, lo cual había que demostrar. □

Ejemplo 2.10.14.

Considere el grupo finito $(\mathbb{Z}_7^*,\cdot)$.

1. Verifique que $(\mathbb{Z}_7^*,\cdot)$ es un grupo cíclico generado por [3].
2. Use el teorema 2.10.6 anterior para hallar todos los generadores de $\mathbb{Z}_7^*$ bajo el producto de clases.

Solución.



1. Observe que

$$([3])^1 = [3], \quad ([3])^2 = [2], \quad ([3])^3 = [6], \quad ([3])^4 = [4], \quad ([3])^5 = [5], \quad ([3])^6 = [1].$$

   Por lo tanto [3] genera a $\mathbb{Z}_7^*$ bajo el producto de clases, es decir $\langle [3] \rangle = \mathbb{Z}_7^*$.

2. Usando la notación del teorema 2.10.6 se tiene que $g = [3]$ y además el orden es $|[3]| = 6$, que precisamente también coincide con el orden de $\mathbb{Z}_7^*$, entonces $n = 6$. Ahora, para hallar los elementos de $\mathbb{Z}_7^*$ que generan a $(\mathbb{Z}_7^*, \cdot)$ se debe encontrar los números $k \in \{1, 2, 3, 4, 5, 6\}$ tales que $(6, k) = 1$, es decir, los números menores que 7 que no tienen divisores en común con 6, esto es:

   - Si $k = 1$ se tiene que $(n, k) = (6, 1) = 1$, entonces, por el teorema 2.10.6 , $\langle ([3])^1 \rangle = \mathbb{Z}_7^*$, pero $\langle 1([3])^1 \rangle = \langle [3] \rangle$. Esto implica que $\langle [3] \rangle = \mathbb{Z}_8$, lo cual ya se tenía.
   - Los números $k \in \{2, 3, 4, 6\}$ se descartan porque sí tienen divisores en común con 6.
   - Si $k = 5$ se tiene que $(n, k) = (6, 5) = 1$, entonces, por el teorema 2.10.6 , $\langle [3]^5 \rangle = \mathbb{Z}_7^*$, pero $\langle [3]^5 \rangle = \langle [2] \rangle$. Esto implica que $\langle [2] \rangle = \mathbb{Z}_7^*$. De hecho, por el resultado del ejemplo 2.10.7 se sabe que si un elemento genera a un grupo, su inverso también. En este caso, note que [2] es el inverso de [3].

   Ahora, por el teorema 2.10.6, los elementos que generan a $(\mathbb{Z}_7^*, \cdot)$ son [2] y [3].

□

Observación 2.10.5.

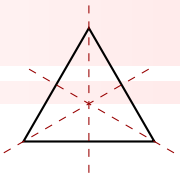
En el caso de la notación de grupos aditivos $(G, +)$ el teorema 2.10.6 se escribe de la siguiente forma: sea $(G, +)$ un grupo finito y cíclico generado por un elemento $g \in G$ de orden $|g| = n$. Sea $k \in \mathbb{N}$ tal que $(n, k) = 1$, entonces $\langle kg \rangle = G$.

Aquí la expresión kg debe entenderse en el sentido de la definición 2.2.1 y la observación 2.2.1:

$$kg = \underbrace{g + g + g + \cdots + g}_{k-veces}.$$

Ejemplo 2.10.15.

Considere el grupo $(\mathbb{Z}_8, +)$, el cual es finito y cíclico. Hallar todos los generadores de $\mathbb{Z}_8$.



Solución. Para encontrar los generadores de $\mathbb{Z}_8$ bajo la suma de clases se usa el teorema 2.10.6 y la observación anterior. Para ello recuerde que

$$\mathbb{Z}_8 := \{[0], [1], [2], [3], [4], [5], [6], [7]\}.$$

Este grupo es de orden $|\mathbb{Z}_8| = 8$, pues tiene 8 elementos. Además, $\mathbb{Z}_8$ es cíclico y el elemento $[1]$ y su inverso $[7]$ son generadores (ver resultado del ejemplo 2.10.7), es decir $\langle [1] \rangle = \mathbb{Z}_8$ y $\langle [7] \rangle = \mathbb{Z}_8$. En la notación del teorema 2.10.6 anterior se tiene que $n = 8$ y $g = [1]$ (también se pudo haber tomado $g = [7]$), entonces, para hallar los elementos de $\mathbb{Z}_8$ que generan a $\mathbb{Z}_8$ bajo la suma se debe hallar los números $k \in \{1, 2, 3, 4, 5, 6, 7\}$ tales que $(8, k) = 1$, es decir, los números menores que 8 y que no tienen divisores en común con él. De hecho, estos números son $k \in \{1, 3, 5, 7\}$. A continuación se analiza cada caso:

- Si $k = 1$ se tiene que $(n, k) = (8, 1) = 1$, entonces, por el teorema 2.10.6, $\langle 1[1] \rangle = \mathbb{Z}_8$, pero $\langle 1[1] \rangle = \langle [1] \rangle$. Esto implica que $\langle [1] \rangle = \mathbb{Z}_8$, lo cual ya se tenía.
- Si $k = 3$ se tiene que $(n, k) = (8, 3) = 1$, entonces, por el teorema 2.10.6, $\langle 3[1] \rangle = \mathbb{Z}_8$, pero $\langle 3[1] \rangle = \langle [3] \rangle$, por lo tanto $\langle [3] \rangle = \mathbb{Z}_8$. Es decir, $[3]$ también es un generador de $\mathbb{Z}_8$.
- Si $k = 5$ se tiene que $(n, k) = (8, 5) = 1$, entonces, por el teorema 2.10.6, $\langle 5[1] \rangle = \mathbb{Z}_8$, pero $\langle 5[1] \rangle = \langle [5] \rangle$, por lo tanto $\langle [5] \rangle = \mathbb{Z}_8$. Es decir, $[5]$ también es un generador de $\mathbb{Z}_8$.
- Si $k = 7$ se tiene que $(n, k) = (8, 7) = 1$, entonces, por el teorema 2.10.6, $\langle 7[1] \rangle = \mathbb{Z}_8$, pero $\langle 7[1] \rangle = \langle [7] \rangle$, por lo tanto $\langle [7] \rangle = \mathbb{Z}_8$. Es decir $[7]$ también es un generador de $\mathbb{Z}_8$, sin embargo, ya este se tenía.

Como no hay más primos relativos con 8, se concluye que los elementos $[1], [3], [5], [7]$ son los generadores de de $\mathbb{Z}_8$. Es decir,

$$\langle [1] \rangle = \langle [3] \rangle = \langle [5] \rangle = \langle [7] \rangle = \mathbb{Z}_8.$$

□

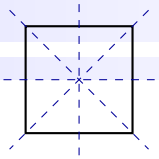
Ejemplo 2.10.16.

Halle todos los subgrupos de $(\mathbb{Z}_8, +)$.

Solución. Del ejemplo anterior se tiene que los subgrupos generados por $[1], [3], [5], [7]$ son el mismo $\mathbb{Z}_8$. Es decir:

$$\langle [1] \rangle = \langle [3] \rangle = \langle [5] \rangle = \langle [7] \rangle = \mathbb{Z}_8.$$

En este punto se debe analizar los otros casos, es decir, $\langle [0] \rangle$, $\langle [2] \rangle$, $\langle [4] \rangle$ y $\langle [6] \rangle$.



- Primero, note que el subgrupo generado por [0] es $\langle[0]\rangle = \{[0]\}$, es decir, es un subgrupo trivial.

- Segundo, note que

$$([2])^1 = 1[2] = [2], \quad ([2])^2 = 2[2] = [4], \quad ([2])^3 = 3[2] = [6], \quad ([2])^4 = 4[2] = [0] \ldots$$

De acuerdo con esta información se tendría que

$$\langle[2]\rangle = \{[0], [2], [4], [6]\},$$

el cual es un subgrupo ya que basta con observar que es cerrado (ver teorema 2.7.3). Ahora, se repite el razonamiento de teorema 2.10.6 usado anteriormente para $\mathbb{Z}_8$, esta vez con el subgrupo de $\mathbb{Z}_8$ generado por [2]. En otras palabras, el subgrupo $\langle[2]\rangle$ juega el papel de $\mathbb{Z}_8$ en el ejemplo anterior. Así, se desea determinar cuáles elementos de $\langle[2]\rangle$ generan a $\langle[2]\rangle$. Para ello, observe que $\langle[2]\rangle$ es un subgrupo de orden $|\langle[2]\rangle| = 4$ pues tiene cuatro elementos. En la notación del teorema 2.10.6, $n = 4$ y $g = [2]$. Por otro lado, los primos relativos con 4 son $k = 1, 3$. De esta forma:

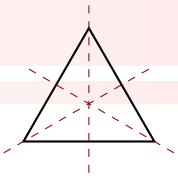
  - Si $k = 1$ se tiene que $(n, k) = (4, 1) = 1$, entonces, por el teorema 2.10.6, $\langle 1[2]\rangle = \langle[2]\rangle$, pero $\langle 1[2]\rangle = \langle[2]\rangle$, por lo tanto $\langle[2]\rangle = \langle[2]\rangle$, lo cual ya se sabía.
  - Si $k = 3$ se tiene que $(n, k) = (4, 3) = 1$, entonces por el teorema 2.10.6, $\langle 3[2]\rangle = \langle[2]\rangle$, pero $\langle 3[2]\rangle = \langle[2] + [2] + [2]\rangle = \langle[6]\rangle$, por lo tanto $\langle[6]\rangle = \langle[2]\rangle$. Es decir, [6] también es un generador de $\langle[2]\rangle$.

Dado que no hay más primos relativos con 4 (menores que 4), se cumple que [2] y [6] generan el mismo subgrupo de $\mathbb{Z}_8$

- Tercero, no es difícil verificar que

$$\langle[4]\rangle = \{[0], [4]\}$$

el cual es un subgrupo pues basta con notar que es cerrado (ver teorema 2.7.3). Luego, se repite el razonamiento del teorema 2.10.6 con el subgrupo de $\mathbb{Z}_8$ generado por [4]. En otras palabras, en este caso, el subgrupo $\langle[4]\rangle$ juega el papel de $\mathbb{Z}_8$ en el ejemplo anterior. Así, se desea saber cuáles elementos de $\langle[4]\rangle$ generan $\langle[4]\rangle$. En este caso $\langle[4]\rangle$ es un subgrupo de orden $|\langle[4]\rangle| = 2$ pues tiene 2 elementos. En la notación del teorema 2.10.6, $n = 2$ y $g = [4]$. Por otro lado, el único primo relativo con 2 (menor que 2) es $k = 1$. Pero si $k = 1$ cumple que que $(n, k) = (2, 1) = 1$, entonces $\langle 1[4]\rangle = \langle[4]\rangle$, pero $\langle 1[4]\rangle = \langle[4]\rangle$, por lo tanto $\langle[4]\rangle = \langle[4]\rangle$. lo cual ya se tenía.



- Cuarto, se debe analizar el subgrupo generado por [6], sin embargo, en el segundo paso se había concluido que $\langle [6] \rangle = \langle [2] \rangle$.

De esta forma, se han encontrado los subgrupos que genera cada clase de $\mathbb{Z}_8$:

$$\langle [0] \rangle, \qquad \langle [1] \rangle = \langle [3] \rangle = \langle [5] \rangle = \langle [7] \rangle = \mathbb{Z}_8, \qquad \langle [2] \rangle = \langle [6] \rangle, \qquad \langle [4] \rangle.$$

Por lo tanto, los subgrupos de $\mathbb{Z}_8$ son

$$\{[0]\}, \quad \langle [2] \rangle, \quad \langle [4] \rangle, \quad \mathbb{Z}_8.$$

Observe que los órdenes de los subgrupos de $\mathbb{Z}_8$ son $1, 2, 4$ y 8, precisamente son divisores de 8, cumpliendo con el teorema 2.9.4 (Teorema de Lagrange). □

Ejemplo 2.10.17.

Halle todos los subgrupos de $(\mathbb{Z}_{18}, +)$.

Solución. Por el resultado del ejemplo 2.10.11 se sabe que $(\mathbb{Z}_{18}, +)$ es generado por [1] y por [17]. Además, observe que $\mathbb{Z}_{18}$ es de orden 18 y los primos relativos con 18 y menores que 18 son $1, 5, 7, 11, 13, 17$. Considerando que [1] genera al grupo $(\mathbb{Z}_{18}, +)$ y siguiendo el mismo razonamiento del ejemplo anterior se tiene que

$$\langle [1] \rangle = \langle [5] \rangle = \langle [7] \rangle = \langle [11] \rangle = \langle [13] \rangle = \langle [17] \rangle = \mathbb{Z}_{18}.$$

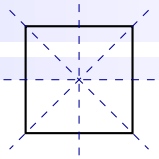
Ahora, se debe valorar qué ocurre con los generados por [0], [2], [3], [4], [6], [8], [9], [10], [12], [14], [15] y [16].

- Primero, y evidentemente, el subgrupo generado por [0] es $\langle [0] \rangle = \{[0]\}$.
- Segundo, se considera el conjunto generado por [2], el cual es:

  $$\langle [2] \rangle = \{[0], [2], [4], [6], [8], [10], [12], [14], [16]\},$$

  el cual es un subgrupo ya que es cerrado (ver teorema 2.7.3). Ahora, se determina cuáles elementos de $\langle [2] \rangle$ generan también a $\langle [2] \rangle$. En este caso el orden de $\langle [2] \rangle$ es 9, pues tiene 9 elementos. Los primos relativos con 9, menores que 9, son $1, 2, 4, 5, 7$ y 8. De esta forma, por el teorema **??** se tiene que:

  - $\langle 1[2] \rangle = \langle [2] \rangle$. es decir $\langle [2] \rangle = \langle [2] \rangle$, que ya se tenía.
  - $\langle 2[2] \rangle = \langle [2] \rangle$, lo cual es equivalente a $\langle [4] \rangle = \langle [2] \rangle$.



- $\langle 4[2]\rangle = \langle [2]\rangle$, lo cual es equivalente a $\langle [8]\rangle = \langle [2]\rangle$.
- $\langle 5[2]\rangle = \langle [2]\rangle$, lo cual es equivalente a $\langle [10]\rangle = \langle [2]\rangle$.
- $\langle 7[2]\rangle = \langle [2]\rangle$, lo cual es equivalente a $\langle [14]\rangle = \langle [2]\rangle$.
- $\langle 8[2]\rangle = \langle [2]\rangle$, lo cual es equivalente a $\langle [16]\rangle = \langle [2]\rangle$.

Por lo tanto, los elementos de $\mathbb{Z}_{18}$ que generan $\langle [2]\rangle$ son [2], [4], [8], [10], [14] y [16]. Es decir,

$$\langle [2]\rangle = \langle [4]\rangle = \langle [8]\rangle = \langle [10]\rangle = \langle [14]\rangle = \langle [16]\rangle .$$

- Tercero, se considera el conjunto generado por [3], el cual es:

$$\langle [3]\rangle = \{[0], [3], [6], [9], [12], [15]\},$$

el cual es un subgrupo ya que es cerrado (ver teorema 2.7.3). Se va a determinar cuáles elementos de $\langle [3]\rangle$ generan también a $\langle [3]\rangle$. Note que el orden de $\langle [3]\rangle$ es 6, pues tiene 6 elementos. Los primos relativos con 6, menores que 6, son 1 y 5. De esta forma, por el teorema 2.10.6 se tiene que:

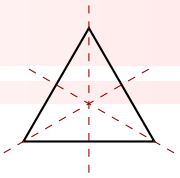
- $\langle 1[3]\rangle = \langle [3]\rangle$. Es decir $\langle [3]\rangle = \langle [3]\rangle$, la cual ya se tenía.
- $\langle 5[3]\rangle = \langle [3]\rangle$, lo cual es equivalente a $\langle [15]\rangle = \langle [3]\rangle$.

Por lo tanto, los elementos de $\mathbb{Z}_{18}$ que generan $\langle [3]\rangle$ son [3] y [15]. Es decir

$$\langle [15]\rangle = \langle [3]\rangle .$$

- Cuarto, se considera el conjunto generado por [4], pero por el segundo paso se sabe que $\langle [4]\rangle = \langle [2]\rangle$.
- Quinto, el conjunto que sigue por analizar es el generado por [6], más aún, en el tercer paso se concluyó que $\langle [6]\rangle = \langle [3]\rangle$.
- Sexto, se debe analizar el conjunto generado por [8], pero ya se tiene que $\langle [8]\rangle = \langle [2]\rangle$ por el segundo paso.
- Séptimo, se considera el conjunto generado por [9], esto es:

$$\langle [9]\rangle = \{[0], [9]\}.$$



Es claro que es cerrado y por lo tanto es un subgrupo. Se quiere determinar cuáles elementos de $\langle[9]\rangle$ generan también a $\langle[9]\rangle$. Pero como $[0]$ no puede generar $\langle[9]\rangle$, entonces este subgrupo solamente tiene como generador a la clase $[9]$.

- Octavo, por los datos obtenidos en los pasos anteriores ya se sabe que $\langle[10]\rangle = \langle[2]\rangle$, $\langle[12]\rangle = \langle[3]\rangle$, $\langle[14]\rangle = \langle[2]\rangle$, $\langle[15]\rangle = \langle[3]\rangle$ y $\langle[16]\rangle = \langle[2]\rangle$

En conclusión, los subgrupos de $\mathbb{Z}_{18}$ son los siguientes:

$$\begin{aligned}
\langle[0]\rangle &= \{[0]\}.\\
\langle[1]\rangle &= \langle[5]\rangle = \langle[7]\rangle = \langle[11]\rangle = \langle[13]\rangle = \langle[17]\rangle = \mathbb{Z}_{18}.\\
\langle[2]\rangle &= \langle[4]\rangle = \langle[8]\rangle = \langle[10]\rangle = \langle[14]\rangle = \langle[16]\rangle.\\
\langle[3]\rangle &= \langle[15]\rangle\\
\langle[9]\rangle
\end{aligned}$$

Finalmente, los subgrupos de $\mathbb{Z}_{18}$ son

$$\{[0]\},\quad \langle[2]\rangle,\quad \langle[3]\rangle,\quad \langle[9]\rangle,\quad \mathbb{Z}_{18}.$$

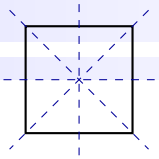
Observe que el orden de cada subgrupo ($1, 2, 6$ y 9), corresponde a un divisor del orden del grupo, es decir, son divisores de 18, cumpliendo con el teorema 2.9.4 (Teorema de Lagrange). □

Ejemplo 2.10.18.

El grupo $(\mathbb{Z}_{20}, +)$ tienes los siguientes subgrupos:

$$\begin{aligned}
\langle[0]\rangle &= \{0\},\\
\langle[1]\rangle &= \mathbb{Z}_{20},\\
\langle[2]\rangle &= \{0, 2, 4, \ldots, 16, 18\},\\
\langle[4]\rangle &= \{0, 4, 8, 12, 16\},\\
\langle[5]\rangle &= \{0, 5, 10, 15\},\\
\langle[10]\rangle &= \{0, 10\}.
\end{aligned}$$

Observe que el orden de estos subgrupos es 1, 20, 10, 5, 2, respectivamente y además el orden de cada uno de estos subgrupos, corresponde a un divisor del orden del grupo, verificando el resultado del teorema 2.9.4 (Teorema de Lagrange).



2.11 Subgrupos Normales

Los subgrupos normales fueron introducidos por Evaristo Galois en el año 1832. Básicamente, si H es un subgrupo de G, H es un subgrupo normal si cada clase izquierda de este grupo es igual a la correspondiente clase derecha.

El objetivo de esta sección es definir el grupo cociente G/N, que consiste en el conjunto de clases izquierdas inducidas por un subgrupo N. Si se considera el conjunto de clases que se obtienen de un subgrupo en un grupo dado y se le trata a este conjunto de dotarlo de una estructura de grupos, en general no es posible a menos que el subgrupo dado sea normal.

Definición 2.11.1:

Sea G un grupo y sea N un subgrupo de G. Se dice que N es un **subgrupo normal** si para cada $x \in G$ se tiene

$$x^{-1}Nx \subseteq N$$

Si N es un subgrupo normal de G se denota $N \lhd G$ o bien $N \ll G$.

Observación 2.11.1.

1. Recuerde que que el conjunto $x^{-1}Nx$ se define por

$$x^{-1}Nx := \{x^{-1}nx : x \in G,\ n \in N\}.$$

   Entonces, de acuerdo con la definición anterior, $N \lhd G$ si para cada $x \in G$ y cada $n \in N$, se tiene $x^{-1}nx \in N$.

2. En el caso de la notación de grupos aditivos $(G, +)$, un subgrupo N de G se llama **normal** si para cada $x \in G$ se tiene

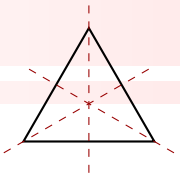
$$-x + N + x \subseteq N,$$

   donde

$$-x + N + x := \{-x + n + x \ : \ x \in G,\ n \in N\}.$$

3. Sea G un grupo y sea N un subgrupo normal de G. Esto es

$$x^{-1}Nx \subseteq N, \quad \text{para todo} \quad x \in G.$$



Como la inclusión anterior se cumple para todo $x \in G$, también se cumple para x^{-1}, es decir

$$(x^{-1})^{-1} N x^{-1} \subseteq N,$$

por lo que

$$xNx^{-1} \subseteq N, \quad \text{para todo} \quad x \in G.$$

En otras palabras, si $N \lhd G$ entonces se cumple tanto $x^{-1}Nx \subseteq N$ como $xNx^{-1} \subseteq N$, para cada $x \in G$.

Ejemplo 2.11.1.

Considere el grupo de Klein $K = \{e, h, r, v\}$ y considere el subgrupo $N = \{e, h\}$. Pruebe que $N \lhd G$.

Demostración. Se debe probar que para cada $x \in K$, se tiene $x^{-1}Nx \subseteq N$. En efecto,

$$\begin{aligned}
e^{-1}Ne &= \{e^{-1}\circ e\circ e,\ e^{-1}\circ h\circ e\} = \{e, h\} = N \subseteq N.\\
h^{-1}Nh &= \{h^{-1}\circ e\circ h,\ h^{-1}\circ h\circ h\} = \{e, h\} = N \subseteq N.\\
r^{-1}Nr &= \{r^{-1}\circ e\circ r,\ r^{-1}\circ h\circ r\} = \{e, h\} = N \subseteq N.\\
v^{-1}Nv &= \{v^{-1}\circ e\circ v,\ v^{-1}\circ h\circ v\} = \{e, h\} = N \subseteq N.
\end{aligned}$$

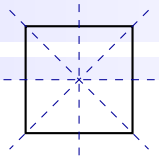
Por lo tanto se cumple que $N \lhd K$. □

Ejemplo 2.11.2.

Considere el grupo simétrico $S_3 = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$ del ejemplo 2.1.30, donde tabla de S_3 con la operación composición usual de funciones corresponde a:

$\circ$	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_1	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_2	σ_2	σ_1	σ_4	σ_3	σ_6	σ_5
σ_3	σ_3	σ_5	σ_1	σ_6	σ_2	σ_4
σ_4	σ_4	σ_6	σ_2	σ_5	σ_1	σ_3
σ_5	σ_5	σ_3	σ_6	σ_1	σ_4	σ_2
σ_6	σ_6	σ_4	σ_5	σ_2	σ_3	σ_1

Sea $H := \{\sigma_1, \sigma_4, \sigma_5\}$. No es difícil comprobar que H es un subgrupo de S_3. Verifique que H es normal.



Demostración. Se debe probar las seis conjuntos

$$\sigma_1^{-1}H\sigma_1,\ \sigma_2^{-1}H\sigma_2,\ \sigma_3^{-1}H\sigma_3,\ \sigma_4^{-1}H\sigma_4,\ \sigma_5^{-1}H\sigma_5 \quad \text{y} \quad \sigma_6^{-1}H\sigma_6$$

son subconjuntos de H. Para ello, observe que

$$\begin{aligned}
\sigma_1^{-1}H\sigma_1 &= \{\sigma_1^{-1}\circ\sigma_1\circ\sigma_1, \sigma_1^{-1}\circ\sigma_4\circ\sigma_1, \sigma_1^{-1}\circ\sigma_5\circ\sigma_1\} = \{\sigma_1, \sigma_4, \sigma_5\} = H \subseteq H.\\
\sigma_2^{-1}H\sigma_2 &= \{\sigma_2^{-1}\circ\sigma_1\circ\sigma_2, \sigma_2^{-1}\circ\sigma_4\circ\sigma_2, \sigma_2^{-1}\circ\sigma_5\circ\sigma_2\} = \{\sigma_1, \sigma_5, \sigma_4\} = H \subseteq H.\\
\sigma_3^{-1}H\sigma_3 &= \{\sigma_3^{-1}\circ\sigma_1\circ\sigma_3, \sigma_3^{-1}\circ\sigma_4\circ\sigma_3, \sigma_3^{-1}\circ\sigma_5\circ\sigma_3\} = \{\sigma_1, \sigma_5, \sigma_4\} = H \subseteq H.\\
\sigma_4^{-1}H\sigma_4 &= \{\sigma_4^{-1}\circ\sigma_1\circ\sigma_4, \sigma_4^{-1}\circ\sigma_4\circ\sigma_4, \sigma_4^{-1}\circ\sigma_5\circ\sigma_4\} = \{\sigma_1, \sigma_4, \sigma_5\} = H \subseteq H.\\
\sigma_5^{-1}H\sigma_5 &= \{\sigma_5^{-1}\circ\sigma_1\circ\sigma_5, \sigma_5^{-1}\circ\sigma_4\circ\sigma_5, \sigma_5^{-1}\circ\sigma_5\circ\sigma_5\} = \{\sigma_1, \sigma_5, \sigma_4\} = H \subseteq H.\\
\sigma_6^{-1}H\sigma_6 &= \{\sigma_6^{-1}\circ\sigma_1\circ\sigma_6, \sigma_6^{-1}\circ\sigma_4\circ\sigma_6, \sigma_6^{-1}\circ\sigma_5\circ\sigma_6\} = \{\sigma_1, \sigma_5, \sigma_4\} = H \subseteq H.
\end{aligned}$$

Por lo tanto se cumple que $H \lhd S_3$. □

Ejemplo 2.11.3.

Considere el mismo grupo simétrico S_3 del ejemplo anterior. Sea $H := \{\sigma_1, \sigma_6\}$. No es difícil comprobar que H es un subgrupo de S_3. Compruebe que H no es normal.

Demostración. Para comprobar que H no es un subgrupo normal de S_3 basta con encontrar un elemento $x \in S_3$ tal que $x^{-1}Hx \nsubseteq H$. Para ver esto, tome $x = \sigma_4$ y note que:

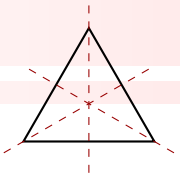
$$\begin{aligned}
\sigma_4^{-1}H\sigma_4 &= \{\sigma_4^{-1}\circ\sigma_1\circ\sigma_4,\ \ \sigma_4^{-1}\circ\sigma_6\circ\sigma_4\}\\
&= \{\sigma_1, \sigma_5\circ\sigma_6\circ\sigma_4\}\\
&= \{\sigma_1, \sigma_2\circ\sigma_4\}\\
&= \{\sigma_1, \sigma_3\} \nsubseteq H.
\end{aligned}$$

Por lo tanto, $H \ntriangleleft S_3$. □

Ejemplo 2.11.4.

Pruebe que $H = \{x \in \mathbb{R} : x = \log b, b \in \mathbb{Q}^+\}$ es subgrupo normal de $(\mathbb{R}, +)$.

Demostración. Primero se debe probar que H es un subgrupo de $\mathbb{R}^+$ bajo la suma usual. Para ello, considere $x = \log b$ y $y = \log c$ dos elementos en H, con $a, b \in \mathbb{Q}^+$. Note que el inverso bajo al suma de $y = \log c$ es



$$-y = -\log c = \log c^{-1} = \log \frac{1}{c} \text{ con } \frac{1}{c} \in \mathbb{Q}^+.$$

Se debe probar que $x + -y \in H$. En efecto,

$$x + -y = \log b + \log \frac{1}{c} = \log \frac{b}{c} \text{ donde } \frac{b}{c} \in \mathbb{Q}^+.$$

De es forma $(H, +) < (\mathbb{R}, +)$. Falta probar que H es normal, para lo cual sea $z \in \mathbb{R}$ y note que

$$-z + H + z = -z + H + z = H \subseteq H.$$

Por lo tanto se concluye que $(H, +) \lhd (\mathbb{R}, +)$. □

Teorema 2.11.1:

Sea $(G, \cdot)$ un grupo. Las siguientes afirmaciones son equivalentes

1. N es un subgrupo normal de G.
2. $x^{-1}Nx = N$, para todo $x \in G$.
3. $xN = Nx$, para todo $x \in G$.

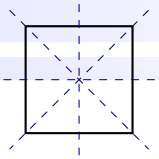
Demostración. Se debe probar que la afirmación uno implica la afirmación dos, que la dos implica la tres y que la tres implica la uno:

(1) $\Rightarrow$ (2). Suponga que $N \lhd G$. Se va a probar que $x^{-1}Nx = N$, para todo $x \in G$. Ahora, como $N \lhd G$ entonces $x^{-1}Nx \subseteq N$ para todo $x \in G$. Falta probar la otra inclusión, es decir, falta probar que $N \subseteq x^{-1}Nx$ para todo $x \in G$. Para ello, sea $n \in N$ y sea $x \in G$, por el punto tres de la observación 2.11.1 se tiene que $xnx^{-1} \in N$. Luego, con este resultado se cumple que

$$x^{-1}(xnx^{-1})x \in x^{-1}Nx,$$

lo cual implica que $n \in x^{-1}Nx$, es decir $N \subseteq x^{-1}Nx$. Por lo tanto, se concluye que $x^{-1}Nx = N$, para todo $x \in G$.

(2) $\Rightarrow$ (3). Suponga que $x^{-1}Nx = N$, para todo $x \in G$, se debe mostrar que $xN = Nx$, para todo



$x \in G$. Con este fin, observe que:

$$\begin{aligned} & x^{-1}Nx = N \\ \Rightarrow\ & x(x^{-1}Nx) = xN \\ \Rightarrow\ & (xx^{-1})Nx = xN \\ \Rightarrow\ & e(Nx) = xN \\ \Rightarrow\ & Nx = xN. \end{aligned}$$

(3) $\Rightarrow$ (1). Suponga que $xN = Nx$, para todo $x \in G$, realizando un proceso análogo al anterior se concluye que $x^{-1}Nx = N$, para todo $x \in G$, en particular $x^{-1}Nx \subseteq N$, para todo $x \in G$, lo que equivale a que $N \lhd G$. □

Ejemplo 2.11.5.

Considere nuevamente el grupo $(S_3, \circ)$, donde

$$S_3 = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}.$$

Sea $H := \{\sigma_1, \sigma_2\}$ y observe que $H < S_3$, sin embargo, H no es un subgrupo normal de S_3. Para verificar esto, en particular note que clase izquierda de H en S_3 determinada por σ_3 es

$$\sigma_3 \circ H = \{\sigma_3 \circ \sigma_1, \sigma_3 \circ \sigma_2\} = \{\sigma_3, \sigma_5\}.$$

Además, la clase derecha de H en S_3 determinada por σ_3 es

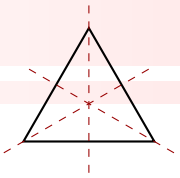
$$H \circ \sigma_3 = \{\sigma_1 \circ \sigma_3,\ \sigma_2 \circ \sigma_3\} = \{\sigma_3, \sigma_4\}$$

Es claro que $\sigma_3\ H \neq H\ \sigma_3$, y por el teorema 2.11.1 anterior se concluye que $H \not\lhd S_3$.

Teorema 2.11.2:

Si G es un grupo abeliano y N es subgrupo de G, entonces N es un subgrupo normal de G, es decir, todo subgrupo de un grupo abeliano es normal.

Demostración. Sea G un grupo abeliano y sea $N < G$, se debe probar que $N \lhd G$. Para ello, sea $x \in G$



y note que:

$$\begin{aligned} x^{-1}Nx &= \{x^{-1}nx \ : \ n \in N\}, \\ &= \{x^{-1}xn \ : \ n \in N\}, \quad \text{porque } G \text{ es abeliano y } x, n \in G. \\ &= \{n \ : \ n \in N\} \\ &= N. \end{aligned}$$

Así N es un subgrupo normal de G. □

Ejemplo 2.11.6.

Considere los siguientes ejemplos:

1. El grupo de Klein es abeliano, de modo que todos sus subgrupos son normales.
2. El grupo $(\mathbb{Z}_n, +)$ es abeliano, por lo que todos sus subgrupos son normales.
3. El grupo $(\mathbb{Z}, +)$ es abeliano, de modo que todos sus subgrupos son normales.
4. Los grupos $(\mathbb{Z}_p^*, \cdot)$ y $(U_n, \cdot)$ son abelianos, entonces todos sus subgrupos son normales.

Teorema 2.11.3:

Sea G un grupo y sea H un subgrupo de G, de índice 2. Entonces, H es un subgrupo normal de G.

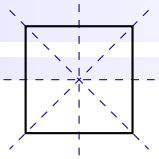
Demostración. Sea $g \in G$, entonces puede ocurrir que $g \in H$ o bien $g \notin H$:

- Si $g \in H$, se cumple que $gH = H = Hg$.
- Si $g \notin H$, es decir, $g \in G - H$, entonces $gH \cap H = \emptyset$, y como solo hay dos clases laterales en que el subgrupo H particiona a G, se concluye que $gH = G - H = Hg$.

En ambos casos $gH = Hg$, por lo tanto y por la parte tres del teorema 2.11.1, H es un subgrupo normal de G. □

Teorema 2.11.4:

Si H es un subgrupo finito de G y si H es el único subgrupo de orden tal que $| \ H \ | = n$, entonces $H \lhd G$.



Demostración. Sea $g \in G$, se va probar primero que $g^{-1}Hg$ es un subgrupo de G. Para ello, tome dos elementos $a, b \in g^{-1}Hg$, de esta forma se puede escribir como $a = g^{-1}h_1g$ y $b = g^{-1}h_2g$ con $h_1, h_2 \in H$, entonces

$$\begin{aligned} ab^{-1} &= (g^{-1}h_1g)(g^{-1}h_2g)^{-1} \\ &= (g^{-1}h_1g)(h_2g)^{-1}(g^{-1})^{-1} \\ &= (g^{-1}h_1g)(g^{-1}h_2^{-1}g) \\ &= g^{-1}h_1h_2^{-1}g. \end{aligned}$$

Es decir, $ab^{-1} \in g^{-1}Hg$, lo cual permite concluir que $g^{-1}Hg < G$. Por otro lado, suponga que $H = \{e, h_1, \ldots, h_{n-1}\}$, entonces

$$g^{-1}Hg = \{g^{-1}eg, g^{-1}h_1g, \ldots, g^{-1}h_{n-1}g\} = \{e, g^{-1}h_1g, \ldots, g^{-1}h_{n-1}g\}.$$

Observe que H y $g^{-1}Hg$ tienen la misma cardinalidad o número de elementos, entonces por hipótesis $|g^{-1}Hg| = n = |H|$ y dado que H es el único subgrupo de G de orden n, se sigue que $g^{-1}Sg = S$. Finalmente, como lo anterior se cumple para un elemento cualquiera $g \in G$, entonces se puede concluir que $H \lhd G$. □

Observación 2.11.2.

En un grupo no abeliano G, deben existir al menos un par de elementos tales que $xy \neq yx$. Sin embargo, existen grupos no abelianos que tienen subgrupos abelianos, por ejemplo el elemento neutro conmuta con cada elemento del grupo, con lo cual $\{e\}$ es un subgrupo abeliano de G. Esta idea se extiende al considerar el conjunto de los elementos de un grupo que conmutan con todos los elementos del grupo.

Definición 2.11.2:

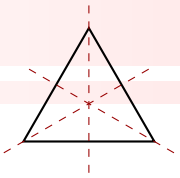
Sea G un grupo, se define el **centro** de G por

$$Z(G) := \{g \in G \ : \ gx = xg, \text{ para todo } x \in G\}.$$

Un elemento $g \in Z(G)$ se llama **un elemento central** de G.

Ejemplo 2.11.7.

Si G es un grupo abeliano, entonces para cada $g \in G$, se tiene $gx = xg$ para todo $x \in G$. Esto significa que cada elemento de G pertenece al centro de G, por lo tanto $Z(G) = G$.



Ejemplo 2.11.8.

Considere el grupo $(GL(2,\mathbb{R}),\cdot)$, donde $GL(2,\mathbb{R}) := \{A \in M(2,\mathbb{R}) : \det A \neq 0\}$. Este grupo se estudió en el ejemplo 2.1.33. Halle el centro $Z\big(GL(2,\mathbb{R})\big)$ de $GL(2,\mathbb{R})$.

Solución. Sea $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ una matriz en el centro de $GL(2,\mathbb{R})$ y sea

$$X = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$$

una matriz $GL(2,\mathbb{R})$. Como $A \in Z\big(GL(2,\mathbb{R})\big)$, entonces

$$AX = XA,$$

es decir,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} x & y \\ z & w \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

lo cual equivale a

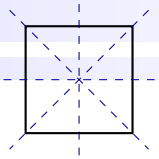
$$\begin{pmatrix} ax+bz & ay+bw \\ cx+dz & cy+dw \end{pmatrix} = \begin{pmatrix} xa+yc & xb+yd \\ za+wc & zb+wd \end{pmatrix}.$$

Igualando las entradas respectivas se obtienen el siguiente sistema de ecuaciones lineales con incógnitas x, y, z y w.

$$\begin{cases} ax+bz &= xa+yc \\ ay+bw &= xb+yd \\ cx+dz &= za+wc \\ cy+dw &= zb+wd \end{cases},$$

el cual se simplifica quedando el sistema homogéneo de la forma

$$\begin{cases} -cy+bz &= 0 \\ -bx+(a-d)y+bw &= 0 \\ cx+(d-a)z-cw &= 0 \end{cases}$$



De acá se concluye que $a = d$, $b = c = 0$. Por lo tanto,

$$Z\big(GL(2,\mathbb{R})\big) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in \mathbb{R} \right\}.$$

□

Ejemplo 2.11.9.

En el caso del grupo S_3, el único elemento de S_3, que conmuta con todos los demás elementos de S_3, es σ_1. Entonces $Z(S_3) = \{\sigma_1\}$.

Teorema 2.11.5:

Sea G un grupo, entonces se tiene que $Z(G)$ es un subgrupo abeliano de G.

Demostración. Primero se debe probar que $Z(G) < G$. Para ello se va utilizar la parte dos de la observación 2.7.2, esto es:

1. Sean $a, b \in Z(G)$ y sea x un elemento cualesquiera de G, note que

   $$(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab).$$

   Por lo tanto $ab \in Z(G)$, es decir, la operación es cerrada.

2. Sea $a \in Z(G)$ y sea x un elemento cualesquiera de G, note que $ax = xa$. Multiplicando por a^{-1} por la derecha y por la izquierda de ambos lados de la igualdad se tiene que $a^{-1}x = xa^{-1}$, con lo cual $a^{-1} \in Z(G)$.

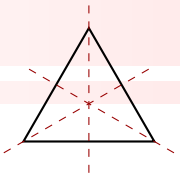
Por lo anterior se concluye que $Z(G)$ es un subgrupo de G. Además $Z(G)$ es abeliano, pues sus elementos conmutan con todos los elementos de G, luego, en particular, conmutan con los del centro de G. □

Teorema 2.11.6:

Sea G un grupo, entonces $Z(G)$ es un subgrupo normal de G.

Demostración. Del teorema anterior se tienen que $Z(G) < G$, falta probar que es normal. Para ello note que

$$g^{-1}Z(G)g := \{g^{-1}zg : z \in Z(G)\}.$$



Luego, sea $x \in g^{-1}Z(G)g$, entonces, para algún $z \in Z(G)$ se cumple que

$$x = g^{-1}zg = g^{-1}(zg) = g^{-1}(gz) = (g^{-1}g)z = ez = z.$$

Es decir, $x \in Z(G)$, por lo tanto $g^{-1}Z(G)g \subseteq Z(G)$, lo que concluye que $Z(G) \lhd G$. □

Definición 2.11.3:

Sea G un grupo y sea $g \in G$, se define el **centralizador** de g en G por

$$Z_G(g) = \{x \in G : xg = gx\}.$$

Observe que el centralizador $Z_G(g)$ de g en G, es el conjunto de todos los elementos de G, que conmutan con g.

Ejemplo 2.11.10.

Si G es un grupo abeliano y si $g \in G$, es claro que $xg = gx$ para cada $x \in G$, entonces $Z_G(g) = G$.

Ejemplo 2.11.11.

Considere el grupo simétrico $(S_3, \circ)$ del ejemplo 2.1.30, donde $S_3 = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$.

1. Puesto que todos los elementos de S_3 conmutan con σ_1, se tiene que $Z_{S_3}(\sigma_1) = S_3$.
2. Los elementos de S_3 conmutan con σ_2, son σ_1 y σ_2, por lo que $Z_{S_3}(\sigma_2) = \{\sigma_1, \sigma_2\}$.
3. Los elementos de S_3 conmutan con σ_3, son σ_1 y σ_3 por lo que $Z_{S_3}(\sigma_3) = \{\sigma_1, \sigma_3\}$.
4. Análogamente se tiene que:

$$Z_{S_3}(\sigma_4) = \{\sigma_1, \sigma_4, \sigma_5\}, \quad Z_{S_3}(\sigma_5) = \{\sigma_1, \sigma_4, \sigma_5\}, \quad Z_{S_3}(\sigma_6) = \{\sigma_1, \sigma_6\}.$$

Ejemplo 2.11.12.

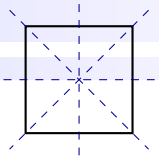
Sea G un grupo y sea $g \in G$, entonces $Z_G(g)$ es un subgrupo de G.

Demostración. Para probar que $Z_G(g) < G$ se va a utilizar la parte dos de la observación 2.7.2:

1. Sean $a, b \in Z_G(g)$, entonces $ag = ga$ y $bg = gb$. Con ello note que

$$(ab)g = a(bg) = a(gb) = (ag)b = (ga)b = g(ab).$$

Así, ab conmuta con g y por lo tanto $ab \in Z_G(g)$.



2. Sea $a \in Z_G(g)$, entonces $ag = ga$, se multiplica esta expresión por a^{-1} tantos por la izquierda y derecha y a ambos lados de la igualdad, obteniendo que $ga^{-1} = a^{-1}g$, es decir, el inverso de a también conmuta con g, por lo tanto $a^{-1} \in Z_G(g)$.

Finalmente se concluye que $Z_G(g) < G$. □

Definición 2.11.4:

Sea G un grupo y sea H un subconjunto no vacío de G. Se define el **normalizador** de H en G por

$$N_G(H) := \left\{ g \in G : \ g^{-1}Hg = H \right\}$$

Ejemplo 2.11.13.

Considere el grupo $(S_3, \circ)$ y sea $H := \{\sigma_1, \sigma_3\}$. Para hallar $N_{S_3}(H)$, se necesita revisar todos los conjuntos de la forma $\sigma_i^{-1}S\sigma_i$, para cada $i = 1, 2, 3, 4, 5, 6$, esto es:

- En el caso de σ_1 se tiene que

$$\sigma_1^{-1}H\sigma_1 = \{\sigma_1^{-1}\circ\sigma_1\circ\sigma_1, \ \ \sigma_1^{-1}\circ\sigma_3\circ\sigma_1\} = \{\sigma_1, \sigma_3\} = H.$$

- En el caso de σ_2 se tiene que

$$\sigma_2^{-1}H\sigma_2 = \{\sigma_2^{-1}\circ\sigma_1\circ\sigma_2, \ \ \sigma_2^{-1}\circ\sigma_3\circ\sigma_2\} = \{\sigma_2\circ\sigma_1\circ\sigma_2, \sigma_2\circ\sigma_3\circ\sigma_2\} = \{\sigma_1, \sigma_6\} \neq H.$$

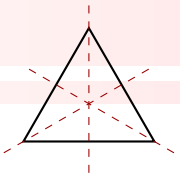
- De forma similar, y para el resto de elementos, se tiene que:

$$\begin{aligned}
\sigma_3^{-1}H\sigma_3 &= \{\sigma_3^{-1}\circ\sigma_1\circ\sigma_3, \ \ \sigma_3^{-1}\circ\sigma_3\circ\sigma_3\} = \{\sigma_3\circ\sigma_1\circ\sigma_3, \ \ \sigma_3\circ\sigma_3\circ\sigma_3\} = \{\sigma_1, \sigma_3\} = H. \\
\sigma_4^{-1}H\sigma_4 &= \{\sigma_4^{-1}\circ\sigma_1\circ\sigma_4, \ \ \sigma_4^{-1}\circ\sigma_3\circ\sigma_4\} = \{\sigma_5\circ\sigma_1\circ\sigma_4, \ \ \sigma_5\circ\sigma_3\circ\sigma_4\} = \{\sigma_1, \sigma_2\} \neq H. \\
\sigma_5^{-1}H\sigma_5 &= \{\sigma_5^{-1}\circ\sigma_1\circ\sigma_5, \ \ \sigma_5^{-1}\circ\sigma_3\circ\sigma_5\} = \{\sigma_4\circ\sigma_1\circ\sigma_5, \ \ \sigma_4\circ\sigma_3\circ\sigma_5\} = \{\sigma_1, \sigma_6\} \neq H. \\
\sigma_6^{-1}H\sigma_6 &= \{\sigma_6^{-1}\circ\sigma_1\circ\sigma_6, \ \ \sigma_6^{-1}\circ\sigma_3\circ\sigma_6\} = \{\sigma_6\circ\sigma_1\circ\sigma_6, \ \ \sigma_6\circ\sigma_3\circ\sigma_6\} = \{\sigma_1, \sigma_2\} \neq H.
\end{aligned}$$

Por lo tanto, $N_{S_3}(H) = \{\sigma_1, \sigma_3\}$.

Ejemplo 2.11.14.

Sea G un grupo abeliano y sea H un subgrupo de G. Por el teorema 2.11 se cumple que $H \lhd G$, es decir, $g^{-1}Hg = H$ para todo $g \in G$, entonces $N_G(H) = G$.



Observación 2.11.3.

A partir del ejemplo anterior, se puede concluir que si G es un grupo (no necesariamente abeliano) y si H es un subgrupo normal de G, entonces $N_G(H) = G$, es decir, el normalizador de cualquier subgrupo normal es el grupo completo.

Ejemplo 2.11.15.

Sea G un grupo y sea H un subconjunto no vacío de G. Mostrar que el normalizador $N_G(H)$ es un subgrupo de G.

Demostración. Para probar que $N_G(H) < G$ se va a utilizar la parte dos de la observación 2.7.2:

1. Sean $a, b \in N_G(H)$, entonces $a^{-1}Ha = H$ y $b^{-1}Hb = H$, se debe probar que $ab \in N_G(H)$, es decir, se debe probar que $(ab)^{-1}H(ab) = H$. En efecto, note que

$$\begin{aligned}
(ab)^{-1}H(ab) &= \left\{(ab)^{-1}s_1(ab) : h_1 \in H\right\} \\
&= \left\{(b^{-1}a^{-1})h_1(ab) : s_1 \in H\right\} \\
&= \left\{b^{-1}(a^{-1}h_1a)b) : s_1 \in H\right\} \\
&= \left\{b^{-1}h_2b : h_2 \in H\right\} \quad \text{porque} \quad a^{-1}Ha = H. \\
&= \left\{h_3 : h_3 \in H\right\} \quad \text{porque} \quad b^{-1}Hb = H. \\
&= H.
\end{aligned}$$

2. Sea $a \in N_G(H)$, es decir $a^{-1}Ha = H$, se debe probar que $a^{-1} \in N_G(H)$. Para ello, sea h un elemento cualquiera de H, entonces, por hipótesis, existe un $h_1 \in H$ tal que $h = a^{-1}h_1a$, esto a su vez implica que $aha^{-1} = h_1$, lo que afirma que $aHa^{-1} = H$ y por lo tanto $a^{-1} \in N_G(H)$.

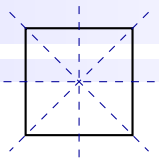
Finalmente se concluye que $N_G(H) < G$. □

Ejemplo 2.11.16.

Sea G un grupo y sea H un subgrupo de G, mostrar que H es un subgrupo normal de $N_G(H)$.

Demostración. La demostración se divide en tres partes:

1. Primero, probar que $H \subseteq N_G(H)$. Para ello, sea $h \in H$, es claro que $h^{-1}h_1h$ está en H para cualquier elemento $h_1 \in H$, por lo tanto $h \in N_G(H)$ y así $H \subseteq N_G(H)$.



2. Segundo, probar que $H < N_G(H)$. Esto es inmediato ya que H en sí mimso es un grupo por hipótesis y por el resultado del ejemplo 2.11.15, $N_G(H)$ también en sí mismo es un grupo y como $H \subseteq N_G(H)$, entonces $H < N_G(H)$.

3. Tercero, probar que $H \lhd N_G(H)$. Para esto, como H es un subgrupo de G, entonces el normalizador de H en G es precisamente el conjunto de todos los elementos $g \in G$ para los cuales $g^{-1}Hg = H$, que es precisamente la condición que define a un subgrupo normal.

□

2.12 Grupo cociente

De acuerdo con la definición 2.9.2, si G es un grupo y H es un subgrupo de G, el conjunto cociente de G/H es el conjunto de clases laterales determinadas por H y corresponde al conjunto

$$G/H := \{gH : g \in G\}$$

El objetivo de este apartado es mostrar que este conjunto se puede dotar de una estructura de grupo cuando H es un subgrupo normal de G.

Teorema 2.12.1:

Sea G un grupo y sea N un subgrupo normal de G. Se define sobre G/N el producto de clases dado por

$$xN \cdot yN := xyN, \tag{2.14}$$

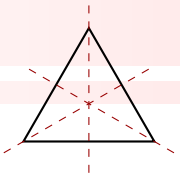
para todos $xN, yN \in G/N$ y para cada $x, y \in G$. Entonces, con esta operación, G/N es un grupo.

Demostración. En lo que sigue, se escribirá $xNyN$ en lugar de $xN \cdot yN$.

1. Primero se debe probar que que la operación 2.14 está bien definida. Sean $xN, yN, zN, wN \in G/N$ con $x, y, z, w \in G$ tales que

$$xN = zN \quad \text{y} \quad yN = wN.$$

Ahora, como $xN = zN$ entonces $x \in zN$ y como $yN = wN$ entonces $y \in wN$. De aquí se obtiene que $xy \in zNwN = zwN$. De forma similar $zw \in xNyN = xyN$. Entonces $xyN \cup zwN \neq \emptyset$ y



por el punto cinco del teorema 2.9.2, se tiene que

$$xyN = zwN,$$

lo que equivale a escribir que $xNyN = zNwN$, por lo tanto la operación 2.14 está bien definida.

2. Ahora se probará que la operación 2.14 es cerrada sobre G/N. Con este fin, considere $xN, yN \in G/N$, donde $x, y \in G$. Luego, como G es grupo, entonces $xy \in G$, lo cual implica que $xyN \in G/N$. Sin embargo, $xyN = xNyN$, lo que concluye que $xNyN \in G/N$.

3. La operación 2.14 es asociativa sobre G/N. Para ver esto, considere $xN, yN, zN \in G/N$ con $x, y, z \in G$. Entonces,

$$\begin{aligned}
\big(xNyN\big)zN &= (xy)NzN \\
&= (xy)zN \\
&= x(yz)N \quad \text{por la asociatividad en } G. \\
&= xN(yz)N \\
&= xN\big(yNzN\big).
\end{aligned}$$

4. El elemento neutro para el producto de clases en G/N es N. En efecto, note que $N = eN$, entonces, para cada $xN \in G/N$, con $x \in G$, se tiene que:

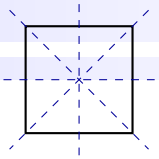
$$eNxN = (ex)N = xN.$$

De forma análoga $xNeN = xN$.

5. En cuanto a los inversos, para cada $xN \in G/N$ con $x \in G$, existe el inverso entonces $(xN)^{-1} = x^{-1}N$. En efecto,

$$\begin{aligned}
xN(xN)^{-1} &= xNx^{-1}N \\
&= xx^{-1}N \\
&= eN \\
&= N.
\end{aligned}$$

Similarmente $x^{-1}NxN = N$.



De acuerdo con los cinco puntos anteriores, se concluye que G/N es grupo con la operación definida por $xNyN = xyN$, donde $x, y \in G$. □

Definición 2.12.1:

Sea G un grupo y N un subgrupo normal de G. El grupo G/N, del teorema 2.12.1 anterior, se llama **grupo cociente** de G sobre N.

Ejemplo 2.12.1.

Considere el grupo de los enteros con la suma usual denotado por $(\mathbb{Z}, +)$ y considere también el subgrupo $5\mathbb{Z}$. Como $\mathbb{Z}$ es un grupo abeliano entonces $5\mathbb{Z}$ es subgrupos normal de $\mathbb{Z}$, esto por el teorema 2.11. Además, por el Teorema 2.12.1, se tendría que $\mathbb{Z}/5\mathbb{Z}$ es un grupo con la suma de clases dada por

$$(x + 5\mathbb{Z}) + (y + 5\mathbb{Z}) = (x + y) + 5\mathbb{Z}$$

para todos $x + 5\mathbb{Z}, y + 5\mathbb{Z}$ con $x, y \in \mathbb{Z}$. De forma explícita, los elementos de $\mathbb{Z}/5\mathbb{Z}$ son las clases izquierdas dadas a continuación:

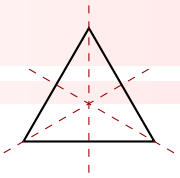
$$\begin{aligned}
0 + 5\mathbb{Z} &= \{\ldots, -5, 0, 5, 10, \ldots\} = 5\mathbb{Z} \\
1 + 5\mathbb{Z} &= \{\ldots, -4, 1, 6, 11, \ldots\} \\
2 + 5\mathbb{Z} &= \{\ldots, -3, 2, 7, 12, \ldots\} \\
3 + 5\mathbb{Z} &= \{\ldots, -2, 3, 8, 13, \ldots\} \\
4 + 5\mathbb{Z} &= \{\ldots, -1, 4, 9, 14, \ldots\}.
\end{aligned}$$

De esta forma, el grupo cociente de $\mathbb{Z}$ sobre $5\mathbb{Z}$ está dado por

$$\mathbb{Z}/5\mathbb{Z} = \{0 + 5\mathbb{Z}, 1 + 5\mathbb{Z}, 2 + 5\mathbb{Z}3 + 5\mathbb{Z}, 4 + 5\mathbb{Z}\}.$$

Más aún, la tabla de este grupo cociente es la siguiente:

$+$	$5\mathbb{Z}$	$1+5\mathbb{Z}$	$2+5\mathbb{Z}$	$3+5\mathbb{Z}$	$4+5\mathbb{Z}$
$5\mathbb{Z}$	$5\mathbb{Z}$	$1+5\mathbb{Z}$	$2+5\mathbb{Z}$	$3+5\mathbb{Z}$	$4+5\mathbb{Z}$
$1+5\mathbb{Z}$	$1+5\mathbb{Z}$	$2+5\mathbb{Z}$	$3+5\mathbb{Z}$	$4+5\mathbb{Z}$	$5\mathbb{Z}$
$2+5\mathbb{Z}$	$2+5\mathbb{Z}$	$3+5\mathbb{Z}$	$4+5\mathbb{Z}$	$5\mathbb{Z}$	$1+5\mathbb{Z}$
$3+5\mathbb{Z}$	$3+5\mathbb{Z}$	$4+5\mathbb{Z}$	$5\mathbb{Z}$	$1+5\mathbb{Z}$	$2+5\mathbb{Z}$
$4+5\mathbb{Z}$	$4+5\mathbb{Z}$	$5\mathbb{Z}$	$1+5\mathbb{Z}$	$2+5\mathbb{Z}$	$3+5\mathbb{Z}$



Ejemplo 2.12.2.

Sea $V := \{e, h, r, v\}$ el grupo de Klein y sea N el subgrupo de V dado por $N := \{e, h\}$. Como V es un grupo abeliano, por el teorema 2.11 se cumple que N es un subgrupo normal de V. En el ejemplo 2.9.1 se observó que las clases izquierdas determinadas por N son N y $\{r, v\}$, por lo que

$$V/N = \{N, rN\}$$

donde $rN = \{r, v\} = vN$. De esta forma, por el Teorema 2.12.1, V/N es un grupo con el producto de clases dado por

$$xNyN = (x \circ y)N$$

para todo $x, y \in V$. De hecho, los posibles productos en V/N son los siguientes

$$\begin{aligned} NN &= eNeN = eeN = N \\ NrN &= eNrN = erN = rN \subset N \\ rNN &= rNeN = reN = rN \subset N \\ rNrN &= rrN = eN = N \end{aligned}$$

En este sentido, la tabla del grupo cociente $(V/N, \cdot)$ está dada por

·	N	rN
N	N	rN
rN	rN	N

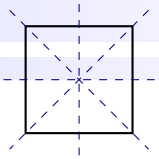
Ejemplo 2.12.3.

Considere el grupo simétrico $S_3 = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$ y considere el subgrupo $H = \{\sigma_1, \sigma_4, \sigma_5\}$, el cual es normal (ver ejemplo 2.11.2). Además, del ejemplo 2.9.2, el conjunto cociente de H en S_3 es

$$S_3/H = \left\{H, \{\sigma_2, \sigma_3, \sigma_6\}\right\}.$$

Además, por el Teorema 2.12.1, S_3/H es un grupo con el producto de clases dado por

$$xHyH = (x \circ y)H$$



para todo $x, y \in S_3$. De hecho, algunos de los posibles productos en S_3/H son los siguientes:

$$\begin{aligned}
\sigma_1 H \sigma_1 H &= (\sigma_1 \circ \sigma_1) H = \sigma_1 H = H \\
\sigma_1 H \sigma_2 H &= (\sigma_1 \circ \sigma_2) H = \sigma_2 H = \{\sigma_2, \sigma_3, \sigma_6\} \\
\sigma_1 H \sigma_3 H &= (\sigma_1 \circ \sigma_3) H = \sigma_3 H = \{\sigma_2, \sigma_3, \sigma_6\} \\
\sigma_1 H \sigma_4 H &= (\sigma_1 \circ \sigma_4) H = \sigma_4 H = H \\
\sigma_1 H \sigma_5 H &= (\sigma_1 \circ \sigma_5) H = \sigma_5 H = H \\
\sigma_1 H \sigma_6 H &= (\sigma_1 \circ \sigma_6) H = \sigma_6 H = \{\sigma_2, \sigma_3, \sigma_6\} \\
\sigma_2 H \sigma_2 H &= (\sigma_2 \circ \sigma_2) H = \sigma_1 H = H \\
\sigma_2 H \sigma_3 H &= (\sigma_2 \circ \sigma_3) H = \sigma_4 H = H \\
\sigma_2 H \sigma_4 H &= (\sigma_2 \circ \sigma_4) H = \sigma_3 H = \{\sigma_2, \sigma_3, \sigma_6\} \\
\sigma_2 H \sigma_5 H &= (\sigma_2 \circ \sigma_5) H = \sigma_6 H = \{\sigma_2, \sigma_3, \sigma_6\} \\
\sigma_2 H \sigma_6 H &= (\sigma_2 \circ \sigma_6) H = \sigma_5 H = H \\
\sigma_3 H \sigma_3 H &= (\sigma_3 \circ \sigma_3) H = \sigma_1 H = H \\
\sigma_3 H \sigma_4 H &= (\sigma_3 \circ \sigma_4) H = \sigma_6 H = \{\sigma_2, \sigma_3, \sigma_6\} \\
\sigma_3 H \sigma_5 H &= (\sigma_3 \circ \sigma_5) H = \sigma_2 H = \{\sigma_2, \sigma_3, \sigma_6\} \\
\sigma_3 H \sigma_6 H &= (\sigma_3 \circ \sigma_6) H = \sigma_4 H = H \\
\sigma_4 H \sigma_4 H &= (\sigma_4 \circ \sigma_4) H = \sigma_5 H = H \\
\sigma_4 H \sigma_5 H &= (\sigma_4 \circ \sigma_5) H = \sigma_1 H = H \\
\sigma_4 H \sigma_6 H &= (\sigma_4 \circ \sigma_6) H = \sigma_3 H = \{\sigma_2, \sigma_3, \sigma_6\} \\
\sigma_5 H \sigma_5 H &= (\sigma_5 \circ \sigma_5) H = \sigma_4 H = H \\
\sigma_5 H \sigma_6 H &= (\sigma_5 \circ \sigma_6) H = \sigma_2 H = \{\sigma_2, \sigma_3, \sigma_6\} \\
\sigma_6 H \sigma_6 H &= (\sigma_6 \circ \sigma_6) H = \sigma_1 H = H
\end{aligned}$$

Observación 2.12.1.

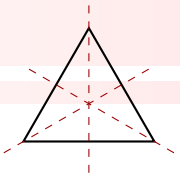
En el teorema 2.12.1 no se puede omitir la condición de ser normal, sobre el grupo N. Para entender esto considere el grupo simétrico $S_3 := \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$ y el subgrupo $H := \{\sigma_1, \sigma_2\}$ de S_3. Note que H no es un subgrupo normal de S_3. Para verificar esto, es suficiente probar que las clases $\sigma_3 H$ y $H\sigma_3$ son diferentes, en efecto:

$$\sigma_3 H = \{\sigma_3 \circ \sigma_1, \sigma_3 \circ \sigma_2\} = \{\sigma_3, \sigma_5\}$$

Por otro lado

$$H\sigma_3 = \{\sigma_1 \circ \sigma_3, \sigma_2 \circ \sigma_3\} = \{\sigma_3, \sigma_4\}$$

Dado que $\sigma_3 H \neq H\sigma_3$, se concluye que H no es un subgrupo normal de S_3. Ahora se va a probar que la



operación en S_3/H no está bien definida. Para ello, las clases laterales en S_3/H están dadas por

$$\begin{aligned}
\sigma_1 H &= \{\sigma_1\circ\sigma_1, \sigma_1\circ\sigma_2\} = \{\sigma_1, \sigma_2\} \\
\sigma_2 H &= \{\sigma_2\circ\sigma_1, \sigma_2\circ\sigma_2\} = \{\sigma_1, \sigma_2\} \\
\sigma_3 H &= \{\sigma_3\circ\sigma_1, \sigma_3\circ\sigma_2\} = \{\sigma_1, \sigma_4\} \\
\sigma_4 H &= \{\sigma_4\circ\sigma_1, \sigma_4\circ\sigma_2\} = \{\sigma_1, \sigma_4\} \\
\sigma_5 H &= \{\sigma_5\circ\sigma_1, \sigma_5\circ\sigma_2\} = \{\sigma_5, \sigma_6\} \\
\sigma_6 H &= \{\sigma_6\circ\sigma_1, \sigma_6\circ\sigma_2\} = \{\sigma_5, \sigma_6\}
\end{aligned}$$

Según los datos anteriores, se puede verificar que

$$\begin{aligned}
\sigma_1 H &= \sigma_2 H \\
\sigma_3 H &= \sigma_4 H \\
\sigma_5 H &= \sigma_6 H
\end{aligned}$$

Sin embargo, observe que

$$\sigma_3 H \sigma_5 H = (\sigma_3\circ\sigma_5) H = \sigma_2 H$$

y además que

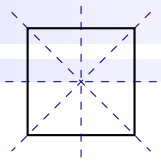
$$\sigma_3 H \sigma_6 H = (\sigma_3\circ\sigma_6) H = \sigma_4 H$$

Es evidente que $\sigma_3 H \sigma_5 H \neq \sigma_3 H \sigma_6 H$, pero $\sigma_5 H = \sigma_6 H$, lo cual se considera como una indefinición. Por lo tanto, la operación 2.14 no está bien definida en S_3/H, donde $H = \{\sigma_1, \sigma_2\}$.

Ejemplo 2.12.4.

Sea $N < G$ y sea $x^2 \in N$ para cada $x \in G$. Muestre que $N \lhd G$ y que el grupo cociente G/N es un grupo abeliano.

Demostración. Primero se debe probar que N es un subgrupo normal de G, es decir, si $x \in G$, se debe



mostrar que $x^{-1}Nx \subseteq N$. Para verificar esto, sea $y \in x^{-1}Nx$, entonces existe un $n \in N$ tal que

$$\begin{aligned} y =& x^{-1}nx \\ =& x^{-1}(x^{-1}x)nx \\ =& (x^{-1}x^{-1})xnx \\ =& (x^{-1})^2(n^{-1}n)xnx \\ =& (x^{-1})^2n^{-1}(nx)(nx) \\ =& (x^{-1})^2n^{-1}(nx)^2. \end{aligned}$$

Por hipótesis $(x^{-1})^2$ y $(nx)^2$ son elementos N, entonces $(x^{-1})^2n^{-1}(nx)^2$ es un elemento de N, por lo que $y \in N$. Con ello, se concluye que $x^{-1}Nx \subseteq N$ y por lo tanto N es un subgrupo normal de G. Para probar que el grupo cociente G/N es abeliano, se usará el resultado del ejercicio 2.8.5, es decir, se probará que $(xN)^2 = N$ para cada $x \in G$. En efecto,

$$(xN)^2 = xNxN = xxN = x^2N.$$

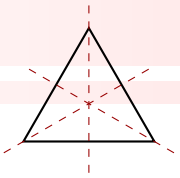
Por hipótesis $x^2 \in N$, entonces, para algún $n \in N$ se tiene que

$$x^2N = nN = N.$$

Esto obedece a que N es cerrado y que

$$nN = \{nn_1 : n_1 \in N\} = \{n_2 : n_2 \in N\} = N.$$

Finalmente $(xN)^2 = N$, con lo cual el grupo cociente G/N es abeliano. □



2.13 Ejercicios

● Ejercicio 2.13.1 (Orden de elementos y grupos factores) R/ p.315

Halle el orden de los siguientes elementos y grupos factores:

El grupo cociente $\mathbb{Z}_6/\langle 3\rangle$

El grupo cociente $(\mathbb{Z}_4 \times \mathbb{Z}_{12})/\langle 2\rangle \times \langle 2\rangle$

El grupo cociente $(\mathbb{Z}_4 \times \mathbb{Z}_{12})/\langle (2,2)\rangle$

La clase $5 + \langle 4\rangle$ como elemento del grupo factor

$\mathbb{Z}_{12}/\langle 4\rangle$

● Ejercicio 2.13.2 (grupo y subgrupo normal) R/ p.321

Sean $a, b \in \mathbb{R},\ a \neq 0,\ f_{a,b} : \mathbb{R} \to \mathbb{R}$ tal que $x \to (ax + b)$

y sean $G = \{f_{a,b} \mid a, b \in \mathbb{R}\},\quad a \neq 0,$ y $N = \{f_{1,b} \mid b \in \mathbb{R}\}$ Muestre que:

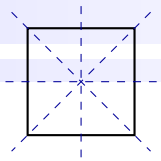
$(G, \circ)$ es un grupo donde $\circ$ denota la operación de composición de funciones,

N es un subgrupo normal en G,

$S = \{f_{a,b} \mid a \in \mathbb{Q}\}$ es un subgrupo normal de G.

● Ejercicio 2.13.3 (grupo y subgrupo normal) R/ p.327

Sea el grupo $GL(2, \mathbb{R})$ muestre que el conjunto siguiente: $T = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc \neq 0 \right\}$ Es un subgrupo normal de $GL(2, \mathbb{R})$.



R/ p.329 ● **Ejercicio 2.13.4 (grupo y subgrupo normal)**

Si $H \lhd G$ y $K \lhd H$. ¿Qué se puede decir de $K \lhd G$?.

Halle los normalizadores de $\{I, r_1\}$, $\{I, r_1, r_2, r_3\}$, $\{I, d_1\}$.

R/ p.331 ● **Ejercicio 2.13.5 (grupo y subgrupo normal)**

Muestre que si S es un subgrupo de índice 2 de un grupo finito G, entonces las clases izquierdas y las derechas correspondientes son las mismas, en otras palabras S es un subgrupo normal del grupo G.

