

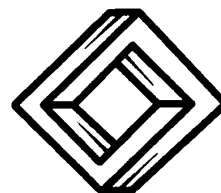
**Publicaciones Electrónicas
Sociedad Matemática Mexicana**

**Un Curso en
Teoría de Grupos**

Alonso Castillo Ramírez

www.smm.org.mx

Serie: Textos. Vol. 23 (2021)



Un Curso en Teoría de Grupos

Alonso Castillo Ramírez

*Centro Universitario de Ciencias Exactas e Ingeniería
Universidad de Guadalajara*



Publicaciones Electrónicas
Sociedad Matemática Mexicana

Índice general

1. Teoría de grupos básica	7
1.1. Grupos	8
1.1.1. Operaciones binarias	8
1.1.2. Grupos	9
1.1.3. Ejercicios	19
1.2. Subgrupos y clases laterales	21
1.2.1. Subgrupos	21
1.2.2. Clases laterales	25
1.2.3. Ejercicios	30
1.3. Subgrupos normales y cocientes	33
1.3.1. Subgrupos normales	33
1.3.2. Grupos cocientes	36
1.3.3. Ejercicios	39
1.4. Homomorfismos	41
1.4.1. Homomorfismos	41
1.4.2. Isomorfismos	44
1.4.3. Ejercicios	49
2. Tipos particulares de grupos	53
2.1. Grupos cíclicos	53
2.1.1. Estructura	53
2.1.2. Homomorfismos de \mathbb{Z}_n a \mathbb{Z}_m .	59
2.1.3. Ejercicios	63
2.2. Grupos abelianos	65
2.2.1. Sumas directas	65
2.2.2. Teorema fundamental de grupos abelianos finitos	67
2.2.3. Ejercicios	72
2.3. Grupos de permutaciones	73
2.3.1. Grupo simétrico	73
2.3.2. Notación cíclica	76
2.3.3. Grupo alternante	82
2.3.4. Ejercicios	87
3. Temas selectos	91
3.1. Acciones de grupos	91
3.1.1. Definiciones y ejemplos	91
3.1.2. Órbitas y estabilizadores	96
3.1.3. Aplicación: conteo de collares	99
3.1.4. Ejercicios	106
3.2. Teoría de Sylow	109
3.2.1. La ecuación de clase	109
3.2.2. Teoremas de Sylow	111
3.2.3. Aplicaciones de la teoría de Sylow	116

3.2.4. Ejercicios	120
3.3. Demostración del Teorema Fundamental de Grupos Abelianos Finitos	122
A. Apéndice A: Prerrequisitos	125
A.1. Teoría de números elemental	125
A.2. Relaciones de equivalencia	128
B. Apéndice B: Proyectos Finales	131

Prefacio

La *teoría de grupos* se encarga del estudio de las estructuras algebraicas conocidas como *grupos*. Debido a su definición sencilla y concisa, los grupos aparecen en casi todas las ramas de las matemáticas puras y aplicadas, e incluso en otras ciencias como física, química, ciencias de materiales y ciencias computacionales.

Los grupos surgieron en el estudio del matemático francés Évariste Galois sobre la insolubilidad de ecuaciones polinómicas de grado 5 o superior, al presentarse como conjuntos de simetrías de las raíces de un polinomio. Parte de la gran trascendencia de los grupos se debe a que capturan perfectamente el concepto de *simetría*, pensado como la transformación de un objeto que no modifica sus propiedades esenciales. Así pues, podemos pensar en simetrías de objetos geométricos, de estructuras moleculares, o de espacios multidimensionales. Por tal motivo, se han convertido en herramientas fundamentales para el estudio de temas como las simetrías moleculares, la criptografía de llave pública, y la física de partículas.

Este texto es una introducción a la teoría de grupos, con énfasis en grupos finitos, el cual fue elaborado para la clase de Teoría de Grupos de la Licenciatura en Matemáticas de la Universidad de Guadalajara. Incluye temas básicos como la definición de grupo, subgrupos, clases laterales, el Teorema de Lagrange, subgrupos normales, grupos cociente, homomorfismos, isomorfismos, automorfismos y los Teoremas de Isomorfía. Además, incluye secciones especializadas en los siguientes tipos de grupos:

1. Grupos cíclicos, donde se examinan los subgrupos de un grupo cíclico y los homomorfismos entre ellos.
2. Grupos abelianos, donde se enuncia y aplica el Teorema Fundamental de Grupos Abelianos Finitos;
3. Grupos de permutaciones, donde se definen y estudian las propiedades básicas de los grupos simétricos y alternantes.

Finalmente, las últimas secciones presentan temas sobre acciones de grupos, incluyendo las demostraciones del Teorema Órbita-Estabilizador, el Teorema de Cayley, y el Teorema de Cauchy-Frobenius, y sobre la teoría de Sylow, incluyendo las demostraciones del Teorema de Cauchy, los tres Teoremas de Sylow, y el Teorema Fundamental de Grupos Abelianos Finitos. El texto también incluye dos apéndices: el primero cubre los prerrequisitos necesarios de teoría de números elemental y relaciones de equivalencia, mientras que el segundo incluye una lista de sugerencias para que los estudiantes de un curso elaboren un proyecto final.

Mi sincero agradecimiento a todos los estudiantes de la Universidad de Guadalajara que han tomado mi clase de Teoría de Grupos y que han colaborado en la revisión de este texto; en particular, mi agradecimiento a Yannick Selwyn Escalera Hernández, estudiante de la Licenciatura en Física, Román Zúñiga

Macías, Oscar Omar Hernández e Ismael Romo Alvarado, estudiantes de la Licenciatura en Matemáticas, por su valiosa ayuda en la escritura y revisión del texto.

Termino con algunas aclaraciones breves sobre la notación usada:

1. El conjunto de los números naturales, denotado por \mathbb{N} , incluye al 0, es decir, $\mathbb{N} = \{0, 1, 2, 3, \dots\}$.
2. Denotamos por \mathbb{Z} y \mathbb{Z}_+ a los conjuntos de enteros y enteros positivos, respectivamente.
3. Denotamos por \mathbb{Q} , \mathbb{R} y \mathbb{C} a los conjuntos de los números racionales, reales y complejos, respectivamente.

1

Teoría de grupos básica

1.1. Grupos

En esta sección asumo que el lector está familiarizado con los temas de teoría de números y relaciones de equivalencia abordados en el Apéndice A, así como con los conceptos básicos de lógica, teoría de conjuntos y funciones que usualmente se estudian en los primeros semestres de un programa universitario de matemáticas. Recomiendo el libro [1] para una revisión detallada de estos conceptos.

1.1.1. Operaciones binarias

Definición 1.1 (operación binaria). Sea G un conjunto no vacío. Una *operación binaria* de G es una función de la forma $f : G \times G \rightarrow G$.

En general, para verificar que una operación binaria $f : G \times G \rightarrow G$ está bien definida hay que asegurarse que realmente $f(a, b) \in G$ para cualquier $(a, b) \in G \times G$. Comúnmente llamamos a esto la propiedad de *cerradura* de la operación.

Ejemplo 1.2. Consideremos algunos ejemplos y contraejemplos.

1. La función $+$: $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ definida como $+(n, m) := n+m$ es una operación binaria del conjunto \mathbb{Z} llamada la *suma usual de números enteros*.
2. La resta **no** es una operación binaria del conjunto \mathbb{N} de números naturales porque no cumple la propiedad de cerradura (por ejemplo, $3-4 = -1 \notin \mathbb{N}$).
3. La función mcd : $\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ que asigna a cualquier par de números naturales su máximo común divisor es una operación binaria de \mathbb{N} .

Una propiedad importante de las funciones es que cada elemento del dominio tiene una única imagen en el codominio. Por lo tanto, para demostrar que una operación binaria $f : G \times G \rightarrow G$ está bien definida, además de verificar la propiedad de cerradura, hay que verificar que si $a = a'$ y $b = b'$, entonces $f(a, b) = f(a', b')$. Comprobar esto es trivial en los ejemplos anteriores, si embargo no es tan obvio cuando los elementos de G son clases de equivalencia que dependen de un representante.

Ejemplo 1.3 (suma módulo n). Sea $\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}$ el conjunto de clases de equivalencia módulo $n \in \mathbb{N}$. Así, cada $[a] \in \mathbb{Z}_n$ es una clase de equivalencia de la forma

$$[a] := \{a + kn : k \in \mathbb{Z}\}.$$

Definimos una operación binaria $f : \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n$, llamada *suma módulo n* , como

$$f([a], [b]) := [a + b], \quad \forall [a], [b] \in \mathbb{Z}_n.$$

Es obvio que f cumple la propiedad de cerradura, porque $[a + b] \in \mathbb{Z}_n$. Ahora demostraremos que si $[a] = [a']$ y $[b] = [b']$, entonces $f([a], [b]) = f([a'], [b'])$. Sabemos que $[a] = [a']$ y $[b] = [b']$ si y solo si

$$a = a' + k_1n \quad \text{y} \quad b = b' + k_2n,$$

para algunos $k_1, k_2 \in \mathbb{Z}$. Sumando las dos ecuaciones previas, obtenemos

$$(a + b) = (a' + b') + (k_1 + k_2)n,$$

lo que implica que $[a + b] = [a' + b']$. Así, $f([a], [b]) = f([a'], [b'])$.

Notación 1.4. Normalmente, denotamos con un punto \cdot a una operación binaria arbitraria de G , y denotamos como $a \cdot b$ a la imagen del par $(a, b) \in G \times G$.

1.1.2. Grupos

Un *grupo* es una estructura algebraica que consiste en un conjunto y una operación binaria que cumple tres propiedades.

Definición 1.5 (grupo). Sea G un conjunto no vacío y \cdot una operación binaria de G . El par (G, \cdot) es un *grupo* si se cumplen las siguientes propiedades:

(G1) Asociatividad. Para toda $a, b, c \in G$, se cumple que

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

(G2) Identidad. Existe un elemento $e \in G$ tal que, para toda $a \in G$,

$$e \cdot a = a \cdot e = a.$$

(G3) Inversos. Para cualquier $a \in G$ existe un $b \in G$ tal que

$$a \cdot b = b \cdot a = e.$$

El elemento $e \in G$ de la propiedad **(G2)** es llamado la *identidad* de G . El elemento $b \in G$ de la propiedad **(G3)** es llamado el *inverso* de $a \in G$ y lo denotamos como a^{-1} .

Para demostrar que (G, \cdot) es un grupo también es importante verificar lo siguiente:

(G0) La operación \cdot está *bien definida* sobre G en el sentido discutido en la sección anterior: $a \cdot b \in G$, para toda $a, b \in G$ (cerradura), y $a = a'$ y $b = b'$ implica $a \cdot b = a' \cdot b'$.

La propiedad **(G0)** está dada implícitamente en la definición 1.5 al asumir que \cdot es una operación binaria (obviamente bien definida).

Definición 1.6 (grupo abeliano). Decimos que un grupo (G, \cdot) es *abeliano* si se cumple la siguiente propiedad:

(G4) *Conmutatividad.* Para toda $a, b \in G$, se cumple que

$$a \cdot b = b \cdot a.$$

Notación 1.7. Normalmente, para simplificar notación, hacemos referencia a un grupo (G, \cdot) simplemente por el conjunto G y decimos que tiene “equipado” la operación binaria. Además, cuando la operación esté clara en el contexto, podemos escribir ab en lugar de $a \cdot b$.

Ejemplo 1.8 (números enteros). Sea $+$ la suma usual de \mathbb{Z} . Demostraremos que el conjunto \mathbb{Z} equipado con $+$ es un grupo abeliano:

(G0) La propiedad de cerradura se cumple porque $n + m \in \mathbb{Z}$ para toda $n, m \in \mathbb{Z}$. Además, obviamente si $n = n'$ y $m = m'$, entonces $n + m = n' + m'$. Por lo tanto, $+$ está bien definida sobre \mathbb{Z} .

(G1) Para toda $n, m, k \in \mathbb{Z}$, se cumple que $(n + m) + k = n + (m + k)$.

(G2) La identidad es $0 \in \mathbb{Z}$ porque $0 + n = n + 0 = n$, para toda $n \in \mathbb{Z}$.

(G3) El inverso de cualquier $n \in \mathbb{Z}$ es $-n \in \mathbb{Z}$ porque $n + (-n) = (-n) + n = 0$.

(G4) Para toda $n, m \in \mathbb{Z}$, se cumple que $n + m = m + n$.

Ejemplo 1.9 (grupo trivial). Consideremos un conjunto con un solo elemento $G = \{e\}$ y una operación binaria \cdot definida como $e \cdot e = e$. Las propiedades **G0-G3** se cumplen trivialmente, así que $\{e\}$ es un grupo al cual llamamos el *grupo trivial*.

Ejemplo 1.10 (enteros módulo n). El conjunto \mathbb{Z}_n de clases de equivalencia módulo n equipado con la suma módulo n es un grupo abeliano:

(G0) Por el ejemplo 1.3, la suma módulo n está bien definida sobre \mathbb{Z}_n .

(G1) Para toda $[a], [b], [c] \in \mathbb{Z}_n$, se cumple que

$$([a] + [b]) + [c] = [(a + b) + c] = [a + (b + c)] = [a] + ([b] + [c]).$$

(G2) La identidad es $[0] \in \mathbb{Z}_n$ porque $[0] + [a] = [0 + a] = [a]$ y $[a] + [0] = [a + 0] = [a]$, para toda $[a] \in \mathbb{Z}_n$.

(G3) El inverso de cualquier $[a] \in \mathbb{Z}_n$ es $[-a] \in \mathbb{Z}_n$ porque $[a] + [-a] = [a + (-a)] = [0]$ y $[-a] + [a] = [(-a) + a] = [0]$.

(G4) Para toda $[a], [b] \in \mathbb{Z}_n$, se cumple que $[a] + [b] = [a + b] = [b + a] = [b] + [a]$.

Definición 1.11 (orden de un grupo). El *orden* de un grupo G , denotado por $|G|$ es simplemente la cardinalidad del conjunto G . Decimos que G es *finito* si su orden es finito, y en caso contrario decimos que es *infinito*.

Ejemplo 1.12. Los siguientes son más ejemplos básicos:

1. Si $(F, +, \times)$ es un campo, tanto $(F, +)$ como (F^*, \times) , donde $F^* = F - \{0\}$, son grupos abelianos.
2. Si $(V, +, \cdot)$ es un espacio vectorial, entonces $(V, +)$ es un grupo abeliano.
3. Sea $i \in \mathbb{C}$ la unidad imaginaria. El conjunto $G = \{1, -1, i, -i\}$ equipado con la multiplicación de números complejos es un grupo abeliano.
4. Sea $\text{GL}_n(F)$ el conjunto de matrices invertibles de $n \times n$ con entradas en un campo F . Para toda $n \geq 2$, el conjunto $\text{GL}_n(F)$, equipado con la multiplicación de matrices, es un grupo llamado el *grupo general lineal de grado n sobre F* . Este grupo es no abeliano, ya que siempre podemos encontrar un par de matrices que no conmutan (Ejercicio 1.4).
5. Para cualquier $n \geq 3$, sea D_{2n} el conjunto de *simetrías* (es decir, funciones que no alteran ni la estructura ni la posición) de un polígono regular con n lados. Si ρ representa una rotación que envía cada vértice a su vecino inmediato, y h representa una reflexión a través de algún eje, entonces

$$D_{2n} = \{\text{id}, \rho, \rho^2, \dots, \rho^{n-1}, h, h\rho, h\rho^2, \dots, h\rho^{n-1}\},$$

donde id representa a la función identidad. El conjunto D_{2n} , equipado con la composición de funciones, es un grupo llamado el *grupo diédrico de orden $2n$* . Los elementos de D_{2n} cumplen las siguientes relaciones, las cuales son suficientes para operar dos elementos cualesquiera,

$$\rho^n = \text{id}, \quad h^2 = \text{id}, \quad h\rho = \rho^{n-1}h.$$

Por ejemplo,

$$(h\rho^2)(h\rho) = (\rho^{-2}h)(h\rho) = \rho^{-2}h^2\rho = \rho^{-2}\rho = \rho^{-1} = \rho^{-1}\rho^n = \rho^{n-1}.$$

Ejemplo 1.13 (grupo de unidades módulo n). Para toda $n \geq 1$, definimos

$$U(n) := \{[a] \in \mathbb{Z}_n : \text{mcd}(a, n) = 1\}.$$

Este conjunto, equipado con la multiplicación $[a] \cdot [b] := [ab]$, es un grupo abeliano:

(G0) Para demostrar la cerradura de la operación es necesario verificar que $[ab] \in U(n)$, para toda $[a], [b] \in U(n)$. Esto es equivalente a demostrar que si $\text{mcd}(a, n) = 1$ y $\text{mcd}(b, n) = 1$, entonces $d := \text{mcd}(ab, n) = 1$. Supongamos que $d > 1$ y sea p un divisor primo de d . Como $p \mid ab$ entonces $p \mid a$ o $p \mid b$, por el Lema de Euclides. Sin perder generalidad, supongamos que $p \mid a$. Además, $p \mid d \mid n$, así que $p \mid \text{mcd}(a, n) = 1$, lo cual contradice que p sea un número primo. Por lo tanto, $d = 1$.

Supongamos ahora que $[a] = [a']$ y $[b] = [b']$. Entonces $a = a' + k_1n$ y $b = b' + k_2n$, para algunos $k_1, k_2 \in \mathbb{Z}$. Luego,

$$[ab] = [(a' + k_1n)(b' + k_2n)] = [a'b' + a'k_2n + b'k_1n + k_1k_2n^2] = [a'b'].$$

Por lo tanto, $[a][b] = [a'][b']$. Esto demuestra que la operación está bien definida.

(G1) Para toda $[a], [b], [c] \in U(n)$, se cumple que

$$([a] \cdot [b]) \cdot [c] = [(ab)c] = [a(bc)] = [a] \cdot ([b] \cdot [c]).$$

(G2) La identidad es $[1] \in U(n)$ porque $[1] \cdot [a] = [1a] = [a]$ y $[a] \cdot [1] = [a1] = [a]$, para toda $[a] \in U(n)$.

(G3) Sea $[a] \in U(n)$. Por definición de $U(n)$, sabemos que $\text{mcd}(a, n) = 1$. Por el Lema de Bezout, existen $b, c \in \mathbb{Z}$ tales que $ab + cn = 1$. Así,

$$[1] = [ab + cn] = [ab] = [a][b].$$

Basta comprobar que $[b] \in U(n)$ para demostrar que $[b]$ es el inverso de $[a]$ en $U(n)$. Sea $d := \text{mcd}(b, n)$. Como $d \mid b$ y $d \mid n$, entonces $d \mid (ab + cn)$. Luego, $d \mid 1$, lo que implica que $d = 1$ y $[b] \in U(n)$.

(G4) Para toda $[a], [b] \in U(n)$, se cumple que $[a] \cdot [b] = [ab] = [ba] = [b] \cdot [a]$.

Observación 1.14. Observemos que la definición del grupo $U(n)$ no depende de los representantes que se tomen, ya que si $[a] = [a']$, entonces $\text{mcd}(a, n) = 1$ si y solo si $\text{mcd}(a', n) = 1$ (Ejercicio 1.5).

Observación 1.15. Para simplificar el lenguaje, cuando consideramos un grupo arbitrario G nos referimos a su operación binaria como “multiplicación” o “producto”, aunque ésta no necesariamente coincida con la multiplicación o producto usual de números. Obviamente, una excepción de esto ocurre cuando el grupo está equipado con una operación binaria denotada por el signo $+$. Más adelante puntualizaremos más a fondo estas diferencias en la notación.

Enunciaremos algunos resultados básicos.

Lema 1.16 (propiedades básicas de grupos). Sea G un grupo.

1. *Cancelación derecha.* Para toda $a, b, c \in G$, si $ac = bc$, entonces $a = b$.
2. *Cancelación izquierda.* Para toda $a, b, c \in G$, si $ca = cb$, entonces $a = b$.
3. *Unicidad de la identidad.* La identidad e de G es única.
4. *Unicidad de los inversos.* Para toda $a \in G$, el inverso de a es único.
5. *Inverso del inverso.* Para toda $a \in G$, $(a^{-1})^{-1} = a$.

6. *Inverso de un producto.* Para toda $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.

Demostración.

1. Observemos que las siguientes igualdades son equivalentes:

$$\begin{aligned} ac &= bc \\ (ac)c^{-1} &= (bc)c^{-1} \\ a(cc^{-1}) &= b(cc^{-1}) \\ ae &= be \\ a &= b. \end{aligned}$$

2. Ejercicio 1.6.

3. Supongamos que e y e' son identidades de G . Por la propiedad **G2**, tenemos que $ea = a = e'a$. Luego, por cancelación derecha, $e = e'$.

4. Ejercicio 1.7.

5. Como $(a^{-1})^{-1}$ es el inverso de a^{-1} , debe satisfacer que $(a^{-1})^{-1}a^{-1} = e$. Además, sabemos que $aa^{-1} = e$. Luego, $(a^{-1})^{-1}a^{-1} = aa^{-1}$, y por cancelación derecha obtenemos que $(a^{-1})^{-1} = a$.

6. Ejercicio 1.8.

□

Definición 1.17 (potencias). Sea G un grupo y $g \in G$. Para $k \in \mathbb{Z}$, definimos la k -ésima potencia de g de la siguiente manera:

$$g^k := \begin{cases} e & k = 0, \\ \underbrace{g \cdot g \cdot g \cdots g}_{k \text{ veces}} & \text{para } k > 0, \\ \underbrace{g^{-1} \cdot g^{-1} \cdots g^{-1}}_{-k \text{ veces}} & \text{para } k < 0. \end{cases}$$

Lema 1.18 (potencias). Sea G un grupo y $g \in G$.

1. Para toda $k, s \in \mathbb{Z}$, $g^k \cdot g^s = g^{k+s}$.
2. Para toda $k \in \mathbb{Z}$, $(g^k)^{-1} = g^{-k}$.
3. Para toda $k, s \in \mathbb{Z}$, $(g^k)^s = g^{ks}$.

Demostración.

1. Analizaremos varios casos. Si $k > 0$ y $s > 0$, entonces

$$g^k \cdot g^s = \underbrace{g \cdot g \cdots g}_{k \text{ veces}} \cdot \underbrace{g \cdot g \cdots g}_{s \text{ veces}} = \underbrace{g \cdot g \cdots g}_{k+s \text{ veces}} = g^{k+s}.$$

Si $k > 0$, $s < 0$, y $k > -s$, entonces

$$g^k \cdot g^s = \underbrace{g \cdot g \cdots g}_{k \text{ veces}} \cdot \underbrace{g^{-1} \cdot g^{-1} \cdots g^{-1}}_{-s \text{ veces}} = \underbrace{g \cdot g \cdots g}_{k-(-s) \text{ veces}} \cdot e \cdots e = g^{k+s}.$$

Si $k > 0$, $s < 0$, y $k < -s$, entonces

$$g^k \cdot g^s = \underbrace{g \cdot g \cdots g}_{k \text{ veces}} \cdot \underbrace{g^{-1} \cdot g^{-1} \cdots g^{-1}}_{-s \text{ veces}} = e \cdots e \cdot \underbrace{g^{-1} \cdot g^{-1} \cdots g^{-1}}_{-s-k \text{ veces}} = g^{k+s}.$$

Si $k < 0$ y $s < 0$, entonces

$$g^k \cdot g^s = \underbrace{g^{-1} \cdot g^{-1} \cdots g^{-1}}_{-k \text{ veces}} \cdot \underbrace{g^{-1} \cdot g^{-1} \cdots g^{-1}}_{-s \text{ veces}} = \underbrace{g^{-1} \cdot g^{-1} \cdots g^{-1}}_{-k-s \text{ veces}} = g^{k+s}.$$

Los otros casos (como $k < 0$ y $s > 0$, o $k = 0$) se analizan de manera similar. Por lo tanto, siempre se cumple que $g^k \cdot g^s = g^{k+s}$.

2. Observemos que $g^k g^{-k} = g^{k+(-k)} = g^0 = e$. Por lo tanto, $(g^k)^{-1} = g^{-k}$
3. Si $s > 0$, tenemos que

$$(g^k)^s = \underbrace{g^k \cdot g^k \cdots g^k}_{s \text{ veces}} = g^{\underbrace{k+k+\cdots+k}_{s \text{ veces}}} = g^{ks}.$$

Si $s < 0$,

$$(g^k)^s = \underbrace{g^{-k} \cdot g^{-k} \cdots g^{-k}}_{-s \text{ veces}} = g^{\underbrace{-k-k-\cdots-k}_{-s \text{ veces}}} = g^{(-k)(-s)} = g^{ks}.$$

□

Notación 1.19. En la definición de potencias usamos la “notación multiplicativa” de un grupo, aunque la operación binaria \cdot puede ser arbitraria. Sin embargo, algunas veces es más conveniente usar la “notación aditiva” en un grupo (como en \mathbb{Z} y \mathbb{Z}_n), y en tales casos una potencia corresponde más bien a una suma iterada. Por lo tanto, cuando usemos notación aditiva, escribiremos kg en lugar de g^k :

$$kg := \begin{cases} 0 & k = 0, \\ \underbrace{g + g + \cdots + g}_{k \text{ veces}} & \text{para } k > 0, \\ \underbrace{(-g) + (-g) + \cdots + (-g)}_{-k \text{ veces}} & \text{para } k < 0. \end{cases}$$

El Cuadro 1.1 resume algunas diferencias entre la notación multiplicativa y la aditiva.

Notación	Operación binaria	Identidad	Inversos	k -Ésima potencia
Multiplicativa	\cdot, \times	$e, 1$	g^{-1}	g^k
Aditiva	$+$	0	$-g$	kg

Cuadro 1.1: Notaciones multiplicativa y aditiva

Definición 1.20 (orden de un elemento). Sea G un grupo y $g \in G$. Decimos que g es de *orden finito* si existe $k \in \mathbb{Z}_+$ tal que $g^k = e$; en otro caso, decimos que g es de *orden infinito*. Si g es de orden finito, el *orden* de g , denotado por $|g|$, es el mínimo entero positivo n tal que $g^n = e$; es decir,

$$|g| := n = \min\{k \in \mathbb{Z}_+ : g^k = e\}.$$

Si g es de orden infinito, escribimos $|g| = \infty$.

Ejemplo 1.21. En \mathbb{Z}_4 , el orden de $[1]$ es 4 porque

$$\begin{aligned} [1] &\neq [0] \\ [1] + [1] &\neq [0] \\ [1] + [1] + [1] &\neq [0] \\ [1] + [1] + [1] + [1] &= [0]. \end{aligned}$$

Por otro lado, el orden de $[2]$ es 2 porque

$$\begin{aligned} [2] &\neq [0] \\ [2] + [2] &= [0]. \end{aligned}$$

Ejemplo 1.22. En $U(5)$, el orden de $[3]$ es 4 porque

$$\begin{aligned} [3] &\neq [1] \\ [3]^2 &= [9] \neq [1] \\ [3]^3 &= [27] \neq [1] \\ [3]^4 &= [81] = [1]. \end{aligned}$$

Ejemplo 1.23. Consideremos al grupo \mathbb{C}^* con la multiplicación. Entonces,

$$|1| = 1, \quad |i| = 4, \quad |2| = \infty.$$

Lema 1.24 (orden de un elemento en un grupo finito). Si G es un grupo finito, entonces todos sus elementos son de orden finito.

Demostración. Sea $g \in G$. Consideremos la lista infinita de potencias positivas de g :

$$g, g^2, g^3, g^4, \dots$$

Todas estas potencias están en G por cerradura. Como G es finito, esta lista debe tener alguna repetición, digamos $g^k = g^s$, donde, sin perder generalidad, $k > s$. Luego, $g^t = e$, donde $t := k - s \in \mathbb{Z}_+$. Por lo tanto, g es de orden finito. \square

Lema 1.25 (orden de un elemento). Sea G un grupo y $g \in G$ un elemento de orden finito. Si $g^k = e$, entonces $|g| \mid k$.

Demostración. Sea $n := |g|$. Por el Algoritmo de la División, existen $q, r \in \mathbb{Z}$, tales que

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

Observemos que

$$g^r = g^{k-qn} = g^k (g^n)^{-q} = ee^{-q} = e,$$

porque $g^k = e$ y $g^n = e$. Por reducción al absurdo, supongamos que $r \neq 0$. Luego, r es un entero positivo menor que n tal que $g^r = e$, lo que contradice que n sea el orden de g . Por lo tanto, $r = 0$ y $n \mid k$. \square

Si G es un grupo finito con $|G| = m$, podemos escribir una tabla $T = (t_{i,j})$, llamada la *tabla de Cayley* de (G, \cdot) , con m filas y m columnas, que determina completamente el comportamiento de la operación binaria del grupo. Para esto, ordenamos de manera arbitraria los elementos del grupo, $G = \{g_1, g_2, \dots, g_m\}$, donde $g_i \neq g_j$ para toda $i \neq j$, y definimos la entrada (i, j) de T como $t_{i,j} := g_i g_j$.

Ejemplo 1.26 (\mathbb{Z}). El Cuadro 1.2 muestra la tabla de Cayley de \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]

Cuadro 1.2: Tabla de Cayley de \mathbb{Z}_5

Notación 1.27. A partir de ahora, representaremos la clase $[a] \in \mathbb{Z}_n$ simplemente como a . Esto nos ayudará a simplificar la notación, pero hay que tener en cuenta que, en este contexto, a no representa un número, sino una clase módulo n . Con esta notación, por ejemplo, $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.

Ejemplo 1.28 ($U(8)$). El Cuadro 1.3 muestra la tabla de Cayley de $U(8)$

·	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Cuadro 1.3: Tabla de Cayley de $U(8)$

Lema 1.29 (tabla de Cayley). Sea G un grupo finito de orden m . La tabla de Cayley $T = (t_{i,j})$ de G se cumplen las siguientes propiedades:

1. No hay dos elementos iguales en una misma fila, o una misma columna, de T .
2. Todos los elementos de G deben aparecer en cada fila o columna de T .
3. G es abeliano si y solo si $t_{i,j} = t_{j,i}$, para toda $i, j = 1, \dots, m$ (i.e. T es una *matriz simétrica*).

Demostración.

1. Si $t_{i,j} = t_{i,k}$, entonces $g_i g_j = g_i g_k$. Por cancelación izquierda, $g_j = g_k$, lo que implica que $j = k$. Esto demuestra que no hay elementos repetidos en una misma fila de T . La demostración es similar para las columnas de T .
2. Cada fila o columna de T debe tener m elementos de G , los cuales deben ser todos distintos por el punto anterior. Como $|G| = m$, entonces todos los elementos de G deben aparecer en cada columna o fila de T .
3. G es abeliano si y solo si $g_i g_j = g_j g_i$ para toda i, j , lo cual se cumple si y solo si $t_{i,j} = t_{j,i}$.

□

Teorema 1.30 (suma directa). Sean G_1 y G_2 grupos. El conjunto

$$G_1 \oplus G_2 := \{(a_1, a_2) : a_1 \in G_1, a_2 \in G_2\},$$

equipado con la operación

$$(a_1, a_2) \cdot (b_1, b_2) := (a_1 b_1, a_2 b_2),$$

es un grupo llamado la *suma directa de G_1 y G_2* .