R/ p.332 ● **Ejercicio 2.13.6 (grupo y subgrupo normal)**

Si N es un subgrupo normal de un grupo finito G, ¿Cúal es la relación entre los órdenes de los grupos G, G/N, N?

R/ p.333 ● **Ejercicio 2.13.7 (grupo y subgrupo normal)**

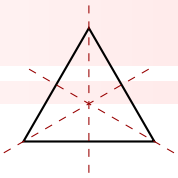
Demostrar que si $A < G$, donde G es un grupo y B es un grupo normal de G, entonces AB es un subgrupo de G.

R/ p.334 ● **Ejercicio 2.13.8 (grupo y subgrupo normal)**

Sean $a, b \in G$, G grupo y defínase:

$$[a, b] = aba^{-1}b^{-1}.$$

Se le llama a este el **conmutador** de a y b. Si C denota el conjunto de todos los productos finitos de conmutadores, entonces pruebe que:



C es un subgrupo de G (conocido como **subgrupo conmutador** o el grupo derivado de G

Muestre que C es normal en G,

Muestre que el grupo G/C es un grupo abeliano.

Demostrar que el inverso de un conmutador es un conmutador.

● **Ejercicio 2.13.9 (grupo y subgrupo normal)** R/ p.339

Muestre que si H y K son subgrupos normales de un grupo G tales que

$$H \cap K = \{e\},$$

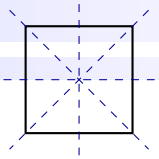
entonces $hk = kh, \quad \forall h \in H$ y $k \in K$.
$hkh^{-1}k^{-1} = h(kh^{-1}k^{-1})$.

● **Ejercicio 2.13.10 (grupo y subgrupo normal)** R/ p.340

Sea G un grupo el cual contiene al menos un subgrupo de un orden fijo dado s. Muestre que la intersección de todos los subgrupos de orden s es un subgrupo normal de G.

● **Ejercicio 2.13.11 (grupo y subgrupo normal)** R/ p.341

Muestre que si $H < G$ y $N \lhd G$ y N es un subgrupo normal en G, entonces $H \cap N$ es un subgrupo normal de H. De un ejemplo de que $H \cap N$ no necesariamente es normal en G.



R/ p.343

● **Ejercicio 2.13.12 (grupo y subgrupo normal)**

Pruebe que cada grupo G es normal en sí mismo, además pruebe que $G/G = G$.

R/ p.344

● **Ejercicio 2.13.13 (grupo y subgrupo normal)**

Muestre que si N es un subgrupo normal de G y $H < G$, entonces

$$HN := \{hn \ : \ h \in H, n \in N, \}$$

es un subgrupo de G.

R/ p.345

● **Ejercicio 2.13.14 (grupo y subgrupo normal)**

Muestre que si N es un subgrupo normal de G y N es un subgrupo G, entonces N es un subgrupo normal de HN

R/ p.347

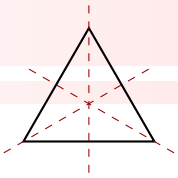
● **Ejercicio 2.13.15 (grupo y subgrupo normal)**

Sean H y K subgrupos de G, muestre que:

HK sea un subgrupo normal de $G \iff HK = KH$

Si H es normal, entonces HK es un subgrupo

Si H y K son normales, entonces HK es un subgrupo normal.



● **Ejercicio 2.13.16 (grupo y subgrupo normal)** R/ p.350

Determine el conjunto de conmutadores del grupo siguiente grupo

$$G = \left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \mid a,\ b \in \mathbb{R},\ b \neq 0 \right\}.$$

● **Ejercicio 2.13.17 (grupo y subgrupo normal)** R/ p.352

Sea $\mathbb{Z} \times \mathbb{Z}$ si se define $(a,b)(c,d) = (a + c(-1)^b, b + d)$. Muestre que G es un grupo no abeliano y determine el conjunto de los conmutadores de este grupo.

● **Ejercicio 2.13.18 (grupo y subgrupo normal)** R/ p.354

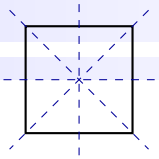
Si N es un subgrupo normal de un grupo G tal que $N \cap G' = \{e\}$ donde G', es el conjunto de conmutadores del grupo G, muestre que $N \subset Z(G)$.

● **Ejercicio 2.13.19 (grupo y subgrupo normal)** R/ p.355

Si $N \ll G$ y tal que $|N| = 2$, muestre que N es un subconjunto del centro del grupo G.

● **Ejercicio 2.13.20 (grupo y subgrupo normal)** R/ p.356

Si M y N subgrupos normales de un grupo G y $M \cap N = \{e\}$. Muestre que $mn = nm; \quad \forall m \in M,\ n \in N,\ m \in M$.



R/ p.357 ● **Ejercicio 2.13.21 (grupo y subgrupo normal)**

Muestre que es imposible que $2|Z(G)| = |G|$.

R/ p.358 ● **Ejercicio 2.13.22 (grupo y subgrupo normal)**

Diga en cada caso si es verdadero o falso:

( ) ¿ Tiene cada subgrupo de orden 4 clases izquierdas?

( ) ¿Puede no tener clases izquierdas un subgrupo finito de un grupo infinito?

( ) ¿Es un subgrupo de un grupo una clase izquierda en si mismo?

( ) ¿Solamente los subgrupos de grupos finitos pueden tener clases izquierdas?

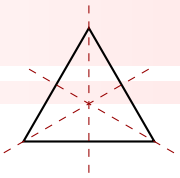
( ) El número de clases izquierdas de un subgrupo de un grupo finito divide al orden del grupo?

( ) ¿Es cada subgrupo de un grupo abeliano un subgrupo normal?

( ) ¿Es cada grupo cociente de un grupo finito un grupo finito?

( ) ¿Es abeliano cada grupo cociente de un grupo abeliano?

( ) ¿Es no abeliano cada grupo cociente de un grupo no abeliano?



2.14 Homomorfismos de Grupos

En el ámbito de la Teoría de Grupos, los homomorfismos emergen como herramientas fundamentales que proporcionan una perspectiva estructural profunda sobre las relaciones entre grupos algebraicos. Definidos de manera abstracta, los homomorfismos son funciones que respetan la operación del grupo, es decir, si $f : G_1 \to G_2$ es un homomorfismo entre los grupos $(G_1, \cdot)$ y $(G_2 *)$, entonces para cualesquiera elementos $x, y \in G_1$, se cumple que $f(x \cdot y) = f(x) * f(y)$. Esta propiedad esencial captura la esencia de las transformaciones entre grupos, preservando sus operaciones fundamentales y, por ende, su estructura algebraica.

La relevancia de los homomorfismos radica en su capacidad para revelar y analizar patrones algebraicos. A través de ellos, es posible entender cómo se relacionan intrínsecamente diferentes grupos, facilitando la comparación y transferencia de propiedades entre ellos. Los homomorfismos permiten descomponer problemas complejos en componentes más manejables al estudiar la imagen y el núcleo del homomorfismo, proporcionando información sobre la estructura interna de los grupos y las formas en que pueden ser mapeados entre sí.

Además, los homomorfismos son cruciales para la construcción de nuevas teorías y métodos dentro de la álgebra abstracta. Permiten definir conceptos como subgrupos normales, cocientes y productos directos, los cuales son fundamentales para la comprensión avanzada de la teoría de grupos. En resumen, los homomorfismos no solo facilitan una comprensión más profunda de las estructuras algebraicas existentes, sino que también abren puertas a nuevas formas de pensar y resolver problemas dentro de la Matemática.

Definición 2.14.1:

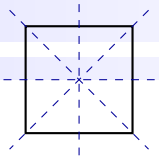
Sean $(G_1, \cdot)$ y $(G_2, *)$ dos grupos. Una función $f : G_1 \to G_2$ se llama **homomorfismo** (de grupos), si para cualesquiera $x, y \in G_1$ se tiene

$$f(x \cdot y) = f(x) * f(y).$$

Si existe tal homomorfismo, se dice que que $(G_1, \cdot)$ y $(G_2, *)$ son grupos **homomorfos**.

Observación 2.14.1.

En la definición anterior, también se usa la notación $f : (G_1, \cdot) \to (G_2, *)$ con el fin de enfatizar las operaciones respectivas sobre G_1 y G_2. Sin embargo, siempre que no haya ambigüedad, se pueden omitir los símbolos "$\cdot$" y "$*$", es decir, se puede escribir $f(xy) = f(x)f(y)$ en lugar de $f(x \cdot y) = f(g) * f(h)$.



Ejemplo 2.14.1.

Sea G un grupo y considere la función identidad $I : G \to G$ definida por

$$I(x) := x \quad \text{para todo } x \in G.$$

Entonces I es un homomorfismo llamado **homomorfismo identidad**.

Demostración. Sean $x, y \in G$. Por la definición de f se tiene

$$\begin{aligned} I(xy) &= xy \\ &= I(x)I(y) \end{aligned}$$

Con ello se prueba que I es un homomorfismo de G en G. □

Ejemplo 2.14.2.

Sea G_1 y G_2 dos grupos. Sea e el elemento neutro de G_2. La función Sea $f : G_1 \to G_2$, definida por

$$f(x) := e, \text{ para todo } x \in G_1$$

es un homomorfismo.

Demostración. Sean $x, y \in G_1$. Dado que f es constante

$$\begin{aligned} h(xy) &= e \\ &= e\,e \\ &= f(x)f(y), \end{aligned}$$

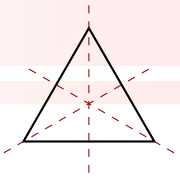
por lo tanto f es un homomorfismo y se dice que el grupo G_1 es homomorfo al grupo G_2. □

Ejemplo 2.14.3.

Sea $f : (\mathbb{R}, +) \to (\mathbb{R} - \{0\}, \cdot)$ definida por

$$f(x) := a^x, \quad \text{para cada } x \in \mathbb{R}, \text{ con } a > 0, a \neq 1.$$

Entonces, la función f es un homomorfismo.



Demostración. Sean $x, y \in \mathbb{R}$. Por las propiedades de la función exponencial y la definición de f se tiene

$$\begin{aligned} f(x+y) &= a^{x+y} \\ &= a^x a^y \\ &= f(x)f(y). \end{aligned}$$

Por lo tanto f es un homomorfismo. También se puede escribir que $(\mathbb{R}, +)$ y $(\mathbb{R} - \{0\}, \cdot)$ son grupos homomorfos. □

Ejemplo 2.14.4.

Considere la función $f : (\mathbb{R}^+, \cdot) \to (\mathbb{R}, +)$ definida por

$$f(x) := \ln x.$$

La función f es un homomorfismo.

Demostración. Sean $x, y \in \mathbb{R}^+$. Por las propiedades de la función logaritmo se tiene

$$\begin{aligned} f(xy) &= \ln(xy) \\ &= \ln x + \ln y \\ &= f(x) + f(y). \end{aligned}$$

De esta forma f es un homomorfismo y por lo tanto $(\mathbb{R}^+, \cdot)$ y $(\mathbb{R}, +)$ son grupos homomorfos. □

Ejemplo 2.14.5.

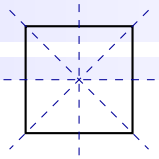
Sea G un grupo abeliano y defina $f : G \to G$ tal que $f(x) := x^2$ para cada $x \in G$. Entonces la función f es un homomorfismo

Demostración. Sean $x, y \in G$ y observe que

$$\begin{aligned} f(xy) &= (xy)^2 \\ &= x^2y^2 \quad \text{porque } G \text{ es un grupo abeliano,} \\ &= f(x)f(y). \end{aligned}$$

Con ello, f es un homomorfismo. □

Ejemplo 2.14.6.



Sea G un grupo y $a \in G$ un elemento fijo. Defina $f_a : G \to G$ tal que $f_a(x) := axa^{-1}$ para cada $x \in G$. Así, f es un homomorfismo.

Demostración. Sean $x, y \in G$ y verifique que

$$\begin{aligned} f_a(xy) &= a(xy)a^{-1} \\ &= a(xa^{-1}ay)a^{-1} \\ &= (axa^{-1})(aya^{-1}) \\ &= f_a(x)f_a(y). \end{aligned}$$

Por lo tanto, f_a es un homomorfismo. □

Ejemplo 2.14.7.

En el ejemplo 2.1.33 se probó que $GL(n,\mathbb{R}) := \{A \in M(n,\mathbb{R}) : \det A \neq 0\}$ es un grupo y considere la función $f : (GL(n,\mathbb{R}),\cdot) \to (\mathbb{R} - \{0\},\cdot)$, donde "$\cdot$" denota el producto de matrices para el dominio y el producto usual de números reales para el codominio, tal que

$$f(A) := \det A,$$

para cada $A \in GL(n,\mathbb{R})$. Entonces, la función f es un homomorfismo.

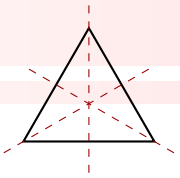
Demostración. Sean $A, B \in GL(n,\mathbb{R})$. Por la definición de f y las propiedades del determinante se puede ver que

$$\begin{aligned} f(AB) &= \det(AB) \\ &= \det A \det B \\ &= f(A)f(B). \end{aligned}$$

Por lo tanto f es un homomorfismo y se puede establecer que $(GL(n,\mathbb{R}),\cdot)$ es homomorfo al grupo dado por $(\mathbb{R} - \{0\},\cdot)$. □

Ejemplo 2.14.8.

Sea $n \in \mathbb{N}$ y defina $f : (U_n,\cdot) \to (U_n,\cdot)$ por $f([x]) := [x]^3$. La función f es un homomorfismo.



Demostración. Sean $[x], [y] \in U_n$, entonces

$$\begin{aligned} f([x][y]) &= f([xy]) \quad \text{por la definición de producto de clases,} \\ &= [xy]^3 \quad \text{por la definición de } f, \\ &= [xy][xy][xy] \quad \text{por la definición 2,2,1,} \\ &= ([x][y])([x][y])([x][y]) \quad \text{por la definición de producto de clases} \\ &= [x][x][x][y][y][y] \quad \text{Pues } U_n \text{ es abeliano y por asociatividad} \\ &= [x]^3[y]^3 \quad \text{por la definición 2,2,1,} \\ &= f([x])f([y]) \end{aligned}$$

De esta manera f es un homomorfismo. □

Ejemplo 2.14.9.

Considere el grupo del ejemplo 2.1.9 dado por

$$\mathbb{S}^1 := \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$$

con la operación

$$(x_1, y_1) * (x_2, y_2) := (x_1x_2 - y_1y_2, x_1y_2 + y_1x_2).$$

Defina la función $f : (\mathbb{R}, +) \to (\mathbb{S}^1, *)$ tal que $f(x) := (\cos(x), \sin(x))$. Mostrar que f es un homomorfismo.

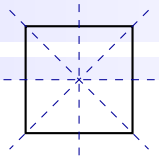
Demostración. Sean $x, y \in \mathbb{R}$ y note que:

$$\begin{aligned} f(x + y) &= (\cos(x + y), \operatorname{sen}(x + y)) \\ &= (\cos(x)\cos(y) - \operatorname{sen}(x)\operatorname{sen}(y), \operatorname{sen}(x)\cos(y) + \cos(x)\operatorname{sen}(y)) \\ &= (\cos(x), \operatorname{sen}(x)) * (\cos(y), \operatorname{sen}(y)) \\ &= f(x) * f(y), \end{aligned}$$

lo cual concluye que f es un homomorfismo entre $(\mathbb{R}, +)$ y $(\mathbb{S}^1, *)$. □

Ejemplo 2.14.10.

Sea G un grupo y sea N un subgrupo normal de un grupo de G. Se define la función $\pi : G \to G/N$ tal que $\pi(x) := xN$. La función π es un homomorfismo llamado el **proyección canónica** G en G/N.



Demostración. Sean $x, y \in G$, entonces,

$$\begin{aligned} \pi(xy) &= xyN \\ &= xNyN \quad \text{por el teorema 2.12.1.} \\ &= \pi(x)\pi(y). \end{aligned}$$

Por lo tanto π es un homomorfismo. □

Ejemplo 2.14.11.

Sea $f : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ definida por $f(x) := x + 1$ para cada $x \in \mathbb{Z}$. La función f no es un homomorfismo de grupos.

Demostración. Es suficiente encontrar un contraejemplo. Para este fin, note que

$$f(2) = 2 + 1 = 3$$

$$f(3) = 3 + 1 = 4$$

De esta forma $f(2) + f(3) = 7$, pero por otro lado

$$f(2 + 3) = f(5) = 5 + 1 = 6.$$

Es decir, $f(2)+f(3) \neq f(2+3)$, con lo cual se comprueba que f no es un homomorfismo de grupos. □

Teorema 2.14.1:

Sean G_1 y G_2 dos grupos cualesquiera y sea $f : G_1 \to G_2$ un homomorfismo. Sean e_1, e_2 los elementos neutros en G_1 y G_2 respectivamente. Entonces

1. $f(e_1) = e_2$.
2. $f(x^{-1}) = (f(x))^{-1}$

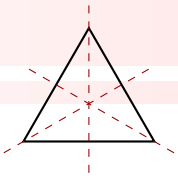
Demostración. A continuación se detalla la demostración en dos partes:

1. Note que

$$f(e_1) = f(e_1e_1) = f(e_1)f(e_1).$$

Con esto claro, opere el elemento $(f(e_1))^{-1}$ a ambos extremos de la igualdad anterior

$$f(e_1)(f(e_1))^{-1} = f(e_1)f(e_1)(f(e_1))^{-1},$$



Usando el hecho que que $f(e_1) \in G_2$ se concluye que

$$e_2 = f(e_1).$$

2. Sea $x \in G_1$, se sabe que $xx^{-1} = e_1$ y que f es un homorfismo, entonces

$$f(x)f(x^{-1}) = f(xx^{-1}) = f(e_1).$$

Por la parte 1 de este teorema se concluye que

$$f(x)f(x^{-1}) = e_2.$$

Ahora, aplique $(f(x))^{-1}$ a ambos lados de la igualdad, esto es:

$$(f(x))^{-1}f(x)f(x^{-1}) = (f(x))^{-1}e_2,$$

lo cual implica que

$$f(x^{-1}) = (f(x))^{-1}.$$

□

Definición 2.14.2:

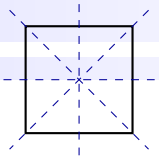
Sea $f : (G_1, \cdot) \to (G_2, *)$ un homomorfismo de grupos.

1. f se llama **monomorfismo** si es inyectivo.
2. f se llama **epimorfismo** si es sobreyectivo.
3. f se llama **isomorfismo** si es biyectivo. En este caso se dice que $(G_1, \cdot)$ y $(G_2, *)$ son **isomorfos** y se denota $G_1 \cong G_2$.
4. Un **automorfismo** es un isomorfismo de un grupo en sí mismo. El conjunto de automorfismos de un grupo G se denota $Aut(G)$. Es decir

$$Aut(G) := \{f : G \to G \mid f \text{ es isomorfismo}\}.$$

Ejemplo 2.14.12.

Sea $f : (\mathbb{R}^+, \cdot) \to (\mathbb{R} - \{0\}, \cdot)$ definido por $f(x) := x^2$. Entonces f es un monomorfismo.



Demostración. Primero se debe mostrar que que f es un homomorfismo. Para ello, considere $x, y \in \mathbb{R}^+$, entonces

$$\begin{aligned} f(xy) &= (xy)^2, \\ &= x^2y^2 \\ &= f(x)f(y). \end{aligned}$$

Por lo tanto f es un homomorfismo. Ahora se debe probar que f es inyectivo, para lo cual sean $x, y \in \mathbb{R}^+$ tales que $f(x) = f(y)$, entonces, por la definición de f, esto implica que $x^2 = y^2$, de lo cual se obtiene que $|x| = |y|$, pero $x > 0$ y $y > 0$, por lo que $x = y$. Por lo tanto, f es inyectiva y así es un monomorfismo. □

Ejemplo 2.14.13.

En el ejemplo 2.14.6 se probó que si G un grupo y si a es un elemento fijo de G, entonces la función $f_a(x) : G \to G$ definida por

$$f_a(x) := axa^{-1}$$

para cada $x \in G$, es un homomorfismo. De hecho, es un automorfismo.

Demostración. En en el ejemplo 2.14.6 ya se verificó que f es un homomorfismo. Falta verificar que f sea inyectiva y sobreyectiva.

- Recuerde que una función f es inyectiva si $f(x) = f(y)$ implica que $x = y$. Así, sean $x, y \in G$ y suponga que

  $$f_a(x) = f_a(y),$$

  esto implica que

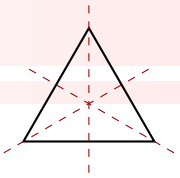
  $$axa^{-1} = aya^{-1}.$$

  Ahora, como a es un elemento de G, este se puede operar convenientemente para concluir que $x = y$.

- Una función es sobreyectiva si para todo y en el codominio, existe un x en el dominio tal que $f(x) = y$. En este sentido, sea $y \in G$ y construya el elemento $x = a^{-1}ya$, el cual pertenece a G porque $a \in G$ y G es un grupo. De acá se deduce que $axa^{-1} = y$, es decir, $f_a(x) = y$.

De esta forma f_a es un automorfismo. □

Observación 2.14.2.



Otra forma de probar que la función f_a presentada en el ejemplo 2.14.13 anterior es un automorfismo es mostrar que f_a posee inversa para cualquier elemento x en G. Considere la función $f_{a^{-1}} : G \to G$ definida por

$$f_{a^{-1}}(x) := a^{-1}xa$$

y observe que

$$\begin{aligned}(f_a \circ f_{a^{-1}})(x) &= f_a(f_{a^{-1}}(x)) \\ &= f_a(a^{-1}xa) \\ &= a(a^{-1}xa)a^{-1} \\ &= (aa^{-1})x(aa^{-1}) \\ &= x.\end{aligned}$$

De forma similar se prueba que

$$(f_{a^{-1}} \circ f_g)(x) = x,$$

lo que implica que $f_{a^{-1}}$ es la inversa de f_a y por lo tanto f_a es un automorfismo.

Ejemplo 2.14.14.

Sea $f : (\mathbb{Z}, +) \to (\mathbb{Z}_n, +)$, definida por $f(x) := [x]_n$, donde $[x]_n$ denota la clase de x en módulo n. La función f es un epimorfismo.

Demostración. Se debe probar que f es un homomorfismo y que es sobreyectiva. Para el primer caso, nean $x, y \in \mathbb{Z}$, entonces

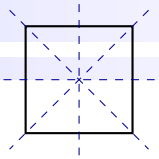
$$\begin{aligned}f(x+y) &= [x+y]_n \\ &= [x]_n + [y]_n \\ &= f(x) + f(y)\end{aligned}$$

Para probar f es sobreyeiva, sea $[y]_n \in \mathbb{Z}_n$, por el algoritmo de la división, existen $q, r \in \mathbb{Z}$ tales que $y = qn + r$ con $0 \leq r < n$. Entonces

$$[y]_n = [qn + r]_n = [qn]_n + [r]_n = [r]_n,$$

por lo que puede tomar $r \in \mathbb{Z}$ como la preimagen de $[y]_n$, pues

$$f(r) = [r]_n = [m]_n.$$



Por lo tanto f es un epimorfismo. □

Ejemplo 2.14.15.

El homomorfismo llamado **proyección canónica** y estudiado en el ejemplo 2.14.10 tal que $\pi : G \to G/N$ con $\pi(x) := xN$ y $N \lhd G$, es un epimorfismo.

Demostración. Sea $xN \in G/N$ una imagen en el dominio tal que $x \in G$. Observe que $\pi(x) = xN$, es decir, x es la preimagen. Por lo tanto, π es sobreyectiva y así es un epimorfismo. □

Ejemplo 2.14.16.

Considere el conjunto $G_1 := \{-1, 1\}$ con la operación "$\cdot$" determinada por la siguiente tabla

$\cdot$	1	-1
-1	-1	1
1	1	-1

y considere el conjunto $G_2 := \{0, 1\}$ con la operación "$*$" cuya tabla es la siguiente

$*$	0	1
0	0	1
1	1	0

Demostrar que $(G_1, \cdot)$ y $(G_2, *)$ son grupos isomorfos.

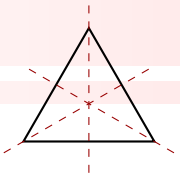
Demostración. Para probar que $(G_1, \cdot)$ y $(G_2, *)$ son grupos basta con observar que son conjuntos finitos y además las operaciones son cerradas. Ahora, para mostrar que son grupos isomorfos, defina la función $f : G_1 \to G_2$ tal que

$$f(1) = 0, \quad f(-1) = 1.$$

Con esto, note que

$$\begin{aligned}
f(1 \cdot 1) &= f(1) = 0 = 0 * 0 = f(1) * f(1).\\
f(-1 \cdot 1) &= f(-1) = 1 = 1 * 0 = f(-1) * f(1).\\
f(-1 \cdot -1) &= f(1) = 0 = 1 * 1 = f(-1) * f(-1).\\
f(1 \cdot -1) &= f(-1) = 1 = 0 * 1 = f(1) * f(-1).
\end{aligned}$$

Con los datos anteriores, se concluye que la función f es un homomorfismo. Además, observe que f es una función biyectiva, entonces $G_1 \cong G_2$. □



Ejemplo 2.14.17.

Sea G un grupo abeliano de orden n. Sea $k \in \mathbb{Z}$ tal que $(n,k) = 1$ y defina $f : G \to G$ por

$$f(x) := x^k,$$

para todo $x \in G$. Así, la función f es un isomorfismo.

Demostración. Para probar que f es un homomorfismo, sean x, y elementos de G y como G es abeliano, entonces $(xy)^k = x^k y^k =$. Con ello note que

$$f(xy) = (xy)^k = x^k y^k = f(x)f(y).$$

Falta probar que f es un isomorfismo, para ello, f es una función entre conjuntos finitos, es suficiente probar que f es sobreyectiva para que sea biyectiva. Con este fin, por el teorema 1.1.4 existen $s, t \in \mathbb{Z}$ tales que $ks + nt = 1$. Ahora, sea $x \in G$ (en el codominio de f) y tome $x^s \in G$ (en el dominio de f), entonces,

$$\begin{aligned} f(x^s) &= (x^s)^k \\ &= (x^s)^k e^t \\ &= (x^s)^k (x^n)^t \quad \text{pues } G \text{ es de orden } n. \\ &= x^{ks} x^{nt} \\ &= x^{ks+nt} \\ &= x^1 \\ &= x. \end{aligned}$$

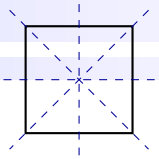
Es decir, para cualquier elemento del codominio se encontró una preimangen en el dominio, esto prueba que f es sobreyectiva y por lo tanto que f es un isomorfismo. □

Ejemplo 2.14.18.

El homomorfismo del ejemplo 2.14.3 es un monomorfismo.

Demostración. Se debe probar que f es inyectiva. Para ello, observe que la derivada de f con respecto a x está dada por

$$f'(x) = \ln a \cdot a^x > 0, \quad \forall x \in \mathbb{R},$$



esto significa que f es estrictamente creciente y por consiguiente es inyectiva. Entonces, como f es homomorfismo inyectivo, es decir, f es un monomorfismo. Otra forma de probar que f se inyectiva es suponer que $f(x) = f(y)$ y fácilmente se concluye que $x = y$. □

Ejemplo 2.14.19.

Sea G_1 el grupo definido en el ejemplo 2.1.29 dado por

$$G_1 := \{y : \mathbb{R} \to \mathbb{R} \ : \ y(x) = mx + b, \ \ m, b \in \mathbb{R}, \ m > 0\},$$

G_1 es el grupo conformado por el conjunto de ecuaciones de las rectas estrictamente crecientes, con la composición de funciones. Sea G_2 el grupo de matrices

$$G_2 = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}, \ a > 0, \ \ a, b \in \mathbb{R} \right\}.$$

con el producto usual de matrices. Entonces, G_1 y G_2 son isomorfos.

Demostración. Para probar que G_1 es isomorfo a G_2 considere la función $f : G_1 \to G_2$ definida por

$$f(ax + b) = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}, \quad \text{donde } a > 0.$$

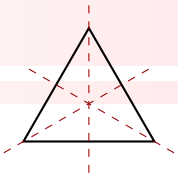
Primero se probará que f es un homomorfismo y luego que es biyectiva.

1. Para probar que f es un homomorfismo Considere $y_1, y_2 \in G_1$ tales que $y_1 = a_1x + b_1$ y $y_2 = a_2x + b_2$, con $a_1, a_2 \in \mathbb{R}^+$, entonces:

$$\begin{aligned} f\left(y_1 \circ y_2\right) = f[(a_1x + b_1)\circ(a_2x + b_2)] &= f[a_1(a_2x + b_2) + b_1] \\ &= f(a_1a_2x + a_1b_2 + b_1) \\ &= \begin{pmatrix} a_1a_2 & a_1b_2 + b_1 \\ 0 & 1 \end{pmatrix}, \quad \text{donde se cumple que } a_1a_2 > 0. \\ &= \begin{pmatrix} a_1 & b_1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ 0 & 1 \end{pmatrix} \\ &= f(y_1)f(y_2). \end{aligned}$$

2. Ahora se probará que f es inyectiva. Sean $y_1, y_2 \in G$ tales que

$$y_1 = a_1x + b_1 \ \text{ y } \ y_2 = a_2x + b_2, \ \ \text{con } a_1, a_2 \in \mathbb{R}^+$$



y suponga que

$$f(y_1) = f(y_2).$$

Entonces

$$\begin{pmatrix} a_1 & b_1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a_2 & b_2 \\ 0 & 1 \end{pmatrix},$$

de donde

$$a_1 = a_2 \text{ y } b_1 = b_2,$$

por lo que

$$a_1 x + b_1 = a_2 x + b_2,$$

lo que implica a su vez que

$$y_1 = y_2.$$

Por lo tanto f es inyectiva. Falta verificar que f sea sobreyectiva. Pare este fin, tome un $y' \in G_2$ tal que $y' = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$. Se debe encontrar un $y \in G_1$ tal que $f(y) = y'$, el cual claramente es $y = ax + b$. Así f es sobreyectiva.

Finalmente se concluye que G_1 y G_2 son isomorfos. □

Ejemplo 2.14.20.

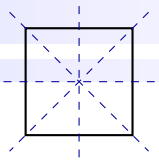
Sea $V = \{e, h, r, v\}$ el grupo de Klein y $H = \{e', g\}$ un grupo de orden 2. Defina la función $f : V \to H$ por

$$\begin{aligned} f(e) &= e', \\ f(h) &= e', \\ f(r) &= g, \\ f(v) &= g. \end{aligned}$$

Muestre que h es un epimorfismo.

Demostración. Primero se prueba que es un homomorfismo. Para ello, y por facilidad de notación, en vez de escribir, por ejemplo, $h \circ r$, se escribe hr. Con esto claro, note que:

- $f(hr) = f(v) = g$, mientras que $f(h)f(r) = e'g = g$, es decir, $f(hr) = f(h)f(r)$.
- $f(eh) = f(h) = e'$, mientras que $f(e)f(h) = e'e' = e'$, es decir, $f(eh) = f(e)f(h)$.
- $f(vv) = f(e) = e'$, mientras que $f(v)f(v) = gg = e'$, es decir, $f(vv) = f(v)f(v)$.



- $f(vh) = f(r) = g$, mientras que $f(v)f(h) = ge' = g$, es decir, $f(vh) = f(v)f(h)$.

En total, se deben probar 16 productos, quedando pendiente 12 más, lo cual le queda al lector. Con ello, se concluye que f es un homomorfismo. Además, note que cada elemento del codominio, en este caso el conjunto $H = \{e', g\}$, está correspondido, lo que implica la sobreyectividad de f. Así, f es un epimorfismo. □

Ejemplo 2.14.21.

El grupo de Klein $V := \{e, h, r, v\}$ es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$ con la suma directa definida en la observación 2.1.3.

Demostración. Recuerde que por el ejemplo 2.1.15 y por la observación 2.1.3, el producto directo de grupos es un grupo con la suma directa, por lo cual $\mathbb{Z}_2 \times \mathbb{Z}_2$ es grupo. Ahora, defina la función dada por $f : V \to \mathbb{Z}_2 \times \mathbb{Z}_2$ tal que

$$\begin{aligned} f(e) &= (0,0), \\ f(h) &= (1,0), \\ f(r) &= (0,1), \\ f(v) &= (1,1). \end{aligned}$$

Para verificar que f es homomorfismo se debe probar que $f(x \circ y) = f(x) + f(y)$ para cualesquiera $x, y \in V$. En efecto,

$$f(e \circ a) = f(a) = (1,0) = (0,0) + (1,0) = f(e) + f(a).$$

De forma análoga se prueban las igualdades

$$f(e \circ h) = f(e) + f(h), \quad f(e \circ r) = f(e) + f(r), \quad f(e \circ v) = f(e) + f(v).$$

Ahora bien, utilizando el hecho de que la suma es en módulo 2, se tiene que

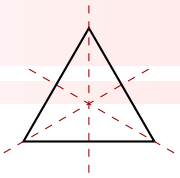
$$f(h \circ h) = f(e) = (0,0) = (1,0) + (1,0) = f(h) + f(h).$$

De forma similar se prueban las igualdades

$$f(r \circ r) = f(r) + f(r), \quad f(v \circ v) = f(v) + f(v).$$

Por otro lado note que

$$f(h \circ r) = f(v) = (1,1) = (1,0) + (0,1) = f(h) + f(r).$$



$$f(r \circ v) = f(h) = (1,0) = (01) + (1,1) = f(r) + f(v).$$

Las demás igualdades se obtienen usando el hecho de que el grupo de Klein es abeliano. Esto concluye la prueba de que f es un homomorfismo. Finalmente, no es difícil observar que f es inyectiva y sobreyectiva, por lo tanto f es un isomorfismo y así, el grupo de Klein $V := \{e, h, r, v\}$ es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$ □

Ejemplo 2.14.22.

Considere el grupo G y el grupo Klein, denotado por V, cuyas tablas se aprecian a continuación de forma respectiva.

	e'	x	x^2	x^3
e'	e'	x	x^2	x^3
x	x	x^2	x^3	e'
x^2	x^2	x^3	e'	x
x^3	x^3	e'	x	x^2

	e	h	r	v
e	e	h	r	v
h	h	e	v	r
r	r	v	e	h
v	v	r	h	e

Muestre que G y V no son isomorfos.

Demostración. Por contradicción, suponga que existe un isomorfismo $f : C \to V$. Por la parte uno del teorema 2.14.1 se debe cumplir que $f(e') = e$. Además, como f es un isomorfismo, en particular es inyectiva, entonces debe darse **solo** una de las siguientes opciones:

$$f(x) = h, \ f(x) = r, \ \text{o} \ f(x) = v.$$

Sin pérdida de la generalidad, suponga que sucede que $f(x) = h$. De acuerdo con la tablas del grupo C y el grupo V se tiene que

$$f\left(x^2\right) = f(xx) = f(x)f(x) = hh = e.$$

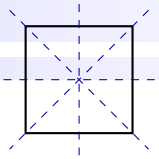
Por lo tanto, se tiene que la imagen e tiene dos preimágenes, siendo estas e' y x^2, lo cual es una contradicción porque se supone que f es inyectiva. □

Teorema 2.14.2: Teorema de Clasificación de Grupos Cíclicos

Sea G un grupo y sea $g \in G$.

1. Si $|g| = \infty$, entonces $\langle g \rangle \cong \mathbb{Z}$.
2. Si $|g| = n$, entonces $\langle g \rangle \cong \mathbb{Z}_n$.

En este caso, las operaciones sobre $\mathbb{Z}$ y $\mathbb{Z}_n$ son la suma usual de enteros y la suma de clases módulo n respectivamente.



Demostración. A continuación se detalla las dos partes de la demostración:

1. Para la primera parte, suponga que $|g| = \infty$. Además, recuerde que $\langle g \rangle = \{g^m : m \in \mathbb{Z}\}$. Defina la función

$$f : \langle g \rangle \to \mathbb{Z} \quad \text{tal que} \quad f\left(g^k\right) = k.$$

Se debe probar que f es un isomorfismo, para lo cual primero que demuestra que f es un homomorfismo.

Sean $g^{k_1}, g^{k_2} \in \langle g \rangle$, para algunos $k_1, k_2 \in \mathbb{Z}$. Entonces

$$\begin{aligned} f\left(g^{k_1} g^{k_2}\right) &= f(g^{k_1+k_2}) \\ &= k_1 + k_2 \\ &= f\left(g^{k_1}\right) + f\left(g^{k_2}\right), \end{aligned}$$

lo cual prueba que en efecto f es un homomorfismo.

Ahora, se verifica que f es inyectiva. Sean $g^{k_1}, g^{k_2} \in \langle g \rangle$ tales que

$$f\left(g^{k_1}\right) = f\left(g^{k_2}\right),$$

entonces, por la definición de f, se tiene $k_1 = k_2$, lo cual implica $g^{k_1} = g^{k_2}$.

Para probar que f es sobreyectiva, para cada $k \in \mathbb{Z}$ observe que la preimagen de k es $g^k \in \langle g \rangle$, pues $f(g^k) = k$, por lo que f sí es sobreyectiva.

De lo anterior, se concluye f es un isomorfismo y por lo tanto $\langle g \rangle$ y $\mathbb{Z}$ son isomorfos, es decir, $\langle g \rangle \cong (\mathbb{Z}, +)$.

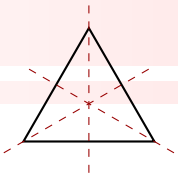
2. Supongamos que $|g| = n$. Esto significa que $\langle g \rangle$ es un conjunto finito de la forma

$$\langle g \rangle = \left\{e, g, g^2, g^3, \ldots, g^{n-1}\right\}$$

Defina la función

$$h : \langle g \rangle \to (\mathbb{Z}_n, +) \quad \text{tal que} \quad h\left(g^k\right) = [k]_n.$$

Se debe probar que f es un isomorfismo, para lo cual primero se muestra que es un homomorfismo.



Sean $g^{k_1}, g^{k_2} \in \langle g \rangle$, para algunos $k_1, k_2 \in \mathbb{Z}$. Entonces

$$\begin{aligned} h\left(g^{k_1} g^{k_2}\right) &= h\left(g^{k_1+k_2}\right) \\ &= [k_1 + k_2]_n \\ &= [k_1]_n + [k_2]_n \\ &= h\left(g^{k_1}\right) + h\left(g^{k_2}\right) \end{aligned}$$

lo cual prueba que h es un homomorfismo.

Ahora se verifica que h es inyectivo. Sean $g^{k_1}, g^{k_2} \in \langle g \rangle$ tales que

$$h\left(g^{k_1}\right) = h\left(g^{k_2}\right),$$

entonces, por la definición de h se tiene que $[k_1]_n = [k_2]_n$, es decir $k_1 \equiv k_2 (mod\ n)$, donde, por la parte dos del teorema (2.6.1), se tiene $g^{k_1} = g^{k_2}$.

Para probar que h es sobreyectiva, considere $[k] \in \mathbb{Z}_n$ y observe que $h(g^k) = [k]$, es decir, cada elemento del codominio posee una preimagen. Finalmente, h es un homomorfismo biyectivo y se concluye que $\langle g \rangle$ y $\mathbb{Z}_n$ son isomorfos, que se denota como $\langle g \rangle \cong \mathbb{Z}_n$.

□

Corolario 2.14.1:

Sea G un grupo cíclico generado por $g \in G$.

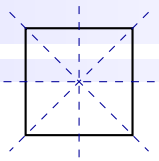
1. Si $|G| = \infty$, entonces $G \cong \mathbb{Z}$.
2. Si $|G| = n$ entonces $G \cong \mathbb{Z}_n$.

Demostración. Es una consecuencia inmediata del teorema anterior, ya que si G es cíclico generado por $g \in G$, entonces $\langle g \rangle = G$. □

Observación 2.14.3.

De acuerdo con la parte uno del corolario anterior, todos los grupos **cíclicos** de orden infinito son isomorfos entre ellos. Además, de acuerdo con la parte dos, dos grupos **cíclicos** del mismo orden son isomorfos entre ellos.

Ejemplo 2.14.23.



En el ejemplo 2.10.5 se determinó que el conjunto de unidades $(U_5, \cdot)$ tal que $U_5 = \{[1], [2], [3], [4]\}$ es un grupo cíclico, además note que es de orden 4. Por su parte, en el ejemplo 2.10.8 se estableció que $(G, \cdot)$, donde $G := \{1, -1, -i, i\}$, $i^2 = -1$, también es un grupo cíclico y es de orden 4. Por el teorema y el corolario anterior, U_5 y G son grupos isomorfos a $\mathbb{Z}_4$, por lo tanto U_5 y G son grupos isomorfos entre sí. Es decir

$$U_5 \cong Z_4 \cong G.$$

Ejemplo 2.14.24.

Considere el grupo $\mathbb{Z}_2 \times \mathbb{Z}_3$, con la suma directa de grupos vista en la observación 2.1.3. Además, note que

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}.$$

Luego, operando el elemento $(1,1)$ consigo mismo reiteradamente se tiene

$$\begin{aligned}
1(1,1) &= (1,1),\\
2(1,1) &= (1,1)+(1,1) = (0,2),\\
3(1,1) &= (1,1)+(1,1)+(1,1) = (1,3),\\
4(1,1) &= 3(1,1)+(1,1) = (1,0)+(1,1) = (0,1),\\
5(1,1) &= 4(1,1)+(1,1), = (0,1)+(1,1) = (1,2),\\
6(1,1) &= 5(1,1)+(1,1) = (0,0).
\end{aligned}$$

De esta forma se tiene que $(1,1)$ genera a $\mathbb{Z}_2 \times \mathbb{Z}_3$, por lo que este grupo es cíclico. Por otro lado, como $|\mathbb{Z}_2 \times \mathbb{Z}_3| = 6$, por el corolario anterior se concluye que $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$.

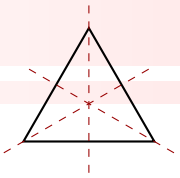
Teorema 2.14.3:

Sean G_1 y G_2 dos grupos tales que $G_1 \cong G_2$, entonces $Aut(G_1) \cong Aut(G_2)$.

Demostración. Recuerde que $Aut(G)$ es el conjunto de automorfismos de un grupo G. Por su parte, como $G_1 \cong G_2$, existe un isomorfismo $f : G_1 \to G_2$. Luego, para cualquier $h \in Aut(G_1)$ defina la función

$$T_f : Aut(G_1) \to Aut(G_2) \quad \text{tal que} \quad T_f(h) := f \circ h \circ f^{-1}.$$

Se debe probar que T_f es un isomorfismos, de la siguiente forma:



1. Primero se probará que T_f es un homomorfismo, para lo cual sean $h_1, h_2 \in Aut(G_1)$, entonces

$$\begin{aligned} T_f(h_1 \circ h_2) &= f \circ (h_1 \circ h_2) \circ f^{-1} \\ &= (f \circ h_1) \circ (f^{-1} \circ f) \circ (h_2 \circ f^{-1}) \\ &= (f \circ h_1 \circ f^{-1}) \circ (f \circ h_2 \circ f^{-1}) \\ &= T_f(h_1) \circ T_f(h_2) \end{aligned}$$

   Por lo tanto, en efecto T_f es un homomorfismo.

2. Segundo, se prueba que T_F es un isomorfismo, es decir, se debe probar que T_f es biyectiva. Para este caso se usará la misma estrategia de la observación 2.14.2, la cual consiste en probar que T_f tiene inversa. Para ello, como f es biyectiva, entonces existe f^{-1}. Luego, para $h \in Aut(G_1)$ se tiene que $T_{f^{-1}}(h) = f^{-1} \circ h \circ f$ y no es difícil verificar que $(T_f \circ T_{f^{-1}})(h) = h = (T_{f^{-1}} \circ T_f)(h)$, con lo cual $T_{f^{-1}}$ es la función inversa de T_f.

Finalmente, según lo demostrado anteriormente, se concluye que $Aut(G_1) \cong Aut(G_2)$. □

2.15 Núcleo e Imagen de un homomorfismo

En esta sección se introducen dos de los conceptos más importantes de la teoría de grupos: el núcleo y la imagen de un homomorfismo. El concepto de núcleo es especialmente significativo, ya que permite derivar teoremas fundamentales que, mediante el uso del concepto de isomorfismo, facilitan establecer relaciones entre estructuras de grupos que inicialmente pueden parecer diferentes.

Definición 2.15.1:

Sean G_1 y G_2 dos grupos y sea $f : G_1 \to G_2$ un homomorfismo.

1. Se define el núcleo de f por

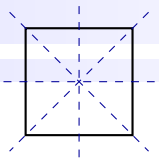
$$\ker(f) := \{x \in G_1 \ : \ f(x) = e_2, \text{ donde } e_2 \text{ es el elemento neutro de } G_2\}.$$

2. Se define la imagen de f por

$$\text{Im}(f) := \{f(x) \ : \ x \in G_1\}.$$

Observación 2.15.1.

1. Es importante notar que el núcleo de un homomorfismo $f : G_1 \to G_2$, es un subconjunto de G_1, mientras que la imagen es un subconjunto de G_2.



2. Por la parte uno del teorema 2.14.1, se tiene que $f(e_1) = e_2$, donde e_1 y e_2 son los elementos neutros de G_1 y G_2 respectivamente, entonces al menos existe el elemento e_1 en el núcleo de f. Por lo tanto, el núcleo de un homomorfismo siempre es un conjunto no vacío.

Ejemplo 2.15.1.

Sea $f : (\mathbb{R}/\{0\}, \cdot) \to (\mathbb{R}, +)$ definida por

$$f(x) := \ln x.$$

Ya se probó en el ejemplo 2.14.4 que f es un homomorfismo. Pruebe que el núcleo de f es

$$\ker(f) = \{1\}.$$

Demostración. Se va utilizar la relación de inclusión para probar que $\ker(f) = \{1\}$, esto es:

- ($\supseteq$) Como $f(1) = \ln(1) = 0$ y dado que el cero es el neutro en $(\mathbb{R}, +)$, se tiene que $1 \in \ker(f)$, por lo que $\{1\} \subseteq \ker(f)$.
- ($\subseteq$) Sea $x \in \ker(f)$, entonces, por definición de núcleo $f(x) = 0$, es decir

  $$\ln x = 0,$$

  y esto sucede si $x = 1$, lo cual implica que $x \in \{1\}$.

Por lo tanto $\ker(f) = \{1\}$. □

Ejemplo 2.15.2.

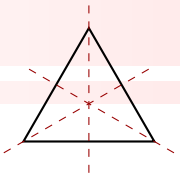
Considere la función $f : (\mathbb{Z}, +) \to (\mathbb{Z}_n, +)$ tal que $f(x) := [x]_n$. En el ejemplo 2.14.14 se probó que f es un homomorfismo. Determine el núcleo de f.

Solución. Por la definición del núcleo de un homomorfismo se tiene que

$$\begin{aligned}\ker(f) &= \{x \in \mathbb{Z} : f(x) = [0]_n\} \\ &= \{x \in \mathbb{Z} : [x]_n = [0]_n\}\end{aligned}$$

Recuerde que si $[x]_n = [0]_n$ entonces $x = nk$ con $k \in \mathbb{Z}$. De esta forma se puede establecer que

$$\ker(f) = \{nk : k \in \mathbb{Z}\} = n\mathbb{Z}.$$



□

Ejemplo 2.15.3.

Considere la función $f : (\mathbb{R}, +) \to (\mathbb{S}^1, *)$ tal que $f(x) := (\cos(x), \sin(x))$. En el ejemplo 2.14.9 se comprobó que f es un homomorfismo, determine su núcleo.

Solución. Recuerde que $\mathbb{S}^1 := \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$ y además que

$$(x_1, y_1) * (x_2, y_2) := (x_1x_2 - y_1y_2, x_1y_2 + y_1x_2).$$

Asimismo, en el ejemplo 2.1.9 se obtuvo que el elemento neutro de $(\mathbb{S}^1, *)$ es el par ordenado $(1, 0) \in \mathbb{S}^1$. Con esto claro, sea $x \in \ker(f)$, entonces $f(x) = (1, 0)$, es decir,

$$(\cos(x), \text{sen}(x)) = (1, 0).$$

De acá se deduce que $\cos(x) = 1$ y $\text{sen}(x) = 0$, esto equivale respectivamente a $x = 2k\pi$ y $x = k\pi$, con $k \in \mathbb{Z}$. Sin embargo, para que ambas condiciones se cumplan simultáneamente, se necesita que $x = 2k\pi$, donde $k \in \mathbb{Z}$. Por lo tanto, el núcleo de f es

$$\ker(f) = \{2k\pi : k \in \mathbb{Z}\}.$$

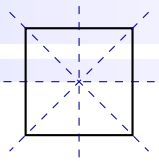
□

Teorema 2.15.1:

Sea $f : G_1 \to G_2$ un homomorfismo. Entonces f es inyectiva si y solo si $\ker(f) = \{e_1\}$, donde e_1 es el elemento neutro en G_1.

Demostración. Primero se probará que si f es inyectiva, entonces $\ker(f) = \{e_1\}$. Luego se demostrará que si $\ker(f) = \{e_1\}$, entonces f es inyectiva.

- ($\Rightarrow$) La hipótesis corresponde a que f es un homomorfismo inyectivo y se debe probar que $\ker(f) = \{e_1\}$. Para este fin, por contradicción, suponga que existe un elemento $g_1 \in G_1$, $g_1 \neq e_1$ tal que $g_1 \in \ker(f)$. Entonces, $f(g_1) = e_2$, donde e_2 es el neutro de G_2. Por el teorema 2.14.1 se tiene que $f(e_1) = e_2$, de esta forma $f(g_1) = f(e_1)$, pero como f es inyectiva, es inmediato que $g_1 = e_1$, lo cual contradice que $g_1 \neq e_1$. Así, $\ker(f) = \{e_1\}$.



- ($\Leftarrow$) En este caso las hipótesis son que f es un homomorfismo y que $\ker(f) = \{e_1\}$, se debe probar que f es inyectiva. Para ello, sean $x, y \in G_1$ tales que

$$f(x) = f(y),$$

entonces

$$f(x)(f(y))^{-1} = f(y)(f(y))^{-1},$$

lo cual implica que

$$f(x)(f(y))^{-1} = e_2.$$

Por otro lado, como f es homomorfismo se tiene que

$$f(xy^{-1}) = e_2$$

y dado que por hipótesis $\ker(f) = \{e_1\}$, se cumple que $xy^{-1} \in \ker(f) = \{e_2\}$, es decir,

$$xy^{-1} = e_1,$$

por lo que $x = y$. Por lo tanto, f es inyectiva.

□

Ejemplo 2.15.4.

En el ejemplo 2.15.1 se probó que $f : (\mathbb{R}^+, \cdot) \to (\mathbb{R}, +)$ tal que $f(x) := \ln x$ es un homomorfismo con núcleo $\ker(f) = \{1\}$, donde el número 1 es el neutro de $(\mathbb{R}^+, \cdot)$. Entonces, por el teorema 2.15.2 se concluye que f es inyectiva.

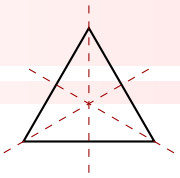
Ejemplo 2.15.5.

En el ejemplo 2.15.2 se halló el núcleo del homomorfismo $f : (\mathbb{Z}, +) \to (\mathbb{Z}_n, +)$ tal que $f(x) := [x]_n$, donde $\ker(f) = n\mathbb{Z} \neq \{[0]_n\}$. Entonces, por el teorema 2.15.2, se concluye que f no es inyectiva.

Ejemplo 2.15.6.

En el ejemplo 2.15.3 se halló el núcleo del homomorfismo $f : (\mathbb{R}, +) \to (\mathbb{S}^1, *)$ defino por el criterio $f(x) := (\cos(x), \sin(x))$, donde $\ker(f) = \{2k\pi : k \in \mathbb{Z}\} \neq \{(1, 0)\}$. Entonces, por el teorema 2.15.2, se concluye que f no es inyectiva.

Ejemplo 2.15.7.



Considere el grupo $M(2,\mathbb{R})$ con la suma usual de matrices. Defina $f : (M(2,\mathbb{R},+)) \to f(M(2,\mathbb{R}),+)$ tal que

$$f\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a-d & 0 \\ 0 & b-c \end{pmatrix}.$$

Muestre que f es un homomorfismo de grupos y determine si f es inyectiva a partir del núcleo de f.

Demostración. Para probar que f es un homomorfismo, tome $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ y $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ elementos de $M(2,\mathbb{R})$ y note que:

$$\begin{aligned} f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right) &= f\begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix} \\ &= \begin{pmatrix} a+a'-d-d' & 0 \\ 0 & b+b'-c-c' \end{pmatrix} \\ &= \begin{pmatrix} a-d & 0 \\ 0 & b-c \end{pmatrix} + \begin{pmatrix} a'-d' & 0 \\ 0 & b'-c' \end{pmatrix} \\ &= f\begin{pmatrix} a & b \\ c & d \end{pmatrix} + f\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}. \end{aligned}$$

Para hallar el núcleo de f, este se define como

$$\ker(f) = \{A \in M(2,\mathbb{R}) : f(A) = 0_{2\times 2}\}.$$

Así, sea $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \ker(f)$, es decir, $f\begin{pmatrix} a & b \\ d & d \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, lo que implica que

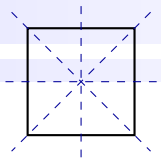
$$f\begin{pmatrix} a-d & 0 \\ 0 & b-c \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

De acá se construye el sistema

$$\begin{cases} a-d=0 \\ b-c=0 \end{cases},$$

de donde se deduce que $a=d$ y $b=c$. De esta forma

$$\ker(f) = \left\{\begin{pmatrix} a & b \\ b & a \end{pmatrix} : a,b \in \mathbb{R}\right\} \neq \left\{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right\},$$



de donde también se deduce que f no es inyectiva. □

Ejemplo 2.15.8.

Considere el grupo cíclico de orden 3 dado por $G = \{e, g, g^2\}$ cuyo cuadro de operaciones se aprecia a continuación:

$\cdot$	e	g	g^2
e	e	g	g^2
g	g	g^2	e
g^2	g^2	e	g

Además, considere el grupo simétrico S_3 del ejemplo 2.1.31 y defina la función $f : (G, \cdot) \to (S_3, \circ)$ por

$$f(e) = \sigma_1, \quad f(g) = \sigma_4, \quad f(g^2) = \sigma_5.$$

Muestre que f es un homomorfismo y establezca si es inyectiva o no a partir de su núcleo.

Demostración. Para probar que f es un homomorfismo note que:

- $f(e \cdot e) = f(e) = \sigma_1 = \sigma_1 \circ \sigma_1 = f(e) \circ f(e)$.
- $f(e \cdot g) = f(g) = \sigma_4 = \sigma_1 \circ \sigma_4 = f(e) \circ f(g)$.
- $f(e \cdot g^2) = f(g^2) = \sigma_5 = \sigma_1 \circ \sigma_5 = f(e) \circ f(g^2)$.
- De forma análoga ocurre para $f(g \cdot e) = f(g) \circ f(e)$ y $f(g^2 \cdot e) = f(g^2) \circ f(e)$.
- $f(g \cdot g) = f(g^2) = \sigma_5 = \sigma_4 \circ \sigma_4 = f(g) \circ f(g)$.
- $f(g \cdot g^2) = f(e) = \sigma_1 = \sigma_4 \circ \sigma_5 = f(g) \circ f(g^2)$.
- $f(g^2 \cdot g) = f(e) = \sigma_1 = \sigma_5 \circ \sigma_4 = f(g^2) \circ f(g)$.
- $f(g^2 \cdot g^2) = f(g) = \sigma_4 = \sigma_5 \circ \sigma_5 = f(g^2) \circ f(g^2)$.

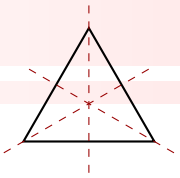
De acuerdo con lo anterior se puede asegurar que f es un homomorfismo. Para hallar su núcleo, se tiene que

$$\ker(f) = \{x \in G : f(x) = \sigma_1\}.$$

Es decir, $\ker(f) = \{e\}$ y por lo tanto, f sí es inyectiva. El ejercicio no lo pide, pero es claro que

$$\mathrm{Im}(f) = \{f(g) : g \in G\} = \{\sigma_1, \sigma_4, \sigma_5\}.$$

□



Teorema 2.15.2:

Sean G_1 y G_2 dos grupos y sea $f : G_1 \to G_2$ un homomorfismo. Entonces

1. $\ker(f)$ es un subgrupo normal de G_1.
2. $\text{Im}(f)$ es un subgrupo de G_2

Demostración.

1. Por facilidad, denote por K el núcleo de f, es decir, $K = \ker(f)$. Se debe probar que para cualquier $g \in G_1$ se tiene $g^{-1}Kg \subseteq K$. Para ello, sea $x \in g^{-1}Kg$, entonces x es de la forma $x = g^{-1}kg$ para algún $k \in K$. Ahora, note que:

$$\begin{aligned} f(x) &= f(g^{-1}kg) \\ &= f(g^{-1})f(k)f(g) \quad \text{pues } f \text{ es un homomorfismo.} \\ &= f(g)^{-1}f(k)f(g) \quad \text{por el teorema 2.14.1.} \\ &= f(g)^{-1}e_2 f(g) \quad \text{pues } k \in K \text{ y donde } e_2 \text{ es el neutro de } G_2. \\ &= f(g)^{-1}f(g) \\ &= e_2. \end{aligned}$$

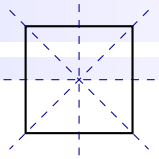
   Esto prueba que $x \in K$ y como $x = g^{-1}Kg$ es arbitrario, se tiene $g^{-1}Kg \subseteq K$. Por lo tanto $\ker(f) \lhd G_1$.

2. Sean $y_1, y_2 \in \text{Im}(f)$, se debe probar que $y_1 y_2^{-1} \in \text{Im}(f)$. Ahora, como $y_1, y_2 \in \text{Im}(f)$, existen $x_1, x_2 \in G_1$ tales que $f(x_1) = y_1$ y $f(x_2) = y_2$. Entonces

$$\begin{aligned} y_1 y_2^{-1} &= f(x_1)f(x_2)^{-1} \\ &= f(x_1)f(x_2^{-1}) \quad \text{por el teorema 2.14.1.} \\ &= f(x_1 x_2^{-1}) \quad \text{pues } f \text{ es un homomorfismo.} \end{aligned}$$

   Luego, dado que $x_1, x_2 \in G_1$ se cumple $x_1 x_2^{-1} \in G_1$ y como $f(x_1 x_2^{-1}) = y_1 y_2^{-1}$, se deduce que la preimagen de $y_1 y_2^{-1}$ es $x_1 x_2^{-1}$, lo cual prueba que $y_1 y_2^{-1} \in \text{Im}(f)$. Por lo tanto, por el teorema 2.7.1, se concluye que $\text{Im}(f) < G_2$.

□



Ejemplo 2.15.9.

En el ejemplo 2.15.2 se halló el núcleo del homomorfismo $f : (\mathbb{Z}, +) \to (\mathbb{Z}_n, +)$ tal que $f(x) := [x]_n$, donde $\ker(f) = n\mathbb{Z}$. Entonces, por el teorema 2.15.2 se concluye que $n\mathbb{Z}$ es un subgrupo normal de $(\mathbb{Z}, +)$.

Ejemplo 2.15.10.

En el ejemplo 2.15.7 se concluyó que

$$\ker(f) = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} : a, b \in \mathbb{R} \right\}$$

es el núcleo del homomorfismo $f : (M(2, \mathbb{R}, +)) \to f(M(2, \mathbb{R}), +)$ tal que

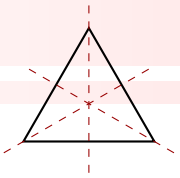
$$f \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a-d & 0 \\ 0 & b-c \end{pmatrix}.$$

Por lo tanto, por el teorema 2.15.2 se establece que $\left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} : a, b \in \mathbb{R} \right\}$ es un subgrupo normal de $(M(2, \mathbb{R}, +))$.

2.16 Teoremas de isomorfismos

En el marco de la Teoría de Grupos, los teoremas de isomorfismos constituyen herramientas esenciales que permiten comprender las relaciones estructurales entre diferentes grupos. De manera objetiva, estos teoremas establecen conexiones algebraicas sustanciales al revelar correspondencias biyectivas entre grupos bajo ciertas condiciones.

La historia de los teoremas de isomorfismo en la Teoría de Grupos se remonta a desarrollos fundamentales a lo largo del siglo XIX y XX en el campo matemático. Aunque el concepto de isomorfismo, que establece una correspondencia biyectiva preservando la estructura algebraica entre dos grupos, era cono-



cido, fue Emil Artin[10] y Richard Brauer [11] quienes, en la década de 1930, formalizaron y generalizaron estos teoremas para una amplia gama de grupos.

La contribución clave de Artin y Brauer permitió establecer conexiones más profundas entre grupos, facilitando la comprensión de sus propiedades comunes. Los teoremas de isomorfismo se volvieron fundamentales para la clasificación de grupos, simplificando el estudio de sus propiedades sin perder la esencia de su estructura algebraica.

A lo largo del tiempo, los teoremas de isomorfismo han evolucionado y se han convertido en un componente central de la Teoría de Grupos moderna. Han encontrado aplicaciones no solo en Matemáticas puras, sino también en áreas como la teoría de números, la criptografía y la física teórica

[10]Emil Artin fue un eminente matemático austriaco nacido el 3 de marzo de 1898 en Viena y fallecido el 20 de diciembre de 1962 en Hamburgo. Su vida y obra dejaron una marca indeleble en la matemática del siglo XX.

Artin realizó contribuciones fundamentales en diversas áreas de las matemáticas, destacando en álgebra, teoría de números y geometría algebraica. Después de completar su doctorado en Viena en 1921, Artin trabajó en varias universidades europeas antes de emigrar a los Estados Unidos en 1938 debido al ascenso del nazismo.

En su carrera, Artin desarrolló conceptos cruciales en álgebra abstracta y teoría de números. Introdujo la noción de anillos noetherianos y noetherianos, estableció la teoría de cuerpos de clases y contribuyó significativamente a la teoría de formas cuadráticas.

Artin también desempeñó un papel vital en la formación de futuros matemáticos. Fue profesor en la Universidad de Gotinga y, más tarde, en la Universidad de Princeton, donde influyó en la formación de la escuela algebraica de Gotinga. Su trabajo y método en la enseñanza impactaron a generaciones de matemáticos.

Emil Artin fue un miembro destacado del grupo Bourbaki y un colaborador activo en el desarrollo de la teoría de números algebraicos. Su legado incluye teoremas y conceptos esenciales en álgebra moderna que continúan siendo fundamentales en la investigación matemática contemporánea. Consultar Zassenhaus (1964)

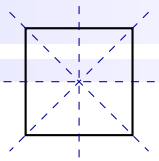
[11]Richard Brauer fue un eminente matemático alemán nacido el 10 de febrero de 1901 en Charlottenburg, Alemania, y fallecido el 17 de abril de 1977 en Belmont, Massachusetts, Estados Unidos. Su carrera en matemáticas abarcó una variedad de áreas, destacándose en la teoría de grupos y la teoría de representación.

Después de completar su doctorado en 1925 bajo la supervisión de Issai Schur en la Universidad de Gotinga, Brauer trabajó en varias instituciones académicas europeas antes de huir de la persecución nazi y establecerse en los Estados Unidos en 1937.

Brauer realizó contribuciones significativas en la teoría de grupos finitos y desarrolló la teoría de bloques, que proporciona un marco para entender los caracteres y representaciones de grupos finitos. También hizo aportes cruciales a la teoría de números algebraicos y la teoría de álgebras asociativas.

Durante su carrera, Brauer fue profesor en la Universidad de Toronto y luego en la Universidad de Harvard. También fue miembro clave del grupo Bourbaki y desempeñó un papel crucial en la expansión y desarrollo de la teoría de grupos finitos.

Su trabajo ha tenido un impacto duradero en la teoría de números y en la teoría de grupos. Brauer recibió numerosos reconocimientos a lo largo de su carrera, incluyendo la Medalla Nacional de Ciencia de los Estados Unidos. Su legado perdura a través de sus contribuciones a la Matemática y su influencia en las generaciones futuras de matemáticos. Consultar O'Connor (2024b)



Teorema 2.16.1: Primer teorema de isomorfismos de grupos

Sea $f : G_1 \to G_2$ un homomosfismo de grupos con núcleo $\ker(f)$ y con imagen $\text{Im}(f)$. Entonces

$$G_1/\ker(f) \cong \text{Im}(f) \tag{2.15}$$

Demostración. Por simplicidad de escritura se usará la letra K para denotar el núcleo de f, es decir $K = \ker(f)$. Observe que por el teorema 2.15.2 ya se tiene que K es un subgrupo normal de G_1, entonces por el teorema 2.12.1 el cociente G_1/K es un grupo. Con esto claro, defina la función $\varphi : G_1/K \to \text{Im}(f)$ tal que

$$\varphi(xK) = f(x), \quad \text{para todo } x \in G_1.$$

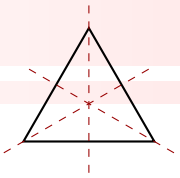
Primero se probará que φ es función, en otras palabras que φ está bien definida. Para ello, sean $x, y \in G_1$, tales que $xK = yK$ en G_1/K. Por la parte cuatro del teorema 2.9.2 se tiene que $x \in yK$, es decir, $x = yk$, para algún $k \in K$, lo cual implica que

$$\begin{aligned} f(x) &= f(yk) \\ &= f(y)f(k) \quad \text{puesto que } f \text{ es un homomorfismo.} \\ &= f(y)e_2 \quad \text{puesto que } k \text{ está en el núcleo de } f. \\ &= f(y), \end{aligned}$$

es decir, $f(x) = f(y)$, entonces se tiene que $\varphi(xK) = \varphi(yK)$, lo que implica que φ está bien definida. Ahora, se probará que φ es un homomorfismo. Sean $xK, yK \in G_1/K$. Por la definición de la operación en G_1/K (teorema 2.12.1) se tiene que

$$\begin{aligned} \varphi(xKyK) &= \varphi(xyK) \\ &= f(xy) \\ &= f(x)f(y) \\ &= \varphi(xK)\varphi(yK). \end{aligned}$$

Entonces, $\varphi(xKyK) = \varphi(xK)\varphi(yK)$, lo que permite establecer que φ es un homomorfismo. También, se debe probar que φ es inyectiva, para lo cual recuerde que el elemento neutro en G_1/K es K y por el teorema 2.15.1 la función φ es inyectiva si y sólo si $\ker(\varphi) = K$. En este sentido, se mostrará que



$\ker(\varphi) = \{K\} = \{\ker(f)\}$. Luego, note que

$$\begin{aligned}\ker(\varphi) =& \{xK \in G_1/K \,:\, \varphi(xk) = e_2\} \\ =& \{xK \in G_1/K \,:\, f(x) = e_2\} \quad \text{puesto que } \varphi(xk) = f(x),\end{aligned}$$

donde e_2 es el elemento neutro en la $\mathrm{Im}(f)$. Además, por el teorema 2.15.2 se tiene que $\mathrm{Im}(f)$ es un subgrupo de G_2, por lo que también $e_2 \in \mathrm{Im}(f)$. De esta forma, si $f(x) = e_2$, entonces x debe ser un elemento del núcleo de f, es decir, $x \in K$, y por lo tanto $xK = K$, de donde se deduce que

$$\begin{aligned}\ker\varphi =& \{xK \in G_1/K \,:\, f(x) = e_2\} \\ =& \{K \in G_1/K \,:\, x \in K\} \\ =& \{K\},\end{aligned}$$

con lo cual se concluye que φ es inyectiva. Finalmente, φ es sobreyectiva por la definición de f, con lo cual φ es biyectiva. En resumen, $\varphi : G_1/K \to \mathrm{Im}(f)$ es una función que corresponde a un isomorfismo y por lo tanto

$$G_1/\ker(f) \cong \mathrm{Im}(f).$$

□

Observación 2.16.1.

Si $f : G_1 \to G_2$ es un homomorfismo sobreyectivo, es decir, $\mathrm{Im}(f) = G_2$, entonces el teorema anterior establece que

$$G_1/\ker(f) \cong G_2.$$

Ejemplo 2.16.1.

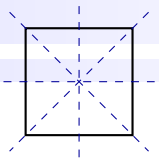
Sea $f : (\mathbb{R}^+, \cdot) \to (\mathbb{R}, +)$ definida por

$$f(x) := \ln x.$$

En el ejemplo 2.15.1 se probó que f es un homomorfismo con núcleo $\ker(f) = \{1\}$. También se probó en el ejemplo 2.15.4 que f es inyectiva y como f es una función estrictamente creciente, f es biyectiva. En particular f es sobreyectiva, es decir, $\mathrm{Im}(f) = \mathbb{R}$, entonces por el primer teorema de isomorfismos de grupos (teorema 2.16.1) se tiene que

$$\mathbb{R}^+/\{1\} \cong \mathbb{R}.$$

Ejemplo 2.16.2.



Considere el homomorfismo $f : (\mathbb{Z}, +) \to (\mathbb{Z}_n, +)$ tal que $f(x) := [x]_n$ donde $\ker(f) = n\mathbb{Z}$ (ver ejemplo 2.15.2). Muestre que

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n.$$

Demostración. De acuerdo con la observación 2.16.1 solo basta verificar que f sea sobreyectiva, es decir, que sea un epimorfismo. En efecto, si dado $[x]_n$ en el dominio $\mathbb{Z}_n$, la preimagen es $x \in \mathbb{Z}$, así f es sobreyectiva y por el primer teorema de isomorfismos de grupos (teorema 2.16.1) se cumple que

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n.$$

□

Ejemplo 2.16.3.

Considere el grupo de matrices $n \times n$ ortogonales con determinante igual a uno definido por

$$SL(n, \mathbb{R}) := \{A \in GL(n, \mathbb{R}) \mid \det(A) = 1\} \quad \text{(ver ejercicio ??)}.$$

Demostrar que $GL(2, \mathbb{R})/SL(2, \mathbb{R}) \cong \mathbb{R} - \{0\}$.

Demostración. Se va a utilizar el primer teorema de isomorfismos de grupos (teorema 2.16.1), para lo cual defina la función

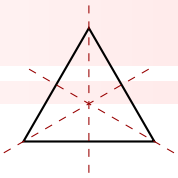
$$f : (GL(2, \mathbb{R}), \cdot) \to (\mathbb{R} - \{0\}, \cdot) \quad \text{tal que } f(A) := \det A.$$

En el ejemplo 2.14.7 se mostró que f es un homomorfismo (tome $n = 2$). Luego, se procede a hallar el núcleo de f. Con este fin, observe que una matriz $A \in GL(2, \mathbb{R})$ está en el núcleo de f si $f(A) = 1$, es decir, si $\det A = 1$, por lo que

$$\begin{aligned} \ker(f) &= \{A \in GL(2, \mathbb{R}) : \det A = 1\} \\ &= SL(2, \mathbb{R}). \end{aligned}$$

Por otro lado, f es un homomorfismo sobreyectivo. Para ver esto, note que dada una arbitraria imagen $x \in \mathbb{R} - \{0\}$, entonces la matriz $\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} \in GL(2, \mathbb{R})$ es una preimagen de x puesto que

$$f\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} = \det\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} = x.$$



Por lo tanto, por el primer teorema de isomorfismos de grupos se concluye que

$$GL(2,\mathbb{R})/SL(2,\mathbb{R}) \cong \mathbb{R} - \{0\}.$$

□

Ejemplo 2.16.4.

Demostrar que

$$\mathbb{Z}/2\mathbb{Z} \cong \{-1, 1\}.$$

Demostración. Considere la función $f : (\mathbb{Z}, +) \to (\{-1, 1\}, \cdot)$ definida por

$$f(x) := \begin{cases} 1 & \text{si} \quad x \text{ es par.} \\ -1 & \text{si} \quad x \text{ es impar.} \end{cases}$$

No es difícil verificar que la función f es un homomorfismo de grupos y que es sobreyectiva, con núcleo $\ker(f) = 2\mathbb{Z}$. Entonces, por el primer teorema de isomorfismos se cumple que $\mathbb{Z}/2\mathbb{Z} \cong \{-1, 1\}$. □

Observación 2.16.2.

Por la observación 2.9.3 se tiene que $\mathbb{Z}/2\mathbb{Z} = \mathbb{Z}_2$, entonces, por el ejemplo anterior el grupo $(\mathbb{Z}_2, +)$ es isomorfo al grupo $(\{-1, 1\}, \cdot)$.

Teorema 2.16.2: Segundo teorema de isomorfismos de grupos.

Sean G un grupo y sean N un subgrupo normal de G y H un subgrupo de G, entonces

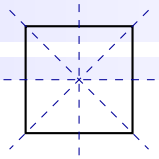
$$H/H \cap N \cong HN/N. \tag{2.16}$$

Demostración. Defina $\varphi : H \to HN/N$ por

$$\varphi(h) := hN,$$

Por el primer teorema de isomorfismos de grupos (teorema 2.16.1) basta probar que φ está bien definida, que es un homomorfismo, que es sobreyectiva y que $\ker(\varphi) = H \cap N$.

1. Para mostrar que φ está bien definida equivale a probar que φ es función. Para ello, considere $x, y \in H$ tales que $x = y$. Esto implica que $xN = yN$ y según como está definido φ, se cumple que $\varphi(x) = \varphi(y)$. Por lo tanto φ está bien definida.



2. Para probar que φ es un homomorfismo, sean $x, y \in H$, entonces

$$\begin{aligned} \varphi(xy) &= (xy)N \\ &= xNyN \quad \text{recordando que } N \lhd G \text{ y usando el teorema 2.12.1.} \\ &= \varphi(x)\varphi(y). \end{aligned}$$

   Esto comprueba que φ en efecto es un homomorfismo.

3. Para verificar que φ es sobreyectiva considere $xN \in HN$ con $x \in H$ y observe que $\varphi(x) = xN$, es decir, la preimagen de xN es x, lo cual prueba que φ es sobreyectiva.

4. Para probar que a $\ker(\varphi) = H \cap N$ se mostrará que se cumplen las inclusiones $\ker(\varphi) \subseteq H \cap N$ y $\ker(\varphi) \supseteq H \cap N$.

   - ($\subseteq$) Sea $x \in \ker(\varphi)$ entonces $\varphi(x) = N$ pues N es el elemento neutro en el grupo cociente HN/N. Además, por la definición de φ se cumple que $xN = N$, de donde se induce que $x \in N$. Por otro lado, $x \in H$ porque es parte del dominio de φ, entonces $x \in H \cap N$. Por lo tanto $\ker(\varphi) \subseteq H \cap N$.
   - ($\supseteq$) Sea $x \in H \cap N$, en particular $x \in N$, entonces $\varphi(x) = xN = N$, es decir, $x \in \ker(\varphi)$, por lo que $H \cap N \subseteq \ker(\varphi)$. De lo anterior se concluye que $H \cap N = \ker(\varphi)$. Además, por el teorema 2.15.2 se cumple que $H \cap N$ es un subgrupo normal de H.

Finalmente, por el primer teorema de isomorfismos se tiene que

$$H/H \cap N = H/\ker(\varphi) \cong \mathrm{Im}(\varphi) = HN/N.$$

□

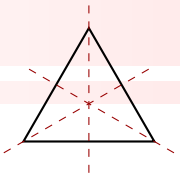
Ejemplo 2.16.5.

Considere el grupo $\mathbb{Z}$ con la suma usual y considere $H := 6\mathbb{Z}$ y $N := 4\mathbb{Z}$. Observe que $6\mathbb{Z} < \mathbb{Z}$ y $4\mathbb{Z} \lhd Z$. Además $6\mathbb{Z} \cap 4\mathbb{Z} = 12\mathbb{Z}$ y $6\mathbb{Z} + 4\mathbb{Z} = 2\mathbb{Z}$. Entonces, por el segundo teorema de isomorfismos se tiene que

$$6\mathbb{Z}/(6\mathbb{Z} \cap 4\mathbb{Z}) \cong (6\mathbb{Z} + 4\mathbb{Z})/4\mathbb{Z},$$

es decir,

$$6\mathbb{Z}/12\mathbb{Z} \cong 2\mathbb{Z}/4\mathbb{Z}.$$



Teorema 2.16.3: Tercer teorema de isomorfismos de grupos.

Sean G un grupo y N y H subgrupos normales de G tales que N es subgrupo de H. Entonces

$$(G/N)/(H/N) \cong G/H \tag{2.17}$$

Demostración. Defina $\varphi : G/N \to G/H$ por

$$\varphi(gN) := gH.$$

Por el primer teorema de isomorfismos de grupos (teorema 2.16.1) es suficiente probar que φ está bien definida, que es un homomorfismo, que es sobreyectiva y que $\ker(\varphi) = H/N$.

1. Para probar que φ está bien definida equivale a verifcar que φ es función. Para ello considere $xN, yN \in G/N$, con $x, y \in G$, tales que $xN = yN$. Entonces, por la parte cuatro del teorema 2.9.2 se tiene que $x \in yN$, es decir, existe un $n \in N$ tal que $x = yn$. Pero como $N < H$ por hipótesis, entonces $n \in H$, así

   $$x = yn \text{ para algún } n \in H.$$

   Esto equivale a que $x \in yH$ lo cual implica que $xH = yH$. Ahora, por la definición de φ esto es

   $$\varphi(xH) = \varphi(yH).$$

   Por lo tanto φ está bien definida.

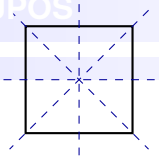
2. Para probar que φ es un homomorfismo, considere $xN, yN \in G/N$, entonces,

   $$\begin{aligned} \varphi(xNyN) &= \varphi(xyN) \\ &= xyH \quad \text{por la definición de } \varphi. \\ &= xHyH \\ &= \varphi(xN)\varphi(yH), \end{aligned}$$

   lo que comprueba que φ es un homomorfismo.

3. Para probar la sobreyectividad de φ considere $xH \in G/H$, con $x \in G$. Observe que una preimagen de xH es $xN \in G/N$ pues $\varphi(xN) = xH$, lo cual muestra que φ es sobreyectiva.

4. Para mostrar que $\ker(\varphi) = H/N$ se usará la definición de igualdad de conjuntos, con lo cual se debe probar que $\ker(\varphi) \subseteq H/N$ y $\ker(\varphi) \supseteq H/N$.



- ($\subseteq$) Sea $xN \in \ker(\varphi)$. Dado que el neutro en G/H es H se tiene que $\varphi(xN) = H$, que a su vez, por la definición de φ, se cumple que $xH = H$. Esto implica que $x \in H$ por lo que $xN \in H/N$. Por lo tanto $\ker(\varphi) \subseteq H/N$.
- ($\supseteq$) Sea $xN \in H/N$ con $x \in H$. Como H es el elemento neutro en G/H y $x \in H$ entonces $\varphi(xN) = xH = H$. Esto quiere decir que $xN \in \ker(\varphi)$, por lo que $H/N \subseteq \ker(\varphi)$. De lo anterior se concluye que $H/N = \ker(\varphi)$. Además, por el teorema 2.15.2 se cumple que H/N es un subgrupo normal de G/N.

Finalmente, por el primer teorema de isomorfismos se tiene que

$$(G/N)/(H/N) = (G/N)/\ker(\varphi) \cong \mathrm{Im}(\varphi) = G/H.$$

□

Ejemplo 2.16.6.

Considere el grupo $G := \mathbb{Z}$ con la suma usual. También considere los subgrupos $H := 2\mathbb{Z}$ y $N := 10\mathbb{Z}$ con la suma de clases respectivas. Como $\mathbb{Z}$ es abeliano, entonces $2\mathbb{Z}$ y $10\mathbb{Z}$ son subgrupos normales de $\mathbb{Z}$. Además, observe que $10\mathbb{Z}$ es un subgrupo de $2\mathbb{Z}$. Entonces por el tercer teorema de isomorfismos se cumple que

$$(\mathbb{Z}/10\mathbb{Z})/(2\mathbb{Z}/10\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}.$$

2.17 Descomposición canónica de un homomorfismo de grupos

De acuerdo con lo que se ha estudiando hasta ahora, es posible que un homomorfismo de grupos se pueda expresar como la composición de un monomorfismo, un isomorfismo y un epimorfismo. Esta descomposición es útil para analizar y entender la estructura de homomorfismos entre grupos. Para explicar la descomposición canónica, considere un homomorfismo de grupos $f : G_1 \to G_2$, además, por simplicidad de escritura se usará la letra K para denotar el núcleo de f, es decir $K = \ker(f)$. La descomposición se realiza en tres pasos:

1. Por el teorema 2.15.2 se tiene que $K \lhd G_1$ y por los ejemplos 2.14.10 y 2.14.15 la función definida por $\pi : G_1 \to G_1/K$ tal que $\pi(x) := xK$ es un epimorfismo.

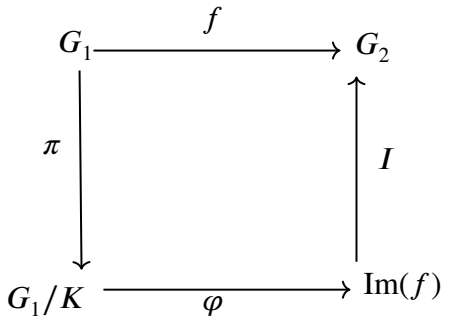
2. Por el primer teorema de isomorfismos de grupos (teorema 2.16.1), se cumple que la función dada por $\varphi : G_1/K \to \mathrm{Im}(f)$ tal que $\varphi(xK) := f(x)$, para cada $x \in G_1$, es un isomorfismo.

3. Considere el homomorfismo dado por la función inclusión $I : \text{Im}(f) \to G_2$ tal que $I(x) := x$ para cada $x \in \text{Im}(f)$. En este caso, como $\text{Im}(f) \subseteq G_2$, entonces I es inyectivo y por lo tanto es un monomorfismo.

Luego, observe que:

$$\begin{aligned}(I \circ \varphi \circ \pi)(x) &= I(\varphi(\pi(x))) \\ &= I(\varphi(xK)) \\ &= I(f(x)) \\ &= f(x).\end{aligned}$$

Por lo tanto, $f(x) = (I \circ \varphi \circ \pi)(x)$, la cual es llamada descomposición canónica de un homomorfismo de grupos. En forma resumida y de esquema se puede expresar de la siguiente manera:



$\pi(x) = xK$, para cada $x \in G_1$, es un epimorfismo.
$\varphi(xK) = f(x)$, para cada $x \in G_1$, es un isomorfismo.
$I(x) = x$, para cada $x \in \text{Im}(f)$, es un monomorfismo.

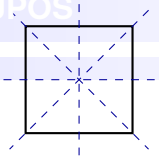
Figura 2.11: Descomposición canónica del homomorfismo f
Fuente: Elaboración propia

Ejemplo 2.17.1.

Considere el homomorfismo $f : (GL(2, \mathbb{R}), \cdot) \to (\mathbb{R} - \{0\}, \cdot)$ definido por

$$f(A) := \det A$$

como en ejemplo 2.14.7 con $n = 2$, donde "$\cdot$" denota el producto usual de matrices para el dominio y el



producto usual de números reales para el codominio. En la demostración del ejemplo 2.16.3 se determinó que

$$\ker(f) = SL(2,\mathbb{R}) = \{A \in GL(2,\mathbb{R}) : \det A = 1\}.$$

Además, note que $\text{Im}(f) = \mathbb{R} - \{0\}$. De esta forma, la descomposición canónica del homomorfismo $f : (GL(2,\mathbb{R}),\cdot) \to (\mathbb{R} - \{0\},\cdot)$ es la siguiente:

- $\pi : GL(2,\mathbb{R}) \to GL(2,\mathbb{R})/SL(2,\mathbb{R})$ definida por $\pi(A) = A \cdot SL(2,\mathbb{R})$, para cada $A \in GL(2,\mathbb{R})$, que es un epimorfismo.
- $\varphi : GL(2,\mathbb{R})/SL(2,\mathbb{R}) \to \mathbb{R} - \{0\}$ tal que $\varphi\big(A \cdot SL(2,\mathbb{R})\big) = f(A) = \det A$, esto para cada $A \in GL(2,\mathbb{R})$, que es un isomorfismo.
- $I : \mathbb{R} - \{0\} \to \mathbb{R} - \{0\}$ tal que $I(x) = x$, para cada $x \in \mathbb{R} - \{0\}$, que es un monomorfismo.

Con esto se tiene que

$$\begin{aligned}(I\circ\varphi\circ\pi)(A) &= I(\varphi(\pi(A)))\\ &= I(\varphi(A \cdot SL(2,\mathbb{R})))\\ &= f(A)\\ &= I(\det A)\\ &= \det A\\ &= f(A).\end{aligned}$$

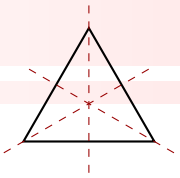
Ejemplo 2.17.2.

Considere el homomorfismo del ejemplo 2.14.14 definido por $f : (\mathbb{Z},+) \to (\mathbb{Z}_n,+)$, tal que $f(x) := [x]_n$, donde $[x]_n$ denota la clase de x en módulo n. Además, en el ejemplo 2.15.2 se concluyó que $\ker(f) = n\mathbb{Z}$. También es importante recordar que por la observación 2.9.3 se tiene que si n es un número entero, entonces

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n.$$

Por otro lado note que $\text{Im}(f) = \mathbb{Z}_n$. Así, la descomposición canónica del homomorfismo dado por $f : (\mathbb{Z},+) \to (\mathbb{Z}_n,+)$ es la siguiente:

- $\pi : \mathbb{Z} \to \mathbb{Z}_n$ tal que $\pi(x) = [x]_n$, para cada $x \in \mathbb{Z}$, que es un epimorfismo.
- $\varphi : \mathbb{Z}_n \to \mathbb{Z}_n$ tal que $\varphi\big([x]_n\big) = f(x) = [x]_n$, esto para cada $x \in \mathbb{Z}$, que es un isomorfismo.



- $I : \mathbb{Z}_n \to \mathbb{Z}_n$ tal que $I([x]_n) = [x]_n$, para cada $[x]_n \in \mathbb{Z}_n$, que es un monomorfismo.

Con esto se tiene que

$$\begin{aligned}(I\circ\varphi\circ\pi)([x]_n) &= I(\varphi(\pi([x]_n)))\\ &= I(\varphi([x_n])\\ &= I(f(x))\\ &= I([x]_n)\\ &= [x]_n\\ &= f(x).\end{aligned}$$

Ejemplo 2.17.3.

En el ejemplo 2.14.9 se probó que $f : (\mathbb{R}, +) \to (\mathbb{S}^1, *)$ tal que $f(x) := (\cos(x), \sin(x))$ es un homomorfismo y en el ejemplo 2.15.3 se determinó que

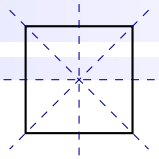
$$\ker(f) = \{2k\pi : k \in \mathbb{Z}\}.$$

Además note que $\mathrm{Im}(f) = \mathbb{S}^1$. De esta forma, la descomposición canónica del homomorfismo definido por $f : (\mathbb{R}, +) \to (\mathbb{S}^1, *)$ es la siguiente:

- $\pi : \mathbb{R}/\ker(f) \to \mathbb{R}$ tal que $\pi(x) = x\ker(f)$, para cada $x \in \mathbb{R}$, que es un epimorfismo.
- $\varphi : \mathbb{R}/\ker(f) \to \mathbb{S}^1$ tal que $\varphi\big(x\ker(f)\big) = f(x) = (\cos(x), \mathrm{sen}(x))$, esto para cada $x \in \mathbb{R}$, que es un isomorfismo.
- $I : \mathbb{S}^1 \to \mathbb{S}^1$ tal que $I(x, y) = (x, y)$, para cada $(x, y) \in \mathbb{S}^1$, que es un monomorfismo.

Adicionalmente, note que

$$\begin{aligned}(I\circ\varphi\circ\pi)(x) &= I(\varphi(\pi(x)))\\ &= I(\varphi(x\ker(f))\\ &= I(f(x))\\ &= I(\cos(x), \mathrm{sen}(x))\\ &= (\cos(x), \mathrm{sen}(x))\\ &= f(x).\end{aligned}$$



2.18 Ejercicios

R/ p.360

● Ejercicio 2.18.1 (Homomorfismo)

Considere $f : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}_n, +)$ definida por $f(x) = [x]$.

Verifique que f es un homomorfismo de grupos.

Halle $\ker(f)$.

R/ p.362

● Ejercicio 2.18.2 (Homomorfismo)

Considere la función $f : (\mathbb{R} \times \mathbb{R}, +) \longrightarrow (\mathbb{R}, +)$ definida por $f(x, y) = x + y$.

Muestre que f es un homomorfismo de grupos.

Muestre que $\ker(f) = \{(x, -x) : x \in \mathbb{R}\}$.

R/ p.364

● Ejercicio 2.18.3 (Homomorfismo)

Sea $n \in \mathbb{N}$ y sea $f : \left(U_n, \cdot\right) \to \left(U_n, \cdot\right)$, definida por

$$f\left([k]\right) := [k]^m$$

Muestre que f es un homomorfismo.

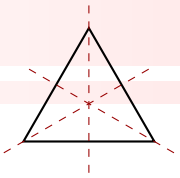
R/ p.366

● Ejercicio 2.18.4 (Homomorfismo)

Considere el grupo $\mathbb{Z}_2 \times \mathbb{Z}_2$, con la operación $([a], [b]) + ([c], [d]) := ([a] + [c], [b + d][])$. Considere también el grupo de unidades $U_8 = \{[1], [3], [5], [7]\}$, con la multiplicación de clases módulo 8. Defina $f : \mathbb{Z}_2 \times \mathbb{Z}_2 \to U_8$ por

$$f([a], [b]) := [3^a 5^b]$$

Muestre que f es un homomorfismo.



● Ejercicio 2.18.5 (Homomorfismo) R/ p.368

Sea $(G, \dot{})$ un grupo. Muestre que el conjunto $Aut(G)$, de automorfismos de G en G, es un grupo con la composición de funciones.

● Ejercicio 2.18.6 (Homomorfismo) R/ p.370

Sean G y H dos grupos tales que $G \cong H$. Muestre que el conjunto $Aut(G) \cong Aut(H)$.

Sugerencia: Como $G \cong H$, existe un isomorfismo $f : G \to H$. Defina $T_f : Aut(G) \to Aut(H)$, por $T_f(h) = f \circ h \circ f^{-1}$.

● Ejercicio 2.18.7 (Homomorfismo) R/ p.372

Considere los siguientes enunciados sobre Homomorfismos de $\mathbb{Z}_n$

Si G es un grupo, $n \in \mathbb{N}$ y $\varphi : \mathbb{Z}_n \to G$ es un homomorfismo, muestre que

$$\varphi([k]) = \varphi([1])^k$$

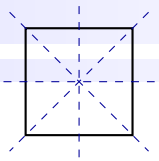
para todo $k \in \mathbb{Z}$. Concluya que $\varphi([1])|n$

Si $\varphi' : \mathbb{Z}_n \to G$ es otro homomorfismo, muestre que $\varphi = \varphi'$ si y solo si $\varphi(1) = \varphi'(1)$.

Si $g \in G$ muestre que la función $\varphi : \mathbb{Z}_n \to G$ dada por $\varphi([k]) = g^k$ está bien definida si y solo si $|g||n$. En tal caso muestre que φ es un homomorfismo.

Concluya que el conjunto de homorfismos de $\mathbb{Z}_n$ en G está en biyección con $\{g \in G : |g||n\}$.

Liste todos los homomorfismos de $\mathbb{Z}_{20}$ en $\mathbb{Z}_{25}$



R/ p.375 ● **Ejercicio 2.18.8 (Homomorfismo)**

Sean G_1 y G_2 grupos y sea $\varphi : G_1 \to G_2$ un isomorfismo.

Muestre que si g y h conmutan en G_1, entonces $\varphi(g)$ y $\varphi(h)$ conmutan en G_2.

Si $g \in G_1$, muestre que g y $\varphi(g)$, tienen el mismo orden.

Muestre que G_1 es Abeliano si y sólo si G_2 es Abeliano.

$x^k = g$ tiene el mismo número de soluciones en G_1 que $f(g) = x^k$ en H.

G_1 y G_2 tienen la misma cardinalidad, es decir, el mismo número de elementos.

R/ p.377 ● **Ejercicio 2.18.9 (Homomorfismo)**

Muestre que el conjunto de matrices

$$Gl(2,\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \quad \in \mathbb{R}, \text{donde} \quad ad - bc \neq 0 \right\}.$$

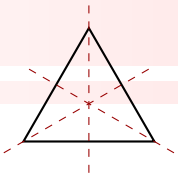
$Gl(2,\mathbb{R})$ con la multiplicación usual de matrices y el grupo $(\mathbb{R},+)$ no son isomorfos.

R/ p.378 ● **Ejercicio 2.18.10 (Homomorfismo)**

Muestre que el grupo $(\mathbb{Q} - \{0\}, \cdot)$ no es isomorfos a $(\mathbb{Z},+)$.

R/ p.379 ● **Ejercicio 2.18.11 (Homomorfismo)**

Muestre que el grupo $(\mathbb{R} - \{0\}, \cdot)$ no es isomorfo a $(\mathbb{R},+)$.



Sugerencia: Considere la ecuación $2x = a$, con $a \in \mathbb{R}$.

● **Ejercicio 2.18.12 (Homomorfismo)** R/ p.381

Se define el conjunto $SL(n,\mathbb{R}) := \{A \in GL(n,\mathbb{R}) : \det A = 1\}$.

Muestre que $SL(n,\mathbb{R})$ es subgrupo de $GL(n,\mathbb{R})$.

Muestre que $GL(n,\mathbb{R})/SL(n,\mathbb{R}) \cong \mathbb{R} - \{0\}$, (aquí $\mathbb{R} - \{0\}$ es grupo con la multiplicación usual)

● **Ejercicio 2.18.13 (Homomorfismo)** R/ p.382

Considere los grupos $\left(\mathbb{Z}_n, +\right)$, $\left(\mathbb{Z}_m, +\right)$ tales que $m|n$. Defina la función $f : \mathbb{Z}_n \to \mathbb{Z}_m$ por

$$f\left([k]_n\right) := [k]_m$$

donde $[k]_n$ y $[k]_m$ denotan las clases de k, módulo n y módulo m, respectivamente.

Muestre que f es un homomorfismo.

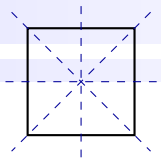
Muestre que $\ker(f) = \langle [m]_n \rangle$.

Muestre que f es sobreyectiva.

Concluya que $\mathbb{Z}_n/\langle [m]_n \rangle \cong \mathbb{Z}_m$

● **Ejercicio 2.18.14 (Homomorfismo)** R/ p.385

Muestre que si $G = \langle g \rangle$ es cíclico de orden finito, entonces $h(g^n) = g^{-n}$ es un automorfismo de G en G.



R/ p.386 ● **Ejercicio 2.18.15 (Homomorfismo)**

Sea $h : (\mathbb{R}, +) \to GL(2, \mathbb{R})$ definido por

$$h(x) = \begin{pmatrix} \cos(x) & \sin(x) \\ -\sin(x) & \cos(x) \end{pmatrix}$$

Muestre que h es un homomorfismo sobreyectivo.

R/ p.388 ● **Ejercicio 2.18.16 (Homomorfismo)**

Encuentre todos los subgrupos no triviales $\mathbb{Z}_2 \times \mathbb{Z}_2$.

R/ p.390 ● **Ejercicio 2.18.17 (Homomorfismo)**

¿Cuáles de los siguientes grupos son isomorfos entre si?

$$(\mathbb{Z}, +),\ (2\mathbb{Z}, +),\ (\mathbb{Z}_{20}, +),\ (\mathbb{Q}^+, +),\ (\mathbb{Q}^+, \cdot),\ (\mathbb{Z}_8, +),\ D_4,\ GL(2, \mathbb{R}).$$

R/ p.392 ● **Ejercicio 2.18.18 (Homomorfismo)**

Muestre que no es posible hallar un isomorfismo entre los grupos $(\mathbb{R}, +)$ y $(\mathbb{R} - \{0\}, \cdot)$.

R/ p.393 ● **Ejercicio 2.18.19 (Homomorfismo)**

Muestre que la condición de ser isomorfismo entre grupos, define una relación de equivalencia sobre el conjunto de todos los grupos.

Capítulo 3

Aplicaciones

Las matemáticas son la poesía del universo lógico

Albert Einstein

La teoría de grupos, una rama importante de las matemáticas, tiene aplicaciones extensas y diversas en diversas disciplinas como la criptografía, la física, la química, la biología, la música y la ingeniería. A continuación se hará una descripción de algunas aplicaciones que presentan el uso de dicha teoría, haciendo énfasis en la criptografía.

3.1 Música

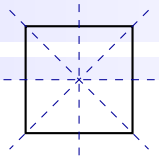
En el contexto de la composición musical, la teoría de grupos ofrece una perspectiva estructurada para analizar las relaciones entre acordes[1] y progresiones armónicas. Una aplicación interesante es la modelación de la transposición musical como una operación de grupo, lo que permite estudiar de manera sistemática cómo varían los acordes al desplazar todas sus notas en la escala.

Para ilustrar esta idea, se adopta una representación simplificada en la que cada acorde se modela como un vector en un espacio tridimensional[2], donde cada componente codifica la presencia o ausencia de una nota esencial del acorde[3]. Aunque en aplicaciones más generales se emplean espacios de mayor di-

[1] Un *acorde* es un conjunto de tres o más notas que se tocan simultáneamente, generando una sonoridad .ªpropiada"para el oído.

[2] Se considera un espacio vectorial de dimensión tres, adecuado para representar acordes formados por tres notas.

[3] En este ejemplo se utiliza una codificación binaria: el número 1 indica la presencia de la nota, mientras que el 0 indica su ausencia.



mensión (por ejemplo, considerando las 12 notas de la escala cromática), este modelo resulta adecuado para ilustrar la idea central.

Es importante aclarar que la escala cromática está compuesta por 12 notas: C, C#, D, D#, E, F, F#, G, G#, A, A# y B. Un posible modelo visual para representar esta escala es el **círculo cromático**, en el cual las 12 notas se disponen de manera equidistante sobre una circunferencia. Por ejemplo:

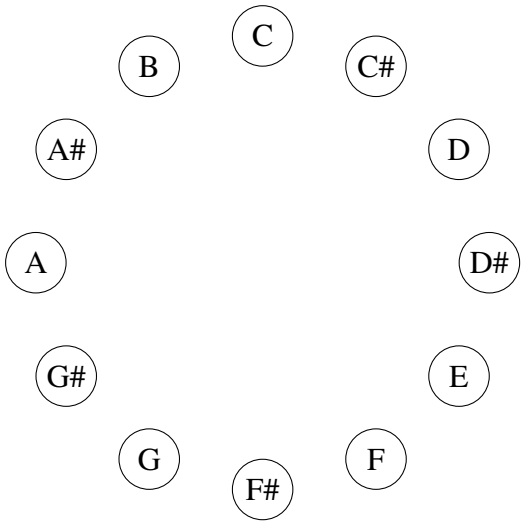


Figura 3.1: Escala cromática representada en el círculo cromático.
Fuente: Elaboración propia

Con esta representación, se puede definir la operación de *transposición* como el desplazamiento uniforme de todas las notas de un acorde por una cantidad fija de semitonos[4]. En nuestro modelo, este desplazamiento se puede interpretar como la suma de un vector constante a la representación del acorde.

Ejemplo 3.1.1.

Supóngase que se está componiendo una canción y se desea analizar la relación entre los acordes utilizados. Considere la siguiente progresión: C mayor (C), G mayor (G) y F mayor (F).

- **Paso 1: Identificación de Acordes:** Se identifican los acordes presentes en la progresión: C mayor, G mayor y F mayor.

[4]La *transposición* consiste en desplazar cada nota de un acorde o melodía por el mismo número de semitonos, preservando las relaciones relativas entre ellas.

- **Paso 2: Representación Vectorial:** Cada acorde se representa mediante un vector en $\mathbb{R}^3$. Por ejemplo, tomando una codificación simplificada, el acorde C mayor, compuesto por las notas C, E y G, se puede representar como el vector $[1, 1, 1]$[5].

- **Paso 3: Aplicación de la Transposición:** Se define la transposición como una operación que desplaza todas las notas de un acorde por un número fijo de semitonos. Sea T_k la transposición por k semitonos y sea v el vector que representa un acorde. Entonces:

$$T_k(v) = v + k \cdot d,$$

donde d es el vector unitario que representa el desplazamiento en nuestro modelo. Por ejemplo, para transponer C mayor ($[1, 1, 1]$) por un tono completo (equivalente a dos semitonos, es decir, $k = 2$), se tiene:

$$T_2([1, 1, 1]) = [1, 1, 1] + 2 \cdot d.$$

Esto implica que cada nota del acorde se eleva en dos semitonos, transformando C mayor en D mayor (compuesto por las notas D, F# y A). Para visualizar este desplazamiento, se muestra el siguiente gráfico:

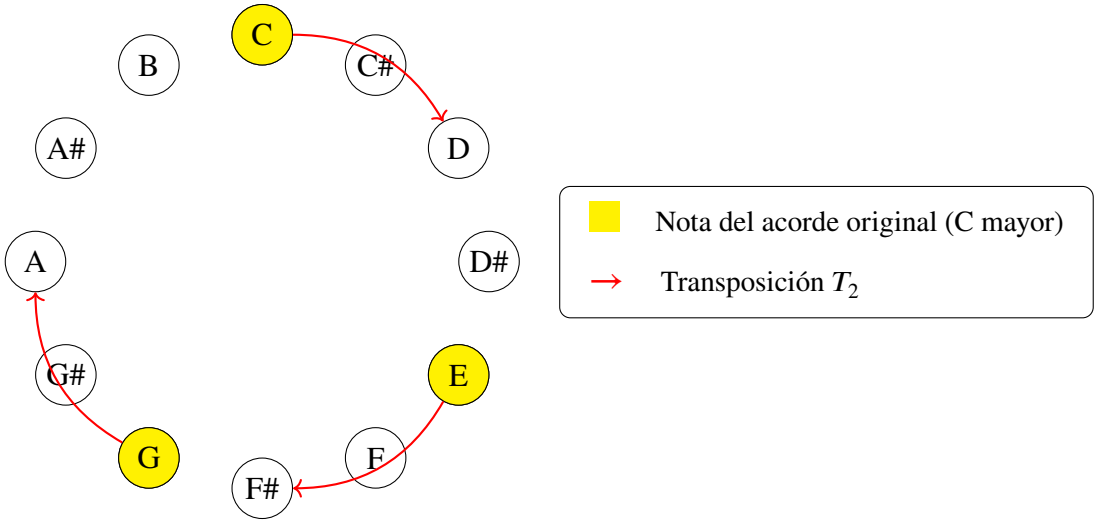
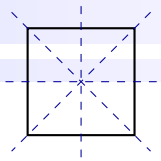


Figura 3.2: Transposición T_2 aplicada a C mayor en el círculo cromático.
Fuente: Elaboración propia

Además, esta operación satisface las propiedades de un grupo:

[5]Esta representación es una abstracción; en contextos más avanzados se emplean codificaciones que consideren la totalidad de las 12 notas del sistema cromático, identificando los acordes con subconjuntos de $\mathbb{Z}_{12}$.



- **Cierre:** La composición de dos transposiciones es otra transposición, es decir, $T_{k_1} \circ T_{k_2} = T_{k_1+k_2}$.
- **Elemento Neutro:** Existe la transposición neutra T_0, que deja inalterado el acorde.
- **Inversos:** Para cada transposición T_k existe un inverso T_{-k}, de modo que $T_k \circ T_{-k} = T_0$.

Este conjunto de transposiciones se identifica con el grupo cíclico $\mathbb{Z}_{12}$[6], lo cual refleja la naturaleza cíclica de la escala musical occidental.

- **Paso 4: Identificación de Patrones:** Al analizar cómo se transforman los acordes mediante la transposición, se pueden identificar patrones y relaciones estructurales. Por ejemplo, se observa que la "forma" interna del acorde se conserva, aunque sus notas se trasladen en el espectro sonoro.
- **Paso 5: Creación de Variaciones:** Con este entendimiento, el compositor puede generar variaciones coherentes en la progresión armónica, explorando otras operaciones del grupo que mantengan la integridad estructural de los acordes.

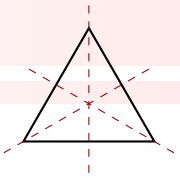
Este enfoque conecta de forma efectiva conceptos matemáticos con la práctica musical. En la práctica, se recurre al grupo cíclico $\mathbb{Z}_{12}$ para modelar las transposiciones que abarcan la totalidad de las notas de la escala cromática, ofreciendo así una representación precisa de las transformaciones musicales.

En este contexto, cada transposición se representa mediante la función T_k, definida formalmente por:

$$T_k \circ T_j = T_{(k+j) \text{ mód } 12},$$

lo que refleja la naturaleza cíclica y estructurada de las operaciones musicales. A continuación, se ilustra la tabla de composición del grupo $\mathbb{Z}_{12}$ en el modelo de transposición T_k:

[6] El grupo cíclico $\mathbb{Z}_{12}$ modela las transposiciones en la música, considerando que hay 12 semitonos en una octava.



$T_k \backslash T_j$	T_0	T_1	T_2	T_3	T_4	T_5	T_6	T_7	T_8	T_9	T_{10}	T_{11}
T_0	T_0	T_1	T_2	T_3	T_4	T_5	T_6	T_7	T_8	T_9	T_{10}	T_{11}
T_1	T_1	T_2	T_3	T_4	T_5	T_6	T_7	T_8	T_9	T_{10}	T_{11}	T_0
T_2	T_2	T_3	T_4	T_5	T_6	T_7	T_8	T_9	T_{10}	T_{11}	T_0	T_1
T_3	T_3	T_4	T_5	T_6	T_7	T_8	T_9	T_{10}	T_{11}	T_0	T_1	T_2
T_4	T_4	T_5	T_6	T_7	T_8	T_9	T_{10}	T_{11}	T_0	T_1	T_2	T_3
T_5	T_5	T_6	T_7	T_8	T_9	T_{10}	T_{11}	T_0	T_1	T_2	T_3	T_4
T_6	T_6	T_7	T_8	T_9	T_{10}	T_{11}	T_0	T_1	T_2	T_3	T_4	T_5
T_7	T_7	T_8	T_9	T_{10}	T_{11}	T_0	T_1	T_2	T_3	T_4	T_5	T_6
T_8	T_8	T_9	T_{10}	T_{11}	T_0	T_1	T_2	T_3	T_4	T_5	T_6	T_7
T_9	T_9	T_{10}	T_{11}	T_0	T_1	T_2	T_3	T_4	T_5	T_6	T_7	T_8
T_{10}	T_{10}	T_{11}	T_0	T_1	T_2	T_3	T_4	T_5	T_6	T_7	T_8	T_9
T_{11}	T_{11}	T_0	T_1	T_2	T_3	T_4	T_5	T_6	T_7	T_8	T_9	T_{10}

Cuadro 3.1: Tabla de composición del grupo $\mathbb{Z}_{12}$ en el modelo de transposición T_k

Fuente: Elaboración propia

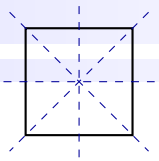
En particular:

- La fila y la columna etiquetadas con T_0 representan la transposición neutra, ya que $T_0 \circ T_j = T_j$ y $T_k \circ T_0 = T_k$.
- Cada entrada $T_{(i+j) \text{ mód } 12}$ se obtiene sumando los índices de la transposición correspondiente a la fila y a la columna, y luego reduciendo módulo 12. Por ejemplo, en la intersección de la fila T_4 y la columna T_9 se obtiene:

$$T_4 \circ T_9 = T_{(4+9) \text{ mód } 12} = T_{13 \text{ mód } 12} = T_1.$$

- Esta tabla refleja la estructura cíclica del grupo $\mathbb{Z}_{12}$, fundamental para modelar las transposiciones en la música occidental, donde existen 12 semitonos por octava.

Esta presentación permite visualizar de forma clara la composición de transposiciones y resalta la simetría y las propiedades grupales inherentes al sistema.



3.2 Teoría de Grafos

La teoría de grafos es una rama de las matemáticas que estudia las relaciones entre objetos a través de estructuras denominadas *grafos*[7]. Esta disciplina ofrece herramientas para analizar la conectividad y propiedades estructurales de las redes, y se utiliza para resolver problemas como la búsqueda de caminos más cortos, la detección de ciclos y el análisis de la estructura global de la red. A continuación se presentan algunas definiciones fundamentales:

- **Nodo (Vértice):** Una entidad u objeto representado en el grafo[8].
- **Arista:** La conexión entre dos nodos[9].
- **Grafo Dirigido:** Un grafo en el que cada arista tiene una dirección específica, indicando un flujo de un nodo a otro.
- **Grafo No Dirigido:** Un grafo en el que las aristas no tienen dirección y simplemente conectan pares de nodos.
- **Grafo Ponderado:** Un grafo en el que a cada arista se le asigna un valor numérico (peso), que puede representar, por ejemplo, la distancia o el tiempo de viaje entre dos nodos.

Entre los problemas clásicos de la teoría de grafos se encuentran la búsqueda de caminos más cortos, la detección de ciclos, el análisis de la conectividad y el estudio de las propiedades estructurales de las redes.

Ejemplo 3.2.1.

Imagine un grafo ponderado que representa una red de ciudades conectadas por carreteras. Cada ciudad se modela como un nodo, y cada carretera se representa mediante una arista ponderada (por ejemplo, según la distancia o el tiempo de viaje).

- **Paso 1: Representación del Grafo.**
  Cada ciudad se modela como un nodo y las carreteras se representan mediante aristas entre estos nodos. El siguiente gráfico ilustra un ejemplo sencillo:

[7] Un *grafo* es una colección de nodos (o vértices) y aristas que conectan pares de nodos.
[8] Un *nodo* es un punto que representa, por ejemplo, una ciudad, una persona o un dato en un conjunto.
[9] Una *arista* es una línea que une dos nodos. Puede ser *dirigida* (con una dirección definida) o *no dirigida* (sin dirección), y a menudo se le asigna un *peso* que cuantifica una medida asociada, como la distancia entre dos ciudades.

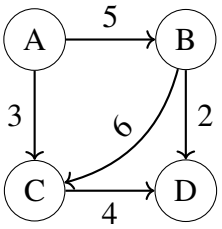


Figura 3.3: Ejemplo de grafo ponderado que representa una red entre las ciudades A, B, C y D en términos de su distancia en kilómetros

Fuente: Elaboración propia

- **Paso 2: Grupo de Automorfismos.**
  La teoría de grupos se relaciona con la teoría de grafos mediante el estudio de los *automorfismos*[10]. El conjunto de todos los automorfismos de un grafo, bajo la operación de composición, forma el *grupo de automorfismos* del grafo.

  Considere el caso de la figura 3.3, en que el grafo tiene la forma de un cuadrado, lo que implica una alta simetría. En este escenario, el grupo de automorfismos es isomorfo al grupo diedral D_4 (de orden 8). La siguiente tabla resume los elementos del grupo, indicando su notación, una breve descripción de la operación y el inverso de cada elemento:

Elemento	Notación	Descripción	Inverso
e	$(A)(B)(C)(D)$	Identidad: no altera los nodos.	e
r	$(A\,B\,C\,D)$	Rotación 90° en sentido horario.	r^3
r^2	$(A\,C)(B\,D)$	Rotación 180°.	r^2
r^3	$(A\,D\,C\,B)$	Rotación 270° en sentido horario.	r
s	$(A\,B)(C\,D)$	Reflexión sobre el eje vertical.	s
t	$(A\,D)(B\,C)$	Reflexión sobre el eje horizontal.	t
u	$(B\,D)$	Reflexión sobre la diagonal que fija A y C.	u
v	$(A\,C)$	Reflexión sobre la diagonal que fija B y D.	v

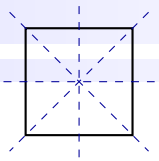
Cuadro 3.2: Propiedades del grupo de automorfismos del grafo simétrico (isomorfo a D_4).

Fuente: Elaboración propia

En este contexto, la permutación

$$r = (A\,B\,C\,D)$$

[10]Un *automorfismo* de un grafo es una biyección de los nodos que preserva la conectividad, es decir, las aristas se mantienen entre los nodos correspondientes.



corresponde a rotar el cuadrado 90° en sentido horario, mientras que la reflexión

$$s = (A\ B)(C\ D)$$

intercambia las ciudades de la parte superior con las de la inferior, manteniendo la conectividad del grafo. La operación en este grupo es la composición de permutaciones, la cual es asociativa; el elemento neutro es e y cada automorfismo posee un inverso, como se muestra en la tabla.

- **Paso 3: Propiedades de Simetría y Aplicaciones.**
  El análisis del grupo de automorfismos permite identificar simetrías en la red. Esto implica que ciertas ciudades pueden intercambiarse sin afectar la conectividad o las distancias en el sistema, lo que resulta útil para simplificar problemas de optimización, como la búsqueda de rutas más cortas o la planificación eficiente.

- **Paso 4: Relación con la Optimización de Rutas.**
  Al reconocer conjuntos de nodos equivalentes a través de los automorfismos, es posible reducir la complejidad de problemas de optimización. Por ejemplo, si dos ciudades son equivalentes desde el punto de vista estructural, pueden tratarse de manera similar en algoritmos que buscan minimizar el costo de una ruta.

  A continuación, se presenta un gráfico que ilustra un ejemplo de grafo simétrico y una posible permutación automórfica:

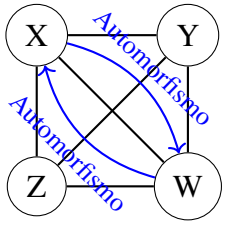
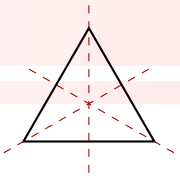


Figura 3.4: Grafo simétrico y un ejemplo de permutación automórfica.
Fuente: Elaboración propia

Esta integración de conceptos de teoría de grafos y teoría de grupos proporciona herramientas analíticas poderosas para comprender la estructura y simetría de las redes. El estudio de los automorfismos es fundamental tanto en el análisis teórico de grafos como en aplicaciones prácticas, tales como la optimización de rutas y el diseño de redes eficientes.



3.3 Simetría en Física

La simetría es una propiedad fundamental en la Física, ya que muchas leyes y ecuaciones físicas se mantienen invariantes bajo ciertas transformaciones. La teoría de grupos proporciona el marco matemático para clasificar y estudiar estas transformaciones, conocidas como *operadores de simetría*.
En Física, se consideran, por ejemplo:

1. **Grupos de Simetría:** Estos grupos están formados por todas las transformaciones que dejan inalterado un sistema físico. Dichas transformaciones pueden ser rotaciones, reflexiones, traslaciones, etc. Cada elemento del grupo puede representarse mediante una matriz que describe su acción sobre estados físicos (por ejemplo, funciones de onda).

2. **Invariancia de las Ecuaciones Físicas:** Muchas ecuaciones fundamentales (por ejemplo, las de la mecánica cuántica) son invariantes bajo operaciones del grupo de simetría asociado. Esto implica que, al aplicar una transformación, la forma de la ecuación permanece igual, lo que nos brinda información sobre las propiedades del sistema.

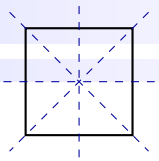
3. **Aplicaciones Prácticas:** La simetría se utiliza, por ejemplo, para derivar reglas de selección en espectroscopia (determinando qué transiciones son permitidas o prohibidas) y para clasificar la estructura de cristales. En Física de partículas, aunque se utilizan conceptos más avanzados como los grupos de Lie, la idea básica es la misma: la simetría guía la formulación de teorías fundamentales.

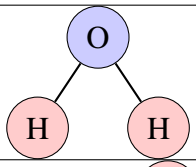
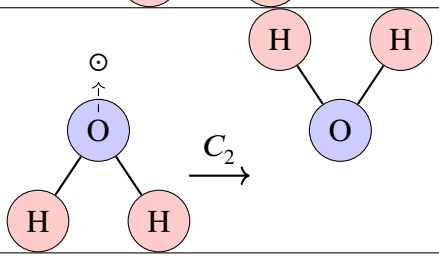
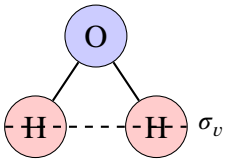
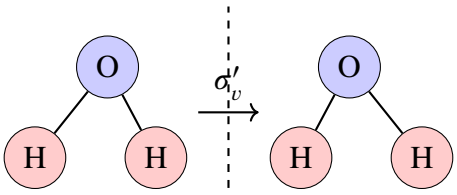
Ejemplo 3.3.1.

Para ilustrar estos conceptos, consideremos el ejemplo de la molécula de agua, que pertenece al grupo puntual C_{2v}. Este grupo tiene cuatro operaciones de simetría:

- E: La identidad (no realiza ninguna transformación).
- C_2: Rotación de 180° alrededor de un eje perpendicular al plano de la molécula.
- σ_v: Reflexión en el plano de la molécula.
- σ_v': Reflexión en un plano perpendicular a la molécula.

A continuación, se muestra una tabla que resume estas operaciones junto con ejemplos visuales que ilustran el efecto de cada transformación sobre una representación simplificada de la molécula de agua.



Operación y Descripción	Ejemplo Visual
E **(Identidad)**: No se realiza ninguna transformación.	
C_2 **(Rotación 180°)**: Rotación de 180° sobre un eje perpendicular al plano de la molécula.	
σ_v **(Reflexión en el plano de la molécula)**: Refleja la molécula a lo largo del plano donde se encuentran los átomos. En una representación bidimensional, la imagen permanece igual (ya que la molécula se encuentra en ese plano).	
σ'_v **(Reflexión en un plano perpendicular)**: Refleja la molécula a través de un plano perpendicular al plano molecular. En este ejemplo, el plano de reflexión es vertical (línea discontinua), lo que intercambia la posición de los átomos de hidrógeno.	

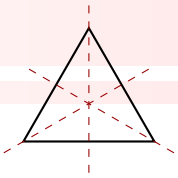
Cuadro 3.3: Operaciones de simetría en la molécula de agua (Grupo C_{2v})

Fuente: Elaboración propia

En tal caso, el grupo C_{2v} es isomorfo al grupo de Klein, por lo que todas sus operaciones cumplen la propiedad conmutativa y cada elemento es de orden 2 (es decir, su composición consigo mismo da la identidad). La tabla de composición se puede definir de la siguiente forma:

$\circ$	E	C_2	σ_v	σ'_v
E	E	C_2	σ_v	σ'_v
C_2	C_2	E	σ'_v	σ_v
σ_v	σ_v	σ'_v	E	C_2
σ'_v	σ'_v	σ_v	C_2	E

Cuadro 3.4: Tabla de composición del grupo C_{2v} (simetría de la molécula de agua).



Esta tabla permite al lector visualizar de forma clara cómo se combinan las operaciones de simetría en el grupo C_{2v}. Cada celda de la tabla representa el resultado de la composición (denotada por $\circ$) de la transformación que figura en la fila con la de la columna correspondiente. La figura 3.5 permite visualizar cómo se combinan una rotación y una reflexión en la molécula de agua, facilitando la comprensión de la composición de operadores de simetría en el contexto de la teoría de grupos aplicada a la Física.

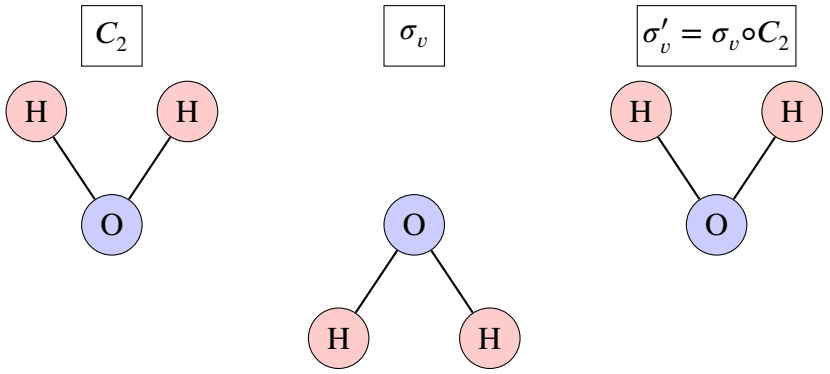
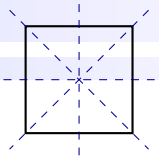


Figura 3.5: Ejemplo de combinación de transformaciones en la molécula de agua: la primera imagen muestra la rotación C_2 (180°), la segunda la reflexión σ_v (en el eje vertical) aplicada a la configuración original, y la tercera el resultado de la composición, σ'_v.

Fuente: Elaboración propia



3.4 Computación

En el diseño de algoritmos de ordenamiento se pueden aplicar conceptos de permutaciones, las cuales forman un grupo. Un ejemplo clásico es el algoritmo de ordenamiento por burbuja[11], que puede interpretarse como una serie de intercambios (transposiciones) entre elementos adyacentes en una lista. Cada intercambio se representa como una permutación en el conjunto de índices, y el conjunto de todas estas permutaciones forma el grupo simétrico S_n, cuya identidad es la permutación que no altera el orden de los elementos.

Para ilustrar este enfoque, se describen a continuación los pasos básicos del algoritmo de burbuja aplicado a una lista de números:

1. **Representación de Permutaciones:** Cada operación de intercambio de dos elementos adyacentes se representa mediante una *transposición*. Por ejemplo, intercambiar los elementos en las posiciones 1 y 2 se denota como (1 2).

2. **Grupo de Permutaciones:** El conjunto de todas las permutaciones posibles de los índices forma el grupo simétrico S_n. En este grupo, la operación es la composición de permutaciones (que es asociativa) y cada transposición es su propio inverso.

3. **Aplicación del Algoritmo:** El algoritmo de burbuja recorre la lista comparando elementos adyacentes y, si están en el orden incorrecto, los intercambia. Cada intercambio corresponde a la aplicación de una transposición en S_n.

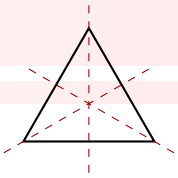
4. **Complejidad:** La cantidad total de intercambios (transposiciones) realizados depende del número de *inversiones* presentes en la lista, lo cual influye directamente en la complejidad temporal del algoritmo.

Ejemplo 3.4.1.

Suponga que se desea ordenar la lista $[5, 2, 8, 3]$ en orden ascendente. El algoritmo de burbuja procede de la siguiente forma:

- **Iteración 1:**
  - Comparar 5 y 2: Como $5 > 2$, se intercambian. La lista se actualiza a $[2, 5, 8, 3]$. (Intercambio: (1 2))

[11] El ordenamiento de burbuja es un método intuitivo de reubicar elementos en una lista mediante intercambios sucesivos de pares adyacentes. Aunque no es el más eficiente, es ampliamente usado en cursos introductorios de programación para ilustrar conceptos básicos.

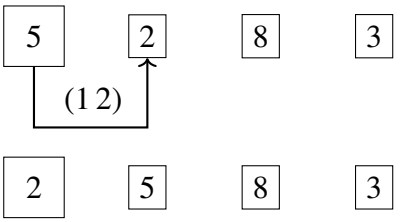


- Comparar 5 y 8: $5 < 8 \rightarrow$ no se realiza intercambio.
- Comparar 8 y 3: Como $8 > 3$, se intercambian. La lista se actualiza a $[2, 5, 3, 8]$. (Intercambio: $(3\,4)$)

- **Iteración 2:**
  - Comparar 2 y 5: $2 < 5 \rightarrow$ no se realiza intercambio.
  - Comparar 5 y 3: Como $5 > 3$, se intercambian. La lista se actualiza a $[2, 3, 5, 8]$. (Intercambio: $(2\,3)$)
- **Iteración 3:** No se realizan intercambios, ya que la lista se encuentra ordenada.

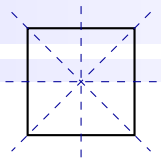
En este ejemplo, los intercambios realizados fueron: $(1\,2)$, $(3\,4)$ y $(2\,3)$. Cada uno de estos intercambios es una transposición en S_4 (el grupo de permutaciones de 4 elementos).

Para visualizar uno de estos intercambios, considere el intercambio $(1\,2)$ en la lista $[5, 2, 8, 3]$. La Figura 3.6 muestra la configuración original y la lista resultante después de aplicar la transposición.



Intercambio $(1\,2)$

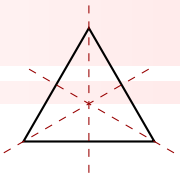
Figura 3.6: Visualización del intercambio $(1\,2)$ en la lista $[5, 2, 8, 3]$.
Fuente: Elaboración propia



El siguiente fragmento de código en Python implementa el algoritmo de burbuja y permite verificar el proceso de ordenamiento:

```
1  def bubble_sort(lst):
2      n = len(lst)
3      # Bucle principal para cada iteracion
4      for i in range(n):
5          # Bucle interno para comparar elementos adyacentes
6          for j in range(0, n - i - 1):
7              if lst[j] > lst[j + 1]:
8                  # Intercambiar elementos (transposicion)
9                  lst[j], lst[j + 1] = lst[j + 1], lst[j]
10     return lst
11
12 # Ejemplo de uso:
13 lista = [5, 2, 8, 3]
14 print("Lista ordenada:", bubble_sort(lista))
```

El algoritmo de burbuja, aunque no es el más eficiente para grandes volúmenes de datos, ilustra de manera sencilla cómo se aplican conceptos de permutaciones y grupos en el diseño de algoritmos. Cada intercambio es una transposición, y el conjunto de todas estas transposiciones forma parte del grupo simétrico S_n. Este enfoque muestra cómo la teoría de grupos proporciona una perspectiva matemática para analizar y entender procesos algorítmicos.



3.5 Criptografía y Teoría de Grupos: Un Vínculo Profundo

Agradecimiento especial en esta sección a los estudiantes Miguel Castillo, Jose Manuel Sandoval y Andy Torres del Instituto Tecnológico de Costa Rica por el aporte de las ideas.

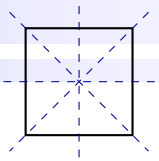
La criptografía, en términos generales, es el estudio y la práctica de técnicas seguras para comunicar información de manera confidencial y protegerla contra manipulaciones no autorizadas. Esta disciplina se basa en la aplicación de algoritmos matemáticos y protocolos específicos con el objetivo de garantizar la privacidad, autenticidad e integridad de la información en entornos donde la seguridad es fundamental.

En su esencia, la criptografía aborda la problemática de la seguridad de la información mediante el desarrollo y la aplicación de métodos que permiten a las partes autorizadas entender el contenido de un mensaje mientras lo mantiene oculto a terceros no autorizados. Se distinguen dos categorías principales de criptografía: la criptografía simétrica, donde se utiliza una clave compartida para cifrar y descifrar información, y la criptografía asimétrica, que emplea un par de claves (pública y privada) para este propósito.

La criptografía desempeña un papel crucial en la seguridad de las comunicaciones electrónicas, las transacciones financieras en línea y la protección de datos sensibles. Su evolución continua se debe a la constante búsqueda de métodos más robustos frente a los avances tecnológicos y las amenazas emergentes en el ámbito digital.

3.5.1. Historia

Según la historia de la criptografía, y como lo relata Communications (2024), en la antigua Esparta del siglo V a.C. se datan los primeros usos de dicha técnica para cifrar mensajes, conocida como la **escítala espartana**. Este método de encriptación de información surgió debido a las continuas guerras, como las guerras médicas y del Peloponeso.



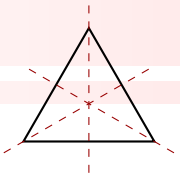
La escítala consistía en una vara alrededor de la cual se enrollaba una cinta de tela con el mensaje. A simple vista, el mensaje parecía indescifrable. Solo aquellas personas que contaran con una vara del mismo tamaño y grosor podían leer el mensaje, al volver a enrollar la cinta sobre esta vara idéntica.

Figura 3.7: Escítala espartana utilizada para cifrar mensajes en la antigua Grecia.
Fuente: Luringen. (2007). Skytale [Fotografía]. Wikimedia Commons.
https://commons.wikimedia.org/wiki/File:Skytale.png

De esta manera, cuando los espartanos necesitaban enviar un mensaje, lo escribían en una cinta enrollada alrededor de una vara designada. Una vez listo el mensaje, enviaban a un mensajero que llevaba la cinta y la guardaba o la usaba como accesorio, ya sea en la cintura o en la muñeca. Al llegar al destinatario, este simplemente desenrollaba la cinta y la enrollaba en una vara idéntica para poder leer el mensaje. De este modo, si el mensajero era capturado por el enemigo, aunque se obtuviera la cinta, el mensaje permanecía ilegible, ya que solo podía descifrarse con una vara del mismo grosor que la original.

Otro de los primeros sistemas de cifrado fue utilizado por el gobernante Julio César, en el siglo I a.C. Según *Hornetsecurity* (2024), el **cifrado de César** se basaba en un método simple de sustitución, en el cual cada letra del mensaje era reemplazada por otra, determinada mediante un desplazamiento fijo en el alfabeto. Por ejemplo, si se establecía un desplazamiento de cuatro lugares a la derecha, para cifrar la palabra “GRACIAS” se obtenía “CÑWYEWO”. Este método impedía que personas no autorizadas descifraran el mensaje sin conocer la clave del desplazamiento; sin embargo, un atacante con conocimientos del sistema solo necesitaba realizar 25 intentos para descubrir la clave.

El cifrado de César también puede representarse mediante álgebra modular, transformando primero las



letras en números (por ejemplo, $A = 0$, $B = 1$, $C = 2$, …, $Z = 26$). De este modo, el cifrado de una letra x con un desplazamiento fijo $n \in \{0, 1, \dots, 25\}$, se expresa matemáticamente como:

$$E_n(x) = (x + n) \pmod{26},$$

mientras que el proceso de desencriptación se define como:

$$D_n(x) = (x - n) \pmod{26}.$$

Por ejemplo, si $A = 0$, se tiene

$$E_0(0) = (0 + 0) \equiv 0 \pmod{26}$$

$$E_1(0) = (0 + 1) \equiv 1 \pmod{26}$$

$$E_2(0) = (0 + 2) \equiv 2 \pmod{26}$$

$$E_3(0) = (0 + 3) \equiv 3 \pmod{26}$$

significa que cada letra A avanza 0, 1, 2 y 3 posiciones en el alfabeto, lo cual equivale a una codificación de A por A,B,C o D en función de $n = 0, 1, 2, 3$ respectivamente. Por otro lado, y considerando que $A = 0$, se tiene

$$D_0(0) = (0 - 0) \equiv 0 \pmod{26}$$

$$D_1(0) = (0 - 1) \equiv (26 - 1) \equiv 25 \pmod{26}$$

$$D_2(0) = (0 - 2) \equiv (26 - 2) \equiv 24 \pmod{26}$$

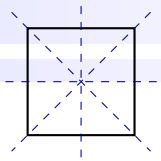
$$D_3(0) = (0 - 3) \equiv (26 - 3) \equiv 23 \pmod{26}$$

significa que cada letra A retrocede 0, 1, 2 y 3 lugares en el alfabeto, lo cual equivale a una codificación de A por A,Z,Y o X en función de $n = 0, 1, 2, 3$ respectivamente.

Ejemplo 3.5.1.

En un sistema de cifrado César, cada letra del alfabeto se desplaza un número fijo de $n = 3$ posiciones hacia adelante, considerando que el alfabeto es cíclico. Si el desplazamiento es de 3 posiciones y el mensaje original es `CRIPTOGRAFÍA`, determine el mensaje cifrado. Se utiliza únicamente letras mayúsculas y se considera un alfabeto de 27 caracteres, incluyendo la letra Ñ[12].

[12]Este ejemplo es una adaptación para incluir la letra ñ, distinguiéndolo del estándar histórico (26 letras latinas).



Solución:

Primero, se asigna un número a cada letra del alfabeto español:

$$A = 0, \quad B = 1, \quad C = 2, \quad \ldots, \quad Z = 26.$$

Para el mensaje CRIPTOGRAFÍA, se asocia cada letra a su correspondiente número:

C	R	I	P	T	O	G	R	A	F	Í	A
2	17	8	15	19	14	6	17	0	5	8	0

El mensaje original se representa como la secuencia numérica:

$$2,\ 17,\ 8,\ 15,\ 19,\ 14,\ 6,\ 17,\ 0,\ 5,\ 8,\ 0.$$

Aplicando el desplazamiento de 3 posiciones hacia adelante (utilizando la operación módulo 27 para mantener la circularidad del alfabeto):

Letra Original	Operación cripotográfica	Letra Codificada
C	$(2+3) \equiv 5 \pmod{26}$	F
R	$(17+3) \equiv 20 \pmod{26}$	U
I	$(8+3) \equiv 11 \pmod{26}$	L
P	$(15+3) \equiv 18 \pmod{26}$	S
T	$(19+3) \equiv 22 \pmod{26}$	W
O	$(14+3) \equiv 17 \pmod{26}$	R
G	$(6+3) \equiv 9 \pmod{26}$	J
R	$(17+3) \equiv 20 \pmod{26}$	U
A	$(0+3) \equiv 3 \pmod{26}$	D
F	$(5+3) \equiv 8 \pmod{26}$	I,
Í	$(8+3) \equiv 11 \pmod{26}$	L
A	$(0+3) \equiv 3 \pmod{26}$	D

Reemplazando los números por las letras correspondientes, el mensaje cifrado es:

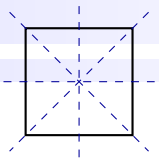
FULSWRJUDILD.

Según Academy (2023), conforme avanzaron la ciencia y la curiosidad del ser humano, las civilizaciones sintieron la necesidad de desarrollar métodos para resolver códigos y cifrados. Así nació el criptoanálisis, que llegó a compararse con una ciencia primitiva, al igual que la criptografía. En este contexto, Al-Kindi, un matemático árabe, creó en el año 800 d.C. el análisis de frecuencia, una técnica que dejó vulnerables a los cifrados por sustitución, como el cifrado de César. Esto obligó a la criptografía a evolucionar para mantener su utilidad.

Figura 3.8: Disco de cifrado de Alberti utilizado para la codificación polialfabética
Fuente: Buonafalce, A. (2008). Alberti cipher disk [Fotografía]. Wikimedia Commons https://es.wikipedia.org/wiki/Cifrado_de_Alberti#/media/Archivo:Alberti_cipher_disk.JPG

En el año 1465, Leone Alberti desarrolló uno de los primeros cifrados polialfabéticos para combatir el análisis de frecuencia. Este cifrado empleaba dos alfabetos distintos: uno para escribir el mensaje original y otro diferente para mostrar el texto codificado. Con este nuevo método, la seguridad del cifrado mejoró considerablemente en comparación con los métodos de sustitución tradicionales.

Más adelante, en el siglo XVI, el diplomático y criptógrafo francés Blaise de Vigenère perfeccionó el cifrado polialfabético. Su método consistía en elegir una palabra clave, cuya primera letra determinaba el alfabeto utilizado para cifrar la primera letra del mensaje, y así sucesivamente. Si el texto era más largo que la clave, esta se reutilizaba tantas veces como fuera necesario para cubrir todo el mensaje (Hornetsecurity, 2024).



Para decodificar el cifrado Vigenère, se utilizaba una tabla específica, como la mostrada en la figura 3.9.

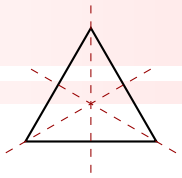
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figura 3.9: Clave del cifrado de Vigenère

Fuente: Adaptado de Larragan (2015)

La tabla de Vigenère, representada en la figura, es un entramado geométrico que materializa la esencia del cifrado polialfabético. Cada celda de esta matriz no es más que la cristalización de un principio algebraico: el grupo cíclico $(\mathbb{Z}_{25}, +)$, donde las letras del alfabeto, de la A a la Z, se traducen en números del 0 al 25.

La primera fila, coronada por la letra A, actúa como un espejo que refleja el alfabeto intacto, pues corresponde al desplazamiento nulo, el elemento identidad de este sistema. A partir de allí, cada fila sucesiva



gira el alfabeto como un engranaje perfecto: la fila B avanza una posición (B ocupa el lugar de C, C el lugar de D, y así hasta sucesivamente hasta Z, que retrocede a la posición de A), la fila C gira dos posiciones, y este patrón se repite hasta la fila Z, que desplaza el alfabeto completo en 25 pasos, cerrando el ciclo.