Demostración.

(G0) Claramente, $(a_1, a_2) \cdot (b_1, b_2) = (a_1 b_1, a_2 b_2) \in G_1 \oplus G_2$, para toda $(a_1, a_2), (b_1, b_2) \in G_1 \oplus G_2$. Además, la operación binaria en $G_1 \oplus G_2$ está bien definida porque las operaciones binarias en cada uno de los grupos G_1 y G_2 están bien definidas.

(G1) Para toda $(a_1, a_2), (b_1, b_2), (c_1, c_2) \in G_1 \oplus G_2$ tenemos que

$$\begin{aligned} (a_1, a_2) \cdot ((b_1, b_2) \cdot (c_1, c_2)) &= (a_1(b_1c_1), a_2(b_2c_2)) \\ &= ((a_1b_1)c_1, (a_2b_2)c_2) \\ &= ((a_1, a_2) \cdot (b_1, b_2)) \cdot (c_1, c_2). \end{aligned}$$

(G2) La identidad de $G_1 \oplus G_2$ es $(e_1, e_2) \in G_1 \oplus G_2$, donde e_i es la identidad de G_i , porque

$$(e_1, e_2) \cdot (a_1, a_2) = (a_1, a_2) = (a_1, a_2) \cdot (e_1, e_2).$$

(G3) El inverso de $(a_1, a_2) \in G_1 \oplus G_2$ es $(a_1^{-1}, a_2^{-1}) \in G_1 \oplus G_2$ porque

$$(a_1, a_2) \cdot (a_1^{-1}, a_2^{-1}) = (e_1, e_2) = (a_1^{-1}, a_2^{-1})(a_1, a_2).$$

□

Observación 1.31. El lector se habrá dado cuenta que el conjunto $G_1 \oplus G_2$ es igual al producto cartesiano $G_1 \times G_2$; la diferencia en la notación se sustenta en que $G_1 \oplus G_2$ representa un grupo equipado con la operación binaria descrita en el teorema anterior mientras que $G_1 \times G_2$ es simplemente un conjunto sin estructura algebraica.

Palabras clave: *operación binaria, grupo, grupo abeliano, orden de un grupo, orden de un elemento, tabla de Cayley, suma directa.*

1.1.3. Ejercicios

Ejercicio 1.1. Determina si las siguientes afirmaciones son verdaderas o falsas, y justifica tu respuesta:

1. La función $\max(a, b)$ que asigna a un par de números enteros el máximo de los dos es una operación binaria de \mathbb{Z} .
2. La división es una operación binaria de \mathbb{Z} .
3. El conjunto de los números impares es un grupo con la suma.
4. Si un grupo es infinito, los órdenes de todos sus elementos son infinitos.

Ejercicio 1.2. Determina si los siguientes conjuntos con operaciones son grupos. Justifica tu respuesta.

1. El conjunto de enteros impares con la suma usual.
2. El conjunto de números enteros con la operación \max .
3. El conjunto de números racionales \mathbb{Q} con operación \star definida por $a \star b = \frac{a+b}{2}$.
4. El conjunto de números reales \mathbb{R} con operación \star definida por $a \star b = a + b + ab$.

Ejercicio 1.3. Sea $G = \{a \in \mathbb{R} : a \neq -1\}$. Consideremos la operación binaria \star definida por $a \star b = a + b + ab$, $\forall a, b \in G$. Demuestra que G equipado con \star es un grupo. ¿Cuál es el inverso de $3 \in G$ en el grupo?

Ejercicio 1.4. Para toda $n \geq 2$, demuestra que el grupo $GL_n(F)$ no es abeliano.

Ejercicio 1.5. Sean $[a], [a'] \in \mathbb{Z}_n$ tales que $[a] = [a']$. Demuestra que $\text{mcd}(a, n) = 1$ si y solo si $\text{mcd}(a', n) = 1$.

Ejercicio 1.6 (cancelación izquierda). Sea G un grupo. Demuestra que, para toda $a, b, c \in G$, si $ca = cb$, entonces $a = b$.

Ejercicio 1.7 (unicidad del inverso). Sea G un grupo. Demuestra que, para toda $a \in G$, el inverso de a es único.

Ejercicio 1.8 (inverso de un producto). Sea G un grupo. Demuestra que, para toda $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.

Ejercicio 1.9. Respecto al grupo \mathbb{Z}_{36} (con la suma de clases) encuentra lo siguiente:

1. El orden del grupo.

2. Los órdenes de los elementos [6] y [11].
3. Los inversos de los elementos [6] y [11].

Ejercicio 1.10. Respecto al grupo $U(36)$ (con el producto de clases) responde lo siguiente:

1. El orden del grupo.
2. Los órdenes de los elementos [5] y [13].
3. Los inversos de los elementos [5] y [13].

Ejercicio 1.11 (órdenes de grupos y elementos). Para cada uno de los siguientes grupos, encuentra el orden del grupo y el orden de cada uno de sus elementos:

$$\mathbb{Z}_{12}, U(10), U(12).$$

Ejercicio 1.12 (grupos módulo n). Escribe las tablas de Cayley de \mathbb{Z}_4 y \mathbb{Z}_6 .

Ejercicio 1.13 (grupos de unidades módulo n). Escribe las tablas de Cayley de $U(10)$ y $U(12)$.

Ejercicio 1.14 (grupos diédricos). Escribe las tablas de Cayley de D_6 y D_8 .

Ejercicio 1.15. Sea G un grupo. Demuestra que $(ab)^2 = a^2b^2$, para todo $a, b \in G$, si y solo si G es abeliano.

Ejercicio 1.16. Sea G un grupo. Demuestra que $(ab)^{-1} = a^{-1}b^{-1}$, para todo $a, b \in G$, si y solo si G es abeliano.

Ejercicio 1.17 (cancelación cruzada). Sea G un grupo con la siguiente propiedad: si $a, b, c \in G$ cumplen que $ab = ca$, entonces $b = c$. Demuestra que G es abeliano.

Ejercicio 1.18. Sea G un grupo finito tal que para toda $g \in G - \{e\}$ se cumple que $|g| = 2$. Demuestra que G es abeliano.

Ejercicio 1.19. Sea G un grupo y sean $g, h \in G$. Demuestra que $|gh| = |hg|$.

Ejercicio 1.20 (★). Usando solo resultados elementales (es decir, sin usar el Teorema de Cauchy), demuestra que si un grupo G tiene orden par, entonces existe un elemento en G de orden 2.

1.2. Subgrupos y clases laterales

1.2.1. Subgrupos

Si G es un grupo con operación \cdot y H un subconjunto de G , denotamos por \cdot_H a la restricción de \cdot en H ; en otras palabras, \cdot_H es la función $\cdot_H : H \times H \rightarrow G$ definida como

$$a \cdot_H b = a \cdot b, \text{ donde } a, b \in H.$$

Definición 1.32 (subgrupo). Sea G un grupo con operación \cdot y $H \subseteq G$. Decimos que H es un *subgrupo* de G , y escribimos $H \leq G$, si el par (H, \cdot_H) es en sí mismo un grupo.

Decimos que H es un *subgrupo propio* de G , y escribimos $H < G$, si $H \leq G$ pero $H \neq G$.

Teorema 1.33 (test del subgrupo 1). Sea G un grupo. Un subconjunto H de G es un subgrupo de G si y solo si se cumplen las siguientes propiedades:

(S1) *Cerradura en H .* Para toda $a, b \in H$, se cumple que $a \cdot b \in H$.

(S2) *Identidad en H .* $e \in H$, donde e es la identidad de G .

(S3) *Inversos en H .* Para cualquier $a \in H$, se cumple que $a^{-1} \in H$.

Demostración.

(\Rightarrow) Si H es un subgrupo de G , entonces el par (H, \cdot_H) es un grupo y claramente se cumplen las propiedades (S1)-(S3).

(\Leftarrow) Supongamos que se cumplen las propiedades (S1)-(S3). Demostraremos que (H, \cdot_H) es un grupo:

(G0) La propiedad (S1) garantiza que \cdot_H es una función de la forma $H \times H \rightarrow H$, así que \cdot_H está bien definida.

(G1) Como G es un grupo, se cumple la propiedad asociativa para todos sus elementos; en particular, se cumple la propiedad asociativa para todos los elementos de $H \subseteq G$.

(G2) Por (S2), el elemento identidad de G está en H , y por lo tanto es el elemento identidad de H .

(G3) Por (S3), todos los elementos de H tienen un inverso.

□

Notación 1.34. Para simplificar notación, si (H, \cdot_H) es un subgrupo de (G, \cdot) , denotamos la operación \cdot_H con el mismo símbolo que la operación de (G, \cdot) .

Ejemplo 1.35. Dado cualquier grupo G , los conjuntos $\{e\}$ y G siempre son subgrupos de G .

Teorema 1.36 (test del subgrupo 2). Sea G un grupo. Un subconjunto H de G es un subgrupo de G si y solo si $H \neq \emptyset$ y, para toda $a, b \in H$, se cumple que $a^{-1}b \in H$.

Demostración.

(\Rightarrow) Si $H \leq G$, entonces $H \neq \emptyset$, por definición de grupo, y además se cumple $a^{-1}b \in H$ para toda $a, b \in H$ por las propiedades **(S1)** y **(S3)**.

(\Leftarrow) Supongamos que $H \subseteq G$ cumple que $H \neq \emptyset$ y $a^{-1}b \in H$ para toda $a, b \in H$. Para demostrar que H es un subgrupo de G usaremos el Test del Subgrupo 1:

(S2) Identidad en H . Como $H \neq \emptyset$, sea $h \in H$. Entonces, $e = h^{-1}h \in H$.

(S3) Inversos en H . Para cualquier $a \in H$, tenemos que $a^{-1} = a^{-1}e \in H$.

(S1) Cerradura en H . Para toda $a, b \in H$, la parte anterior implica que $a^{-1} \in H$, y por lo tanto $ab = (a^{-1})^{-1}b \in H$.

□

Teorema 1.37 (test del subgrupo para grupos finitos). Sea G un grupo finito. Un subconjunto H de G es un subgrupo de G si y solo si $H \neq \emptyset$ y, para toda $a, b \in H$, se cumple que $ab \in H$.

Demostración.

(\Rightarrow) Si $H \leq G$, entonces claramente $H \neq \emptyset$ y $ab \in H$ para toda $a, b \in H$.

(\Leftarrow) Supongamos que $H \subseteq G$ cumple que $H \neq \emptyset$ y que H cumple la cerradura. Usaremos el Test del Subgrupo 1:

(S1) Cerradura en H . Esta propiedad está dada por hipótesis.

(S2) Identidad en H . Como $H \neq \emptyset$, existe un $h \in H$. Por el Lema 1.24, existe $t > 0$ tal que $h^t = e$. Como $h^t \in H$ por cerradura, obtenemos que $e \in H$.

(S3) Inversos en H . Sea $h \in H$ arbitrario. Si $h = e$, entonces $h^{-1} = e \in H$ por el punto (S2). Supongamos que $h \neq e$. Por el Lema 1.24, existe $t > 0$ tal que $h^t = e$. De hecho, $t > 1$, ya que $t = 1$ implica que $h = e$, contradiciendo el supuesto. Luego $hh^{t-1} = e$ implica que $h^{-1} = h^{t-1}$. Además, $t - 1 > 0$, así que $h^{-1} = h^{t-1} \in H$ por cerradura.

□

Definición 1.38 (subgrupo cíclico generado por g). Sea G un grupo. Definimos al *grupo cíclico generado por $g \in G$* como el conjunto

$$\langle g \rangle = \{g^k : k \in \mathbb{Z}\}.$$

Si la operación de G está escrita de forma aditiva, entonces

$$\langle g \rangle = \{kg : k \in \mathbb{Z}\}.$$

Teorema 1.39 (subgrupo cíclico generado por g). Sea G un grupo y $g \in G$. Entonces, $\langle g \rangle$ es un subgrupo abeliano de G .

Demostración. Usaremos el Teorema 1.33 del test del subgrupo y verificaremos que cumple la propiedad conmutativa:

(S1) Para toda $g^k, g^s \in \langle g \rangle$, tenemos que $g^k g^s = g^{k+s} \in \langle g \rangle$.

(S2) Por definición, $e = g^0 \in \langle g \rangle$.

(S3) El inverso de cualquier $g^k \in \langle g \rangle$ es g^{-k} , el cual es claramente un elemento de $\langle g \rangle$.

(G4) Para toda $g^k, g^s \in \langle g \rangle$, tenemos que $g^k g^s = g^{k+s} = g^{s+k} = g^s g^k$.

□

Teorema 1.40 (orden de $\langle g \rangle$). Sea G un grupo y $g \in G$ un elemento de orden finito. Si $d := |g|$,

$$\langle g \rangle = \{e, g, g^2, \dots, g^{d-1}\}.$$

En particular,

$$|\langle g \rangle| = |g|.$$

Demostración. Claramente, $S := \{e, g, g^2, \dots, g^{d-1}\} \subseteq \langle g \rangle$. Para demostrar la otra contención, sea $g^k \in \langle g \rangle$, con $k \in \mathbb{Z}$, un elemento arbitrario. Usamos el Algoritmo de la División entre k y $d := |g|$:

$$k = qd + r, \quad \text{donde } q, r \in \mathbb{Z}, \text{ y } 0 \leq r < d.$$

Observemos que $g^r \in S$ y $g^r = g^{k-qd} = g^k (g^d)^{-q} = g^k$, porque $g^d = e$. Por lo tanto, $g^k = g^r \in S$.

Para demostrar que $|\langle g \rangle| = d$ basta con verificar que todos los elementos de S son distintos. Efectivamente, si $g^i = g^j$ para algunos $0 \leq i < j < d$, entonces $g^{j-i} = e$ donde $0 < j - i < d$, lo que contradice que d sea el menor entero positivo tal que $g^d = e$. □

Definición 1.41 (grupo cíclico). Decimos que un grupo G es *cíclico* si existe $g \in G$ tal que $G = \langle g \rangle$.

Ejemplo 1.42. Para cualquier $n \in \mathbb{N}$, el grupo \mathbb{Z}_n es cíclico. Demostraremos que $\mathbb{Z}_n = \langle [1] \rangle$. Para cualquier $[k] \in \mathbb{Z}_n$,

$$[k] = \underbrace{[1] + [1] + \dots + [1]}_{k \text{ veces}} = k[1].$$

Por lo tanto,

$$\langle [1] \rangle := \{k[1] : k \in \mathbb{Z}\} = \{[k] : k \in \mathbb{Z}\} = \mathbb{Z}_n.$$

Ejemplo 1.43. El grupo \mathbb{Z} es cíclico porque $\mathbb{Z} = \langle 1 \rangle$. Para cada $n \in \mathbb{Z}$, denotamos al subgrupo cíclico generado por n como $n\mathbb{Z}$, es decir

$$n\mathbb{Z} = \langle n \rangle = \{kn : k \in \mathbb{Z}\}.$$

Ejemplo 1.44. Los subgrupos cíclicos de \mathbb{Z}_6 son:

$$\begin{aligned} \langle 0 \rangle &= \{0\} \\ \langle 1 \rangle &= \{0, 1, 2, 3, 4, 5\} = \langle 5 \rangle \\ \langle 2 \rangle &= \{0, 2, 4\} = \langle 4 \rangle \\ \langle 3 \rangle &= \{0, 3\}. \end{aligned}$$

Observación 1.45. Si $G = \langle g \rangle$ es un grupo cíclico, entonces es abeliano: en efecto, para cualquier $g^k, g^s \in \langle g \rangle$, tenemos que $g^k g^s = g^{k+s} = g^{s+k} = g^s g^k$.

Teorema 1.46 (centro). Sea G un grupo. El conjunto

$$Z(G) := \{g \in G : gh = hg, \forall h \in G\}$$

es un subgrupo abeliano de G , llamado el *centro de G* .

Demostración. Usaremos el Teorema 1.33 del test del subgrupo y verificaremos que cumple la propiedad conmutativa:

(S1) Sean $g_1, g_2 \in Z(G)$, así que g_1 y g_2 conmutan con cualquier elemento de G . Luego, para toda $h \in G$,

$$(g_1 g_2)h = g_1 h g_2 = h(g_1 g_2), \implies g_1 g_2 \in Z(G).$$

(S2) Sabemos que la identidad conmuta con cualquier elemento de G , así que $e \in Z(G)$.

(S3) Sea $g \in Z(G)$. Entonces, para toda $h \in G$,

$$gh = hg \implies hg^{-1} = g^{-1}h \implies g^{-1} \in Z(G).$$

(G4) Claramente, para toda $g_1, g_2 \in Z(G)$, tenemos que $g_1 g_2 = g_2 g_1$.

□

Observación 1.47. Un grupo G es abeliano si y solo si $Z(G) = G$.

Observación 1.48. Sean H y K subgrupos de un grupo G . En general, la unión $H \cup K$ no es un subgrupo de G (Ejercicio 1.23), pero la intersección $H \cap K$ siempre es un subgrupo de G (Ejercicio 1.22).

El producto de los subgrupos H y K está definido por

$$HK := \{hk : h \in H, k \in K\},$$

el cual no es necesariamente un subgrupo de G . En el caso finito, podemos deducir la siguiente fórmula importante para la cardinalidad del conjunto HK .

Proposición 1.49 (fórmula del producto). Sean H y K subgrupos de un grupo finito G . Entonces,

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Demostración. Ejercicio 1.42. □

1.2.2. Clases laterales

Definición 1.50 (clase lateral). Sea H un subgrupo de un grupo G y $a \in G$. La *clase lateral izquierda* de H en G con representante a es el conjunto

$$aH := \{ah : h \in H\}.$$

Similarmente, la *clase lateral derecha* de H en G con representante a es el conjunto

$$Ha := \{ha : h \in H\}.$$

En esta sección demostraremos resultados principalmente sobre clases laterales izquierdas, aunque debe ser claro que hay resultados análogos para clases laterales derechas.

Lema 1.51 (mód(H)). Sea H un subgrupo de un grupo G . Las clases laterales izquierdas de H en G son las clases de equivalencia de la relación de equivalencia mód (H) definida como sigue: para toda $a, b \in G$,

$$a \equiv b \pmod{H} \iff \exists h \in H : a = bh.$$

Demostración. Demostraremos primero que la relación mód (H) es una relación de equivalencia sobre G :

(E1) *Reflexividad.* $a \equiv a \pmod{H}$ porque $a = ae$, donde $e \in H$.

(E2) *Simetría.* Si $a \equiv b \pmod{H}$, entonces $a = bh$ para algún $h \in H$. Luego, $b = ah^{-1}$ con $h^{-1} \in H$, lo que implica que $b \equiv a \pmod{H}$.

(E3) *Transitividad.* Supongamos que $a \equiv b \pmod{H}$ y $b \equiv c \pmod{H}$. Entonces, $a = bh_1$ y $b = ch_2$, donde $h_1, h_2 \in H$. Luego, $a = (ch_2)h_1 = c(h_2h_1)$, con $h_2h_1 \in H$. Esto implica que $a \equiv c \pmod{H}$.

Finalmente, observemos que la clase de equivalencia de $a \in G$ bajo esta relación es:

$$\begin{aligned} [a] &:= \{b \in G : b \equiv a \pmod{H}\} \\ &= \{b \in G : b = ah, h \in H\} \\ &= \{ah : h \in H\} = aH. \end{aligned}$$

□

Notación 1.52. Para cualquier $H \leq G$, denotamos por G/H al conjunto de clases laterales izquierdas de H en G , es decir,

$$G/H := \{aH : a \in G\}.$$

Lema 1.53 (igualdad de clases laterales). Sea H un subgrupo de un grupo G y $a, b \in G$. Entonces,

$$aH = bH \Leftrightarrow b \in aH \Leftrightarrow a^{-1}b \in H.$$

Demostración. Como aH y bH son clases de equivalencia, sabemos que $aH = bH$ si y solo si $a \equiv b \pmod{H}$. Ahora, observemos que

$$a \equiv b \pmod{H} \Leftrightarrow b = ah \text{ para algún } h \in H \Leftrightarrow b \in aH.$$

Para demostrar la segunda equivalencia, solo hay que observar que $b = ah$ para algún $h \in H$ si y solo si $a^{-1}b \in H$. \square

Corolario 1.54. Sea H un subgrupo de un grupo G y $a \in G$. Entonces, $aH = eH$ si y solo si $a \in H$.

Observación 1.55. Una clase lateral aH de H en G en general no es un subgrupo de G . De hecho, si aH es un subgrupo, entonces $e \in aH$, y por el lema anterior, $aH = eH$. Por lo tanto, la única clase lateral de H en G que es un subgrupo de G es $eH = H$.

Notación 1.56. Cuando la operación de un grupo G se escribe en notación aditiva, denotamos por $a + H$ a la clase lateral izquierda de un subgrupo H en G con representante $a \in G$.

Ejemplo 1.57. Consideremos el subgrupo $\langle 2 \rangle = \{0, 2, 4, 6\}$ en \mathbb{Z}_8 . La clase lateral $1 + \langle 2 \rangle$ se obtiene sumando 1 a cada uno de los elementos de $\langle 2 \rangle = \{0, 2, 4, 6\}$, es decir,

$$1 + \langle 2 \rangle = \{1, 3, 5, 7\}.$$

Por el Lema de Igualdad de Clases Laterales, podemos tomar a cualquier elemento de la clase lateral como su representante:

$$1 + \langle 2 \rangle = 3 + \langle 2 \rangle = 5 + \langle 2 \rangle = 7 + \langle 2 \rangle.$$

Definición 1.58 (partición uniforme). Una *partición uniforme* de un conjunto A es una partición $\mathcal{P} = \{P_i \subseteq A : i \in I\}$ de A tal que $|P_i| = |P_j|$ para toda $P_i, P_j \in \mathcal{P}$.

Lema 1.59 (partición en clases laterales). El conjunto de clases laterales G/H es una partición uniforme de G .

Demostración. Las clases laterales forman una partición de G porque son clases de equivalencia de una relación de equivalencia sobre G . Para demostrar que la partición es uniforme, debemos demostrar que $|aH| = |bH|$, para toda $a, b \in G$. Consideremos la función $\beta : aH \rightarrow bH$ definida por $\beta(ah) = bh$, para toda $h \in H$. Esta función está bien definida y es inyectiva porque, para toda $h_1, h_2 \in H$,

$$ah_1 = ah_2 \Leftrightarrow h_1 = h_2 \Leftrightarrow bh_1 = bh_2 \Leftrightarrow \beta(ah_1) = \beta(ah_2).$$

Además, claramente β es sobreyectiva porque la preimagen de cualquier $bh \in bH$ es $ah \in aH$. \square

Corolario 1.60. Sea H un subgrupo de G . Para toda $a \in H$, $|aH| = |H|$.

Ejemplo 1.61. Las clases laterales de $\langle 2 \rangle$ en \mathbb{Z}_6 son:

$$\begin{aligned} 0 + \langle 2 \rangle &= \{0, 2, 4\} = 2 + \langle 2 \rangle = 4 + \langle 2 \rangle, \\ 1 + \langle 2 \rangle &= \{1, 3, 5\} = 3 + \langle 2 \rangle = 5 + \langle 2 \rangle. \end{aligned}$$

Las clases laterales de $\langle 3 \rangle$ en \mathbb{Z}_6 son:

$$\begin{aligned} 0 + \langle 3 \rangle &= \{0, 3\} = 3 + \langle 3 \rangle, \\ 1 + \langle 3 \rangle &= \{1, 4\} = 4 + \langle 3 \rangle, \\ 2 + \langle 3 \rangle &= \{2, 5\} = 5 + \langle 3 \rangle. \end{aligned}$$

Ejemplo 1.62. Sea $n \in \mathbb{N}$. En general, para cualquier $k \in \mathbb{Z}$, una clase lateral $k + n\mathbb{Z}$ del subgrupo $n\mathbb{Z} = \langle n \rangle$ de \mathbb{Z} es igual a

$$k + n\mathbb{Z} = \{k, k \pm n, k \pm 2n, k \pm 3n, \dots\}.$$

Así vemos que hay n clases laterales en $\mathbb{Z}/n\mathbb{Z}$:

$$\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \dots, (n-1) + n\mathbb{Z}\}.$$

Lema 1.63 (clases laterales derechas). Sea H un subgrupo de un grupo G .

1. Para cualquier $a, b \in G$, se cumple que $Ha = Hb$ si y solo si $ab^{-1} \in H$.
2. El conjunto de clases laterales derechas $H \setminus G := \{Ha : a \in G\}$ es una partición uniforme de G .

Demostración. Ejercicio 1.32. \square

Lema 1.64 (índice). Sea H un subgrupo de un grupo G . El número de distintas clases laterales izquierdas de H en G es igual al número de distintas clases laterales derechas de H en G .

Demostración. Demostraremos que $|G/H| = |H \setminus G|$. Consideremos la función

$$\beta : (G/H) \rightarrow (H \setminus G) \text{ definida por } \beta(aH) = Ha^{-1}, \forall a \in G.$$

Esta función está bien definida y es inyectiva porque

$$aH = bH \Leftrightarrow a^{-1}b \in H \Leftrightarrow a^{-1}(b^{-1})^{-1} \in H \Leftrightarrow Ha^{-1} = Hb^{-1},$$

donde la última equivalencia se obtiene usando el Lema 1.63. Además, claramente β es sobreyectiva porque la preimagen de cualquier $Ha \in H \setminus G$ es $a^{-1}H \in G/H$. \square

Definición 1.65 (índice). Sea H un subgrupo de un grupo G . El *índice de H en G* es el número de distintas clases laterales (izquierdas o derechas) de H en G , y se denota como $[G : H]$.

Observación 1.66. Claramente $[G : H] = |G/H|$, ya que G/H es el conjunto de clases laterales izquierdas de H en G .

Teorema 1.67 (Lagrange). Sea H un subgrupo de un grupo finito G . Entonces,

$$|G| = [G : H] \cdot |H|.$$

Demostración. Sea $G/H = \{a_1H, a_2H, \dots, a_rH\}$, donde $r := [G : H]$. Como G es igual a la unión disjunta de las clases laterales tenemos que

$$|G| = \left| \bigcup_{i=1}^r a_iH \right| = \sum_{i=1}^r |a_iH|.$$

Por el Corolario 1.60, $|a_iH| = |H|$ para toda i . Por lo tanto,

$$|G| = \sum_{i=1}^r |H| = r|H| = [G : H]|H|.$$

\square

Corolario 1.68. Sea H un subgrupo de un grupo finito G . Entonces, el orden de H divide al orden de G .

Ejemplo 1.69. Los subgrupos $\langle 2 \rangle$ y $\langle 3 \rangle$ de \mathbb{Z}_6 tienen 3 y 2 elementos, respectivamente. Esto claramente concuerda con que $2 \mid 6$ y $3 \mid 6$.

Ejemplo 1.70. Cualquier grupo G de orden 12 puede tener subgrupos de órdenes 1, 2, 3, 4, 6 y 12. Sin embargo, G no puede tener subgrupos de órdenes 5, 7, 8, 9, 10 y 11, porque no son divisores de 12.

Observación 1.71. El converso del corolario anterior no es necesariamente cierto; es decir, si k es un divisor de $|G|$, no necesariamente existe un subgrupo $H \leq G$ tal que $|H| = k$. Veremos ejemplos de esto en el Capítulo 3.

Corolario 1.72. Sea H un subgrupo de un grupo finito G . Entonces,

$$|G/H| = \frac{|G|}{|H|}.$$

Corolario 1.73. Sea G un grupo finito de orden n .

1. $|g|$ divide a $|G|$, para toda $g \in G$.
2. $g^n = e$, para toda $g \in G$.

Demostración.

1. Por el Teorema 1.40, $|g| = |\langle g \rangle|$. Por lo tanto, por el Corolario 1.68, $|g|$ divide a $|G|$.
2. Por el punto anterior, sabemos que $|g|$ divide a n , es decir, $n = qd$, donde $d = |g|$ y $q \in \mathbb{Z}$. Luego, $g^n = g^{qd} = (g^d)^q = e^q = e$.

□

Corolario 1.74. Sea G un grupo de orden primo p . Entonces, G es cíclico.

Demostración. Ejercicio 1.37

□

Palabras clave: *subgrupo, tests de subgrupos, grupo cíclico, centro, clase lateral, índice de un subgrupo, teorema de Lagrange.*

1.2.3. Ejercicios

Ejercicio 1.21 (subgrupos). Sea G un grupo. Demuestra que los siguientes conjuntos son subgrupos de G .

1. El centralizador de $a \in G$ definido como $C(a) := \{g \in G : ga = ag\}$.
2. El centralizador de $H \leq G$ definido como $C(H) := \{g \in G : gh = hg, \forall h \in H\}$.
3. Cuando G es abeliano, el conjunto $T := \{g \in G : g^3 = e\}$.
4. Cuando G es abeliano, el conjunto $K := \{g \in G : |g| < \infty\}$.

Ejercicio 1.22 (intersección de subgrupos). Sean H y K subgrupos de un grupo G . Demuestra que $H \cap K$ es un subgrupo de G .

Ejercicio 1.23 (unión de subgrupos). Sean H y K subgrupos de un grupo G . Demuestra que $H \cup K$ es un subgrupo de G si y solo si $H \subseteq K$ o $K \subseteq H$.

Ejercicio 1.24 (producto de subgrupos). Sean H y K subgrupos de un grupo abeliano G . Demuestra que HK es un subgrupo de G .

Ejercicio 1.25 (subgrupo generado). Dado un subconjunto S de un grupo G , definimos al *subgrupo generado* por S como

$$\langle S \rangle := \{s_1 s_2 \dots s_k : s_i \in S \cup S^{-1}, k \geq 1\} \cup \{e\};$$

donde $S^{-1} := \{s^{-1} : s \in S\}$. Demuestra que $\langle S \rangle$ es un subgrupo de G .

Ejercicio 1.26 (subgrupo generado). Sea S un subconjunto de un grupo G . Demuestra que $\langle S \rangle$ es el subgrupo de G más pequeño que contiene a S ; es decir, si H es un subgrupo de G tal que $S \subseteq H$, entonces $\langle S \rangle \subseteq H$.

Ejercicio 1.27. Sea H un subgrupo de G y $g \in G$ un elemento de orden n . Demuestra que si $g^k \in H$, donde $\text{mcd}(n, k) = 1$, entonces $g \in H$.

Ejercicio 1.28. Sea H un subgrupo de un grupo G . Sin usar la relación mód (H) , demuestra que si $aH \neq bH$, entonces $(aH) \cap (bH) = \emptyset$.

Ejercicio 1.29. Sea H un subgrupo de un grupo G y $a \in G$. Demuestra que aH es un subgrupo de G si y solo si $a \in H$.

Ejercicio 1.30 (índice uno). Sea H un subgrupo de un grupo G . Demuestra que $[G : H] = 1$ si y solo si $G = H$.

Ejercicio 1.31 (producto de índices). Sean $H \leq K \leq G$. Demuestra que $[G : H] = [G : K][K : H]$.