Esta estructura no es arbitraria. Cada letra del texto plano, al intersectarse con una clave específica (una fila de la tabla), se transforma en un símbolo cifrado mediante una suma modular. Por ejemplo, si la letra E (valor 4) se cifra con la clave B (valor 1), el resultado será F (valor 5), operación que en $\mathbb{Z}_{25}$ se escribe como $4 + 1 \equiv 5$. Para descifrar, basta con restar el valor de la clave en este mismo universo modular, donde cada elemento tiene un inverso aditivo que garantiza la reversibilidad del proceso.

Lo fascinante yace en su simetría matemática: la tabla es un catálogo completo de todas las posibles traslaciones en $\mathbb{Z}_{25}$, un sistema cerrado donde ninguna operación escapa de los límites del alfabeto. Esta elegancia no solo permitió a criptógrafos del Renacimiento proteger mensajes con claves repetidas, sino que también revela, siglos después, cómo la criptografía clásica se sustenta en pilares abstractos del álgebra moderna. Cada fila es una manifestación de un grupo cíclico, cada columna un recordatorio de que incluso en el arte secreto de los códigos, subyace el orden inmutable de las matemáticas.

Ejemplo 3.5.2.

Para ilustrar el procedimiento de descifrado por medio de la tabla de Vigenère, se considera el siguiente mensaje cifrado:

`kevsyjms`

y la palabra clave:

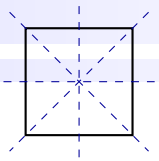
`casa`

En primer lugar, se distribuye la clave bajo cada letra del texto cifrado. Dado que la palabra `casa` consta de cuatro letras, se repite tantas veces como sea necesario para cubrir todas las posiciones:

Texto cifrado:	k	e	v	s	y	j	m	s
Clave:	c	a	s	a	c	a	s	a

A continuación, se recurre a la tabla de Vigenère para descifrar cada carácter de la siguiente manera:

1. Se localiza la **fila** correspondiente a la letra cifrada (por ejemplo, “k”).
2. Se identifica la **columna** asociada a la letra de la clave (en este caso, “c”).



3. En la **intersección** de esa fila y columna, se obtiene la letra descifrada.

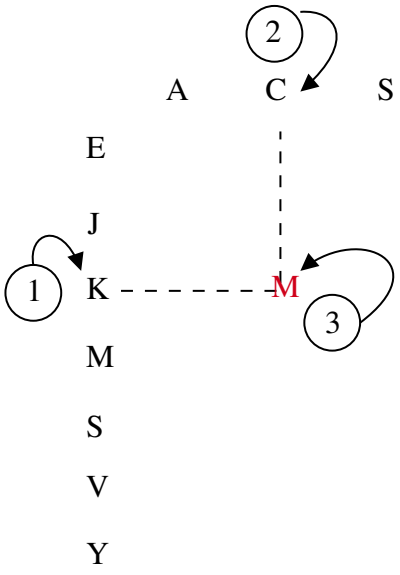


Figura 3.10: Descripción visual de los pasos en el descifrado de Vigenère
Fuente: Elaboración propia

Este procedimiento se repite para todas las letras, avanzando de manera simultánea sobre el texto cifrado y la clave. Al concluir, se obtiene:

Texto cifrado:	k	e	v	s	y	j	m	s
Clave:	c	a	s	a	c	a	s	a
Texto plano:	m	e	n	s	a	j	e	s

De esta manera, se recupera la palabra original que es `mensajes`. Un ejemplo por pasos y con decodificación inversa se presenta a continuación.

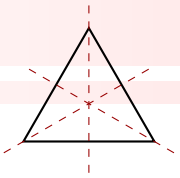
Ejemplo 3.5.3.

Utilizando el cifrado de Vigenère, se requiere cifrar y descifrar el siguiente mensaje con la clave "CRIPTO":

- **Mensaje original:** "CRIPTOGRAFIA ES SEGURA".
- **Clave:** "CRIPTO".

Se plantea:

1. ¿Cuál es el mensaje cifrado?
2. ¿Cómo se puede descifrar el mensaje utilizando la clave?



Solución

El cifrado de Vigenère utiliza una clave repetitiva para transformar el mensaje. El proceso de cifrado se rige por la siguiente fórmula:

$$C_i \equiv (M_i + K_i) (\text{mod } 26),$$

donde:

- M_i es el valor numérico de la i-ésima letra del mensaje.
- K_i es el valor numérico de la i-ésima letra de la clave (repetida según sea necesario).
- C_i es el valor numérico de la letra cifrada.

Paso 1: Asignación de valores numéricos Se asigna un valor a cada letra del alfabeto:

$$A = 0, \quad B = 1, \quad C = 2, \quad \ldots, \quad Z = 25.$$

El mensaje original:

`CRIPTOGRAFIA ES SEGURA`

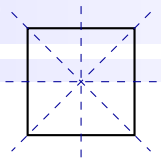
se convierte en la siguiente secuencia numérica:

C	R	I	P	T	O	G	R	A	F	I	A	E	S	S	E	G	U	R	A
2	17	8	15	19	14	6	17	0	5	8	0	4	18	18	4	6	20	17	0

La clave “CRIPTO” se repite para cubrir todo el mensaje. La representación numérica de la clave es:

C	R	I	P	T	O
2	17	8	15	19	14

y se repite según sea necesario: `CRIPTO CRIPTO CRIPTO`, etc.



Paso 2: Cifrado del mensaje Se cifra cada letra sumando el valor correspondiente de la clave y aplicando el módulo 25. Se detalla a continuación:

Letra Original con su letra clave	Operación cripotográfica	Letra Codificada
C_1 (C)	$(2+2) \equiv 4 \pmod{25}$	E
C_2 (R)	$(171+17) \equiv 8 \pmod{25}$	I
C_3 (I)	$(8+8) \equiv 16 \pmod{25}$	Q
C_4 (P)	$(15+15) \equiv 4 \pmod{25}$	E
C_5 (T)	$(19+19) \equiv 12 \pmod{25}$	M
C_6 (O)	$(14+14) \equiv 2 \pmod{25}$	C
C_7 (C)	$(6+2) \equiv 8 \pmod{25}$	I
C_8 (R)	$(17+17) \equiv 8 \pmod{25}$	I
C_9 (I)	$(0+8) \equiv 8 \pmod{25}$	I
C_{10} (P)	$(5+15) \equiv 20 \pmod{25}$	U
C_{11} (T)	$(8+19) \equiv 1 \pmod{25}$	B
C_{12} (O)	$(0+14) \equiv 14 \pmod{25}$	O
C_{13} (C)	$(4+2) \equiv 6 \pmod{25}$	G
C_{14} (R)	$(18+17) \equiv 9 \pmod{25}$	J
C_{15} (I)	$(18+8) \equiv 0 \pmod{25}$	A
C_{16} (P)	$(4+15) \equiv 19 \pmod{25}$	T
C_{17} (T)	$(6+19) \equiv 25 \pmod{25}$	Z
C_{18} (O)	$(20+14) \equiv 8 \pmod{25}$	I
C_{19} (C)	$(17+2) \equiv 19 \pmod{25}$	T
C_{20} (R)	$(0+17) \equiv 17 \pmod{25}$	R

Por lo tanto, el mensaje cifrado es:

`EIQEMCIIIUBOGJATZITR`.

Paso 3: Descifrado del mensaje El proceso de descifrado utiliza la fórmula inversa:

$$M_i \equiv (C_i - K_i) \pmod{25}$$

Aplicando esta fórmula a cada letra del mensaje cifrado, se obtiene:

Letra Codificada	Operación cripotográfica "inversa"	Letra Original
M_1 (E)	$(4-2) \equiv 2 \pmod{25}$	C
M_2 (I)	$(8-17) \equiv 17 \pmod{25}$	R
M_3 (Q)	$(16-8) \equiv 8 \pmod{25}$	I
M_4 (E)	$(4-15) \equiv 15 \pmod{25}$	P
M_5 (M)	$(12-19) \equiv 19 \pmod{25}$	T
M_6 (C)	$(2-14) \equiv 14 \pmod{25}$	O
M_7 (I)	$(8-2) \equiv 6 \pmod{25}$	G
M_8 (I)	$(8-17) \equiv 17 \pmod{25}$	R
M_9 (I)	$(8-8) \equiv 0 \pmod{25}$	A
M_{10} (U)	$(20-15) \equiv 5 \pmod{25}$	F
M_{11} (B)	$(1-19) \equiv 8 \pmod{25}$	I
M_{12} (O)	$(0-14) \equiv 14 \pmod{25}$	A
M_{13} (G)	$(6-2) \equiv 4 \pmod{25}$	E
M_{14} (J)	$(9-17) \equiv 18 \pmod{25}$	S
M_{15} (A)	$(0-8) \equiv 18 \pmod{25}$	S
M_{16} (T)	$(19-15) \equiv 4 \pmod{25}$	E
M_{17} (Z)	$(25-19) \equiv 6 \pmod{25}$	G
M_{18} (I)	$(8-14) \equiv 20 \pmod{25}$	U
M_{19} (T)	$(19-2) \equiv 17 \pmod{25}$	R
M_{20} (R)	$(17-17) \equiv 0 \pmod{25}$	A

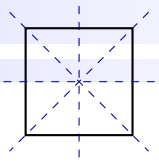
Al convertir los valores numéricos de vuelta a letras, se obtiene el mensaje descifrado:

`CRIPTOGRAFIA ES SEGURA.`

Con lo anterior, se comprueba que el proceso de cifrado y descifrado con el cifrado de Vigenère utilizando la clave "CRIPTO" es correcto.

La Criptografía en el siglo XIX y XX

Según Sidhpurwala (2023), a inicios del siglo XIX comenzaron a introducirse herramientas electrónicas, lo que permitió a Hebern diseñar la máquina de rotor. Este dispositivo empleaba un disco giratorio con una clave que codificaba una tabla de sustitución, de manera que cada pulsación de tecla generaba un resultado cifrado.



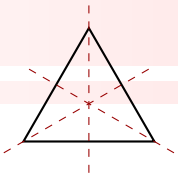
Este avance marcó el inicio de máquinas más eficientes para el cifrado, lo que llevó al ingeniero alemán Arthur Scherbius a desarrollar la máquina Enigma hacia el final de la Primera Guerra Mundial. Enigma se convirtió en una herramienta crucial durante la Segunda Guerra Mundial, ya que permitía a los alemanes comunicar sus estrategias de manera segura. Su sistema utilizaba tres o cuatro rotores que giraban a distintas velocidades según se digitaban las letras, generando un cifrado que se consideró prácticamente indestructible. La clave de cifrado dependía del ajuste inicial de los rotores y se modificaba cada 24 horas, lo que dificultaba su descifrado.

Sin embargo, en el bando contrario, el matemático e informático británico Alan Turing emprendió en 1945 la tarea de descifrar Enigma. Para ello, diseñó la máquina de Turing, considerada el primer ordenador, capaz de determinar la clave diaria de Enigma y, con ello, decodificar los mensajes alemanes. Este logro, según historiadores, fue revolucionario, ya que contribuyó a acortar la guerra y salvar millones de vidas humanas.

En 1948, el matemático e ingeniero Claude Shannon publicó su obra *A Mathematical Theory of Communication*, en la que abordó la transmisión de información a través de canales de comunicación. En este trabajo, introdujo el concepto de **entropía de la información**[13], una medida fundamental en la teoría de la información que permite cuantificar la incertidumbre o imprevisibilidad en un sistema de comunicación. Sus aportes revolucionaron el campo, proporcionando bases sólidas para la criptografía y la comprensión de los datos, razón por la cual es considerado el padre de la criptografía moderna (Pires, 2024).

Con el avance de la tecnología, surgieron nuevos métodos de encriptación y desencriptación, los cuales han evolucionado con el tiempo. Uno de los primeros enfoques fue la criptografía simétrica, que utiliza una única clave secreta tanto para cifrar como para descifrar mensajes. Sin embargo, este método presentaba un problema fundamental: la necesidad de compartir la clave entre los participantes, lo que podía comprometer la seguridad. Para solucionar esta limitación, se desarrolló la criptografía asimétrica, que emplea un par de claves: una pública, accesible para todos, y una privada, conocida solo por su propietario. Este modelo redujo significativamente los riesgos asociados a la distribución de claves (Communications, 2024).

[13]La entropía de la información, refleja la "sorpresa.º ïnformaciónçontenida en un mensaje o evento. A mayor entropía, mayor incertidumbre y más información se requiere para describir o predecir el evento. La entropía se relaciona con la probabilidad, siendo alta cuando los eventos son igualmente probables y baja cuando un evento es mucho más probable que otros. Con aplicaciones en campos como la compresión de datos, criptografía, procesamiento del lenguaje natural e inteligencia artificial, la entropía es una herramienta poderosa para cuantificar la incertidumbre y la información en un conjunto de datos, revelando que a mayor entropía, más impredecible es el sistema y más información se necesita para comprenderlo.



Dentro de la criptografía asimétrica destacan dos algoritmos ampliamente utilizados. El primero es el algoritmo RSA, cuyo nombre proviene de los apellidos de sus creadores (Rivest, Shamir y Adleman). Su seguridad se basa en la dificultad de factorizar números extremadamente grandes, lo que lo convierte en un sistema resistente a ataques. El segundo es la criptografía de curva elíptica, considerada aún más segura y eficiente, lo que la hace especialmente difícil de vulnerar por parte de los hackers cibernéticos (Communications, 2024).

En la actualidad, uno de los avances más notables en este campo es el uso de la criptografía en criptomonedas, que emplean principios criptográficos para garantizar la seguridad de las transacciones y regular la creación de nuevas unidades. Entre ellas, Bitcoin es la más reconocida. Además, la criptografía cuántica ha surgido como una nueva frontera en el área, gracias a los avances en la computación cuántica. Estos sistemas están diseñados para resistir ataques potenciales de computadoras cuánticas, aunque aún se encuentran en fase de desarrollo y representan el futuro de la criptografía.

3.5.2. Encriptación Simétrica y Asimétrica

La encriptación es un proceso fundamental en la seguridad de la información y se clasifica principalmente en dos categorías: **encriptación simétrica** y **encriptación asimétrica**. Ambos métodos se basan en principios matemáticos y utilizan funciones específicas para transformar un mensaje original en un texto cifrado.

Matemáticamente, el proceso de encriptación E se define como:

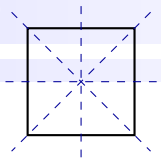
$$c = E(k, m)$$

donde c es el texto cifrado, m es el mensaje original y k es la clave utilizada en el cifrado. Para recuperar el mensaje original, se aplica la función de desencriptación D:

$$m = D(k, c)$$

La relación entre E y D debe cumplir que sean funciones inversas:

$$D(k, E(k, m)) = m$$



Encriptación Simétrica

La encriptación simétrica utiliza una única clave k compartida entre el emisor y el receptor para cifrar y descifrar la información. Uno de los algoritmos más utilizados en este tipo de encriptación es el **AES (Advanced Encryption Standard)**, el cual emplea operaciones matemáticas avanzadas, como la multiplicación en un campo finito y sustituciones de bytes. AES permite el uso de claves de 128, 192 o 256 bits, proporcionando distintos niveles de seguridad.

Sin embargo, la seguridad de este método depende de la confidencialidad de la clave. Si un atacante obtiene acceso a ella, puede descifrar toda la información protegida. Para mitigar este riesgo, es recomendable el uso de claves largas y aleatorias, así como su renovación periódica.

Encriptación Asimétrica

A diferencia de la encriptación simétrica, la **encriptación asimétrica** (o criptografía de clave pública) utiliza un par de claves:

- **Clave pública** k_p: Puede ser compartida libremente.
- **Clave privada** k_{pr}: Se mantiene en secreto y solo la conoce el propietario.

El proceso de encriptación y desencriptación se define matemáticamente como:

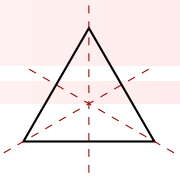
$$c = E(k_p, m)$$

$$m = D(k_{pr}, c)$$

Una propiedad clave de la encriptación asimétrica es que es **computacionalmente difícil** determinar k_{pr} a partir de k_p y m:

$$D(k_{pr}, E(k_p, m)) = m$$

Un ejemplo clásico de encriptación asimétrica es el **algoritmo RSA**, cuyo nivel de seguridad se basa en la dificultad de factorizar números compuestos muy grandes. Además, este tipo de encriptación permite funciones avanzadas como las **firmas digitales**, donde un remitente firma un mensaje con su clave privada, permitiendo que cualquiera lo verifique utilizando su clave pública.



Comparación matemática entre encriptación simétrica y asimétrica

Desde un enfoque matemático, la encriptación simétrica y asimétrica presentan diferencias fundamentales:

Característica	Encriptación Simétrica	Encriptación Asimétrica
Uso de claves	Una sola clave secreta k	Par de claves: k_p (pública) y k_{pr} (privada)
Rapidez	Rápida y eficiente	Más lenta, requiere más recursos computacionales
Seguridad	Riesgo si la clave es comprometida	Mayor seguridad al no compartir clave privada
Aplicaciones	Cifrado de datos en reposo y transmisión de datos	Autenticación, firmas digitales, SSL/TLS

Cuadro 3.5: Comparación entre encriptación simétrica y asimétrica

3.5.3. Algoritmo de Exponenciación Rápida

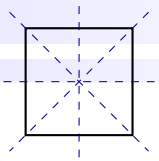
En muchos sistemas criptográficos, como los criptosistemas RSA y Diffie-Hellman, es necesario calcular grandes potencias de un número g módulo otro número N, donde N puede tener cientos de dígitos. Un cálculo ingenuo de g^A mediante multiplicaciones repetidas es ineficiente. Por ejemplo, calcular $g^{2^{1000}}$ de forma directa tomaría más tiempo que la edad estimada del universo.

Una solución más eficiente proviene de la **exponenciación rápida**, que se basa en la descomposición del exponente en su representación binaria y el uso de cuadrados sucesivos para reducir la cantidad de operaciones.

Relación con Teoría de Grupos

En el contexto de la teoría de grupos, este método es fundamental en el estudio de grupos cíclicos y exponentes en grupos finitos. Si consideramos un grupo finito G de orden n con un generador g, entonces cualquier elemento del grupo puede escribirse como g^k para algún entero k. La exponenciación rápida permite calcular eficientemente potencias de g, lo que es útil en algoritmos criptográficos y en el estudio de isomorfismos entre grupos cíclicos.

Dado un grupo G, el subconjunto generado por g es un subgrupo cíclico de G, denotado como:



$$\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$$

Si G es cíclico de orden n, la exponenciación rápida permite determinar la equivalencia de elementos y calcular eficientemente exponentes módulo n, facilitando la verificación de isomorfismos entre grupos cíclicos.

Ejemplo 3.5.4.

Suponga que se quiere calcular 3^{218} mod 1000. El primer paso es expresar 218 en base 2:

$$218 = 2^1 + 2^3 + 2^4 + 2^6 + 2^7$$

Entonces, se reescribe la potencia:

$$3^{218} = 3^{2^1} \cdot 3^{2^3} \cdot 3^{2^4} \cdot 3^{2^6} \cdot 3^{2^7}$$

Se calcula las potencias por cuadrados sucesivos:

i	3^{2^i} (mod1000)
0	3
1	9
2	81
3	561
4	721
5	841
6	281
7	961

Ahora, se usa esta tabla para seleccionar las potencias necesarias:

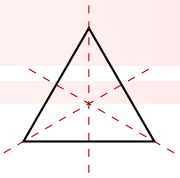
$$3^{218} = 3^{2^1} \cdot 3^{2^3} \cdot 3^{2^4} \cdot 3^{2^6} \cdot 3^{2^7} \equiv 9 \cdot 561 \cdot 721 \cdot 281 \cdot 961 \ (\text{mod}1000)$$

Realizando las multiplicaciones módulo 1000, se obtiene:

$$3^{218} \equiv 489 \ (\text{mod}1000)$$

Algoritmo de Exponenciación Rápida

El algoritmo de exponenciación rápida se estructura en tres pasos:



1. **Expansión binaria del exponente:** Se expresa A en su forma binaria:

$$A = A_0 + A_1 \cdot 2 + A_2 \cdot 2^2 + A_3 \cdot 2^3 + \cdots + A_r \cdot 2^r$$

donde $A_0, \ldots, A_r \in \{0, 1\}$ y $A_r = 1$.

2. **Cálculo de las potencias intermedias:** Se calculan las potencias $g^{2^i} \pmod{N}$ mediante cuadrados sucesivos:

$$a_0 \equiv g \pmod{N}$$

$$a_1 \equiv a_0^2 \pmod{N}$$

$$a_2 \equiv a_1^2 \pmod{N}$$

$$\vdots$$

$$a_r \equiv a_{r-1}^2 \pmod{N}$$

Esto requiere r multiplicaciones.

3. **Cálculo de g^A mod N:** Se usa la expansión binaria para seleccionar los valores de a_i donde $A_i = 1$ y multiplicarlos:

$$g^A = g^{A_0 + A_1 \cdot 2 + A_2 \cdot 2^2 + \cdots + A_r \cdot 2^r}$$

$$= g^{A_0} \cdot (g^2)^{A_1} \cdot (g^{2^2})^{A_2} \cdots (g^{2^r})^{A_r}$$

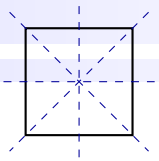
$$\equiv a_0^{A_0} \cdot a_1^{A_1} \cdot a_2^{A_2} \cdots a_r^{A_r} \pmod{N}$$

Este método optimiza el cálculo exponencial en grupos cíclicos y se usa en criptografía moderna. Además, permite estudiar isomorfismos entre grupos, ya que si G y H son grupos cíclicos, entonces $G \cong H$ si comparten la misma estructura de orden y exponentes, lo cual se puede verificar eficientemente con exponenciación rápida.

Ejemplo 3.5.5.

A continuación se presenta un ejemplo concreto que ilustra el algoritmo de exponenciación rápida, siguiendo los tres pasos dados originalmente.

1. Expansión binaria del exponente



Sea $A = 13$. Su representación en base 2 es:

$$13_{10} = 1101_2,$$

lo que se descompone como:

$$13 = 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$$

Por lo tanto, se tienen los coeficientes:

$$A_3 = 1, \quad A_2 = 1, \quad A_1 = 0, \quad A_0 = 1$$

2. Cálculo de las potencias intermedias

Sea $g = 3$ y $N = 17$. Se definen las potencias intermedias mediante cuadrados sucesivos:

- **Paso 2.1:**

$$a_0 \equiv g \pmod{N} \quad \Rightarrow \quad a_0 = 3 \pmod{17}, \text{ o simplemente } a_0 = 3$$

- **Paso 2.2:**

$$a_1 \equiv a_0^2 \pmod{N} \quad \Rightarrow \quad a_1 = 3^2 \pmod{17} = 9 \pmod{17}, \text{ o bien } a_1 = 9$$

- **Paso 2.3:**

$$a_2 \equiv a_1^2 \pmod{N} \quad \Rightarrow \quad a_2 = 9^2 \pmod{17} = 81 \pmod{17}$$

Como $81 = 17 \cdot 4 + 13$, se tiene:

$$a_2 = 13$$

- **Paso 2.4:**

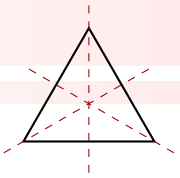
$$a_3 \equiv a_2^2 \pmod{N} \quad \Rightarrow \quad a_3 = 13^2 \pmod{17} = 169 \pmod{17}.$$

Dado que $169 = 17 \cdot 9 + 16$, se obtiene:

$$a_3 = 16$$

3. Cálculo de 3^{13} **mod** 17

Utilizando la expansión binaria del exponente, se multiplican las potencias intermedias correspondientes



a los dígitos binarios que son 1:

$$3^{13} = 3^{1\cdot 2^0+0\cdot 2^1+1\cdot 2^2+1\cdot 2^3} = a_0^{A_0} \cdot a_1^{A_1} \cdot a_2^{A_2} \cdot a_3^{A_3}$$

Sustituyendo los valores (recordando que $A_0 = 1$, $A_1 = 0$, $A_2 = 1$ y $A_3 = 1$):

$$3^{13} \pmod{17} \equiv a_0^1 \cdot a_1^0 \cdot a_2^1 \cdot a_3^1 \pmod{17} = 3 \cdot 1 \cdot 13 \cdot 16 \pmod{17}$$

Realizando las operaciones:

$$3 \cdot 13 = 39, \quad 39 \cdot 16 = 624.$$

Para hallar 624 (mod 17), se observa que:

$$624 = 17 \cdot 36 + 12,$$

por lo que:

$$624 \equiv 12 \pmod{17}$$

Finalmente,

$$3^{13} \equiv 12 \pmod{17}$$

De esta forma, el proceso del cálculo se divide en tres pasos fundamentales:

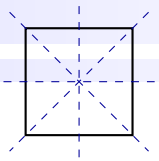
1. **Expansión binaria del exponente:** Se representa el exponente A en base 2. En este ejemplo, 13 se expresa como 1101_2.

2. **Cálculo de las potencias intermedias:** Se calculan los valores $a_0, a_1, a_2, \ldots, a_r$ mediante la técnica de cuadrados sucesivos, tal como se realizó para obtener $a_0 = 3$, $a_1 = 9$, $a_2 = 13$ y $a_3 = 16$.

3. **Cálculo final mediante multiplicación:** Se usan los dígitos binarios de A para seleccionar y multiplicar las potencias intermedias correspondientes, obteniéndose así $3^{13} \pmod{17} = 12$.

3.5.4. El problema del logaritmo discreto

El problema del logaritmo discreto surge en el contexto de los **grupos cíclicos**, desempeñando un papel fundamental en criptografía. Consideremos un grupo cíclico finito G, generado por un elemento g, lo que significa que todo elemento del grupo puede expresarse como una potencia de g. Matemáticamente, esto se traduce en que, para cualquier $h \in G$, existe un entero x tal que:



$$h = g^x.$$

El valor x en esta ecuación se conoce como el **logaritmo discreto** de h en base g y se denota como:

$$\log_g(h) = x.$$

El problema del logaritmo discreto consiste en determinar x dado g y h, es decir, resolver la ecuación:

$$h = g^x \pmod{p},$$

donde p es un número primo (en el caso del grupo multiplicativo $\mathbb{Z}_p^*$), o más generalmente, encontrar el exponente x en un grupo finito arbitrario.

Dificultad computacional

Calcular $g^x \pmod{p}$ mediante exponenciación modular es una tarea eficiente, ya que se puede realizar con el algoritmo de **exponenciación rápida**. Sin embargo, el problema inverso, es decir, encontrar x dado g y h, es significativamente más difícil. Se recomienda consultar a Menezes, van Oorschot y Vanstone (1996)

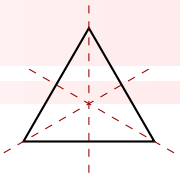
Esta dificultad es precisamente lo que hace atractivo al problema del logaritmo discreto en aplicaciones criptográficas. En criptografía, es esencial que ciertas operaciones sean fáciles de realizar, mientras que su operación inversa sea lo suficientemente difícil de calcular sin información adicional. El logaritmo discreto cumple con esta condición, ya que:

- Es fácil calcular $g^x \pmod{p}$.
- Es computacionalmente difícil recuperar x a partir de $g^x \pmod{p}$ sin conocer x.

Aplicaciones en criptografía

El problema del logaritmo discreto es la base de seguridad de diversos sistemas criptográficos, entre los que destacan:

- **El protocolo de intercambio de claves de Diffie-Hellman**.
- **El algoritmo de cifrado ElGamal**.



El protocolo de intercambio de claves de Diffie-Hellman El algoritmo de Diffie-Hellman resuelve el problema de cómo dos partes pueden generar una clave secreta compartida a través de un canal de comunicación inseguro. Suponga que Alice y Bob desean compartir una clave secreta, pero cualquier información que intercambien puede ser observada por un atacante, Eve.
El protocolo se basa en el hecho de que el problema del logaritmo discreto en el grupo multiplicativo $\mathbb{Z}_p^*$ es difícil de resolver. El procedimiento es el siguiente:

1. Alice y Bob acuerdan un número primo grande p y un generador g de $\mathbb{Z}_p^*$. Estos valores son públicos.

2. Alice elige un número secreto a y calcula:

$$A \equiv g^a \pmod{p}.$$

3. Bob elige un número secreto b y calcula:

$$B \equiv g^b \pmod{p}.$$

4. Alice y Bob intercambian A y B a través del canal público.

5. Ahora, cada uno calcula la clave secreta compartida:

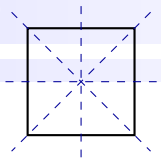
$$S \equiv B^a \equiv (g^b)^a \equiv g^{ab} \pmod{p}, \quad \text{(calculado por Alice)}$$

$$S \equiv A^b \equiv (g^a)^b \equiv g^{ab} \pmod{p}, \quad \text{(calculado por Bob)}$$

Ambos obtienen el mismo valor S sin haber transmitido directamente la clave secreta. Eve, que conoce los valores públicos p, g, A y B, no puede calcular S sin resolver el problema del logaritmo discreto, lo cual es computacionalmente inviable si p es suficientemente grande.

En síntesis, el intercambio de claves Diffie-Hellman se fundamenta en el problema del logaritmo discreto en grupos cíclicos, lo que lo convierte en un mecanismo seguro para el establecimiento de claves compartidas. Por otro lado, los sistemas basados en curvas elípticas aprovechan la estructura de estos cuerpos, donde los puntos sobre la curva forman un grupo abeliano. La dificultad para resolver el logaritmo discreto en estos grupos incrementa la seguridad del algoritmo.

Ejemplo 3.5.6.



Sea $p = 56509$ un número primo, y $g = 2$ una raíz primitiva módulo p. Se desea calcular el logaritmo discreto de $h = 38679$, es decir, encontrar x tal que:

$$2^x \equiv 38679 \pmod{56509}.$$

El único método inmediato sería calcular:

$$2^2, 2^3, 2^4, 2^5, \ldots \pmod{56509}$$

hasta encontrar un valor igual a 38679. Utilizando una computadora, se encuentra que:

$$\log_2(38679) = 11235.$$

Se puede verifica esto calculando:

$$2^{11235} \pmod{56509}.$$

Considere nuevamente el problema en donde Alice y Bob desean compartir una clave secreta nuevamente con valores numéricos:

Ejemplo 3.5.7.

Alice utiliza un sistema RSA para firmar digitalmente un mensaje y enviárselo a Bob. Se le asignan los siguientes parámetros:

- Clave pública: $(e, n) = (7, 55)$.
- Clave privada: $d = 23$.
- Mensaje a firmar: $M = 15$.

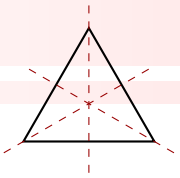
Se requiere:

1. Determinar la firma digital generada por Alice utilizando su clave privada.
2. Verificar, desde la perspectiva de Bob, la autenticidad del mensaje recibido.

Solución

1. Generación de la firma digital Alice firma el mensaje M utilizando su clave privada d mediante la fórmula:

$$S \equiv M^d \pmod{n}.$$



Dado que $M = 15$, $d = 23$ y $n = 55$, se tiene:

$$S \equiv 15^{23} \bmod 55.$$

Utilizaremos el método de exponenciación rápida para calcular $15^{23} \pmod{55}$.

Cálculo mediante potencias sucesivas:

- $15^1 \equiv 15 \pmod{55}$.
- Observe que

$$\begin{aligned} 15^2 = 225 &\equiv (225 - 4 \cdot 55) \pmod{55} \\ &= (225 - 220) \pmod{55} \end{aligned}$$

  Como $225 - 220 \equiv 5 \pmod{55}$ entonces

$$15^2 \equiv 5225 - 220 = 5 \pmod{55}$$

- DE la misma manera

$$15^4 = (15^2)^2 \equiv 5^2 \pmod{55} = 25 \pmod{55}.$$

- Similarmente

$$15^8 = (15^4)^2 \equiv 25^2 \pmod{55}$$

  pero

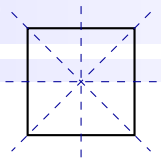
$$625 \equiv (625 - 11 \cdot 55) \pmod{55} = 20 \pmod{55}.$$

  Entonces

$$15^8 \equiv 20 \pmod{55}$$

- Finalmente

$$15^{16} = (15^8)^2 \equiv 20^2 \pmod{55} = 400 \pmod{55}$$



pero

$$400 \equiv (400 - 7 \cdot 55) \pmod{55} = 15 \pmod{55}$$

por lo que

$$15^{16} \equiv 15 \pmod{55}$$

Ahora, dado que $23 = 16 + 4 + 2 + 1$, se tiene:

$$15^{23} \equiv 15^{16} \cdot 15^4 \cdot 15^2 \cdot 15^1 \pmod{55}.$$

Sustituyendo los valores obtenidos:

$$15^{23} \equiv 15 \cdot 25 \cdot 5 \cdot 15 \pmod{55}.$$

Realizando las multiplicaciones:

$$\begin{aligned} 15 \cdot 25 &= 375 \equiv (375 - 6 \cdot 55) \pmod{55} = (375 - 330) \pmod{55} = 45 \pmod{55}, \\ 45 \cdot 5 &= 225 \equiv (225 - 4 \cdot 55) \pmod{55} = (225 - 220) \pmod{55} = 5 \pmod{55}, \\ 5 \cdot 15 &= 75 \equiv (75 - 1 \cdot 55) \pmod{55} = 20 \pmod{55}. \end{aligned}$$

Por lo tanto, la firma digital generada por Alice es:

$$S = 20.$$

2. Verificación de la firma (Desde la perspectiva de Bob) Bob verifica la autenticidad del mensaje recibido utilizando la clave pública, calculando:

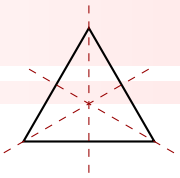
$$M' \equiv S^e \pmod{n}.$$

Con $S = 20$, $e = 7$ y $n = 55$, se tiene:

$$M' \equiv 20^7 \pmod{55}.$$

Procedamos a calcular $20^7 \pmod{55}$ mediante potencias sucesivas:

- $20^1 \equiv 20 \pmod{55}$.



- $20^2 = 20^2 = 400 \equiv (400 - 7 \cdot 55) \pmod{55} = (400 - 385) \pmod{55} = 15 \pmod{55}$.
- $20^4 \equiv (20^2)^2 \equiv 15^2 \pmod{55} = 225 \pmod{55}$

  Pero

$$225 \equiv (225 - 4 \cdot 55) \pmod{55} = (225 - 220) \pmod{55} = 5 \pmod{55}.$$

  Por lo que

$$20^4 \equiv 5 \pmod{55}$$

Como $7 = 4 + 2 + 1$, se tiene:

$$20^7 \equiv 20^4 \cdot 20^2 \cdot 20^1 \pmod{55}.$$

Sustituyendo los valores:

$$20^7 \equiv 5 \cdot 15 \cdot 20 \pmod{55}.$$

Realizamos las multiplicaciones:

$$5 \cdot 15 = 75 \equiv 75 - 1 \cdot 55 = 20 \pmod{55},$$

$$20 \cdot 20 = 400 \equiv 400 - 7 \cdot 55 = 400 - 385 = 15 \pmod{55}.$$

De este modo:

$$M' = 15.$$

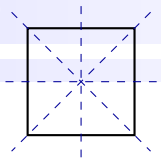
Dado que $M' = 15$ coincide con el mensaje original M, Bob confirma la autenticidad del mensaje firmado.

Conclusión: La firma digital generada por Alice es $S = 20$ y, al ser verificada mediante la clave pública, se recupera el mensaje original $M = 15$, lo que garantiza la integridad y autenticidad del mensaje.

Resistencia frente a ataques

Existen varios algoritmos que intentan resolver el problema del logaritmo discreto de manera eficiente, entre ellos:

- **Método baby-step giant-step**.
- **Algoritmo de Pollard rho**.



- **Algoritmo de descenso numérico en cuerpos finitos**.

Sin embargo, estos métodos tienen costos computacionales elevados y su eficiencia decrece rápidamente conforme aumenta el tamaño del grupo. Por esta razón, los grupos finitos utilizados en aplicaciones criptográficas suelen tener tamaños en el orden de 2^{1024} o mayores, lo que hace que los ataques conocidos sean impracticables con la tecnología actual.

Relación con teoría de grupos

En la teoría de grupos, el logaritmo discreto está estrechamente vinculado con la estructura de los **grupos cíclicos** y los **isomorfismos**. Dado un grupo cíclico $G = \langle g \rangle$, podemos definir el homomorfismo:

$$\varphi : \mathbb{Z} \to G, \quad \varphi(x) = g^x.$$

Este homomorfismo es sobreyectivo y si G es finito de orden n, entonces induce un isomorfismo entre $\mathbb{Z}/n\mathbb{Z}$ y G. Resolver el logaritmo discreto equivale a encontrar la preimagen x bajo este isomorfismo, lo que es computacionalmente difícil en ciertos grupos.
En el contexto de criptografía, la elección del grupo adecuado es crucial para la seguridad del sistema. Si bien algunos grupos permiten resolver el logaritmo discreto en tiempo subexponencial, otros, como los grupos de curvas elípticas, ofrecen mayor resistencia a ataques.

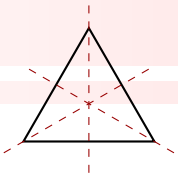
3.5.5. Estándares de Cifrado de Datos. Conexión con teoría de Grupos y Estructuras Algebraicas

La criptografía ha evolucionado significativamente con el tiempo, impulsada por la necesidad de proteger información sensible contra ataques. En el contexto de los **grupos cíclicos** y la **teoría de números**, los estándares de cifrado han aprovechado problemas matemáticos difíciles, como la exponenciación modular y el logaritmo discreto, para garantizar la seguridad de los sistemas modernos. A continuación, se presentan algunos de los principales estándares criptográficos utilizados en la actualidad.[14]

El Estándar de Cifrado de Datos (DES)

El **Data Encryption Standard** (DES) es un algoritmo de cifrado simétrico desarrollado en la década de 1970 y publicado por el *National Bureau of Standards* (NBS) en 1977. Su objetivo era proteger da-

[14]Los algoritmos de cifrado modernos no solo garantizan la confidencialidad de la información, sino que además se fundamentan en profundas estructuras algebraicas. RSA, AES, Diffie-Hellman y otros protocolos utilizan, respectivamente, grupos cíclicos, cuerpos finitos y grupos abelianos (en el caso de las curvas elípticas) para asegurar que operaciones matemáticas aparentemente sencillas sean, desde el punto de vista computacional, difíciles de revertir sin la clave adecuada.



tos electrónicos gubernamentales no clasificados. DES emplea una clave de 56 bits para cifrar bloques de datos de 64 bits mediante un conjunto de permutaciones y sustituciones basadas en estructuras algebraicas.

Sin embargo, debido a los avances tecnológicos, el tamaño de la clave de DES se volvió insuficiente. A medida que la capacidad computacional aumentó, la seguridad del algoritmo disminuyó drásticamente. La siguiente tabla ilustra la progresión de ataques exitosos contra DES:

Año	Evento
1973	Publicación del estándar por el NBS.
1997	Primera desencriptación pública de un mensaje cifrado con DES.
1998	Clave DES descifrada en 56 horas.
1999	Clave DES descifrada en 22 horas y 15 minutos.
2017	Clave DES descifrada en 25 segundos.

Cuadro 3.6: Cronología de la vulnerabilidad del algoritmo DES

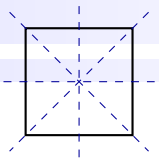
Debido a estas vulnerabilidades, surgió la necesidad de desarrollar algoritmos de cifrado más robustos, lo que llevó al establecimiento de nuevos estándares criptográficos.

AES: Advanced Encryption Standard

Tras la obsolescencia de DES, se introdujo el **Advanced Encryption Standard** (AES) como reemplazo. AES es un cifrado **simétrico**, lo que significa que utiliza la misma clave para cifrar y descifrar los datos. Su principal ventaja radica en su eficiencia y seguridad, logradas mediante el uso de operaciones matriciales sobre cuerpos finitos, lo que está directamente relacionado con la **teoría de grupos**.
AES cifra bloques de datos de 128 bits utilizando claves de 128, 192 o 256 bits. Dependiendo de la longitud de la clave, el cifrado se realiza en 10, 12 o 14 rondas, en las cuales se aplican operaciones de sustitución, permutación y combinación de datos. Estas operaciones están fundamentadas en el álgebra modular y la teoría de cuerpos finitos, lo que garantiza una transformación irreversible sin la clave correcta.

Actualmente, AES es ampliamente utilizado en:

- Cifrado de datos en discos y sistemas de archivos.
- Seguridad en redes inalámbricas (como WPA2).
- Protocolos de comunicación segura en internet.



En síntesis, aunque es un algoritmo simétrico, AES opera sobre bloques de datos mediante operaciones que se desarrollan en cuerpos finitos, concretamente en $GF(2^8)$. Las operaciones de sustitución y permutación, esenciales para la difusión y confusión del algoritmo, se basan en cálculos en este cuerpo finito, lo que evidencia la relación con la teoría de grupos y el álgebra modular.

RSA: Rivest-Shamir-Adleman

El algoritmo RSA (Rivest-Shamir-Adleman) es un sistema de **cifrado asimétrico** basado en la dificultad de **factorizar números grandes**, un problema fundamental en la teoría de números. A diferencia de AES, RSA utiliza un par de claves:

- **Clave pública** (k_p): Se utiliza para cifrar los datos.
- **Clave privada** (k_{pr}): Se usa para descifrar los datos.

Matemáticamente, RSA se basa en el hecho de que es fácil calcular:

$$c \equiv m^e \pmod{N},$$

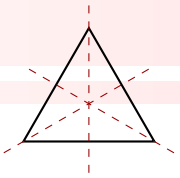
pero es difícil invertir el proceso sin conocer la factorización de N, es decir, hallar m a partir de:

$$m \equiv c^d \pmod{N}.$$

donde $N = pq$, con p y q números primos grandes.
Dado que el cifrado y descifrado implican exponenciación modular, el uso de **exponenciación rápida** es crucial en la implementación de RSA, optimizando los cálculos en **grupos cíclicos**. RSA se usa principalmente en:

- Seguridad de comunicaciones en internet (HTTPS).
- Firmas digitales y autenticación.
- Intercambio seguro de claves en sistemas híbridos que combinan RSA con AES.

En síntesis, Este algoritmo se apoya en el grupo multiplicativo de enteros módulo n (donde $n = pq$ es el producto de dos primos grandes). La seguridad de RSA se fundamenta en la dificultad de factorizar n y, en particular, en la complejidad de invertir la exponenciación modular en un grupo cíclico sin conocer la descomposición en factores primos.



3.5.6. Uso de la Tecnología en Criptografía

La criptografía ha evolucionado desde métodos simples, como el **Cifrado de César**, hasta sistemas avanzados basados en problemas matemáticos complejos, como se ha visto.

Hoy en día, tecnologías modernas han adaptado este principio, permitiendo su visualización en línea. Un ejemplo es la herramienta *Invent with Python*, donde los usuarios pueden experimentar con la clave de cifrado para encriptar mensajes:

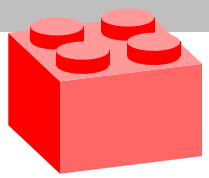
https://inventwithpython.com/cipherwheel/

3.5.7. Perspectivas Futuras de la Criptografía

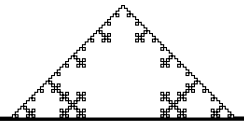
El futuro de la criptografía se dirige hacia métodos resistentes a la computación cuántica. Actualmente, se investiga la **criptografía poscuántica**, basada en problemas matemáticos que las computadoras cuánticas no pueden resolver eficientemente. Entre las técnicas en desarrollo destacan:

- Cifrado basado en **redes euclidianas** y **logaritmos en curvas elípticas**.
- Algoritmos de **firma digital** resistentes a la computación cuántica.
- Protocolos de intercambio de claves utilizando **criptografía cuántica**.

Estos avances garantizarán la seguridad de los sistemas de información en la era de la computación cuántica, asegurando la protección de datos sensibles en el futuro.



Soluciones



Soluciones de la sección 1.3

Ver p.12

Solución 1.3.1 (Divisibilidad)

Como $a, b \in \mathbb{Z}$ tales que $a|b$ se tiene que

$a|b \Leftrightarrow b = ak, k \in \mathbb{Z} \Leftrightarrow b = (-a)(-k), k \in \mathbb{Z} \Leftrightarrow b = -ar, r = -k \in \mathbb{Z} \Leftrightarrow \boxed{-a \mid b}$

$a|b \Leftrightarrow b = ak, k \in \mathbb{Z} \Leftrightarrow -b = -(ak), k \in \mathbb{Z} \Leftrightarrow -b = a(-k), k \in \mathbb{Z} \Leftrightarrow -b = am, m = -k \in \mathbb{Z} \Leftrightarrow \boxed{a \mid (-b)}$

$a|b \Leftrightarrow b = ak, k \in \mathbb{Z} \Leftrightarrow -b = -(ak), k \in \mathbb{Z} \Leftrightarrow -b = (-a)k, k \in \mathbb{Z} \Leftrightarrow \boxed{(-a) \mid (-b)}$

□

Ver p.12

Solución 1.3.2 (Divisibilidad)

En efecto

$a|b \Leftrightarrow b = ak, k \in \mathbb{Z} \Leftrightarrow cb = cak, k \in \mathbb{Z} \Leftrightarrow cb = a(ck), k \in \mathbb{Z} \Leftrightarrow cb = al, ck = l \in \mathbb{Z} \Leftrightarrow \boxed{a \mid cb}$

$a|b \Leftrightarrow b = ak_1, k_1 \in \mathbb{Z}$. Luego $a|c \Leftrightarrow c = ak_2, k_2 \in \mathbb{Z}$. Se sigue que $bc = (ak_1)(ak_2) = a^2k, k = k_1k_2 \in \mathbb{Z} \Leftrightarrow \boxed{a^2 \mid bc}$

□

Ver p.12

Solución 1.3.3 (Divisibilidad)

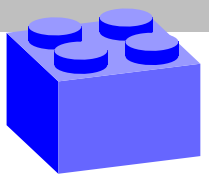
La solución de este ejercicio radica en la implementación de la inducción matemática. Puede definir

$$P(n) : n^3 + 2n = 3k, \text{para algún } k \in \mathbb{Z}.$$

Hay que mostrar que

$$P(n+1) : (n+1)^3 + 2(n+1) = 3r, \text{para algún } r \in \mathbb{Z}$$

Note que $(n+1)^3 + 2(n+1) = (n^3 + 2n) + 3(n^2 + n + 1)$ es divisible por 3 porque $n^3 + 2n$ lo es (gracias a la hipótesis de inducción) y $3(n^2 + n + 1)$ también lo es (porque es 3 veces un número entero). Por lo tanto, la suma también es divisible por 3.



□

Solución 1.3.4 (Divisibilidad) Ver p.12

Sea $a = 2k + 1$ y $b = 2l + 1$, $k, l \in \mathbb{N}$. Luego el término $a^2 - b^2$ se puede escribir como

$$a^2 - b^2 = (a + b)(a - b) = 4((k - l)(k + l + 1))$$

el cual es divisible por 8 si $(k + l + 1)$ o $(k - l)$ es divisible por 2. Si $k - l$ es par, se termina la prueba. Si $k - l$ es impar, $k - l + 1$ es par, y por lo tanto $k + l + 1 = (k - l + 1) + 2l$ es par y también se termina la prueba. En cualquier caso, $(k - l)(k + l + 1)$ es divisible por 2 y, por ende, $a^2 - b^2$ es divisible por 8.

□

Solución 1.3.5 (Residuo) Ver p.12

Sea $a = 2k + 1$, donde k es un número entero. Luego:

$$(2k + 1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$$

Si k es par sucede que $k^2 + k$ es múltiplo de dos y con ello $4(k^2 + k) + 1 = 4(2r) + 1 = 8r + 1, r \in \mathbb{Z}$ con lo cual el residuo es 1.

Si k es impar sucede que $k^2 + k$ es múltiplo de dos también y con ello $4(k^2 + k) + 1 = 4(2p) + 1 = 8p + 1, p \in \mathbb{Z}$ con lo cual el residuo es 1.

En cualquier caso, si a es impar, al dividir este número por 8 el residuo es 1.

□

Solución 1.3.6 (Divisibilidad) Ver p.13

Esta es una prueba que se hace en dos direcciones. Esto es:

1. Suponga que $a|b$. Esto significa que existe un entero k tal que $b = a \cdot k$. Dividiendo ambos lados por d, se tiene

   $$\frac{b}{d} = \frac{a \cdot k}{d}$$

   Dado que d divide a a (es decir, $a = d \cdot m$), se puede reescribir la expresión como

   $$\frac{b}{d} = \frac{d \cdot m \cdot k}{d}$$

   Simplificando

   $$\frac{b}{d} = m \cdot k$$

lo que implica que $\frac{a}{d}\left|\frac{b}{d}\right.$.

2.Suponga que $\frac{a}{d}\left|\frac{b}{d}\right.$. Esto significa que existe un entero m tal que

$$\frac{b}{d} = \frac{a}{d} \cdot m$$

Multiplicando ambos lados por d, se tiene que $b = a \cdot m$. Esto demuestra que $a|b$.

Con ambas explicaciones se completa el ejercicio.

□

Ver p.13 **Solución 1.3.7 (Divisibilidad)**

Sea $a = 2k + 1$, donde k es un número entero. Luego:

$$(2k+1)^2 + (2k+1+2)^2 + (2k+1+4)^2 + 1 = 12k^2 + 36k + 36 = 12(k^2 + 3k + 3)$$

Mostrando lo solicitado.

□

Ver p.13 **Solución 1.3.8 (Divisibilidad)**

Para este ejercicio se toma+1n dos casos

1.Sea $a = 2k + 1$, donde k es un número entero. Luego:

$$(2k+1)(2k+1+1) = 2(2k+1)(k+1)$$

Mostrando lo solicitado.

2.Sea $a = 2r$, donde r es un número entero. Luego:

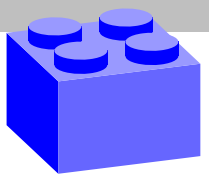
$$(2r)(2r+1) = 2(r)(2r+1)$$

Mostrando lo solicitado.

□

Ver p.13 **Solución 1.3.9 (Algoritmo de la división)**

La afirmación se refiere al algoritmo de la división. Para ello se debe probar la existencia y unicidad.



1. **Existencia:** Primero, se prueba la existencia de q y r que satisfacen la condición dada. Considere la siguiente expresión:

$$a = qb + r$$

Donde q es el cociente y r es el residuo tal que $2b \leq r < 3b$. Se puede reescribir la desigualdad como $b \leq r < 2b$. Ahora, dividiendo ambos lados por b se obtiene:

$$1 \leq \frac{r}{b} < 2$$

Dado que r/b es el cociente y es un número entero, esto significa que el cociente debe ser 1. Por lo tanto, $q = 1$ y $r = a - b$. Entonces, la existencia de q y r está demostrada.

2. **Unicidad:** Se debe probar que no puede haber otros valores para q y r que cumplan con la condición dada.

Suponga que existen dos conjuntos distintos de valores q_1, r_1 y q_2, r_2 que satisfacen $a = q_1 b + r_1$ y $a = q_2 b + r_2$ con $2b \leq r_1 < 3b$ y $2b \leq r_2 < 3b$.

Restando las dos ecuaciones se tiene:

$$(q_1 - q_2)b + (r_1 - r_2) = 0$$

Esto implica que b divide a $(r_1 - r_2)$. Dado que $2b \leq r_1, r_2 < 3b$, la única manera en que b puede dividir $(r_1 - r_2)$ es si $r_1 = r_2$.

Por lo tanto, se prueba que si hay dos conjuntos distintos de valores q_1, r_1 y q_2, r_2 que satisfacen la condición dada, entonces $r_1 = r_2$. Pero esto contradice la condición de unicidad de los residuos en la división, lo que significa que no puede haber dos conjuntos distintos de valores. Por lo tanto, los valores q y r son únicos.

Se ha demostrado tanto la existencia como la unicidad de los enteros q y r que cumplen con la condición dada en el algoritmo de la división para este ejercicio.

□

Solución 1.3.10 (Divisibilidad) Ver p.13

La afirmación se refiere al algoritmo de la división. Para demostrar que $b|a$ si y solo si el residuo de dividir a por b es igual a cero, se deben analizar ambas direcciones.

1. $b|a \Rightarrow$ Residuo $= 0$: Suponga que $b|a$, es decir, $a = bq$ para algún entero q. Utilizando la definición de divisibilidad, esto implica que existe un cociente q tal que a es divisible por b.

   Expresando a en términos de b y q:

   $$a = bq$$

   Al aplicar el algoritmo de la división, el residuo (r) es igual a cero.

   Por lo tanto, se demuestra que si $b|a$, entonces el residuo de dividir a por b es igual a cero.

2. Residuo $= 0 \Rightarrow b|a$: Ahora, suponga que el residuo de dividir a por b es igual a cero, es decir, existe un entero q tal que $a = bq + 0$.

   Esto implica que $a = bq$ y, por lo tanto, $b|a$ según la definición de divisibilidad.

   Entonces, se demuestra que si el residuo de dividir a por b es igual a cero, entonces $b|a$.

Conclusión:
Al combinar ambas direcciones, se prueba el enunciado.

□

Ver p.13

Solución 1.3.11 (Divisibilidad)

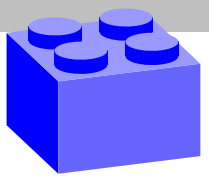
Para demostrar que cualquier número entero de la forma $6k+5$ es también de la forma $3m+2$, se establece una relación entre k y m.

- **Demostración de $6k + 5$ es $3m + 2$:**

  - Tome un número entero de la forma $6k + 5$, donde k es cualquier número entero.
  - Divida $6k + 5$ por 3 y observe los posibles residuos.
  - Si k es par, es decir, $k = 2r$ para un entero r, entonces $6k + 5 = 6(2r) + 5 = 12r + 5 = 3(4r) + 5 = 3(4r) + 3 + 2 = 3m + 2$ con $m = 4r + 1$, es decir, $6k$ es múltiplo de 3 y el residuo al dividir $6k + 5$ por 3 será 2.
  - Si k es impar, es decir, $k = 2r + 1$ para un entero r, entonces $6k + 5 = 6(2r + 1) + 5 = 12r + 6 + 5 = 3(4r) + 9 + 2 = 3(4r + 3) + 2 = 3m + 2$ con $m = 4r + 3$, es decir, al dividir $6k + 5$ por 3 el residuo será 2 también.

  Así, se demuestra que cualquier número de la forma $6k + 5$ se puede expresar como $3m + 2$.

- **Demostración de que lo contrario no sucede:**



- Suponga que $3m + 2$ es de la forma $6k + 5$, donde m y k son números enteros.
- Al restar 2 de ambos lados se obtiene $3m = 6k + 3$.
- Dividiendo ambos lados por 3, se obtiene $m = 2k + 1$.
- Esto significa que m es impar. En efecto: suponga que k pueda ser par o impar.
- Si k es par ($k = 2l$ para l entero), entonces $m = 2(2l) + 1 = 4l + 1$ representa un impar.
- Si k es impar ($k = 2s + 1$ para s entero), entonces $m = 2(2s + 1) + 1 = 4s + 3$ representa un impar.
- En ambos casos, $2k + 1$ siempre es un número impar, lo cual contradice la suposición de que m puede ser cualquier número entero.

Por lo tanto, no se puede expresar cualquier número de la forma $3m + 2$ como $6k + 5$.

□

Solución 1.3.12 (Divisibilidad) Ver p.14

Considere un número entero n, y se examina el cuadrado de n, denotado como n^2.

- **Caso 1: n es múltiplo de 3:**
  - Si n es un múltiplo de 3, entonces n puede expresarse como $3k$ para algún entero k.
  - El cuadrado de n es $n^2 = (3k)^2 = 9k^2$, que es un múltiplo de 3 ($9k^2 = 3 \cdot 3k^2$).
  - Por lo tanto, en este caso, n^2 se puede expresar como $3k$.
- **Caso 2: n deja un residuo de 1 al dividirse por 3:**
  - Si n deja un residuo de 1 al dividirse por 3, entonces n puede expresarse como $3k + 1$ para algún entero k.
  - El cuadrado de n es $n^2 = (3k + 1)^2 = 9k^2 + 6k + 1$, que es de la forma $3k + 1$ ($9k^2 + 6k = 3 \cdot (3k^2 + 2k)$).
  - En este caso, n^2 se puede expresar como $3k + 1$.
- **Caso 3: n deja un residuo de 2 al dividirse por 3:**
  - Si n deja un residuo de 2 al dividirse por 3, entonces n puede expresarse como $3k + 2$ para algún entero k.

- El cuadrado de n es $n^2 = (3k+2)^2 = 9k^2 + 12k + 4$, que es de la forma $3k$ $(9k^2 + 12k = 3 \cdot (3k^2 + 4k))$.
- En este caso, n^2 se puede expresar como $3k$.

Por lo tanto, para cualquier número entero n, el cuadrado de n puede expresarse de la forma $3k$ o $3k+1$. □

Ver p.14

Solución 1.3.13 (Divisibilidad)

Suponga por contradicción que existen enteros a y b tales que $a+b = 100$ y $(a,b) = 3$, donde (a,b) denota el máximo común divisor (mcd) de a y b.

Note que si $(a,b) = 3$, entonces 3 divide tanto a a como a b, ya que 3 es el máximo común divisor. Por lo tanto, a y b son múltiplos de 3.

Dado que $a+b = 100$, se pueden considerar las posibles combinaciones de a y b módulo 3, esto es

Caso 1: Si $a \equiv 0 \pmod 3$ y $b \equiv 0 \pmod 3$, entonces $a+b \equiv 0 \pmod 3$, lo cual no es posible ya que $a+b = 100 \equiv 1 \pmod 3$.

Caso 2: Si $a \equiv 1 \pmod 3$ y $b \equiv 2 \pmod 3$, o viceversa, entonces $a+b \equiv 0 \pmod 3$, lo cual también es incompatible con $a+b = 100 \equiv 1 \pmod 3$.

Caso 3: Si $a \equiv 2 \pmod 3$ y $b \equiv 1 \pmod 3$, o viceversa, entonces $a+b \equiv 0 \pmod 3$, lo cual es incompatible con $a+b = 100 \equiv 1 \pmod 3$.

En todos los casos, se llega a una contradicción, ya que no es posible que la suma de a y b sea 100 módulo 3. Por lo tanto, la suposición inicial de que existen enteros a y b que cumplen ambas condiciones es falsa.

Se concluyen que no existen enteros a y b tales que $a+b = 100$ y $(a,b) = 3$. □

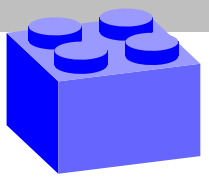
Ver p.14

Solución 1.3.14 (Divisibilidad)

Suponga que $(a,b) = 1$, es decir, los números a y b son primos relativos.

Considere el máximo común divisor $d = (2a+b, a+2b)$.

Caso 1: Suponga que $d = 1$. Esto significa que $2a+b$ y $a+2b$ son primos relativos, ya que no tienen factores primos comunes.



Caso 2: Suponga que $d = 3$. Esto implicaría que $2a + b$ y $a + 2b$ son múltiplos de 3, pero uno de ellos no puede ser divisible por 3 ya que a y b son primos relativos ($(a, b) = 1$). Por lo tanto, ambos $2a + b$ y $a + 2b$ deben ser divisibles por 3.

Ahora, note que $2a + b + (a + 2b) = 3a + 3b = 3(a + b)$. Esto implica que 3 divide a la suma $2a + b + (a + 2b)$. Por lo tanto, 3 divide tanto a $2a + b$ como a $a + 2b$, y en consecuencia, $d = (2a + b, a + 2b) = 3$.

En resumen, se ha demostrado que si $(a, b) = 1$, entonces $(2a + b, a + 2b)$ es igual a 1 o 3. □

Solución 1.3.15 (Divisibilidad) Ver p.14

Consideremos el máximo común divisor $d = (a + b, ab)$.

Suposición por Contradicción:

Suponga por contradicción que $d > 1$. Esto implica que d tiene que ser un número primo, ya que cualquier factor común de $a + b$ y ab sería también un factor común de a y b, lo cual contradice la premisa de que $(a, b) = 1$.

Análisis:

Dado que $d > 1$, se puede decir que d es un factor común de $a + b$ y ab. Esto implica que d divide tanto a $a + b$ como a ab.

Recuerde que $a + b$ es la suma de a y b, y ab es el producto de a y b.

Si d divide a $a + b$, entonces d divide a a y b por separado.

Si d divide a ab, entonces d divide a a o b o ambos.

Esto contradice la suposición inicial de que $(a, b) = 1$, ya que si d divide a a, b o ambos, entonces d sería mayor que 1.

Por lo tanto, se llega a la conclusión de que nuestra suposición inicial es incorrecta, y $d = (a + b, ab)$ debe ser igual a 1.

Conclusión:

Se ha demostrado que si $(a, b) = 1$, entonces $(a + b, ab) = 1$.

□

Ver p.14

Solución 1.3.16 (Divisibilidad)

Observe que

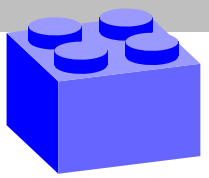
$$\begin{aligned} 2456 &= (-1) \cdot (-1234) + 222 \\ -1234 &= (-6) \cdot 222 + 68 \\ 222 &= 3 \cdot 68 + 18 \\ 68 &= 3 \cdot 18 + 14 \\ 18 &= 1 \cdot 14 + 4 \\ 14 &= 3 \cdot 4 + 2 \\ 4 &= 2 \cdot \boxed{2} + 0 \end{aligned}$$

El último residuo no nulo es 2. De esta forma, el máximo común divisor es 2, o bien $(2456, -1234) = 2$.

Observe que

$$\begin{aligned} 7098 &= 1 \cdot 5096 + 2002 \\ 5096 &= 2 \cdot 2002 + 1092 \\ 2002 &= 1 \cdot 1092 + 910 \\ 1092 &= 1 \cdot 910 + 182 \\ 910 &= 5 \cdot \boxed{182} + 0 \end{aligned}$$

El último residuo no nulo es 182. De esta forma, el máximo común divisor es 182, o bien $(5096, 7098) = 182$.



Observe que

$$\begin{aligned} 12321 &= (1)\cdot(8658) + 3663 \\ 8658 &= (2)\cdot 3663 + 1332 \\ 3663 &= (2)\cdot 1332 + 999 \\ 1332 &= (1)\cdot 999 + 333 \\ 999 &= 3\cdot \boxed{333} + 0 \end{aligned}$$

El último residuo no nulo es 333. De esta forma, el máximo común divisor es 333, o bien $(12321, 8658) = 333$.

Observe que

$$\begin{aligned} 1740 &= 11\cdot 156 + 84 \\ 156 &= 1\cdot 84 + 72 \\ 84 &= 1\cdot 72 + 12 \\ 72 &= 6\cdot \boxed{12} + 0 \end{aligned}$$

El último residuo no nulo es 12. De esta forma, el máximo común divisor es 12, o bien $(156, 1740) = 12$.

□

Solución 1.3.17 (Divisibilidad) Ver p.15

Para hallar s y t tales que $(56, 72) = 56s + 72t$, se puede aplicar el algoritmo de la división

de Euclides de la siguiente manera:

$$\begin{aligned} 72 &= 1 \cdot 56 + 16 \\ 56 &= 3 \cdot 16 + 8 \\ 16 &= 2 \cdot 8 + 0 \end{aligned}$$

En tal caso $(72, 56) = 8$. Ahora, se trabaja hacia atrás para expresar cada residuo como combinación lineal de 56 y 72:

$$\begin{aligned} 8 &= 56 - 3 \cdot 16 \\ &= 56 - 3 \cdot (72 - 56 \cdot 1) \\ &= 4 \cdot 56 - 3 \cdot 72 \end{aligned}$$

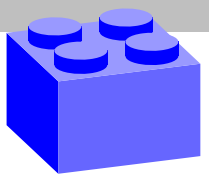
Por lo tanto, $\boxed{s = 4}$ y $\boxed{t = -3}$, y se cumple la igualdad $(56, 72) = 56s + 72t$.

Para hallar s y t tales que $(24, 138) = 24s + 138t$, podemos aplicar el algoritmo de la división de Euclides de la siguiente manera:

$$\begin{aligned} 138 &= 5 \cdot 24 + 18 \\ 24 &= 1 \cdot 18 + 6 \\ 18 &= 3 \cdot 6 + 0 \end{aligned}$$

En tal caso $(24, 138) = 6$. Ahora, se trabaja hacia atrás para expresar cada residuo como una combinación lineal de 24 y 138:

$$\begin{aligned} 6 &= 24 - 1 \cdot 18 \\ &= 24 - 1 \cdot (138 - 5 \cdot 24) \\ &= 6 \cdot 24 - 1 \cdot 138 \end{aligned}$$



Por lo tanto, $\boxed{s = 6}$ y $\boxed{t = -1}$, y se cumple la igualdad $(24, 138) = 24s + 138t$.

Para hallar s y t tales que $(119, 272) = 119s + 272t$, aplicamos el algoritmo de la división de Euclides:

$$\begin{aligned} 272 &= 2 \cdot 119 + 34 \\ 119 &= 3 \cdot 34 + 17 \\ 34 &= 2 \cdot 17 + 0 \end{aligned}$$

En tal caso $(119, 272) = 17$. Ahora, se trabaja hacia atrás para expresar cada residuo como combinación lineal de 119 y 272:

$$\begin{aligned} 17 &= 119 - 3 \cdot 34 \\ &= 119 - 3 \cdot (272 - 2 \cdot 119) \\ &= 7 \cdot 119 - 3 \cdot 272 \end{aligned}$$

Por lo tanto, $\boxed{s = 7}$ y $\boxed{t = -3}$, y se cumple la igualdad $(119, 272) = 119s + 272t$.

□

Solución 1.3.18 (Divisibilidad) Ver p.15

Dado que $ab \equiv 0$ (mód p), significa que p divide a ab exactamente. Esto se puede expresar como $ab = kp$, donde k es un entero.

Ahora, si p divide al producto de dos enteros, entonces p debe dividir al menos a uno de los dos enteros. Es decir, si p divide a ab, entonces p debe dividir a a o a b (o ambos).

Considere dos casos:

Caso 1: Si p divide a a, entonces se puede escribir $a = mp$, donde m es un entero. Ahora,

$ab = kp$ se convierte en $(mp)b = kp$, lo que implica que $b = kb$. Esto significa que p divide a b.

Caso 2: Si p divide a b, entonces se puede escribir $b = np$, donde n es un entero. Ahora, $ab = kp$ se convierte en $a(np) = kp$, lo que implica que $a = kn$. Esto significa que p divide a a.

En ambos casos, se demuestra que si p divide a ab, entonces p debe dividir a a o a b. En términos de congruencia modular, esto se expresa como $[a] = [0]$ o $[b] = [0]$ cuando $ab \equiv 0 \pmod{p}$.

Dada la congruencia $ab \equiv ac \pmod{p}$, se puede restar ac de ambos lados de la congruencia:

$$ab - ac \equiv 0 \pmod{p}$$

Factorizando a del lado izquierdo, se obtiene:

$$a(b - c) \equiv 0 \pmod{p}$$

Dado que $[a] \neq [0]$, esto implica que a no es divisible por p, es decir, p no divide a a. Por lo tanto, p debe dividir al factor $(b - c)$ en el lado izquierdo de la congruencia. Es decir

$$(b - c) \equiv 0 \pmod{p}$$

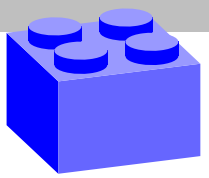
Y bien

$$b \equiv c \pmod{p}$$

En otras palabras, b y c son congruentes módulo p, lo que se expresa como $[b] = [c]$.

Recuerde que si dos números tienen el mismo cuadrado módulo p, entonces son congruentes módulo p o tienen una relación de congruencia módulo p con sus negativos.