Ejercicio 1.32 (clases laterales derechas). Demuestra el Lema 1.63.

Ejercicio 1.33. Encuentra todas las clases laterales de H en G en cada uno de los siguientes casos:

- a) $H = \langle 4 \rangle$ y $G = \mathbb{Z}$.
- b) $H = \langle 4 \rangle$ y $G = 2\mathbb{Z}$.
- c) $H = \langle 2 \rangle$ y $G = \mathbb{Z}_{12}$.
- d) $H = \langle 0, 3, 6, 9 \rangle$ y \mathbb{Z}_{12} .
- e) $H = \{1, 11\}$ y $G = U(30)$

Ejercicio 1.34. Supongamos que K es un subgrupo propio de H y H es un subgrupo propio de G . Si $|K| = 42$ y $|G| = 420$, ¿cuáles son los posibles valores para $|H|$?

Ejercicio 1.35. Supongamos que K es un subgrupo propio de H y H es un subgrupo propio de G . Si $|K| = 30$ y $|G| = 120$, ¿cuáles son los posibles valores para $|H|$?

Ejercicio 1.36. Sea G un grupo de orden p^2 , donde p es un número primo.

1. Enlista los posibles órdenes de los elementos de G .
2. Demuestra que G debe tener al menos un elemento de orden p .

Ejercicio 1.37 (grupo de orden primo). Sea G un grupo de orden primo p . Demuestra que G debe ser cíclico.

Ejercicio 1.38 (producto de subconjuntos). Sean A y B subconjuntos de un grupo G . Definimos el producto de A y B por $AB := \{ab : a \in A, b \in B\}$. Demuestra que si $e \in B$, entonces $A \subseteq AB$. Además, demuestra que, para cualquier subconjunto C de G ,

$$A(BC) = (AB)C.$$

Ejercicio 1.39 (producto de subgrupos). Sean H y K subgrupos de un grupo G . Demuestra que el producto $HK := \{hk : h \in H, k \in K\}$ es un subgrupo de G si y solo si $HK = KH$.

Ejercicio 1.40 (producto de subgrupos). Sean H y K subgrupos de un grupo G . Demuestra que si HK es un subgrupo de G , entonces $HK = \langle H \cup K \rangle$.

Ejercicio 1.41 (ley modular). Sean H y K subgrupos de un grupo G , y sea S un subgrupo de H . Entonces,

$$S(H \cap K) = H \cap (SK).$$

Ejercicio 1.42 (fórmula del producto). Sean H y K subgrupos de un grupo finito G . Consideremos los siguientes conjuntos de clases laterales $\mathcal{A} := \{aK : a \in HK\}$ y $\mathcal{B} = \{h(H \cap K) : h \in H\}$. Demuestra que la función

$$\beta : \mathcal{A} \rightarrow \mathcal{B} \text{ definida como } \beta(hkK) = h(H \cap K), \forall hk \in HK$$

es una biyección bien definida. Concluye usando el Teorema de Lagrange que

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Ejercicio 1.43 (★). Sea G un grupo con una cantidad finita de subgrupos. Demuestra que G es finito.

1.3. Subgrupos normales y cocientes

1.3.1. Subgrupos normales

Definición 1.75 (subgrupo normal). Sea H un subgrupo de un grupo G . Decimos que H es *normal* en G , y escribimos $H \trianglelefteq G$, si

$$aH = Ha, \forall a \in G.$$

Observación 1.76. Es fácil verificar que en cualquier grupo G , tanto el subgrupo trivial $\{e\}$ como G mismo son subgrupos normales de G ; es decir, siempre se cumple que $\{e\} \trianglelefteq G$ y $G \trianglelefteq G$.

Observación 1.77. Claramente, si G es un grupo abeliano, entonces todos sus subgrupos son normales.

Lema 1.78 (subgrupo normal). Sea H un subgrupo de un grupo G . Las siguientes afirmaciones son equivalentes:

1. H es normal en G .
2. $H = aHa^{-1}$, para toda $a \in G$.
3. $aha^{-1} \in H$, para toda $a \in G$, $h \in H$.
4. Para toda $a \in G$, $h \in H$, existen $h', h'' \in H$ tales que $ah = h'a$ y $ha = ah''$.

Demostración.

- (1.) \Rightarrow (2.) Supongamos que $H \trianglelefteq G$. Por definición, $aH = Ha$, para toda $a \in G$. Multiplicando por a^{-1} , obtenemos que $aHa^{-1} = H$, para toda $a \in G$, lo que demuestra (2).
- (2.) \Rightarrow (3.) Supongamos que $H = aHa^{-1}$, para toda $a \in G$. Entonces, $aha^{-1} \in aHa^{-1} = H$, para toda $a \in G$, $h \in H$, lo que demuestra (3).
- (3.) \Rightarrow (4.) Supongamos que $aha^{-1} \in H$, para toda $a \in G$, $h \in H$. Luego, existe $h' \in H$ tal que $aha^{-1} = h'$, lo que prueba que $ah = h'a$. La hipótesis también implica que $a^{-1}ha \in H$ para toda $a \in G$, $h \in H$. Luego, existe $h'' \in H$ tal que $a^{-1}ha = h''$. Esto demuestra que $ha = ah''$.
- (4.) \Rightarrow (1.) Supongamos que se cumple (4). Para demostrar que H es normal en G , debemos probar que $aH = Ha$, para toda $a \in G$. Sea $ah \in aH$. Por hipótesis, existe $h' \in H$ tal que $ah = h'a \in Ha$. Por lo tanto, $aH \subseteq Ha$. Sea ahora $ha \in Ha$. Por hipótesis, existe $h'' \in H$ tal que $ha = ah'' \in aH$. Por lo tanto $Ha \subseteq aH$. Esto demuestra que $aH = Ha$, para toda $a \in G$.

□

Definición 1.79 (conjugado). Sea G un grupo y $a, h \in G$. El *conjugado* de h por a es el elemento $aha^{-1} \in G$.

Observación 1.80. El inverso del conjugado aha^{-1} es $ah^{-1}a^{-1}$ porque

$$(aha^{-1})(ah^{-1}a^{-1}) = ahh^{-1}a^{-1} = aa^{-1} = e.$$

La k -ésima potencia del conjugado aha^{-1} es igual a ah^ka^{-1} porque

$$(aha^{-1})^k = \underbrace{(aha^{-1})(aha^{-1}) \dots (aha^{-1})}_{k \text{ veces}} = \underbrace{ahh \dots ha^{-1}}_{k \text{ veces}} = ah^ka^{-1}.$$

Observación 1.81. Usando la Definición 1.79 anterior, el punto (3.) del Lema 1.78 establece que H es normal en G si y solo si el conjugado de cualquier elemento de H por cualquier elemento de G está en H .

Ejemplo 1.82. Sea G un grupo. Usaremos el punto (3.) del Lema 1.78 para demostrar que el centro $Z(G) = \{g \in G : ga = ag, \forall a \in G\}$ es normal en G . Sean $a \in G$ y $z \in Z(G)$. Entonces, $aza^{-1} = aa^{-1}z = z \in Z(G)$. Por lo tanto, $Z(G) \trianglelefteq G$.

Lema 1.83. Sean G un grupo y $H \leq G$. Si $[G : H] = 2$ entonces $H \trianglelefteq G$.

Demostración. Necesitamos mostrar que $Ha = aH$ para toda $a \in G$. Para $a \in H$ esto es obvio, porque $aH = H = Ha$. Tomemos $a \in G - H$. Entonces $aH \neq H$. Sabemos que $aH \cap H = \emptyset$ y $G = H \cup aH$, como solo hay dos clases laterales, se tiene que $aH = G - H$. Por la misma razón, $Ha = G - H$, de donde se sigue el resultado. \square

Ejemplo 1.84. El subgrupo de rotaciones $\langle \rho \rangle = \{\text{id}, \rho, \rho^2, \dots, \rho^{n-1}\}$ del grupo diédrico D_{2n} es normal ya que es de índice 2.

Observación 1.85 (test del subgrupo normal). Combinamos el Test del Subgrupo 2 con el Lema 1.78 para deducir el siguiente test de normalidad: un subconjunto H es un subgrupo normal de G si y solo si se cumple lo siguiente:

(N1) $e \in H$.

(N2) $h_1^{-1}h_2 \in H$, para toda $h_1, h_2 \in H$.

(N3) $aha^{-1} \in H$, para toda $a \in G, h \in H$.

Ejemplo 1.86. Si $H \leq K$ y $K \leq G$, siempre se cumple que $H \leq G$. Esto es porque la propiedad de ser subgrupo es una propiedad intrínseca de H , la cual no depende del grupo en el que esté contenido. Por otro lado, no es verdad que si $H \trianglelefteq K$ y $K \trianglelefteq G$, entonces $H \trianglelefteq G$. Para ver un ejemplo de esto consideremos al grupo diédrico $G = D_8$ con la notación del Ejemplo 1.12. Usando el test del subgrupo normal, podemos verificar que $H = \{\text{id}, h\}$ es un subgrupo normal de $K = \{\text{id}, \rho^2, h, \rho^2h\}$ y que K es un subgrupo normal de $G = D_8$. Sin embargo, H no es subgrupo normal de G , ya que, por ejemplo, $\rho h \rho^{-1} = \rho^2h \notin H$.

Este ejemplo nos demuestra que la relación de ser subgrupo normal no es transitiva.

Definición 1.87 (conmutador). Sea G un grupo y $a, b \in G$. El *conmutador* de a y b , denotado por $[a, b]$, es

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

El *subgrupo conmutador* de G , denotado por G' es

$$G' := \langle [a, b] : a, b \in G \rangle;$$

es decir, el subgrupo generado por los conmutadores (para la definición de *subgrupo generado* ver el Ejercicio 1.25). En otras palabras, G' es el subgrupo de G que consiste en todos los productos de conmutadores en G y sus inversos.

Observación 1.88. Dos elementos $a, b \in G$ conmutan si y solo si $[a, b] = e$. Además, $[a, b]^{-1} = [b, a]$ porque

$$[a, b][b, a] = (aba^{-1}b^{-1})(bab^{-1}a^{-1}) = aba^{-1}ab^{-1}a^{-1} = abb^{-1}a^{-1} = aa^{-1} = e.$$

Esto muestra que el inverso de un conmutador es un conmutador.

Observación 1.89. El producto de dos conmutadores no necesariamente es un conmutador; sin embargo, G' es un subgrupo de G por definición, ya que está constituido por todos los posibles productos de los conmutadores.

Observación 1.90. Sean $a, b, g \in G$. El conjugado del conmutador $[a, b]$ por g es un conmutador porque

$$\begin{aligned} g[a, b]g^{-1} &= g(aba^{-1}b^{-1})g^{-1} \\ &= ga(g^{-1}g)b(g^{-1}g)a^{-1}(g^{-1}g)b^{-1}g^{-1} \\ &= [(gag^{-1}), (gbg^{-1})]. \end{aligned}$$

Proposición 1.91. Sea G un grupo. El subgrupo conmutador G' es normal en G .

Demostración. Usaremos el Lema 1.78 (3). Sean $h \in G'$ y $g \in G$ arbitrarios: debemos probar que $ghg^{-1} \in G'$. Por definición del subgrupo conmutador, sabemos que h es producto de conmutadores, es decir, $h = [a_1, b_1][a_2, b_2] \dots [a_k, b_k]$ para algunos $a_i, b_i \in G$, $i = 1, 2, \dots, k$, y $k \in \mathbb{N}$. Usando la observación anterior sobre conjugados obtenemos lo siguiente:

$$\begin{aligned} ghg^{-1} &= g[a_1, b_1][a_2, b_2] \dots [a_k, b_k]g^{-1} \\ &= g[a_1, b_1]g^{-1}g[a_2, b_2]g^{-1}g \dots g^{-1}g[a_k, b_k]g^{-1} \\ &= [ga_1g^{-1}, gb_1g^{-1}][ga_2g^{-1}, gb_2g^{-1}] \dots [ga_kg^{-1}, gb_kg^{-1}] \in G'. \end{aligned}$$

□

1.3.2. Grupos cocientes

Parte de la importancia de los subgrupos normales es que nos permiten definir una operación natural entre sus clases laterales.

Lema 1.92. Sea H un subgrupo de un grupo G . La operación \cdot en el conjunto de clases laterales G/H dada por $aH \cdot bH := abH$, $a, b \in G$, está bien definida si y solo si H es subgrupo normal de G .

Demostración.

(\Rightarrow) Supongamos que la operación $aH \cdot bH := abH$, $a, b \in G$, está bien definida. Como $eH = hH$ para toda $h \in H$, tenemos que

$$(eH)(bH) = (hH)(bH) \text{ para toda } b \in G.$$

Usando la definición de la multiplicación de clases laterales obtenemos que

$$bH = hbH \implies b^{-1}hb \in H, \text{ para toda } b \in G.$$

Esto demuestra que H es normal en G .

(\Leftarrow) Supongamos que H es normal en G . Supongamos además que $a_1H = a_2H$ y que $b_1H = b_2H$. Debemos demostrar que $(a_1H)(b_1H) = (a_2H)(b_2H)$. Usamos el Lema 1.53:

$$\begin{aligned} a_1H = a_2H &\implies a_1 \in a_2H \implies a_1 = a_2h_1 \text{ para algún } h_1 \in H \\ b_1H = b_2H &\implies b_1 \in b_2H \implies b_1 = b_2h_2 \text{ para algún } h_2 \in H. \end{aligned}$$

Luego,

$$a_1b_1 = (a_2h_1)(b_2h_2) = (a_2b_2)(h_1'h_2), \text{ para algún } h_1' \in H,$$

donde usamos el hecho que $H \trianglelefteq G$ y el Lema 1.78 (4.) para conmutar b . Lo anterior implica que $a_1b_1 \in a_2b_2H$ y

$$a_1b_1H = a_2b_2H \implies (a_1H)(b_1H) = (a_2H)(b_2H).$$

□

Teorema 1.93 (grupo cociente). Sea H un subgrupo de un grupo G . El conjunto de las clases laterales G/H equipado con la operación $aH \cdot bH := abH$, $a, b \in G$, es un grupo si y solo si H es un subgrupo normal de G .

Demostración.

(\Rightarrow) Si G/H es un grupo, en particular la operación entre clases laterales está bien definida. Por el Lema 1.92, esto implica que H es normal en G .

(\Leftarrow) Supongamos que H es normal en G . Demostraremos que G/H es un grupo:

(G0) La operación es claramente cerrada, y, por el Lema 1.92, está bien definida.

(G1) Para cualquier $aH, bH, cH \in G/H$ se cumple que

$$aH \cdot (bH \cdot cH) = a(bc)H = (ab)cH = (aH \cdot bH) \cdot cH.$$

(G2) La identidad es $eH \in G/H$ porque, para cualquier $aH \in G/H$,

$$eH \cdot aH = eaH = aH = aeH = aH \cdot eH.$$

(G3) El inverso de $aH \in G/H$ es $a^{-1}H \in G/H$ porque

$$aH \cdot a^{-1}H = aa^{-1}H = eH = a^{-1}aH = a^{-1}H \cdot aH.$$

□

Ejemplo 1.94. Consideremos el subgrupo $\langle 3 \rangle = \{0, 3\}$ de \mathbb{Z}_6 , el cual es normal porque \mathbb{Z}_6 es abeliano. El grupo cociente es

$$\mathbb{Z}_6/\langle 3 \rangle = \{0 + \langle 3 \rangle, 1 + \langle 3 \rangle, 2 + \langle 3 \rangle\},$$

y su tabla de Cayley está dada por el Cuadro 1.4.

+	0 + $\langle 3 \rangle$	1 + $\langle 3 \rangle$	2 + $\langle 3 \rangle$
0 + $\langle 3 \rangle$	0 + $\langle 3 \rangle$	1 + $\langle 3 \rangle$	2 + $\langle 3 \rangle$
1 + $\langle 3 \rangle$	1 + $\langle 3 \rangle$	2 + $\langle 3 \rangle$	0 + $\langle 3 \rangle$
2 + $\langle 3 \rangle$	2 + $\langle 3 \rangle$	0 + $\langle 3 \rangle$	1 + $\langle 3 \rangle$

Cuadro 1.4: Tabla de Cayley de $\mathbb{Z}_6/\langle 3 \rangle$

Ejemplo 1.95. Consideremos el subgrupo $5\mathbb{Z} = \{5k : k \in \mathbb{Z}\}$ de \mathbb{Z} . Entonces,

$$\mathbb{Z}/5\mathbb{Z} = \{0 + 5\mathbb{Z}, 1 + 5\mathbb{Z}, 2 + 5\mathbb{Z}, 3 + 5\mathbb{Z}, 4 + 5\mathbb{Z}\}.$$

Algunos ejemplos de sumas en el grupo $\mathbb{Z}/5\mathbb{Z}$ son:

$$\begin{aligned} (1 + 5\mathbb{Z}) + (1 + 5\mathbb{Z}) &= 2 + 5\mathbb{Z}, \\ (2 + 5\mathbb{Z}) + (3 + 5\mathbb{Z}) &= 5 + 5\mathbb{Z} = 0 + 5\mathbb{Z}, \\ (4 + 5\mathbb{Z}) + (3 + 5\mathbb{Z}) &= 7 + 5\mathbb{Z} = 2 + 5\mathbb{Z}. \end{aligned}$$

Ejemplo 1.96. Sea G un grupo y H un subgrupo de G de índice 2. Por el Lema 1.83 sabemos que H es normal en G y por el Teorema de Lagrange $|G/H| = 2$. Esto implica que el grupo G/H tiene exactamente dos clases laterales eH y gH , las cuales cumplen que $(gH) \cdot (gH) = eH$.

Las siguientes son un par de aplicaciones del uso de grupos cociente.

Proposición 1.97. Sea G un grupo. Si G no es abeliano, entonces el grupo cociente $G/Z(G)$ no es cíclico.

Demostración. Sea $Z := Z(G)$. Demostraremos la proposición contrapuesta: si G/Z es cíclico, entonces G es abeliano. Sea gZ el generador de G/Z .

Sean $a, b \in G$ elementos arbitrarios. Entonces, existen $i, j \in \mathbb{Z}$ tales que

$$\begin{aligned} aZ &= (gZ)^i = g^i Z, \\ bZ &= (gZ)^j = g^j Z. \end{aligned}$$

Luego, existen $z_1, z_2 \in Z$ tales que $a = g^i z_1$ y $b = g^j z_2$. Como z_1 y z_2 conmutan con todos los elementos de G y $g^i g^j = g^{i+j} = g^{j+i} = g^j g^i$, deducimos que

$$ab = (g^i z_1)(g^j z_2) = g^i g^j z_1 z_2 = g^j g^i z_2 z_1 = g^j z_2 g^i z_1 = ba.$$

Esto demuestra que G es abeliano. \square

Proposición 1.98. Sea G un grupo y $N \leq G$. Entonces, $N \trianglelefteq G$ y G/N es abeliano si y solo si $G' \leq N$.

Demostración.

(\Rightarrow) Supongamos que N es normal en G y G/N es abeliano. Esto implica que las clases laterales de conmutadores son triviales en G/N ; es decir, para todo $a, b \in G$,

$$[a, b]N = aba^{-1}b^{-1}N = (aN)(bN)(a^{-1}N)(b^{-1}N) = eN.$$

Por lo tanto, $[a, b] \in N$, para toda $a, b \in G$, lo que demuestra que $G' \leq N$.

(\Leftarrow) Supongamos que $G' \leq N$. Para toda $n \in N$, $a \in G$, tenemos

$$ana^{-1} = ana^{-1}n^{-1}n = [a, n]n \in N.$$

Luego, N es normal en G . Ahora, veamos que, para todo $a, b \in G$,

$$[a, b] \in N \Rightarrow [a, b]N = eN \Rightarrow aba^{-1}b^{-1}N = eN.$$

Por definición de la operación entre clases laterales, obtenemos que

$$aba^{-1}b^{-1}N = (aN)(bN)(aN)^{-1}(bN)^{-1} = eN.$$

Multiplicando por la derecha la igualdad de ambos lados por $(bN)(aN)$ obtenemos que $(aN)(bN) = (bN)(aN)$, para todo $a, b \in G$. Esto demuestra que G/N es abeliano. \square

Palabras clave: subgrupo normal, conjugado, conmutador, subgrupo conmutador, grupo cociente.

1.3.3. Ejercicios

Ejercicio 1.44 (subgrupo especial lineal). Sea $GL_n(F)$ el grupo general lineal de grado n sobre F . Demuestra que el grupo especial lineal, definido por

$$SL_n(F) := \{A \in GL_n(F) : \det(A) = 1\},$$

es un subgrupo normal de $GL_n(F)$.

Ejercicio 1.45. ¿Cuál es el orden de $14 + \langle 8 \rangle$ en el grupo cociente $\mathbb{Z}_{24}/\langle 8 \rangle$?

Ejercicio 1.46 (orden del conjugado). Sea G un grupo y $a, g \in G$. Demuestra que $|g| = |aga^{-1}|$.

Ejercicio 1.47 (conjugación de elementos). Sea G un grupo. Demuestra que la conjugación de elementos de G define una relación de equivalencia sobre G .

Ejercicio 1.48 (conjugación de subgrupos). Sea $H \leq G$ y $a \in G$. Definimos al conjugado de H como $aHa^{-1} := \{aha^{-1} : h \in H\}$. Demuestra que aHa^{-1} es un subgrupo de G y que $|H| = |aHa^{-1}|$.

Ejercicio 1.49 (centralizador de un subgrupo). Sea H un subgrupo normal de G . Demuestra que el centralizador de H , definido por $C(H) := \{g \in G : gh = hg, \forall h \in H\}$ es un subgrupo normal de G .

Ejercicio 1.50 (normalizador de un subgrupo). Sea H un subgrupo de G . Definimos al normalizador de H como $N(H) := \{g \in G : H = gHg^{-1}\}$. Demuestra que $H \trianglelefteq N(H)$ y que $C(H) \trianglelefteq N(H)$.

Ejercicio 1.51 (normalizador de un subgrupo). Sea H un subgrupo de G . Demuestra que H es normal en G si y solo si $N(H) = G$.

Ejercicio 1.52. Sea G un grupo. Consideremos al *subgrupo diagonal* de $G \oplus G$ definido por $\text{diag}(G) := \{(g, g) : g \in G\}$. Demuestra que $\text{diag}(G)$ es normal en $G \oplus G$ si y solo si G es abeliano. Cuando G es finito, ¿Cuál es el índice de $\text{diag}(G)$ en $G \oplus G$?

Ejercicio 1.53 (producto de subgrupos). Sea G un grupo y $H, K \leq G$.

1. Si $H \trianglelefteq G$, demuestra que $HK = KH$.
2. Si $H \trianglelefteq G$, demuestra que $HK \leq G$.
3. Si $H \trianglelefteq G$ y $K \trianglelefteq G$, demuestra que $HK \trianglelefteq G$.
4. Si $H \trianglelefteq G$, $K \trianglelefteq G$ y $H \cap K = \{e\}$, demuestra que $hk = kh$, para toda $h \in H, k \in K$.

Ejercicio 1.54 (cociente cíclico). Sea $G = \langle g \rangle$ un grupo cíclico y H un subgrupo normal de G . Demuestra que G/H es cíclico.

Ejercicio 1.55 (subgrupo de índice 2). Sea H un subgrupo de G de índice 2.

1. Demuestra que $a^2 \in H$ para toda $a \in G$.
2. Sea $K \leq G$. Demuestra que $K \leq H$ o que exactamente la mitad de los elementos de K están en H (i.e. $|K \cap H| = \frac{|K|}{2}$).

Ejercicio 1.56. Sea H un subgrupo normal de un grupo G . Demuestra que si $|G/H| = n$, entonces $g^n \in H$ para toda $g \in G$.

Ejercicio 1.57. Consideremos a \mathbb{Q} como grupo con la suma usual. Demuestra que \mathbb{Q}/\mathbb{Z} es un grupo infinito en el cual todos sus elementos tienen orden finito.

Ejercicio 1.58. Sea G un grupo finito y sea $N \trianglelefteq G$ tal que $[G : N] = k$. Demuestra que si $g \in G$ cumple que $\text{mcd}(|g|, k) = 1$, entonces $g \in N$.

Ejercicio 1.59. Sea H un subgrupo normal de un grupo G . Si $g \in G$ es un elemento de orden finito, demuestra que el orden de gH como elemento de G/H divide a $|g|$.

1.4. Homomorfismos

1.4.1. Homomorfismos

Definición 1.99 (homomorfismo). Sean G_1 y G_2 grupos. Un *homomorfismo* es una función $\phi : G_1 \rightarrow G_2$ tal que

$$\phi(gh) = \phi(g)\phi(h), \quad \forall g, h \in G_1.$$

Informalmente, decimos que un homomorfismo *preserva las operaciones* entre los grupos.

Observación 1.100. Es importante observar que en la igualdad $\phi(gh) = \phi(g)\phi(h)$ la operación del lado izquierdo entre g y h es la correspondiente a G_1 , mientras que la operación del lado derecho entre $\phi(g)$ y $\phi(h)$ es la correspondiente a G_2 .

Ejemplo 1.101. 1. La función $\phi : \mathbb{Z} \rightarrow \mathbb{Z}$ definida por $\phi(x) = 2x, \forall x \in \mathbb{Z}$, es un homomorfismo porque

$$\phi(x + y) = 2(x + y) = 2x + 2y = \phi(x) + \phi(y), \quad \text{para toda } x, y \in \mathbb{Z}.$$

2. Considerando a \mathbb{R}^* como grupo bajo la multiplicación usual, la función $\phi : \mathbb{R}^* \rightarrow \mathbb{R}^*$ definida por $\phi(x) = 2x, \forall x \in \mathbb{R}^*$, **no** es un homomorfismo porque

$$\phi(xy) = 2xy \neq \phi(x)\phi(y) = 4xy, \quad \text{para toda } x, y \in \mathbb{R}^*.$$

3. La función $\phi : \text{GL}_n(\mathbb{R}) \rightarrow \mathbb{R}^*$ definida por $\phi(A) = \det(A), \forall A \in \text{GL}_n(\mathbb{R})$, es un homomorfismo porque

$$\phi(AB) = \det(AB) = \det(A)\det(B) = \phi(A)\phi(B), \quad \text{para toda } A, B \in \text{GL}_n(\mathbb{R})$$

4. Sea G un grupo y $N \trianglelefteq G$. La función $\phi : G \rightarrow G/N$ definida por $\phi(g) = gN, \forall g \in G$, es un homomorfismo porque

$$\phi(gh) = ghN = (gN)(hN) = \phi(g)\phi(h), \quad \text{para toda } g, h \in G.$$

Este homomorfismo se llama el *homomorfismo natural de G a G/N* .

Lema 1.102 (propiedades de homomorfismos). Sea $\phi : G_1 \rightarrow G_2$ un homomorfismo. Entonces:

1. $\phi(e_1) = e_2$, donde e_i es la identidad de $G_i, i = 1, 2$.
2. $\phi(g^{-1}) = \phi(g)^{-1}$, para toda $g \in G_1$
3. $\phi(g^k) = \phi(g)^k$, para toda $k \in \mathbb{Z}, g \in G_1$.
4. Si $g \in G_1$ es un elemento de orden finito, entonces $|\phi(g)| \mid |g|$.

Demostación.

1. Como $e_1e_1 = e_1$, debe cumplirse que $\phi(e_1e_1) = \phi(e_1)$. Aplicando la propiedad de homomorfismo del lado izquierdo, obtenemos que $\phi(e_1)\phi(e_1) = \phi(e_1)$. Finalmente, por cancelación, $\phi(e_1) = e_2$.
2. Observemos que $\phi(e_1) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1})$. Por el punto anterior, $e_2 = \phi(g)\phi(g^{-1})$, lo que implica que $\phi(g)^{-1} = \phi(g^{-1})$.
3. Ejercicio 1.61.
4. Sea $|g| = n$. Por el punto anterior, $\phi(g)^n = \phi(g^n) = \phi(e_1) = e_2$. Por el Lema 1.25, concluimos que $|\phi(g)|$ divide a n .

□

Sea $\phi : G_1 \rightarrow G_2$ un homomorfismo. Recordemos que para cualquier subconjunto $H \subseteq G_1$, la *imagen de H bajo ϕ* es

$$\phi(H) := \{\phi(h) : h \in H\}.$$

En particular, la *imagen de ϕ* es $\text{Im}(\phi) := \phi(G_1)$, y sabemos que ϕ es sobreyectivo si y solo si $\phi(G_1) = G_2$.

Por otro lado, dado $K \subseteq G_2$, la *preimagen de K bajo ϕ* es el conjunto

$$\phi^{-1}(K) := \{g \in G_1 : \phi(g) \in K\}.$$

Esta notación no debe confundir al lector: el símbolo $\phi^{-1}(K)$ no implica que la función ϕ deba ser invertible; podemos perfectamente definir preimágenes de conjuntos bajo funciones no invertibles. Sin embargo, cuando ϕ sí es invertible, resulta que $\phi^{-1}(K)$ coincide con la imagen de K bajo la función ϕ^{-1} .

Lema 1.103 (propiedades de subgrupos bajo homomorfismos). Sea $\phi : G_1 \rightarrow G_2$ un homomorfismo. Entonces:

1. Si $H \leq G_1$, entonces $\phi(H) \leq G_2$.
2. Si $H \leq G_1$ es cíclico, o abeliano, entonces $\phi(H)$ es cíclico, o abeliano, respectivamente.
3. Si $H \trianglelefteq G_1$, entonces $\phi(H) \trianglelefteq \phi(G_1)$.
4. Si $K \leq G_2$, entonces $\phi^{-1}(K) \leq G_1$.
5. Si $K \trianglelefteq G_2$, entonces $\phi^{-1}(K) \trianglelefteq G_1$.

Demostación.

1. Observemos que $e_2 = \phi(e_1) \in \phi(H)$ porque $e_1 \in H$. Sean $\phi(h_1), \phi(h_2) \in \phi(H)$ elementos arbitrarios. Entonces,

$$\phi(h_1)^{-1}\phi(h_2) = \phi(h_1^{-1})\phi(h_2) = \phi(h_1^{-1}h_2) \in \phi(H).$$

Por el Test del Subgrupo 2, $\phi(H) \leq G_2$.

2. Ejercicio 1.62.

3. Sean $\phi(g) \in \phi(G_1)$ y $\phi(h) \in \phi(H)$. Entonces,

$$\phi(g)\phi(h)\phi(g)^{-1} = \phi(g)\phi(h)\phi(g^{-1}) = \phi(ghg^{-1}) \in \phi(H),$$

porque $ghg^{-1} \in H$. Por lo tanto, $\phi(H) \trianglelefteq \phi(G_1)$.

4. Primero, $e_1 \in \phi^{-1}(K)$ porque $\phi(e_1) = e_2 \in K$. Ahora, sean $a, b \in \phi^{-1}(K)$ elementos arbitrarios. Por definición de preimagen, tenemos que $\phi(a), \phi(b) \in K$. Luego,

$$\phi(a^{-1}b) = \phi(a)^{-1}\phi(b) \in K.$$

Esto muestra que $a^{-1}b \in \phi^{-1}(K)$, y entonces $\phi^{-1}(K) \leq G_1$.