Así, dada la congruencia $a^2 \equiv b^2 \pmod{p}$, se puede restar b^2 de ambos lados de la congruencia:



$$a^2 - b^2 \equiv 0 \pmod{p}$$

Factorizando el lado izquierdo como $(a+b)(a-b)$, se obtiene:

$$(a+b)(a-b) \equiv 0 \pmod{p}$$

Ahora, hay dos posibilidades:

1. $(a+b) \equiv 0 \pmod{p}$: En este caso, $a+b$ es divisible por p, lo que implica que $a \equiv -b \pmod{p}$. Por lo tanto, $[a] = -[b]$.
2. Si $(a-b) \equiv 0 \pmod{p}$: En este caso, $a-b$ es divisible por p, lo que implica que $a \equiv b \pmod{p}$. Por lo tanto, $[a] = [b]$.

En ambos casos, si $a^2 \equiv b^2 \pmod{p}$, entonces $[a] = [b]$ o $[a] = -[b]$.

□

Solución 1.3.19 (Divisibilidad) Ver p.15

La congruencia $a \equiv b \pmod{n}$ implica que n divide a $(a-b)$. Esto significa que existe un entero k tal que $a - b = kn$.

Ahora, multiplicando ambos lados por c se tiene que

$$c(a-b) = ckn$$

Esto se puede expresar como $ca - cb = ckn$, o bien, se puede interpretar que cn divide a $ca - cb$, es decir $ca \equiv cb \pmod{cn}$.

Observación: Como $c > 0$ se tiene que $cn > 0$ haciendo viable la división.

□

Solución 1.3.20 (Divisibilidad) Ver p.15

Dado que $a \equiv b \pmod{n}$, se sabe que n divide a $a-b$. Además, dado que a y b son divisibles por d, se puede expresar a y b como $a = md$ y $b = nd$ donde $m, n \in \mathbb{Z}$.

La congruencia $a \equiv b \pmod{n}$ implica que n divide a $a-b$, entonces:

$$n \mid (a-b)$$

Sustituyendo $a = md$ y $b = nd$ en la expresión anterior:

$$n \mid (md - nd)$$

Factorizando d se obtiene:

$$n \mid d(m - n)$$

Ahora, dado que n y d son ambos divisibles por d, se puede cancelar el factor común d en ambos lados de la congruencia:

$$\frac{n}{d} \mid (m - n)$$

Esto significa que $\frac{n}{d}$ divide a $m - n$. En términos de congruencia modular, se puede expresar esto como:

$$m \equiv n \left(\text{mód } \frac{n}{d}\right)$$

Ahora, utilizando la definición de congruencia modular, se puede escribir la última expresión como:

$$\frac{a}{d} \equiv \frac{b}{d} \left(\text{mód } \frac{n}{d}\right)$$

□

Ver p.16 **Solución 1.3.21 (Divisibilidad)**

Tome $n = 15$, $a = 4$ y $b = 11$.

- Al calcular a^2 y b^2 se tiene:

$$4^2 \equiv 16 \equiv 1 \pmod{15}$$

$$11^2 \equiv 121 \equiv 1 \pmod{15}$$

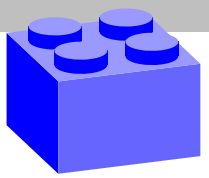
- Observe que $a^2 \equiv b^2 \pmod{15}$ ya que ambos son congruentes a 1 módulo 15.

- Sin embargo, $a \not\equiv b \pmod{15}$ ya que $4 \not\equiv 11 \pmod{15}$.

□

Ver p.16 **Solución 1.3.22 (Divisibilidad)**

Dada la congruencia $a \equiv b \pmod{n}$, esto significa que n divide a $a - b$. De esta forma, se puede expresar



esta divisibilidad como $a - b = nk$ para algún entero k.

Ahora, considere el máximo común divisor de a y n, es decir, (a, n). Se sabe que (a, n) divide a a y n, por lo tanto, también debe dividir a cualquier combinación lineal de a y n. En particular, (a, n) debe dividir a $a-b$.

Similarmente, el máximo común divisior de b y n divide a $a - b$, ya que n también divide a $a - b$ (por la congruencia dada).

Entonces, tanto (a, n) como (b, n) dividen a $a - b$, es decir

$$(a - b)|(a, n) \text{ y } (a - b)|(b, n)$$

Esto implica que ambos comparten los mismos factores primos (o potencias de los factores primos) que dividen a $a - b$.

En resumen, si $a \equiv b \pmod{n}$, entonces $(a, n) = (b, n)$.

□

Soluciones de la sección 2.3

Ver p.68

Solución 2.3.1 (Grupo)

Se tiene que

Se intenta probar que $(\mathbb{R}, *)$ es un grupo y se revisa si falla alguna de las condiciones asociadas. Esto es:

- **Cerradura:** ya se indica en el enunciado.
- **Asociatividad:** observe que para $a, b, c \in \mathbb{R}$ se tiene que

$$a * (b * c) = a * (\pi bc) = \pi a(\pi bc) = \pi(\pi ab)c = \pi(a * b)c = (a * b) * c.$$

- **Neutro:** se puede llegar a mostrar que el neutro es $e = \dfrac{1}{\pi}$ ya que

$$\frac{1}{\pi} * a = \pi\left(\frac{1}{\pi}\right)a = a = \pi a\left(\frac{1}{\pi}\right) = a * \frac{1}{\pi}.$$

- **Inverso:** se puede llegar a mostrar que el inverso para cualquier $a \neq 0$ es $a^{-1} = \dfrac{1}{\pi^2 a}$ ya que

$$a * \left(\frac{1}{\pi^2 a}\right) = \pi a\left(\frac{1}{\pi^2 a}\right) = \frac{1}{\pi}$$

En este caso, existe el 0 como número real que no tiene inverso, por lo cual la estructura dada no es un grupo. Si el cero no se toma en cuenta si se cumple que la operación con el conjunto dado forman un grupo.

En tal caso

$$3^3 * \left[7 * \left(2 * \frac{1}{4}\right)^{-1}\right]^4 = \frac{1037232}{\pi^2}$$

Nota: observe que

$$a^2 = a * a = \pi aa = \pi a^2.$$

$$a^3 = a * a * a = \pi a^2 * a = \pi(\pi a^2)a = \pi^2 a^3.$$

$$a^4 = a * a * a * a = \pi a^2 * \pi a^2 = \pi(\pi a^2)(\pi a^2) = \pi^3 a^4.$$

□

Solución 2.3.2 (Grupo) Ver p.69

En primer lugar, observe que 1 es el neutro en A, ya que para todo $x \in A$ se cumple que

$$x \cdot 1 = x.$$

No obstante, para cualquier valor de x menor a la unidad, este no tiene inverso multiplicativo ya que $\frac{1}{x} > 1$, quedando por fuera de A. Por ejemplo, $\frac{1}{2} \in A$ pero $2 \notin A$. En dicha situación, no se cumple la propiedad de cierre al calcular inversos.

□

Solución 2.3.3 (Grupo) Ver p.69

Se intenta probar que $(\mathbb{R} \times \mathbb{R}^*, \cdot)$ es un grupo y se revisa si falla alguna de las condiciones asociadas. Esto es:

- **Cerradura:** dado que $b \neq 0$ y $d \neq 0$ se tiene que $2bd \neq 0$. Esto es suficiente para justificar que si $(a, b) \in \mathbb{R} \times \mathbb{R}^*$ y $(c, d) \in \mathbb{R} \times \mathbb{R}^*$ entonces $(a+c-4, 2bd) \in \mathbb{R} \times \mathbb{R}^*$.
- **Asociatividad:** observe que para $(a, b), (c, d), (e, f) \in \mathbb{R} \times \mathbb{R}^*$ se tiene que

  $$(a, b) \cdot ((c, d) \cdot (e, f)) = (a, b) \cdot (c + e - 4, 2df) = (a + c + e - 8, 4bdf).$$

  Por otro lado

  $$((a, b) \cdot (c, d)) \cdot (e, f) = (a + c - 4, 2bd) \cdot (e, f) = (a + c + e - 8, 4bdf),$$

  lo cual prueba esta propiedad.
- **Neutro:** se puede llegar a mostrar que el neutro es $e = \left(4, \frac{1}{2}\right)$ ya que

  $$(a, b) \cdot \left(4, \frac{1}{2}\right) = (a, b).$$

- **Inverso:** se puede llegar a mostrar que el inverso para cualquier elemento es

$(a,b)^{-1} = \left(8-a, \frac{1}{4b}\right)$ ya que

$$(a,b)\cdot\left(8-a,\frac{1}{4b}\right) = \left(4,\frac{1}{2}\right).$$

En este caso, el conjunto con la operación indicada si forman un grupo.

En tal caso

$$(2,-1)^3 \cdot \left[\left(0,\frac{1}{3}\right)\cdot(1,-1)^{-1}\right]^2 = \left(-4,-\frac{4}{9}\right).$$

Nota: Observe que

$$(a,b)^2 = (a,b)\cdot(a,b) = (2a-4, 2b^2).$$

$$(a,b)^3 = (a,b)\cdot(a,b)\cdot(a,b) = (a,b)\cdot(2a-4,2b^2) = (3a-8,4b^3).$$

□

Ver p.69

Solución 2.3.4 (Grupo)

Se intenta probar que $]0,+\infty[-\{1\},*)$ es un grupo y se revisa si falla alguna de las condiciones asociadas. Esto es:

- **Cerradura:** dado que $a>0$ y $a\neq 1$ y $b>0$ y $b\neq 1$ se tiene que $a^{\ln b}>0$ y $a^{\ln b}\neq 1$. Esto es suficiente para justificar que si $a\in G$ y $b\in G$ entonces $a*b\in G$.

- **Asociatividad:** observe que para $a,b,c\in G$ se tiene que

$$a*(b*c) = a*(b^{\ln c}) = a^{\ln(b^{\ln c})} = a^{\ln c\cdot lnb}.$$

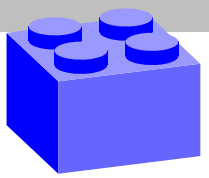
  Por otro lado

$$(a*b)*c = a^{\ln b}*c = (a^{\ln b})^{\ln c} = a^{\ln b\cdot \ln c},$$

  lo cual prueba esta propiedad.

- **Neutro:** se puede llegar a mostrar que el número e es el neutro. En efecto

$$a*e = a \Leftrightarrow a^{\ln e} = a.$$



De igual forma

$$e * a = a \Leftrightarrow e^{\ln a} = a.$$

- **Inverso:** se puede llegar a mostrar que el inverso para cualquier elemento es $a^{-1} = e^{1/\ln a}$ ya que

$$a * e^{1/\ln a} = a^{\ln e^{1/\ln a}} = a^{\frac{1}{\ln a}\cdot \ln e} = a^{\frac{\ln e}{\ln a}} = a^{\log_a e} = e.$$

En este caso, el conjunto con la operación indicada si forma un grupo.

□

Solución 2.3.5 (Grupo)

Ver p.70

Se probará que $(P(U), \triangle)$ es un grupo. Esto es

1. **Cerradura:** dado que $A, B \subset U$, entonces tanto $A-B$ como $B-A$ son subconjuntos de U. La unión de subconjuntos de U también es un subconjunto de U. Por lo tanto, $A \triangle B = (A - B) \cup (B - A)$ es un subconjunto de U, y por ende, pertenece a $P(U)$. Esto demuestra la propiedad de cerradura.

2. **Asociatividad:** para probar la asociatividad, considere tres conjuntos A, B, y C en $P(U)$. Se necesita mostrar que $(A \triangle B) \triangle C = A \triangle (B \triangle C)$. Para ello se usala definición de diferencia simétrica, esto es:

$$(A \triangle B) \triangle C = [(A \triangle B) - C] \cup [C - (A \triangle B)].$$

Sustituyendo $A \triangle B = (A - B) \cup (B - A)$, se obtiene:

$$(A \triangle B) \triangle C = \{[(A - B) \cup (B - A)] - C\} \cup \{C - [(A - B) \cup (B - A)]\}.$$

De forma similar se concluye que

$$A \triangle (B \triangle C) = \{A - [(B - C) \cup (C - B)]\} \cup \{[(B - C) \cup (C - B)] - A\}.$$

Ambas expresiones se simplifican a:

$$(A \triangle B) \triangle C = (A \cup B \cup C) - [(A \cap B) \cup (B \cap C) \cup (C \cap A)],$$

$$A \triangle (B \triangle C) = (A \cup B \cup C) - [(A \cap B) \cup (B \cap C) \cup (C \cap A)].$$

Por lo tanto, dado que la operación $\triangle$ se define en términos de uniones y diferencias de conjuntos, y se sabe que las operaciones de unión y diferencia de conjuntos son asociativas, se concluye que la operación $\triangle$ también es asociativa.

3. **Neutro:** el elemento neutro en este caso es el conjunto vacío $\emptyset$, ya que $A - \emptyset = A$ y $\emptyset - A = \emptyset$. Por lo tanto, $A \triangle \emptyset = (A - \emptyset) \cup (\emptyset - A) = A \cup \emptyset = A$. Esto muestra que el conjunto vacío es el elemento neutro.

4. **Inverso:** el inverso de un conjunto A con respecto a esta operación es el mismo conjunto A, ya que $A \triangle A = (A - A) \cup (A - A) = \emptyset \cup \emptyset = \emptyset$. Esto significa que cada elemento es su propio inverso.

En este caso, el conjunto con la operación indicada forma un grupo.

□

Ver p.70

Solución 2.3.6 (Grupo)

Note que la matriz nula $0_2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ no está en G. Ahora, se probará que G es un grupo con la multiplicación usual de matrices, esto es:

1. **Cerradura:** dadas dos matrices en G,

$$A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, \quad B = \begin{pmatrix} c & d \\ -d & c \end{pmatrix},$$

el producto AB es

$$AB = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac - bd & ad + bc \\ -bc - ad & ac - bd \end{pmatrix}.$$

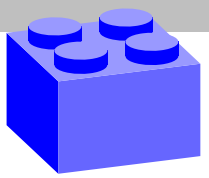
Para que $AB \in G$, se necesita que $(ac - bd)^2 + (ad + bc)^2 \neq 0$. Pero $(ac - bd)^2 + (ad + bc)^2 = (a^2 + b^2)(c^2 + d^2)$, donde cada factor es no nulo. Por lo tanto, $AB \in G$, cumpliendo la propiedad de la cerradura.

2. **Asociatividad:** la asociatividad es una propiedad general de la multiplicación de matrices, por lo que se cumple sin necesidad de demostración específica. Es decir, es una propiedad heredada.

3. **Neutro:** el elemento neutro bajo la multiplicación de matrices es la matriz identidad I_2 definida por

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

que pertenece a G ya que $1^2 + 0^2 = 1 \neq 0$.



4.**Inverso:** para cada matriz en G,

$$A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix},$$

su determinante es $a^2 + b^2$, el cual es distindo cero, así posee inversa, la cual está dada por

$$A^{-1} = \frac{1}{a^2 + b^2} \begin{pmatrix} a & -b \\ b & a \end{pmatrix},$$

que también pertenece a G. Además, note que $AA^{-1} = A^{-1} = I_2$.

En este caso, el conjunto con la operación indicada forma un grupo. □

Solución 2.3.7 (Grupo) Ver p.70

Se probará que $(\mathbb{Z} \times \mathbb{Z}, *)$ es un grupo, esto es:

1.**Cerradura:** Sean $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}$. Entonces,

$$(a, b) * (c, d) = (a + c, (-1)^c b + d).$$

Como $a + c$ y $(-1)^c b + d$ son ambos enteros (la suma y producto de enteros son enteros, y b y d se multiplican o suman por enteros), el resultado pertenece a $\mathbb{Z} \times \mathbb{Z}$. Esto demuestra la propiedad de cerradura.

2.**Asociatividad:** observe que

$$\begin{aligned}((a, b) * (c, d)) * (e, f) &= (a + c, (-1)^c b + d) * (e, f) \\ &= ((a + c) + e, (-1)^e((-1)^c b + d) + f) \\ &= (a + c + e, (-1)^{e+c} b + (-1)^e d + f) \\ &= (a + (c + e), (-1)^{c+e} b + (-1)^e d + f) \\ &= (a, b) * (c + e, (-1)^e d + f) \\ &= (a, b) * ((c, d) * (e, f))\end{aligned}$$

Esto demuestra que la operación $*$ es asociativa.

3.**Neutro:** el elemento neutro bajo esta operación debe satisfacer $(a, b) * (e_1, e_2) = (a, b)$ para todo $(a, b) \in \mathbb{Z} \times \mathbb{Z}$. Esto significa que $a + e_1 = a$ y $(-1)^{e_1} b + e_2 = b$. Por lo tanto, e_1 debe ser 0 (ya que $a + 0 = a$) y para que $(-1)^{e_1} b = b$, e_1 puede ser cualquier entero par, pero dado que también se necesita que e_2 no altere b, e_2 debe ser 0. Así, el elemento neutro es $(0, 0)$.

4. **Inverso:** para encontrar el inverso de un elemento (a, b), se necesita $(a, b) * (c, d) = (0, 0)$. Esto implica que $a + c = 0$ y $(-1)^c b + d = 0$. Por lo tanto, $c = -a$. Para satisfacer $(-1)^{-a} b + d = 0$, se requiere que $d = (-1)^a b$, cuando a es impar, o simplemente $d = -b$, cuando a es par, lo que siempre da un par $(c, d) \in \mathbb{Z} \times \mathbb{Z}$ que funciona como inverso para (a, b).

En este caso, el conjunto con la operación indicada forma un grupo.

□

Ver p.70

Solución 2.3.8 (Grupo)

Se probará que $(A, +)$ forma un grupo bajo la multiplicación usual de matrices, tal que $A = \{a \in \mathbb{Z} : a \equiv 0 \pmod 3\}$. Esto es:

1. **Cerradura:** dado que $a, b \in A$, ambos son divisibles por 3, es decir, existen enteros k, l tales que $a = 3k$ y $b = 3l$. La suma $a + b = 3k + 3l = 3(k + l)$ también es divisible por 3, lo que significa que $a + b \equiv 0 \pmod 3$ y, por lo tanto, $a + b \in A$.

2. **Asociatividad:** la asociatividad es una propiedad inherente de la suma de números enteros, es decir, para cualquier $a, b, c \in \mathbb{Z}$, se cumple que $(a + b) + c = a + (b + c)$. Dado que todos los elementos de A son números enteros, la operación de suma en A también es asociativa.

3. **Neutro:** dado que 0 es divisible por 3, $0 \in A$, cumpliendo con la definición de elemento neutro dentro del conjunto A, ya que $a + 0 = a$ para cualquier entero a.

4. **Inverso:** para cada elemento $a \in A$, se necesita encontrar un elemento $b \in A$ tal que $a + b = 0$. Dado que a es divisible por 3, es decir, $a = 3k$ para algún entero k, el inverso de a es $-a = -3k$, que también es divisible por 3, y por lo tanto, $-a \in A$. Esto demuestra que cada elemento tiene un inverso en A.

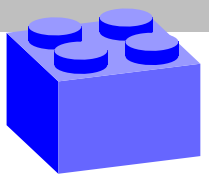
En este caso, el conjunto con la operación indicada forma un grupo.

□

Ver p.70

Solución 2.3.9 (Grupo)

Para probar que B no es un grupo con la operación de suma usual de números enteros, se debe verificar que Bno satisface alguna de las cuatro propiedades fundamentales de un grupo con respecto a la operación: cerradura, asociatividad, existencia de elemento neutro y existencia de inverso para cada elemento. La suma de enteros es bien conocida por ser asociativa, así que se debe hacer un enfoque en las otras tres propiedades.



1. **Cerradura:** tome dos elementos arbitrarios $a, b \in B$, entonces $a \equiv 1 \pmod 3$ y $b \equiv 1 \pmod 3$. Ahora, es necesario cuestionar si su suma $a + b$ también pertenece a B.

   Si $a \equiv 1 \pmod 3$ y $b \equiv 1 \pmod 3$, entonces $a = 3k + 1$ y $b = 3m + 1$ para algunos enteros k y m. Por lo tanto, $a + b = 3k + 1 + 3m + 1 = 3(k + m) + 2$. Esto implica que $a + b \equiv 2 \pmod 3$ y no $1 \pmod 3$ como se requiere para que un elemento pertenezca a B. Esto muestra que B no es cerrado bajo la operación de suma.

2. **Neutro:** el elemento neutro en el contexto de la suma de enteros es 0, pero $0 \not\equiv 1 \pmod 3$, por lo que $0 \notin B$. Esto significa que no existe un elemento neutro dentro de B que satisfaga la propiedad para todo elemento en B bajo la suma.

3. **Inverso:** aún si se intentara encontrar inversos dentro de B, el hecho de que B no es cerrado bajo la suma y la ausencia de un verdadero elemento neutro dentro de B hace imposible cumplir esta propiedad.

Por lo tanto, se ha demostrado que B no es un grupo bajo la suma usual de números enteros.

□

Solución 2.3.10 (Grupo) Ver p.71

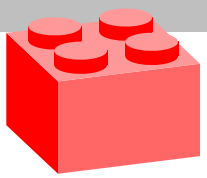
Para el caso de la suma usual de matrices se tiene que

1. **Cerradura:** sean $A, B \in Sym(n, \mathbb{R})$ con $A = A^t$ y $B = B^t$. Considere $C = A + B$. Para demostrar que C es simétrica, note que $C^t = (A+B)^t = A^t + B^t = A + B = C$. Dado que $C^t = C$, la cerradura queda mostrada.

2. **Asociatividad:** la suma de matrices siempre es asociativa, por lo que para cualesquiera $A, B, C \in Sym(n, \mathbb{R})$, se tiene $A + (B + C) = (A + B) + C$.

3. **Neutro:** La matriz nula cuadrada 0_n, donde todas sus entradas son 0, es el elemento neutro para la suma de matrices. Por definición, $0_n = 0_n^t$, lo que significa que la matriz cero es simétrica y pertenece a $Sym(n, \mathbb{R})$. En consecuencia, $A + 0_n = A$ para cualquier $A \in Sym(n, \mathbb{R})$, cumpliendo la propiedad del elemento neutro.

4. **Inverso:** Para cada $A \in Sym(n, \mathbb{R})$, la matriz $-A$ es su inverso aditivo, ya que $A + (-A) = 0$. Como A es simétrica, $(-A)^t = -A^t = -A$, mostrando que $-A$ también es simétrica y pertenece a $Sym(n, \mathbb{R})$. Esto cumple la propiedad de tener inverso para cada elemento.



Soluciones

Se concluye que para el caso de la suma usual de matrices el conjunto dado si forma un grupo. Ahora para el caso del producto de matrices se tiene que la propiedad de cerradura no es viable. En efecto, la multiplicación de dos matrices simétricas A y B no garantiza una matriz simétrica como resultado. Específicamente, $AB = (AB)^t$ solo si A y B conmutan, es decir, $AB = BA$, lo cual no es cierto en general para cualquier par de matrices simétricas.

Conclusión:

1. $Sym(n, \mathbb{R})$ **si** es un grupo bajo la suma de matrices, ya que cumple con todas las propiedades requeridas: cerradura, elemento neutro, inverso y asociatividad.

2. $Sym(n, \mathbb{R})$ **no** es un grupo bajo la multiplicación de matrices, principalmente porque no cumple con la propiedad de cerradura y porque no todas las matrices tienen inversos que también sean matrices simétricas en $Sym(n, \mathbb{R})$.

□

Ver p.71

Solución 2.3.11 (Grupo)

Se probará que $(G, *)$ es un grupo. En efecto:

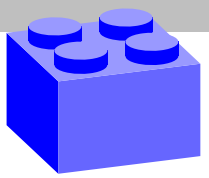
1. **Cerradura:** sean $a, b \in G$. Entonces, $a \neq -1$ y $b \neq -1$. Observe que

$$\begin{aligned} a * b &= a + b + ab \\ &= (a + ab) + b \\ &= (a(1 + b)) + b \end{aligned}$$

   Como $a \neq -1$, entonces $1+b \neq 0$. Por lo tanto, $a(1+b)$ es un número real diferente de -1. Además, b también es un número real diferente de -1. La suma de dos números reales diferentes de -1 es un número real diferente de -1. Por lo tanto, $a * b \neq -1$, lo que significa que la operación $*$ es cerrada en G.

2. **Asociatividad:** para demostrar que la operación $*$ es asociativa, se debe verificar que para cualquier $a, b, c \in G$, se cumple la siguiente igualdad:

$$(a * b) * c = a * (b * c)$$



Así, con el lado izquierdo de la ecuación se tiene

$$\begin{aligned}(a * b) * c &= (a + b + ab) * c \\ &= (a + b + ab) + c + (a + b + ab)c \\ &= a + b + ab + c + ac + bc + abc\end{aligned}$$

Ahora, desarrollando el lado derecho de la ecuación:

$$\begin{aligned}a * (b * c) &= a * (b + c + bc) \\ &= a + b + c + bc + a(b + c + bc) \\ &= a + b + c + bc + ab + ac + abc\end{aligned}$$

Observe que ambos lados de la ecuación son idénticos. Por lo tanto, la operación $*$ es asociativa.

3.**Neutro:** considere $e = 0$. Se tiene que

$$\begin{aligned}e * a &= 0 + a + 0a \\ &= a\end{aligned}$$

y

$$\begin{aligned}a * e &= a + 0 + a \cdot 0 \\ &= a\end{aligned}$$

En ambos casos, el resultado es a. Por lo tanto, $e = 0$ es el elemento neutro de $(G, *)$.

4.**Inverso:** considere $b = \dfrac{-a}{a+1}$. Se tiene que:

$$\begin{aligned}a * b &= a + \frac{-a}{a+1} + a \cdot \frac{-a}{a+1} \\ &= a + \frac{-a}{a+1}(1 + a) \\ &= a - a \\ &= 0\end{aligned}$$

y

$$\begin{aligned} b * a &= \frac{-a}{a+1} + a + \frac{-a}{a+1} \cdot a \\ &= \frac{-a}{a+1} + \frac{-a}{a+1} \cdot a + a \\ &= \frac{-a}{a+1}(1+a) + a \\ &= -a + a \\ &= 0 \end{aligned}$$

En ambos casos, se obtiene la identidad. Por lo tanto, cada $a \in G$ tiene un inverso $b = \frac{-a}{a+1}$.

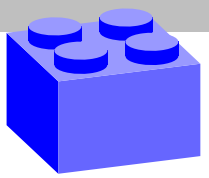
En este caso, el conjunto con la operación indicada forma un grupo.

Observe que

$$\begin{aligned} 5 * x * 2 = 8 &\Leftrightarrow 5 * x * 2 * 2^{-1} = 8 * 2^{-1} \\ &\Leftrightarrow 5 * x = 8 * \frac{-2}{2+1} \\ &\Leftrightarrow 5 * x = 8 * \frac{-2}{3} \\ &\Leftrightarrow 5 * x = 8 + \frac{-2}{3} + 8 * \frac{-2}{3} \\ &\Leftrightarrow 5 * x = 2 \\ &\Leftrightarrow 5^{-1} * 5 * x = 5^{-1} * 2 \\ &\Leftrightarrow x = \frac{-5}{5+1} * 2 \\ &\Leftrightarrow x = \frac{-5}{6} * 2 \\ &\Leftrightarrow x = \frac{-5}{6} + 2 + \frac{-5}{6} * 2 \\ &\Leftrightarrow x = -\frac{1}{2} \end{aligned}$$

□

Soluciones



Solución 2.3.12 (Grupo)

Ver p.71

Se probará que $(\overline{G}, \circ)$ es un grupo. Aquí, la operación es la composición de funciones, lo que significa que si se tiene dos funciones L_a y L_b de $\overline{G}$, su composición $L_a \circ L_b$ también debe ser un elemento de $\overline{G}$. En efecto:

1. **Cerradura:** para demostrar la cerradura, considere dos elementos arbitrarios L_a y L_b de $\overline{G}$, donde $a, b \in G$. La composición de L_a y L_b es una función $L_a \circ L_b : G \to G$ definida por $(L_a \circ L_b)(x) = L_a(L_b(x)) = L_a(bx) = a(bx)$ para todo $x \in G$. Dado que G es un grupo, se sabe que $ab \in G$, y por lo tanto, $a(bx) = (ab)x$, lo cual es simplemente la acción de L_{ab} en x. Esto muestra que $L_a \circ L_b = L_{ab}$, lo que implica que la composición de cualquier par de elementos en $\overline{G}$ resulta en otro elemento de $\overline{G}$, satisfaciendo la propiedad de cerradura.

2. **Asociatividad:** la asociatividad en $\overline{G}$ proviene directamente de la asociatividad en G. Si se tiene tres elementos L_a, L_b, y L_c en $\overline{G}$, entonces para todo $x \in G$, $(L_a \circ (L_b \circ L_c))(x) = L_a((L_b \circ L_c)(x)) = L_a(L_b(L_c(x))) = a(b(cx)) = (ab)c)x = ((L_a \circ L_b) \circ L_c)(x)$, lo que muestra que la composición de funciones en $\overline{G}$ es asociativa.

3. **Neutro:** el elemento neutro en G es un elemento e tal que $eg = ge = g$ para todo $g \in G$. La función correspondiente en $\overline{G}$ es L_e, donde $L_e(x) = ex = x$ para todo $x \in G$. Esto muestra que L_e actúa como el elemento neutro en $\overline{G}$ porque la composición de L_e con cualquier $L_g \in \overline{G}$ resulta en L_g. Es decir, $L_e \circ L_g = L_g \circ L_e = L_g$ para todo $g \in G$.

4. **Inverso:** para cada $g \in G$, existe un inverso $g^{-1} \in G$ tal que $gg^{-1} = g^{-1}g = e$, donde e es el elemento neutro en G. La función correspondiente a g^{-1} en $\overline{G}$ es $L_{g^{-1}}$, y para cualquier $x \in G$, se tiene que $L_g \circ L_{g^{-1}}(x) = L_g(L_{g^{-1}}(x)) = L_g(g^{-1}x) = (gg^{-1})x = ex = x$, y similarmente $L_{g^{-1}} \circ L_g(x) = x$. Esto significa que $L_{g^{-1}}$ es el inverso de L_g en $\overline{G}$, cumpliendo la propiedad de tener inverso para cada elemento.

En este caso, el conjunto con la operación indicada forma un grupo.

□

Solución 2.3.13 (Grupo)

Ver p.71

Se probará que $(G, \circ)$ es grupo con la composición de funciones. En efecto:

1. **Cerradura:** se debe demostrar que la composición de dos funciones en G también pertenece a G. Sean $T_{a,b}$ y $T_{c,d}$ dos funciones en G, donde $a, c \neq 0$. La composición $T_{a,b} \circ T_{c,d}$ se define como:

$$(T_{a,b} \circ T_{c,d})(x) = T_{a,b}(T_{c,d}(x)) = T_{a,b}(cx + d) = a(cx + d) + b = acx + (ad + b)$$

Dado que $ac \neq 0$ (porque tanto a como c son distintos de cero), la función compuesta $T_{ac,ad+b}$ pertenece a G, cumpliendo la propiedad de cerradura.

2. **Asociatividad:** la asociatividad para la composición de funciones siempre se mantiene. Si se tiene tres funciones en G, $T_{a,b}$, $T_{c,d}$, y $T_{e,f}$, entonces para todo $x \in \mathbb{R}$:

$$((T_{a,b} \circ T_{c,d}) \circ T_{e,f})(x) = (T_{a,b} \circ (T_{c,d} \circ T_{e,f}))(x)$$

Esto se debe a que la composición de funciones es inherentemente asociativa, cumpliendo dicha propiedad.

3. **Neutro:** el elemento neutro e en este grupo es una función tal que $e(x) = x$ para todo $x \in \mathbb{R}$. La función $T_{1,0}$ actúa como el elemento neutro, ya que $T_{1,0}(x) = 1x+0 = x$. Por lo tanto, para cualquier función $T_{a,b} \in G$, se tiene:

$$(T_{a,b} \circ T_{1,0})(x) = T_{a,b}(x) = (T_{1,0} \circ T_{a,b})(x)$$

Lo que indica que $T_{1,0}$ no cambia el efecto de cualquier otra función en G, cumpliendo la propiedad del elemento neutro.

4. **Inverso:** para cada función $T_{a,b} \in G$, se necesita encontrar otra función en G tal que su composición devuelva el elemento neutro $T_{1,0}$. La función inversa $T_{a',b'}$ debe satisfacer:

$$(T_{a,b} \circ T_{a',b'})(x) = T_{1,0}(x) = x$$

Resolviendo para a' y b', se encuentra que la composición $T_{a,b}(T_{a',b'}(x)) = ax + b$ donde $x = T_{a',b'}(x) = a'x + b'$ debe igualar x. Esto se satisface si $a' = 1/a$ y $b' = -b/a$, demostrando que cada función en G tiene un inverso en G.

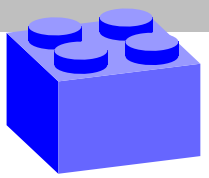
En este caso, el conjunto con la operación indicada forma un grupo.

□

Ver p.72

Solución 2.3.14 (Grupo)

Para demostrar que el conjunto K junto con la operación $*$ forma un grupo, se debe verificar que cumple con las cuatro propiedades que definen a un grupo: cerradura, asocialtivi-



dad, existencia de elemento neutro y existencia de inverso. Dado que K es un subconjunto de G_1 y G_1 es un grupo, la propiedad de asociatividad se hereda directamente para los elementos en K, así que el enfoque se hará en las otras tres propiedades.

1. **Cerradura:** se debe demostrar que si $g, h \in K$, entonces $g * h \in K$. Por definición de K, se tiene que $\varphi(g) = \overline{e}$ y $\varphi(h) = \overline{e}$. Usando la propiedad de de φ, se tiene que:

$$\varphi(g * h) = \varphi(g) \cdot \varphi(h) = \overline{e} \cdot \overline{e} = \overline{e}$$

   Esto muestra que $g * h$ también cumple con la condición para estar en K, por lo tanto, K es cerrado bajo la operación $*$.

2. **Neutro:** dado que G_1 es un grupo, existe un elemento neutro e en G_1 tal que para cualquier elemento $g \in G_1$, se tiene $g * e = e * g = g$. Para que K sea un grupo, e también debe ser el elemento neutro en K. Debido a la propiedades de φ, se cumple que:

$$\varphi(e) = \overline{e}$$

   Esto significa que $e \in K$, ya que su imagen bajo φ es el elemento neutro en G_2, cumpliendo así con la definición de K. Por lo tanto, el elemento neutro de G_1 también sirve como elemento neutro en K.

3. **Inverso:** para cualquier $g \in K$, se necesita encontrar un $g^{-1} \in K$ tal que $g * g^{-1} = g^{-1} * g = e$, donde e es el elemento neutro en G_1 (y por lo tanto en K). Se sabe que $\varphi(g) = \overline{e}$, y se quiere mostrar que $\varphi(g^{-1}) = \overline{e}$, donde g^{-1} es el inverso de g en G_1. Dado que G_1 es un grupo, se sabe que cada elemento tiene un inverso. Usando la propiedad de φ, se tiene:

$$\varphi(g) \cdot \varphi(g^{-1}) = \varphi(g * g^{-1}) = \varphi(e) = \overline{e}$$

   Pero dado que $\varphi(g) = \overline{e}$, esto implica que:

$$\overline{e} \cdot \varphi(g^{-1}) = \overline{e}$$

Por las propiedades de los grupos, esto significa que $\varphi(g^{-1}) = \overline{e}$, por lo tanto, $g^{-1} \in K$.

En este caso, el conjunto con la operación indicada forma un grupo.

Para demostrar que R junto con la operación $\cdot$ forma un grupo, se debe verificar que cumple con las cuatro propiedades fundamentales de los grupos: cerradura, asociatividad, existencia de elemento neutro, y existencia de inverso. Dado que R es un subconjunto de G_2 y G_2 es un grupo, la propiedad de asociatividad se hereda directamente para los elementos en R, así que el enfoque se hará en las otras tres propiedades

1. **Cerradura:** para demostrar la clausura, se necesita mostrar que si $h, k \in R$, entonces $h \cdot k \in R$. Por definición de R, existen $g, g' \in G_1$ tales que $\varphi(g) = h$ y $\varphi(g') = k$. Usando la propiedad de φ, se tiene que:

$$\varphi(g * g') = \varphi(g) \cdot \varphi(g') = h \cdot k$$

Dado que $g * g' \in G_1$ y $\varphi(g * g') = h \cdot k$, esto significa que $h \cdot k$ es la imagen bajo φ de algún elemento en G_1, y por lo tanto, $h \cdot k \in R$, lo que demuestra la clausura.

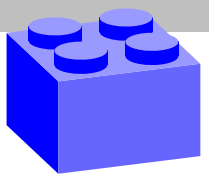
2. **Neutro:** el elemento neutro en G_2 es $\overline{e}$. Para que R sea un grupo bajo la operación $\cdot$, $\overline{e}$ debe estar en R. Debido a las propiedades de φ se tiene que:

$$\varphi(e) = \overline{e}$$

Esto significa que el elemento neutro de G_2, $\overline{e}$, es la imagen de $e \in G_1$ bajo φ, y por lo tanto, $\overline{e} \in R$.

3. **Inverso:** para demostrar que cada elemento en R tiene un inverso en R, tome cualquier $h \in R$. Por definición de R, existe un $g \in G_1$ tal que $\varphi(g) = h$. Dado que G_1 es un grupo, g tiene un inverso $g^{-1} \in G_1$ tal que $g * g^{-1} = g^{-1} * g = e$, donde e es el elemento neutro en G_1. Utilizando la propiedad de φ, se tiene que:

$$\varphi(g) \cdot \varphi(g^{-1}) = \varphi(g * g^{-1}) = \varphi(e) = \overline{e}$$



Y también:

$$\varphi(g^{-1}) \cdot \varphi(g) = \varphi(g^{-1} * g) = \varphi(e) = \overline{e}$$

Esto significa que $\varphi(g^{-1})$ es el inverso de h en G_2, y dado que $g^{-1} \in G_1$, $\varphi(g^{-1})$ es la imagen de algún elemento en G_1, lo que implica que el inverso de h, $\varphi(g^{-1})$, está en R.

En este caso, el conjunto con la operación indicada forma un grupo.

□

Solución 2.3.15 (Grupo)

Ver p.72

Para demostrar que $(\mathcal{F}(\mathbb{R}), +)$ es un grupo, se debe verificar que cumple con las cuatro propiedades que definen a un grupo: cerradura, existencia de elemento neutro, existencia de inverso y asociatividad. En efecto:

1. **Cerradura:** sea $f, g \in \mathcal{F}(\mathbb{R})$, entonces para todo $x \in \mathbb{R}$, $(f+g)(x) = f(x)+g(x)$. Ya que la suma de dos números reales es otro número real, $(f+g)(x) \in \mathbb{R}$. Por lo tanto, $f+g$ es una función de $\mathbb{R}$ en $\mathbb{R}$, lo que implica que $f+g \in \mathcal{F}(\mathbb{R})$.

2. **Asociatividad:** Sean $f, g, h \in \mathcal{F}(\mathbb{R})$. Entonces, para todo $x \in \mathbb{R}$,

$$((f+g)+h)(x) = (f+g)(x) + h(x) = (f(x)+g(x)) + h(x) =$$

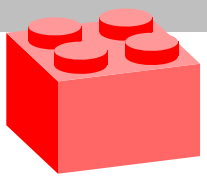
$$f(x) + (g(x)+h(x)) = (f+(g+h))(x)$$

   Esto muestra que la operación de suma es asociativa.

3. **Elemento Neutro:** el elemento neutro en este grupo es la función constante 0, denotada como $e(x) = 0$ para todo $x \in \mathbb{R}$. Para cualquier función $f \in \mathcal{F}(\mathbb{R})$, se tiene que $(f+e)(x) = f(x) + e(x) = f(x) + 0 = f(x)$ para todo $x \in \mathbb{R}$. Esto demuestra que $f + e = f$, lo que significa que e es el elemento neutro del grupo.

4. **Inverso:** para cualquier $f \in \mathcal{F}(\mathbb{R})$, se define $g(x) = -f(x)$ para todo $x \in \mathbb{R}$. Entonces $(f+g)(x) = f(x) + g(x) = f(x) - f(x) = 0$, lo que es igual a $e(x)$ para todo x. Por lo tanto, g es el inverso de f, y $g \in \mathcal{F}(\mathbb{R})$.

En este caso, el conjunto con la operación indicada forma un grupo.



Soluciones

Para mostrar que $(\mathcal{F}(\mathbb{R}), \cdot)$ no forma un grupo, basta con encontrar un caso en el que no se cumpla alguna de las propiedades necesarias para ser un grupo. Las propiedades necesarias para ser un grupo son: cerradura, asociatividad, elemento neutro y elemento inverso. Aunque la operación de multiplicación es cerrada y asociativa en $\mathcal{F}(\mathbb{R})$, y existe un elemento neutro $e(x) = 1$ para todo $x \in \mathbb{R}$ (ya que $f(x) \cdot 1 = f(x)$ para toda función f), el problema surge al considerar la existencia de elementos inversos para todas las funciones en $\mathcal{F}(\mathbb{R})$. En efecto, considere la función constante $f(x) = 0$ para todo $x \in \mathbb{R}$. Esta función pertenece a $\mathcal{F}(\mathbb{R})$. Para que $(\mathcal{F}(\mathbb{R}), \cdot)$ sea un grupo, debe existir un inverso multiplicativo $g \in \mathcal{F}(\mathbb{R})$ tal que $f(x) \cdot g(x) = 1$ para todo $x \in \mathbb{R}$. Sin embargo, no existe tal función g porque para todo x,

$$0 \cdot g(x) = 0 \neq 1.$$

Esta contradicción muestra que no todas las funciones en $\mathcal{F}(\mathbb{R})$ tienen un inverso multiplicativo, lo cual es necesario para la definición de un grupo. Por lo tanto, $(\mathcal{F}(\mathbb{R}), \cdot)$ **no es un grupo debido a la violación de la propiedad del elemento inverso.**

Para demostrar que $(C^0(\mathbb{R}), +)$ es un grupo, se debe verificar que cumple con las cuatro propiedades fundamentales de los grupos con respecto a la operación de suma: cerradura, asociatividad, elemento neutro e inverso. En efecto:

1. **Cerradura:** sean $f, g \in C^0(\mathbb{R})$, lo que significa que f y g son continuas. La suma de dos funciones continuas, $f + g$, definida por $(f + g)(x) = f(x) + g(x)$ para todo $x \in \mathbb{R}$, es también una función continua. Esto se debe a que la suma de funciones continuas es continua. Por lo tanto, $f + g \in C^0(\mathbb{R})$.

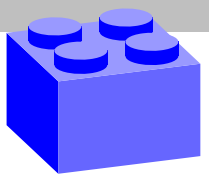
2. **Asociatividad:** la asociatividad de la suma en $(C^0(\mathbb{R}), +)$ se deriva directamente de la asociatividad de la suma en $\mathbb{R}$. Sean $f, g, h \in C^0(\mathbb{R})$. Entonces, para todo $x \in \mathbb{R}$,

$$((f + g) + h)(x) = (f + g)(x) + h(x) = (f(x) + g(x)) + h(x) =$$

$$f(x) + (g(x) + h(x)) = (f + (g + h))(x)$$

   Esto muestra que la operación de suma es asociativa para funciones en $C^0(\mathbb{R})$.

3. **Neutro:** el elemento neutro en este grupo es la función constante 0, denotada como



$e(x) = 0$ para todo $x \in \mathbb{R}$. Esta función es claramente continua. Para cualquier función $f \in C^0(\mathbb{R})$, se tiene que $(f + e)(x) = f(x) + e(x) = f(x) + 0 = f(x)$ para todo x. Esto demuestra que $f + e = f$, confirmando que e es el elemento neutro del grupo.

4. **Inverso:** para cualquier $f \in C^0(\mathbb{R})$, se define $g(x) = -f(x)$ para todo $x \in \mathbb{R}$. La función g es continua, ya que la negación de una función continua es continua. Entonces, $(f + g)(x) = f(x) + g(x) = f(x) - f(x) = 0$, lo que es igual a $e(x)$ para todo x. Esto demuestra que g es el inverso de f, y $g \in C^0(\mathbb{R})$.

En este caso, el conjunto con la operación indicada forma un grupo.

Para demostrar que $(F^I(\mathbb{R}), +)$ es un grupo, se necesita verificar que cumple con las cuatro propiedades fundamentales de los grupos con respecto a la operación de suma: cerradura, asociatividad, neutro e inverso. En efecto:

1. **Cerradura:** sean $f, g \in F^I(\mathbb{R})$, lo que significa que $f(-x) = -f(x)$ y $g(-x) = -g(x)$ para todo $x \in \mathbb{R}$. Considere la suma $f + g$ y evaluando en $-x$:

$$(f + g)(-x) = f(-x) + g(-x) = -f(x) - g(x) = -(f(x) + g(x)) = -(f + g)(x).$$

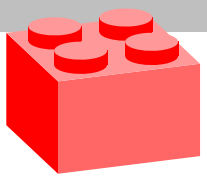
Esto muestra que $f + g \in F^I(\mathbb{R})$, cumpliendo la propiedad de cerradura.

2. **Asociatividad:** la asociatividad de la suma en $F^I(\mathbb{R})$ se deriva directamente de la asociatividad de la suma en $\mathbb{R}$.

3. **Neutro:** el elemento neutro es la función $e(x) = 0$ para todo $x \in \mathbb{R}$. Es fácil verificar que e pertenece a $F^I(\mathbb{R})$ porque $e(-x) = 0 = -0 = -e(x)$. Para cualquier función $f \in F^I(\mathbb{R})$, se tiene que $f + e = f$, satisfaciendo la propiedad del elemento neutro.

4. **Inverso:** Para cada $f \in F^I(\mathbb{R})$, se define $g(x) = -f(x)$. Es claro que $g \in F^I(\mathbb{R})$ porque $g(-x) = -f(-x) = -(-f(x)) = f(x)$. Además, $f + g = 0 = e$, lo que muestra que cada elemento tiene un inverso aditivo en $F^I(\mathbb{R})$.

En este caso, el conjunto con la operación indicada forma un grupo.



Soluciones

Para demostrar que $(F^+(\mathbb{R}), \cdot)$ es un grupo y que $(F^+(\mathbb{R}), +)$ no es un grupo, se debe analizar cada estructura con respecto a las propiedades de un grupo: cerradura, elemento neutro, elemento inverso y asociatividad.

$(F^+(\mathbb{R}), \cdot)$ **como grupo** Observe que se cumplen todas las propiedades respectivas. A saber:

1. **Cerradura:** para cualquier $f, g \in F^+(\mathbb{R})$, donde $f(x) > 0$ y $g(x) > 0$ para todo $x \in \mathbb{R}$, el producto $f \cdot g$, definido como $(f \cdot g)(x) = f(x)g(x)$, también es mayor que cero para todo $x \in \mathbb{R}$. Esto se debe a que el producto de dos números positivos es positivo. Por lo tanto, $f \cdot g \in F^+(\mathbb{R})$.

2. **Asociatividad:** la multiplicación de funciones reales es asociativa. Por lo tanto, para cualquier $f, g, h \in F^+(\mathbb{R})$, se tiene que $(f \cdot g) \cdot h = f \cdot (g \cdot h)$.

3. **Neutro:** el elemento neutro en esta operación es la función constante $e(x) = 1$ para todo $x \in \mathbb{R}$, ya que $1 > 0$ y $f(x) \cdot 1 = f(x)$ para cualquier función $f \in F^+(\mathbb{R})$.

4. **Inverso:** para cada $f \in F^+(\mathbb{R})$, existe un inverso $g \in F^+(\mathbb{R})$ tal que $f(x)g(x) = 1$, definido por $g(x) = \frac{1}{f(x)}$. Dado que $f(x) > 0$, $g(x) > 0$ también, lo que implica que $g \in F^+(\mathbb{R})$.

Estas propiedades demuestran que $(F^+(\mathbb{R}), \cdot)$ **es un grupo.**

$(F^+(\mathbb{R}), +)$ **no es grupo**

Para demostrar que $(F^+(\mathbb{R}), +)$ no es un grupo, basta con encontrar una propiedad de los grupos que no se cumpla.

Cerradura: aunque para cualquier $f, g \in F^+(\mathbb{R})$, la suma $f + g$, definida como $(f + g)(x) = f(x) + g(x)$, también resulta en una función donde $f(x) + g(x) > 0$ para todo $x \in \mathbb{R}$, lo cual satisface la propiedad de cerradura, el problema surge con el elemento inverso.

Elemento inverso: para que $F^+(\mathbb{R}), +)$ sea un grupo, cada elemento $f \in F^+(\mathbb{R})$ debe tener un inverso aditivo $g \in F^+(\mathbb{R})$ tal que $f(x) + g(x) = e$, donde e es el elemento neutro. Sin embargo, el elemento neutro para la adición sería una función $e(x) = 0$ para

todo $x \in \mathbb{R}$, pero este $e(x)$ no pertenece a $F^+(\mathbb{R})$ ya que no es estrictamente mayor que cero. Además, no existe una función $g \in F^+(\mathbb{R})$ tal que la suma de g y cualquier función positiva f resulte en cero o en otra función positiva constante, ya que $f(x) > 0$ y $g(x)$ debería ser negativa para restar $f(x)$ a cero, lo cual contradice la definición de $F^+(\mathbb{R})$.

Por lo tanto, $(F^+(\mathbb{R}), +)$ no satisface la propiedad de tener un elemento inverso para cada elemento en el conjunto, **lo que significa que no es un grupo.**

□

Solución 2.3.16 (Grupo)

Ver p.73

Después de realizar las operaciones de multiplicación de matrices, se obtienen los siguientes resultados:

- Para $\mathbf{i}^2, \mathbf{j}^2, \mathbf{k}^2$, todos resultan en $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, lo que demuestra que $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$.
- Para $\mathbf{ij}$, se obtiene $\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$, que es precisamente $\mathbf{k}$, y para $\mathbf{ji}$, se obtiene $\begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$, que es $-\mathbf{k}$. Esto confirma que $\mathbf{ij} = -\mathbf{ji} = \mathbf{k}$.
- Para $\mathbf{jk}$, se obtiene $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, que es $\mathbf{i}$, y para $\mathbf{kj}$, se obtiene $\begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$, que es $-\mathbf{i}$. Esto verifica que $\mathbf{jk} = -\mathbf{kj} = \mathbf{i}$.
- Finalmente, para $\mathbf{ki}$, se obtiene $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, que es $\mathbf{j}$, y para $\mathbf{ik}$, el resultado es $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, que es $-\mathbf{j}$. Esto muestra que $\mathbf{ki} = -\mathbf{ik} = \mathbf{j}$.

Estos resultados demuestran las propiedades especificadas del grupo de cuaterniones, utilizando la multiplicación de matrices para $\mathbf{i}, \mathbf{j}, \mathbf{k}$ y sus combinaciones.

Para demostrar que el conjunto $Q_8 := \{-\mathbf{1}, -\mathbf{i}, -\mathbf{j}, -\mathbf{k}, \mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ forma un grupo con la operación de multiplicación de matrices, se debe verificar las siguientes propiedades de un grupo: cerradura, asociatividad, elemento neutro y elemento inverso. En efecto:

1. **Cerradura:** basado en la demostración anterior, donde se probó que $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$, $\mathbf{ij} = -\mathbf{ji} = \mathbf{k}$, $\mathbf{jk} = -\mathbf{kj} = \mathbf{i}$, y $\mathbf{ki} = -\mathbf{ik} = \mathbf{j}$, es fácil verificar que multiplicar cualquiera de los elementos de Q_8 por otro elemento de Q_8 resulta en otro elemento dentro de Q_8. Por ejemplo, $-\mathbf{i} \cdot -\mathbf{i} = \mathbf{i}^2 = -1$, que es equivalente a $-\mathbf{1}$, que está en Q_8.

2. **Asociatividad:** la asociatividad se cumple debido a la naturaleza de la multiplicación de matrices, que es asociativa. Por lo tanto, no se necesita verificar cada posible combinación de elementos en Q_8 para demostrar esta propiedad.

3. **Neutro:** El elemento $\mathbf{1}$ actúa como el elemento neutro, ya que la multiplicación de cualquier elemento de Q_8 por $\mathbf{1}$ da como resultado el mismo elemento, por ejemplo, $\mathbf{i} \cdot \mathbf{1} = \mathbf{i}$ y $-\mathbf{i} \cdot \mathbf{1} = -\mathbf{i}$.

4. **Inverso:** cada elemento en Q_8 tiene un inverso dentro del conjunto. Por ejemplo, el inverso de $\mathbf{i}$ es $-\mathbf{i}$ ya que $\mathbf{i} \cdot -\mathbf{i} = -1 = -\mathbf{1}$, y el inverso de $\mathbf{j}$ es $-\mathbf{j}$, y así sucesivamente para los demás elementos.

Dado que Q_8 cumple con todas las propiedades requeridas para ser un grupo bajo la operación de multiplicación de matrices, **se concluye que Q_8 es efectivamente un grupo.** Este grupo es conocido como el grupo de cuaterniones, que juega un papel importante en la Matemática y la Física, especialmente en el estudio de rotaciones en el espacio tridimensional.

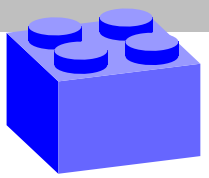
□

Ver p.73

Solución 2.3.17 (Grupo)

Recuerde que:

- $\mathbb{Z}_5$ es el conjunto de clases de equivalencia de los enteros módulo 5, con la operación de suma: $\{0, 1, 2, 3, 4\}$.
- $\mathbb{Z}_5^*$ es el conjunto de elementos invertibles en $\mathbb{Z}_5$ bajo la multiplicación, es decir, elementos con inverso multiplicativo: $\{1, 2, 3, 4\}$.
- U_5 generalmente se refiere al grupo de unidades de $\mathbb{Z}_5$. No obstante como la cantidad se refiere a un número primor sucede que $U_5, \cdot$ coincide con $\mathbb{Z}_5\ *, \cdot$.
- $\mathbb{Z}_6$ es el conjunto de clases de equivalencia de los enteros módulo 6, con la operación de suma: $\{0, 1, 2, 3, 4, 5\}$.



De esta forma:

- **Tabla de grupo para** $(\mathbb{Z}_5, +)$

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

- **Tabla de grupo para** $(\mathbb{Z}_5^*, \cdot)$

$\cdot$	1	2	3	4
1	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

- **Tabla de grupo para** $(\mathbb{Z}_6, +)$

$*$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

□

Solución 2.3.18 (Grupo) Ver p.73

Dado que $xz = yz$, se desea manipular esta ecuación para çancelar"z de ambos lados. Para hacerlo, se utiliza la existencia del inverso de z, denotado como z^{-1}.

De esta manera, se multiplica ambos lados de la ecuación $xz = yz$ por z^{-1} a la derecha. Debido a la asociatividad, podemos reorganizar los paréntesis sin cambiar el resultado. Esto es:

$$(xz)z^{-1} = (yz)z^{-1}$$

Aplicando la asociatividad:

$$x(zz^{-1}) = y(zz^{-1})$$

Ahora, se sabe que $zz^{-1} = e$, donde e es el elemento identidad en G. Entonces, reemplazando:

$$xe = ye$$

Y, dado que el elemento de identidad e tiene la propiedad de que $ae = ea = a$ para todo $a \in G$, se tiene:

$$x = y$$

Esto completa la demostración.

□

Ver p.73

Solución 2.3.19 (Grupo)

Dadas las condiciones:

1. $a^5 = e$,
2. $b^4 = e$,
3. $ab = ba^3$,

Se quiere demostrar

1. $a^2b = ba$,
2. $ab^3 = b^3a^2$,

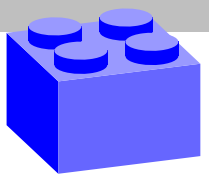
Demostración de $a^2b = ba$

Se comienza multiplicando la ecuación $ab = ba^3$ por a a la izquierda:

$$\begin{aligned} a(ab) &= a(ba^3) \\ a^2b &= (ab)a^3 \quad \text{(por asociatividad y definición)} \\ a^2b &= (ba^3)a^3 \quad \text{(condición dada } ab = ba^3\text{)} \\ a^2b &= ba^6 \quad \text{(definición)} \end{aligned}$$

Como $a^5 = e$, entonces $aa^5 = a^6 = ae = a$ lo que simplifica la expresión a:

$$a^2b = ba \quad \text{(definición y condición dada)}$$



Esto demuestra lo primero.

Demostración de $ab^3 = b^3a^2$

Con base en el resultado anterior, se multiplica la ecuación $a^2b = ba$ por b^3 a la izquierda:

$$b^3(a^2b) = b^3(ba)$$
$$(b^3a^2)b = b^4a \quad \text{(definición y asociatividad)}$$

Como $b^4 = e$ se tiene que:

$$(b^3a^2)b = ea \quad \text{(definición y condición dada)}$$
$$(b^3a^2)b = a \quad \text{(definición de neutro } ae = ea = a\text{)}$$

Ahora, se multiplicamos la ecuación $(b^3a^2)b = a$ por b^3 a la izquierda:

$$\begin{aligned}((b^3a^2)b)b^3 &= ab^3 \\ (b^3a^2)b^4 &= ab^3 \quad \text{(definición)} \\ (b^3a^2)e &= ab^3 \quad \text{(condición dada)} \\ b^3a^2 &= ab^3 \quad \text{(definición de neutro } ae = ea = a\text{)}\end{aligned}$$

Se demuestra que $a^2b = ba$ y $ab^3 = b^3a^2$.

Observación: La ecuación $ab = ba^3$ se conoce como ecuación de Schreier. Esta ecuación se utiliza en la teoría de grupos para estudiar la estructura de los grupos.

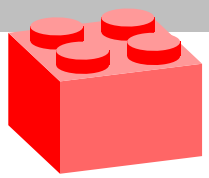
□

Solución 2.3.20 (Grupo)

Ver p.73

La demostración se divide en dos partes: la implicación directa ($a \cdot b = c \cdot b \Rightarrow a = c$) y la implicación inversa ($a = c \Rightarrow a \cdot b = c \cdot b$).

Implicación directa ($a \cdot b = c \cdot b \Rightarrow a = c$)



Soluciones

Hipótesis: Suponga que $a \cdot b = c \cdot b$.

Prueba: Dado que G es un grupo, para cualquier elemento $b \in G$, existe un inverso $b^{-1} \in G$ tal que $b \cdot b^{-1} = b^{-1} \cdot b = e$, donde e es el elemento identidad de G. Con base en esto, se multiplica ambos lados de la ecuación $a \cdot b = c \cdot b$ por b^{-1} a la derecha. El resultado es $(a \cdot b) \cdot b^{-1} = (c \cdot b) \cdot b^{-1}$. Usando la propiedad asociativa para reorganizar los paréntesis sin cambiar el resultado se obtiene $a \cdot (b \cdot b^{-1}) = c \cdot (b \cdot b^{-1})$. Como $b \cdot b^{-1} = e$, la ecuación se simplifica a $a \cdot e = c \cdot e$. Por último, dado que el elemento identidad e tiene la propiedad de que $x \cdot e = x$ para cualquier $x \in G$, se concluye que $a = c$.

Implicación inversa: $(a = c \Rightarrow a \cdot b = c \cdot b)$

Hipótesis: Suponga que $a = c$.

Prueba: Dado que $a = c$, se multiplica ambos lados de esta ecuación por b a la derecha. Esto da como respuesta $a \cdot b = c \cdot b$.

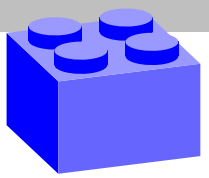
Por tanto, se ha demostrado que en un grupo G, $a \cdot b = c \cdot b$ si y solo si $a = c$.

La demostración se divide en dos partes: la implicación directa $(b \cdot a = b \cdot c \Rightarrow a = c)$ y la implicación inversa $(a = c \Rightarrow b \cdot a = b \cdot c)$.

Implicación directa $(b \cdot a = b \cdot c \Rightarrow a = c)$

Hipótesis: Suponga que $b \cdot a = b \cdot c$.

Prueba: Dado que G es un grupo, para cualquier elemento $b \in G$, existe un inverso $b^{-1} \in G$ tal que $b \cdot b^{-1} = b^{-1} \cdot b = e$, donde e es el elemento identidad de G. Con base en esto, se multiplica ambos lados de la ecuación $b \cdot a = b \cdot c$ por b^{-1} a la izquierda. El resultado es $b^{-1} \cdot (b \cdot a) = b^{-1} \cdot (b \cdot c)$. Usando la propiedad asociativa para reorganizar los paréntesis sin cambiar el resultado se obtiene $(b^{-1} \cdot b) \cdot a = (b^{-1} \cdot b) \cdot c$. Como $b^{-1} \cdot b = e$, la ecuación se simplifica a $e \cdot a = e \cdot c$. Por último, dado que el elemento identidad e tiene la propiedad de que $e \cdot x = x$ para cualquier $x \in G$, se concluye que $a = c$.



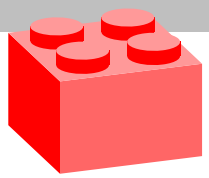
Implicación inversa: $(a = c \Rightarrow b \cdot a = b \cdot c)$

Hipótesis: Suponga que $a = c$.

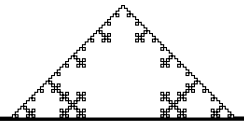
Prueba: Dado que $a = c$, se multiplica ambos lados de esta ecuación por b a la izquierda. Esto da como respuesta $b \cdot a = b \cdot c$.

Por tanto, se ha demostrado que en un grupo G, $b \cdot a = b \cdot c$ si y solo si $a = c$.

□



Soluciones



Soluciones de la sección 2.8

Ver p.101

Solución 2.8.1 (Grupo Abeliano)

Para demostrar que el conjunto de matrices ($M(m,n,\mathbb{R})$ con la operación de suma es un grupo abeliano, se debe verificar cinco propiedades: cerradura, asociatividad, existencia del elemento neutro, existencia del inverso y la conmutatividad.

1. **Cerradura:** dado que se está considerando la suma de matrices en $M(m,n,\mathbb{R})$, la suma de dos matrices en este conjunto también es una matriz en $M(m,n,\mathbb{R})$. Por lo tanto, la propiedad de cerradura se cumple.

2. **Asociatividad:** la suma de matrices es asociativa, es decir, para cualesquiera matrices A, B, C en $M(m,n,\mathbb{R})$, se cumple $(A+B)+C = A+(B+C)$.

3. **Neutro:** la matriz nula $O_{m\times n}$ sirve como el elemento neutro para la suma en $M(m,n,\mathbb{R})$. Para cualquier matriz A en $M(m,n,\mathbb{R})$, se cumple $A + O_{m\times n} = A$.

4. **Inverso:** Cada matriz A en $M(m,n,\mathbb{R})$ tiene un inverso aditivo, que es la matriz opuesta $-A$. Esto se cumple ya que $A + (-A) = O_{m\times n}$.

5. **Conmutatividad:** la operación es abeliana porque la suma de matrices es conmutativa, es decir, $A + B = B + A$ para cualquier par de matrices A, B en $M(m,n,\mathbb{R})$.

□

Ver p.101

Solución 2.8.2 (Grupo Abeliano)

Para demostrar que el conjunto G con la operación de composición de funciones es un grupo abeliano, se debe verificar cinco propiedades: cerradura, asociatividad, existencia del elemento neutro, existencia del inverso y la conmutatividad.

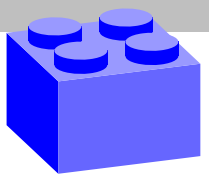
1. **Cerradura:** considere $y_1(x) = a_1x + b_1$ y $y_2(x) = a_2x + b_2$ con $a_1, a_2 > 0$, entonces

$$(y_1 \circ y_2)(x) = y_1(y_2(x)) = y_1(a_2x + b_2) = a_1(a_2x + b_2) + b_1 = a_1a_2x + (a_1b_2 + b_1).$$

   Como $a_1a_2 > 0$, se sigue que $y_1 \circ y_2 \in G$.

2. **Asociatividad:** la composición de funciones es naturalmente asociativa. Es decir, para cualquier $y_1, y_2, y_3 \in G$,

$$(y_1 \circ y_2) \circ y_3 = y_1 \circ (y_2 \circ y_3).$$



3.**Neutro:** el elemento neutro en este grupo es la función $e(x) = x$, que corresponde a tomar $a = 1$ y $b = 0$. Comprobar que $e(x) = x$ actúa como neutro es directo:

$$(y \circ e)(x) = y(x) \quad \text{y} \quad (e \circ y)(x) = y(x).$$

4.**Inverso:** si $y(x) = ax + b$, su inverso $y^{-1}(x)$ debe satisfacer $(y \circ y^{-1})(x) = x$. Resolviendo $ax + b = y$ para x, se obtiene que $x = \dfrac{y - b}{a}$ y considerando que $x = y^{-1}(x)$ se tiene que

$$y^{-1}(x) = \frac{x - b}{a}.$$

Se verifica que $y^{-1} \in G$ porque $\dfrac{1}{a} > 0$.

5.**Conmutatividad:** para que G sea Abeliano, debe cumplirse que $y_1 \circ y_2 = y_2 \circ y_1$ para todo $y_1, y_2 \in G$. Tome $y_1(x) = a_1 x + b_1$ y $y_2(x) = a_2 x + b_2$:

$$(y_1 \circ y_2)(x) = a_1(a_2 x + b_2) + b_1 = a_1 a_2 x + (a_1 b_2 + b_1),$$

$$(y_2 \circ y_1)(x) = a_2(a_1 x + b_1) + b_2 = a_1 a_2 x + (a_2 b_1 + b_2).$$

Observe que $(y_1 \circ y_2)(x) = (y_2 \circ y_1)(x)$ si y solo si $a_1 b_2 + b_1 = a_2 b_1 + b_2$. En general, esto no es cierto para todos los valores de a_1, a_2, b_1, b_2 en los reales. Por lo tanto, G **no es Abeliano**. En resumen, G es un grupo bajo la composición de funciones, pero no es un grupo Abeliano.

□

Solución 2.8.3 (Grupo Abeliano)

Ver p.101

Para demostrar que el conjunto $(\mathbb{Q}^+, *)$ es un grupo Abeliano, se necesita verificar primero que es grupo bajo la operación definida $p * q = \frac{pq}{2}$ y luego mostrar que esta operación es conmutativa:

1.**Cerradura:** si $p, q \in \mathbb{Q}^+$ y ambos son positivos, entonces pq también es positivo. Por lo tanto, $\frac{pq}{2}$ también es positivo y pertenece a $\mathbb{Q}^+$.

2.**Asociatividad:** para $p, q, r \in \mathbb{Q}^+$, se tiene:

$$(p * q) * r = \left(\frac{pq}{2}\right) * r = \frac{\left(\frac{pq}{2}\right) r}{2} = \frac{pqr}{4}$$

y

$$p * (q * r) = p * \left(\frac{qr}{2}\right) = \frac{p\left(\frac{qr}{2}\right)}{2} = \frac{pqr}{4}$$

Esto demuestra que $(p * q) * r = p * (q * r)$.

3. **Neutro:** el elemento neutro e debe cumplir $e * p = p * e = p$. Esto implica:

$$\frac{ep}{2} = p \Rightarrow ep = 2p \Rightarrow e = 2$$

Por lo tanto, el elemento neutro es 2 que pertenece a los números racionales positivos.

4. **Inverso:** el inverso de p, denotado p^{-1}, debe satisfacer $p * p^{-1} = 2$. Esto implica:

$$\frac{pp^{-1}}{2} = 2 \Rightarrow pp^{-1} = 4 \Rightarrow p^{-1} = \frac{4}{p}$$

Dado que $p \in \mathbb{Q}^+$ y $p > 0$, $p^{-1} = \frac{4}{p}$ también es positivo y pertenece a $\mathbb{Q}^+$.

5. **Conmutatividad:** la operación es conmutativa porque:

$$p * q = \frac{pq}{2} = \frac{qp}{2} = q * p$$

para todo $p, q \in \mathbb{Q}^+$.