5. Ejercicio 1.64.

□

Lema 1.104 (composición de homomorfismos). Sean $\phi_1 : G_1 \rightarrow G_2$ y $\phi_2 : G_2 \rightarrow G_3$ homomorfismos. La composición $\phi_2 \circ \phi_1 : G_1 \rightarrow G_3$ es un homomorfismo.

Demostración. Para toda $g, h \in G_1$, se cumple que

$$\phi_2 \circ \phi_1(gh) = \phi_2(\phi_1(gh)) = \phi_2(\phi_1(g)\phi_1(h)) = (\phi_2 \circ \phi_1)(g)(\phi_2 \circ \phi_1)(h).$$

Por lo tanto, $\phi_2 \circ \phi_1$ es un homomorfismo. □

Definición 1.105 (kernel). Sea $\phi : G_1 \rightarrow G_2$ un homomorfismo. El *kernel* de ϕ es el conjunto

$$\ker(\phi) := \{g \in G_1 : \phi(g) = e_2\}.$$

Ejemplo 1.106. 1. El kernel del homomorfismo $\phi : \mathbb{Z} \rightarrow \mathbb{Z}$ definido por $\phi(x) = 2x, \forall x \in \mathbb{Z}$, es

$$\ker(\phi) = \{x \in \mathbb{Z} : \phi(x) = 0\} = \{x \in \mathbb{Z} : 2x = 0\} = \{0\}.$$

2. El kernel del homomorfismo $\phi : \text{GL}_n(\mathbb{R}) \rightarrow \mathbb{R}^*$ definido por $\phi(A) = \det(A), \forall A \in \text{GL}_n(\mathbb{R})$, es

$$\ker(\phi) = \{A \in \text{GL}_n(\mathbb{R}) : \det(A) = 1\} = \text{SL}_n(\mathbb{R}).$$

3. Sea G un grupo y $N \trianglelefteq G$. El kernel del homomorfismo natural $\phi : G \rightarrow G/N$ es

$$\ker(\phi) = \{a \in G : \phi(a) = eN\} = \{a \in G : aN = eN\} = \{a \in G : a \in N\} = N.$$

Lema 1.107 (kernel). Sea $\phi : G_1 \rightarrow G_2$ un homomorfismo. Entonces:

1. $\ker(\phi) \leq G_1$.
2. $\phi : G_1 \rightarrow G_2$ es inyectivo si y solo si $\ker(\phi) = \{e_1\}$.

Demostración.

1. Usaremos el Test del Subgrupo Normal:

(N1) $e_1 \in \ker(\phi)$ porque $\phi(e_1) = e_2$.

(N2) Sean $a, b \in \ker(\phi)$, lo que implica que $\phi(a) = e_2$ y $\phi(b) = e_2$.
Entonces,

$$\phi(a^{-1}b) = \phi(a)^{-1}\phi(b) = e_2^{-1}e_2 = e_2 \implies a^{-1}b \in \ker(\phi).$$

(N3) Sea $g \in G_1$ y $a \in \ker(\phi)$. Entonces,

$$\phi(gag^{-1}) = \phi(g)\phi(a)\phi(g)^{-1} = \phi(g)e_2\phi(g)^{-1} = e_2.$$

Por lo tanto, $gag^{-1} \in \ker(\phi)$.

2. Demostraremos cada implicación:

(\implies) Supongamos que $\phi : G_1 \rightarrow G_2$ es inyectivo y sea $a \in \ker(\phi)$. Luego, $\phi(a) = e_2 = \phi(e_1)$. Por inyectividad, $a = e_1$, lo que demuestra que $\ker(\phi) \subseteq \{e_1\}$. Como claramente se cumple la inclusión opuesta, $\ker(\phi) = \{e_1\}$.

(\impliedby) Supongamos que $\ker(\phi) = \{e_1\}$. Sean $a, b \in G_1$ tales que $\phi(a) = \phi(b)$. Observemos que

$$\phi(a) = \phi(b) \implies \phi(a)\phi(b)^{-1} = e_2 \implies \phi(ab^{-1}) = e_2.$$

Entonces, $ab^{-1} \in \ker(\phi) = \{e_1\}$, lo que implica que $ab^{-1} = e_1$. Así, $a = b$ y $\phi : G_1 \rightarrow G_2$ es inyectivo.

□

1.4.2. Isomorfismos

Definición 1.108 (isomorfismo). Sean G_1 y G_2 grupos. Un *isomorfismo* entre G_1 y G_2 es un homomorfismo biyectivo. En caso de que exista un isomorfismo entre G_1 y G_2 decimos que G_1 y G_2 son *isomorfos* y escribimos $G_1 \cong G_2$.

Lema 1.109 (inverso de un isomorfismo). Sea $\phi : G_1 \rightarrow G_2$ un isomorfismo. Entonces, $\phi^{-1} : G_2 \rightarrow G_1$ también es un isomorfismo.

Demostración. Como $\phi : G_1 \rightarrow G_2$ es biyectivo, existe su función inversa $\phi^{-1} : G_2 \rightarrow G_1$, la cual también es biyectiva. Solo hace falta demostrar que ϕ^{-1} es un homomorfismo. Sean $y_1, y_2 \in G_2$ elementos arbitrarios. Por sobreyectividad de

ϕ , existen $x_1, x_2 \in G_1$ tales que $\phi(x_1) = y_1$ y $\phi(x_2) = y_2$. Debido a que ϕ es un homomorfismo, sabemos que cumple

$$\phi(x_1x_2) = \phi(x_1)\phi(x_2).$$

Aplicando ϕ^{-1} de ambos lados y sustituyendo $\phi(x_i) = y_i$, obtenemos que

$$\phi^{-1}(\phi(x_1x_2)) = \phi^{-1}(\phi(x_1)\phi(x_2)) \Rightarrow x_1x_2 = \phi^{-1}(y_1y_2).$$

Finalmente, sustituyendo $x_i = \phi^{-1}(y_i)$ obtenemos que

$$\phi^{-1}(y_1)\phi^{-1}(y_2) = \phi^{-1}(y_1y_2).$$

Por lo tanto, ϕ^{-1} es un isomorfismo. \square

Teorema 1.110 (relación isomorfía). La relación de isomorfía \cong entre grupos es una relación de equivalencia.

Demostración. Sean G_1, G_2 y G_3 grupos.

(E1) *Reflexividad.* La función identidad $\text{id} : G_1 \rightarrow G_1$ es un isomorfismo, así que $G_1 \cong G_1$.

(E2) *Simetría.* Supongamos que $G_1 \cong G_2$, así que existe un isomorfismo $\phi : G_1 \rightarrow G_2$. Por el lema anterior, $\phi^{-1} : G_2 \rightarrow G_1$ es un isomorfismo, y entonces $G_2 \cong G_1$.

(E3) *Transitividad.* Supongamos que $G_1 \cong G_2$ y $G_2 \cong G_3$. Entonces, existen isomorfismos $\phi_1 : G_1 \rightarrow G_2$ y $\phi_2 : G_2 \rightarrow G_3$. Como la composición de biyecciones es biyección y la composición de homomorfismos es homomorfismo, entonces $\phi_2 \circ \phi_1 : G_1 \rightarrow G_3$ es un isomorfismo. Por lo tanto, $G_1 \cong G_3$. \square

La *clase de isomorfía* de un grupo G es la colección de todos los grupos isomorfos a G ; es decir, las clases de isomorfía son las clases de equivalencia bajo la relación de isomorfía.

Lema 1.111 (propiedades de isomorfismos). Sea $\phi : G_1 \rightarrow G_2$ un isomorfismo. Entonces:

1. $|G_1| = |G_2|$.
2. G_1 es abeliano, o cíclico, si y solo si G_2 es abeliano, o cíclico, respectivamente.
3. $|\phi(g)| = |g|$ para toda $g \in G_1$.

Demostración.

1. G_1 y G_2 tienen la misma cardinalidad porque ϕ es una biyección.

2. Supongamos que G_1 es abeliano y sean $y_1, y_2 \in G_2$. Por sobreyectividad de ϕ , existen $x_1, x_2 \in G_1$ tales que $\phi(x_i) = y_i$, $i = 1, 2$. Luego,

$$y_1 y_2 = \phi(x_1) \phi(x_2) = \phi(x_1 x_2) = \phi(x_2 x_1) = \phi(x_2) \phi(x_1) = y_2 y_1.$$

Por lo tanto G_2 es abeliano.

Por otro lado, supongamos que G_1 es cíclico y $G_1 = \langle g \rangle$. Por sobreyectividad de ϕ , para todo $y \in G_2$ existe $g^i \in G_1$ tal que $\phi(g^i) = y$. Luego, $y = \phi(g)^i$, lo que demuestra que $G_2 = \langle \phi(g) \rangle$.

Las implicaciones recíprocas se demuestran análogamente usando el isomorfismo $\phi^{-1} : G_2 \rightarrow G_1$.

3. El Lema 1.102 (4.) nos dice que si $g \in G$ es de orden finito, entonces $|\phi(g)|$ divide a $|g|$. Aplicando el mismo lema al homomorfismo ϕ^{-1} , obtenemos que $|g| = |\phi^{-1}(\phi(g))|$ divide a $|\phi(g)|$. Esto demuestra que si g es de orden finito, entonces $|\phi(g)| = |g|$. Por otro lado, supongamos que $|g| = \infty$. Por reducción al absurdo, si $|\phi(g)| = m < \infty$, entonces

$$g^m = \phi^{-1}(\phi(g))^m = \phi^{-1}(\phi(g)^m) = \phi^{-1}(e_2) = e_1.$$

Esto contradice que g no es de orden finito, por lo que $|\phi(g)| = \infty$.

□

Ejemplo 1.112. El lema anterior puede servir para determinar cuándo dos grupos **no** son isomorfos. Por ejemplo:

1. Los grupo \mathbb{Z}_4 y \mathbb{Z}_5 no son isomorfos porque no tienen el mismo tamaño.
2. Los grupos \mathbb{Z}_8 y D_8 no son isomorfos, porque el primero es abeliano pero el segundo no es abeliano.
3. Los grupos \mathbb{C}^* y \mathbb{R}^* no son isomorfos porque el primero tiene un elemento de orden 4 (que es $i \in \mathbb{C}^*$) mientras que el segundo no tiene ningún elemento de orden 4.

Teorema 1.113 (Primer Teorema de Isomorfía). Sea $\phi : G_1 \rightarrow G_2$ un homomorfismo. Entonces,

$$G_1 / \ker(\phi) \cong \phi(G_1).$$

Demostración. Consideremos la función $\psi : G_1 / \ker(\phi) \rightarrow \phi(G_1)$ definida de la siguiente forma

$$\psi(g \ker(\phi)) = \phi(g), \quad \forall g \ker(\phi) \in G_1 / \ker(\phi).$$

Demostraremos que ψ es un isomorfismo bien definido en cuatro pasos.

1. *Bien definido.* Supongamos que $g_1 \ker(\phi) = g_2 \ker(\phi)$. Entonces $g_2^{-1} g_1 \in \ker(\phi)$, lo que significa que

$$\phi(g_2^{-1} g_1) = e_2 \Rightarrow \phi(g_2)^{-1} \phi(g_1) = e_2 \Rightarrow \phi(g_1) = \phi(g_2).$$

Por definición de ψ , tenemos que $\psi(g_1 \ker(\phi)) = \psi(g_2 \ker(\phi))$.

2. *Homomorfismo.* Para cualquier $g_1 \ker(\phi), g_2 \ker(\phi) \in G_1/\ker(\phi)$,

$$\begin{aligned}\psi(g_1 \ker(\phi)g_2 \ker(\phi)) &= \psi(g_1g_2 \ker(\phi)) = \phi(g_1g_2) \\ &= \phi(g_1)\phi(g_2) = \psi(g_1 \ker(\phi))\psi(g_2 \ker(\phi)).\end{aligned}$$

3. *Inyectivo.* Supongamos que $\psi(g_1 \ker(\phi)) = \psi(g_2 \ker(\phi))$. Por definición de ψ ,

$$\phi(g_1) = \phi(g_2) \Rightarrow \phi(g_2)^{-1}\phi(g_1) = e_2 \Rightarrow \phi(g_2^{-1}g_1) = e_2.$$

Luego $g_2^{-1}g_1 \in \ker(\phi)$, lo que implica que $g_1 \ker(\phi) = g_2 \ker(\phi)$.

4. *Sobreyectivo.* Sea $\phi(g) \in \phi(G_1)$ un elemento arbitrario. Claramente, su preimagen bajo ψ es $g \ker(\phi) \in G_1/\ker(\phi)$, lo que demuestra que ψ es sobreyectivo. □

Corolario 1.114. Sea $\phi : G_1 \rightarrow G_2$ un homomorfismo. Si H es un subgrupo finito de G_1 , entonces $|\phi(H)|$ divide a $|H|$.

Demostración. La restricción de ϕ a H nos da un homomorfismo $\phi|_H : H \rightarrow G_2$. Por el Primer Teorema de Isomorfía,

$$H/\ker(\phi|_H) \cong \phi(H).$$

Ahora, como H es finito, usamos el Teorema de Lagrange,

$$|\phi(H)| = |H/\ker(\phi|_H)| = \frac{|H|}{|\ker(\phi|_H)|}.$$

Luego, $|\phi(H)||\ker(\phi|_H)| = |H|$, lo que demuestra el corolario. □

Definición 1.115 (automorfismo). Un *automorfismo* de un grupo G es un isomorfismo de la forma $\phi : G \rightarrow G$.

Proposición 1.116 (grupo de automorfismos). El conjunto de automorfismos de un grupo G , denotado por

$$\text{Aut}(G) := \{\phi : G \rightarrow G \mid \phi \text{ es un automorfismo}\},$$

es un grupo equipado con la composición de funciones.

Demostración.

(G0) Por el Lema 1.104, la composición de dos automorfismos de G es un automorfismo de G .

(G1) La composición de funciones siempre es una operación asociativa.

(G2) La función identidad $\text{id} : G \rightarrow G$ es un automorfismo, así que $\text{id} \in \text{Aut}(G)$.

(G3) Por el Lema 1.109, la inversa de un automorfismo de G es un automorfismo de G .

□

Proposición 1.117 (automorfismo interno). Sea G un grupo y $g \in G$ un elemento fijo. La función $\phi_g : G \rightarrow G$ definida por

$$\phi_g(x) := gxg^{-1}, \quad \forall x \in G$$

es un automorfismo de G , el cual es llamado el *automorfismo interno inducido por g* .

Demostración. La función ϕ_g es biyectiva porque $\phi_{g^{-1}}$ es su inversa; efectivamente, para toda $x \in G$ se cumple

$$\begin{aligned} \phi_g \circ \phi_{g^{-1}}(x) &= g(g^{-1}xg)g^{-1} = x \\ \phi_{g^{-1}} \circ \phi_g(x) &= g^{-1}(gxg^{-1})g = x. \end{aligned}$$

Alternativamente, el lector puede demostrar directamente que ϕ_g es inyectiva y sobreyectiva. Además, ϕ_g es un homomorfismo: para toda $x, y \in G$,

$$\phi_g(xy) = gxyg^{-1} = (gxg^{-1})(gyg^{-1}) = \phi_g(x)\phi_g(y).$$

□

Proposición 1.118 (automorfismos internos). El conjunto de automorfismos internos

$$\text{Inn}(G) := \{\phi_g \in \text{Aut}(G) : g \in G\}$$

es un subgrupo normal de $\text{Aut}(G)$.

Demostración. Usaremos el Test del Subgrupo Normal:

(N1) Claramente, $\text{id} = \phi_e \in \text{Inn}(G)$.

(N2) Sean $g, h \in G$. Observemos que, para toda $x \in G$,

$$\phi_g \circ \phi_h(x) = g(hxh^{-1})g^{-1} = (gh)x(gh)^{-1} = \phi_{gh}(x).$$

Además, $(\phi_g)^{-1} = \phi_{g^{-1}}$, porque $\phi_g \circ \phi_{g^{-1}} = \phi_{gg^{-1}} = \phi_e = \text{id}$. Por lo tanto,

$$(\phi_g)^{-1} \circ \phi_h = \phi_{g^{-1}} \circ \phi_h = \phi_{g^{-1}h} \in \text{Inn}(G).$$

(N3) Sea $\phi_g \in \text{Inn}(G)$ y $\sigma \in \text{Aut}(G)$. Entonces, para toda $x \in G$,

$$\sigma \circ \phi_g \circ \sigma^{-1}(x) = \sigma(g\sigma^{-1}(x)g^{-1}) = \sigma(g)x\sigma(g)^{-1} = \phi_{\sigma(g)}(x).$$

Por lo tanto, $\sigma \circ \phi_g \circ \sigma^{-1} = \phi_{\sigma(g)} \in \text{Inn}(G)$.

□

Palabras clave: homomorfismo, kernel, isomorfismo, Primer Teorema de Isomorfía, automorfismo, automorfismo interno.

1.4.3. Ejercicios

Ejercicio 1.60. Determina si las siguientes funciones son homomorfismos de grupos, y en caso de serlo, encuentra su kernel e imagen.

1. $\phi : \mathbb{R}^* \rightarrow \mathbb{R}^*$ definido como $\phi(x) = x^4$, donde $\mathbb{R}^* := \mathbb{R} \setminus \{0\}$ es un grupo con la multiplicación.
2. $\phi : \mathbb{R}^* \rightarrow \mathbb{R}^*$ definido como $\phi(x) = 5x$, donde $\mathbb{R}^* := \mathbb{R} \setminus \{0\}$ es un grupo con la multiplicación.
3. $\phi : \mathbb{Z} \rightarrow \mathbb{Z}$ definido como $\phi(x) = 5x$, donde \mathbb{Z} es un grupo con la suma.
4. $\phi : \mathbb{R} \rightarrow \mathbb{R}^*$ definido como $\phi(x) = 2^x$, donde \mathbb{R} y \mathbb{R}^* son grupos con la suma y la multiplicación, respectivamente.
5. $\phi : \mathbb{Z} \oplus \mathbb{Z} \rightarrow \mathbb{Z}$ definido como $\phi(x, y) = x - y$.

Ejercicio 1.61. Sea $\phi : G_1 \rightarrow G_2$ un homomorfismo. Demuestra por inducción que $\phi(g^k) = \phi(g)^k$, para toda $k \in \mathbb{Z}$, $g \in G_1$.

Ejercicio 1.62. Sea $\phi : G_1 \rightarrow G_2$ un homomorfismo. Demuestra que si $H \leq G_1$ es cíclico, o abeliano, entonces $\phi(H)$ es cíclico, o abeliano, respectivamente.

Ejercicio 1.63. Sea G un grupo abeliano y sean $\phi : G \rightarrow G$ y $\tau : G \rightarrow G$ homomorfismos. Demuestra que la función $\phi\tau : G \rightarrow G$ definida por

$$\phi\tau(g) = \phi(g)\tau(g), \quad \forall g \in G$$

es un homomorfismo.

Ejercicio 1.64. Sea $\phi : G_1 \rightarrow G_2$ un homomorfismo. Demuestra que si $K \trianglelefteq G_2$, entonces $\phi^{-1}(K) \trianglelefteq G_1$.

Ejercicio 1.65. Demuestra que \mathbb{Z}_{12} no es isomorfo a $\mathbb{Z}_2 \oplus \mathbb{Z}_6$.

Ejercicio 1.66. Demuestra que $U(8)$ no es isomorfo a $U(10)$, pero $U(8)$ y $U(12)$ son isomorfos.

Ejercicio 1.67. Sean $\phi_1 : G_1 \rightarrow G_2$ y $\phi_2 : G_2 \rightarrow G_3$ homomorfismos. Demuestra que $\ker(\phi_2 \circ \phi_1) = \phi_1^{-1}(\ker(\phi_2))$.

Ejercicio 1.68. Sean $\phi_1 : G_1 \rightarrow G_2$ y $\phi_2 : G_2 \rightarrow G_3$ homomorfismos. Demuestra que $\ker(\phi_1) \subseteq \ker(\phi_2 \circ \phi_1)$. Si ϕ_1 y ϕ_2 son sobreyectivos y G_i es finito, $i = 1, 2, 3$, escribe el índice $[\ker(\phi_2 \circ \phi_1) : \ker(\phi_1)]$ en términos de $|G_2|$ y $|G_3|$.

Ejercicio 1.69. Sea G un grupo. Demuestra que $\phi : G \rightarrow G$ definido como $\phi(x) = x^{-1}$ es un automorfismo si y solo si G es abeliano.

Ejercicio 1.70. Sea G un grupo. Demuestra que $\phi : G \rightarrow G$ definido como $\phi(x) = x^2$ es un homomorfismo si y solo si G es abeliano. ¿Es ϕ un automorfismo de G ?

Ejercicio 1.71. Para cualquier $n \in \mathbb{N}$, demuestra que hay un número infinito de grupos de orden n , pero que solo hay un número finito de clases de isomorfía de grupos de orden n . (Sugerencia: argumenta que solo es posible equiparle una cantidad finita de operaciones binarias distintas a un conjunto finito.)

Ejercicio 1.72 (Segundo Teorema de Isomorfía). Sea K un subgrupo de un grupo G y N un subgrupo normal de G . Demuestra lo siguiente:

$$K/(K \cap N) \cong KN/N.$$

(Sugerencia: demuestra que $\phi : K \rightarrow KN/N$ definido por $\phi(k) = kN$ es un homomorfismo sobreyectivo con kernel $K \cap N$.)

Ejercicio 1.73 (Tercer Teorema de Isomorfía). Si M y N son subgrupos normales de G y $N \leq M$, demuestra lo siguiente:

1. M/N es un subgrupo normal de G/N .
2. $(G/N)/(M/N) \cong G/M$. (*)

Ejercicio 1.74 (Teorema de Correspondencia). Sea G un grupo y N un subgrupo normal de G . Demuestra lo siguiente:

1. Si K es un subgrupo tal que $N \leq K \leq G$, entonces K/N es un subgrupo de G/N .
2. Si \bar{K} es un subgrupo de G/N , entonces $K := \{g \in G : gN \in \bar{K}\}$ es un subgrupo de G que contiene a N y cumple que $\bar{K} = K/N$.

Ejercicio 1.75. Sean A , B y C grupos. Considera una sucesión de homomorfismos

$$\{e\} \xrightarrow{\phi_1} A \xrightarrow{\phi_2} B \xrightarrow{\phi_3} C \xrightarrow{\phi_4} \{e\},$$

tales que $\text{im}(\phi_i) = \ker(\phi_{i+1})$, para $i = 1, 2, 3$. Demuestra lo siguiente:

1. ϕ_2 es inyectivo.
2. ϕ_3 es sobreyectivo.

3. $B/A \cong C$.

Ejercicio 1.76. Demuestra que para cualquier grupo G ,

$$\text{Inn}(G) \cong G/Z(G).$$

(Sugerencia: demuestra que la función $\Phi : G \rightarrow \text{Inn}(G)$ definida por $\Phi(g) = \phi_g$, $\forall g \in G$, es un homomorfismo sobreyectivo con kernel $Z(G)$ y usa el Primer Teorema de Isomorfía).

Ejercicio 1.77. Sea G un grupo finito y $\sigma \in \text{Aut}(G)$ un automorfismo que solo fija a la identidad (i.e., si $g \neq e$ entonces $\sigma(g) \neq g$). Demuestra que $G = \{g^{-1}\sigma(g) : g \in G\}$.

2

Tipos particulares de grupos

2.1. Grupos cíclicos

2.1.1. Estructura

Sea G un grupo y $g \in G$. Por el Teorema 1.40, sabemos que si $|g| = n$, entonces el subgrupo cíclico generado por g es

$$\langle g \rangle = \{e, g, g^2, \dots, g^{n-1}\} \text{ y } |\langle g \rangle| = |g|.$$

En esta sección, nos enfocaremos en estudiar la estructura del grupo $\langle g \rangle$. Recordemos que G en sí mismo es cíclico si existe un $g \in G$ tal que $G = \langle g \rangle$. En los resultados de esta sección, algunas veces asumiremos que todo el grupo G es cíclico, pero otras veces G será un grupo arbitrario y nos enfocaremos en su subgrupo $\langle g \rangle$.

Observación 2.1. Sea $g \in G$ tal que $|g| = n < \infty$. El Lema 1.25 establece que si $g^k = e$ para algún $k \in \mathbb{Z}$, entonces $n \mid k$. Por otro lado, si $n \mid k$, entonces $k = qn$, para algún $q \in \mathbb{Z}$, lo que implica que $g^k = g^{qn} = (g^n)^q = e^q = e$. Así, podemos decir que $g^k = e$ si y solo si $n \mid k$.

Lema 2.2 (criterios para igualdad de potencias). Sea G un grupo y $g \in G$.

1. Si $|g| = n < \infty$, entonces $g^i = g^j$ si y solo si $i = j \pmod{n}$.
2. Si $|g| = \infty$, entonces $g^i = g^j$ si y solo si $i = j$.

Demostración.

1. Usando la observación previa,

$$g^i = g^j \Leftrightarrow g^{i-j} = e \Leftrightarrow n \mid (i-j) \Leftrightarrow i = j \pmod{n}.$$

2. Como $|g| = \infty$, tenemos que $g^k = e$ si y solo si $k = 0$. Por lo tanto,

$$g^i = g^j \Leftrightarrow g^{i-j} = e \Leftrightarrow i-j = 0 \Leftrightarrow i = j.$$

□

Teorema 2.3 (clases de isomorfía de grupos cíclicos). Sea G un grupo cíclico.

1. Si G es finito de orden n , entonces $G \cong \mathbb{Z}_n$.
2. Si G es infinito, entonces $G \cong \mathbb{Z}$.

Demostración.

1. Sea G un grupo cíclico de orden n . Entonces $G = \langle g \rangle$, para algún $g \in G$, con $|g| = n$, y

$$G = \{e, g, g^2, \dots, g^{n-1}\}.$$

Consideremos la función $\phi : G \rightarrow \mathbb{Z}_n$ definida por $\phi(g^i) = [i] \in \mathbb{Z}_n$, para toda i . Por el criterio (1) para igualdad de potencias,

$$g^i = g^j \Leftrightarrow i = j \pmod{n} \Leftrightarrow [i] = [j] \Leftrightarrow \phi(g^i) = \phi(g^j).$$

Esto implica que ϕ está bien definida y es inyectiva. Además, claramente ϕ es sobreyectiva. Finalmente,

$$\phi(g^i g^j) = \phi(g^{i+j}) = [i+j] = [i] + [j] = \phi(g^i) + \phi(g^j).$$

Por lo tanto, ϕ es un isomorfismo.

2. Sea $G = \langle g \rangle$ un grupo cíclico infinito. Consideramos la función $\psi : G \rightarrow \mathbb{Z}$ definida por $\psi(g^i) = i \in \mathbb{Z}$. Por el criterio (2) para igualdad de potencias,

$$g^i = g^j \Leftrightarrow i = j \Leftrightarrow \psi(g^i) = \psi(g^j).$$

Esto implica que ψ está bien definida y es inyectiva. Además, claramente ψ es sobreyectiva. Finalmente,

$$\psi(g^i g^j) = \psi(g^{i+j}) = i + j = \psi(g^i) + \psi(g^j).$$

Por lo tanto, ψ es un isomorfismo.

□

Observación 2.4. Sea G cualquier grupo y $g \in G$. En general, $\langle g \rangle$ es el subgrupo de G más pequeño que contiene a g ; es decir, si H es un subgrupo de G tal que $g \in H$, entonces $\langle g \rangle \subseteq H$. Esto es fácil de verificar usando la cerradura de H , ya que $g \in H$ implica que $g^k \in H$, para toda $k \in \mathbb{Z}$.

Teorema 2.5 (orden de potencias). Sea G un grupo y $g \in G$ un elemento de orden n . Para cualquier $k \in \mathbb{Z}_+$,

1. $\langle g^k \rangle = \langle g^{\text{mcd}(n,k)} \rangle$.
2. $|g^k| = \frac{n}{\text{mcd}(n,k)}$.

Demostración.

1. Sea $d := \text{mcd}(n, k)$. Como $d \mid k$, existe $q \in \mathbb{Z}$ tal que $k = qd$. Luego, $g^k = (g^d)^q \in \langle g^d \rangle$. Por la observación anterior, tenemos que $\langle g^k \rangle \subseteq \langle g^d \rangle$. Por otro lado, por el Lema de Bezout, sabemos que existen $t_1, t_2 \in \mathbb{Z}$ tales que $d = t_1n + t_2k$. Luego,

$$g^d = g^{t_1n + t_2k} = (g^n)^{t_1} (g^k)^{t_2} = e^{t_1} (g^k)^{t_2} = (g^k)^{t_2} \in \langle g^k \rangle.$$

Por la observación anterior, $\langle g^d \rangle \subseteq \langle g^k \rangle$. Esto demuestra que $\langle g^d \rangle = \langle g^k \rangle$.

2. Primero demostraremos que si $k \mid n$, entonces $|g^k| = \frac{n}{k}$. Vemos que

$$(g^k)^{\frac{n}{k}} = g^{k \frac{n}{k}} = g^n = e.$$

Sin embargo, para todo $i \in \mathbb{Z}_+$ tal que $i < \frac{n}{k}$ se tiene que $ik < n$, por lo que $(g^k)^i \neq e$, por definición de $n = |g|$. Luego, $\frac{n}{k}$ es el menor entero positivo tal que $(g^k)^{\frac{n}{k}} = e$, lo que significa que $|g^k| = \frac{n}{k}$.

Para demostrar el caso general (cuando k no necesariamente divide a n), usamos el punto anterior de este lema y el hecho de que $\text{mcd}(n, k) \mid n$:

$$|g^k| = |\langle g^k \rangle| = |\langle g^{\text{mcd}(n, k)} \rangle| = |g^{\text{mcd}(n, k)}| = \frac{n}{\text{mcd}(n, k)}.$$

□

Ejemplo 2.6. Sea G cualquier grupo y $g \in G$ un elemento de orden 12. Con el teorema anterior podemos calcular el orden de cualquier potencia de g , por ejemplo:

$$\begin{aligned} |g^2| &= \frac{12}{\text{mcd}(12, 2)} = \frac{12}{2} = 6, & |g^5| &= \frac{12}{\text{mcd}(12, 5)} = \frac{12}{1} = 12, \\ |g^8| &= \frac{12}{\text{mcd}(12, 8)} = \frac{12}{4} = 3, & |g^9| &= \frac{12}{\text{mcd}(12, 9)} = \frac{12}{3} = 4. \end{aligned}$$

Corolario 2.7. Sea $g \in G$ un elemento de orden n . Entonces, $\langle g^i \rangle = \langle g^j \rangle$ si y solo si $\text{mcd}(n, i) = \text{mcd}(n, j)$.

Demostración.