Dado que $(\mathbb{Q}^+, *)$ cumple todas las propiedades de un grupo y la operación $*$ es conmutativa, se puede concluir que $(\mathbb{Q}^+, *)$ es un grupo Abeliano. □

Ver p.101

Solución 2.8.4 (Grupo Abeliano)

"($\Leftarrow$)"**Si G es Abeliano, entonces** $(ab)^2 = a^2b^2$

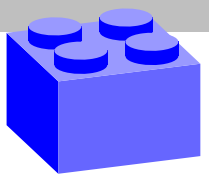
Suponga que G es un grupo Abeliano. Esto implica que para todos $a, b \in G$, $ab = ba$. Ahora

$$(ab)^2 = ab \cdot ab = abab$$

Dado que el grupo es Abeliano, se pueden reorganizar los términos ab y ba libremente, por lo tanto:

$$abab = aabb = a^2b^2$$

Esto demuestra que si el grupo G es Abeliano, entonces $(ab)^2 = a^2b^2$.



("⇒") **Si** $(ab)^2 = a^2b^2$ **para todo** $a, b \in G$**, entonces** G **es Abeliano**

Suponga que para cualesquiera $a, b \in G$, se cumple que $(ab)^2 = a^2b^2$. Se desea demostrar que $ab = ba$, lo que haría a G un grupo Abeliano.

Dado que $(ab)^2 = a^2b^2$, se tiene:

$$abab = aabb$$

Ahora, usando la propiedad de cancelación en grupos (la cual es válida porque todo grupo tiene inversos multiplicativos), se puede operar la igualdad anterior por los inversos respectivos tanto por en la izquerda de la igualdad como por la derecha, obteniendo que $ba = ab$.

Conclusión

Por lo tanto, G es un grupo Abeliano si y solo si $(ab)^2 = a^2b^2$ para todos a, b en G.

□

Solución 2.8.5 (Grupo Abeliano) Ver p.101

Para probar que el grupo G es abeliano, tome dos elementos arbitrarios $a, b \in G$ y se tiene que mostrar que $ab = ba$.

Dado que $a^2 = e$ y $b^2 = e$, se puede escribir que $a^2b^2 = e$. Además, usando la misma hipótesis, y como $ab \in G$, entonces $(ab)^2 = e$. Con ello se deduce que

$$a^2b^2 = (ab)^2,$$

luego use el ejercicio anterior y se concluye que G es Abeliano.

Observación: Este ejercicio se usará más adelante para el ejemplo 2.12.

□

Solución 2.8.6 (Grupo Abeliano) Ver p.102

Considere un grupo $(G, \cdot)$ con $|G| = 3$. Como G tiene exactamente tres elementos, denote a estos por por e (el elemento neutro), a, y b.

$\cdot$	e	a	b
e	e	a	b
a	a	a^2	ab
b	b	ba	b^2

Analizando la tabla, los productos posibles son:

1. a^2 y b^2 son los inversos de a y b respectivamente, porque $a^3 = e$ y $b^3 = e$.

2. Si ab o ba fuesen igual a e, a, o b, por las propiedades del grupo y la necesidad de que los productos estén cerrados dentro de G, se debe tener $ab = ba$.

Luego, la conmutatividad se sigue de la restricción de que cualquier producto como ab o ba debe resultar en un elemento del grupo, y dado que los elementos son limitados y el grupo está cerrado bajo la operación, se tiene:

$$ab = ba$$

Lo que implica que G es Abeliano.

Observación: La Tabla de Cayley es una herramienta utilizada en teoría de grupos para visualizar la estructura de operaciones de un grupo. Es esencialmente una tabla que representa la operación de grupo y muestra cómo los elementos del grupo interactúan entre sí bajo esta operación. La tabla toma su nombre del matemático británico Arthur Cayley, quien fue uno de los primeros en desarrollar este concepto en el siglo XIX.

□

Ver p.102

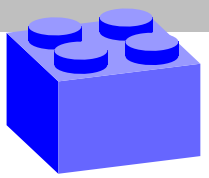
Solución 2.8.7 (Subgrupo)

Para probar que $hS = S$ para cualquier $h \in S$, donde S es un subgrupo de un grupo, se siguen los siguientes pasos:

1. $hS \subseteq S$**:** Sea $h \in S$ y $s \in S$. Entonces $hs \in S$ porque S es un subgrupo, y por definición de subgrupo, el producto de dos elementos de S debe también estar en S. Por lo tanto, cada elemento de hS está en S.

2. $S \subseteq hS$**:** De nuevo, sea $h \in S$ y considere cualquier $s \in S$. Como S es un subgrupo, el inverso de h, denotado h^{-1}, también está en S. Entonces para cualquier $s \in S$, podemos escribir s como $hh^{-1}s$. Observe que $h^{-1}s \in S$ porque ambos h^{-1} y s están en S y S es cerrado bajo la operación del grupo. Por lo tanto, $s = h(h^{-1}s)$ está en hS. Esto muestra que cada elemento de S está en hS.

Habiendo demostrado que $hS \subseteq S$ y $S \subseteq hS$, se concluye que $hS = S$.



Por otro lado, para probar que $S = Sh$ para cualquier $h \in S$, donde S es un subgrupo de un grupo, se siguen pasos similares a los anteriores:

1. $Sh \subseteq S$: Siguiendo un razonamiento similar, para cualquier $s \in S$ y $h \in S$, el producto sh está en S debido a que S es un subgrupo. Así, cada elemento de Sh está en S.

2. $S \subseteq Sh$**:** Nuevamente, como $h^{-1} \in S$, para cualquier $s \in S$, el elemento $s = sh^{-1}h$ puede ser reescrito como $(sh^{-1})h$. Aquí, $sh \in S$ porque s y h están en S y S es cerrado bajo la operación. Entonces, $s \in Sh$. Esto muestra que cada elemento de S también está en Sh.

Con esto, $Sh \subseteq S$ y $S \subseteq Sh$, se concluye que $Sh = S$.

Sea S es un subgrupo de un grupo, para mostrar que $x^{-1}y \in S$ si y solo si $xS = Sy$, se deben probar dos implicaciones:

Parte 1: ($\Rightarrow$) **Si** $x^{-1}y \in S$**, entonces** $xS = Sy$
Suponga que $x^{-1}y \in S$. Se quiere mostrar que $xS = Sy$:

En efecto, como $x^{-1}y \in S$, entonces existe un $t \in S$ tal que $x^{-1}y = t$. Multiplicando ambos lados de esta igualdad por x, se tiene que $y = xt$. Ahora, tome cualquier elemento de Sy, por ejemplo sy, donde $s \in S$.Entonces:

$$sy = (xt)s = x(ts) = xs' \quad \text{donde } s' = ts \in S.$$

Esto muestra que $sy = x(s')$ donde $s' \in S$. Como existe una igualdad, se concluye que $xS = Sy$.

Parte 2: ($\Leftarrow$) **Si** $xS = Sy$**, entonces** $x^{-1}y \in S$

Ahora suponga que $xS = Sy$. Se quiere demostrar que $x^{-1}y \in S$:

Dado que $xS = Sy$, cualquier elemento de Sy está en xS. En particular, el elemento $y \in Sy$ (tomando $s = e$ donde e es el elemento neutro en S y $y = ey$). Entonces,

como $y \in xS$, existe un $s \in S$ tal que $y = xs$.

Multiplicando ambos lados de esta igualdad por x^{-1} desde la izquierda, se obtiene:

$$x^{-1}y = s.$$

Como $s \in S$, se tiene que $x^{-1}y \in S$.

Esto completa la prueba de que $x^{-1}y \in S \iff xS = Sy$.

□

Ver p.102

Solución 2.8.8 (Grupo y subgrupo)

Para mostrar que $\mathbb{Z} \times \mathbb{Z}$ es un grupo bajo la operación $(a, b) + (c, d) = (a + c, b + d)$, se verifica que cumple las cuatro propiedades fundamentales de un grupo:

1. **Cerradura:** sean $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ y $(c, d) \in \mathbb{Z} \times \mathbb{Z}$. Entonces,

$$(a, b) + (c, d) = (a + c, b + d).$$

Puesto que $a + c \in \mathbb{Z}$ y $b + d \in \mathbb{Z}$ (porque $\mathbb{Z}$ es cerrado bajo la suma), se sigue que $(a + c, b + d) \in \mathbb{Z} \times \mathbb{Z}$. Por lo tanto, $\mathbb{Z} \times \mathbb{Z}$ es cerrado bajo la suma.

2. **Asociatividad:** Se debe verificar que para todos $(a, b), (c, d), (e, f) \in \mathbb{Z} \times \mathbb{Z}$,

$$((a, b) + (c, d)) + (e, f) = (a, b) + ((c, d) + (e, f)).$$

Calculando ambos lados:

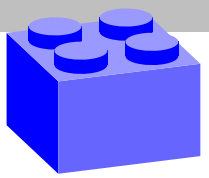
$$((a, b) + (c, d)) + (e, f) = (a + c, b + d) + (e, f) = ((a + c) + e, (b + d) + f)$$

$$= (a + c + e, b + d + f),$$

$$(a, b) + ((c, d) + (e, f)) = (a, b) + (c + e, d + f) = (a + (c + e), b + (d + f))$$

$$= (a + c + e, b + d + f).$$

Dado que ambas expresiones son iguales, se cumple la propiedad asociativa.



3. **Neutro:** se debe encontrar un elemento neutro $e \in \mathbb{Z} \times \mathbb{Z}$ tal que para cualquier $(a, b) \in \mathbb{Z} \times \mathbb{Z}$,

$$(a, b) + e = (a, b).$$

Considere $e = (0, 0)$. Entonces,

$$(a, b) + (0, 0) = (a + 0, b + 0) = (a, b).$$

Por lo tanto, $(0, 0)$ es el elemento neutro en $\mathbb{Z} \times \mathbb{Z}$.

4. **Inverso:** para cada $(a, b) \in \mathbb{Z} \times \mathbb{Z}$, se debem encontrar un inverso $(c, d) \in \mathbb{Z} \times \mathbb{Z}$ tal que

$$(a, b) + (c, d) = (0, 0).$$

Considere $(c, d) = (-a, -b)$. Entonces,

$$(a, b) + (-a, -b) = (a - a, b - b) = (0, 0).$$

Así, para cada $(a, b) \in \mathbb{Z} \times \mathbb{Z}$, $(-a, -b)$ es su inverso.

Por lo tanto, $\mathbb{Z} \times \mathbb{Z}$ es un grupo con la suma definida.

Para demostrar que $H := \{(m, n) \in \mathbb{Z} \times \mathbb{Z} : 2m - 3n = 0\}$ es un subgrupo de $\mathbb{Z} \times \mathbb{Z}$, se debe verificar que H cumple las condiciones de ser un subgrupo. En particular, se debe mostrar que:

1. H es no vacío.
2. H es cerrado bajo la operación de grupo.
3. H contiene los inversos de sus elementos.

En tal caso

1. Para probar que H es no vacío, se debe encontrar al menos un elemento en H. Considere $(m, n) = (3k, 2k)$ para cualquier $k \in \mathbb{Z}$. Entonces,

$$2(3k) - 3(2k) = 6k - 6k = 0.$$

Por lo tanto, cualquier $(3k, 2k) \in H$. En particular, $(0, 0) \in H$ ya que $2 \cdot 0 - 3 \cdot 0 = 0$. Esto muestra que H es no vacío.

2. Para mostrar que H es cerrado bajo la operación de grupo, considere dos elementos (m_1, n_1) y (m_2, n_2) en H. Esto significa que $2m_1 - 3n_1 = 0$ y $2m_2 - 3n_2 = 0$. Se debe probar que $(m_1 + m_2, n_1 + n_2) \in H$.

   Observe que:

$$2(m_1 + m_2) - 3(n_1 + n_2) = (2m_1 - 3n_1) + (2m_2 - 3n_2) = 0 + 0 = 0.$$

   Por lo tanto, $(m_1 + m_2, n_1 + n_2) \in H$, lo que muestra que H es cerrado bajo la suma.

3. Para mostrar que H contiene los inversos de sus elementos, considere un elemento $(m, n) \in H$. Esto significa que $2m - 3n = 0$. Se debe probar que $(-m, -n) \in H$.

   Calculando:

$$2(-m) - 3(-n) = -2m + 3n = -(2m - 3n) = -0 = 0.$$

   Por lo tanto, $(-m, -n) \in H$, lo que muestra que H contiene los inversos de sus elementos.

Por lo tanto, H es un subgrupo de $\mathbb{Z} \times \mathbb{Z}$.

□

Ver p.102

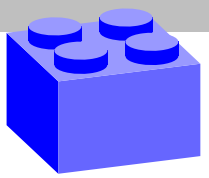
Solución 2.8.9 (Subgrupo)

Para demostrar que H es un subgrupo de $\mathbb{Q}^*$, se necesita verificar que H cumple las siguientes propiedades:

1. H es no vacío.
2. H es cerrado bajo la operación de grupo (multiplicación).
3. H contiene los inversos de sus elementos.

En tal caso:

1. Se puede observar que H contiene el elemento 1, que es un número racional no nulo. Por lo tanto, H es no vacío.



2.Para mostrar que H es cerrado bajo la multiplicación, tome dos elementos cualesquiera a y b en H. Por la definición de H, estos elementos pueden ser expresados como potencias de 2 o fracciones con potencias de 2:

$$a = 2^m \quad \text{y} \quad b = 2^n$$

donde m y n son enteros (positivos, negativos o cero). Debe mostrar que el producto $a \cdot b \in H$. Luego

$$a \cdot b = 2^m \cdot 2^n = 2^{m+n}$$

Dado que $m+n$ es un entero, 2^{m+n} es una potencia de 2, lo cual implica que $2^{m+n} \in H$. Por lo tanto, H es cerrado bajo la multiplicación.

3.Para mostrar que H contiene los inversos de sus elementos, considere un elemento $a \in H$. Por la definición de H, este elemento puede ser expresado como una potencia de 2:

$$a = 2^m$$

donde m es un entero. El inverso de a en $\mathbb{Q}^*$ es a^{-1}:

$$a^{-1} = (2^m)^{-1} = 2^{-m}$$

Dado que $-m$ es también un entero, 2^{-m} es una potencia de 2 o su inverso, lo cual implica que $2^{-m} \in H$. Por lo tanto, H contiene los inversos de sus elementos.

Por lo tanto, H es un subgrupo de $\mathbb{Q}^*$.

□

Solución 2.8.10 (Subgrupo) Ver p.103

Como V es fiito, para demostrar que $H < V$ solo basta verificar que H cumple la propiedad de cerradura, esto es: connsidere los elementos de H, que son e y r. Se necesita verificar que el producto de cualquier par de elementos en H también está en H. Se usa la tabla de Cayley del grupo de Klein para V:

$\circ$	e	h	v	r
e	e	h	v	r
h	h	e	r	v
v	v	r	e	h
r	r	v	h	e

Observe las combinaciones posibles dentro de H:

- $e \circ e = e$
- $e \circ r = r$
- $r \circ e = r$
- $r \circ r = e$

Todos estos productos están en H. Por lo tanto, H es cerrado bajo la operación $\circ$. Por lo tanto, H es un subgrupo de V, y se escribe:

$$H < V$$

.

□

Ver p.103

Solución 2.8.11 (Subgrupo)

Para demostrar que $SO(n, \mathbb{R})$ es un subgrupo de $GL(n, \mathbb{R})$ bajo la multiplicación usual de matrices, se necesita verificar las siguientes propiedades:

1. **Cerradura:** Para todos $A, B \in SO(n, \mathbb{R})$, $AB \in SO(n, \mathbb{R})$.
2. **Elemento identidad:** El elemento identidad de $GL(n, \mathbb{R})$ está en $SO(n, \mathbb{R})$.
3. **Inversos:** Para cada $A \in SO(n, \mathbb{R})$, el inverso de A está en $SO(n, \mathbb{R})$.

Recuerde que el grupo $SO(n, \mathbb{R})$ se define como el grupo de todas las matrices ortogonales A de tamaño $n \times n$ con determinante 1:

$$SO(n, \mathbb{R}) = \{A \in GL(n, \mathbb{R}) \mid A^T A = I \text{ y } \det(A) = 1\}.$$

Con base en este se tiene:

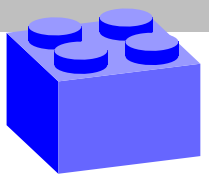
1. Sean $A, B \in SO(n, \mathbb{R})$. Se debe mostrar que $AB \in SO(n, \mathbb{R})$.

   Ortogonalidad: $A^T A = I$ y $B^T B = I$. Entonces,

   $$(AB)^T (AB) = B^T A^T AB = B^T I B = B^T B = I.$$

   Así, AB es ortogonal.

   Cerradura:



Determinante: $\det(A) = 1$ y $\det(B) = 1$. Entonces,

$$\det(AB) = \det(A)\det(B) = 1 \cdot 1 = 1.$$

Por lo tanto, AB tiene determinante 1.

Con estas dos propiedades, $AB \in SO(n, \mathbb{R})$, demostrando el cierre.

2.El elemento identidad en $GL(n, \mathbb{R})$ es la matriz identidad I. Claramente

$$I^T I = I \quad \text{y} \quad \det(I) = 1.$$

Por lo tanto, $I \in SO(n, \mathbb{R})$.

3.Sea $A \in SO(n, \mathbb{R})$. Se debe mostrar que $A^{-1} \in SO(n, \mathbb{R})$.

Ortogonalidad: $A^T A = I$ implica que $A^{-1} = A^T$. Entonces,

$$(A^{-1})^T A^{-1} = (A^T)^T A^T = AA^T = I,$$

así que A^{-1} es ortogonal.

Determinante: $\det(A) = 1$. Se sabe que

$$\det(A^{-1}) = \frac{1}{\det(A)} = \frac{1}{1} = 1.$$

Por lo tanto, A^{-1} tiene determinante 1.

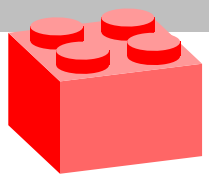
Con estas dos propiedades, $A^{-1} \in SO(n, \mathbb{R})$.

Por lo tanto, $SO(n, \mathbb{R})$ es un subgrupo de $GL(n, \mathbb{R})$.

□

Solución 2.8.12 (Grupo y subgrupo)

Ver p.103



Soluciones

Para probar que $(\mathbb{R}^* \times \mathbb{R}, *)$ es un grupo bajo la operación definida por

$$(a, b) * (c, d) = (4ac, b + d + 3),$$

se necesita verificar las siguientes propiedades: cerradura, asociatividad, neutro e inverso. En efecto:

1. **Cerradura:** dado $(a, b), (c, d) \in \mathbb{R}^* \times \mathbb{R}$, se tiene

   $$(a, b) * (c, d) = (4ac, b + d + 3).$$

   Claramente, $4ac \in \mathbb{R}^*$ ya que a y c son elementos no nulos de $\mathbb{R}$, y $b + d + 3 \in \mathbb{R}$. Por lo tanto, $(4ac, b + d + 3) \in \mathbb{R}^* \times \mathbb{R}$. Esto muestra que el conjunto es cerrado bajo la operación $*$.

2. **Asociatividad:** para verificar la asociatividad, se toma $(a, b), (c, d), (e, f) \in \mathbb{R}^* \times \mathbb{R}$ y se comprueba que

   $$(a, b) * ((c, d) * (e, f)) = ((a, b) * (c, d)) * (e, f).$$

   En efecto, en primer lugar se observa que

   $$(c, d) * (e, f) = (4ce, d + f + 3)$$

   Luego

   $$(a)\ \ (a, b) * (4ce, d + f + 3) = (4a \cdot 4ce, b + (d + f + 3) + 3) = (16ace, b + d + f + 6)$$

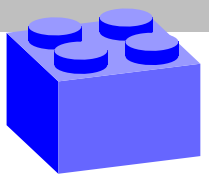
   Por otro lado,

   $$(a, b) * (c, d) = (4ac, b + d + 3).$$

   Luego

   $$(b)\ \ (4ac, b + d + 3) * (e, f) = (4 \cdot 4ac \cdot e, (b + d + 3) + f + 3) = (16ace, b + d + f + 6)$$

   Note que (a) y (b) son expresiones iguales. Esto muestra que la operación es asociativa.



3.**Neutro:** se busca $(e_1, e_2) \in \mathbb{R}^* \times \mathbb{R}$ tal que para todo $(a, b) \in \mathbb{R}^* \times \mathbb{R}$,

$$(e_1, e_2) * (a, b) = (4e_1 a, e_2 + b + 3) = (a, b).$$

Esto ofrece las ecuaciones:

$$4e_1 a = a \quad \text{y} \quad e_2 + b + 3 = b.$$

De la primera ecuación, $(4e_1 = 1)$, se tiene $e_1 = \frac{1}{4}$. De la segunda ecuación, se obtiene $e_2 + 3 = 0$, lo que da $e_2 = -3$. Por lo tanto, el elemento identidad es $\left(\frac{1}{4}, -3\right)$.

4.**Inverso:** para cada $(a, b) \in \mathbb{R}^* \times \mathbb{R}$, se busca $(a', b') \in \mathbb{R}^* \times \mathbb{R}$ tal que

$$(a, b) * (a', b') = \left(4aa', b + b' + 3\right) = \left(\frac{1}{4}, -3\right).$$

Esto genera las ecuaciones:

$$4aa' = \frac{1}{4} \quad \text{y} \quad b + b' + 3 = -3.$$

De la primera ecuación, $a' = \frac{1}{16a}$. De la segunda ecuación, $b' = -6 - b$. Así, el inverso de (a, b) es $\left(\frac{1}{16a}, -6 - b\right)$, que está en $\mathbb{R}^* \times \mathbb{R}$.

Por lo tanto, $(\mathbb{R}^* \times \mathbb{R}, *)$ **es un grupo.**

Para verificar que $H = \{(x, -3) \mid x \in \mathbb{R}^*\}$ es un subgrupo de $\mathbb{R}^* \times \mathbb{R}$ bajo la operación $*$ definida por

$$(a, b) * (c, d) = (4ac, b + d + 3),$$

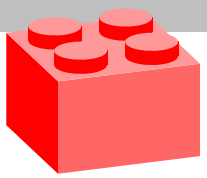
se necesita demostrar que H cumple con las propiedades de un subgrupo:

1.**Cierre:** para todos $(a, -3), (c, -3) \in H$, $(a, -3) * (c, -3) \in H$.

2.**Elemento identidad:** el elemento identidad del grupo $(\mathbb{R}^* \times \mathbb{R}, *)$ está en H.

3.**Inversos:** para cada $(a, -3) \in H$, el inverso $(a', b') \in H$ tal que $(a, -3) * (a', b') = e$, donde e es el elemento identidad del grupo.

Con base en esto se tiene:



Soluciones

1. **Cerradura:** considere dos elementos $(a,-3)$ y $(c,-3)$ en H. Se calcula su producto bajo la operación $*$, es decir

$$(a,-3)*(c,-3)=(4ac,-3+(-3)+3)=(4ac,-3).$$

Dado que $4ac\in\mathbb{R}^*$, se tiene que $(4ac,-3)\in H$. Por lo tanto, H es cerrado bajo la operación $*$.

2. **Elemento identidad:** el elemento identidad de $(\mathbb{R}^*\times\mathbb{R},*)$ es $\left(\frac{1}{4},-3\right)$. Claramente, $\left(\frac{1}{4},-3\right)\in H$. Así, H contiene el elemento identidad del grupo.

3. **Inversos:** para cada $(a,-3)\in H$, se debe encontrar su inverso $(a',-3)\in H$ tal que

$$(a,-3)*(a',-3)=\left(\frac{1}{4},-3\right).$$

De esta forma:

$$(a,-3)*(a',-3)=(4aa',-3+(-3)+3)=(4aa',-3).$$

Para que esto sea igual a $\left(\frac{1}{4},-3\right)$, se necesita que:

$$4aa'=\frac{1}{4}.$$

Por lo tanto, $a'=\frac{1}{16a}$. Así, el inverso de $(a,-3)$ es $\left(\frac{1}{16a},-3\right)$, que está en H.

Por lo tanto, H es un subgrupo de $(\mathbb{R}^*\times\mathbb{R},*)$ y se escribe

$$H<\mathbb{R}^*\times\mathbb{R}.$$

□

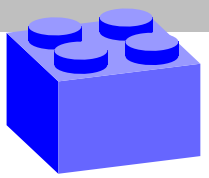
Ver p.103

Solución 2.8.13 (Subgrupo)

Para mostrar que $H=\{x\in G : x^n=e\}$ es un subgrupo de G, donde G es un grupo abeliano con elemento neutro e y n es un entero positivo, se necesita verificar las siguientes propiedades:

1. **Cerradura:** para todos $x,y\in H$, $x\cdot y\in H$.

2. **Elemento identidad:** $e\in H$.



3.**Inversos:** para cada $x \in H$, el inverso $x^{-1} \in H$.

Con base en esto se tiene:

1.**Cerradura:** tome $x, y \in H$. Entonces, por definición de H, se tiene:

$$x^n = e \quad \text{y} \quad y^n = e.$$

Se necesita mostrar que $(x \cdot y) \in H$, es decir, que $(x \cdot y)^n = e$. Dado que G es abeliano, se puede usar la propiedad conmutativa para escribir:

$$(x \cdot y)^n = x^n \cdot y^n.$$

Como $x^n = e$ y $y^n = e$, se tiene:

$$(x \cdot y)^n = e \cdot e = e.$$

Por lo tanto, $x \cdot y \in H$.

2.**Elemento Identidad:** el elemento identidad e de G debe satisfacer la condición para pertenecer a H. Verificando:

$$e^n = e \cdot e \cdot \ldots \cdot e = e$$

(ya que multiplicar el elemento identidad consigo mismo cualquier número de veces sigue siendo e). Por lo tanto, $e \in H$.

3.**Inversos:** Sea $x \in H$. Se necesita mostrar que $x^{-1} \in H$. Se Sabe que $x \in H$ implica

$$x^n = e.$$

y se quiere ver si $(x^{-1})^n = e$.

Primero, considere el producto $x \cdot x^{-1} = e$. Elevando ambos lados de esta igualdad a la potencia n, se obtiene:

$$(x \cdot x^{-1})^n = e^n.$$

Dado que $e^n = e$, se sigue que:

$$(x \cdot x^{-1})^n = e.$$

Dado que G es abeliano, se puede usar la propiedad conmutativa para escribir:

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

Como $x^n = e$, esto se simplifica a:

$$e = e \cdot (x^{-1})^n = (x^{-1})^n.$$

Por lo tanto, $x^{-1} \in H$.

Por lo tanto, H es un subgrupo de G y se escribe

$$H < G.$$

□

Ver p.103

Solución 2.8.14 (Subgrupo)

Para demostrar que $H = \bigcap_{i=1}^{n} H_i$ es un subgrupo de G, donde $H_1, H_2, \ldots, H_n$ son subgrupos de G, se necesita verificar que H cumple con las propiedades de un subgrupo:

1. **Cerradura:** para todos $x, y \in H$, $x \cdot y \in H$.
2. **Elemento identidad:** el elemento identidad $e \in H$.
3. **Inversos:** para cada $x \in H$, el inverso $x^{-1} \in H$.

Con base en lo anterior se tiene:

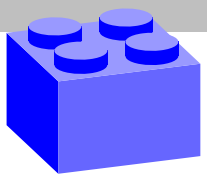
1. **Cerradura:** sean $x, y \in H$. Esto significa que $x, y \in H_i$ para todos $i = 1, 2, \ldots, n$. Dado que cada H_i es un subgrupo de G, y los subgrupos son cerrados bajo la operación del grupo, se tiene que $x \cdot y \in H_i$ para todos $i = 1, 2, \ldots, n$. Por lo tanto, $x \cdot y \in \bigcap_{i=1}^{n} H_i = H$.
2. **Elemento identidad:** dado que cada H_i es un subgrupo de G, el elemento identidad e de G pertenece a cada H_i. Por lo tanto, $e \in H_i$ para todos $i = 1, 2, \ldots, n$, lo que implica que $e \in \bigcap_{i=1}^{n} H_i = H$.
3. **Inversos:** sea $x \in H$. Esto significa que $x \in H_i$ para todos $i = 1, 2, \ldots, n$. Dado que cada H_i es un subgrupo, el inverso $x^{-1} \in H_i$ para todos $i = 1, 2, \ldots, n$. Por lo tanto, $x^{-1} \in \bigcap_{i=1}^{n} H_i = H$.

Por lo tanto, H es un subgrupo de G, o bien,

$$H = \bigcap_{i=1}^{n} H_i < G$$

□

Soluciones



Solución 2.8.15 (Subgrupo) Ver p.104

Para demostrar que $H = \bigcup_{n\in\mathbb{N}} H_n$ es un subgrupo de G, donde $H_1 \subset H_2 \subset H_3 \subset \cdots$ es una sucesión de subgrupos de G, se debe verificar que H cumple con las tres propiedades de un subgrupo:

1. **Cerradura:** para todos $x, y \in H$, $x \cdot y \in H$.
2. **Elemento Identidad:** el elemento identidad $e \in H$.
3. **Inversos:** para cada $x \in H$, el inverso $x^{-1} \in H$.

Con base en lo anterior se tiene:

1. **Cerradura:** sean $x, y \in H$. Por la definición de H, existen $m, n \in \mathbb{N}$ tales que $x \in H_m$ y $y \in H_n$. Sin pérdida de generalidad, suponga que $m \leq n$. Dado que $H_m \subset H_n$, se tiene $x \in H_n$. Dado que H_n es un subgrupo, el producto $x \cdot y \in H_n$. Como $H_n \subset H$, tenemos $x \cdot y \in H$. Esto prueba el cierre de H.
2. **Elemento Identidad:** dado que cada H_n es un subgrupo, el elemento identidad e de G pertenece a cada H_n. Por lo tanto, $e \in H_n$ para todo $n \in \mathbb{N}$, lo que implica que $e \in H$.
3. **Inversos:** sea $x \in H$. Entonces, existe algún $n \in \mathbb{N}$ tal que $x \in H_n$. Dado que H_n es un subgrupo, el inverso $x^{-1} \in H_n$. Como $H_n \subset H$, se tiene que $x^{-1} \in H$.

Por lo tanto, H es un subgrupo de G, o bien,

$$H = \bigcup_{n\in\mathbb{N}} H_n < G.$$

□

Solución 2.8.16 (Subgrupo) Ver p.104

Para demostrar que si K es un subgrupo de H y H es un subgrupo de G, entonces K es un subgrupo de G, se necesita verificar que K cumple con las propiedades de un subgrupo en G:

1. **Cerradura:** para todos $x, y \in K$, $x \cdot y \in K$.
2. **Elemento identidad:** el elemento identidad $e_G \in K$.
3. **Inversos:** para cada $x \in K$, el inverso $x^{-1} \in K$.

En efecto

1. **Cerradura:** dado que K es un subgrupo de H, K es cerrado bajo la operación en H. Esto significa que para todos $x, y \in K$, $x \cdot y \in K$.

   Dado que H es un subgrupo de G, la operación en H es la misma que la operación en G. Por lo tanto, para todos $x, y \in K$, el producto $x \cdot y$ en G está en K. Así, K es cerrado bajo la operación en G.

2. **Elemento identidad:** Dado que H es un subgrupo de G, contiene el elemento identidad e_G de G.

   Dado que K es un subgrupo de H, también contiene el elemento identidad de H. Pero el elemento identidad de H es el mismo que el de G porque H es un subgrupo de G. Por lo tanto, $e_G \in K$.

3. **Inversos:** Dado que K es un subgrupo de H, para cada $x \in K$, su inverso $x^{-1} \in K$.

   Dado que H es un subgrupo de G, la operación de tomar el inverso en H es la misma que en G. Por lo tanto, para cada $x \in K$, el inverso x^{-1} en G también está en K.

Por lo tanto, K es un subgrupo de G, o bien,

$$K < G.$$

□

Ver p.104

Solución 2.8.17 (Subgrupo)

Para demostrar que $H \cup K$ es un subgrupo de G si y solo si $H \subset K$ o $K \subset H$, se necesita considerar ambas direcciones de la implicación.

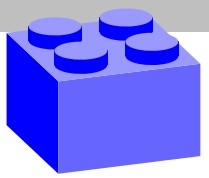
Direción: Si $H \cup K$ es un subgrupo de G, entonces $H \subset K$ o $K \subset H$.

Suponga que $H \cup K$ es un subgrupo de G. Se quiere demostrar que $H \subset K$ o $K \subset H$.

Dado que $H \cup K$ es un subgrupo de G, es cerrado bajo la operación del grupo, tome $h \in H$ y $k \in K$. Como $H \cup K$ es un subgrupo, el producto $h \cdot k$ debe estar en $H \cup K$.

Considere los siguientes casos:

- **Caso 1:** $h \in H \cap K$.



Si $h \in H \cap K$, entonces $h \in H$ y $h \in K$. En este caso, no hay nada que demostrar, ya que h pertenece a ambos subgrupos.

- **Caso 2:** $h \in H - K$ y $k \in K - H$.

Suponga que existe $h \in H - K$ y $k \in K - H$. Entonces, considere el producto $h \cdot k$. Como $h \cdot k \in H \cup K$, se tiene dos subcasos:

- Si $h \cdot k \in H$, entonces $k = h^{-1} \cdot (h \cdot k) \in H$ (porque $h^{-1} \in H$ y H es cerrado bajo la operación de grupo), lo que implica que $k \in H$, una contradicción porque se asumió que $k \in K - H$.
- - Si $h \cdot k \in K$, entonces $h = (h \cdot k) \cdot k^{-1} \in K$ (porque $k^{-1} \in K$ y K es cerrado bajo la operación de grupo), lo que implica que $h \in K$, una contradicción porque se asumió que $h \in H - K$.

Por lo tanto, no puede haber elementos $h \in H - K$ y $k \in K - H$. Esto implica que $H \subset K$ o $K \subset H$.

Dirección: Si $H \subset K$ o $K \subset H$, entonces $H \cup K$ es un subgrupo de G.

Suponga que $H \subset K$ o $K \subset H$. Sin pérdida de generalidad, suponga que $H \subset K$. (El argumento es similar si $K \subset H$.)

Si $H \subset K$, entonces $H \cup K = K$. Dado que K es un subgrupo de G, K es cerrado bajo la operación de grupo, contiene el elemento identidad y contiene los inversos de sus elementos. Por lo tanto, K es un subgrupo de G, y como $H \cup K = K$, se sigue que $H \cup K$ es un subgrupo de G.

Se ha demostrado que $H \cup K$ es un subgrupo de G si y solo si $H \subset K$ o $K \subset H$.

□

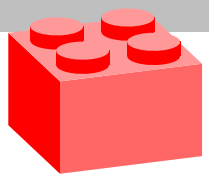
Solución 2.8.18 (Subgrupo)

Ver p.104

Para demostrar que si H y K son subgrupos de un grupo abeliano G, entonces HK es un subgrupo de G, se necesita verificar que HK cumple con las propiedades de un subgrupo:

1. **Cerradura:** Para todos $a, b \in HK$, $a \cdot b \in HK$.
2. **Elemento identidad:** El elemento identidad $e \in HK$.
3. **Inversos:** Para cada $a \in HK$, el inverso $a^{-1} \in HK$.

Con base en lo anterior se sigue que:



Soluciones

1. **Cerradura:** Sean $a, b \in HK$. Entonces existen $h_1, h_2 \in H$ y $k_1, k_2 \in K$ tales que $a = h_1k_1$ y $b = h_2k_2$. Se quiere demostrar que $a \cdot b \in HK$:

   $$a \cdot b = (h_1k_1) \cdot (h_2k_2).$$

   Dado que G es abeliano, se pueden reordenar los factores:

   $$a \cdot b = h_1k_1h_2k_2 = h_1h_2k_1k_2.$$

   Como H y K son subgrupos, $h_1h_2 \in H$ y $k_1k_2 \in K$. Por lo tanto, $h_1h_2 \in H$ y $k_1k_2 \in K$, lo que implica que:

   $$a \cdot b = (h_1h_2)(k_1k_2) \in HK.$$

   Esto muestra que HK es cerrado bajo la operación del grupo.

2. **Elemento identidad:** El elemento identidad e de G pertenece a H y a K porque H y K son subgrupos. Entonces, $e \cdot e = e \in HK$. Por lo tanto, HK contiene el elemento identidad.

3. **Inversos:** Sea $a \in HK$. Entonces, existe $h \in H$ y $k \in K$ tales que $a = hk$. Se quiere demostrar que $a^{-1} \in HK$.

   Dado que G es abeliano, el inverso de a es:

   $$a^{-1} = (hk)^{-1} = k^{-1}h^{-1}.$$

   Como H y K son subgrupos, $h^{-1} \in H$ y $k^{-1} \in K$. Dado que G es abeliano, se pueden reordenar los factores:

   $$a^{-1} = k^{-1}h^{-1} = h^{-1}k^{-1} \in HK.$$

   Esto muestra que HK contiene los inversos de sus elementos.

Por lo tanto, HK es un subgrupo de G, o bien,

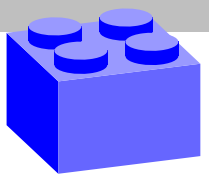
$$HK < G.$$

□

Ver p.104

Solución 2.8.19 (Subgrupo)

Para demostrar que HK es un subgrupo de G si y sólo si $HK = KH$, donde H y K son subgrupos de G, se probarán ambas direcciones de la implicación.



Dirección 1: Si $HK < G$, entonces $HK = KH$

Dado que HK es un subgrupo de G, para cada $h \in H$ y $k \in K$, el producto $hk \in HK$. Como HK es un subgrupo, es cerrado bajo la operación de grupo y contiene los inversos de sus elementos. Considere un elemento arbitrario $hk \in HK$. Se quiere mostrar que cualquier elemento en HK también puede escribirse como un producto de un elemento de K y un elemento de H, es decir, que $hk \in KH$.

Con base en lo anterior, sea $hk \in HK$. Ya que HK es un subgrupo, $(hk)^{-1} \in HK$. Pero,

$$(hk)^{-1} = k^{-1}h^{-1}.$$

Dado que $h^{-1} \in H$ y $k^{-1} \in K$, se tiene que $k^{-1}h^{-1} \in KH$.

Como HK es un subgrupo, contiene todos los productos y sus inversos, y por tanto,

$$k^{-1}h^{-1} \in HK \implies (k^{-1}h^{-1})^{-1} \in HK.$$

Pero,

$$(k^{-1}h^{-1})^{-1} = hk.$$

Esto muestra que $hk \in KH$. Así, $HK \subseteq KH$.

De manera similar, tomando cualquier $kh \in KH$, se puede mostrar que $kh \in HK$. Por lo tanto, $KH \subseteq HK$.

Se concluye que $HK = KH$.

Dirección 2: Si $HK = KH$, entonces $HK < G$

Suponga que $HK = KH$. Se quiere demostrar que HK es un subgrupo de G.

Para ser un subgrupo, HK debe satisfacer las siguientes propiedades:

1. **Cierre:** Para todos $x, y \in HK$, $xy \in HK$.

2. **Elemento identidad:** El elemento identidad $e \in HK$.

3. **Inversos:** Para cada $x \in HK$, $x^{-1} \in HK$.

Con base en lo anterior se sigue que

1. **Cerradura:** Sea $a, b \in HK$. Entonces, $a = h_1k_1$ y $b = h_2k_2$ para algunos $h_1, h_2 \in H$ y $k_1, k_2 \in K$. Se quiere mostrar que $ab \in HK$.

   Considere:

   $$ab = (h_1k_1)(h_2k_2).$$

   Dado que $KH = HK$, se puede reordenar $k_1h_2 \in KH$ como $k_1h_2 = h_3k_3$ para algún $k_3 \in K$ y $h_3 \in H$. Por lo tanto,

   $$ab = h_1(k_1h_2)k_2 = h_1(h_3k_3)k_2 = (h_1h_3)(k_3k_2).$$

   Como $h_1h_3 \in H$ y $K_3k_2 \in K$, se tiene que $ab \in HK$. Esto muestra que HK es cerrado bajo la operación de grupo.

2. **Elemento identidad:** El elemento identidad e de G pertenece a ambos H y K porque son subgrupos. Por lo tanto,

   $$e = ee \in HK.$$

   Esto muestra que el elemento identidad $e \in HK$.

3. **Inversos:** Sea $x \in HK$. Entonces, $x = hk$ para algún $h \in H$ y $k \in K$. Se quiere mostrar que $x^{-1} \in HK$.

   Considere:

   $$x^{-1} = (hk)^{-1} = k^{-1}h^{-1}.$$

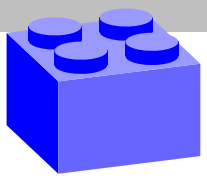
   Dado que $k^{-1} \in K$ y $h^{-1} \in H$, y utilizando la propiedad $HK = KH$, se puede escribir:

   $$k^{-1}h^{-1} = h^{-1}k^{-1} \in KH = HK.$$

   Por lo tanto, $x^{-1} \in HK$.

Se ha demostrado que HK es un subgrupo de G si y solo si $HK = KH$.

□



Solución 2.8.20 (Centralizador y Subgrupo) Ver p.105

Para demostrar que el centro $Z(G)$ de un grupo G es un subgrupo de G, se necesita verificar que $Z(G)$ cumple con las tres propiedades de un subgrupo:

1. **Cerradura:** Para todos $a, b \in Z(G)$, $ab \in Z(G)$.

2. **Elemento identidad:** El elemento identidad $e \in Z(G)$.

3. **Inversos:** Para cada $a \in Z(G)$, el inverso $a^{-1} \in Z(G)$.

Con base en lo anterior se tiene:

1. **Cerradura:** Sea $a, b \in Z(G)$. Esto significa que a y b conmutan con todos los elementos de G, es decir,

$$ax = xa \quad \text{y} \quad bx = xb \quad \text{para todo } x \in G.$$

   Se quiere demostrar que $ab \in Z(G)$, es decir, que $(ab)x = x(ab)$ para todo $x \in G$. Considere:

$$(ab)x = a(bx).$$

   Dado que $b \in Z(G)$, se sabe que $bx = xb$. Sustituyendo esto en la ecuación anterior se obtiene:

$$(ab)x = a(xb).$$

   Dado que $a \in Z(G)$, se sabe que $ax = xa$. Aplicando esto, se obtiene:

$$a(xb) = (ax)b = (xa)b = x(ab).$$

   Por lo tanto, $(ab)x = x(ab)$ para todo $x \in G$, lo que implica que $ab \in Z(G)$. Esto demuestra que $Z(G)$ es cerrado bajo la operación de grupo.

2. **Elemento identidad:** El elemento identidad e de G conmuta con todos los elementos de G. Es decir, para todo $x \in G$,

$$ex = xe = x.$$

   Por lo tanto, $e \in Z(G)$.

3. **Inversos:** Sea $a \in Z(G)$. Esto significa que a conmuta con todos los elementos de G, es decir,

$$ax = xa \quad \text{para todo } x \in G.$$

Se quiere demostrar que $a^{-1} \in Z(G)$, es decir, que $a^{-1}x = xa^{-1}$ para todo $x \in G$.

Considere:

$$aa^{-1} = e = a^{-1}a$$

Multiplicando ambos lados de la ecuación $ax = xa$ por a^{-1} a la izquierda, se obtiene:

$$a^{-1}(ax) = a^{-1}(xa).$$

Simplificando, se tiene:

$$a^{-1}(ax) = a^{-1}(xa) \Leftrightarrow (a^{-1}a)x = a^{-1}(xa) \Leftrightarrow x = a^{-1}(xa)$$

Multiplicando ambos lados por a^{-1} a la derecha se obtiene:

$$xa^{-1} = a^{-1}(xa)a^{-1} \Leftrightarrow xa^{-1} = (a^{-1}x)(aa^{-1}) \Leftrightarrow xa^{-1} = a^{-1}x$$

Por lo tanto, $a^{-1} \in Z(G)$.

Por lo tanto, $Z(G)$ es un subgrupo de G, es decir,

$$Z(G) < G.$$

□

Ver p.105

Solución 2.8.21 (Centralizador y Subgrupo)

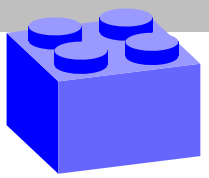
Para demostrar que el centralizador $C_G(A)$ de A en G es un subgrupo de G, se necesita verificar que $C_G(A)$ cumple con las tres propiedades de un subgrupo:

1. **Cerradura:** Para todos $x, y \in C_G(A)$, $xy \in C_G(A)$.
2. **Elemento identidad:** El elemento identidad $e \in C_G(A)$.
3. **Inversos:** Para cada $x \in C_G(A)$, el inverso $x^{-1} \in C_G(A)$.

Con base en lo anterior se tiene

1. **Cerradura:** Sean $x, y \in C_G(A)$. Esto significa que x y y conmutan con todos los elementos de A, es decir,

$$xa = ax \quad \text{y} \quad ya = ay \quad \text{para todo } a \in A.$$



Se quiere demostrar que $xy \in C_G(A)$, es decir, que $(xy)a = a(xy)$ para todo $a \in A$. Considere:

$$(xy)a = x(ya).$$

Dado que $y \in C_G(A)$, se sabe que $ya = ay$. Sustituyendo esto en la ecuación anterior se tiene:

$$(xy)a = x(ay).$$

Dado que $x \in C_G(A)$, se sabe que $xa = ax$. Aplicando esto, se tiene:

$$x(ay) = (xa)y = (ax)y = a(xy).$$

Por lo tanto, $(xy)a = a(xy)$ para todo $a \in A$, lo que implica que $xy \in C_G(A)$. Esto demuestra que $C_G(A)$ es cerrado bajo la operación de grupo.

2. **Elemento identidad:** El elemento identidad e de G conmuta con todos los elementos de G y, por lo tanto, con todos los elementos de A. Es decir, para todo $a \in A$,

$$ea = ae = a.$$

Por lo tanto, $e \in C_G(A)$.

3. **Inversos:** Sea $x \in C_G(A)$. Esto significa que x conmuta con todos los elementos de A, es decir,

$$xa = ax \quad \text{para todo } a \in A.$$

Se quiere demostrar que $x^{-1} \in C_G(A)$, es decir, que $x^{-1}a = ax^{-1}$ para todo $a \in A$.

Considere:

$$xx^{-1} = e = x^{-1}x$$

Multiplicando ambos lados de la ecuación $xa = ax$ por x^{-1} a la izquierda, se obtiene:

$$x^{-1}(xa) = x^{-1}(ax).$$

Simplificando, se tiene:

$$(x^{-1}x)a = x^{-1}(ax) \Leftrightarrow a = x^{-1}(ax)$$

Multiplicando ambos lados por x^{-1} a la derecha, se obtiene:

$$ax^{-1} = x^{-1}(ax)x^{-1} \Leftrightarrow ax^{-1} = (x^{-1}a)(xx^{-1}) \Leftrightarrow ax^{-1} = x^{-1}a$$

Por lo tanto, $x^{-1} \in C_G(A)$.

Por lo tanto, $C_G(A)$ es un subgrupo de G, o bien,

$$C_G(A) < G.$$

□

Soluciones de la sección 2.13

Solución 2.13.1 (Orden de elementos y grupos factores) Ver p.155

Para hallar el orden del grupo cociente $\mathbb{Z}_6/\langle 3\rangle$, se siguen los siguientes pasos:

1. **Identificar el subgrupo $\langle 3\rangle$:**

   En el grupo $\mathbb{Z}_6$, el elemento 3 genera el subgrupo $\langle 3\rangle$, que consiste en todos los múltiplos de 3 en $\mathbb{Z}_6$:

   $$\langle 3\rangle = \{0, 3\}$$

   Aquí, 0 y 3 son los únicos múltiplos de 3 en $\mathbb{Z}_6$.

2. **Determinar los elementos del grupo cociente $\mathbb{Z}_6/\langle 3\rangle$:**

   El grupo cociente $\mathbb{Z}_6/\langle 3\rangle$ consiste en las clases laterales de $\langle 3\rangle$ en $\mathbb{Z}_6$. Las clases laterales son conjuntos de la forma $a + \langle 3\rangle$, donde $a \in \mathbb{Z}_6$.

   Las clases laterales son:

   $$0 + \langle 3\rangle = \{0, 3\}$$

   $$1 + \langle 3\rangle = \{1, 4\}$$

   $$2 + \langle 3\rangle = \{2, 5\}$$

   $$3 + \langle 3\rangle = \{3, 0\} = \{0, 3\} = 0 + \langle 3\rangle$$

   $$4 + \langle 3\rangle = \{4, 1\} = 1 + \langle 3\rangle$$

   $$5 + \langle 3\rangle = \{5, 2\} = 2 + \langle 3\rangle$$

   Observe que $3+\langle 3\rangle$, $4+\langle 3\rangle$, y $5+\langle 3\rangle$ ya están representados por las clases laterales $0+\langle 3\rangle$, $1+\langle 3\rangle$, y $2+\langle 3\rangle$, respectivamente. Por lo tanto, se tienen 3 clases laterales distintas:

   $$\{0 + \langle 3\rangle, 1 + \langle 3\rangle, 2 + \langle 3\rangle\}$$

3. **Calcular el orden del grupo cociente $\mathbb{Z}_6/\langle 3\rangle$:**

   El orden del grupo cociente $\mathbb{Z}_6/\langle 3\rangle$ es igual al número de clases laterales de

$\langle 3 \rangle$ en $\mathbb{Z}_6$, que se han determinado, es decir 3.

Por lo tanto, el orden del grupo cociente $\mathbb{Z}_6/\langle 3 \rangle$ es 3.

Para hallar el orden del grupo cociente $(\mathbb{Z}_4 \times \mathbb{Z}_{12})/\langle 2 \rangle \times \langle 2 \rangle$, así como el orden de sus elementos y grupos factores, se procede de la siguiente manera:

1. **Entender la estructura del grupo original y del subgrupo:**

   El grupo $\mathbb{Z}_4 \times \mathbb{Z}_{12}$ consta de pares de elementos, donde el primer componente proviene de $\mathbb{Z}_4$ y el segundo de $\mathbb{Z}_{12}$. Es decir, cada elemento del grupo se puede expresar como (a, b) con $a \in \{0, 1, 2, 3\}$ y $b \in \{0, 1, 2, \ldots, 11\}$.

   El subgrupo $\langle 2 \rangle \times \langle 2 \rangle$ se refiere a los elementos generados por $(2, 0)$ en $\mathbb{Z}_4$ y $(0, 2)$ en $\mathbb{Z}_{12}$. Este subgrupo contiene los elementos $(2k, 2j)$ donde $k = 0, 1$ (dado que 2 tiene orden 2 en $\mathbb{Z}_4$) y $j = 0, 1, 2, \ldots, 5$ (dado que 2 tiene orden 6 en $\mathbb{Z}_{12}$).

2. **Determinar los elementos del subgrupo $\langle 2 \rangle \times \langle 2 \rangle$:**

   El subgrupo es:

   $$\langle 2 \rangle \times \langle 2 \rangle = \{(2k, 2j) \mid k = 0, 1; j = 0, 1, 2, 3, 4, 5\}$$

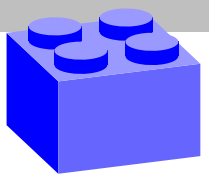
   Esto incluye 2 valores para k y 6 valores para j, así que el subgrupo tiene $2 \times 6 = 12$ elementos.

3. **Calcular el orden del grupo cociente $(\mathbb{Z}_4 \times \mathbb{Z}_{12})/\langle 2 \rangle \times \langle 2 \rangle$:**

4. El orden del grupo original es $4 \times 12 = 48$, y el orden del subgrupo es 12. El orden del grupo cociente, según el teorema de Lagrange, es el cociente de estos dos órdenes:

   $$\frac{48}{12} = 4$$

5. **Encontrar las clases laterales del subgrupo en el grupo:**



Para simplificar, considere elementos representativos de cada clase lateral de la forma $(a, b) + \langle 2\rangle \times \langle 2\rangle$ donde $a \in \{0, 1\}$ y $b \in \{0, 1\}$ porque los múltiplos de 2 en cada coordenada ya están en $\langle 2\rangle \times \langle 2\rangle$. Esto da las siguientes clases laterales posibles:

$$(0,0) + \langle 2\rangle \times \langle 2\rangle, \quad (1,0) + \langle 2\rangle \times \langle 2\rangle, \quad (0,1) + \langle 2\rangle \times \langle 2\rangle, \quad (1,1) + \langle 2\rangle \times \langle 2\rangle$$

6. **Orden de los elementos en el grupo cociente:**

   Cada elemento en el grupo cociente es una clase lateral. El orden de un elemento $(a, b) + \langle 2\rangle \times \langle 2\rangle$ en el grupo cociente es el menor número n tal que $n(a, b) \in \langle 2\rangle \times \langle 2\rangle$. Dado que el orden del grupo cociente es 4 y es pequeño, se puede deducir que el orden de cada elemento podría ser 1, 2, o 4 dependiendo de cómo se combinan a y b con las propiedades de $\mathbb{Z}_4$ y $\mathbb{Z}_{12}$.

El grupo cociente $(\mathbb{Z}_4 \times \mathbb{Z}_{12})/\langle 2\rangle \times \langle 2\rangle$ **es por tanto un grupo de orden 4.**

Para analizar el grupo cociente $(\mathbb{Z}_4 \times \mathbb{Z}_{12})/\langle (2, 2)\rangle$, primero se identifica la estructura y orden del subgrupo generado por el elemento $(2, 2)$, y luego se calcula el orden del grupo cociente y las propiedades de sus elementos y subgrupos.

1. **Identificar el subgrupo** $\langle (2, 2)\rangle$

   El elemento $(2, 2)$ pertenece al grupo producto $\mathbb{Z}_4 \times \mathbb{Z}_{12}$. Para entender el subgrupo generado por $(2, 2)$, se debe considerar la periodicidad de cada componente:

   La primera componente, 2 en $\mathbb{Z}_4$, se repite cada 2 operaciones, ya que $2 + 2 = 0$ mód 4.

   La segunda componente, 2 en $\mathbb{Z}_{12}$, se repite cada 6 operaciones, ya que $2 \times 6 = 12 \equiv 0 \mod 12$.

   Así, el elemento $(2, 2)$ tiene un orden que es el mínimo común múltiplo de los órdenes de sus componentes, 2 y 6, que es 6. Esto significa que el subgrupo

$\langle(2,2)\rangle$ es:

$$\langle(2,2)\rangle =$$

$$\{(0,0),(2,2),(4,4),$$

$$(6,6) \equiv (2,6) \equiv (2,0),$$

$$(8,8) \equiv (0,8) \equiv (0,8),$$

$$(10,10) \equiv (2,10) \equiv (2,10)\}$$

Pero se simplifica por las congruencias en cada componente:

$$\langle(2,2)\rangle = \{(0,0),(2,2),(0,4),(2,6),(0,8),(2,10)\}$$

2. **Calcular el orden del grupo cociente** $(\mathbb{Z}_4 \times \mathbb{Z}_{12})/\langle(2,2)\rangle$

   El orden del grupo original, $\mathbb{Z}_4 \times \mathbb{Z}_{12}$, es $4 \times 12 = 48$. El subgrupo $\langle(2,2)\rangle$ tiene 6 elementos. Utilizando el Teorema de Lagrange, el orden del grupo cociente es:

$$\frac{48}{6} = 8$$

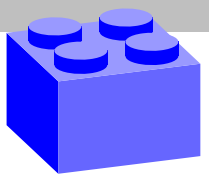
3. **Características de los elementos en el grupo cociente**

   El grupo cociente consistirá en las clases laterales de $\langle(2,2)\rangle$ en $\mathbb{Z}_4 \times \mathbb{Z}_{12}$. Cada clase lateral puede representarse sumando un elemento del grupo original que no está en $\langle(2,2)\rangle$ a cada elemento del subgrupo. Los representantes de las clases podrían elegirse de manera sistemática considerando los residuos menores posibles en ambas coordenadas que no están ya en $\langle(2,2)\rangle$.

El grupo cociente $(\mathbb{Z}_4 \times \mathbb{Z}_{12})/\langle(2,2)\rangle$ **es un grupo de orden 8.**

Para hallar el orden del elemento $5 + \langle 4\rangle$ en el grupo cociente $\mathbb{Z}_{12}/\langle 4\rangle$, se siguen estos pasos:

1. **Identificar el subgrupo** $\langle 4\rangle$ **en** $\mathbb{Z}_{12}$**:**



El subgrupo $\langle 4 \rangle$ está generado por 4 en $\mathbb{Z}_{12}$, que contiene los múltiplos de 4:

$$\langle 4 \rangle = \{0, 4, 8\}$$

2.**Determinar las clases laterales de $\langle 4 \rangle$ en $\mathbb{Z}_{12}$:**

El grupo cociente $\mathbb{Z}_{12}/\langle 4 \rangle$ consiste en las clases laterales de $\langle 4 \rangle$:

$$0 + \langle 4 \rangle = \{0, 4, 8\}$$

$$1 + \langle 4 \rangle = \{1, 5, 9\}$$

$$2 + \langle 4 \rangle = \{2, 6, 10\}$$

$$3 + \langle 4 \rangle = \{3, 7, 11\}$$

3.**Encontrar el orden del elemento $5 + \langle 4 \rangle$:**

Para hallar el orden de $5 + \langle 4 \rangle$ en $\mathbb{Z}_{12}/\langle 4 \rangle$, se necesita encontrar el menor entero positivo n tal que $n(5 + \langle 4 \rangle) = \langle 4 \rangle$.

Se multiplica el representante 5 por n y se observa cuándo se vuelve un múltiplo de 4 en $\mathbb{Z}_{12}$:

$$n \cdot 5 \equiv 0 \mod 4$$

Resolviendo esta congruencia,se busca el menor n tal que:

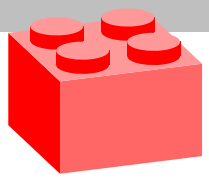
$$5n \equiv 0 \mod 4$$

Para que esto ocurra, n debe ser un múltiplo de 4, ya que 5 y 4 son coprimos. Por lo tanto, n debe ser 4. Verificando:

$$5 \cdot 4 = 20 \equiv 0 \mod 12$$

Así, el orden del elemento $5 + \langle 4 \rangle$ es 4.

El orden del elemento $5 + \langle 4 \rangle$ en el grupo cociente $\mathbb{Z}_{12}/\langle 4 \rangle$ es 4.



Soluciones

Para determinar el orden del grupo cociente $\mathbb{Z}_{12}/\langle 4\rangle$ y sus elementos, se procede de la siguiente manera:

1. **Analizar el subgrupo** $\langle 4\rangle$:

   En $\mathbb{Z}_{12}$, el subgrupo generado por el elemento 4, $\langle 4\rangle$, incluye todos los múltiplos de 4 módulo 12:

   $$\langle 4\rangle = \{0, 4, 8\}$$

   Este subgrupo tiene 3 elementos.

2. **Calcular el orden del grupo cociente** $\mathbb{Z}_{12}/\langle 4\rangle$

   Dado que el subgrupo $\langle 4\rangle$ tiene 3 elementos, el orden del grupo cociente, según el Teorema de Lagrange, es el cociente entre el orden del grupo original $\mathbb{Z}_{12}$ y el orden del subgrupo:

   $$\text{Orden de } \mathbb{Z}_{12}/\langle 4\rangle = \frac{\text{Orden de } \mathbb{Z}_{12}}{\text{Orden de } \langle 4\rangle} = \frac{12}{3} = 4$$

   Por lo tanto, el grupo cociente $\mathbb{Z}_{12}/\langle 4\rangle$ es un grupo de orden 4.

3. **Describir los elementos del grupo cociente y sus órdenes**

   Los elementos del grupo cociente son las clases laterales de $\langle 4\rangle$ en $\mathbb{Z}_{12}$. Cada clase lateral se puede describir como sigue:

   $$0 + \langle 4\rangle = \{0, 4, 8\}$$

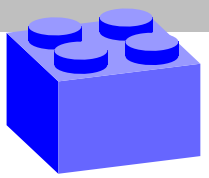
   $$1 + \langle 4\rangle = \{1, 5, 9\}$$

   $$2 + \langle 4\rangle = \{2, 6, 10\}$$

   $$3 + \langle 4\rangle = \{3, 7, 11\}$$

4. **Paso 4: Orden de cada elemento en el grupo cociente:**

   Para hallar el orden de un elemento como $a + \langle 4\rangle$ en $\mathbb{Z}_{12}/\langle 4\rangle$, se busca el menor número positivo n tal que $na \equiv 0 \mod 12$, donde a es un representante de



la clase lateral.

Por ejemplo, el orden de $1 + \langle 4 \rangle$ es el menor n tal que $n \cdot 1$ es un múltiplo de 4 (que son los elementos de $\langle 4 \rangle$):

$$n \equiv 0 \mod 4 \Rightarrow n = 4$$

Así, el orden de $1 + \langle 4 \rangle$ es 4. Similarmente, los otros elementos $2 + \langle 4 \rangle$ y $3 + \langle 4 \rangle$ también tendrán orden 4, ya que 12 es el primer múltiplo común de 4 y estos números.

El grupo cociente $\mathbb{Z}_{12}/\langle 4 \rangle$ es un grupo de orden 4. Cada elemento no trivial del grupo cociente (diferente de la clase lateral $0 + \langle 4 \rangle$) tiene orden 4.

□

Solución 2.13.2 (grupo y subgrupo normal)

Ver p.155

Para mostrar que $(G, \circ)$ es un grupo, donde $\circ$ denota la operación de composición de funciones, se debe verificar que G satisface las cuatro propiedades de un grupo: cerradura, asociatividad, existencia de un elemento identidad, y existencia de elementos inversos.

1. **Cerradura:** Para mostrar la cerradura, se necesita demostrar que la composición de dos funciones en G también pertenece a G. Sean $f_{a,b}$ y $f_{a',b'}$ dos elementos de G. La composición $f_{a,b} \circ f_{a',b'}$ se define por:

$$(f_{a,b} \circ f_{a',b'})(x) = f_{a,b}(f_{a',b'}(x))$$

Primero se evalúa $f_{a',b'}(x)$:

$$f_{a',b'}(x) = a'x + b'$$

Luego se evalúa $f_{a,b}$ en este resultado:

$$f_{a,b}(a'x + b') = a(a'x + b') + b = aa'x + ab' + b$$

Por lo tanto:

$$(f_{a,b} \circ f_{a',b'})(x) = aa'x + (ab' + b)$$

Note que $aa' \neq 0$ porque $a \neq 0$ y $a' \neq 0$, y tanto aa' como $ab' + b$ son números reales. Así, $f_{aa',ab'+b}$ es una función de la misma forma que los elementos de G, lo que demuestra que $f_{a,b} \circ f_{a',b'} \in G$. Por lo tanto, G es cerrado bajo la composición.

2. **Asociatividad:** La composición de funciones es asociativa por definición. Para cualquier $f_{a,b}, f_{a',b'}, f_{a'',b''} \in G$:

$$(f_{a,b} \circ (f_{a',b'} \circ f_{a'',b''}))(x) = ((f_{a,b} \circ f_{a',b'}) \circ f_{a'',b''})(x)$$

Esto se sigue de la propiedad de la composición de funciones.

3. **Identidad:** Para la existencia de un elemento identidad, se necesita una función $f_{e,f}$ tal que, para cualquier $f_{a,b} \in G$:

$$f_{e,f} \circ f_{a,b} = f_{a,b} \circ f_{e,f} = f_{a,b}$$

Considere la función $f_{1,0}(x) = 1x + 0 = x$. Para cualquier $f_{a,b}(x) = ax + b$:

$$(f_{1,0} \circ f_{a,b})(x) = f_{1,0}(f_{a,b}(x)) = f_{1,0}(ax + b) = ax + b = f_{a,b}(x)$$

$$(f_{a,b} \circ f_{1,0})(x) = f_{a,b}(f_{1,0}(x)) = f_{a,b}(x) = ax + b = f_{a,b}(x)$$

Así, $f_{1,0}$ actúa como el elemento identidad en G.

4. **Inversos:** Para cada $f_{a,b} \in G$, se necesita encontrar una función $f_{a',b'} \in G$ tal que:

$$f_{a,b} \circ f_{a',b'} = f_{a',b'} \circ f_{a,b} = f_{1,0}$$

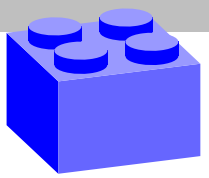
Para $f_{a,b}(x) = ax + b$, se busca $f_{a',b'}(x) = a'x + b'$ tal que:

$$(f_{a,b} \circ f_{a',b'})(x) = f_{1,0}(x) = x$$

$$a(a'x + b') + b = x$$

Esto se descompone en:

$$aa'x + ab' + b = x$$



Para que esto sea igual a x, se necesita que $aa' = 1$ y $ab' + b = 0$. Esto da:

$$a' = \frac{1}{a} \quad \text{y} \quad b' = -\frac{b}{a}$$

Así, la función inversa de $f_{a,b}$ es $f_{a^{-1},-\frac{b}{a}}$, y se nota que esta también pertenece a G porque $a^{-1} \neq 0$.

Por lo tanto, $(G, \circ)$ **es un grupo con la operación de composición de funciones.**

Para mostrar que N es un subgrupo normal de G, se necesita verificar dos cosas:

1. N es un subgrupo de G.
2. N es un subgrupo de G

Recuerde que G es el conjunto de todas las funciones de la forma $f_{a,b}(x) = ax + b$ con $a \neq 0$, y N es el conjunto de todas las funciones de la forma $f_{1,b}(x) = x + b$.

Para que N sea un subgrupo de G, debe cumplir con las siguientes propiedades:

- **Cerradura:** La composición de dos elementos en N también está en N.
- **Identidad:** Existe un elemento identidad en N.
- **Inversos:** Cada elemento en N tiene un inverso en N.

Con base en lo anterior se tiene:

- **Cerradura:** Sean f_{1,b_1} y f_{1,b_2} dos elementos en N. Su composición es:

$$(f_{1,b_1} \circ f_{1,b_2})(x) = f_{1,b_1}(f_{1,b_2}(x)) = f_{1,b_1}(x + b_2) = (x + b_2) + b_1 = x + (b_1 + b_2)$$

  La función resultante f_{1,b_1+b_2} está en N porque es de la forma $x + (b_1 + b_2)$.

- **Identidad:** La función identidad en N es $f_{1,0}(x) = x$. Para cualquier $f_{1,b}(x) = x + b$ en N:

$$(f_{1,0} \circ f_{1,b})(x) = f_{1,0}(x + b) = x + b$$

$$(f_{1,b} \circ f_{1,0})(x) = f_{1,b}(x) = x + b$$

  Así, $f_{1,0}$ actúa como la identidad en N.

- **Inversos:** Para cada $f_{1,b}(x) = x+b$ en N, se tiene que la función $f_{1,-b}$ es su inverso. En efecto:

$$(f_{1,b} \circ f_{1,-b})(x) = f_{1,-b} \circ f_{1,b}(x) = x$$

ya que

$$(f_{1,b} \circ f_{1,-b})(x) = f_{1,b}(x-b) = (x-b)+b = x$$

$$(f_{1,-b} \circ f_{1,b})(x) = f_{1,-b}(x+b) = (x+b)-b = x$$

Por lo tanto, $f_{1,-b}$ es el inverso de $f_{1,b}$ y está en N.

Ahora, para mostrar que N es un subgrupo normal de G, se debe demostrar que para cualquier $g \in G$ y $n \in N$, el conjugado de n por g está en N. Es decir, se necesita mostrar que $g \circ n \circ g^{-1} \in N$.

Sea $g = f_{a,b}$ con $a \neq 0$ y $n = f_{1,c}$. Considere el conjugado $f_{a,b} \circ f_{1,c} \circ f_{a,b}^{-1}$.

Primero, encuentre $f_{a,b}^{-1}$. Se sabe que $f_{a,b}(x) = ax + b$, así que su inverso es:

$$f_{a,b}^{-1}(x) = \frac{x-b}{a}$$

Ahora, calcule el conjugado:

$$(f_{a,b} \circ f_{1,c} \circ f_{a,b}^{-1})(x) = f_{a,b}(f_{1,c}(f_{a,b}^{-1}(x)))$$

Primero se evalúa $f_{a,b}^{-1}(x)$:

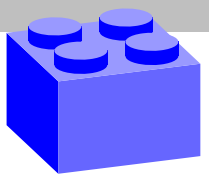
$$f_{a,b}^{-1}(x) = \frac{x-b}{a}$$

Luego se evalúa $f_{1,c}$ en este resultado:

$$f_{1,c}\left(\frac{x-b}{a}\right) = \frac{x-b}{a} + c$$

Finalmente, se evalúa $f_{a,b}$ en este resultado:

$$f_{a,b}\left(\frac{x-b}{a} + c\right) = a\left(\frac{x-b}{a} + c\right) + b = (x-b) + ac + b = x + ac$$



Así, se tiene que:

$$(f_{a,b} \circ f_{1,c} \circ f_{a,b}^{-1})(x) = x + ac$$

Note que $x + ac$ es de la forma $f_{1,ac}(x)$, que está en N. Esto muestra que $g \circ n \circ g^{-1} \in N$ para cualquier $g \in G$ y $n \in N$.