(\Rightarrow) Supongamos que $\langle g^i \rangle = \langle g^j \rangle$. Por el teorema anterior,

$$|g^i| = |g^j| \Rightarrow \frac{n}{\text{mcd}(n, i)} = \frac{n}{\text{mcd}(n, j)} \Rightarrow \text{mcd}(n, i) = \text{mcd}(n, j).$$

(\Leftarrow) Supongamos que $\text{mcd}(n, i) = \text{mcd}(n, j)$. Por el teorema anterior,

$$\langle g^i \rangle = \langle g^{\text{mcd}(n, i)} \rangle = \langle g^{\text{mcd}(n, j)} \rangle = \langle g^j \rangle.$$

□

Corolario 2.8. Sea $G = \langle g \rangle$ un grupo cíclico de orden n . La potencia g^k es un generador de G (es decir, $G = \langle g^k \rangle$) si y solo si $\text{mcd}(n, k) = 1$.

Demostración. Observemos que $\langle g \rangle = \langle g^k \rangle$ si y solo si $|g| = |g^k|$ si y solo si $n = \frac{n}{\text{mcd}(n, k)}$, lo cual se cumple si y solo si $\text{mcd}(n, k) = 1$. \square

Teorema 2.9 (teorema fundamental de grupos cíclicos). Sea G un grupo cíclico.

1. Todo subgrupo de G es cíclico.
2. Si G tiene orden finito n , para cada divisor $k|n$ existe un único subgrupo H_k de G de orden k . Explícitamente, si $G = \langle g \rangle$, entonces $H_k = \langle g^{\frac{n}{k}} \rangle$. Además, no existen otros subgrupos de G distintos de los descritos anteriormente.

Demostración.

1. Supongamos que $G = \langle g \rangle = \{g^i : i \in \mathbb{Z}\}$ y sea H un subgrupo de G . Si $H = \{e\}$, entonces $H = \langle e \rangle$ es cíclico. Supongamos que $H \neq \{e\}$ y sea m el menor entero positivo tal que $g^m \in H$.

Afirmación: $H = \langle g^m \rangle$.

Claramente, $\langle g^m \rangle \subseteq H$, por cerradura. Para demostrar la otra contención, sea $g^s \in H$ un elemento arbitrario de H . Por el algoritmo de la división, existen $q, r \in \mathbb{Z}$ tales que $s = qm + r$ con $0 \leq r < m$. Observemos que, por cerradura, $g^r = g^{s - qm} = g^s (g^m)^{-q} \in H$, puesto que $g^s, g^m \in H$. De tal forma, si $r \neq 0$, entonces r es un entero positivo menor que m tal que $g^r \in H$. Esto contradice la elección de m . Por lo tanto, $r = 0$, lo que implica que $s = qm$. Así, $g^s = g^{qm} = (g^m)^q \in \langle g^m \rangle$, lo que demuestra que $H \subseteq \langle g^m \rangle$.

2. Sea $G = \langle g \rangle$ con $|g| = n$, y sea k un divisor de n . Definimos el subgrupo $H_k := \langle g^{\frac{n}{k}} \rangle$. Por el Teorema 2.5:

$$|H_k| = |g^{\frac{n}{k}}| = \frac{n}{\text{mcd}(n, n/k)} = \frac{n}{n/k} = k.$$

Ahora demostraremos que el grupo H_k es el único subgrupo de G de orden k . Sea H' un subgrupo de G de orden k . Por la parte (1.) de este teorema, H' es cíclico así que $H' = \langle g^s \rangle$ para algún $s \in \mathbb{Z}$. Por el Teorema 2.5:

$$\frac{n}{\text{mcd}(n, n/k)} = k = |H'| = |g^s| = \frac{n}{\text{mcd}(n, s)}.$$

Por lo tanto, $\text{mcd}(n, n/k) = \text{mcd}(n, s)$. Por el Corolario 2.7, $H_k = \langle g^{\frac{n}{k}} \rangle = \langle g^s \rangle = H'$.

Finalmente, el Teorema de Lagrange implica que no pueden existir subgrupos de G cuyos órdenes no dividan a n .

□

Observación 2.10. A través del isomorfismo de la demostración del Teorema 2.3, podemos enunciar los resultados anteriores para el grupo cíclico \mathbb{Z}_n :

1. Para toda $k \in \mathbb{Z}_n$, $\langle k \rangle = \langle \text{mcd}(n, k) \rangle$.
2. Para toda $k \in \mathbb{Z}_n$, $|k| = \frac{n}{\text{mcd}(n, k)}$.
3. Para toda $i, j \in \mathbb{Z}_n$, $\langle i \rangle = \langle j \rangle$ si y solo si $\text{mcd}(n, i) = \text{mcd}(n, j)$.
4. El elemento $k \in \mathbb{Z}_n$ genera a \mathbb{Z}_n si y solo si $\text{mcd}(n, k) = 1$.
5. Para cada $k \mid n$, existe un único subgrupo de \mathbb{Z}_n de orden k , dado por $H_k = \langle \frac{n}{k} \rangle$.

Ejemplo 2.11. Los generadores de \mathbb{Z}_{12} son 1, 5, 7, y 11, es decir,

$$\mathbb{Z}_{12} = \langle 1 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 11 \rangle.$$

Ejemplo 2.12. Si p es primo, entonces todo $k \in \mathbb{Z}_p$ con $k \neq 0$ es generador de \mathbb{Z}_p .

Observación 2.13. Los generadores de \mathbb{Z}_n son precisamente los elementos del grupo $U(n) = \{k \in \mathbb{Z}_n : \text{mcd}(n, k) = 1\}$.

Definición 2.14 (función φ de Euler). La *función phi de Euler* es la función $\varphi : \mathbb{Z}_+ \rightarrow \mathbb{Z}_+$ dada por

$$\varphi(n) = |\{k \in \mathbb{Z}_+ : 1 \leq k \leq n \text{ y } \text{mcd}(n, k) = 1\}| = |U(n)|.$$

Lema 2.15 (función φ de Euler). Sea $n \in \mathbb{Z}_+$.

1. El número de elementos generadores de \mathbb{Z}_n es $\varphi(n)$.
2. Para cualquier $k \mid n$, el número de elementos de \mathbb{Z}_n de orden k es $\varphi(k)$.

Demostración.

1. Esta parte es trivial, puesto que el conjunto de generadores de \mathbb{Z}_n es $U(n)$.
2. Por el Teorema Fundamental de Grupos Cíclicos, \mathbb{Z}_n tiene un único subgrupo de orden k , dado por $H_k = \langle \frac{n}{k} \rangle$. Si $a \in \mathbb{Z}_n$ es un elemento de orden k , entonces $\langle a \rangle$ es un subgrupo de orden k ; por unicidad, tenemos que $H_k = \langle a \rangle$. Por lo tanto, los elementos de \mathbb{Z}_n de orden k son precisamente los generadores del subgrupo H_k . Por el punto anterior, el número de generadores de H_k es $\varphi(k)$.

□

Lema 2.16 (contención entre subgrupos de un grupo cíclico). Sea $G = \langle g \rangle$ un grupo cíclico de orden n y $H_k := \langle g^{\frac{n}{k}} \rangle$, para $k \mid n$. Para toda $k, s \mid n$,

$$H_k \subseteq H_s \text{ si y solo si } k \mid s.$$

Demostración. Si $H_k \subseteq H_s$, el Teorema de Lagrange implica que $k \mid s$, puesto que $|H_k| = k$ y $|H_s| = s$. Por otro lado, supongamos que $k \mid s$. Por el Teorema Fundamental de Grupos Cíclicos, sabemos que H_s tiene un único subgrupo K de orden k . Sin embargo, K también es subgrupo de G , así que la unicidad de los subgrupos implica que $H_k = K \subseteq H_s$. \square

Sea G un grupo y $\text{Sub}(G) := \{H : H \leq G\}$ el conjunto de subgrupos de G . El conjunto parcialmente ordenado $(\text{Sub}(G), \subseteq)$, donde \subseteq es la inclusión de subconjuntos, se llama la *retícula*¹ de subgrupos de G . Normalmente es conveniente visualizar a $(\text{Sub}(G), \subseteq)$ mediante una gráfica cuyos vértices, o nodos, son los elementos de $\text{Sub}(G)$, y dibujamos una arista de H_1 a H_2 si $H_1 \subseteq H_2$. Al ser \subseteq siempre una relación reflexiva y transitiva, podemos simplificar su grafo omitiendo las aristas de un vértice a sí mismo, y omitiendo las aristas que puedan deducirse por transitividad: el diagrama resultante se llama el *diagrama de Hasse* de la retícula de subgrupos de G .

Ejemplo 2.17. Podemos usar el Teorema Fundamental de los Grupos Cíclicos y el lema anterior para dibujar el diagrama de la retícula de subgrupos de \mathbb{Z}_6 . Sabemos que los subgrupos de \mathbb{Z}_6 son $H_k = \langle \frac{6}{k} \rangle$, para $k \mid 6$. Explícitamente,

$$\begin{aligned} H_1 &= \langle 0 \rangle = \{0\}, \\ H_2 &= \langle 3 \rangle = \{0, 3\} \cong \mathbb{Z}_2, \\ H_3 &= \langle 2 \rangle = \{0, 2, 4\} \cong \mathbb{Z}_3, \\ H_6 &= \langle 1 \rangle = \mathbb{Z}_6. \end{aligned}$$

El diagrama de la retícula de subgrupos de \mathbb{Z}_6 está dado por la Figura 2.1.

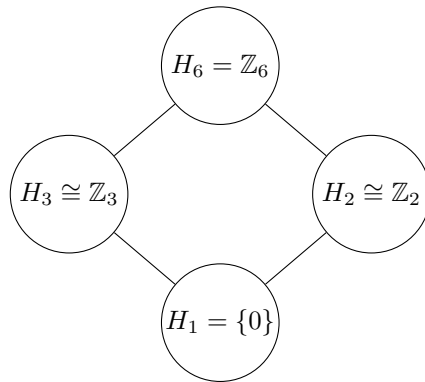
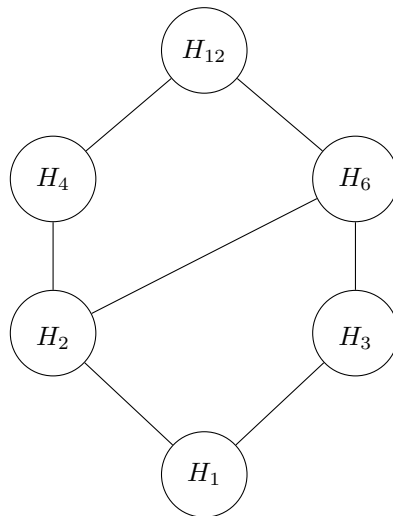
Ejemplo 2.18. Dibujaremos el diagrama de la retícula de subgrupos de \mathbb{Z}_{12} . Sus subgrupos son:

$$\begin{aligned} H_1 &= \langle 0 \rangle = \{0\}, \\ H_2 &= \langle 6 \rangle = \{0, 6\} \cong \mathbb{Z}_2, \\ H_3 &= \langle 4 \rangle = \{0, 4, 8\} \cong \mathbb{Z}_3, \\ H_4 &= \langle 3 \rangle = \{0, 3, 6, 9\} \cong \mathbb{Z}_4, \\ H_6 &= \langle 2 \rangle = \{0, 2, 4, 6, 8, 10\} \cong \mathbb{Z}_6, \\ H_{12} &= \langle 1 \rangle = \mathbb{Z}_{12}. \end{aligned}$$

El diagrama de la retícula de subgrupos de \mathbb{Z}_{12} está dado por la Figura 2.2.

Es sencillo darse cuenta que la retícula de subgrupos de \mathbb{Z}_n es de hecho isomorfa a la retícula $(\text{div}(n), |)$, donde $\text{div}(n)$ es el conjunto de divisores de n y $|$ es la relación de orden parcial de divisibilidad.

¹Formalmente, una *retícula* es un conjunto parcialmente ordenado en el que todo par de

Figura 2.1: Diagrama de Hasse de la retícula de subgrupos de \mathbb{Z}_6 .Figura 2.2: Diagrama de Hasse de la retícula de subgrupos de \mathbb{Z}_{12} .

2.1.2. Homomorfismos de \mathbb{Z}_n a \mathbb{Z}_m .

El objetivo de esta sección es encontrar todos los homomorfismos que existen entre dos grupos cíclicos finitos.

Lema 2.19. Sea $\phi : \mathbb{Z}_n \rightarrow \mathbb{Z}_m$ un homomorfismo. Entonces, existe $a \in \mathbb{Z}_m$ tal que $\phi(x) = ax$, para toda $x \in \mathbb{Z}_n$.

elementos tiene un único supremo (mínima cota superior) y un único ínfimo (máxima cota inferior). El Ejercicio 2.6 demuestra que $(\text{Sub}(G), \subseteq)$ es efectivamente una retícula.

Demostración. Definimos $a := \phi(1)$. Usando la propiedad de homomorfismos, vemos que, para toda $x \in \mathbb{Z}_n$,

$$\phi(x) = \phi\left(\underbrace{1 + 1 + \cdots + 1}_{x \text{ veces}}\right) = \underbrace{\phi(1) + \phi(1) + \cdots + \phi(1)}_{x \text{ veces}} = ax.$$

□

Observación 2.20. La demostración anterior de hecho establece que todo homomorfismo $\phi : \mathbb{Z}_n \rightarrow \mathbb{Z}_m$ está completamente determinado por $\phi(1)$.

Resulta natural preguntarse ahora si para cualquier $a \in \mathbb{Z}_m$ podemos definir un homomorfismo $\phi : \mathbb{Z}_n \rightarrow \mathbb{Z}_m$ por $\phi(x) = ax$, para toda $x \in \mathbb{Z}_n$. De entrada, podría parecer que no hay problema, pues ϕ satisface la propiedad de homomorfismos:

$$\phi(x_1 + x_2) = a(x_1 + x_2) = ax_1 + ax_2 = \phi(x_1) + \phi(x_2), \quad \forall x_1, x_2 \in \mathbb{Z}_n.$$

Sin embargo, el problema es que estas propuestas algunas veces no están bien definidas, como lo muestra el siguiente ejemplo.

Ejemplo 2.21. Definimos a $\phi : \mathbb{Z}_4 \rightarrow \mathbb{Z}_6$ como $\phi(x) = 2x$, para toda $x \in \mathbb{Z}_4$. Para que ϕ sea una función bien definida, debe cumplir que si $x = y \pmod{4}$ entonces $\phi(x) = \phi(y) \pmod{6}$. Sin embargo, $0 = 4 \pmod{4}$ pero $\phi(0) = 0 \neq \phi(4) = 8 \pmod{6}$. Por lo tanto, ϕ no es una función bien definida.

Lema 2.22. Sea $a \in \mathbb{Z}_m$ y consideremos a $\phi : \mathbb{Z}_n \rightarrow \mathbb{Z}_m$ dada por $\phi(x) = ax$, para toda $x \in \mathbb{Z}_n$. Entonces, ϕ es una función bien definida si y solo si a es un múltiplo de $\frac{m}{\text{mcd}(n,m)}$.

Demostración.

(\Rightarrow) Supongamos que ϕ es una función bien definida. Como $0 = n \pmod{n}$, debemos tener que $\phi(0) = \phi(n) \pmod{m}$, es decir $0 = an \pmod{m}$. Esto implica que $m \mid an$, por lo que existe $t \in \mathbb{Z}$ tal que $an = tm$. Dividiendo de ambos lados por $\text{mcd}(n,m)$, obtenemos

$$a \frac{n}{\text{mcd}(n,m)} = t \frac{m}{\text{mcd}(n,m)}.$$

Como $\frac{n}{\text{mcd}(n,m)}$ y $\frac{m}{\text{mcd}(n,m)}$ son primos relativos (pues estamos cancelando todos los divisores comunes), podemos concluir que $\frac{m}{\text{mcd}(n,m)} \mid a$.

(\Leftarrow) Si a es múltiplo de $\frac{m}{\text{mcd}(n,m)}$, existe $t \in \mathbb{Z}$ tal que $a = \frac{m}{\text{mcd}(n,m)}t$. Para demostrar que ϕ es una función bien definida, supongamos que $x = y$

mód (n) . Entonces existe $r \in \mathbb{Z}$ tal que $x = y + rn$. Multiplicando por a , obtenemos

$$\begin{aligned} ax = ay + arn &\Rightarrow ax = ay + \left(\frac{m}{\text{mcd}(n, m)}\right) trn \\ &\Rightarrow ax = ay + \left(\frac{n}{\text{mcd}(n, m)}\right) trm \\ &\Rightarrow ax = ay \pmod{m}. \end{aligned}$$

Por lo tanto, $\phi(x) = \phi(y) \pmod{m}$.

□

Teorema 2.23 (homomorfismos entre grupos cíclicos finitos). Sean $n, m \in \mathbb{Z}_+$. El número de homomorfismos de \mathbb{Z}_n a \mathbb{Z}_m es exactamente $d := \text{mcd}(n, m)$. Explícitamente, estos homomorfismos están dados por

$$\phi_a(x) = ax, \quad \forall x \in \mathbb{Z}_n, \quad \text{donde } a \in \left\{0, \frac{m}{d}, \frac{2m}{d}, \dots, \frac{(d-1)m}{d}\right\}.$$

Demostación. Por el Lema 2.19, sabemos que todos los homomorfismos de \mathbb{Z}_n a \mathbb{Z}_m tienen la forma $\phi_a(x) = ax, \forall x \in \mathbb{Z}_n$, para algún $a \in \mathbb{Z}_m$. Por el Lema 2.22, deducimos que ϕ_a es un homomorfismo bien definido si y solo si a es un múltiplo de $\frac{m}{d}$. El teorema queda demostrado observando que los elementos de \mathbb{Z}_m que son múltiplos de $\frac{m}{d}$ son precisamente $0, \frac{m}{d}, \frac{2m}{d}, \dots, \frac{(d-1)m}{d}$. □

Ejemplo 2.24. Existen exactamente $2 = \text{mcd}(4, 6)$ homomorfismos de \mathbb{Z}_4 a \mathbb{Z}_6 los cuales están dados por

$$\begin{aligned} \phi_0(x) &= 0, \quad \forall x \in \mathbb{Z}_4, \\ \phi_3(x) &= 3x, \quad \forall x \in \mathbb{Z}_4. \end{aligned}$$

Observación 2.25. Si $n = m$, el teorema anterior implica que existen $n = \text{mcd}(n, n)$ homomorfismos de \mathbb{Z}_n a \mathbb{Z}_n ; es decir, para todo $a \in \mathbb{Z}_n$, tenemos un homomorfismo $\phi_a : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ dado por $\phi_a(x) = ax, \forall x \in \mathbb{Z}_n$. En esta situación resulta relevante preguntarnos cuáles de estos homomorfismos son automorfismos (es decir, cuáles son biyectivos).

Teorema 2.26 (automorfismos de \mathbb{Z}_n). El homomorfismo $\phi_a : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ dado por $\phi_a(x) = ax, \forall x \in \mathbb{Z}_n$ es un automorfismo si y solo si $\text{mcd}(n, a) = 1$. Además,

$$\text{Aut}(\mathbb{Z}_n) \cong U(n).$$

Demostación. Primero hay que verificar que la función ϕ_a es sobreyectiva si y solo si a es un generador de \mathbb{Z}_n , lo cual sabemos que se cumple si y solo si $\text{mcd}(n, a) = 1$. Dado que \mathbb{Z}_n es un conjunto finito, toda función sobreyectiva de \mathbb{Z}_n en \mathbb{Z}_n debe ser inyectiva (ver la Observación 2.44). Luego, hay que verificar

que la función $\Phi : \text{Aut}(\mathbb{Z}_n) \rightarrow U(n)$, dada por $\Phi(\phi_a) = a \in U(n)$, $\forall \phi_a \in \text{Aut}(\mathbb{Z}_n)$, es un isomorfismo. Se deja como ejercicio completar todos los detalles de esta demostración (Ejercicio 2.10). \square

Palabras clave: *criterio para igualdad de potencias, clases de isomorfía de grupos cíclicos, orden de potencias, teorema fundamental de grupos cíclicos, retícula de subgrupos, homomorfismos entre grupos cíclicos.*

2.1.3. Ejercicios

Ejercicio 2.1. Encuentra todos los generadores de cada uno de los siguientes grupos: \mathbb{Z}_8 , \mathbb{Z}_{20} y \mathbb{Z} .

Ejercicio 2.2. Encuentra un generador para cada subgrupo de \mathbb{Z}_{42} y dibuja el diagrama de Hasse de su retícula de subgrupos. ¿Cuáles de estos subgrupos son normales?

Ejercicio 2.3. Sea G un grupo de orden 24 y $a \in G$. Si $a^8 \neq e$ y $a^{12} \neq e$, demuestra que $G = \langle a \rangle$.

Ejercicio 2.4. Sea G un grupo y $a \in G$ tal que $|a| = 15$. Encuentra los órdenes de los siguientes elementos: a^3 , a^9 , a^{10} y a^{14} .

Ejercicio 2.5. Sea G un grupo finito (no necesariamente cíclico) de orden n . Para cualquier $k \mid n$, demuestra que el número de elementos de G de orden k es un múltiplo de $\varphi(k)$.

Ejercicio 2.6 (supremo e ínfimo). Si (P, \leq) es un conjunto parcialmente ordenado y $a, b \in P$, el *supremo* de a y b , denotado por $\sup(a, b)$, es la mínima cota superior del conjunto $\{a, b\}$, mientras que el *ínfimo* de a y b , denotado por $\inf(a, b)$, es la máxima cota inferior del conjunto $\{a, b\}$. En el conjunto parcialmente ordenado $(\text{Sub}(G), \subseteq)$, donde G es cualquier grupo, demuestra que todo par de elementos tiene un único supremo y un único ínfimo.

Ejercicio 2.7. Encuentra todos los homomorfismos de \mathbb{Z}_{10} a \mathbb{Z}_{10} . Encuentra todos los automorfismos de \mathbb{Z}_{10} .

Ejercicio 2.8. Encuentra todos los homomorfismos de \mathbb{Z}_{10} a \mathbb{Z}_{20} .

Ejercicio 2.9 (homomorfismos con grupos cíclicos infinitos). Sea $n \in \mathbb{Z}_+$. Encuentra lo siguiente:

1. Todos los homomorfismos de \mathbb{Z}_n a \mathbb{Z} .
2. Todos los homomorfismos de \mathbb{Z} a \mathbb{Z}_n .
3. Todos los homomorfismos de \mathbb{Z} a \mathbb{Z} .

Ejercicio 2.10 (automorfismos de \mathbb{Z}_n). Demuestra que el homomorfismo $\phi_a : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ dado por $\phi_a(x) = ax, \forall x \in \mathbb{Z}_n$ es un automorfismo si y solo si $\text{mcd}(n, a) = 1$. Además, demuestra que

$$\text{Aut}(\mathbb{Z}_n) \cong U(n).$$

(Sugerencia: sigue los pasos descritos en la demostración del Teorema 2.26).

Ejercicio 2.11 (grupo de homomorfismos). Sea $\text{Hom}(\mathbb{Z}_n, \mathbb{Z}_m)$ el conjunto de todos los homomorfismos de \mathbb{Z}_n a \mathbb{Z}_m . Definimos la *suma de homomorfismos* de la siguiente manera: dados $\phi_1, \phi_2 \in \text{Hom}(\mathbb{Z}_n, \mathbb{Z}_m)$, $\phi_1 + \phi_2$ es la función definida como $(\phi_1 + \phi_2)(x) = \phi_1(x) + \phi_2(x), \forall x \in \mathbb{Z}_n$. Demuestra que $\text{Hom}(\mathbb{Z}_n, \mathbb{Z}_m)$, equipado con la suma de homomorfismos, es un grupo isomorfo a \mathbb{Z}_d , con $d = \text{mcd}(n, m)$.

2.2. Grupos abelianos

2.2.1. Sumas directas

Para estudiar grupos abelianos es importante que estudiemos más a fondo el concepto de suma directa de grupos.

Recordemos que la suma directa de dos grupos G_1 y G_2 es el grupo

$$G_1 \oplus G_2 := \{(g_1, g_2) : g_1 \in G_1, g_2 \in G_2\},$$

con operación

$$(g_1, g_2)(h_1, h_2) = (g_1 h_1, g_2 h_2), \quad \forall g_i, h_i \in G_i.$$

La suma directa de dos grupos puede generalizarse de manera natural a la suma directa de una familia finita de grupos G_1, G_2, \dots, G_t :

$$G_1 \oplus G_2 \oplus \dots \oplus G_t = \{(g_1, g_2, \dots, g_t) : g_i \in G_i\},$$

con operación

$$(g_1, g_2, \dots, g_t)(h_1, h_2, \dots, h_t) = (g_1 h_1, g_2 h_2, \dots, g_t h_t), \quad \forall g_i, h_i \in G_i.$$

Observación 2.27. A las sumas directas de familias finitas de grupos también se les llama *producto directo*, y algunos libros usan el símbolo \times en lugar de \oplus . El significado de producto directo y suma directa solo difiere cuando consideramos una familia infinita de grupos $\{G_i : i \in I\}$. En este caso:

$$\prod_{i \in I} G_i = \{(g_i : i \in I) : g_i \in G_i\}$$

$$\bigoplus_{i \in I} G_i = \{(g_i : i \in I) : g_i \in G_i \text{ y } g_j \neq e_j \text{ solo para un número finito de } j\text{'s}\}.$$

Para tener como referencia, si $I = \mathbb{N}$, entonces $\prod_{i \in I} G_i$ es análogo al conjunto de series de potencia formales $\sum_{i=1}^{\infty} a_i x^i$ (las cuales pueden tener un número infinito de términos no nulos), mientras que $\bigoplus_{i \in I} G_i$ es análogo al conjunto de polinomios $\sum_{i=1}^n a_i x^i$ (los cuales solo tienen un número finito de términos no nulos, pero su grado puede ser arbitrariamente grande). De cualquier forma, en el resto de este capítulo solo trabajaremos con sumas directas de familias finitas de grupos, las cuales son equivalentes a los productos directos en este caso.

Lema 2.28 (propiedades de la suma directa). Sean G , H y K grupos.

1. $|G \oplus H| = |G||H|$.
2. $G \oplus H \cong H \oplus G$.
3. $(G \oplus H) \oplus K \cong G \oplus (H \oplus K)$.
4. Si $G \cong H$, entonces $G \oplus K \cong H \oplus K$.

Demostación.

1. $G \oplus H$ consiste en pares (g, h) tales que $g \in G$ y $h \in H$, así que, como conjunto, $G \oplus H$ es igual a producto cartesiano $G \times H$. Sabemos que $|G \oplus H| = |G \times H| = |G||H|$.
2. Ejercicio 2.12.
3. Consideremos la función $\phi : (G \oplus H) \oplus K \rightarrow G \oplus (H \oplus K)$ definida por

$$\phi((g, h), k) := (g, (h, k)), \quad \forall g \in G, h \in H, k \in K.$$

Es sencillo verificar que ϕ es un isomorfismo.

4. Sea $\phi : G \rightarrow H$ un isomorfismo, y consideremos la función $\psi : G \oplus K \rightarrow H \oplus K$ definida por

$$\psi(g, k) := (\phi(g), k), \quad \forall g \in G, k \in K.$$

Observemos que

$$\psi(g_1, k_1) = \psi(g_2, k_2) \Rightarrow (\phi(g_1), k_1) = (\phi(g_2), k_2).$$

Entonces, $\phi(g_1) = \phi(g_2)$ y $k_1 = k_2$. Como ϕ es inyectiva, $g_1 = g_2$, por lo que $(g_1, k_1) = (g_2, k_2)$. Luego, ψ es inyectiva.

Si $(h, k) \in H \oplus K$, es un elemento arbitrario, su preimagen bajo ψ es $(\phi^{-1}(h), k) \in G \oplus K$. Luego, ψ es sobreyectiva.

Finalmente,

$$\begin{aligned} \psi((g_1, k_1)(g_2, k_2)) &= \psi(g_1g_2, k_1k_2) \\ &= (\phi(g_1g_2), k_1k_2) \\ &= (\phi(g_1)\phi(g_2), k_1k_2) \\ &= (\phi(g_1), k_1)(\phi(g_2), k_2) \\ &= \psi(g_1, k_1)\psi(g_2, k_2). \end{aligned}$$

Por lo tanto, ψ es un isomorfismo. □

Lema 2.29 (orden de un elemento en la suma directa). Sean G_1, G_2, \dots, G_t grupos y $(g_1, g_2, \dots, g_t) \in G_1 \oplus G_2 \oplus \dots \oplus G_t$. Entonces,

$$|(g_1, g_2, \dots, g_t)| = \text{mcm}(|g_1|, |g_2|, \dots, |g_t|).$$

Demostación. Sea $m = \text{mcm}(|g_1|, |g_2|, \dots, |g_t|)$ y $r = |(g_1, g_2, \dots, g_t)|$. Debido a que $|g_i| \mid m$, tenemos que

$$(g_1, g_2, \dots, g_t)^m = ((g_1)^m, (g_2)^m, \dots, (g_t)^m) = (e_1, e_2, \dots, e_t),$$

donde e_i es la identidad de G_i . Por el Lema 1.25, $r \mid m$. Por otro lado, por definición de r ,

$$(e_1, e_2, \dots, e_t) = (g_1, g_2, \dots, g_t)^r = ((g_1)^r, (g_2)^r, \dots, (g_t)^r),$$

así que $(g_i)^r = e_i$ para toda i . De nuevo por el Lema 1.25, $|g_i| \mid r$, para toda i . Al ser m el mínimo común múltiplo de los $|g_i|$, tenemos que $m \mid r$. Por lo tanto, $r = m$. \square

Ejemplo 2.30. Consideremos el grupo $G = \mathbb{Z}_2 \oplus \mathbb{Z}_3$. Por el lema anterior, $|(1, 1)| = \text{mcm}(|1|, |1|) = \text{mcm}(2, 3) = 6$. Podemos verificar esto:

$$\begin{aligned} 1 \cdot (1, 1) &= (1, 1) \\ 2 \cdot (1, 1) &= (1, 1) + (1, 1) = (0, 2) \\ 3 \cdot (1, 1) &= (1, 1) + (1, 1) + (1, 1) = (1, 0) \\ 4 \cdot (1, 1) &= (1, 1) + (1, 1) + (1, 1) + (1, 1) = (0, 1) \\ 5 \cdot (1, 1) &= (1, 1) + (1, 1) + (1, 1) + (1, 1) + (1, 1) = (1, 2) \\ 6 \cdot (1, 1) &= (1, 1) + (1, 1) + (1, 1) + (1, 1) + (1, 1) + (1, 1) = (0, 0). \end{aligned}$$

Teorema 2.31 (descomposición del grupo $U(st)$). Sean $s, t \in \mathbb{Z}_+$ tales que $\text{mcd}(s, t) = 1$. Entonces,

$$U(st) \cong U(s) \oplus U(t).$$

Demostración. Definimos una función $\phi : U(st) \rightarrow U(s) \oplus U(t)$ por

$$\phi([x]_{st}) = ([x]_s, [x]_t),$$

donde $[x]_{st}$, $[x]_s$ y $[x]_t$ representan la clase de equivalencia de x módulo st , s y t , respectivamente. Es sencillo verificar que ϕ es un isomorfismo bien definido (Ejercicio 2.14). \square

2.2.2. Teorema fundamental de grupos abelianos finitos

Recordemos que todo grupo cíclico es abeliano, pues para toda $g^k, g^s \in G = \langle g \rangle$, tenemos que $g^k g^s = g^{k+s} = g^{s+k} = g^s g^k$. La suma directa de grupos abelianos es un grupo abeliano (ver Ejercicio 2.13), así que en particular, la suma directa de grupos cíclicos es un grupo abeliano. Resulta que todo grupo abeliano finito puede descomponerse como una suma directa de grupos cíclicos.