Se ha demostrado que N es un subgrupo normal de G, ya que es cerrado bajo la composición, contiene la identidad, tiene inversos, y es invariante bajo conjugación por cualquier elemento de G.

Para mostrar que $S = \{f_{a,b} \mid a \in \mathbb{Q}, b \in \mathbb{R}\}$ es un subgrupo normal de $G = \{f_{a,b} \mid a \in \mathbb{R}, b \in \mathbb{R}, a \neq 0\}$, se siguen los siguientes pasos:

1. Mostrar que S es un subgrupo de G.
2. Mostrar que S es normal en G.

Para que S sea un subgrupo de G, se debe verificar las tres propiedades de un subgrupo: cerradura, existencia de identidad e inversos.

- **Cerradura:** Sean $f_{a,b}$ y $f_{c,d}$ dos elementos de S, donde $a, c \in \mathbb{Q}$ y $b, d \in \mathbb{R}$. Se quiere ver si la composición $f_{a,b} \circ f_{c,d}$ también está en S.

  $$(f_{a,b} \circ f_{c,d})(x) = f_{a,b}(f_{c,d}(x)) = f_{a,b}(cx + d) = a(cx + d) + b = (ac)x + (ad + b)$$

  Dado que a y c son racionales, su producto ac también es racional. Además, $ad + b$ es real porque es una combinación de números reales. Por lo tanto, $f_{ac,ad+b} \in S$.

- **Identidad:** La función identidad en G es $f_{1,0}(x) = x$. Dado que $1 \in \mathbb{Q}$ y $0 \in \mathbb{R}$, la identidad $f_{1,0}$ está en S.

- **Inversos:** Para cada $f_{a,b} \in S$, se necesita encontrar un $f_{a',b'} \in S$ tal que:

  $$f_{a,b} \circ f_{a',b'} = f_{a',b'} \circ f_{a,b} = f_{1,0}$$

  Se sabe que $f_{a,b}(x) = ax + b$ y se quiere que $f_{a,b} \circ f_{a',b'} = f_{1,0}$. Considere $f_{a',b'}(x) = \frac{x-b}{a}$:

  $$f_{a,b} \circ f_{a',b'}(x) = f_{a,b}\left(\frac{x-b}{a}\right) = a\left(\frac{x-b}{a}\right) + b = x - b + b = x$$

$$f_{a',b'} \circ f_{a,b}(x) = f_{a',b'}(ax+b) = \frac{ax+b-b}{a} = \frac{ax}{a} = x$$

Entonces, $f_{a',b'}(x) = \frac{x-b}{a}$ es el inverso de $f_{a,b}$. Dado que $a \in \mathbb{Q}$, y se tiene que $a' = \frac{1}{a} \in \mathbb{Q}$, y dado que $b \in \mathbb{R}$, entonces $-\frac{b}{a} \in \mathbb{R}$. Por lo tanto, el inverso de $f_{a,b}$ está en S.

Para mostrar que S es un subgrupo normal de G, se debe demostrar que para cualquier $g \in G$ y $s \in S$, el conjugado de s por g está en S. Es decir, se necesita mostrar que $g \circ s \circ g^{-1} \in S$.

Sea $g = f_{\alpha,\beta} \in G$ con $\alpha \in \mathbb{R}, \beta \in \mathbb{R}, \alpha \neq 0$ y $s = f_{a,b} \in S$ con $a \in \mathbb{Q}, b \in \mathbb{R}$. Considere el conjugado $f_{\alpha,\beta} \circ f_{a,b} \circ f_{\alpha,\beta}^{-1}$.

Primero, encuentre $f_{\alpha,\beta}^{-1}$. Se sabe que $f_{\alpha,\beta}(x) = \alpha x + \beta$, así que su inverso es:

$$f_{\alpha,\beta}^{-1}(x) = \frac{x-\beta}{\alpha}$$

Ahora, calcule el conjugado:

$$(f_{\alpha,\beta} \circ f_{a,b} \circ f_{\alpha,\beta}^{-1})(x) = f_{\alpha,\beta}(f_{a,b}(f_{\alpha,\beta}^{-1}(x)))$$

Primero se evalúa $f_{\alpha,\beta}^{-1}(x)$:

$$f_{\alpha,\beta}^{-1}(x) = \frac{x-\beta}{\alpha}$$

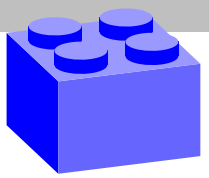
Luego se evalúa $f_{a,b}$ en este resultado:

$$f_{a,b}\left(\frac{x-\beta}{\alpha}\right) = a\left(\frac{x-\beta}{\alpha}\right) + b = \frac{a(x-\beta)}{\alpha} + b$$

Finalmente, se evalúa $f_{\alpha,\beta}$ en este resultado:

$$f_{\alpha,\beta}\left(\frac{a(x-\beta)}{\alpha} + b\right) = \alpha\left(\frac{a(x-\beta)}{\alpha} + b\right) + \beta = a(x-\beta) + \alpha b + \beta = ax - a\beta + \alpha b + \beta$$

Simplificando la expresión:



$$f_{\alpha,\beta} \circ f_{a,b} \circ f_{\alpha,\beta}^{-1}(x) = ax + (\alpha b - a\beta + \beta)$$

Note que el coeficiente de x sigue siendo a, que es racional, y el término constante $\alpha b - a\beta + \beta$ es real porque es una combinación de números reales. Así, la función resultante está en S, ya que es de la forma $f_{a,(\alpha b - a\beta + \beta)}$ con $a \in \mathbb{Q}$.

Se ha demostrado que $S = \{f_{a,b} \mid a \in \mathbb{Q}, b \in \mathbb{R}\}$ es un subgrupo normal de G, ya que es cerrado bajo la composición, contiene la identidad, tiene inversos, y es invariante bajo conjugación por cualquier elemento de G.

□

Solución 2.13.3 (grupo y subgrupo normal) Ver p.155

Para demostrar que el conjunto T es un subgrupo normal de $GL(2,\mathbb{R})$, se necesita primero verificar que T es un subgrupo y luego demostrar que es normal en $GL(2,\mathbb{R})$.

Verificación de Subgrupo

Se Define el conjunto T como:

$$T = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc \neq 0 \right\}.$$

Se quiere verificar que T cumple con las propiedades de un subgrupo:

1. **Cierre:** Para todos $A, B \in T$, $AB \in T$
2. **Elemento identidad**: El elemento identidad $I \in T$.
3. **Inversos:** Para cada $A \in T$, el inverso $A^{-1} \in T$.

Con base en lo anterior se tiene:

1. **Cierre:** Sea $A, B \in T$. Esto significa que A y B son matrices de 2×2 con determinantes no nulos. Se quiere demostrar que $AB \in T$, es decir, que el determinante de AB es no nulo.

   Recuerde que para cualquier par de matrices A y B de 2×2, se cumple la propiedad del determinante:

   $$\det(AB) = \det(A) \cdot \det(B).$$

Dado que $A, B \in T$, se tiene que $\det(A) \neq 0$ y $\det(B) \neq 0$. Entonces,

$$\det(AB) = \det(A) \cdot \det(B) \neq 0.$$

Por lo tanto, $AB \in T$.

2. **Elemento identidad:** El elemento identidad en $GL(2, \mathbb{R})$ es la matriz identidad:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

El determinante de la matriz identidad es:

$$\det(I) = 1 \neq 0.$$

Por lo tanto, $I \in T$.

3. **Inversos:** Sea $A \in T$. Esto significa que A es una matriz de 2×2 con determinante no nulo. Se quiere demostrar que $A^{-1} \in T$, es decir, que el inverso de A tiene un determinante no nulo.

Se sabe que para cualquier matriz invertible A, su inverso A^{-1} existe y se cumple:

$$\det(A^{-1}) = \frac{1}{\det(A)}.$$

Dado que $A \in T$, se tiene que $\det(A) \neq 0$. Entonces,

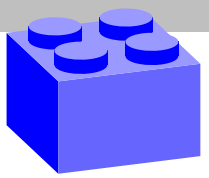
$$\det(A^{-1}) = \frac{1}{\det(A)} \neq 0.$$

Por lo tanto, $A^{-1} \in T$.

Verificación de Normalidad

Para demostrar que T es un subgrupo normal de $GL(2, \mathbb{R})$, se necesita mostrar que para cualquier $A \in GL(2, \mathbb{R})$ y cualquier $B \in T$, el conjugado $ABA^{-1} \in T$.

Sea $A \in GL(2, \mathbb{R})$ y $B \in T$. Se quiere demostrar que $ABA^{-1} \in T$.



Para ello, se calcula el determinante del conjugado:

$$\det(ABA^{-1}) = \det(A)\det(B)\det(A^{-1}).$$

Recuerde que para cualquier matriz A, se cumple:

$$\det(A^{-1}) = \frac{1}{\det(A)}.$$

Entonces,

$$\det(ABA^{-1}) = \det(A)\det(B)\frac{1}{\det(A)} = \det(B).$$

Dado que $B \in T$, se tiene que $\det(B) \neq 0$. Por lo tanto,

$$\det(ABA^{-1}) = \det(B) \neq 0.$$

Esto implica que $ABA^{-1} \in T$. Por lo tanto, T es un subgrupo normal de $GL(2, \mathbb{R})$.

□

Solución 2.13.4 (grupo y subgrupo normal) Ver p.156

La respuesta es que no se puede generalizar la transitividad para subgrupos normales. Para ello considere el grupo alternado A_4, a H un subgrupo de A_4 el cual se define como:

$$H = \{I, (12)(34), (13)(24), (14)(23)\}$$

y a K el siguiente subgrupo de H:

$$K = \{I, (12)(34)\}$$

Observe que el subgrupo H consiste en la identidad y las tres transposiciones dobles. Se verificará que H es un subgrupo normal de A_4.

Normalidad de H en A_4:

- Dado que $H \subseteq A_4$ y H es normal en S_4, H también es normal en A_4 porque cualquier conjugación en A_4 es también una conjugación en S_4.

Por lo tanto, H es normal en A_4, o bien,

$$H \lhd A_4$$

Ahora se quiere verificar si K es un subgrupo normal de H.

Normalidad de K en H:

- K es normal en H porque H es un grupo abeliano. En un grupo abeliano, todos los subgrupos son normales.
- Para cualquier $h \in H$ y $k \in K$, $hkh^{-1} = khh^{-1} = k$. Por lo tanto, $K \triangleleft H$.

¿K es normal en A_4?:

- Hay que verificar si K es normal en A_4 considerando la conjugación por elementos en A_4.
- Tome $k = (12)(34) \in K$ y $a = (123) \in A_4$. Se calcula el conjugado:

$$aka^{-1} = (123)(12)(34)(132) = (13)(24)$$

- El resultado $(13)(24)$ no está en K ya que $K = \{I, (12)(34)\}$.

Esto muestra que K no es normal en A_4:

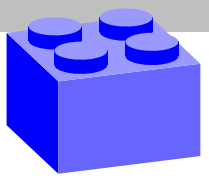
$$K \not\triangleleft A_4$$

Este contraejemplo muestra que, aunque K sea normal en H y H sea normal en $G = A_4$, no necesariamente implica que K sea normal en $G = A_4$.

A continuación, se calcularan los normalizadores de varios subconjuntos en un grupo de simetrías, que para fines ilustrativos, se trata del grupo de simetrías de un cuadrado (grupo diédrico D_4).

1. **Normalizador de $\{I, r_1\}$**

- **Subgrupo:** $\{I, r_1\}$ contiene la identidad y una rotación de 90°.
- **Normalizador:** Dado que r_1 no conmuta con todas las reflexiones o rotaciones que no sean de 90° múltiplos (como r_2 o r_3), su normalizador estará formado por elementos que al actuar por conjugación sobre r_1 den como resultado r_1 o r_1^{-1}.
- **Resultado:** $N_G(\{I, r_1\}) = \{I, r_1, r_2, r_3\}$, que son todas las rotaciones.



2.**Normalizador de** $\{I, r_1, r_2, r_3\}$

- **Subgrupo:** $\{I, r_1, r_2, r_3\}$ es el subgrupo de todas las rotaciones.
- **Normalizador:** Cualquier elemento del grupo D_4 conjugando un elemento de este subconjunto resulta en otro elemento dentro del subconjunto, debido a la naturaleza abeliana de las rotaciones dentro de D_4.
- **Resultado:** $N_G(\{I, r_1, r_2, r_3\}) = D_4$.

3.**Normalizador de** $\{I, d_1\}$

- **Subgrupo:** $\{I, d_1\}$ incluye la identidad y una reflexión específica.
- **Normalizador**: Los elementos que al actuar por conjugación sobre d_1 lo mantienen o invierten. En el caso del grupo diédrico, las reflexiones son conjugadas de otras por rotaciones.
- **Resultado:** $N_G(\{I, d_1\})$ incluirá las dos reflexiones que son simétricas respecto al eje de d_1 y las rotaciones que son simetrías respecto a ese eje, es decir, $\{I, r_2, d_1, d_3\}$ donde r_2 es una rotación de 180° y d_3 es la reflexión perpendicular a d_1.

Estos cálculos asumen un entendimiento estándar del grupo diédrico D_4 y sus operaciones de simetría.

□

Solución 2.13.5 (grupo y subgrupo normal) Ver p.156

Para demostrar que un subgrupo S de índice 2 en un grupo finito G es normal, es decir, que las clases izquierdas y derechas son las mismas, se puede seguir un argumento basado en la estructura de las clases laterales y la aritmética de grupos.

Propiedades de los subgrupos de índice 2

1.**Índice de un subgrupo:** El índice de un subgrupo S en G, denotado $[G : S]$, es el número de clases laterales distintas de S en G. Si S tiene índice 2 en G, entonces hay exactamente dos clases laterales de S en G.

2.**Clases Laterales:** Las clases laterales de S en G pueden ser izquierdas o derechas. Dado que S tiene índice 2, esto significa que además de S mismo, hay exactamente una otra clase lateral, ya sea izquierda o derecha. Si $a \notin S$, entonces las clases laterales son:

- Clase lateral izquierda: aS
- Clase lateral derecha: Sa

Demostración de que S es Normal

Suponga que $a \notin S$: Si esto sucede, entonces, como S tiene índice 2, las clases laterales de S deben cubrir todo G. Esto significa que G se puede escribir como la unión disjunta de S y aS (o Sa). Es decir, $G = S \cup aS = S \cup Sa$.

Demostración de que las clases izquierdas y derechas son iguales: Dado que G es finito y S tiene índice 2, cada elemento de G que no está en S debe estar en aS y en Sa. Por lo tanto, $aS = Sa$.

Si $aS = Sa$, entonces para cualquier elemento $s \in S$, $as \in aS$ y $as \in Sa$. Esto implica que $aSa^{-1} = S$ La igualdad $aSa^{-1} = S$ muestra que para cualquier $a \in G$, $aSa^{-1} \subseteq S$. Como S y aS (o Sa) cubren todo G, y $S = aSa^{-1}$, S es normal en G.

Conclusión

Dado que S tiene índice 2 en G, las clases laterales izquierdas aS y las clases laterales derechas Sa son iguales para cualquier $a \in G$. Esto implica que S es normal en G (es decir, $aSa^{-1} = S$ para todo $a \in G$). En términos grupales, un subgrupo de índice 2 es siempre normal porque sus clases laterales (izquierda y derecha) coinciden necesariamente, cubriendo todo el grupo sin solapamiento más allá de S mismo. □

Ver p.156

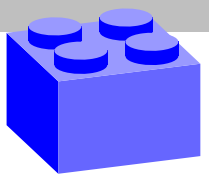
Solución 2.13.6 (grupo y subgrupo normal)

Cuando N es un subgrupo normal de un grupo finito G, hay una relación muy específica entre los órdenes de G, el grupo cociente G/N, y N. Esta relación es expresada por el teorema de Lagrange se clarifica mediante el concepto de grupo cociente, es decir:

$$\text{ord}(N) \text{ divide a ord}(G)$$

Dado que N es un subgrupo normal de G, se puede formar el grupo cociente G/N.

Este grupo está compuesto por las clases laterales de N en G. Cada elemento de G/N es una clase lateral de la forma gN para algún $g \in G$.



Así, el orden del grupo cociente G/N, que se denota como ord(G/N), es igual al número de clases laterales de N en G. Según el teorema de Lagrange, se tiene que:

$$\text{ord}(G/N) = \frac{\text{ord}(G)}{\text{ord}(N)}$$

Se concluye que el producto del orden del subgrupo normal N y el orden del grupo cociente G/N es igual al orden de G, o bien

$$\text{ord(G)} = \text{ord}(N)\text{ord}(G/N)$$

□

Solución 2.13.7 (grupo y subgrupo normal) Ver p.156

Para demostrar que AB es un subgrupo de G, donde A es un subgrupo de G y B es un subgrupo normal de G, se siguen los pasos estándares para demostrar que un subconjunto de un grupo es, de hecho, un subgrupo. En particular, se debe demostrar que AB cumple con las tres propiedades básicas de un subgrupo:

1. **Cierre:** Si $x, y \in AB$, entonces $xy \in AB$.

2. **Identidad:**: El elemento identidad de G, denotado como e, debe estar en AB.

3. **Inversos**: Si $x \in AB$, entonces $x^{-1} \in AB$.

Con base en lo anterior se tiene

1. **Cierre:** Sean x y y dos elementos arbitrarios de AB. Por definición de AB, existen $a, a' \in A$ y $b, b' \in B$ tales que $x = ab$ y $y = a'b'$. Se debe mostrar que su producto, xy, también pertenece a AB.

   $$xy = (ab)(a'b') = aba'b'$$

   Dado que B es normal en G, se puede reorganizar los términos que involucran elementos de B. La normalidad de B implica que para todo $g \in G$ y $b \in B$, $gbg^{-1} \in B$. Por tanto, se puede escribir $ba' = a''b''$ para algunos $a'' \in A$ y $b'' \in B$ ya que $a' \in A \subseteq G$ y A es un subconjunto de G. Entonces,

   $$xy = aba'b' = a(a'b)b' = aa''b''b' = (aa'')b''b'$$

   Como $aa'' \in A$ (porque A es subgrupo y cerrado bajo la operación), y $b''b' \in B$ (porque B es subgrupo y cerrado bajo la operación), entonces $xy = (aa'')(b''b') \in AB$. Por lo tanto, AB es cerrado bajo la operación.

2. **Identidad:** El elemento identidad e de G debe estar en AB. Note que $e = ee$, donde e es también el elemento identidad para A y B, ya que ambos son subgrupos de G. Como $e \in A$ y $e \in B$, entonces $e \in AB$.

3. **Inversos:** Sea $x \in AB$, entonces $x = ab$ para algún $a \in A$ y $b \in B$. Se quiere demostrar que x^{-1} también está en AB. Note que

$$x^{-1} = (ab)^{-1} = b^{-1}a^{-1}$$

Dado que B es normal y $a^{-1} \in G$, $b^{-1}a^{-1} = a'b'$ para algunos $a' \in A$ y $b' \in B$. Por lo tanto, $x^{-1} \in AB$.

Por lo tanto, se ha demostrado que AB es un subgrupo de G.

□

Ver p.156

Solución 2.13.8 (grupo y subgrupo normal)

Para probar que el conjunto C, definido como el conjunto de todos los productos finitos de conmutadores de elementos de G, es un subgrupo de G, se necesita verificar que C satisface las propiedades de un subgrupo:

1. **Cierre:** Si $x, y \in C$, entonces $xy \in C$.

2. **Identidad:** El elemento identidad e de G debe estar en C.

3. **Inversos:** Si $x \in C$, entonces $x^{-1} \in C$.

Con base en lo anterior se tiene

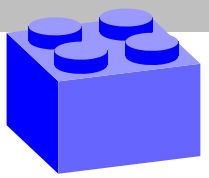
1. **Cierre:** Considere x y y en C. Por definición, x y y son productos finitos de conmutadores en G. Es decir,

$$x = [a_1, b_1][a_2, b_2] \dots [a_m, b_m]$$

y

$$y = [c_1, d_1][c_2, d_2] \dots [c_n, d_n]$$

donde $a_i, b_i, c_j, d_j \in G$.



El producto xy será:

$$xy = [a_1, b_1][a_2, b_2] \dots [a_m, b_m][c_1, d_1][c_2, d_2] \dots [c_n, d_n]$$

Como xy también es un producto finito de conmutadores en G, xy pertenece a C. Esto demuestra que C es cerrado bajo la operación de multiplicación de G.

2. **Identidad:** El elemento identidad e en G se puede expresar como un conmutador de cualquier elemento consigo mismo. Es decir,

$$e = [a, a] = aa^{-1}aa^{-1} = e$$

Así que e es también un conmutador, y por tanto, $e \in C$.

3. **Inversos:** Sea x un elemento de C. Entonces,

$$x = [a_1, b_1][a_2, b_2] \dots [a_m, b_m]$$

El inverso de x se calcula como:

$$x^{-1} = ([a_m, b_m]^{-1} \dots [a_2, b_2]^{-1}[a_1, b_1]^{-1})$$

Dado que el inverso de un conmutador $[a, b] = aba^{-1}b^{-1}$ es $[a, b]^{-1} = [b, a]$, que también es un conmutador, cada $[a_i, b_i]^{-1}$ en x^{-1} es $[b_i, a_i]$, y por lo tanto x^{-1} es también un producto finito de conmutadores. Esto significa que $x^{-1} \in C$.

Por lo tanto, C es un subgrupo de G.

Para demostrar que el subgrupo C, que consiste en todos los productos finitos de conmutadores de un grupo G, es normal en G, se necesita mostrar que para cualquier $g \in G$ y cualquier $c \in C$, el conjugado gcg^{-1} pertenece a C. Esto se puede hacer utilizando propiedades de conmutadores y la estructura de C.

Una propiedad clave de los conmutadores es que los conjugados de conmutadores también son conmutadores. Específicamente, para cualquier $g, a, b \in G$, el conjugado del

conmutador $[a, b]$ por g es:

$$g[a,b]g^{-1} = g(aba^{-1}b^{-1})g^{-1} = (gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1} = [gag^{-1}, gbg^{-1}]$$

Con base en esto, considere un elemento $c \in C$. Por definición, c es un producto finito de conmutadores. Suponga que:

$$c = [a_1, b_1][a_2, b_2] \cdots [a_n, b_n]$$

donde $a_i, b_i \in G$. Se quiere mostrar que $gcg^{-1} \in C$. Considere:

$$gcg^{-1} = g([a_1, b_1][a_2, b_2] \cdots [a_n, b_n])g^{-1}$$

Usando la propiedad de los conjugados de productos, se puede distribuir la conjugación sobre el producto:

$$gcg^{-1} = (g[a_1, b_1]g^{-1})(g[a_2, b_2]g^{-1}) \cdots (g[a_n, b_n]g^{-1})$$

Como se mencionó anteriormente, para cada conmutador $[a_i, b_i]$:

$$g[a_i, b_i]g^{-1} = [ga_ig^{-1}, gb_ig^{-1}]$$

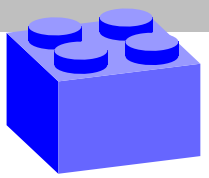
Así que:

$$gcg^{-1} = [ga_1g^{-1}, gb_1g^{-1}][ga_2g^{-1}, gb_2g^{-1}] \cdots [ga_ng^{-1}, gb_ng^{-1}]$$

Cada término en el producto gcg^{-1} es un conmutador, y por lo tanto gcg^{-1} es un producto finito de conmutadores. Por la definición de C, esto significa que $gcg^{-1} \in C$. Con esto, se ha demostrado que para cualquier $g \in G$ y cualquier $c \in C$, el elemento $gcg^{-1} \in C$. Esto prueba que C es un subgrupo normal de G, o bien,

$$C \triangleleft G$$

Para mostrar que el grupo cociente G/C es abeliano, se necesita probar que cualquier par de elementos en G/C conmutan. Recuerde que C es el subgrupo conmutador de G, definido como el conjunto generado por todos los conmutadores $[a, b] = aba^{-1}b^{-1}$ para $a, b \in G$. Dicho de otra forma, C contiene exactamente los elementos de G que son



necesarios para çorregir"la falta de conmutatividad entre cualesquiera dos elementos en G.

Propiedades del Grupo Cociente G/C

En el grupo cociente G/C, los elementos son las clases laterales de la forma gC para cada $g \in G$. El producto de dichas clases laterales se define como:

$$(gC)(hC) = (gh)C$$

Comprobación de la Conmutatividad

Para demostrar que G/C es abeliano, se necesita verificar que:

$$(gC)(hC) = (hC)(gC)$$

para todos $g, h \in G$.

Aplicando la definición del producto de clases laterales, esto se reduce a demostrar que:

$$(gh)C = (hg)C$$

o equivalentemente, que:

$$gh(hg)^{-1} \in C$$

Calculando el elemento $gh(hg)^{-1}$:

$$gh(hg)^{-1} = gh(g^{-1}h^{-1}) = ghg^{-1}h^{-1}$$

El término $ghg^{-1}h^{-1}$ es precisamente el conmutador $[g, h]$. Por definición, C es el subgrupo generado por todos los conmutadores de G, lo que implica que cualquier conmutador $[g, h]$ está en C.

Dado que $[g, h] = ghg^{-1}h^{-1} \in C$, se tiene que:

$$(gh)C = (hg)C$$

y por lo tanto:

$$(gC)(hC) = (hC)(gC)$$

Esto muestra que G/C es abeliano.

Cualquier par de elementos en G/C conmutan, por lo que la operación en G/C es conmutativa.

La razón subyacente de esta propiedad es que al factorizar G por C, se está eliminando todos los .ºbstáculos.ª la conmutatividad en G. El grupo cociente G/C çolapsa"todas las distinciones entre elementos que no conmutan en G al nivel de sus conmutadores, lo que hace que el grupo resultante sea abeliano.

Para demostrar que el inverso de un conmutador es también un conmutador, considere un conmutador genérico en un grupo G. Recuerde primero la definición de un conmutador para elementos a y b en G:

$$[a, b] = aba^{-1}b^{-1}$$

Se quiere encontrar el inverso de $[a, b]$ y mostrar que este inverso puede expresarse como un conmutador de dos elementos de G. De esta forma

1. **Encontrar el inverso de** $[a, b]$: El inverso de un elemento en un grupo, dado por g, se define como el elemento g^{-1} tal que $gg^{-1} = g^{-1}g = e$, donde e es el elemento identidad del grupo. Aplicando esta definición al conmutador $[a, b]$, se tiene:

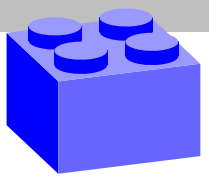
   $$[a, b]^{-1} = (aba^{-1}b^{-1})^{-1}$$

   Usando la propiedad de que el inverso de un producto es el producto de los inversos en orden inverso, se obtiene:

   $$[a, b]^{-1} = (b^{-1})^{-1}(a^{-1})^{-1}b^{-1}a^{-1} = bab^{-1}a^{-1}$$

2. **Demostrar que el inverso es un conmutador:** Ahora, se desea expresar $[a, b]^{-1}$ como un conmutador. Observe la expresión obtenida:

   $$[a, b]^{-1} = bab^{-1}a^{-1}$$



Se puede reordenar esta expresión para hacerla aparecer como un conmutador de b y a, pero con a y b intercambiados y en el orden inverso para uno de los elementos. Esto es

$$[a,b]^{-1} = bab^{-1}a^{-1} = [b,a]$$

Así, se ha mostrado que el inverso del conmutador $[a,b]$ es igual al conmutador $[b,a]$. Esto prueba que el inverso de un conmutador es también un conmutador.

□

Solución 2.13.9 (grupo y subgrupo normal) Ver p.157

Para demostrar que si H y K son subgrupos normales de un grupo G tales que $H \cap K = \{e\}$, entonces cualquier par de elementos $h \in H$ y $k \in K$ conmutan, es decir, $hk = kh$, se puede utilizar la teoría de conmutadores y propiedades de los subgrupos normales. Recordando:

1. **Normalidad de H y K:** Dado que H y K son subgrupos normales de G, se tiene que para cualquier $g \in G$, $h \in H$, y $k \in K$:

$$ghg^{-1} \in H \quad \text{y} \quad gkg^{-1} \in K$$

2. **Definición del conmutador:** El conmutador de dos elementos a y b en G está definido como:

$$[a,b] = aba^{-1}b^{-1}$$

Con base en lo anterior, sucede que el conmutador de $h \in H$ y $k \in K$ es:

$$[h,k] = hkh^{-1}k^{-1}$$

Por la normalidad de H y K, se tiene que:

- Si $hkh^{-1} \in K$ y $k^{-1} \in K$ entonces $(hkh^{-1})k^{-1} \in K \Leftrightarrow hkh^{-1}k^{-1} = [h,k] \in K$
- Si $h \in H$ y $kh^{-1}k^{-1} \in H$ entonces $h(kh^{-1}k^{-1}) \in H \Leftrightarrow hkh^{-1}k^{-1} = [h,k] \in H$

Por ende, $[h,k] \in H \cap K$.

Dado que $H \cap K = \{e\}$, esto significa que el único elemento común entre H y K es el elemento identidad e. Entonces, debe ser el caso que:

$$hkh^{-1}k^{-1} = e$$

Esto implica directamente que:

$$hk = kh$$

Esto muestra que cualquier $h \in H$ y $k \in K$ conmuta.

□

Ver p.157

Solución 2.13.10 (grupo y subgrupo normal)

Para demostrar que la intersección de todos los subgrupos de orden s de un grupo G es un subgrupo normal de G se puede proceder de la siguiente manera:

Denotación y definición

Sea $\mathcal{H}$ el conjunto de todos los subgrupos de G de orden s. Suponga que $\mathcal{H} \neq \emptyset$ (dado que G contiene al menos un subgrupo de orden s). Definina N como la intersección de todos los subgrupos en $\mathcal{H}$:

$$N = \bigcap_{H \in \mathcal{H}} H$$

N es un subgrupo

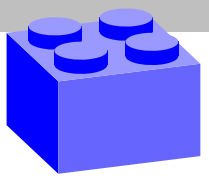
Para demostrar que N es un subgrupo, se necesita verificar que N cumple las propiedades básicas de un subgrupo:

- **Cerradura bajo la operación:** Si $x, y \in N$, entonces x, y están en cada subgrupo $H \in \mathcal{H}$. Como cada H es un subgrupo, $xy \in H$ para cada H, y por lo tanto $xy \in N$.
- **Existencia del elemento identidad**: El elemento identidad e de G está en cada subgrupo de G, por lo que $e \in N$.
- **Existencia de inversos**: Si $x \in N$, entonces x está en cada $H \in \mathcal{H}$. Como cada H es un subgrupo, $x^{-1} \in H$ para cada H, y por lo tanto $x^{-1} \in N$.

Esto demuestra que N es un subgrupo.

N es normal en G

Para demostrar que N es normal en G, considere un elemento arbitrario $g \in G$ y se demostrará que



$gNg^{-1} \subseteq N$.

Argumento clave

1. **Conjugación y permutación de subgrupos:** Dado que H es un subgrupo de orden s y $g \in G$, el conjugado de H por g es:
$$gHg^{-1} = \{ghg^{-1} \mid h \in H\}$$
El conjunto gHg^{-1} es también un subgrupo de G y tiene el mismo orden s, porque la conjugación por g reordena los elementos de H pero no cambia su cantidad.

2. **Conjugación y la intersección**: Para cualquier $x \in N$, x pertenece a todos los subgrupos de $\mathcal{H}$. Entonces, para cualquier $H \in \mathcal{H}$, $x \in H$. Considere el conjugado gxg^{-1} para algún $g \in G$:
$$gxg^{-1} \in gHg^{-1}$$
Dado que gHg^{-1} es también un subgrupo de orden s, pertenece a $\mathcal{H}$.

3. **Pertinencia a la intersección**: Ya que $gHg^{-1} \in \mathcal{H}$ para cada $H \in \mathcal{H}$, y $x \in H$ implica que $gxg^{-1} \in gHg^{-1}$, esto debe ser cierto para todos los subgrupos $H \in \mathcal{H}$. Por lo tanto, gxg^{-1} pertenece a todos los subgrupos de $\mathcal{H}$.

Conclusión

Dado que $gxg^{-1} \in H$ para cada $H \in \mathcal{H}$, se sigue que $gxg^{-1} \in N$. Esto demuestra que $gNg^{-1} \subseteq N$, lo que implica que N es un subgrupo normal de G.

Por lo tanto, la intersección de todos los subgrupos de orden s en G es un subgrupo normal de G.

□

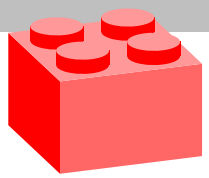
Solución 2.13.11 (grupo y subgrupo normal)

Ver p.157

Para demostrar que si H es un subgrupo de G y N es un subgrupo normal de G, entonces $H \cap N$ es un subgrupo normal de H, se seguirán los pasos siguientes:

Paso 1: $H \cap N$ es un subgrupo de H

En efecto,



Soluciones

1. **Identidad**: Como $e \in H$ y $e \in N$ (donde e es el elemento identidad de G), entonces $e \in H \cap N$.

2. **Cerradura:** Si $x, y \in H \cap N$, entonces $x, y \in H$ y $x, y \in N$. Dado que H y N son subgrupos, $xy \in H$ y $xy \in N$, por lo que $xy \in H \cap N$.

3. **Inversos**: Si $x \in H \cap N$, entonces $x \in H$ y $x \in N$. Dado que H y N son subgrupos, $x^{-1} \in H$ y $x^{-1} \in N$, por lo que $x^{-1} \in H \cap N$.

Esto demuestra que $H \cap N$ es un subgrupo de H.

Paso 2: $H \cap N$ es un subgrupo normal de H

Para demostrar que $H \cap N$ es un subgrupo normal de H, se necesita mostrar que para todo $h \in H$ y todo $x \in H \cap N$, se cumple que $hxh^{-1} \in H \cap N$.

Dado que $x \in H \cap N$, se tiene $x \in N$. Dado que N es normal en G, se cumple que $hxh^{-1} \in N$ para cualquier $h \in G$. Como $h \in H \subseteq G$, también se tiene que $hxh^{-1} \in N$.

Además, dado que $x \in H \cap N$, se tiene $x \in H$. Como $h, x \in H$ y H es un subgrupo, $hxh^{-1} \in H$.

Por lo tanto, $hxh^{-1} \in H \cap N$. Esto demuestra que $H \cap N$ es normal en H.

Ejemplo de que $H \cap N$ no necesariamente es normal en G

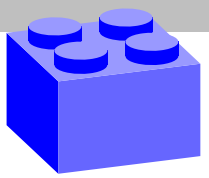
Considere el grupo simétrico $G = S_3$ y $N = G$. El grupo S_3 es el grupo de todas las permutaciones de tres elementos y tiene orden 6.

Tome un subgrupo H de orden 2, por ejemplo, $H = \{e, (12)\}$. Aquí (12) es la permutación que intercambia los elementos 1 y 2.

$H \cap N = H \cap S_3 = H$, ya que $N = S_3$.

Se quire ver si $H \cap N$ (que es igual a H) es normal en G.

Recuerde que para ser normal, para cualquier $g \in G$ y $h \in H$, ghg^{-1} debe estar en H.



Considere $g = (123) \in S_3$ y $h = (12) \in H$:

$$(123)(12)(321) = (132)$$

(132) no está en $H = \{e, (12)\}$, por lo que H no es normal en G.

□

Solución 2.13.12 (grupo y subgrupo normal) Ver p.158

Para demostrar que cada grupo G es normal en sí mismo y que el grupo cociente G/G es trivial, se procede en dos partes:

Parte 1: G es normal en sí mismo

Un subgrupo N de un grupo G es normal si para cada $g \in G$ y cada $n \in N$, el conjugado $gng^{-1} \in N$.

Para demostrar que G es normal en sí mismo, se debe mostrar que para cualquier $g \in G$ y cualquier $x \in G$, el elemento gxg^{-1} está en G. Esto es evidente, ya que gxg^{-1} es un elemento de G y G contiene todos sus propios elementos.

Formalmente, se puede escribir:

$$\text{Para cualquier } g \in G \text{ y cualquier } x \in G, \quad gxg^{-1} \in G$$

Esto cumple la definición de normalidad, y por lo tanto, G es normal en sí mismo:

$$G \lhd G$$

Parte 2: G/G es trivial

El grupo cociente G/G está formado por las clases laterales de G en sí mismo. La clase lateral izquierda de cualquier elemento $g \in G$ es:

$$gG = \{gx \mid x \in G\} = G$$

Esto significa que todas las clases laterales de G en sí mismo son simplemente G. Por lo tanto, hay exactamente una clase lateral en G/G, que es G mismo.

En otras palabras, el grupo cociente G/G contiene exactamente un elemento, la clase lateral de G. Es-

te grupo cociente es el grupo trivial, que se denota usualmente como $\{e\}$ donde e es el elemento identidad.

Se puede expresar esto formalmente como:

$$G/G = \{eG\} = \{G\}$$

□

Ver p.158

Solución 2.13.13 (grupo y subgrupo normal)

Para demostrar que si N es un subgrupo normal de G y H es un subgrupo de G, entonces HN definido como

$$HN := \{hn \mid h \in H, n \in N\}$$

es un subgrupo de G, se debe verificar que HN cumple con las propiedades de un subgrupo: cerradura bajo la operación, existencia del elemento identidad, y cerradura bajo la inversión.

Propiedades de un subgrupo

1. **Cerradura:** Sea $x, y \in HN$. Entonces, existen $h_1, h_2 \in H$ y $n_1, n_2 \in N$ tales que $x = h_1n_1$ y $y = h_2n_2$.

   Para la prueba, considere el producto xy:

   $$xy = (h_1n_1)(h_2n_2)$$

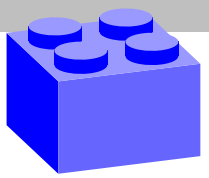
   Usando la asociatividad de la operación del grupo G, se tiene:

   $$xy = h_1(n_1h_2)n_2$$

   Dado que N es normal en G, el producto n_1h_2 puede ser escrito como h_2n_1' para algún $n_1' \in N$ (específicamente, $n_1h_2 = h_2(h_2^{-1}n_1h_2) = h_2n_1'$). Por lo tanto:

   $$xy = h_1h_2n_1'n_2$$

   Dado que $h_1, h_2 \in H$ y H es un subgrupo, $h_1h_2 \in H$. Asimismo, dado que $n_1', n_2 \in N$ y N es un



subgrupo, $n_1' n_2 \in N$. Así, se puede escribir:

$$xy = (h_1 h_2)(n_1' n_2) \in HN$$

Esto muestra que HN es cerrado bajo la operación de G.

2. **Existencia del elemento identidad:**

3. El elemento identidad e de G se puede expresar como $e = ee$ donde $e \in H$ y $e \in N$ (ya que ambos son subgrupos y contienen el elemento identidad).

   Por lo tanto, el elemento identidad $e \in HN$.

4. **Cerradura bajo la inversión:** Sea $x \in HN$. Entonces, existe $h \in H$ y $n \in N$ tales que $x = hn$.

   Para la prueba, considere el inverso de x:

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

   Dado que $n \in N$ y N es un subgrupo, $n^{-1} \in N$. Asimismo, dado que $h \in H$ y H es un subgrupo, $h^{-1} \in H$.

   Entonces, se necesita ver si $n^{-1}h^{-1} \in HN$.

   Usando la propiedad de normalidad de N, se sabe que para $h^{-1} \in H$ y $n^{-1} \in N$, $h^{-1}n^{-1}(h^{-1})^{-1} = h^{-1}n^{-1}h \in N$. Entonces se puede escribir $h^{-1}n^{-1} = n'h^{-1}$ para algún $n' \in N$.

   Por lo tanto:

   $$x^{-1} = n^{-1}h^{-1} = h^{-1}n' \in HN$$

   Esto muestra que $x^{-1} \in HN$.

Por lo tanto, HN es un subgrupo de G.

□

Solución 2.13.14 (grupo y subgrupo normal) Ver p.158

Para demostrar que si N es un subgrupo normal de G y H es un subgrupo de G, entonces N es un subgrupo normal de HN, sigamos los siguientes pasos:

Paso 1: HN es un subgrupo de G

Como ya se ha demostrado anteriormente, si H es un subgrupo de G y N es un subgrupo normal de G, entonces HN es un subgrupo de G.

Paso 2: Demostración de que N es un subgrupo normal de HN

Para demostrar que N es un subgrupo normal de HN, se necesita demostrar que para cualquier $x \in HN$ y $n \in N$, se cumple que $xnx^{-1} \in N$.

Sea $x \in HN$. Por definición, se puede escribir x como $x = h_1 n_1$ para algún $h_1 \in H$ y $n_1 \in N$.

Ahora considere el conjugado de $n \in N$ por x:

$$xnx^{-1} = (h_1 n_1)n(n_1^{-1} h_1^{-1})$$

Se debe analizar esta expresión paso a paso:

1. **Conjugación de n por n_1**: Como $n_1 \in N$ y N es un subgrupo (de hecho, un subgrupo normal) de G, sabemos que $n_1 n n_1^{-1} \in N$.

2. **Conjugación de $n_1 n n_1^{-1}$ por h_1**: Como $h_1 \in H$ y N es un subgrupo normal de G, se sabe que h_1 permuta N dentro de G. Es decir, $h_1(n_1 n n_1^{-1})h_1^{-1} \in N$.

   Ahora combinando estos pasos:

   $$xnx^{-1} = (h_1 n_1)n(n_1^{-1} h_1^{-1})$$

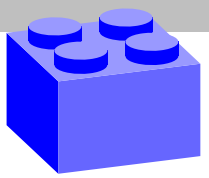
   Primero se calcula $n_1 n n_1^{-1} \in N$ y luego se conjuga el resultado por h_1:

   $$xnx^{-1} = h_1(n_1 n n_1^{-1})h_1^{-1}$$

   Debido a que N es normal en G y el resultado $n_1 n n_1^{-1} \in N$, al conjugar esto por h_1, dado que $h_1 \in H \subseteq G$, se obtiene que:

   $$h_1(n_1 n n_1^{-1})h_1^{-1} \in N$$

   Por lo tanto, $xnx^{-1} \in N$ para cualquier $x \in HN$ y $n \in N$.



Se ha demostrado que N es un subgrupo normal de HN. Para cualquier $x \in HN$ y $n \in N$, el elemento conjugado xnx^{-1} permanece en N. Esto cumple la definición de normalidad, y por lo tanto, $N \triangleleft HN$.

□

Solución 2.13.15 (grupo y subgrupo normal) Ver p.158

HK es un subgrupo normal de G si y solo si $HK = KH$

Demostración:

($\Rightarrow$) Si HK es un subgrupo normal de G, entonces $HK = KH$:

Si HK es un subgrupo normal de G, entonces para cualquier $g \in G$ y cualquier $x \in HK$, se tiene que $gxg^{-1} \in HK$.

Considere un elemento $h \in H$ y un elemento $k \in K$. Entonces, $hk \in HK$. Como HK es normal, para cualquier $g \in G$, se cumple:

$$ghkg^{-1} = h'k' \in HK$$

$$(ghg^{-1})(gkg^{-1}) = h'k' \in HK$$

Dado que $ghg^{-1} \in H$ (porque H es normal en G) y $gkg^{-1} \in K$ (porque K es normal en G), se puede escribir:

$$ghg^{-1} \cdot k \in HK \text{ y } hkg^{-1} \in HK$$

Es decir, cualquier producto de la forma $ghg^{-1}k$ y hkg^{-1} puede ser escrito como un elemento en HK.

Ahora, para mostrar que $HK = KH$, considere $h \in H$ y $k \in K$. Se quiere ver que $hk \in KH$. Dado que H es normal, se tiene que:

$$k^{-1}hk = h' \in H$$

lo que implica que:

$$hk = kh' \in KH$$

Dado que esto es cierto para cualquier $h \in H$ y $k \in K$, se concluye que:

$$HK = KH$$

($\Leftarrow$) Si $HK = KH$, entonces HK es un subgrupo normal de G:

Suponga que $HK = KH$. Se quiere demostrar que HK es un subgrupo normal de G. Para esto, tome cualquier $g \in G$ y cualquier $x \in HK$. Se debe mostrar que $gxg^{-1} \in HK$.

Sea $x \in HK$. Entonces $x = h_1k_1$ para algún $h_1 \in H$ y $k_1 \in K$. Considere:

$$gxg^{-1} = g(h_1k_1)g^{-1} = (gh_1g^{-1})(gk_1g^{-1})$$

Dado que H y K son subgrupos normales de G, se tiene:

$$gh_1g^{-1} \in H \quad \text{y} \quad gk_1g^{-1} \in K$$

Por lo tanto:

$$gxg^{-1} = (gh_1g^{-1})(gk_1g^{-1}) \in HK$$

Esto muestra que HK es invariante bajo conjugación por cualquier elemento de G, por lo tanto, HK es un subgrupo normal de G.

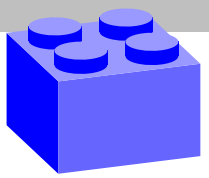
Si H es normal, entonces HK es un subgrupo

Demostración:

Si H es normal en G, entonces para cualquier $k \in K$, el conjugado kHk^{-1} está contenido en H. Se desea mostrar que HK es un subgrupo de G.

Para esto, se verifican las propiedades de un subgrupo:

- **Cerradura**: Sea $x, y \in HK$. Entonces $x = h_1k_1$ y $y = h_2k_2$ para algunos $h_1, h_2 \in$



H y $k_1, k_2 \in K$. Considere el producto:

$$xy = (h_1k_1)(h_2k_2) = h_1(k_1h_2k_1^{-1})k_1k_2$$

Dado que H es normal en G, $k_1h_2k_1^{-1} \in H$. Entonces, se puede escribir:

$$xy = h_1h_3k_1k_2 \quad \text{para algún } h_3 \in H$$

Como $h_1h_3 \in H$ y $k_1k_2 \in K$, se tiene que $xy \in HK$.

- **Identidad:** El elemento identidad e de G puede escribirse como $e = ee$ donde $e \in H$ y $e \in K$. Por lo tanto, $e \in HK$.
- **Inversos**: Sea $x \in HK$. Entonces $x = hk$ para algún $h \in H$ y $k \in K$.

Considere el inverso de x:

$$x^{-1} = (hk)^{-1} = k^{-1}h^{-1}$$

Dado que $k^{-1} \in K$ y $h^{-1} \in H$, y H es normal en G, se tiene que:

$$k^{-1}h^{-1} = h'k' \quad \text{para algún } h' \in H \text{ y } k' \in K$$

Por lo tanto, $x^{-1} \in HK$.

Esto muestra que HK es un subgrupo de G.

Si H y K son normales, entonces HK es un subgrupo normal

Demostración:

Dado que H y K son subgrupos normales de G, se quiere demostrar que HK es un subgrupo normal de G.

De la primer parte, se sabe que si H y K son normales, entonces $HK = KH$. Ahora, se necesita mostrar que HK es un subgrupo normal de G.

Para esto, tome cualquier $g \in G$ y cualquier $x \in HK$. Se debe mostrar que $gxg^{-1} \in HK$.

Sea $x \in HK$. Entonces $x = h_1k_1$ para algún $h_1 \in H$ y $k_1 \in K$. Considere:

$$gxg^{-1} = g(h_1k_1)g^{-1} = (gh_1g^{-1})(gk_1g^{-1})$$

Dado que H y K son subgrupos normales de G, sucede que:

$$gh_1g^{-1} \in H \quad \text{y} \quad gk_1g^{-1} \in K$$

Por lo tanto:

$$gxg^{-1} = (gh_1g^{-1})(gk_1g^{-1}) \in HK$$

Esto muestra que HK es invariante bajo conjugación por cualquier elemento de G, y por lo tanto, HK es un subgrupo normal de G.

□

Ver p.159

Solución 2.13.16 (grupo y subgrupo normal)

Para determinar el conjunto de conmutadores del grupo G, considere las matrices en G. El grupo G está compuesto por matrices de la forma

$$G = \left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \mid a \in \mathbb{R},\ b \in \mathbb{R},\ b \neq 0 \right\}.$$

Para encontrar el conjunto de conmutadores, se necesita considerar el conmutador de dos elementos A y B en G. Sea

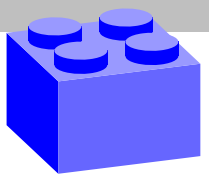
$$A = \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \quad \text{y} \quad B = \begin{pmatrix} 1 & c \\ 0 & d \end{pmatrix},$$

donde $a, c \in \mathbb{R}$ y $b, d \in \mathbb{R} - \{0\}$. El conmutador $[A, B]$ se define como

$$[A, B] = ABA^{-1}B^{-1}.$$

Primero, se calcula A^{-1} y B^{-1}:

$$A^{-1} = \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -a/b \\ 0 & 1/b \end{pmatrix},$$



$$B^{-1} = \begin{pmatrix} 1 & c \\ 0 & d \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -c/d \\ 0 & 1/d \end{pmatrix}.$$

Ahora, se calcula los productos AB, A^{-1}, y B^{-1}:

$$AB = \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix}\begin{pmatrix} 1 & c \\ 0 & d \end{pmatrix} = \begin{pmatrix} 1 & a+c \\ 0 & bd \end{pmatrix}.$$

$$ABA^{-1} = \begin{pmatrix} 1 & a+c \\ 0 & bd \end{pmatrix}\begin{pmatrix} 1 & -a/b \\ 0 & 1/b \end{pmatrix} = \begin{pmatrix} 1 & \frac{a+c-a}{b} \\ 0 & d \end{pmatrix} = \begin{pmatrix} 1 & \frac{c}{b} \\ 0 & d \end{pmatrix}.$$

$$ABA^{-1}B^{-1} = \begin{pmatrix} 1 & \frac{c}{b} \\ 0 & d \end{pmatrix}\begin{pmatrix} 1 & -c/d \\ 0 & 1/d \end{pmatrix} = \begin{pmatrix} 1 & \frac{c}{b} - \frac{c}{d} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & c\left(\frac{1}{b} - \frac{1}{d}\right) \\ 0 & 1 \end{pmatrix}.$$

El término $c\left(\frac{1}{b} - \frac{1}{d}\right)$ puede ser simplificado como:

$$c\left(\frac{d-b}{bd}\right).$$

Por lo tanto, el conmutador $[A, B]$ se puede escribir como:

$$[A, B] = \begin{pmatrix} 1 & c\left(\frac{d-b}{bd}\right) \\ 0 & 1 \end{pmatrix}.$$

Observe que el conmutador de dos elementos de G siempre tiene la forma:

$$\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix},$$

donde $k = c\left(\frac{d-b}{bd}\right)$ para algunos $a, c \in \mathbb{R}$ y $b, d \in \mathbb{R} - \{0\}$.

Conjunto de conmutadores

El conjunto de todos los conmutadores de G es:

$$\left\{ \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \mid k \in \mathbb{R} \right\}.$$

Este conjunto es un subgrupo del grupo G y está compuesto por matrices donde el término en la diagonal

es 1, y el término en la posición (1,2) es cualquier número real k.

□

Ver p.159

Solución 2.13.17 (grupo y subgrupo normal)

Para demostrar que $G = \mathbb{Z} \times \mathbb{Z}$ con la operación $(a, b)(c, d) = (a + c(-1)^b, b + d)$ es un grupo no abeliano y para determinar el conjunto de los conmutadores de este grupo, se siguen los siguientes pasos:

Verificación de que G es un grupo

Primero, se debe verificar que G es un grupo bajo esta operación.

1. **Asociatividad:** Se verifica si la operación es asociativa. Sean (a, b), (c, d), y $(e, f) \in G$. Se necesita verificar si $((a, b)(c, d))(e, f) = (a, b)((c, d)(e, f))$.

$$(a, b)(c, d) = (a + c(-1)^b, b + d)$$

$$(c, d)(e, f) = (c + e(-1)^d, d + f)$$

Entonces,

$$((a, b)(c, d))(e, f) = (a + c(-1)^b, b + d)(e, f) = ((a + c(-1)^b) + e(-1)^{b+d}, (b + d) + f)$$

y

$$(a, b)((c, d)(e, f)) = (a, b)(c + e(-1)^d, d + f) =$$

$$(a + (c + e(-1)^d)(-1)^b, b + (d + f)) = (a + c(-1)^b + e(-1)^{b+d}, b + d + f)$$

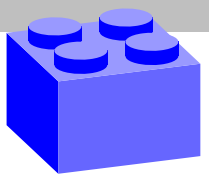
Ambos resultados son iguales, por lo tanto, la operación es asociativa.

2. **Identidad:** La identidad en G debe ser un elemento (e_1, e_2) tal que para cualquier $(a, b) \in G$,

$$(a, b)(e_1, e_2) = (a, b) \quad \text{y} \quad (e_1, e_2)(a, b) = (a, b)$$

En tal caso $(e_1, e_2) = (0, 0)$. En efecto:

$$(a, b)(0, 0) = (a + 0(-1)^b, b + 0) = (a, b)$$



$$(0,0)(a,b) = (0 + a(-1)^0, 0 + b) = (a,b)$$

Por lo tanto, $(0,0)$ es el elemento identidad.

3. **Inverso:** El inverso de $(a,b) \in G$ debe ser un elemento (a',b') tal que

$$(a,b)(a',b') = (0,0) \quad \text{y} \quad (a',b')(a,b) = (0,0)$$

Considere $(a',b') = (-a(-1)^b, -b)$. Así:

$$(a,b)(-a(-1)^b, -b) = (a - a(-1)^b(-1)^b, b - b) = (0,0)$$

$$(-a(-1)^b, -b)(a,b) = (-a(-1)^b + a(-1)^b, -b + b) = (0,0)$$

Por lo tanto, $(a',b') = (-a(-1)^b, -b)$ es el inverso de (a,b).

Con asociatividad, identidad y existencia de inversos verificadas, G es un grupo.

G es no abeliano

Para demostrar que G es no abeliano, se debe encontrar un par de elementos (a,b) y (c,d) en G tal que $(a,b)(c,d) \neq (c,d)(a,b)$.

Considere $(1,1)$ y $(1,0)$:

$$(1,1)(1,0) = (1 + 1(-1)^1, 1 + 0) = (1 - 1, 1) = (0,1)$$

$$(1,0)(1,1) = (1 + 1(-1)^0, 0 + 1) = (1 + 1, 1) = (2,1)$$

Como $(0,1) \neq (2,1)$, G es no abeliano.

Conjunto de los conmutadores

El conmutador de dos elementos (a,b) y (c,d) en G está definido como:

$$[(a,b),(c,d)] = (a,b)(c,d)(a,b)^{-1}(c,d)^{-1}$$

Primero se calcula los inversos:

$$(a,b)^{-1} = (-a(-1)^b, -b)$$

$$(c,d)^{-1} = (-c(-1)^d, -d)$$

Entonces,

$$[(a,b),(c,d)] = (a + c(-1)^b, b + d)(-a(-1)^{b+d}, -b)(-c(-1)^d, -d)$$

Simplificando paso a paso:

$$(a+c(-1)^b, b+d)(-a(-1)^{b+d}, -b) = \left((a + c(-1)^b) - a(-1)^{b+d}(-1)^{b+d}, (b + d) - b\right) = (a+c(-1)^b - a, d)$$

$$(a+c(-1)^b-a, d)(-c(-1)^d, -d) = \left((a + c(-1)^b - a) + (-c(-1)^d)(-1)^d, d - d\right) = (a+c(-1)^b-a-c(-1)^d, 0)$$

Note que si b y d son tales que $(a + c(-1)^b - a - c(-1)^d = 0)$, entonces $(a + c(-1)^b - a - c(-1)^d = 0)$ es la forma del conmutador.

Se puede ver que $(a + c(-1)^b - a - c(-1)^d = 0)$ implica $(c(-1)^b - c(-1)^d = 0)$.

En particular, si b y d son tales que $(-1)^b = (-1)^d$, entonces $c(-1)^b - c(-1)^d = 0$.

Conclusión:

El conjunto de los conmutadores de G está formado por elementos $(a, 0)$ donde $a \in \mathbb{Z}$. Este conjunto es un subgrupo de G.

□

Ver p.159

Solución 2.13.18 (grupo y subgrupo normal)

Para demostrar que si N es un subgrupo normal de un grupo G tal que $N \cap G' = \{e\}$, donde G' es el subgrupo conmutador de G (el conjunto de todos los conmutadores de G), entonces $N \subset Z(G)$ (donde $Z(G)$ es el centro de G), se siguen los siguientes pasos:

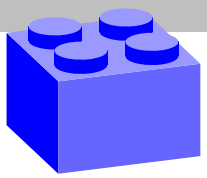
Mostrar que $N \subseteq Z(G)$

Tome un elemento $n \in N$. Se quiere demostrar que n conmuta con todos los elementos de G, es decir, que $n \in Z(G)$. En otras palabras, hay que probar que para todo $g \in G$, $ng = gn$.

Considere el conmutador de n y g:

$$[n, g] = ngn^{-1}g^{-1}$$

Dado que $n \in N$ y N es normal en G, $ngn^{-1} \in G$ para todo $g \in G$. Por lo tanto, $[n, g] \in G'$ porque G'



es el subgrupo conmutador que contiene todos los conmutadores de G.

Usar la intersección trivial

Se sabe que $N \cap G' = \{e\}$. Esto implica que el único elemento que N y G' tienen en común es el elemento identidad e. Entonces, si $[n, g] \in N$ y $[n, g] \in G'$, se debe tener $[n, g] = e$ porque $N \cap G' = \{e\}$.

Por lo tanto:

$$[n, g] = ngn^{-1}g^{-1} = e \implies ng = gn$$

Esto muestra que n conmuta con cualquier $g \in G$.

Conclusión

Se concluye que $N \subseteq Z(G)$, es decir, N está contenido en el centro de G.

□

Solución 2.13.19 (grupo y subgrupo normal) Ver p.159

Para demostrar que si N es un subgrupo normal de G con $|N| = 2$, entonces N es un subconjunto del centro del grupo G (denotado por $Z(G)$), se siguen los siguientes pasos:

Normalidad y conjugación:

Se quiere demostrar que n conmuta con todos los elementos de G, es decir, probar que $n \in Z(G)$. Para esto, considere el efecto de la conjugación sobre n.

Dado que N es normal en G, para cualquier $g \in G$, el elemento conjugado gng^{-1} debe pertenecer a N. Dado que $N = \{e, n\}$, esto implica que gng^{-1} debe ser e o n.

Considerar los posibles valores de gng^{-1}

1. **Caso $gng^{-1} = e$:**

$$gng^{-1} = e \implies n = g^{-1}eg = e \implies n = e$$

Esto es imposible ya que $n \neq e$ por definición.

2.**Caso** $gng^{-1} = n$**:**

$$gng^{-1} = n \implies gn = ng$$

Esto implica que n conmuta con g.

Conclusión:

Dado que para cualquier $g \in G$, el elemento n conmuta con g, esto significa que $n \in Z(G)$.

Por lo tanto, $N \subseteq Z(G)$.

□

Ver p.159

Solución 2.13.20 (grupo y subgrupo normal)

Para demostrar que si M y N son subgrupos normales de un grupo G y $M \cap N = \{e\}$, entonces $mn = nm$ para todo $m \in M$ y $n \in N$, considere el conmutador $[m, n]$, definido como:

$$[m, n] = mnm^{-1}n^{-1}$$

Debido a la normalidad de M y N, los siguientes hechos son ciertos:

- Como N es normal en G, el elemento $m^{-1}n^{-1}m \in N$.
- Como M es normal en G, el elemento $nm^{-1}n^{-1} \in M$.

Luego

- Dado que M es normal, $mnm^{-1} \in N$, porque $n^{-1} \in N$ y $m^{-1}n^{-1}m \in N$.
- De manera similar, dado que N es normal, $nm^{-1}n^{-1} \in M$, porque $m \in M$ y $n^{-1}mn^{-1} \in M$.

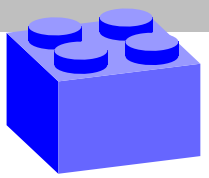
Por lo tanto, $mnm^{-1}n^{-1} \in M$ porque $mnm^{-1} \in N$ y $n^{-1} \in N$.

Como $M \cap N = \{e\}$. Esto significa que cualquier elemento que está simultáneamente en M y N debe ser la identidad e. Por lo tanto, dado que se ha establecido que el conmutador $[m, n] = mnm^{-1}n^{-1} \in M \cap N$, esto implica que:

$$[m, n] \in M \quad \text{y} \quad [m, n] \in N$$

y así

$$[m, n] = e$$



es decir

$$mnm^{-1}n^{-1} = e \implies mn = nm$$

Esto concluye la prueba de que M y N conmutan elemento por elemento.

□

Solución 2.13.21 (grupo y subgrupo normal) Ver p.160

Para demostrar que $2|Z(G)| \neq |G|$, se supondrá lo contrario, lo cual se deriva en una contradicción.

Suponga que $2|Z(G)| = |G|$. Esto implica que el orden del centro de G, $Z(G)$, es exactamente la mitad del orden del grupo G. Con base en el Teorema de Lagrange se sigue que:

$$[G : Z(G)] = \frac{|G|}{|Z(G)|} = 2$$

Esto significa que hay exactamente dos clases laterales de $Z(G)$ en G. En particular, $Z(G)$ es un subgrupo de índice 2 en G, lo cual significa que $Z(G)$ es normal.

Además, si $Z(G)$ tiene índice 2, entonces G puede descomponerse en dos clases laterales de $Z(G)$:

$$G = Z(G) \cup gZ(G)$$

Si se toma cualquier elemento $h \in G$, entonces h debe estar en una de las dos clases laterales $Z(G)$ o $gZ(G)$. Considere los siguientes casos:

1. **Caso** $h \in Z(G)$: Por la definición del centro, cualquier $h \in Z(G)$ conmuta con todos los elementos de G.

2. **Caso** $h \in gZ(G)$**:** En este caso, se puede escribir $h = gc$ para algún $c \in Z(G)$. Considere la conmutación de h con un elemento $k \in G$:

$$hk = (gc)k = g(ck) = g(kc) = (gk)c$$

Ahora, considere kh:

$$kh = k(gc) = (kg)c$$

Dado que $g \notin Z(G)$, hay algún $k \in G$ tal que $gk \neq kg$. Por lo tanto, para algún k, se tiene que:

$$g(kc) \neq (kg)c$$

Esto significa que no se cumple la conmutación para todos los elementos fuera del centro.

Dado que se asume que $2|Z(G)| = |G|$ implica que cualquier elemento fuera del centro debe conmutar con los elementos en el centro, pero al mismo tiempo hay elementos fuera del centro que no conmutan con algún otro elemento del grupo, esto genera una contradicción. Por lo tanto, la suposición de que $2|Z(G)| = |G|$ es incorrecta. Así, es imposible que $2|Z(G)| = |G|$. Por lo tanto, $2|Z(G)| \neq |G|$.

□

Ver p.160

Solución 2.13.22 (grupo y subgrupo normal)

Se analiza cada afirmación una por una y se determinará si son verdaderas o falsas.

1. ¿Tiene cada subgrupo de orden 4 clases izquierdas?

Falso. Todos los subgrupos, independientemente de su orden, tienen clases izquierdas. Las clases laterales (izquierdas y derechas) son una propiedad de cualquier subgrupo en un grupo, no dependen del orden del subgrupo.

2. ¿Puede no tener clases izquierdas un subgrupo finito de un grupo infinito?

Falso. Todo subgrupo, ya sea finito o infinito, tiene clases laterales izquierdas y derechas. Esto es parte de la estructura fundamental de un grupo y sus subgrupos.

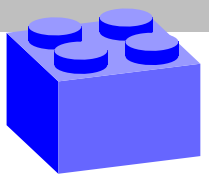
3. ¿Es un subgrupo de un grupo una clase izquierda en sí mismo?

Verdadero. Un subgrupo H de un grupo G es una clase lateral izquierda en sí mismo. Es decir, $H = eH$, donde e es el elemento identidad de G.

4. ¿Solamente los subgrupos de grupos finitos pueden tener clases izquierdas?

Falso. Tanto los subgrupos de grupos finitos como los de grupos infinitos tienen clases laterales izquierdas. La existencia de clases laterales no depende de la finitud del grupo.

5. ¿El número de clases izquierdas de un subgrupo de un grupo finito divide al orden del grupo?



Verdadero. Esto es una consecuencia del teorema de Lagrange. El número de clases laterales de un subgrupo H en un grupo finito G es el índice $[G : H]$, que divide al orden de G.

6. ¿Es cada subgrupo de un grupo abeliano un subgrupo normal?

Verdadero. En un grupo abeliano, todos los subgrupos son normales porque todos los elementos conmuten entre sí.

7. ¿Es cada grupo cociente de un grupo finito un grupo finito?

Verdadero. Si G es un grupo finito y N es un subgrupo normal de G, entonces el grupo cociente G/N es también finito.

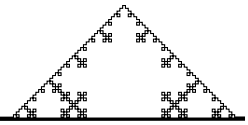
8. ¿Es abeliano cada grupo cociente de un grupo abeliano?

Verdadero. Si G es un grupo abeliano y N es un subgrupo normal de G, entonces el grupo cociente G/N es también abeliano.

9. ¿Es no abeliano cada grupo cociente de un grupo no abeliano?

Falso. No necesariamente. Un grupo no abeliano puede tener un subgrupo normal tal que el cociente sea abeliano. Por ejemplo, el grupo simétrico S_3 no es abeliano, pero su subgrupo alternado A_3 es abeliano, y S_3/A_3 es un grupo abeliano.

□



Soluciones de la sección 2.18

Ver p.198

Solución 2.18.1 (Homomorfismo)

Para verificar que $f : (\mathbb{Z}, +) \to (\mathbb{Z}_n, +)$ definida por $f(x) = [x]$ es un homomorfismo de grupos, se debe comprobar que f preserva la operación de grupo, es decir, que para todos $x, y \in \mathbb{Z}$, se cumple:

$$f(x + y) = f(x) + f(y)$$

Paso 1: Definición de f

La función f está definida como:

$$f(x) = [x]$$

donde $[x]$ denota la clase de equivalencia de x módulo n en el grupo $\mathbb{Z}_n$.

Paso 2: Verificación de la propiedad de homomorfismo

Para verificar la propiedad de homomorfismo, tome $x, y \in \mathbb{Z}$. Se debe mostrar que:

$$f(x + y) = f(x) + f(y)$$

Luego, se calculamos cada lado de la ecuación por separado.

Lado izquierdo: Por la definición de f,

$$f(x + y) = [x + y]$$

Lado derecho: Por la definición de f,

$$f(x) = [x] \quad \text{y} \quad f(y) = [y]$$

En el grupo $(\mathbb{Z}_n, +)$, la suma de dos clases de equivalencia se define como la clase de equivalencia de la suma de sus representantes. Por lo tanto,

$$f(x) + f(y) = [x] + [y] = [x + y]$$

Paso 3: Conclusión

Comparando ambos lados, se obtiene:

$$f(x + y) = [x + y] = [x] + [y] = f(x) + f(y)$$

Esto demuestra que f preserva la operación de grupo, es decir, f es un homomorfismo de grupos.

Para encontrar el núcleo de f, que se denota por $\ker(f)$, se debe identificar todos los elementos $x \in \mathbb{Z}$ tales que $f(x) = [x] = [0]$ en $\mathbb{Z}_n$. Esto significa que se busca todos los enteros x que son congruentes con 0 módulo n.