El objetivo de esta sección es entender y aplicar el siguiente teorema:

Teorema 2.32 (teorema fundamental de grupos abelianos finitos). Sea G un grupo abeliano finito. Entonces,

1. **Descomposición primaria:** Existen potencias de primos $q_i := p_i^{m_i}$, para $i = 1, 2, \dots, t$, donde los primos p_i no son necesariamente distintos entre sí, tales que

$$G \cong \mathbb{Z}_{q_1} \oplus \mathbb{Z}_{q_2} \oplus \dots \oplus \mathbb{Z}_{q_t}.$$

Las potencias de primos q_1, q_2, \dots, q_t se llaman los *divisores elementales* de G .

2. **Descomposición en factores invariantes:** Existen enteros positivos k_1, k_2, \dots, k_r , donde $k_r \mid k_{r-1} \mid \dots \mid k_2 \mid k_1$, tales que

$$G \cong \mathbb{Z}_{k_1} \oplus \mathbb{Z}_{k_2} \oplus \dots \oplus \mathbb{Z}_{k_r}.$$

Los enteros k_1, k_2, \dots, k_r se llaman los *factores invariantes* de G .

Corolario 2.33. Todo grupo abeliano finito es isomorfo a un producto directo de grupos cíclicos.

Observación 2.34. Sea G un grupo abeliano finito de orden n . Si q_1, q_2, \dots, q_t son los divisores elementales de G , entonces $\prod_{i=1}^t q_i = n$, puesto que

$$\prod_{i=1}^t q_i = |\mathbb{Z}_{q_1} \oplus \mathbb{Z}_{q_2} \oplus \dots \oplus \mathbb{Z}_{q_t}| = |G| = n.$$

Similarmente, si k_1, k_2, \dots, k_r son los factores invariantes de G , entonces $\prod_{i=1}^r k_i = n$, puesto que

$$\prod_{i=1}^r k_i = |\mathbb{Z}_{k_1} \oplus \mathbb{Z}_{k_2} \oplus \dots \oplus \mathbb{Z}_{k_r}| = |G| = n.$$

No demostraremos el Teorema 2.32 por ahora, pero lo ejemplificaremos y lo aplicaremos para obtener las clases de isomorfía de todos los grupos abelianos de orden n . En particular, el Teorema 2.32 implica que las clases de isomorfía de grupos abelianos siempre tienen un representante que es una suma directa de grupos cíclicos.

Ejemplo 2.35 (grupos abelianos de orden p). Recordemos que si G es un grupo de orden p , donde p es un número primo, entonces G debe ser un grupo cíclico. Por lo tanto, $G \cong \mathbb{Z}_p$, lo que quiere decir que \mathbb{Z}_p determina a la única clase de isomorfía de grupos de orden p .

Ejemplo 2.36 (grupos abelianos de orden 4). Sea G un grupo abeliano de orden 4. Por el Teorema Fundamental de Grupos Abelianos Finitos, G debe ser isomorfo a la suma directa de grupos cíclicos, es decir

$$G \cong \mathbb{Z}_4 \quad \text{o} \quad G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2.$$

- Si $G \cong \mathbb{Z}_4$, entonces G tiene un único divisor elemental $q_1 = 2^2 = 4$ y un único factor invariante $k_1 = 4$.
- Si $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$, entonces G tiene divisores elementales $q_1 = 2$ y $q_2 = 2$ y factores invariantes $k_1 = 2$ y $k_2 = 2$.

Como $\mathbb{Z}_4 \not\cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ (ya que en el primero existe un elemento de orden 4 mientras que en el segundo todos sus elementos distintos de la identidad tienen orden 2), concluimos que existen exactamente 2 clases de isomorfía de grupos abelianos de orden 4.

El siguiente lema es un criterio muy importante para determinar cuándo dos grupos abelianos son isomorfos.

Lema 2.37 (criterio de isomorfía para sumas directas de grupos cíclicos).

Sean $s, t \in \mathbb{Z}_+$.

$$\mathbb{Z}_s \oplus \mathbb{Z}_t \cong \mathbb{Z}_{st} \iff \text{mcd}(s, t) = 1.$$

Demostración. Esta demostración se simplifica bastante considerando el siguiente hecho:

$$\text{mcd}(s, t) = 1 \iff \text{mcm}(s, t) = st.$$

(\Rightarrow) Usando la contrapuesta, supongamos que $\text{mcd}(s, t) > 1$. Entonces, $\text{mcm}(s, t) < st$. Observemos que $|a| \leq s$ y $|b| \leq t$ para toda $a \in \mathbb{Z}_s$ y $b \in \mathbb{Z}_t$. Por el Lema 2.29,

$$|(a, b)| = \text{mcm}(|a|, |b|) \leq \text{mcm}(s, t) < st,$$

para todo $(a, b) \in \mathbb{Z}_s \oplus \mathbb{Z}_t$. Por lo tanto, no hay ningún elemento en $\mathbb{Z}_s \oplus \mathbb{Z}_t$ de orden st , lo que implica que no es cíclico. Luego $\mathbb{Z}_s \oplus \mathbb{Z}_t \not\cong \mathbb{Z}_{st}$.

(\Leftarrow) Supongamos que $\text{mcd}(s, t) = 1$, por lo que $\text{mcm}(s, t) = st$. Aplicando el Lema 2.29 al elemento $(1, 1) \in \mathbb{Z}_s \oplus \mathbb{Z}_t$,

$$|(1, 1)| = \text{mcm}(|1|, |1|) = \text{mcm}(s, t) = st.$$

Por lo tanto, $\mathbb{Z}_s \oplus \mathbb{Z}_t = \langle (1, 1) \rangle$ es cíclico. Puesto que $|\mathbb{Z}_s \oplus \mathbb{Z}_t| = st$, el Teorema 2.3 implica que $\mathbb{Z}_s \oplus \mathbb{Z}_t \cong \mathbb{Z}_{st}$.

□

	Descomposición primaria	Desc. factores invariantes
Clase de isomorfía 1	$\mathbb{Z}_4 \oplus \mathbb{Z}_9$	\mathbb{Z}_{36}
Clase de isomorfía 2	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9$	$\mathbb{Z}_{18} \oplus \mathbb{Z}_2$
Clase de isomorfía 3	$\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$	$\mathbb{Z}_{12} \oplus \mathbb{Z}_3$
Clase de isomorfía 4	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$	$\mathbb{Z}_6 \oplus \mathbb{Z}_6$

Cuadro 2.1: Clases de isomorfía de grupos abelianos de orden 36.

Ejemplo 2.38 (grupos abelianos de orden 36). Hay 4 clases de isomorfía de grupos abelianos de orden 36. Representantes de estas clases de isomorfía están dados por la Tabla 2.1. Usando el Lema 2.37, es fácil verificar que la descomposición primaria es isomorfa a la descomposición en factores invariantes de un mismo renglón, por ejemplo $\mathbb{Z}_4 \oplus \mathbb{Z}_9 \cong \mathbb{Z}_{36}$ porque $\text{mcd}(4, 9) = 1$. Similarmente, podemos verificar que descomposiciones de distintos renglones no son isomorfas, por ejemplo $\mathbb{Z}_{18} \oplus \mathbb{Z}_2 \not\cong \mathbb{Z}_{36}$ porque $\text{mcd}(18, 2) = 2$.

Definición 2.39 (partición de un número). Sea $k \in \mathbb{Z}_+$. Una *partición* de k es un conjunto de números positivos $\{m_1, m_2, \dots, m_\ell\}$ tal que

$$k = m_1 + m_2 + \dots + m_\ell$$

Ejemplo 2.40 (grupos abelianos de orden p^k). Sea p un número primo y $k \in \mathbb{Z}_+$. El Teorema Fundamental de Grupos Abelianos Finitos implica que hay una biyección entre las clases de isomorfía de grupos abelianos de orden p^k y particiones de k . En particular, dada una partición $k = m_1 + m_2 + \dots + m_\ell$ tenemos la clase de isomorfía

$$\mathbb{Z}_{p^{m_1}} \oplus \mathbb{Z}_{p^{m_2}} \oplus \dots \oplus \mathbb{Z}_{p^{m_\ell}}.$$

Si ordenamos la partición $m_1 > m_2 > \dots > m_\ell$, entonces en estos casos la descomposición primaria coincide con la descomposición en factores invariantes.

Orden de G	Particiones de k	Clases de isomorfía
p	1	\mathbb{Z}_p
p^2	2	\mathbb{Z}_{p^2}
	1 + 1	$\mathbb{Z}_p \oplus \mathbb{Z}_p$
p^3	3	\mathbb{Z}_{p^3}
	2 + 1	$\mathbb{Z}_{p^2} \oplus \mathbb{Z}_p$
	1 + 1 + 1	$\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$
p^4	4	\mathbb{Z}_{p^4}
	3 + 1	$\mathbb{Z}_{p^3} \oplus \mathbb{Z}_p$
	2 + 2	$\mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}$
	2 + 1 + 1	$\mathbb{Z}_{p^2} \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$
	1 + 1 + 1 + 1	$\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$

Cuadro 2.2: Clases de isomorfía de grupos abelianos G de orden p^k

Ejemplo 2.41. Consideremos el grupo abeliano

$$G = \mathbb{Z}_6 \oplus \mathbb{Z}_{20} \oplus \mathbb{Z}_{36}.$$

Encontraremos las dos descomposiciones de G establecidas en el Teorema 2.32.

1. **Descomposición primaria:** Debemos encontrar potencias de primos (los divisores elementales de G) tales que G se descomponga como la suma

directa de grupos cíclicos de cuyos órdenes son esas potencias de primos. Por el lema anterior,

$$\mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3, \quad \mathbb{Z}_{20} \cong \mathbb{Z}_{2^2} \oplus \mathbb{Z}_5, \quad \mathbb{Z}_{36} \cong \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{3^2}.$$

Por lo tanto,

$$\begin{aligned} G &\cong (\mathbb{Z}_2 \oplus \mathbb{Z}_3) \oplus (\mathbb{Z}_{2^2} \oplus \mathbb{Z}_5) \oplus (\mathbb{Z}_{2^2} \oplus \mathbb{Z}_{3^2}), \\ &\cong \mathbb{Z}_2 \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{3^2} \oplus \mathbb{Z}_5. \end{aligned}$$

Por lo tanto, los divisores elementales de G son 2 , 2^2 , 2^2 , 3 , 3^2 y 5 .

2. **Descomposición en factores invariantes:** Para encontrar esta descomposición podemos usar la descomposición primaria de G encontrada en el punto anterior. El primer factor invariante será el producto de los divisores elementales más grandes que sean potencias de primos distintos, es decir $k_1 = 2^2 3^2 5 = 180$. Los divisores elementales que sobran son 2 , 2^2 y 3 , así que el segundo factor invariante será el producto de estos divisores elementales que sean más grandes y potencias de primos distintos; es decir, $k_2 = 2^2 3 = 12$. Finalmente, solo queda el divisor elemental 2 , así que $k_3 = 2$. Por lo tanto, la descomposición de G en factores invariantes es

$$G \cong \mathbb{Z}_{180} \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_2,$$

donde $2 \mid 12 \mid 180$.

Palabras clave: *suma directa, teorema fundamental de grupos abelianos finitos, criterio de isomorfía para sumas directas de grupos cíclicos.*

2.2.3. Ejercicios

Ejercicio 2.12. Sean G y H grupos. Demuestra que $G \oplus H \cong H \oplus G$.

Ejercicio 2.13. Sean G_1, G_2, \dots, G_t grupos abelianos. Demuestra que $G_1 \oplus G_2 \oplus \dots \oplus G_t$ es un grupo abeliano.

Ejercicio 2.14. Sean $s, t \in \mathbb{Z}_+$ tales que $\text{mcd}(s, t) = 1$. Demuestra que la función $\phi : U(st) \rightarrow U(s) \oplus U(t)$ dada por

$$\phi([x]_{st}) = ([x]_s, [x]_t),$$

es un isomorfismo bien definido.

Ejercicio 2.15. ¿Cuál es el menor entero positivo n tal que existen tres grupos abelianos de orden n no isomorfos? ¿Cuáles son estos grupos?

Ejercicio 2.16. Encuentra todos los grupos abelianos, salvo isomorfismos, de orden 360.

Ejercicio 2.17. Encuentra, salvo isomorfismo, todos los grupos abelianos de orden 200. Para cada uno de ellos, escribe tanto la descomposición primaria como la descomposición en factores invariantes.

Ejercicio 2.18. Demuestra que existen dos grupos abelianos no isomorfos de orden 108 que tienen exactamente un subgrupo de orden 3.

Ejercicio 2.19. Sean p_1, p_2, \dots, p_k números primos distintos. ¿Cuántos grupos abelianos hay, salvo isomorfismos, de orden $p_1 \times p_2 \times \dots \times p_k$?

Ejercicio 2.20. Para cualquier $k \in \mathbb{Z}_+$, definimos por $\text{par}(k)$ al número de particiones de k . Por ejemplo, $\text{par}(3) = 3$ y $\text{par}(4) = 5$. Demuestra que el número de clases de isomorfía de grupos abelianos de orden $n \in \mathbb{Z}_+$ es

$$\text{par}(k_1) \cdot \text{par}(k_2) \cdot \dots \cdot \text{par}(k_r),$$

donde $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ es la factorización de n en primos distintos.

Ejercicio 2.21 (★). Supongamos que G es un grupo abeliano finito que tiene exactamente un subgrupo para cada divisor de $|G|$. Demuestra que G debe ser cíclico.

2.3. Grupos de permutaciones

2.3.1. Grupo simétrico

Definición 2.42 (permutación). Una *permutación* de un conjunto A es simplemente una función biyectiva $\alpha : A \rightarrow A$.

En esta sección estudiaremos permutaciones de conjuntos finitos. Sin pérdida de generalidad, podemos asumir siempre que nuestro conjunto finito es

$$[n] := \{1, 2, \dots, n\}, \quad \text{con } n \in \mathbb{Z}_+.$$

A diferencia de las funciones con dominios infinitos, una función $\alpha : [n] \rightarrow [n]$ puede representarse mediante una lista, pues está totalmente determinada por las imágenes de $1, 2, \dots, n$.

De esta forma, dada cualquier permutación $\alpha : [n] \rightarrow [n]$, podemos representarla mediante la *notación en dos líneas* como

$$\alpha = \begin{pmatrix} 1 & 2 & \dots & n \\ \alpha(1) & \alpha(2) & \dots & \alpha(n) \end{pmatrix},$$

o mediante la *notación en una línea* como

$$\alpha = \alpha(1)\alpha(2)\dots\alpha(n).$$

Ejemplo 2.43. Sea $n = 4$ y consideremos la permutación $\alpha : [4] \rightarrow [4]$ definida por

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}.$$

En notación en una línea esta permutación es $\alpha = 3412$.

Observación 2.44. Una función $\alpha : [n] \rightarrow [n]$ es inyectiva si y solo si los elementos de la lista $\alpha(1)\alpha(2)\dots\alpha(n)$ son todos distintos entre sí. Además, es equivalente que todos los elementos de la lista sean distintos entre sí a que todos los números $1, 2, \dots, n$ aparezcan en la lista. Esto demuestra que una función $\alpha : [n] \rightarrow [n]$ es inyectiva si y solo si es sobreyectiva.

Definición 2.45 (punto fijo). Un elemento $i \in [n]$ es un *punto fijo* de una permutación $\alpha : [n] \rightarrow [n]$ si $\alpha(i) = i$. Denotamos al conjunto de puntos fijos de α como

$$\text{fix}(\alpha) := \{i \in [n] : \alpha(i) = i\}.$$

Definición 2.46 (soporte). El *soporte* de una permutación $\alpha : [n] \rightarrow [n]$ es el conjunto

$$\text{supp}(\alpha) := \{i \in [n] : \alpha(i) \neq i\}.$$

Observación 2.47. Para cualquier permutación $\alpha : [n] \rightarrow [n]$,

$$\text{supp}(\alpha) = [n] - \text{fix}(\alpha).$$

Ejemplo 2.48. Consideremos $\alpha : [5] \rightarrow [5]$ definida por

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix}.$$

Entonces, $\text{fix}(\alpha) = \{3\}$ y $\text{supp}(\alpha) = \{1, 2, 4, 5\}$.

Teorema 2.49 (grupo simétrico). Sea $n \in \mathbb{Z}_+$. El conjunto de todas las permutaciones de $[n]$,

$$S_n := \{\alpha : [n] \rightarrow [n] \mid \alpha \text{ es biyectiva}\},$$

equipado con la composición de funciones, es un grupo.

Demostración.

- (G0) Si $\alpha, \beta \in S_n$, entonces $\alpha \circ \beta \in S_n$ ya que la composición de funciones biyectivas es biyectiva.
- (G1) La composición de funciones siempre es una operación asociativa.
- (G2) La función identidad $\text{id} : [n] \rightarrow [n]$ es biyectiva, así que $\text{id} \in S_n$.
- (G3) Todas las funciones biyectivas tiene una inversa: si $\alpha \in S_n$, entonces $\alpha^{-1} \in S_n$.

□

Definición 2.50 (grupo simétrico). Al grupo S_n lo llamamos el *grupo simétrico de grado n* .

Notación 2.51. Denotaremos la composición de dos permutaciones $\alpha, \beta \in S_n$ simplemente como $\alpha\beta$ en lugar de $\alpha \circ \beta$. Además, nos referimos a $\alpha\beta$ como el *producto* de permutaciones, a pesar de que estrictamente se trate de la composición.

Ejemplo 2.52. El grupo simétrico S_3 tiene 6 elementos; explícitamente,

$$S_3 = \{\beta_1, \beta_2, \beta_3, \beta_4, \beta_5, \beta_6\},$$

donde los β_i 's están definidos en la Tabla 2.3.

Observación 2.53. La cardinalidad de S_n es

$$|S_n| = n! := n \cdot (n-1) \cdots \cdots 2 \cdot 1.$$

Es fácil comprobar esto ya que los elementos de S_n pueden verse como listas de elementos no repetidos de $[n]$. Así pues, hay n posibilidades para la primera entrada de la lista, $n-1$ posibilidades para la segunda entrada, y así sucesivamente hasta llegar a tener solo 1 posibilidad para la n -ésima entrada. El principio del producto de combinatoria nos permite concluir que hay precisamente $n!$ listas con elementos no repetidos de $[n]$.

Permutación	Not. en una línea	Permutación	Not. en una línea
$\beta_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$	123	$\beta_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$	132
$\beta_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$	213	$\beta_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$	231
$\beta_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$	321	$\beta_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$	312

Cuadro 2.3: Permutaciones de $\{1, 2, 3\}$.

$$\beta_2\beta_3 = \begin{pmatrix} 1 & 2 & \textcircled{3} \\ 2 & 1 & \textcircled{3} \end{pmatrix} \begin{pmatrix} \textcircled{1} & 2 & 3 \\ \textcircled{3} & 2 & 1 \end{pmatrix} = \begin{pmatrix} \boxed{1} & 2 & 3 \\ \boxed{3} & 1 & 2 \end{pmatrix} = \beta_6.$$

Figura 2.3: Composición de permutaciones.

Ejemplo 2.54. Para realizar la composición de permutaciones debemos rastrear a dónde son enviados cada uno de los elementos de $[n]$, iniciando de derecha a izquierda (ya que en ese orden se hace la composición de funciones). Por ejemplo, hacemos la composición de β_2 y β_3 en S_3 en la Figura 2.3.

Definición 2.55 (permutaciones disjuntas). Decimos que dos permutaciones $\alpha, \beta \in S_n$ son *disjuntas* si $\text{supp}(\alpha) \cap \text{supp}(\beta) = \emptyset$.

Ejemplo 2.56. Consideremos las permutaciones

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix} \quad \text{y} \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$$

Entonces α y β son permutaciones disjuntas, puesto que $\text{supp}(\alpha) = \{4, 5\}$ y $\text{supp}(\beta) = \{1, 2, 3\}$.

Lema 2.57 (permutaciones disjuntas conmutan). Si α y β son permutaciones disjuntas, entonces $\alpha\beta = \beta\alpha$.

Demostración. Hay que demostrar que $\alpha\beta(c) = \beta\alpha(c)$, para toda $c \in [n]$.

- **Caso 1:** $c \in \text{supp}(\alpha)$. Al ser permutaciones disjuntas, $c \notin \text{supp}(\beta)$ por lo que $c \in \text{fix}(\beta)$. Luego, $\alpha\beta(c) = \alpha(c)$. Por otro lado, $\alpha(c) \neq c$ implica que $\alpha(\alpha(c)) \neq \alpha(c)$, por lo que $\alpha(c) \in \text{supp}(\alpha)$ y $\alpha(c) \notin \text{supp}(\beta)$. Por lo tanto,

$$\beta\alpha(c) = \alpha(c) = \alpha\beta(c).$$

- **Caso 2:** $c \in \text{supp}(\beta)$. Este caso es análogo al anterior.
- **Caso 3:** $c \notin \text{supp}(\alpha)$ y $c \notin \text{supp}(\beta)$. Entonces, $c \in \text{fix}(\alpha)$ y $c \in \text{fix}(\beta)$ por lo que

$$\alpha\beta(c) = \alpha(c) = c = \beta(c) = \beta\alpha(c).$$

□

2.3.2. Notación cíclica

En esta sección presentaremos un tercer tipo de notación para permutaciones el cual es muy conveniente para deducir ciertas propiedades tales como el orden de la permutación.

Definición 2.58 (ciclo). Un *ciclo de longitud k* , o un *k -ciclo*, es una permutación $\alpha \in S_n$ tal que existen $a_1, a_2, \dots, a_k \in [n]$ que cumplen lo siguiente:

$$\begin{aligned} \alpha(a_i) &= a_{i+1}, & \forall i = 1, 2, \dots, k-1 \\ \alpha(a_k) &= a_1 \\ \alpha(b) &= b, & \forall b \in [n] - \{a_1, \dots, a_k\}. \end{aligned}$$

En tal caso, denotamos al k -ciclo como

$$\alpha = (a_1, a_2, \dots, a_k).$$

Es importante hacer énfasis en que todos los números que no aparecen en un k -ciclo quedan fijos al aplicar la permutación.

Si $\alpha = (a_1, a_2, \dots, a_k)$, en ocasiones es conveniente abusar de la notación y escribir

$$\alpha(a_i) = a_{i+1 \bmod k},$$

dado que $\alpha(a_i) = a_{i+1}$ para $i = 1, \dots, k-1$ y $\alpha(a_k) = a_1$.

Ejemplo 2.59. Con la notación del Ejemplo 2.52, los elementos de S_3 en notación cíclica son:

$$\begin{array}{lll} \beta_1 = (1) & \beta_2 = (1, 2) & \beta_3 = (1, 3) \\ \beta_4 = (2, 3) & \beta_5 = (1, 2, 3) & \beta_6 = (1, 3, 2) \end{array}$$

Ejemplo 2.60. Existen varias formas distintas de representar una misma permutación en notación cíclica. Por ejemplo, si $\alpha \in S_4$ está definida por

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

en notación cíclica tenemos

$$\alpha = (1, 2, 3, 4) = (2, 3, 4, 1) = (3, 4, 1, 2) = (4, 1, 2, 3).$$

En general, un mismo k -ciclo siempre puede escribirse de k formas distintas:

$$(a_1, a_2, \dots, a_k) = (a_2, a_3, \dots, a_k, a_1) = \dots = (a_k, a_1, a_2, \dots, a_{k-1}).$$

Además, la identidad de S_n puede escribirse en notación cíclica de n formas distintas, pues siempre es igual a cualquier 1-ciclo:

$$\text{id} = (1) = (2) = \dots = (n).$$

Ejemplo 2.61. No necesariamente toda permutación puede escribirse como un solo ciclo. Por ejemplo, si $\beta \in S_5$ está definida por

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 3 & 5 \end{pmatrix}$$

no podemos escribir a β como un solo ciclo. Sin embargo, podemos escribir a β como el producto de dos 2-ciclos y un 1-ciclo:

$$\beta = (1, 2)(3, 4)(5).$$

Dada la convención de que los números que no aparecen en un ciclo quedan fijos, siempre es posible omitir la escritura de los 1-ciclos:

$$\beta = (1, 2)(3, 4)(5) = (1, 2)(3, 4).$$

Ejemplo 2.62. Para obtener el producto (o composición) de permutaciones en notación cíclica debemos rastrear cada $i \in [n]$ en cada uno de los ciclos, siempre de derecha a izquierda (ya que este es el orden en el que se hace la composición de funciones). Por ejemplo, si $\alpha = (1, 2, 3, 5)(4, 6)$ y $\beta = (3, 2, 4)(1, 5, 6)$, podemos obtener que

$$\alpha\beta = (1, 2, 3, 5) \begin{matrix} \xrightarrow{\beta} \\ \text{---} \end{matrix} \begin{matrix} \text{---} \\ \xrightarrow{\alpha} \end{matrix} (4, 6)(3, 2, 4)(1, 5, 6) = (2, 6)(4, 5)$$

$$\beta\alpha = (3, 2, 4) \begin{matrix} \xrightarrow{\alpha} \\ \text{---} \end{matrix} \begin{matrix} \text{---} \\ \xrightarrow{\beta} \end{matrix} (1, 2, 3, 5)(4, 6) = (1, 4)(3, 6).$$

Teorema 2.63 (permutaciones como ciclos). Toda permutación en S_n se puede escribir como un producto de ciclos disjuntos.

Demostración. Sea $\alpha \in S_n$. Haremos la demostración por inducción sobre $s := |\text{supp}(\alpha)|$.

Caso base: Si $s = 0$, entonces $\alpha = \text{id}$, y puede escribirse como un 1-ciclo:
 $\alpha = (1)$.

Hipótesis de inducción: Supongamos que toda permutación $\beta \in S_n$ tal que $|\text{supp}(\beta)| < s$ puede escribirse como el producto de ciclos disjuntos.

Paso de inducción: Tomemos un $i \in \text{supp}(\alpha)$ arbitrario y consideremos el subconjunto I de $[n]$ definido por

$$I := \{\alpha^k(i) : k \in \mathbb{Z}\}$$

Como el conjunto $[n]$ es finito, I debe ser finito, por lo que debe haber repeticiones en los elementos descritos arriba. Si $\alpha^k(i) = \alpha^r(i)$, para algunos k, r , entonces $\alpha^{k-r}(i) = i$. Luego, sea m el menor entero no negativo tal que $\alpha^m(i) = i$. Esto nos permite describir a I como un conjunto finito con los siguientes elementos distintos:

$$I = \{i, \alpha(i), \alpha^2(i), \dots, \alpha^{m-1}(i)\}.$$

Definimos una permutación $\beta \in S_n$ como sigue: para toda $j \in [n]$,

$$\beta(j) := \begin{cases} j & \text{si } j \in I \\ \alpha(j) & \text{si } j \in [n] - I. \end{cases}$$

Afirmación: $\beta : [n] \rightarrow [n]$ es efectivamente una permutación.

Para demostrar esto verificamos que β es inyectiva y usamos la Observación 2.44. Si $\beta(j_1) = \beta(j_2)$, entonces o $j_1, j_2 \in I$ o $j_1, j_2 \in [n] - I$ (no es posible que $j_1 \in I$ y $j_2 \in [n] - I$, porque esto implica que $j_1 = \alpha(j_2)$ y $j_1 = \alpha^r(i)$ para algún r , por lo que $j_2 = \alpha^{r-1}(i) \in I$, lo cual es una contradicción). En el primer caso, tenemos directamente que $j_1 = j_2$ y en el segundo caso $\alpha(j_1) = \alpha(j_2)$ implica que $j_1 = j_2$. Por lo tanto, β es efectivamente una permutación.

Afirmación: $\alpha = (i, \alpha(i), \alpha^2(i), \dots, \alpha^{m-1}(i))\beta$.

Es sencillo verificar esto simplemente evaluando cada elemento de $[n]$ de ambos lados de la igualdad.

Afirmación: $|\text{supp}(\beta)| < |\text{supp}(\alpha)|$.

Observemos que β tiene más puntos fijos que α , porque todo punto fijo de α está fijo en β y al menos $i \in [n]$ es punto fijo de β que no es punto fijo de α (porque $i \in \text{supp}(\alpha)$). En otras palabras, el soporte de β está estrictamente contenido en el soporte de α .

Por hipótesis de inducción, β puede escribirse como un producto de ciclos disjuntos. Además, cada uno de los ciclos que aparecen en β son disjuntos con el ciclo $(i, \alpha(i), \alpha^2(i), \dots, \alpha^{m-1}(i))$ porque β fija todos los puntos de I . Por lo tanto, α puede escribirse como un producto de ciclos disjuntos.

□

Definición 2.64 (estructura cíclica). La *estructura cíclica* de $\alpha \in S_n$ es el multiconjunto² formado por las longitudes de los ciclos en la descomposición de α en ciclos disjuntos. En otras palabras, si

$$\alpha = (a_{1,1}, \dots, a_{1,k_1})(a_{2,1}, \dots, a_{2,k_2}) \dots (a_{r,1}, \dots, a_{r,k_r}),$$

²Esencialmente, un *multiconjunto* es una modificación del concepto de conjunto en el cual se permite la repetición de los elementos que pertenecen a él.

donde $a_{i,j} \neq a_{s,t}$ para toda $(i,j) \neq (s,t)$, la estructura cíclica de α es $\{k_1, k_2, \dots, k_r\}$.

El siguiente resultado se debe al matemático italiano Paolo Ruffini en 1799.

Teorema 2.65 (orden de una permutación). Sea $\alpha \in S_n$ una permutación con estructura cíclica $\{k_1, k_2, \dots, k_r\}$. Entonces,

$$|\alpha| = \text{mcm}(k_1, k_2, \dots, k_r).$$

Demostración. Consideremos la descomposición de α en ciclos disjuntos

$$\alpha = \alpha_1 \alpha_2 \dots \alpha_r,$$

donde, para cada $i = 1, \dots, r$, α_i es un ciclo de longitud k_i . Demostraremos el teorema por inducción sobre r .

Caso base: Se deja como ejercicio demostrar que un solo ciclo de longitud k_1 tiene orden k_1 (Ejercicio 2.31).

Hipótesis de inducción: Supongamos que toda permutación $\beta \in S_n$ con estructura cíclica $\{t_1, \dots, t_s\}$, donde $s < r$, cumple que $|\beta| = \text{mcm}(t_1, \dots, t_s)$.