Definición del núcleo

El núcleo de un homomorfismo $f : G \to H$ es el conjunto de todos los elementos en G que se mapean al elemento identidad de H. En este caso, $G = (\mathbb{Z}, +)$ y $H = (\mathbb{Z}_n, +)$, y el elemento identidad en $\mathbb{Z}_n$ es 0.

$$\ker(f) = \{x \in \mathbb{Z} : f(x) = 0\}$$

Cálculo del núcleo

Para este homomorfismo $f(x) = [x]$:

$$\ker(f) = \{x \in \mathbb{Z} : [x] = 0\}$$

La clase de equivalencia $[x]$ es $[0]$ en $\mathbb{Z}_n$ si y solo si x es un múltiplo de n. Es decir, x debe ser de la forma $x = kn$ para algún $k \in \mathbb{Z}$.

Por lo tanto,

$$\ker(f) = \{x \in \mathbb{Z} : x = kn \text{ para algún } k \in \mathbb{Z}\} = n\mathbb{Z}$$

Conclusión

El núcleo de f es el conjunto de todos los múltiplos de n:

$$\ker(f) = n\mathbb{Z}$$

Esto se puede interpretar como el subgrupo de $\mathbb{Z}$ generado por n.

□

Ver p.198

Solución 2.18.2 (Homomorfismo)

Para verificar que $f : (\mathbb{R} \times \mathbb{R}, +) \to (\mathbb{R}, +)$ definida por $f(x, y) = x + y$ es un homomorfismo de grupos, se debe comprobar que f preserva la operación de grupo, es decir, que para todos $(x_1, y_1), (x_2, y_2) \in \mathbb{R} \times \mathbb{R}$, se cumple:

$$f((x_1, y_1) + (x_2, y_2)) = f(x_1, y_1) + f(x_2, y_2)$$

Paso 1: Definición de la operación en $\mathbb{R} \times \mathbb{R}$

En $(\mathbb{R} \times \mathbb{R}, +)$, la operación es la suma componente a componente:

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$

Paso 2: Evaluación de f en la suma de dos elementos

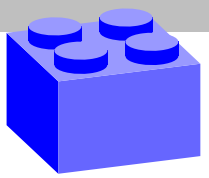
Considere dos elementos (x_1, y_1) y $(x_2, y_2) \in \mathbb{R} \times \mathbb{R}$. Se necesita evaluar f en la suma de estos dos elementos:

$$f((x_1, y_1) + (x_2, y_2)) = f(x_1 + x_2, y_1 + y_2)$$

Por la definición de f,

$$f(x_1 + x_2, y_1 + y_2) = (x_1 + x_2) + (y_1 + y_2)$$

Paso 3: Evaluación de f en cada elemento y suma de los resultados



Ahora se evalúa f en (x_1, y_1) y (x_2, y_2) por separado, y se suman los resultados:

$$f(x_1, y_1) = x_1 + y_1$$

$$f(x_2, y_2) = x_2 + y_2$$

Sumando estos resultados se tiene:

$$f(x_1, y_1) + f(x_2, y_2) = (x_1 + y_1) + (x_2 + y_2)$$

Paso 4: Comparación de ambos lados

Comparando ambos lados, se tiene:

$$f((x_1, y_1) + (x_2, y_2)) = (x_1 + x_2) + (y_1 + y_2)$$

$$f(x_1, y_1) + f(x_2, y_2) = (x_1 + y_1) + (x_2 + y_2)$$

Se observa que son iguales, es decir:

$$f((x_1, y_1) + (x_2, y_2)) = f(x_1, y_1) + f(x_2, y_2)$$

Conclusión

Por lo tanto, $f : (\mathbb{R} \times \mathbb{R}, +) \to (\mathbb{R}, +)$ definida por $f(x, y) = x + y$ es un homomorfismo de grupos.

Para demostrar que el núcleo de f es $\ker(f) = \{(x, -x) \mid x \in \mathbb{R}\}$, donde $f : (\mathbb{R} \times \mathbb{R}, +) \to (\mathbb{R}, +)$ está definida por $f(x, y) = x + y$, se siguen los siguientes pasos:

Definición del núcleo

El núcleo de un homomorfismo f es el conjunto de todos los elementos en el dominio que se mapean al elemento identidad del codominio. En este caso, el elemento identidad en el grupo de llegada $(\mathbb{R}, +)$ es 0. Por lo tanto,

$$\ker(f) = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid f(x, y) = 0\}$$

Evaluación de f en (x, y)

La función f está definida como $f(x, y) = x + y$. Se quiere encontrar todos los pares $(x, y) \in \mathbb{R} \times \mathbb{R}$ para los cuales $f(x, y) = 0$. Por la definición de f esta escuación es equivalente a

$$x + y = 0$$

Solución de la ecuación

La ecuación $x + y = 0$ puede resolverse para y:

$$y = -x$$

El conjunto de todos los pares (x, y) que satisfacen esta ecuación es $\{(x, -x) \mid x \in \mathbb{R}\}$.

Conclusión

Se sigue que

$$\ker(f) = \{(x, -x) \mid x \in \mathbb{R}\}$$

Esto significa que el núcleo del homomorfismo f está formado por todos los pares $(x, -x)$ donde x es cualquier número real.

□

Ver p.198

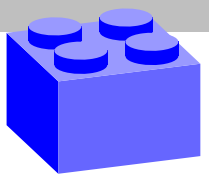
Solución 2.18.3 (Homomorfismo)

Para demostrar que la función $f : (U_n, \cdot) \to (U_n, \cdot)$ definida por $f([k]) = [k]^m$ es un homomorfismo de grupos, se necesita verificar que f preserva la operación de grupo. Específicamente, se debe mostrar que para todos $[a], [b] \in U_n$, se cumple:

$$f([a] \cdot [b]) = f([a]) \cdot f([b])$$

Paso 1: Definición de U_n

El conjunto U_n es el grupo de unidades módulo n. Esto significa que U_n está formado por todas las clases



de equivalencia de enteros que son coprimos con n, bajo la multiplicación módulo n. Es decir,

$$U_n = \{[k] \in \mathbb{Z}_n : (k, n) = 1\}$$

Paso 2: Definición de la función f

La función f está definida como:

$$f\big([k]\big) = [k]^m$$

donde $[k]^m$ denota la m-ésima potencia de $[k]$ en U_n.

Paso 3: Verificación de la propiedad de homomorfismo

Para verificar que f es un homomorfismo, considere dos elementos $[a], [b] \in U_n$. Se quiere demostrar que:

$$f([a] \cdot [b]) = f([a]) \cdot f([b])$$

Evaluación de $f([a] \cdot [b])$

Primero, se evaluá f en el producto $[a] \cdot [b]$:

$$f([a] \cdot [b]) = f([ab])$$

Por la definición de f,

$$f([ab]) = [ab]^m$$

Evaluación de $f([a]) \cdot f([b])$

Ahora se evalúa f en $[a]$ y $[b]$ por separado, y luego se toma el producto de los resultados:

$$f([a]) = [a]^m \quad \text{y} \quad f([b]) = [b]^m$$

El producto de estos dos elementos en U_n es:

$$f([a]) \cdot f([b]) = [a]^m \cdot [b]^m$$

Dado que la operación en U_n es la multiplicación módulo n, se puede escribir:

$$[a]^m \cdot [b]^m = ([a] \cdot [b])^m = [ab]^m$$

Paso 4: Comparación de ambos lados

Comparando ambos lados, se tiene:

$$f([a] \cdot [b]) = [ab]^m$$

$$f([a]) \cdot f([b]) = ([a] \cdot [b])^m = [ab]^m$$

Ambos son iguales, es decir:

$$f([a] \cdot [b]) = f([a]) \cdot f([b])$$

Conclusión

Se ha demostrado que f preserva la operación de grupo. Por lo tanto, $f : \left(U_n, \cdot\right) \to \left(U_n, \cdot\right)$ definida por $f\left([k]\right) = [k]^m$ es un homomorfismo de grupos.

□

Ver p.198

Solución 2.18.4 (Homomorfismo)

Para demostrar que $f : \mathbb{Z}_2 \times \mathbb{Z}_2 \to U_8$ definida por $f([a],[b]) = [3^a 5^b]$ es un homomorfismo de grupos, se debe verificar que f preserva la operación de grupo. Específicamente, se necesita mostrar que para todos $([a],[b]),([c],[d]) \in \mathbb{Z}_2 \times \mathbb{Z}_2$, se cumple:

$$f(([a],[b]) + ([c],[d])) = f([a],[b]) \cdot f([c],[d])$$

Paso 1: Definición de la operación en $\mathbb{Z}_2 \times \mathbb{Z}_2$

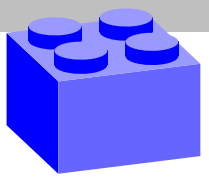
En el grupo $\mathbb{Z}_2 \times \mathbb{Z}_2$ con la operación suma componente a componente, se tiene:

$$([a],[b]) + ([c],[d]) = ([a+c],[b+d])$$

Paso 2: Definición de la función f

La función f está definida como:

$$f([a],[b]) = [3^a 5^b]$$



donde $[3^a 5^b]$ denota la clase de equivalencia de $3^a 5^b$ módulo 8.

Paso 3: Verificación de la propiedad de homomorfismo

Para verificar que f es un homomorfismo, considere dos elementos $([a],[b])$ y $([c],[d]) \in \mathbb{Z}_2 \times \mathbb{Z}_2$. Se quiere demostrar que:

$$f(([a],[b]) + ([c],[d])) = f([a],[b]) \cdot f([c],[d])$$

Evaluación de $f(([a],[b]) + ([c],[d]))$

Primero, se evaluá f en el elemento suma $([a],[b]) + ([c],[d])$:

$$f(([a],[b]) + ([c],[d])) = f([a+c],[b+d])$$

Por la definición de f,

$$f([a+c],[b+d]) = [3^{a+c}5^{b+d}]$$

Evaluación de $f([a],[b]) \cdot f([c],[d])$ Ahora se evaluá f en $([a],[b])$ y $([c],[d])$ por separado, y luego se toma el producto de los resultados:

$$f([a],[b]) = [3^a 5^b] \quad \text{y} \quad f([c],[d]) = [3^c 5^d]$$

El producto de estos dos elementos en U_8 es:

$$f([a],[b]) \cdot f([c],[d]) = [3^a 5^b] \cdot [3^c 5^d] = [3^a 3^c 5^b 5^d] = [3^{a+c}5^{b+d}]$$

Paso 4: Comparación de ambos lados

Comparando ambos lados, se tiene:

$$f(([a],[b]) + ([c],[d])) = [3^{a+c}5^{b+d}]$$

$$f([a],[b]) \cdot f([c],[d]) = [3^{a+c}5^{b+d}]$$

Ambos son iguales, es decir:

$$f(([a],[b])+([c],[d])) = f([a],[b]) \cdot f([c],[d])$$

Conclusión

Se ha demostrado que f preserva la operación de grupo. Por lo tanto, $f : \mathbb{Z}_2 \times \mathbb{Z}_2 \to U_8$ definida por $f([a],[b]) = [3^a 5^b]$ es un homomorfismo de grupos.

□

Ver p.199

Solución 2.18.5 (Homomorfismo)

Para demostrar que el conjunto de automorfismos $Aut(G)$ de un grupo $(G,\cdot)$ es un grupo bajo la composición de funciones, se debe verificar que se cumplen las propiedades de un grupo: cerradura, existencia de un elemento identidad, existencia de inversos y asociatividad.

Definición de automorfismo

Un automorfismo de G es un isomorfismo de G en sí mismo, es decir, una función biyectiva $\phi : G \to G$ tal que para todos $x, y \in G$,

$$\phi(x \cdot y) = \phi(x) \cdot \phi(y).$$

Paso 1: Cerradura

Se debe demostrar que la composición de dos automorfismos es un automorfismo.

Sean $\phi, \psi \in Aut(G)$. Se necesita mostrar que la composición $\phi \circ \psi$ también es un automorfismo de G.

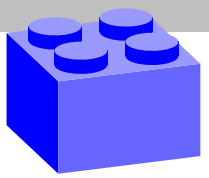
1. **Homomorfismo:** Sea $x, y \in G$. Entonces,

$$(\phi\circ\psi)(x \cdot y) = \phi(\psi(x \cdot y)) = \phi(\psi(x) \cdot \psi(y)) = \phi(\psi(x)) \cdot \phi(\psi(y)) = (\phi\circ\psi)(x) \cdot (\phi\circ\psi)(y).$$

   Esto muestra que $\phi\circ\psi$ es un homomorfismo.

2. **Biyectividad:** Dado que ϕ y ψ son biyectivas, su composición $\phi\circ\psi$ también es biyectiva.

Dado que $\phi\circ\psi$ es un homomorfismo biyectivo, es un automorfismo. Por lo tanto, $Aut(G)$ es cerrado bajo la composición de funciones.



Paso 2: Elemento identidad

Se debe demostrar que existe un elemento identidad en $Aut(G)$. La identidad del grupo de automorfismos es la función identidad $id_G : G \to G$ definida por $id_G(x) = x$ para todos $x \in G$.

1. **Homomorfismo:** Para todos $x, y \in G$,

$$id_G(x \cdot y) = x \cdot y = id_G(x) \cdot id_G(y).$$

   Por lo tanto, id_G es un homomorfismo.

2. **Biyectividad**: La función identidad id_G es claramente biyectiva.

Por lo tanto, id_G es un automorfismo y actúa como el elemento identidad en $Aut(G)$.

Paso 3: Inversos

Se debe demostrar que cada automorfismo tiene un inverso en $Aut(G)$.

Sea $\phi \in Aut(G)$. Dado que ϕ es biyectiva, existe una función inversa $\phi^{-1} : G \to G$ tal que $\phi \circ \phi^{-1} = id_G$ y $\phi^{-1} \circ \phi = id_G$.

1. **Homomorfismo:** Para todos $x, y \in G$,

$$\phi^{-1}(x \cdot y) = \phi^{-1}(\phi(\phi^{-1}(x)) \cdot \phi(\phi^{-1}(y))) = \phi^{-1}(\phi(\phi^{-1}(x) \cdot \phi^{-1}(y))) = \phi^{-1} \circ \phi(\phi^{-1}(x) \cdot \phi^{-1}(y)) = \phi^{-1}(x) \cdot \phi^{-1}(y).$$

   Esto muestra que ϕ^{-1} es un homomorfismo.

2. **Biyectividad**: La función inversa ϕ^{-1} es biyectiva.

Por lo tanto, ϕ^{-1} es un automorfismo. Así, cada automorfismo en $Aut(G)$ tiene un inverso en $Aut(G)$.

Paso 4: Asociatividad

La composición de funciones es asociativa. Para cualquier $\phi, \psi, \theta \in Aut(G)$,

$$(\phi \circ (\psi \circ \theta))(x) = \phi((\psi \circ \theta)(x)) = \phi(\psi(\theta(x))) = (\phi \circ \psi)(\theta(x)) = ((\phi \circ \psi) \circ \theta)(x).$$

Por lo tanto,

$$\phi \circ (\psi \circ \theta) = (\phi \circ \psi) \circ \theta.$$

Conclusión

Se ha demostrado que $Aut(G)$ satisface todas las propiedades de un grupo: cerradura, existencia de un elemento identidad, existencia de inversos y asociatividad. Por lo tanto, $Aut(G)$ es un grupo bajo la composición de funciones.

□

Ver p.199

Solución 2.18.6 (Homomorfismo)

Para demostrar que si G y H son grupos tales que $G \cong H$, entonces $Aut(G) \cong Aut(H)$, se siguen los pasos y la sugerencia dada. La clave está en utilizar un isomorfismo entre G y H para construir un isomorfismo entre sus conjuntos de automorfismos.

Paso 1: Definición del isomorfismo f

Dado que $G \cong H$, existe un isomorfismo $f : G \to H$. Esto significa que f es una función biyectiva tal que para todos $g_1, g_2 \in G$,

$$f(g_1 \cdot g_2) = f(g_1) \cdot f(g_2).$$

Paso 2: Definición de T_f

Defina una función $T_f : Aut(G) \to Aut(H)$ de la siguiente manera:

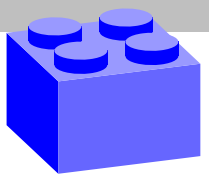
$$T_f(h) = f \circ h \circ f^{-1}$$

para cada $h \in Aut(G)$.

Paso 3: T_f es un homomorfismo

Primero, se verifica que T_f es un homomorfismo. Sea $h_1, h_2 \in Aut(G)$. Se necesita mostrar que

$$T_f(h_1 \circ h_2) = T_f(h_1) \circ T_f(h_2).$$



Evaluando ambos lados:

$$T_f(h_1 \circ h_2) = f \circ (h_1 \circ h_2) \circ f^{-1} = f \circ h_1 \circ h_2 \circ f^{-1}.$$

Por otro lado,

$$T_f(h_1) \circ T_f(h_2) = (f \circ h_1 \circ f^{-1}) \circ (f \circ h_2 \circ f^{-1}).$$

Dado que la composición de funciones es asociativa,

$$(f \circ h_1 \circ f^{-1}) \circ (f \circ h_2 \circ f^{-1}) = f \circ h_1 \circ (f^{-1} \circ f) \circ h_2 \circ f^{-1} = f \circ h_1 \circ h_2 \circ f^{-1}.$$

Esto muestra que

$$T_f(h_1 \circ h_2) = T_f(h_1) \circ T_f(h_2).$$

Paso 4: T_f es inyectivo

Para demostrar que T_f es inyectivo, suponga que $T_f(h_1) = T_f(h_2)$. Esto significa que

$$f \circ h_1 \circ f^{-1} = f \circ h_2 \circ f^{-1}.$$

Multiplicando ambos lados por f^{-1} desde la izquierda y f desde la derecha, se obtiene:

$$h_1 = h_2.$$

Por lo tanto, T_f es inyectivo.

Paso 5: T_f es sobreyectivo

Para demostrar que T_f es sobreyectivo, tome cualquier $g \in Aut(H)$. Necesitamos encontrar un $h \in Aut(G)$ tal que $T_f(h) = g$.

Defina $h = f^{-1} \circ g \circ f$. se verificará que $h \in Aut(G)$:

- **Homomorfismo:** Para $x, y \in G$,

  $$h(xy) = f^{-1}(g(f(xy))) = f^{-1}(g(f(x)f(y))) = f^{-1}(g(f(x))g(f(y))) = f^{-1}(g(f(x)))f^{-1}(g(f(y))) = h(x)h(y).$$

  Esto muestra que h es un homomorfismo.

- **Biyectividad:** Dado que f y g son biyectivos, h también biyectivo.

Por lo tanto, $h \in Aut(G)$ y

$$T_f(h) = f \circ (f^{-1} \circ g \circ f) \circ f^{-1} = g.$$

Esto muestra que T_f es sobreyectivo.

Conclusión:
Dado que T_f es un homomorfismo biyectivo (es decir, un isomorfismo), se ha demostrado que $Aut(G) \cong Aut(H)$.

□

Ver p.199

Solución 2.18.7 (Homomorfismo)

Si G es un grupo, $n \in \mathbb{N}$ y $\varphi : \mathbb{Z}_n \to G$ es un homomorfismo, muestre que

$$\varphi([k]) = \varphi([1])^k$$

para todo $k \in \mathbb{Z}$. Concluya que $\varphi([1]) \mid n$.

Demostración:

Dado que φ es un homomorfismo, para cualquier $[a], [b] \in \mathbb{Z}_n$, se tiene:

$$\varphi([a] + [b]) = \varphi([a]) \cdot \varphi([b]).$$

Ahora, tome $k \in \mathbb{Z}$. Se puede escribir $[k]$ como la suma de k veces $[1]$:

$$[k] = [1] + [1] + \cdots + [1] \quad \text{(k veces)}.$$

Aplicando el homomorfismo φ y usando la propiedad de homomorfismo:

$$\varphi([k]) = \varphi([1] + [1] + \cdots + [1]) = \varphi([1]) \cdot \varphi([1]) \cdot \cdots \cdot \varphi([1]) = \varphi([1])^k.$$

Esto demuestra que $\varphi([k]) = \varphi([1])^k$.

Conclusión: Dado que $\varphi([n]) = \varphi([0]) = e_G$, se tiene:

$$\varphi([1])^n = e_G.$$

Por lo tanto, el orden de $\varphi([1])$ divide n.

Si $\varphi' : \mathbb{Z}_n \to G$ es otro homomorfismo, muestre que $\varphi = \varphi'$ si y solo si $\varphi(1) = \varphi'(1)$.

Demostración:

($\Rightarrow$) Suponga que $\varphi = \varphi'$. Entonces, claramente $\varphi([1]) = \varphi'([1])$.

($\Leftarrow$) Suponga que $\varphi([1]) = \varphi'([1])$. Se quiere mostrar que $\varphi([k]) = \varphi'([k])$ para todo $k \in \mathbb{Z}$.

Para cualquier $k \in \mathbb{Z}$, se tiene:

$$\varphi([k]) = \varphi([1])^k = (\varphi'([1]))^k = \varphi'([k]).$$

Por lo tanto, $\varphi = \varphi'$.

Si $g \in G$, muestre que la función $\varphi : \mathbb{Z}_n \to G$ dada por $\varphi([k]) = g^k$ está bien definida si y solo si $|g| \mid n$. En tal caso, muestre que φ es un homomorfismo.

Demostración:

Para que φ esté bien definida, se necesita que $\varphi([k]) = \varphi([l])$ cuando $[k] = [l]$ en $\mathbb{Z}_n$. Esto significa que si $k \equiv l \pmod{n}$, entonces $g^k = g^l$.

Si $k \equiv l \pmod{n}$, entonces $k = l + mn$ para algún $m \in \mathbb{Z}$. Se necesita que:

$$g^k = g^{l+mn} = g^l \cdot (g^n)^m = g^l,$$

lo cual es cierto si y solo si $g^n = e_G$. Esto es cierto si y solo si el orden de g divide n.

Por lo tanto, φ está bien definida si y solo si $|g| \mid n$.

Homomorfismo: Si $|g| \mid n$, entonces:

$$\varphi([k+l]) = g^{k+l} = g^k \cdot g^l = \varphi([k]) \cdot \varphi([l]).$$

Por lo tanto, φ es un homomorfismo.

Concluya que el conjunto de homomorfismos de $\mathbb{Z}_n$ en G está en biyección con $\{g \in G : |g| \mid n\}$.

Demostración:

Por el resultado del punto 3, cada homomorfismo $\varphi : \mathbb{Z}_n \to G$ está determinado por $\varphi([1])$. La condición para que φ esté bien definida es que $|\varphi([1])| \mid n$.

Entonces, hay una correspondencia biunívoca entre los homomorfismos de $\mathbb{Z}_n$ en G y los elementos $g \in G$ tales que $|g| \mid n$. Esta correspondencia es:

$$\varphi \mapsto \varphi([1]).$$

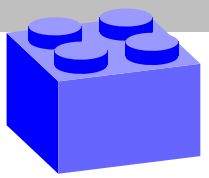
Liste todos los homomorfismos de $\mathbb{Z}_{20}$ en $\mathbb{Z}_{25}$.

Demostración:

Se buscan homomorfismos $\varphi : \mathbb{Z}_{20} \to \mathbb{Z}_{25}$. Dado que $\mathbb{Z}_{25}$ es un grupo cíclico de orden 25, los elementos $g \in \mathbb{Z}_{25}$ tales que $|g| \mid 20$ son:

$$[0], [5], [10], [15], [20].$$

Para cada uno de estos elementos, se define un homomorfismo $\varphi : \mathbb{Z}_{20} \to \mathbb{Z}_{25}$ tal que $\varphi([k]) = g^k$, donde $g \in \{[0], [5], [10], [15], [20]\}$.



Los homomorfismos son:

$$\varphi_0([k]) = [0],\ \varphi_5([k]) = [5k],\ \varphi_{10}([k]) = [10k],\ \varphi_{15}([k]) = [15k],\ \varphi_{20}([k]) = [20k].$$

Esto lista todos los homomorfismos de $\mathbb{Z}_{20}$ en $\mathbb{Z}_{25}$.

□

Solución 2.18.8 (Homomorfismo)

Ver p.200

Si g y h conmutan en G_1, entonces $\varphi(g)$ y $\varphi(h)$ conmutan en G_2.

Demostración:

Si g y h conmutan en G_1, entonces $gh = hg$. Aplicando φ a ambos lados de la ecuación:

$$\varphi(gh) = \varphi(hg).$$

Dado que φ es un homomorfismo, se tiene:

$$\varphi(g)\varphi(h) = \varphi(h)\varphi(g).$$

Por lo tanto, $\varphi(g)$ y $\varphi(h)$ conmutan en G_2.

Si $g \in G_1$, entonces g y $\varphi(g)$ tienen el mismo orden.

Demostración:

Sea $g \in G_1$ con orden n, es decir, $g^n = e_{G_1}$ y n es el menor entero positivo para el cual esto se cumple. Se quiere demostrar que $\varphi(g)$ tiene el mismo orden en G_2.

Dado que φ es un homomorfismo, se tiene:

$$\varphi(g^n) = \varphi(e_{G_1}) = e_{G_2}.$$

Además, $\varphi(g^n) = (\varphi(g))^n$, lo que implica que $(\varphi(g))^n = e_{G_2}$. Por lo tanto, el orden de $\varphi(g)$ en G_2 es menor o igual a n.

Suponga que el orden de $\varphi(g)$ es $m < n$. Entonces, $(\varphi(g))^m = e_{G_2}$. Aplicando φ^{-1} a ambos lados de la ecuación, se tiene:

$$\varphi^{-1}((\varphi(g))^m) = \varphi^{-1}(e_{G_2}).$$

Dado que φ^{-1} es un homomorfismo,

$$(\varphi^{-1}(\varphi(g)))^m = e_{G_1} \implies g^m = e_{G_1}.$$

Esto contradice el hecho de que n es el orden de g en G_1. Por lo tanto, el orden de $\varphi(g)$ en G_2 debe ser n. Así, g y $\varphi(g)$ tienen el mismo orden.

G_1 es abeliano si y sólo si G_2 es abeliano.

Demostración:

Suponga que G_1 es abeliano. Entonces, para todos $g, h \in G_1$,

$$gh = hg.$$

Aplicando φ,

$$\varphi(g)\varphi(h) = \varphi(h)\varphi(g).$$

Esto muestra que $\varphi(g)$ y $\varphi(h)$ conmutan en G_2. Dado que g y h fueron escogidos arbitrariamente, G_2 es abeliano.

Ahora, suponga que G_2 es abeliano. Entonces, para todos $\varphi(g), \varphi(h) \in G_2$,

$$\varphi(g)\varphi(h) = \varphi(h)\varphi(g).$$

Aplicando φ^{-1},

$$\varphi^{-1}(\varphi(g)\varphi(h)) = \varphi^{-1}(\varphi(h)\varphi(g)).$$

Dado que φ^{-1} es un homomorfismo,

$$gh = hg.$$

Esto muestra que g y h conmutan en G_1. Por lo tanto, G_1 es abeliano.

La ecuación $x^k = g$ tiene el mismo número de soluciones en G_1 que $f(g) = x^k$ en G_2.

Demostración:

Sea $x^k = g$ una ecuación en G_1. Se quiere demostrar que el número de soluciones en G_1 es igual al número de soluciones de $f(g) = x^k$ en G_2.

Sea $\varphi : G_1 \to G_2$ un isomorfismo. Entonces, $\varphi(x^k) = (\varphi(x))^k$. Si $x_1, x_2, \ldots, x_n$ son soluciones de $x^k = g$ en G_1, entonces $\varphi(x_1), \varphi(x_2), \ldots, \varphi(x_n)$ son soluciones de $(\varphi(x))^k = \varphi(g)$ en G_2.

Como φ es biyectivo, el número de soluciones de $x^k = g$ en G_1 es igual al número de soluciones de $(\varphi(x))^k = \varphi(g)$ en G_2.

G_1 y G_2 tienen la misma cardinalidad, es decir, el mismo número de elementos.

Demostración:

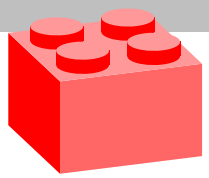
Dado que $\varphi : G_1 \to G_2$ es un isomorfismo, es una función biyectiva. Una función biyectiva entre dos conjuntos implica que los conjuntos tienen la misma cardinalidad. Por lo tanto, G_1 y G_2 tienen el mismo número de elementos.

□

Solución 2.18.9 (Homomorfismo)

Ver p.200

Para demostrar que el conjunto de matrices $GL(2, \mathbb{R})$ con la multiplicación usual de matrices y el grupo $(\mathbb{R}, +)$ no son isomorfos, se debe encontrar una propiedad de uno de estos grupos que no se comparte con el otro. Una diferencia fundamental entre estos grupos es su estructura algebraica.



Soluciones

1. Estructura de $GL(2,\mathbb{R})$

El grupo $GL(2,\mathbb{R})$ es el conjunto de todas las matrices 2×2 invertibles con entradas reales. Las matrices en $GL(2,\mathbb{R})$ tienen la forma:

$$GL(2,\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in \mathbb{R} \text{ y } ad - bc \neq 0 \right\}$$

La operación en $GL(2,\mathbb{R})$ es la multiplicación de matrices. Es importante notar que la multiplicación de matrices en general no es conmutativa; es decir, para dos matrices $A, B \in GL(2,\mathbb{R})$, generalmente $AB \neq BA$.

2. Estructura de $(\mathbb{R},+)$

El grupo $(\mathbb{R},+)$ es el conjunto de todos los números reales bajo la operación de suma. En este grupo, la operación es conmutativa; es decir, para cualquier $x, y \in \mathbb{R}$, se cumple que $x + y = y + x$.

Conclusión

Dado que $GL(2,\mathbb{R})$ tiene una operación no conmutativa y $(\mathbb{R},+)$ tiene una operación conmutativa, no puede existir un isomorfismo entre estos dos grupos. Por lo tanto, $GL(2,\mathbb{R})$ y $(\mathbb{R},+)$ no son isomorfos.

□

Ver p.200

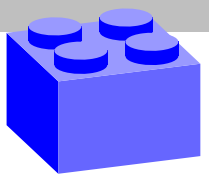
Solución 2.18.10 (Homomorfismo)

Para demostrar que el grupo $(\mathbb{Q}-\{0\},\cdot)$ no es isomorfo al grupo $(\mathbb{Z},+)$, podemos usar propiedades distintivas de estos grupos. Una diferencia clave entre estos dos grupos es el comportamiento de las soluciones a ciertas ecuaciones en estos grupos.

1. Estructura de $(\mathbb{Q}-\{0\},\cdot)$

El grupo $(\mathbb{Q}-\{0\},\cdot)$ consiste en todos los números racionales distintos de cero bajo la operación de multiplicación. Este grupo es abeliano (conmutativo).

2. Estructura de $(\mathbb{Z},+)$



El grupo $(\mathbb{Z}, +)$ consiste en todos los números enteros bajo la operación de suma. Este grupo también es abeliano (conmutativo).

3. Propiedad distintiva

Considere la ecuación $x^2 = 4$

En $(\mathbb{Q} - \{0\}, \cdot)$:

Buscando soluciones en el grupo $(\mathbb{Q} - \{0\}, \cdot)$:

$$x^2 = 4 \implies x \cdot x = 4.$$

En $(\mathbb{Q} - \{0\}, \cdot)$, hay dos soluciones para esta ecuación:

$$x = 2 \quad \text{y} \quad x = -2.$$

En $(\mathbb{Z}, +)$:

Buscando soluciones en el grupo $(\mathbb{Z}, +)$:

$$x + x = 4 \implies 2x = 4 \implies x = 2.$$

En $(\mathbb{Z}, +)$, hay una única solución para esta ecuación:

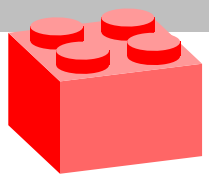
$$x = 2.$$

4. Conclusión

La ecuación $x^2 = 4$ tiene dos soluciones en $(\mathbb{Q} - \{0\}, \cdot)$, pero solo una solución en $(\mathbb{Z}, +)$. Esta diferencia en el número de soluciones demuestra que no puede existir un isomorfismo entre $(\mathbb{Q} - \{0\}, \cdot)$ y $(\mathbb{Z}, +)$. Si existiera un isomorfismo, debería preservar la estructura del grupo, incluyendo el número de soluciones para cualquier ecuación.

Por lo tanto, el grupo $(\mathbb{Q} - \{0\}, \cdot)$ no es isomorfo al grupo $(\mathbb{Z}, +)$.

□



Soluciones

Ver p.200

Solución 2.18.11 (Homomorfismo)

Para demostrar que el grupo $(\mathbb{R}-\{0\},\cdot)$ no es isomorfo al grupo $(\mathbb{R},+)$, se puede utilizar las propiedades distintivas de estos grupos, especialmente con respecto a la solución de ciertas ecuaciones. Siguiendo la sugerencia, considere la ecuación $2x=a$ en cada uno de estos grupos.

1. Estructura de $(\mathbb{R}-\{0\},\cdot)$

El grupo $(\mathbb{R}-\{0\},\cdot)$ consiste en todos los números reales distintos de cero bajo la operación de multiplicación. Este grupo es abeliano (conmutativo).

2. Estructura de $(\mathbb{R},+)$

El grupo $(\mathbb{R},+)$ consiste en todos los números reales bajo la operación de suma. Este grupo también es abeliano (conmutativo).

3. Análisis de la ecuación $2x=a$

En $(\mathbb{R},+)$**:**

Considere la ecuación $2x=a$ en el grupo $(\mathbb{R},+)$:

$$2x=a \implies x+x=a \implies x=\frac{a}{2}.$$

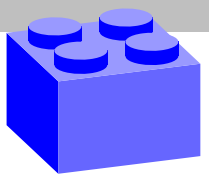
Para cualquier $a\in\mathbb{R}$, siempre existe una única solución $x=\frac{a}{2}\in\mathbb{R}$.

En $(\mathbb{R}-\{0\},\cdot)$**:**

Considere la ecuación $2x=a$ en el grupo $(\mathbb{R}-\{0\},\cdot)$:

$$2x=a \implies x^2=a.$$

Para que esta ecuación tenga solución en $\mathbb{R}-\{0\}$, a debe ser un número positivo, ya que x debe ser un número real no nulo y cuadrado de un número real no nulo solo puede ser positivo. Esto implica que si $a<0$, la ecuación no tiene solución en $(\mathbb{R}-\{0\},\cdot)$.



4. Conclusión

La ecuación $2x = a$ en el grupo $(\mathbb{R}, +)$ tiene una única solución para cualquier $a \in \mathbb{R}$. Sin embargo, en el grupo $(\mathbb{R} - \{0\}, \cdot)$, la ecuación $2x = a$ solo tiene solución si a es positivo.

Esta diferencia en las soluciones demuestra que no puede existir un isomorfismo entre $(\mathbb{R} - \{0\}, \cdot)$ y $(\mathbb{R}, +)$. Un isomorfismo debe preservar la estructura algebraica de los grupos, incluyendo las soluciones de las ecuaciones.

Por lo tanto, el grupo $(\mathbb{R} - \{0\}, \cdot)$ no es isomorfo al grupo $(\mathbb{R}, +)$.

□

Solución 2.18.12 (Homomorfismo) Ver p.201

Para demostrar que $SL(n, \mathbb{R})$ es un subgrupo de $GL(n, \mathbb{R})$, se debe verificar que cumple las tres propiedades de un subgrupo:

- Cerradura bajo la operación de grupo (multiplicación de matrices).
- Contiene el elemento identidad.
- Contiene el inverso de cada uno de sus elementos.

1. **Cerradura:** Sean $A, B \in SL(n, \mathbb{R})$. Entonces $\det(A) = 1$ y $\det(B) = 1$. Se quiere demostrar que $AB \in SL(n, \mathbb{R})$.

$$\det(AB) = \det(A) \cdot \det(B) = 1 \cdot 1 = 1.$$

   Por lo tanto, $AB \in SL(n, \mathbb{R})$, lo que demuestra la cerradura.

2. **Elemento identidad:** El elemento identidad en $GL(n, \mathbb{R})$ es la matriz identidad I, que satisface $\det(I) = 1$. Por lo tanto, $I \in SL(n, \mathbb{R})$.

3. **Inverso:** Para cualquier $A \in SL(n, \mathbb{R})$, se sabe que $\det(A) = 1$. Se quiere demostrar que $A^{-1} \in SL(n, \mathbb{R})$.

$$\det(A^{-1}) = \frac{1}{\det(A)} = \frac{1}{1} = 1.$$

   Por lo tanto, $A^{-1} \in SL(n, \mathbb{R})$.

Dado que $SL(n,\mathbb{R})$ cumple con las tres propiedades, se concluye que $SL(n,\mathbb{R})$ es un subgrupo de $GL(n,\mathbb{R})$.

Para demostrar que el grupo cociente $GL(n,\mathbb{R})/SL(n,\mathbb{R})$ es isomorfo al grupo $\mathbb{R}-\{0\}$ con la multiplicación usual, se puede definir un homomorfismo sobreyectivo cuyo núcleo sea $SL(n,\mathbb{R})$.

Considere el determinante como un homomorfismo:

$$\det : GL(n,\mathbb{R}) \to \mathbb{R}-\{0\}.$$

El determinante de una matriz $A \in GL(n,\mathbb{R})$ es un número real no nulo. Este es un homomorfismo porque para $A, B \in GL(n,\mathbb{R})$:

$$\det(AB) = \det(A)\cdot\det(B).$$

Sobreyectividad:

Para cualquier $r \in \mathbb{R}-\{0\}$, existe una matriz diagonal $D \in GL(n,\mathbb{R})$ tal que $\det(D) = r$. Por ejemplo, se puede tomar $D = \operatorname{diag}(r,1,1,\ldots,1)$.

Núcleo:

El núcleo de det es el conjunto de matrices en $GL(n,\mathbb{R})$ cuyo determinante es 1, que es precisamente $SL(n,\mathbb{R})$:

$$\ker(\det) = SL(n,\mathbb{R}).$$

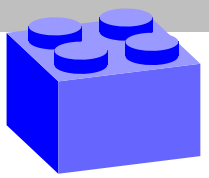
Por el Primer Teorema de Isomorfismo para grupos, el homomorfismo det induce un isomorfismo:

$$GL(n,\mathbb{R})/SL(n,\mathbb{R}) \cong \mathbb{R}-\{0\}.$$

Esto demuestra que $GL(n,\mathbb{R})/SL(n,\mathbb{R})$ es isomorfo al grupo multiplicativo $\mathbb{R}-\{0\}$.

□

Ver p.201 **Solución 2.18.13 (Homomorfismo)**



Mostrar que f es un homomorfismo.

Demostración:

Un homomorfismo de grupos debe preservar la operación de grupo. Aquí, las operaciones son sumas módulo n y módulo m, respectivamente.

Para cualquier $[a]_n, [b]_n \in \mathbb{Z}_n$:

$$f([a]_n + [b]_n) = f([a+b]_n).$$

Por la definición de f:

$$f([a+b]_n) = [a+b]_m.$$

Ahora evaluando $f([a]_n) + f([b]_n)$:

$$f([a]_n) + f([b]_n) = [a]_m + [b]_m = [a+b]_m.$$

Como ambos resultados son iguales, f preserva la operación de grupo, es decir,

$$f([a]_n + [b]_n) = f([a]_n) + f([b]_n).$$

Por lo tanto, f es un homomorfismo.

Mostrar que $\ker(f) = \langle [m]_n \rangle$.

Demostración:

El núcleo de f es el conjunto de elementos en $\mathbb{Z}_n$ que se mapean al elemento identidad en $\mathbb{Z}_m$, es decir, la clase $[0]_m$:

$$\ker(f) = \{[k]_n \in \mathbb{Z}_n \mid f([k]_n) = [0]_m\}.$$

Por la definición de f, esto es:

$$\ker(f) = \{[k]_n \in \mathbb{Z}_n \mid [k]_m = [0]_m\}.$$

Esto significa que $k \equiv 0 \pmod{m}$. En otras palabras, k es un múltiplo de m:

$$\ker(f) = \{[k]_n \in \mathbb{Z}_n \mid k = jm \text{ para algún } j \in \mathbb{Z}\} = \langle [m]_n \rangle.$$

Por lo tanto,

$$\ker(f) = \langle [m]_n \rangle.$$

Mostrar que f es sobreyectiva.

Demostración:

Una función es sobreyectiva si cada elemento en el codominio tiene al menos un elemento en el dominio que se mapea a él. Para cualquier $[r]_m \in \mathbb{Z}_m$, considere $[r]_n \in \mathbb{Z}_n$.

Entonces,

$$f([r]_n) = [r]_m.$$

Dado que para cualquier $[r]_m$ en $\mathbb{Z}_m$ se puede encontrar un $[r]_n \in \mathbb{Z}_n$ que se mapea a él, f es sobreyectiva.

Concluir que $\mathbb{Z}_n/\langle [m]_n \rangle \cong \mathbb{Z}_m$.

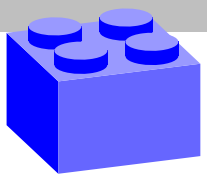
Demostración:

Dado que $f : \mathbb{Z}_n \to \mathbb{Z}_m$ es un homomorfismo sobreyectivo y $\ker(f) = \langle [m]_n \rangle$, por el Primer Teorema de Isomorfismo, se tiene que:

$$\mathbb{Z}_n/\ker(f) \cong \text{im}(f).$$

Se sabe que $\text{im}(f) = \mathbb{Z}_m$, por lo que:

$$\mathbb{Z}_n/\ker(f) \cong \mathbb{Z}_m.$$



Dado que $\ker(f) = \langle [m]_n \rangle$, esto implica que:

$$\mathbb{Z}_n / \langle [m]_n \rangle \cong \mathbb{Z}_m.$$

□

Solución 2.18.14 (Homomorfismo)

Ver p.201

Para demostrar que $h(g^n) = g^{-n}$ es un automorfismo del grupo cíclico $G = \langle g \rangle$ de orden finito, se debe verificar dos propiedades fundamentales de los automorfismos:

1. **Homomorfismo:** h debe ser un homomorfismo, es decir, $h(g^a \cdot g^b) = h(g^a) \cdot h(g^b)$ para todos $a, b \in \mathbb{Z}$.
2. **Biyectividad:** h debe ser una función biyectiva, es decir, h debe ser inyectiva (uno a uno) y sobreyectiva (encima).

1. Verificar que h es un homomorfismo

Sean $a, b \in \mathbb{Z}$. Considere el producto de dos elementos en G:

$$g^a \cdot g^b = g^{a+b}.$$

Aplicando h a ambos lados:

$$h(g^a \cdot g^b) = h(g^{a+b}) = g^{-(a+b)}.$$

Ahora, evaluando $h(g^a) \cdot h(g^b)$ por separado:

$$h(g^a) = g^{-a} \quad \text{y} \quad h(g^b) = g^{-b}.$$

Multiplicando estos resultados, se obtiene:

$$h(g^a) \cdot h(g^b) = g^{-a} \cdot g^{-b} = g^{-(a+b)}.$$

Como ambos lados son iguales, se cumple que:

$$h(g^a \cdot g^b) = h(g^a) \cdot h(g^b).$$

Esto muestra que h es un homomorfismo.

2. Verificar que h es biyectivo

Para verificar que h es biyectivo, se debe demostrar que h es inyectivo y sobreyectivo.

- **Inyectividad**: Suponga que $h(g^a) = h(g^b)$. Esto implica que:

$$g^{-a} = g^{-b}.$$

  Dado que G es cíclico de orden finito, cada elemento g^k tiene un inverso único. Por lo tanto, la única manera en que $g^{-a} = g^{-b}$ es que $a = b$. Esto muestra que h es inyectivo.

- **Sobreyectividad:** Para demostrar que h es sobreyectivo, se debe demostrar que para cada $g^k \in G$, existe un $g^m \in G$ tal que $h(g^m) = g^k$. Sea $g^k \in G$. Se quiere encontrar un m tal que:

$$h(g^m) = g^k \implies g^{-m} = g^k \implies -m \equiv k \pmod{|G|}.$$

  Dado que G tiene orden finito, por ejemplo n, para cada k existe un m tal que $m \equiv -k \pmod{n}$. Por lo tanto, h es sobreyectivo.

Conclusión

Dado que se ha demostrado que $h(g^n) = g^{-n}$ es un homomorfismo biyectivo, se concluye que h es un automorfismo de G.

□

Ver p.202

Solución 2.18.15 (Homomorfismo)

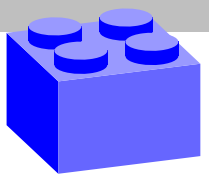
Para demostrar que $h : (\mathbb{R}, +) \to GL(2, \mathbb{R})$ definido por

$$h(x) = \begin{pmatrix} \cos(x) & \sin(x) \\ -\sin(x) & \cos(x) \end{pmatrix}$$

es un homomorfismo sobreyectivo, se debe verificar dos propiedades:

- **Homomorfismo:** h debe preservar la operación de grupo, es decir, para todos $x, y \in \mathbb{R}$,

$$h(x + y) = h(x)h(y).$$



- **Sobreyectividad**: Para cualquier matriz $A \in GL(2, \mathbb{R})$ que está en la imagen de h, debe existir un $x \in \mathbb{R}$ tal que $h(x) = A$.

1. Verificar que h es un homomorfismo

Para demostrar que h es un homomorfismo, considere dos elementos $x, y \in \mathbb{R}$.

Evaluando $h(x + y)$:

$$h(x+y) = \begin{pmatrix} \cos(x+y) & \sin(x+y) \\ -\sin(x+y) & \cos(x+y) \end{pmatrix}.$$

Usando las identidades trigonométricas para la suma de ángulos, se sabe que:

$$\cos(x+y) = \cos(x)\cos(y) - \sin(x)\sin(y)$$

$$\sin(x+y) = \sin(x)\cos(y) + \cos(x)\sin(y)$$

Por lo tanto,

$$h(x+y) = \begin{pmatrix} \cos(x)\cos(y) - \sin(x)\sin(y) & \sin(x)\cos(y) + \cos(x)\sin(y) \\ -(\sin(x)\cos(y) + \cos(x)\sin(y)) & \cos(x)\cos(y) - \sin(x)\sin(y) \end{pmatrix}.$$

Ahora evaluando el producto $h(x)h(y)$:

$$h(x) = \begin{pmatrix} \cos(x) & \sin(x) \\ -\sin(x) & \cos(x) \end{pmatrix}$$

$$h(y) = \begin{pmatrix} \cos(y) & \sin(y) \\ -\sin(y) & \cos(y) \end{pmatrix}$$

Multiplicando $h(x)$ y $h(y)$:

$$h(x)h(y) = \begin{pmatrix} \cos(x) & \sin(x) \\ -\sin(x) & \cos(x) \end{pmatrix} \begin{pmatrix} \cos(y) & \sin(y) \\ -\sin(y) & \cos(y) \end{pmatrix}$$

$$= \begin{pmatrix} \cos(x)\cos(y) - \sin(x)\sin(y) & \cos(x)\sin(y) + \sin(x)\cos(y) \\ -\sin(x)\cos(y) - \cos(x)\sin(y) & -\sin(x)\sin(y) + \cos(x)\cos(y) \end{pmatrix}$$

$$= \begin{pmatrix} \cos(x+y) & \sin(x+y) \\ -\sin(x+y) & \cos(x+y) \end{pmatrix}.$$

Así, se ha demostrado que:

$$h(x+y) = h(x)h(y).$$

Por lo tanto, h es un homomorfismo.

2. Verificar que h es sobreyectivo

Se quiere demostrar que para cualquier matriz $A \in GL(2,\mathbb{R})$ de la forma:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

donde $\det(A) = 1$, existe un $x \in \mathbb{R}$ tal que $h(x) = A$.

Para que una matriz de la forma

$$\begin{pmatrix} \cos(x) & \sin(x) \\ -\sin(x) & \cos(x) \end{pmatrix}$$

sea igual a A, se necesita que:

$$a = \cos(x), \quad b = \sin(x), \quad c = -\sin(x), \quad d = \cos(x).$$

La condición de que $\det(A) = 1$ se satisface porque:

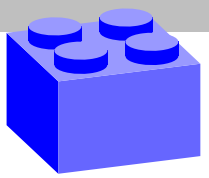
$$\det(A) = ad - bc = \cos^2(x) + \sin^2(x) = 1.$$

Esto muestra que cualquier matriz ortogonal con determinante 1 se puede expresar como $h(x)$ para algún $x \in \mathbb{R}$.

Conclusión

Se ha demostrado que h es un homomorfismo y que es sobreyectivo.

□



Solución 2.18.16 (Homomorfismo)

Ver p.202

El grupo $\mathbb{Z}_2 \times \mathbb{Z}_2$ es un grupo abeliano finito de orden 4. Los elementos de $\mathbb{Z}_2 \times \mathbb{Z}_2$ son $(0,0)$, $(0,1)$, $(1,0)$, y $(1,1)$. Para encontrar todos los subgrupos no triviales de $\mathbb{Z}_2 \times \mathbb{Z}_2$, primero se recuerda que un subgrupo de un grupo finito de orden n debe tener un orden que divide n (Teorema de Lagrange).

Dado que $|\mathbb{Z}_2 \times \mathbb{Z}_2| = 4$, los posibles órdenes de los subgrupos son 1, 2, y 4. Los subgrupos triviales son $\{(0,0)\}$ (el subgrupo de orden 1) y $\mathbb{Z}_2 \times \mathbb{Z}_2$ (el subgrupo de orden 4). Aquí se busca los subgrupos no triviales, por lo que se busca subgrupos de orden 2.

Subgrupos de orden 2

Un subgrupo de orden 2 debe contener dos elementos, incluyendo el elemento neutro $(0,0)$. El otro elemento debe ser de orden 2, es decir, un elemento a tal que $2a = (0,0)$. Los elementos de $\mathbb{Z}_2 \times \mathbb{Z}_2$ que tienen esta propiedad son $(0,1)$, $(1,0)$, y $(1,1)$, ya que:

$$(0,1) + (0,1) = (0,0)$$

$$(1,0) + (1,0) = (0,0)$$

$$(1,1) + (1,1) = (0,0)$$

Cada uno de estos elementos genera un subgrupo de orden 2 junto con el elemento neutro $(0,0)$.

Listado de subgrupos no triviales

- El subgrupo generado por $(0,1)$:

$$\langle (0,1) \rangle = \{(0,0), (0,1)\}$$

- El subgrupo generado por $(1,0)$:

$$\langle (1,0) \rangle = \{(0,0), (1,0)\}$$

- El subgrupo generado por $(1,1)$:

$$\langle (1,1) \rangle = \{(0,0),(1,1)\}$$

Conclusión:

Los subgrupos no triviales de $\mathbb{Z}_2 \times \mathbb{Z}_2$ son:

$$\{(0,0),(0,1)\}$$

$$\{(0,0),(1,0)\}$$

$$\{(0,0),(1,1)\}$$

□

Ver p.202

Solución 2.18.17 (Homomorfismo)

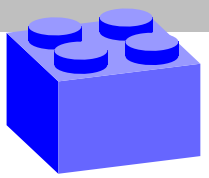
Para determinar cuáles de los grupos mencionados son isomorfos entre sí, considere las propiedades de cada uno y se usan las pistas proporcionadas.

Lista de grupos:

1. $(\mathbb{Z}, +)$
2. $(2\mathbb{Z}, +)$
3. $(\mathbb{Z}_{20}, +)$
4. $(\mathbb{Q}^+, +)$
5. $(\mathbb{Q}^+, \cdot)$
6. $(\mathbb{Z}_8, +)$
7. D_4 (el grupo diédrico de orden 8)
8. $GL(2, \mathbb{R})$ (el grupo de matrices invertibles 2×2 con entradas reales)

Propiedades de los grupos:

Soluciones



1.$(\mathbb{Z}, +)$: Infinito, cíclico, abeliano.

2.$(2\mathbb{Z}, +)$: Infinito, cíclico, abeliano. Isomorfo a $(\mathbb{Z}, +)$. Un isomorfismo puede definirse por $h(n) = 2n$.

3.$(\mathbb{Z}_{20}, +)$: Finito, cíclico de orden 20, abeliano.

4.$(\mathbb{Q}^+, +)$: Infinito, abeliano, no cíclico. Notar que $\mathbb{Q}^+ = \{a/b \mid a, b \in \mathbb{Z}, b \neq 0\}$.

5.$(\mathbb{Q}^+, \cdot)$:Infinito, abeliano. No cíclico porque no hay un único elemento cuya potencia genere todos los números racionales positivos.

6.$(\mathbb{Z}_8, +)$: Finito, cíclico de orden 8, abeliano.

7.D_4: Finito, no abeliano. El grupo diédrico de orden 8 (simetrías del cuadrado).

8.$GL(2, \mathbb{R})$: Infinito, no abeliano. Grupo de matrices invertibles 2×2 con entradas reales.

Isomorfismos y no isomorfismos:

- $(\mathbb{Z}, +)$ y $(2\mathbb{Z}, +)$ son isomorfos: $h(n) = 2n$ es un isomorfismo.
- $(\mathbb{Z}_{20}, +)$ y $(\mathbb{Z}_8, +)$ no son isomorfos entre sí ni a ningún otro grupo en la lista, ya que son cíclicos de órdenes diferentes y no hay ningún otro grupo en la lista que tenga el mismo orden o estructura cíclica finita. También, grupos finitos cíclicos no pueden ser isomorfos a grupos infinitos.
- $(\mathbb{Q}^+, +)$ y $(\mathbb{Q}^+, \cdot)$ no son isomorfos entre sí ni a ningún otro grupo en la lista. Estos grupos tienen estructuras diferentes: $(\mathbb{Q}^+, +)$ es aditivo, mientras que $(\mathbb{Q}^+, \cdot)$ es multiplicativo. Además, no son cíclicos, mientras que algunos de los otros grupos lo son.
- D_4 y $GL(2, \mathbb{R})$ no son isomorfos entre sí ni a ningún otro grupo en la lista, ya que son no abelianos. El resto de los grupos en la lista son abelianos.

Conclusión:

1.$(\mathbb{Z}, +)$ y $(2\mathbb{Z}, +)$ son isomorfos.

2.$(\mathbb{Z}_{20}, +)$ no es isomorfo a $(\mathbb{Z}_8, +)$ ni a ningún otro grupo en la lista.

3.$(\mathbb{Q}^+, +)$ y $(\mathbb{Q}^+, \cdot)$ no son isomorfos entre sí ni a ningún otro grupo en la lista.

4. D_4 no es isomorfo a $GL(2,\mathbb{R})$ ni a ningún otro grupo en la lista.

Entonces, la clasificación es:

- Grupos isomorfos: $(\mathbb{Z},+)$ y $(2\mathbb{Z},+)$.
- Grupos no isomorfos a ningún otro en la lista:
  - $(\mathbb{Z}_{20},+)$
  - $(\mathbb{Q}^+,+)$
  - $(\mathbb{Q}^+,\cdot)$
  - $(\mathbb{Z}_8,+)$
  - D_4
  - $GL(2,\mathbb{R})$.

□

Ver p.202

Solución 2.18.18 (Homomorfismo)

Para demostrar que no es posible hallar un isomorfismo entre los grupos $(\mathbb{R},+)$ y $(\mathbb{R}-\{0\},\cdot)$, se pued analizar propiedades fundamentales de estos grupos que no son compatibles entre sí. Una diferencia clave entre estos dos grupos es la estructura de sus subgrupos.

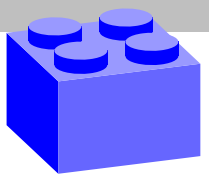
Propiedad 1: Estructura de Subgrupos

Subgrupos de $(\mathbb{R},+)$:

- En el grupo $(\mathbb{R},+)$, cualquier subgrupo es de una de las siguientes formas:
  1. $\{0\}$
  2. $r\mathbb{Z}$ para algún $r \in \mathbb{R}$
  3. $r\mathbb{Z} + s\mathbb{Z}$ para algún $r, s \in \mathbb{R}$ que sean linealmente independientes sobre los racionales (esto es, $\mathbb{R}$ considerado como un espacio vectorial sobre $\mathbb{Q}$).
  4. $\mathbb{R}$ mismo.

Es decir, $(\mathbb{R},+)$ tiene subgrupos generados por cualquier número real r, y también puede tener subgrupos densos en $\mathbb{R}$.

Subgrupos de $(\mathbb{R}-\{0\},\cdot)$:



- En el grupo $(\mathbb{R} - \{0\}, \cdot)$, los subgrupos son más restrictivos. Algunos ejemplos de subgrupos son:
  1. $\{1\}$ (subgrupo trivial)
  2. Los conjuntos $\{a^n \mid n \in \mathbb{Z}\}$ para algún $a \in \mathbb{R} - \{0\}$ (subgrupos cíclicos multiplicativos).
  3. $\mathbb{R}^+$ (los números reales positivos bajo la multiplicación).

Además, $(\mathbb{R} - \{0\}, \cdot)$ no tiene subgrupos cíclicos que incluyan todos los números reales no nulos porque no hay un solo número real cuyo conjunto de todas las potencias (positivas y negativas) cubra todos los reales no nulos.

Propiedad 2: Cardinalidad de los Subgrupos

Para un isomorfismo entre dos grupos, la estructura de subgrupos debe preservarse. En particular, la cardinalidad de los subgrupos debe coincidir.

Contradicción con Subgrupos de Orden 2:

- En $(\mathbb{R}, +)$, no existen subgrupos de orden finito mayores que 1, porque cualquier subgrupo no trivial debe ser infinito. Específicamente, no existe un elemento $x \in \mathbb{R}$ tal que $2x = 0$ aparte de $x = 0$.
- En $(\mathbb{R} - \{0\}, \cdot)$, existen subgrupos de orden 2. Por ejemplo, $\{-1, 1\}$ es un subgrupo de orden 2, ya que $(-1)^2 = 1$ y $1^2 = 1$.

Conclusión

Dado que $(\mathbb{R} - \{0\}, \cdot)$ tiene subgrupos de orden 2 y $(\mathbb{R}, +)$ no tiene subgrupos de orden 2, no puede existir un isomorfismo entre $(\mathbb{R}, +)$ y $(\mathbb{R} - \{0\}, \cdot)$. Un isomorfismo debe preservar la estructura de subgrupos, pero aquí se encuentra una discrepancia clara en la existencia de subgrupos de orden 2 en $(\mathbb{R} - \{0\}, \cdot)$ y la ausencia de tales subgrupos en $(\mathbb{R}, +)$.

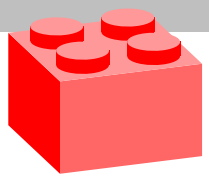
Por lo tanto, no es posible hallar un isomorfismo entre estos dos grupos.

□

Solución 2.18.19 (Homomorfismo)

Ver p.202

Para demostrar que la condición de ser un isomorfismo entre grupos define una relación de equivalencia sobre el conjunto de todos los grupos, se necesita demostrar que esta relación cumple con las tres propiedades de una relación de equivalencia: reflexividad, simetría y transitividad.



Soluciones

1. **Reflexividad:** Un grupo es isomorfo a sí mismo. Formalmente, para cualquier grupo G, existe un isomorfismo $f : G \to G$ dado por la función identidad id_G.

   - La identidad en G se define como:

   $$\mathrm{id}_G(g) = g \quad \text{para todo } g \in G.$$

   - La función identidad id_G es un homomorfismo porque para cualquier $g, h \in G$,

   $$\mathrm{id}_G(g \cdot h) = g \cdot h = \mathrm{id}_G(g) \cdot \mathrm{id}_G(h).$$

   - La función identidad es biyectiva (inyectiva y sobreyectiva).

   Por lo tanto, id_G es un isomorfismo, y la relación de isomorfismo es reflexiva.

2. **Simetría:** Si G es isomorfo a H, entonces H es isomorfo a G. Formalmente, si existe un isomorfismo $f : G \to H$, entonces existe un isomorfismo $f^{-1} : H \to G$.

   - Dado que f es un isomorfismo, f es una función biyectiva y preserva la operación de grupo.
   - La inversa f^{-1} también preserva la operación de grupo porque, para cualquier $h_1, h_2 \in H$, existe $g_1, g_2 \in G$ tal que $f(g_1) = h_1$ y $f(g_2) = h_2$. Entonces,

   $$f^{-1}(h_1 \cdot h_2) = f^{-1}(f(g_1) \cdot f(g_2)) = f^{-1}(f(g_1 \cdot g_2)) = g_1 \cdot g_2 = f^{-1}(h_1) \cdot f^{-1}(h_2).$$

   - f^{-1} es biyectiva porque f lo es.

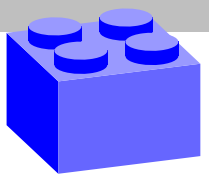
   Por lo tanto, si $f : G \to H$ es un isomorfismo, $f^{-1} : H \to G$ también lo es, y la relación de isomorfismo es simétrica.

3. **Transitividad:** Si G es isomorfo a H y H es isomorfo a K, entonces G es isomorfo a K. Formalmente, si existen isomorfismos $f : G \to H$ y $g : H \to K$, entonces la composición $g \circ f : G \to K$ es un isomorfismo.

   - La composición de dos homomorfismos es un homomorfismo. Para cualquier $g_1, g_2 \in G$,

   $$(g \circ f)(g_1 \cdot g_2) = g(f(g_1 \cdot g_2)) = g(f(g_1) \cdot f(g_2)) = g(f(g_1)) \cdot g(f(g_2)) = (g \circ f)(g_1) \cdot (g \circ f)(g_2).$$

   - La composición de dos funciones biyectivas es una función biyectiva.



Por lo tanto, $g \circ f : G \to K$ es un isomorfismo, y la relación de isomorfismo es transitiva.

Conclusión

Dado que la relación de ser isomorfismo entre grupos es reflexiva, simétrica y transitiva, concluimos que esta relación define una relación de equivalencia sobre el conjunto de todos los grupos.

□

Bibliografía

Biggs, N. L., Lloyd, E. K., y Wilson, R. J. (1976). *Graph theory 1736–1936*. Oxford University Press.

Communications. (2024, febrero). De Esparta a la criptografía cuántica: Breve historia de la encriptación de datos y sus tipos. *BBVA Noticias*.https://www.bbva.com/es/innovacion/de-esparta-a-la-criptografia-cuantica-breve-historia-de-la-encriptacion-de-datos-y-sus-tipos/

Cameron, P. J. (1999). *Permutation groups*. Cambridge University Press.

Cormen, T. H., Leiserson, C. E., Rivest, R. L., y Stein, C. (2009). *Introduction to algorithms*. The MIT Press.

Cotton, F. A. (1990). *Chemical applications of group theory*. John Wiley y Sons.

Dummit, D. S., y Foote, R. M. (2004). *Abstract algebra* (3rd ed.). John Wiley y Sons, Inc.

Encyclopedia.com. (s.f.). Chevalley, Claude. https://www.encyclopedia.com/science/dictionaries-thesauruses-pictures-and-press-releases/chevalley-claude

Fernández, T., y Tamaro, E. (2004). Biografía de Joseph-Louis de Lagrange. En *Biografías y Vidas: la enciclopedia biográfica en línea*. https://www.biografiasyvidas.com/biografia/l/lagrange.htm

Fraleígh, J. B. (1988). *Algebra abstracta primer curso*. Addison-Wesley Iberoamericana, S. A.

Gallian, J. A. (2010). *Contemporary abstract algebra* (7th ed.). Brooks/Cole, Cengage Learning.

Godsil, C., y Royle, G. (2001). *Algebraic graph theory*. Springer.

Goldenberg, E. (2024, 26 de enero). *Évariste Galois: A misfortunate genius who solved the unsolvable*. The Science Survey. https://thesciencesurvey.com/spotlight/2024/01/26/evariste-galois-a-misfortunate-genius-who-solved-the-unsolvable/

González, F. (2003). *Álgebra I*. Editorial Universidad Estatal a Distancia.

Herstein, I. N. (1991). *Topics in algebra*. John Wiley y Sons.

Historia Universal. (2024). *Niels Henrik Abel: matemático noruego conocido por su trabajo en teoría de ecuaciones*. https://historiauniversal.org/niels-henrik-abel-matematico-noruego-conocido-por-su-trabajo-en-teoria-de-ecuaciones/

Hungerford, T. W. (1980). *Algebra* (8th ed.). Springer-Verlag. https://doi.org/10.1007/978-1-4612-6101-8

Kempf, G. R. (1995). *Álgebraic structures*. Friedr. Vieweg y Sohn Verlagsgesellschaft mbH.

Klein, F. (1892–1893). A comparative review of recent researches in geometry (M. W. Haskell, Trans.). *Bulletin of the New York Mathematical Society*, 2, 215–249. https://math.ucr.edu/home/baez/erlangen/

Knuth, D. E. (1998). *The art of computer programming, volume 3: sorting and searching* (2nd ed., Trabajo original publicado en 1973). Addison-Wesley Professional.

Koblitz, N., Menezes, A., y Vanstone, S. (2000). The state of elliptic curve cryptography. *Designs, Codes and Cryptography*, 19, 173–193.

Lewin, D. (1987). *Generalized musical intervals and transformations*. Yale University Press.

Menezes, A. J., van Oorschot, P. C., y Vanstone, S. A. (1996). *Handbook of applied cryptography*. CRC Press.

Monteiro, R. T. (2016). *Post-quantum cryptography: Lattice-based cryptography and analysis of NTRU public-key cryptosystem* [Tesis doctoral no publicada].

Murillo, M., y González, J. F. (2006). *Teoría de los números*. Instituto Tecnológico de Costa Rica.

Nettles, B., y Graf, E. (1997). *The chord scale theory y jazz harmony*. Advance Music.

O'Connor, J. J., y Robertson, E. F. (2024a). *Emmy Noether. MacTutor History of Mathematics Archive*. University of St Andrews. https://mathshistory.st-andrews.ac.uk/Biographies/Noether_Emmy/

O'Connor, J. J., y Robertson, E. F. (2024b). *Richard Brauer. MacTutor History of Mathematics Archive*. University of St Andrews. https://mathshistory.st-andrews.ac.uk/Biographies/Brauer/

Pires, L. (2024, junio). *¿Quién fue Claude Shannon y cómo revolucionó la era digital?* https://www.eset.com/latam/blog/cultura-y-seguridad-digital/quien-fue-claude-shannon-y-como-revoluciono-la-era-digital/

Rotman, J. J. (1995). *An introduction to the theory of groups* (4th ed.). Springer-Verlag. https://doi.org/10.1007/978-1-4612-4176-8

Rotman, J. J. (2015). *Advanced modern algebra* (3rd ed., Part 1). American Mathematical Society. https://doi.org/10.1090/gsm/165

Sedgewick, R., y Wayne, K. (2011). *Algorithms*. Addison-Wesley.

Sepanski, M. R. (2010). *Álgebra*. American Mathematical Society.

Silverman, J. H., Pipher, J., y Hoffstein, J. (2008). *An introduction to mathematical cryptography* (Vol. 1). Springer.

Tinkham, M. (1964). *Group theory and its application to the quantum mechanics of atomic spectra*. McGraw-Hill.

Tinkham, M. (2003). *Group theory and quantum mechanics*. Dover Publications.

Tymoczko, D. (2011). *A geometry of music: Harmony and counterpoint in the extended common practice*. Oxford University Press.

Velasco, J. J. (2014, mayo). *Breve historia de la criptografía*. elDiario.es. https://www.eldiario.es/turing/criptografia/breve-historia-criptografia_1_4878763.html.

Wirth, N. (1976). *Algorithms + data structures = programs*. Prentice-Hall.

Zassenhaus, H. (1964). Emil Artin, his life and his work. *Notre Dame Journal of Formal Logic*, 5(1), 1–9.

"Introducción a la Teoría de Grupos" es una obra indispensable para aquellos que desean adentrarse en el fascinante mundo de la teoría de grupos

La progresión del material es gradual y cuidadosamente estructurada, facilitando la asimilación de conceptos abstractos para lectores tanto novatos como aquellos con experiencia previa en matemáticas. La inclusión de ejemplos ilustrativos y ejercicios prácticos refuerza la comprensión y ofrece a los lectores la oportunidad de aplicar activamente lo aprendido.

En resumen, "Introducción a la Teoría de Grupos" se erige como un recurso esencial que equilibra la claridad expositiva con la profundidad conceptual, brindando a los lectores una entrada accesible y enriquecedora a este apasionante dominio matemático.

TEC | Tecnológico de Costa Rica

Revista digital
MATEMÁTICA
Educación e Internet