Paso de inducción: Definimos la permutación

$$\beta := \alpha_2 \dots \alpha_r.$$

Observemos que $\alpha = \alpha_1 \beta$, que β tiene estructura cíclica $\{k_2, \dots, k_r\}$ y, por hipótesis de inducción, $|\beta| = \text{mcm}(k_2, \dots, k_r)$. Sean

$$a := |\alpha| \quad \text{y} \quad m := \text{mcm}(k_1, |\beta|) = \text{mcm}(k_1, k_2, \dots, k_r).$$

Demostraremos que $a = m$, mostrando que $a \mid m$ y $m \mid a$.

Afirmación: a divide a m

Como m es múltiplo de k_1 y de $|\beta|$, tenemos que $\alpha_1^m = (1)$ y $\beta^m = (1)$. Debido a que α_1 y β consisten en ciclos disjuntos, el Lema 2.57 implica que α_1 y β conmutan. Luego,

$$\alpha^m = (\alpha_1 \beta)^m = \alpha_1^m \beta^m = (1).$$

Por el Lema 1.25, $a = |\alpha|$ divide a m .

Afirmación: m divide a a

Observemos que

$$(1) = \alpha^a = \alpha_1^a \beta^a \quad \Rightarrow \quad \alpha_1^a = \beta^{-a}.$$

Por los Ejercicios 2.23 y 2.24,

$$\text{supp}(\alpha_1^a) = \text{supp}(\beta^{-a}) \subseteq \text{supp}(\alpha_1) \cap \text{supp}(\beta).$$

Al ser α_1 y β permutaciones disjuntas, $\text{sup}(\alpha_1) \cap \text{sup}(\beta) = \emptyset$, por lo que $\text{sup}(\alpha_1^a) = \text{sup}(\beta^{-a}) = \emptyset$. Esto demuestra que

$$\alpha_1^a = \beta^{-a} = (1) \quad \Rightarrow \quad \alpha_1^a = (1) \text{ y } \beta^a = (1).$$

Nuevamente, por el Lema 1.25, $|\alpha_1| = k_1 \mid a$ y $|\beta| \mid a$; es decir, a es un múltiplo común de k_1 y $|\beta|$. Por la propiedad del mínimo común múltiplo, m divide a a .

□

Ejemplo 2.66. Si $\alpha = (1, 2)(3, 4, 5)$, entonces $|\alpha| = \text{mcm}(2, 3) = 6$.

Ejemplo 2.67. Si $\beta = (1, 2)(3, 2, 5)$, entonces no es verdad que el orden de β sea 6, pues los ciclos dados en esta descomposición de β no son disjuntos. Podemos expresar a β como producto de ciclos disjuntos simplemente haciendo el producto entre $(1, 2)$ y $(3, 2, 5)$:

$$\beta = (1, 2)(3, 2, 5) = (1, 2, 5, 3) \quad \Rightarrow \quad |\beta| = 4.$$

Ejemplo 2.68. La lista de órdenes de las permutaciones en S_n puede obtenerse analizando las posibles estructuras cíclicas en S_n .

Est. cíclica	{1}	{2}	{3}	{4}	{2, 2}
Ejemplo	(1)	(1, 2)	(1, 2, 3)	(1, 2, 3, 4)	(1, 2)(3, 4)
Orden	1	2	3	4	2

Cuadro 2.4: Órdenes de los elementos de S_4 .

Est. cíclica	{1}	{2}	{3}	{4}	{5}	{2, 2}	{2, 3}
Ejemplo	(1)	(1, 2)	(1, 2, 3)	(1, 2, 3, 4)	(1, 2, 3, 4, 5)	(1, 2)(3, 4)	(1, 2)(3, 4, 5)
Orden	1	2	3	4	5	2	6

Cuadro 2.5: Órdenes de los elementos de S_5 .

Observación 2.69. Las estructuras cíclicas de S_n están en biyección con las *particiones* de n en el sentido de teoría de números, es decir, con las formas de escribir a n como una suma de enteros positivos. Por ejemplo, cuando $n = 5$, la estructura cíclica {2} corresponde a la partición $2+1+1+1$, mientras que {2, 3} corresponde a $2+3$. De hecho, dada una estructura cíclica $\{k_1, k_2, \dots, k_r\}$, la partición de n está dada por

$$k_1 + k_2 + \dots + k_r + \underbrace{1 + 1 + \dots + 1}_{n - k_1 - \dots - k_r \text{ veces}}.$$

Los siguientes resultados nos dan una forma para obtener, de manera sencilla, el conjugado de una permutación.

Lema 2.70 (conjugación de k -ciclos). Sea $\alpha \in S_n$ cualquier permutación y $(a_1, a_2, \dots, a_k) \in S_n$ un k -ciclo. Entonces,

$$\alpha(a_1, a_2, \dots, a_k)\alpha^{-1} = (\alpha(a_1), \alpha(a_2), \dots, \alpha(a_k)).$$

Demostración. Demostraremos que

$$\alpha(a_1, a_2, \dots, a_k)\alpha^{-1}(c) = (\alpha(a_1), \alpha(a_2), \dots, \alpha(a_k))(c), \quad \forall c \in [n].$$

Caso 1: $c = \alpha(a_i)$, para algún i . Del lado derecho obtenemos que

$$(\alpha(a_1), \alpha(a_2), \dots, \alpha(a_k))(\alpha(a_i)) = \alpha(a_{(i+1) \bmod k}).$$

Para calcular el lado izquierdo, primero observamos que $c = \alpha(a_i)$ implica que $\alpha^{-1}(c) = a_i$. Entonces,

$$\alpha(a_1, a_2, \dots, a_k)\alpha^{-1}(c) = \alpha(a_1, a_2, \dots, a_k)(a_i) = \alpha(a_{(i+1) \bmod k}).$$

Caso 2: $c \neq \alpha(a_i)$ para toda i . Del lado derecho obtenemos que c queda fijo

$$(\alpha(a_1), \alpha(a_2), \dots, \alpha(a_k))(c) = c.$$

Observando que $c \neq \alpha(a_i)$ para toda i implica que $\alpha^{-1}(c) \neq a_i$ para toda i , obtenemos que

$$\alpha(a_1, a_2, \dots, a_k)\alpha^{-1}(c) = \alpha(\alpha^{-1}(c)) = c.$$

□

Corolario 2.71 (conjugado de una permutación). Sean α y β permutaciones. Supongamos que la descomposición en ciclos disjuntos de β es

$$\beta = (b_{1,1}, \dots, b_{1,k_1}) \dots (b_{r,1}, \dots, b_{r,k_r}).$$

Entonces,

$$\alpha\beta\alpha^{-1} = (\alpha(b_{1,1}), \dots, \alpha(b_{1,k_1})) \dots (\alpha(b_{r,1}), \dots, \alpha(b_{r,k_r})).$$

Demostración. Aplicando el lema anterior, podemos obtener lo siguiente:

$$\begin{aligned} \alpha\beta\alpha^{-1} &= \alpha(b_{1,1}, \dots, b_{1,k_1}) \dots (b_{r,1}, \dots, b_{r,k_r})\alpha^{-1} \\ &= \alpha(b_{1,1}, \dots, b_{1,k_1})\alpha^{-1}\alpha \dots \alpha^{-1}\alpha(b_{r,1}, \dots, b_{r,k_r})\alpha^{-1} \\ &= (\alpha(b_{1,1}), \dots, \alpha(b_{1,k_1})) \dots (\alpha(b_{r,1}), \dots, \alpha(b_{r,k_r})). \end{aligned}$$

□

Ejemplo 2.72. Sean $\alpha = (2, 5)$ y sea $\beta = (1, 2, 3, 4)$. Usando el corolario anterior obtenemos que

$$\alpha\beta\alpha^{-1} = (\alpha(1), \alpha(2), \alpha(3), \alpha(4)) = (1, 5, 3, 4).$$

Ejemplo 2.73. Sean $\alpha = (1, 2, 3)(4, 5)$ y sea $\beta = (1, 3)(2, 4)$. Usando el corolario anterior obtenemos que

$$\alpha\beta\alpha^{-1} = (\alpha(1), \alpha(3))(\alpha(2), \alpha(4)) = (2, 1)(3, 5).$$

2.3.3. Grupo alternante

Definición 2.74 (transposición). Una permutación es una *transposición* si es un 2-ciclo.

Ejemplo 2.75. Todas las transposiciones de S_4 son:

$$(1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4).$$

Teorema 2.76 (descomposición en transposiciones). Toda permutación se puede escribir como el producto de transposiciones.

Demostración. Por el Teorema 2.63, toda permutación puede escribirse como producto de ciclos disjuntos, así que, para demostrar este teorema, basta con probar que todo ciclo puede escribirse como el producto de transposiciones. Dado cualquier ciclo (a_1, a_2, \dots, a_k) , con $k \geq 2$, observemos que

$$(a_1, a_2, \dots, a_k) = (a_1, a_2)(a_2, a_3) \dots (a_{k-2}, a_{k-1})(a_{k-1}, a_k),$$

lo cual puede verificarse directamente evaluando cada a_i en ambos lados de la igualdad. Finalmente, si $k = 1$, tenemos a la permutación identidad, la cual puede descomponerse como

$$(1) = (1, 2)(1, 2).$$

□

Observación 2.77. La descomposición en transposiciones de un ciclo no es única. Por ejemplo, además de la descomposición dada en el teorema anterior usando transposiciones de elementos consecutivos del ciclo, también tenemos la siguiente descomposición usando al primer elemento como “ancla”:

$$(a_1, a_2, \dots, a_k) = (a_1, a_k)(a_1, a_{k-1}) \dots (a_1, a_3)(a_1, a_2).$$

Ejemplo 2.78. Observemos las siguientes descomposiciones en transposiciones:

$$\begin{aligned} (1, 2, 3, 4, 5) &= (1, 2)(2, 3)(3, 4)(4, 5) = (1, 5)(1, 4)(1, 3)(1, 2), \\ (1, 3, 4)(5, 6) &= (1, 3)(3, 4)(5, 6) = (1, 4)(1, 3)(5, 6), \\ (3, 5, 2) &= (3, 5)(3, 2) = (3, 5)(3, 2)(1, 4)(1, 4). \end{aligned}$$

En particular, el último ejemplo muestra que el número de transposiciones que aparecen en la descomposición tampoco es único.

Observación 2.79. Recordemos que un subconjunto S genera a un grupo G si todos los elementos de G pueden ser expresados como productos de los elementos de $S \cup S^{-1}$ (ver Ejercicio 1.25). Por lo tanto, el Teorema 2.76 establece que todo grupo simétrico S_n es generado por el conjunto de sus transposiciones.

Definición 2.80 (función signo). Para cualquier $n \geq 2$, definimos la *función signo* $\text{sgn} : S_n \rightarrow \{1, -1\}$ como

$$\text{sgn}(\alpha) = (-1)^s, \quad \forall \alpha \in S_n,$$

donde s es el número de transposiciones que aparecen en la descomposición de α .

Observación 2.81. Por la definición de la función signo podemos deducir que, para cualquier $\alpha \in S_n$, $\text{sgn}(\alpha) = 1$ si y solo si existe una descomposición de α en un número par de transposiciones, y $\text{sgn}(\alpha) = -1$ si y solo si existe una descomposición de α en un número impar de transposiciones.

Como vimos en el Ejemplo 2.78, el número de transposiciones que aparecen en las descomposiciones no es único. Por ejemplo, si $\alpha := (1, 2, 3)$, entonces

$$\alpha = (1, 2)(2, 3) \quad \text{y} \quad \alpha = (1, 2)(2, 3)(1, 2)(1, 2),$$

por lo podemos obtener $\text{sgn}(\alpha) = (-1)^2 = 1$, ó $\text{sgn}(\alpha) = (-1)^4 = 1$. El siguiente resultado demuestra que, independientemente de la descomposición en transposiciones que usemos para $\alpha \in S_n$, el resultado de la función signo aplicada en α siempre será el mismo.

Teorema 2.82 (función signo). La función signo $\text{sgn} : S_n \rightarrow \{1, -1\}$ está bien definida.

Demostración. Debemos demostrar que el número de transposiciones en la descomposición de cualquier permutación es siempre par, o siempre impar. Empezaremos demostrando que la identidad siempre se descompone en un número par de transposiciones.

Afirmación: Si $\text{id} = \tau_r \tau_{r-1} \dots \tau_2 \tau_1$, donde las τ_i 's son transposiciones, entonces r es par.

No es posible que $r = 1$, pues una transposición no es igual a la identidad. Luego $r \geq 2$. Demostraremos por inducción que r debe ser par.

Caso base: Si $r = 2$, entonces r es par, justo como se necesita.

Hipótesis de inducción: Si id se descompone en un producto de s transposiciones, con $s < r$, entonces s es par.

Paso de inducción: Si $\tau_i = \tau_{i-1}$, para algún i , entonces $\tau_i \tau_{i-1} = \text{id}$. En esta situación, podríamos omitir el producto $\tau_i \tau_{i-1}$ para obtener una descomposición de id en $r - 2$ transposiciones. Por hipótesis de inducción, que $r - 2$ es par, lo que implica que r es par.

Para usar reducción al absurdo, supongamos que $\tau_i \neq \tau_{i-1}$ para toda i . Sean $\tau_2 = (c, d)$ y $\tau_1 = (a, b)$. Demostraremos que podemos reemplazar a $\tau_2 \tau_1$ por un producto de dos transposiciones $\tau_2^{(1)} \tau_1^{(1)}$ donde el número a solo aparece en la transposición de la izquierda. Analizaremos tres casos:

Caso 1: τ_2 y τ_1 son disjuntas. Entonces τ_2 y τ_1 conmutan, por lo que

$$\tau_2\tau_1 = (c, d)(a, b) = (a, b)(c, d).$$

Caso 2: $\text{supp}(\tau_2) \cap \text{supp}(\tau_1) = \{a\}$. Sin perder generalidad, supongamos que $a = d$. Luego,

$$\tau_2\tau_1 = (c, a)(a, b) = (a, b)(b, c).$$

Caso 3: $\text{supp}(\tau_2) \cap \text{supp}(\tau_1) = \{b\}$. Sin perder generalidad, supongamos que $b = d$. Luego,

$$\tau_2\tau_1 = (c, b)(a, b) = (a, c)(c, b).$$

El caso $\text{supp}(\tau_2) \cap \text{supp}(\tau_1) = \{a, b\}$ no es posible pues $\tau_2 \neq \tau_1$.

Con lo anterior, obtenemos una nueva descomposición

$$\text{id} = \tau_r\tau_{r-1} \dots \tau_3\tau_2^{(1)}\tau_1^{(1)},$$

donde el número a aparece por primera vez (yendo de derecha a izquierda) en $\tau_2^{(1)}$. Usamos el argumento del párrafo anterior para reemplazar a $\tau_3\tau_2^{(1)}$ y obtener otra descomposición

$$\text{id} = \tau_r\tau_{r-1} \dots \tau_3^{(2)}\tau_2^{(2)}\tau_1^{(1)},$$

donde el número a aparece por primera vez en $\tau_3^{(2)}$. Continuando este proceso $r - 1$ veces obtenemos una descomposición

$$\text{id} = \tau_r^{(r-1)}\tau_{r-1}^{(r-1)} \dots \tau_2^{(2)}\tau_1^{(1)},$$

donde el número a aparece por primera vez en $\tau_r^{(r-1)}$. Sin embargo, esto implica que a no queda fijo en este producto de transposiciones, lo cual es una contradicción, pues a obviamente queda fijo al aplicar id . Esto concluye la demostración.

Afirmación: Sea $\alpha \in S_n$ una permutación tal que

$$\alpha = \tau_r\tau_{r-1} \dots \tau_2\tau_1 = \sigma_s\sigma_{s-1} \dots \sigma_2\sigma_1,$$

donde las τ_i 's y σ_j 's son transposiciones. Entonces, r es par si y solo si s es par.

Como las transposiciones tienen orden 2, se cumple que $\tau_i^{-1} = \tau_i$, para toda i . Despejando la igualdad de arriba, obtenemos que

$$\text{id} = \sigma_s\sigma_{s-1} \dots \sigma_2\sigma_1\tau_1 \dots \tau_{r-1}\tau_r.$$

Por la afirmación anterior, $r + s$ debe ser un número par, lo que implica que r es par si y solo si s es par. \square

Definición 2.83 (paridad). Decimos que una permutación $\alpha \in S_n$ es *par* si $\text{sgn}(\alpha) = 1$, y decimos que es *impar* si $\text{sgn}(\alpha) = -1$.

En otras palabras, una permutación es par, o impar, si puede descomponerse en un número par, o impar, de transposiciones, respectivamente. El Teorema 2.82 implica que una permutación no puede ser par e impar al mismo tiempo.

Ejemplo 2.84 (permutaciones pares e impares). 1. La permutación $(1, 2, 3, 4)$ es impar pues puede escribirse como un producto de 3 transposiciones:

$$(1, 2, 3, 4) = (1, 4)(1, 3)(1, 2).$$

2. La permutación $(1, 2, 3, 4)(5, 6)$ es par pues puede escribirse como un producto de 4 transposiciones:

$$(1, 2, 3, 4)(5, 6) = (1, 4)(1, 3)(1, 2)(5, 6).$$

3. Como sabemos, cualquier k -ciclo (a_1, a_2, \dots, a_k) puede escribirse como un producto de $k - 1$ transposiciones:

$$(a_1, a_2, \dots, a_k) = (a_1, a_k)(a_1, a_{k-1}) \dots (a_1, a_2).$$

Por lo tanto, un k -ciclo es una permutación par si k es impar, y es una permutación impar si k es par.

Teorema 2.85 (función signo es homomorfismo). Consideremos al conjunto $\{1, -1\}$ como un grupo equipado con la multiplicación. Entonces, la función signo $\text{sgn} : S_n \rightarrow \{1, -1\}$ es un homomorfismo.

Demostración. Sean $\alpha, \beta \in S_n$ permutaciones con las siguientes descomposiciones en transposiciones: $\alpha = \tau_r \dots \tau_2 \tau_1$ y $\beta = \sigma_s \dots \sigma_2 \sigma_1$. Entonces,

$$\begin{aligned} \text{sgn}(\alpha\beta) &= \text{sgn}(\tau_r \dots \tau_2 \tau_1 \sigma_s \dots \sigma_2 \sigma_1) \\ &= (-1)^{r+s} = (-1)^r (-1)^s \\ &= \text{sgn}(\alpha) \text{sgn}(\beta). \end{aligned}$$

Esto demuestra que sgn es un homomorfismo. \square

Definición 2.86 (grupo alternante). El *grupo alternante de grado n* se define como el kernel de la función signo:

$$A_n := \ker(\text{sgn}) = \{\alpha \in S_n : \text{sgn}(\alpha) = 1\} = \{\alpha \in S_n : \alpha \text{ es par}\}.$$

Observación 2.87. Dado que la función signo es un homomorfismo y A_n es su kernel, el Lema 1.107 implica que A_n es un subgrupo normal de S_n .

Teorema 2.88 (orden de A_n). Para cualquier $n \geq 2$,

$$|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}.$$

En otras palabras, el índice de A_n en S_n es 2.

Demostración. Sea I_n el conjunto de permutaciones impares en S_n . Claramente, $S_n = A_n \cup I_n$, donde la unión es disjunta porque ninguna permutación puede ser par e impar al mismo tiempo. Primero demostraremos que $|A_n| = |I_n|$. Consideremos la función $\psi : A_n \rightarrow I_n$ dada por

$$\psi(\alpha) = \alpha(1, 2), \quad \forall \alpha \in A_n.$$

Observemos que si α es par, entonces $\alpha(1, 2)$ es impar (pues estamos agregando una transposición), por lo que el codominio de ψ es efectivamente I_n . Demostraremos que ψ es una biyección.

1. ψ es inyectiva. Para cualesquiera $\alpha, \beta \in A_n$,

$$\psi(\alpha) = \psi(\beta) \Rightarrow \alpha(1, 2) = \beta(1, 2) \Rightarrow \alpha = \beta.$$

2. ψ es sobreyectiva. Sea $\gamma \in I_n$ una permutación impar arbitraria. Entonces, $\gamma(1, 2)$ es par y

$$\psi(\gamma(1, 2)) = \gamma(1, 2)(1, 2) = \gamma.$$

Por lo anterior,

$$|S_n| = |A_n \cup I_n| = |A_n| + |I_n| = |A_n| + |A_n| = 2|A_n|.$$

Por lo tanto, $|A_n| = \frac{|S_n|}{2}$. □

Ejemplo 2.89. El grupo A_3 tiene orden $\frac{3!}{2} = 3$; explícitamente,

$$A_3 = \{(1), (1, 2, 3), (1, 3, 2)\}.$$

El grupo A_4 tiene orden $\frac{4!}{2} = 12$; explícitamente

$$A_4 = \left\{ \begin{array}{cccccc} (1), & (1, 2)(3, 4), & (1, 3)(2, 4), & (1, 4)(2, 3), & (1, 2, 3), & (1, 3, 2), \\ (1, 2, 4), & (1, 4, 2), & (1, 3, 4), & (1, 4, 3), & (2, 3, 4), & (2, 4, 3) \end{array} \right\}.$$

Palabras clave: *permutación, grupo simétrico, soporte, notación cíclica, estructura cíclica, orden de una permutación, transposición, paridad, grupo alternante.*

2.3.4. Ejercicios

Ejercicio 2.22. Da un ejemplo de una función $f : \mathbb{Z} \rightarrow \mathbb{Z}$ que sea inyectiva pero no sobreyectiva, y da un ejemplo de una función $g : \mathbb{Z} \rightarrow \mathbb{Z}$ que sea sobreyectiva pero no inyectiva.

Ejercicio 2.23. Para cualquier $\alpha \in S_n$ y $k \in \mathbb{Z}_+$, demuestra que

1. $\text{fix}(\alpha) \subseteq \text{fix}(\alpha^k)$.
2. $\text{supp}(\alpha^k) \subseteq \text{supp}(\alpha)$.

Ejercicio 2.24. Para cualquier $\alpha \in S_n$, demuestra que

1. $\text{fix}(\alpha) = \text{fix}(\alpha^{-1})$.
2. $\text{supp}(\alpha) = \text{supp}(\alpha^{-1})$.

Ejercicio 2.25. Escribe la siguiente permutación en notación cíclica:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 7 & 2 & 1 & 3 & 6 \end{pmatrix}$$

Ejercicio 2.26. Escribe todos los elementos de S_4 en notación cíclica.

Ejercicio 2.27. Sea $\alpha \in S_n$. Demuestra que la relación sobre $[n] = \{1, 2, \dots, n\}$ definida como

$$i \sim j \iff \exists k \geq 0 \text{ tal que } \alpha^k(i) = j$$

es una relación de equivalencia. Describe las clases de equivalencia en esta relación de equivalencia.

Ejercicio 2.28. Demuestra que la descomposición de una permutación en producto de ciclos disjuntos es única salvo el orden en el que aparecen los ciclos.

Ejercicio 2.29. Escribe cada una de las siguientes permutaciones como producto de ciclos disjuntos y encuentra sus órdenes:

1. $(1, 2, 3, 5)(4, 1, 3)$.
2. $(1, 3, 2, 5, 6)(2, 3)(4, 6, 5, 1, 2)$.
3. $(1, 2)(1, 3)(2, 3)(1, 4, 2)$.
4. $(1, 2, 4)(3, 5, 7)$.

Ejercicio 2.30. Determina si las siguientes permutaciones son pares o impares:

1. $(1, 3, 5)$.
2. $(1, 3, 5, 6)$.
3. $(1, 2)(1, 3, 4)(1, 5, 2)$.
4. $(1, 2, 4, 3)(3, 5, 2, 1)$.

Ejercicio 2.31. Demuestra que el orden de un k -ciclo (a_1, a_2, \dots, a_k) es k .

Ejercicio 2.32. Escribe todas las posibles estructuras cíclicas y órdenes de los elementos de los siguientes grupos: S_6 y A_6 .

Ejercicio 2.33. Escribe todas las posibles estructuras cíclicas y órdenes de los elementos de los siguientes grupos: S_7 y A_7 .

Ejercicio 2.34. Sea H un subgrupo de S_n . Demuestra que $H \leq A_n$ o exactamente la mitad de los elementos de H son pares.

Ejercicio 2.35. Encuentra el conjugado $\alpha\beta\alpha^{-1}$ en cada una de las siguientes situaciones:

1. $\alpha = (1, 2, 3, 4)$ y $\beta = (1, 3)$.
2. $\alpha = (1, 5)(2, 4)$ y $\beta = (1, 2)(2, 4, 5)$.
3. $\alpha = (1, 2)$ y $\beta = (2, 3)$.
4. $\alpha = (1, 3)(5, 6)$ y $\beta = (1, 2, 3, 4, 5)$.

Ejercicio 2.36. Demuestra que dos permutaciones $\alpha, \beta \in S_n$ son conjugadas si y solo si α y β tienen la misma estructura cíclica.

Ejercicio 2.37. Sea $H = \{(1), (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$. Demuestra que H es un subgrupo normal de A_4 . Escribe todas las clases laterales del grupo cociente A_4/H .

Ejercicio 2.38. Para $n \geq 2$, Demuestra que S_n es generado por los siguientes conjuntos:

1. $S := \{(1, 2), (2, 3), \dots, (n-1, n)\}$

2. $S := \{(1, 2), (1, 3), \dots, (1, n)\}$

3. $S := \{(1, 2), (1, 2, \dots, n)\}$

(Sugerencia: en cada caso, demuestra que toda transposición puede escribirse como productos de elementos en $S \cup S^{-1}$ y usa el Teorema 2.76.)

Ejercicio 2.39 (*). Para $n \geq 3$, demuestra que A_n es generado por el conjunto de 3-ciclos.

Ejercicio 2.40. Para $n \geq 3$ demuestra que S_n no es abeliano.

Ejercicio 2.41. Para $n \geq 3$ demuestra que el centro de S_n es trivial, es decir $Z(S_n) = \{(1)\}$.

3

Temas selectos

3.1. Acciones de grupos

3.1.1. Definiciones y ejemplos

Definición 3.1 (acción de grupo - primera definición). Sean G un grupo y X un conjunto. Una *acción* de G en X es una función $\cdot : G \times X \rightarrow X$ que cumple lo siguiente:

- a) $e \cdot x = x$ para todo $x \in X$.
- b) $g \cdot (h \cdot x) = (gh) \cdot x$ para todo $g, h \in G, x \in X$.

Cuando existe una acción de G en X , la cual está clara en el contexto, decimos que G *actúa* en X .

Observación 3.2. En la definición de acción de G en X denotamos a la imagen de $(g, x) \in G \times X$ por $g \cdot x$.

Ejemplo 3.3 (acción regular izquierda). Sea G un grupo y $X = G$. Definimos $\cdot : G \times X \rightarrow X$ por

$$g \cdot x := gx, \quad \forall g, x \in G.$$

Verificamos que esto es una acción de G en G :

- a) $e \cdot x = ex = x$, para todo $x \in G$.
- b) $g \cdot (h \cdot x) = g(hx) = (gh)x = (gh) \cdot x$, para todo $g, h, x \in G$.

Esta acción se llama la *acción regular izquierda de G en G* , y es equivalente a multiplicar elementos de G por la izquierda.

Ejemplo 3.4 (acción regular derecha). Sea G un grupo y $X = G$. Podríamos pensar en definir una acción análoga a la acción regular izquierda de G en G de la siguiente forma: $g \cdot x := xg$, para todo $g, x \in G$. Sin embargo, esto no cumple la propiedad b) en la definición de acción: $g \cdot (h \cdot x) = (xh)g \neq (gh) \cdot x = x(gh)$. Para solucionar esto, multiplicamos por la derecha por g^{-1} ; es decir, definimos

$$g \cdot x := xg^{-1}, \quad \forall g, x \in G.$$

Verificamos que esto es una acción de G en G :

- a) $e \cdot x = xe^{-1} = xe = x$, para todo $x \in G$.
- b) $g \cdot (h \cdot x) = (xh^{-1})g^{-1} = x(gh)^{-1} = (gh) \cdot x$, para todo $g, h, x \in G$.

Esta acción se llama la *acción regular derecha de G en G* .

Ejemplo 3.5 (acción por conjugación). Sea G un grupo y $X = G$. Definimos $\cdot : G \times X \rightarrow X$ por

$$g \cdot x := gxg^{-1}, \quad \forall g, x \in G.$$

Verificamos que esto es una acción de G en G :

- a) $e \cdot x = exe^{-1} = x$, para todo $x \in G$.
- b) $g \cdot (h \cdot x) = g(hxh^{-1})g^{-1} = (gh)x(gh)^{-1} = (gh) \cdot x$, para todo $g, h, x \in G$.

Esta acción se llama la *acción por conjugación de G en G* .

Ejemplo 3.6 (acción natural de S_n). Sea $G = S_n$ y $X = [n] = \{1, 2, \dots, n\}$. Definimos $\cdot : S_n \times [n] \rightarrow [n]$ por

$$\alpha \cdot k := \alpha(k), \quad \forall \alpha \in S_n, k \in [n].$$

Verificamos que esto es una acción de S_n en $[n]$:

- a) $\text{id} \cdot k = \text{id}(k) = k$, para todo $k \in [n]$.
- b) $\alpha \cdot (\beta \cdot k) = \alpha(\beta(k)) = (\alpha \circ \beta)(k) = (\alpha \circ \beta) \cdot k$, para todo $\alpha, \beta \in S_n, k \in [n]$.

Ejemplo 3.7 (acción en clases laterales). Sea G un grupo, H un subgrupo de G , y $X = G/H = \{aH : a \in G\}$ el conjunto de clases laterales izquierdas de H en G . Definimos $\cdot : G \times G/H \rightarrow G/H$ por

$$g \cdot aH := gaH, \quad \forall g \in G, aH \in G/H.$$

Se trata de una función bien definida, pues si $aH = bH$ entonces $gaH = gbH$. Verificamos que esto es una acción de G en G/H :

- a) $e \cdot aH = eaH = aH$, para todo $aH \in G/H$.
- b) $g \cdot (h \cdot aH) = g(ha)H = (gh)aH = (gh) \cdot aH$, para todo $g, h \in G, aH \in G/H$.

Ejemplo 3.8 (acción por conjugación en subgrupos). Sea G un grupo y $X = \{H : H \leq G\}$ el conjunto de todos los subgrupos de G . Definimos $\cdot : G \times X \rightarrow X$ por

$$g \cdot H := gHg^{-1} = \{ghg^{-1} : h \in H\}, \quad \forall g \in G, H \in X.$$

Para demostrar que se trata de una función bien definida, hay que verificar que gHg^{-1} efectivamente pertenece a X , es decir, que gHg^{-1} es un subgrupo de G (Ejercicio 3.4). Verificamos que esto es una acción de G en X :

- a) $e \cdot H = eHe^{-1} = H$, para todo $H \in X$.
- b) $g \cdot (k \cdot H) = g(kHk^{-1})g^{-1} = (gk)H(gk)^{-1} = (gk) \cdot H$, para todo $g, k \in G$, $H \in X$.

Ejemplo 3.9 (acción de traslación). Sea G un grupo y A un conjunto. Denotamos por A^G al conjunto de todas las funciones con dominio G y codominio A ; es decir,

$$A^G := \{\phi : G \rightarrow A\}.$$

Definimos $\cdot : G \times A^G \rightarrow A^G$ de la siguiente forma: para cualquier $g \in G$, $\phi \in A^G$, obtenemos una función $g \cdot \phi \in A^G$ dada por

$$(g \cdot \phi)(h) := \phi(g^{-1}h), \quad \forall h \in G.$$

Verificamos que esto es una acción de G en A^G :

- a) $(e \cdot \phi)(h) = \phi(e^{-1}h) = \phi(h)$, para toda $h \in G$. Esto implica que $e \cdot \phi = \phi$, para toda $\phi \in A^G$.
- b) $g \cdot (k \cdot \phi)(h) = (k \cdot \phi)(g^{-1}h) = \phi(k^{-1}g^{-1}h) = \phi((gk)^{-1}h) = (gk \cdot \phi)(h)$, para toda $h \in G$. Esto implica que $g \cdot (k \cdot \phi) = gk \cdot \phi$ para toda $g, k \in G$, $\phi \in A^G$.

Esta acción se llama la *acción de traslación* de G en A^G .

Existe una definición de acción de grupo equivalente a la definición 3.1, la cual nos ofrece otro punto de vista interesante.

Dado cualquier conjunto X , $\text{Sym}(X)$ es el grupo de todas las biyecciones de X en X equipado con la composición de funciones. Si $X = [n]$, entonces $\text{Sym}([n]) = S_n$.

Definición 3.10 (acción de grupo - segunda definición). Sea G un grupo y X un conjunto. Una *acción* de G en X es un homomorfismo $\rho : G \rightarrow \text{Sym}(X)$.

Teorema 3.11. Las definiciones 3.1 y 3.10 de acción de grupo son equivalentes.

Demostración. Sea G un grupo y X un conjunto. Demostraremos que toda acción de G en X en el sentido de la definición 3.1 induce una acción de G en X en el sentido de la definición 3.10, y viceversa.

Afirmación: *Toda acción $\cdot : G \times X \rightarrow X$ induce un homomorfismo $\rho : G \rightarrow \text{Sym}(X)$.*

Sea $\cdot : G \times X \rightarrow X$ una acción en el sentido de la definición 3.1. Definimos una función $\rho : G \rightarrow \text{Sym}(X)$ de la siguiente forma: para cada $g \in G$, $\rho(g) : X \rightarrow X$ es la función definida por:

$$\rho(g)(x) := g \cdot x, \quad \forall x \in X.$$

Para demostrar que $\rho : G \rightarrow \text{Sym}(X)$ está bien definida, hay que verificar que $\rho(g) \in \text{Sym}(X)$, es decir, que $\rho(g) : X \rightarrow X$ es una biyección:

1. Para demostrar que $\rho(g)$ es inyectiva, supongamos que $\rho(g)(x) = \rho(g)(y)$. Esto significa, por definición, que $g \cdot x = g \cdot y$. Aplicando la acción de g^{-1} de ambos lados de la igualdad, obtenemos

$$\begin{aligned} g^{-1} \cdot (g \cdot x) &= g^{-1} \cdot (g \cdot y) \Rightarrow (g^{-1}g) \cdot x = (g^{-1}g) \cdot y \\ &\Rightarrow e \cdot x = e \cdot y \\ &\Rightarrow x = y. \end{aligned}$$

2. Para demostrar que $\rho(g)$ es sobreyectiva, sea $y \in X$ un elemento arbitrario. Entonces, su preimagen bajo $\rho(g)$ es $g^{-1} \cdot y \in X$, porque

$$\rho(g)(g^{-1} \cdot y) = g \cdot (g^{-1} \cdot y) = (gg^{-1}) \cdot y = e \cdot y = y.$$

Finalmente, comprobamos que $\rho : G \rightarrow \text{Sym}(X)$ es un homomorfismo: para toda $g, h \in G, x \in X$,

$$\rho(gh)(x) = gh \cdot x = g \cdot (h \cdot x) = \rho(g)(\rho(h)(x)) = \rho(g) \circ \rho(h)(x).$$

Esto implica que $\rho(gh) = \rho(g)\rho(h)$, para toda $g, h \in G$, por lo que ρ es un homomorfismo.

Afirmación: *Todo homomorfismo $\rho : G \rightarrow \text{Sym}(X)$ induce una acción $\cdot : G \times X \rightarrow X$.*

Sea $\rho : G \rightarrow \text{Sym}(X)$ un homomorfismo (una acción de G en X en el sentido de la Definición 3.10). Definimos una función $G \times X \rightarrow X$ de la siguiente forma:

$$g \cdot x := \rho(g)(x), \quad \forall g \in G, x \in X.$$

Verificamos que esto cumple las propiedades de acción de acuerdo a la Definición 3.1:

- a) Observemos que $\rho(e) = \text{id} \in \text{Sym}(X)$, ya que homomorfismos mandan la identidad de un grupo a la identidad del otro. Por lo tanto, $e \cdot x = \rho(e)(x) = \text{id}(x) = x$, para toda $x \in X$.
- b) $g \cdot (h \cdot x) = \rho(g)(\rho(h)(x)) = \rho(g) \circ \rho(h)(x) = \rho(gh)(x) = (gh) \cdot x$, para toda $g, h \in G, x \in X$.

Con esto terminamos la demostración del teorema. \square

Observación 3.12. Intuitivamente, podemos visualizar la conexión entre $\cdot : G \times X \rightarrow X$ y $\rho : G \rightarrow \text{Sym}(X)$ de la siguiente forma: para cualquier $g \in G$, $\rho(g) : X \rightarrow X$ es la función de “aplicar puntito”, es decir $\rho(g) = g \cdot$, donde $g \cdot$ denota intuitivamente la función $(g \cdot)(x) := g \cdot x$, para toda $x \in X$.

Definición 3.13 (kernel de una acción). Sea $\rho : G \rightarrow \text{Sym}(X)$ una acción. El *kernel* de la acción es simplemente el kernel de ρ :

$$\ker(\rho) = \{g \in G : \rho(g) = \text{id}\} = \{g \in G : g \cdot x = x, \forall x \in X\}.$$

El lado derecho de la igualdad de arriba representa el kernel de la acción usando la notación $\cdot : G \times X \rightarrow X$.

Definición 3.14 (acción fiel). Una acción de G en X se dice *fiel* si su kernel es trivial, es decir, $\ker(\rho) = \{e\}$.

Observación 3.15. Si G actúa fielmente en X , entonces podemos aplicar el Primer Teorema de Isomorfía a $\rho : G \rightarrow \text{Sym}(X)$ para deducir que

$$\frac{G}{\ker(\rho)} \cong \rho(G) \Rightarrow G \cong \rho(G) \leq \text{Sym}(X).$$

Esto significa que si G actúa fielmente en X , entonces G es isomorfo a un subgrupo de $\text{Sym}(X)$.

Ejemplo 3.16 (kernel). A continuación obtenemos los kernels de algunas de las acciones de los ejemplos anteriores:

1. Si ρ es la acción regular izquierda de G en G , entonces

$$\ker(\rho) = \{g \in G : gh = h, \forall h \in G\} = \{e\}.$$

Esto demuestra que la acción regular izquierda de G en G es fiel.

2. Si ρ es la acción por conjugación de G en G , entonces

$$\ker(\rho) = \{g \in G : ghg^{-1} = h, \forall h \in G\} = \{g \in G : gh = hg, \forall h \in G\} = Z(G).$$

3. Si ρ es la acción de G en sus clases laterales izquierdas G/H , entonces

$$\begin{aligned} \ker(\rho) &= \{g \in G : gaH = aH, \forall aH \in G/H\} \\ &= \{g \in G : a^{-1}ga \in H, \forall a \in G\} \\ &= \{g \in G : g \in aHa^{-1}, \forall a \in G\} \\ &= \bigcap_{a \in G} aHa^{-1}. \end{aligned}$$

El siguiente resultado establece que todo grupo puede verse como un subgrupo de algún grupo simétrico.

Teorema 3.17 (Cayley). Para todo grupo G existe un conjunto X tal que G es isomorfo a un subgrupo de $\text{Sym}(X)$.

Demostración. Como se vio en el ejemplo anterior, la acción regular izquierda de G en G es fiel, por lo que la Observación 3.15 implica que G es isomorfo a un subgrupo de $\text{Sym}(G)$. \square

El Teorema de Cayley implica que la comprensión total de los grupos simétricos $\text{Sym}(X)$ y sus subgrupos nos llevaría a la comprensión total de todos los grupos G . Sin embargo, la estructura de los subgrupos de $\text{Sym}(X)$ es extremadamente compleja, por lo que esto en realidad no representa una simplificación en la tarea de comprender todos los grupos.

3.1.2. Órbitas y estabilizadores

Definición 3.18 (órbita). Sea G un grupo que actúa en X . La *órbita* de $x \in X$ es el siguiente subconjunto de X

$$\text{Orb}(x) := \{g \cdot x : g \in G\}.$$

Lema 3.19. Sea G un grupo que actúa en X .

1. $\text{Orb}(x) = \text{Orb}(y)$ si y solo si $y \in \text{Orb}(x)$.
2. El conjunto de órbitas $\{\text{Orb}(x) : x \in X\}$ forma una partición de X .

Demostración.

1. Supongamos que $\text{Orb}(x) = \text{Orb}(y)$. Como todo elemento pertenece a su propia órbita (pues $y = e \cdot y$), tenemos $y \in \text{Orb}(y) = \text{Orb}(x)$. Supongamos ahora que $y \in \text{Orb}(x)$, es decir, que existe $g \in G$ tal que $y = g \cdot x$. Sea $h \cdot y \in \text{Orb}(y)$; sustituyendo,

$$h \cdot y = h \cdot (g \cdot x) = hg \cdot x \in \text{Orb}(x).$$

Esto demuestra que $\text{Orb}(y) \subseteq \text{Orb}(x)$. Como $y = g \cdot x$ implica que $x = g^{-1} \cdot y$, podemos repetir el argumento anterior para deducir que $\text{Orb}(x) \subseteq \text{Orb}(y)$. Por lo tanto, $\text{Orb}(x) = \text{Orb}(y)$.

2. Como $x \in \text{Orb}(x)$, para toda $x \in X$, claramente tenemos que

$$X = \bigcup_{x \in X} \text{Orb}(x).$$

Sean $\text{Orb}(x)$ y $\text{Orb}(y)$ órbitas tales que $\text{Orb}(x) \neq \text{Orb}(y)$; demostraremos que son disjuntas. Supongamos que existe $z \in \text{Orb}(x) \cap \text{Orb}(y)$. Luego $z \in \text{Orb}(x)$ y $z \in \text{Orb}(y)$. Por el punto anterior, $\text{Orb}(z) = \text{Orb}(x)$ y $\text{Orb}(z) = \text{Orb}(y)$, lo que implica que $\text{Orb}(x) = \text{Orb}(y)$. Esto es una contradicción. Por lo tanto, $\text{Orb}(x) \cap \text{Orb}(y) = \emptyset$.

□

Observación 3.20. Alternativamente a la demostración anterior, podemos verificar que la relación \sim sobre X , definida por $x \sim y$ si y solo si existe $g \in G$ tal que $y = g \cdot x$, es una relación de equivalencia cuyas clases de equivalencia son las órbitas de la acción.

Definición 3.21 (acción transitiva). La acción de un grupo G sobre X es llamada *transitiva* si $X = \text{Orb}(x)$, para algún (o, equivalentemente, para toda) $x \in X$.

Observación 3.22. Si G actúa transitivamente en X , entonces para toda $x, y \in X$ tenemos que $\text{Orb}(x) = X = \text{Orb}(y)$. Así, podemos deducir que una acción de G en X es transitiva si y solo si para toda $x, y \in X$ existe $g \in G$ tal que $y = g \cdot x$.

Ejemplo 3.23 (órbitas). Obtenemos las órbitas en algunas de las acciones definidas en la sección anterior.

1. Consideremos la acción regular izquierda de G en G . Para cualquier $x \in G$,

$$\text{Orb}(x) = \{gx : g \in G\} = G.$$

Por lo tanto, esta acción es transitiva.

2. Consideremos la acción por conjugación de G en G . Para cualquier $x \in G$,

$$\text{Orb}(x) = \{gxg^{-1} : g \in G\} =: \text{Cl}(x).$$

En el caso de esta acción, la órbita de $x \in G$ es igual a la *clase de conjugación* de x .

3. Consideremos la acción de G en las clases laterales G/H . Para cualquier $aH \in G/H$,

$$\text{Orb}(aH) = \{gaH : g \in G\} = G/H.$$

Por lo tanto, esta acción es transitiva.

4. Consideremos la acción por conjugación de G en sus subgrupos. Para cualquier $H \leq G$,

$$\text{Orb}(H) = \{gHg^{-1} : g \in G\} =: \text{Cl}(H).$$

En el caso de esta acción, la órbita de $H \leq G$ es igual a la *clase de conjugación* de H .

Definición 3.24 (estabilizador). Sea G un grupo que actúa en X . El *estabilizador* de $x \in X$ es el siguiente subconjunto de G :

$$\text{Stab}(x) := \{g \in G : g \cdot x = x\}.$$

Proposición 3.25. Sea G un grupo que actúa en X . Para cualquier $x \in X$, $\text{Stab}(x)$ es un subgrupo de G .

Demostración. Usaremos el Test del Subgrupo I:

1. Claramente $e \in \text{Stab}(x)$ pues $e \cdot x = x$.
2. Si $g, h \in \text{Stab}(x)$, entonces $g \cdot x = x$ y $h \cdot x = x$. Observemos que

$$gh \cdot x = g \cdot (h \cdot x) = g \cdot x = x.$$

Por lo tanto $gh \in \text{Stab}(x)$.

3. Si $g \in \text{Stab}(x)$, entonces $g \cdot x = x$. Aplicando la acción de g^{-1} en ambos lados de la igualdad, obtenemos

$$g^{-1} \cdot (g \cdot x) = g^{-1} \cdot x \Rightarrow x = g^{-1} \cdot x.$$

Por lo tanto, $g^{-1} \in \text{Stab}(x)$.

□

Ejemplo 3.26 (estabilizadores). Obtenemos estabilizadores en algunas de las acciones definidas en la sección anterior.

1. Consideremos la acción regular izquierda de G en G . Para cualquier $x \in G$,

$$\text{Stab}(x) = \{g \in G : gx = x\} = \{e\}.$$

2. Consideremos la acción por conjugación de G en G . Para cualquier $x \in G$,

$$\text{Stab}(x) = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\} =: C(x).$$

En el caso de esta acción, el estabilizador de $x \in G$ es igual al *centralizador* de x .

3. Consideremos la acción de G en las clases laterales G/H . Para cualquier $aH \in G/H$,

$$\begin{aligned} \text{Stab}(aH) &= \{g \in G : gaH = aH\} = \{g \in G : a^{-1}ga \in H\} \\ &= \{g \in G : g \in aHa^{-1}\} = aHa^{-1}. \end{aligned}$$

4. Consideremos la acción por conjugación de G en sus subgrupos. Para cualquier $H \leq G$,

$$\text{Stab}(H) = \{g \in G : gHg^{-1} = H\} =: N(H).$$

En el caso de esta acción, el estabilizador de $H \leq G$ es igual al *normalizador* de H .

Teorema 3.27 (órbita-estabilizador). Sea G un grupo que actúa en X . Para cualquier $x \in X$,

$$|\text{Orb}(x)| = [G : \text{Stab}(x)],$$

donde $[G : \text{Stab}(x)]$ denota el índice de $\text{Stab}(x)$ en G .

Demostración. Definimos una función $\phi : \text{Orb}(x) \rightarrow G/\text{Stab}(x)$ por

$$\phi(g \cdot x) := g\text{Stab}(x), \quad \forall g \cdot x \in \text{Orb}(x).$$

Observemos que

$$g \cdot x = h \cdot x \Leftrightarrow h^{-1}g \cdot x = x \Leftrightarrow h^{-1}g \in \text{Stab}(x) \Leftrightarrow g\text{Stab}(x) = h\text{Stab}(x).$$

Esto implica que ϕ está bien definida y es inyectiva.

Para demostrar que ϕ es sobreyectiva, sea $g\text{Stab}(x)$ una clase lateral arbitraria en $G/\text{Stab}(x)$. Es claro que su preimagen bajo ϕ es $g \cdot x$, pues $\phi(g \cdot x) = g\text{Stab}(x)$, lo que implica que ϕ es sobreyectiva. □

Observación 3.28. El teorema anterior es válido incluso cuando la cardinalidad de $\text{Orb}(x)$ es infinita, pues su demostración se hizo construyendo una biyección.

Corolario 3.29. Sea G un grupo finito que actúa en X . Para toda $x \in X$, $|\text{Orb}(x)|$ divide a $|G|$.

Demostración. Obtenemos el resultado aplicando el Teorema Órbita-Estabilizador y el Teorema de Lagrange. □

3.1.3. Aplicación: conteo de collares

Supongamos que un fabricante de collares dispone de q colores y n piedras. ¿Cuántos collares *no equivalentes* puede fabricar? Aquí consideramos que dos collares son equivalentes si podemos obtener uno del otro a través de una rotación.¹

La pregunta del párrafo es mucho más complicada de lo que parece. Por ejemplo, la Figura 3.1 ilustra todos los collares no equivalentes que pueden fabricarse con 2 colores (blanco y negro) y 4 piedras. Para tener una idea de cómo se complican las cosas cuando q y n crecen, se deja como ejercicio ilustrar todos los collares no equivalentes con 3 colores y 4 piedras, y con 2 colores y 5 piedras.

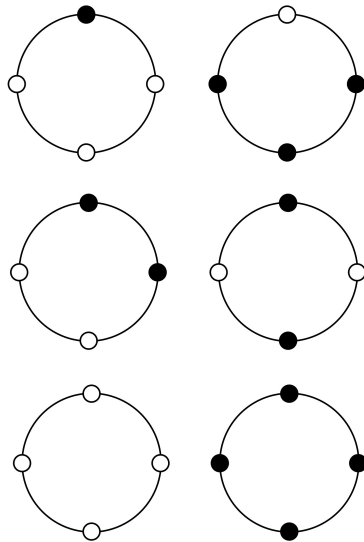


Figura 3.1: Collares no equivalentes con 2 colores y 4 piedras.

Para empezar a modelar este problema, sea A un conjunto con q elementos (los colores) y consideremos el grupo \mathbb{Z}_n (cuyos elementos serán las etiquetas de las piedras). Con esto, un collar es simplemente una función $f : \mathbb{Z}_n \rightarrow A$, la cual indica el color de cada una de las piedras. Por ejemplo, si $A = \{\text{negro, blanco}\}$ y $n = 4$, entonces la siguiente función representa un collar donde la primera

¹Para simplificar las cosas, no consideramos reflexiones de los collares, las cuales en realidad deberían incluirse para hacer un modelado más realista del problema.

piedra es negra y las demás son blancas:

$$f = \begin{cases} 1 \mapsto \text{negro} \\ 2 \mapsto \text{blanco} \\ 3 \mapsto \text{blanco} \\ 4 \mapsto \text{blanco} \end{cases}$$

Las etiquetas de los colores son irrelevantes, así que podemos simplificar las cosas considerando $A = \{0, 1, \dots, q-1\}$, siempre que A tenga q colores. Además, podemos identificar una función $f : \mathbb{Z}_n \rightarrow A$ con una n -tupla, donde la i -ésima posición contiene a la imagen de $i \in \mathbb{Z}_n$ bajo f , es decir

$$f = (f(1), f(2), \dots, f(n)).$$

Para el caso $A = \{\text{negro}, \text{blanco}\}$, podemos hacer la identificación $0 = \text{blanco}$ y $1 = \text{negro}$, y la función f , con la primera piedra negra y las demás blancas, queda como

$$f = (1, 0, 0, 0).$$

Consideramos ahora la acción de traslación de \mathbb{Z}_n en $A^{\mathbb{Z}_n}$, dada por

$$k \cdot f(i) := f(i - k), \quad \forall k, i \in \mathbb{Z}_n, f \in A^{\mathbb{Z}_n},$$

donde hay que recordar que la resta $i - k$ se hace módulo n , pues estamos operando elementos del grupo \mathbb{Z}_n . En la notación como n -tuplas, esta acción es equivalente a lo siguiente:

$$k \cdot (f(1), f(2), \dots, f(n)) := (f(1-k), f(2-k), \dots, f(n-k)), \quad \forall k \in \mathbb{Z}_n, f \in A^{\mathbb{Z}_n}.$$

Si $k = 1$, vemos que

$$1 \cdot (f(1), f(2), f(3), \dots, f(n)) = (f(n), f(1), f(2), \dots, f(n-1)),$$

es decir, que la acción de $1 \in \mathbb{Z}_n$ sobre f representa una rotación de un lugar hacia la derecha de los elementos de la n -tupla. Similarmente, la acción de $k \in \mathbb{Z}_n$ sobre f representa una rotación de k lugares hacia la derecha de los elementos de la n -tupla.

La Figura 3.2 muestra a todos los elementos de $A^{\mathbb{Z}_4}$, con $A = \{0, 1\}$, representados por 4-tuplas y agrupados en órbitas bajo la acción de traslación de \mathbb{Z}_4 . Es fácil observar que cada una de estas órbitas representa uno de los collares no equivalentes dados por la Figura 3.1.

Observación 3.30. El número de collares no equivalentes bajo rotaciones que pueden fabricarse con q colores y n piedras es igual al número de órbitas de la acción de traslación de \mathbb{Z}_n sobre $A^{\mathbb{Z}_n}$, donde $|A| = q$.

El siguiente teorema es precisamente lo que necesitamos para resolver este problema, el cual también se conoce como el Lema de Burnside.

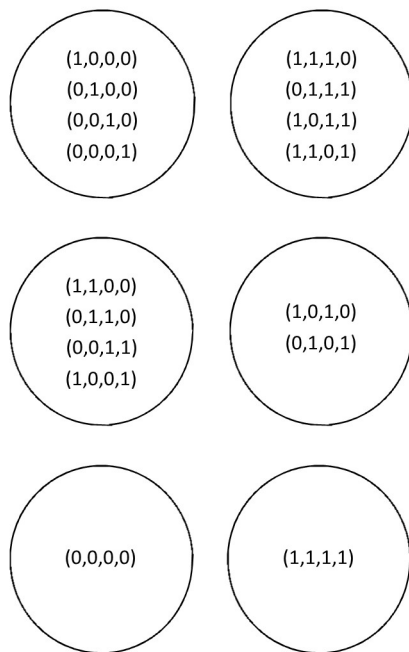


Figura 3.2: Órbitas de la acción de traslación de \mathbb{Z}_4 en $\{0,1\}^{\mathbb{Z}_4}$.

Teorema 3.31 (Cauchy-Frobenius). Sea G un grupo finito que actúa en un conjunto finito X . El número de órbitas de la acción es igual a

$$\frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|,$$

donde $\text{Fix}(g) := \{x \in X : g \cdot x = x\}$ es el conjunto de *puntos fijos* bajo $g \in G$.

Demostración. Consideremos el siguiente conjunto:

$$\mathcal{F} := \{(g, x) \in G \times X : g \cdot x = x\}.$$

Vamos a contar la cardinalidad de \mathcal{F} de dos formas distintas.

1. Por un lado,

$$\mathcal{F} = \bigcup_{g \in G} \{(g, x) : x \in X, g \cdot x = x\}.$$

Debido a que la unión es disjunta, tenemos que

$$\begin{aligned} |\mathcal{F}| &= \sum_{g \in G} |\{(g, x) : x \in X, g \cdot x = x\}| \\ &= \sum_{g \in G} |\{x \in X : g \cdot x = x\}| \\ &= \sum_{g \in G} |\text{Fix}(g)|. \end{aligned}$$

2. Por otro lado,

$$\mathcal{F} = \bigcup_{x \in X} \{(g, x) : g \in G, g \cdot x = x\}.$$

De nuevo la unión es disjunta, así que

$$\begin{aligned} |\mathcal{F}| &= \sum_{x \in X} |\{(g, x) : g \in G, g \cdot x = x\}| \\ &= \sum_{x \in X} |\{g \in G : g \cdot x = x\}| \\ &= \sum_{x \in X} |\text{Stab}(x)| = \sum_{x \in X} \frac{|G|}{|\text{Orb}(x)|}, \end{aligned}$$

donde la última igualdad se deduce del Teorema Órbita-Estabilizador.

Sean O_1, O_2, \dots, O_t las órbitas de la acción de G en X . Debido a que $\text{Orb}(x) = \text{Orb}(y) = O_i$, para toda x y y en una misma órbita O_i , tenemos

$$\begin{aligned} |\mathcal{F}| &= |G| \sum_{x \in X} \frac{1}{|\text{Orb}(x)|} = |G| \sum_{i=1}^t \sum_{x \in O_i} \frac{1}{|\text{Orb}(x)|} \\ &= |G| \sum_{i=1}^t \sum_{x \in O_i} \frac{1}{|O_i|} = |G| \sum_{i=1}^t |O_i| \frac{1}{|O_i|} \\ &= |G| \sum_{i=1}^t 1 = |G|t. \end{aligned}$$

Comparando lo obtenido en los puntos (1.) y (2.) anteriores,

$$|\mathcal{F}| = \sum_{g \in G} |\text{Fix}(g)| = |G|t,$$

donde t es el número de órbitas de la acción. Con esto el teorema queda demostrado. \square

Observación 3.32. El Teorema de Cauchy-Frobenius puede interpretarse de la siguiente forma: el número de órbitas de la acción de G en X es igual al promedio del número de puntos fijos de los elementos de G .

Definición 3.33 (puntos fijos). Sea G un grupo que actúa en X . Para cualquier subconjunto $K \subseteq G$, definimos al conjunto de puntos fijos de K como

$$\text{Fix}(K) := \{x \in X : k \cdot x = x, \forall k \in K\}.$$

Lema 3.34. Sea G un grupo que actúa en X . Para todo $g \in G$,

$$\text{Fix}(g) = \text{Fix}(\langle g \rangle).$$

Demostración. Sea $x \in \text{Fix}(\langle g \rangle)$. Luego, $g^k \cdot x = x$, para toda $k \in \mathbb{Z}$. En particular, $g \cdot x = x$, por lo que $x \in \text{Fix}(g)$. Esto demuestra que $\text{Fix}(\langle g \rangle) \subseteq \text{Fix}(g)$.

Por otro lado, sea $x \in \text{Fix}(g)$. Luego $g \cdot x = x$, y, para toda $k \geq 0$, tenemos

$$g^k \cdot x = \underbrace{g \cdot (g \cdot \dots (g \cdot x))}_{k \text{ veces}} = x.$$

Similarmente, $g \cdot x = x$ implica $g^{-1} \cdot x = x$, por lo que $g^k \cdot x = x$, para toda $k < 0$. Esto demuestra que $x \in \text{Fix}(\langle g \rangle)$, y $\text{Fix}(g) \subseteq \text{Fix}(\langle g \rangle)$. \square

Si H es un subgrupo de G , recordemos que $H \backslash G = \{Hg : g \in G\}$ denota al conjunto de clases laterales derechas de H en G .

Teorema 3.35. Sea A un conjunto, G un grupo y H un subgrupo de G . Respecto a la acción de traslación de G en A^G ,

$$|\text{Fix}(H)| = |A^{H \backslash G}|,$$

donde $A^{H \backslash G}$ es el conjunto de funciones de $H \backslash G$ en A .

Demostración. Definimos una función $\beta : \text{Fix}(H) \rightarrow A^{H \backslash G}$ como sigue: para toda $x \in \text{Fix}(H)$, $\beta(x) \in A^{H \backslash G}$ es la función definida por

$$\beta(x)(Hg) := x(g), \quad \forall Hg \in H \backslash G.$$

Recordemos que $\text{Fix}(H) \subseteq A^G$ en esta acción, por lo que tiene sentido evaluar $x : G \rightarrow A$ en $g \in G$. Demostraremos que β es una biyección bien definida.

1. **β está bien definida.** Para mostrar esto, debemos verificar que para toda $x \in \text{Fix}(H)$, $\beta(x) : H \backslash G \rightarrow A$ es una función bien definida. Supongamos que $Hg_1 = Hg_2$. Luego $g_1 = hg_2$, para algún $h \in H$ y

$$\beta(x)(Hg_1) = x(g_1) = x(hg_2) = (h^{-1} \cdot x)(g_2) = x(g_2) = \beta(x)(Hg_2),$$

donde la penúltima igualdad es cierta ya que $h^{-1} \cdot x = x$, porque $x \in \text{Fix}(H)$.

2. **β es inyectiva.** Supongamos que $\beta(x) = \beta(y)$, para algunos $x, y \in \text{Fix}(H)$. Luego, para toda $g \in G$,

$$x(g) = \beta(x)(Hg) = \beta(y)(Hg) = y(g).$$

Esto implica que $x = y$.

3. β es sobreyectiva. Sea $\hat{x} : H \setminus G \rightarrow A$ un elemento arbitrario de $A^{H \setminus G}$. Definimos $x \in A^G$ por $x(g) := \hat{x}(Hg)$. Observemos que $x \in \text{Fix}(H)$ porque, para toda $h \in H$,

$$(h \cdot x)(g) = x(h^{-1}g) = \hat{x}(Hh^{-1}g) = \hat{x}(Hg) = x(g).$$

Además, x es una preimagen de \hat{x} bajo β , ya que para toda $g \in G$,

$$\beta(x)(Hg) = x(g) = \hat{x}(Hg),$$

lo que implica que $\beta(x) = \hat{x}$.

□

Observación 3.36. Es un resultado básico de técnicas de conteo que

$$|A^G| = |A|^{|G|},$$

debido a que toda función $f \in A^G$ se identifica con la tupla $(f(g) : g \in G)$, y hay $|A|$ posibles entradas para cada posición de la tupla. Similarmente,

$$|A^{H \setminus G}| = |A|^{|H \setminus G|} = |A|^{[G:H]},$$

donde $[G : H]$ es el índice de H en G .

Teorema 3.37 (conteo de collares). El número de collares no equivalentes bajo rotaciones que pueden fabricarse con q colores y n piedras es igual a

$$\frac{1}{n} \sum_{k=1}^n q^{\text{mcd}(k,n)}.$$

Demostración. Sea $c(q, n)$ el número de collares no equivalentes bajo rotaciones que pueden fabricarse con q colores y n piedras. Como observamos anteriormente, $c(q, n)$ es igual al número de órbitas de la acción de traslación de \mathbb{Z}_n en $A^{\mathbb{Z}_n}$, donde $|A| = q$. Por el Teorema de Cauchy-Frobenius,

$$c(q, n) = \frac{1}{|\mathbb{Z}_n|} \sum_{k \in \mathbb{Z}_n} |\text{Fix}(k)| = \frac{1}{n} \sum_{k=1}^n |\text{Fix}(k)|.$$

Por los lemas anteriores, para cualquier $k \in \mathbb{Z}_n$,

$$|\text{Fix}(k)| = |\text{Fix}(\langle k \rangle)| = |A|^{[\mathbb{Z}_n : \langle k \rangle]} = q^{[\mathbb{Z}_n : \langle k \rangle]}.$$

Por el Teorema de Lagrange,

$$[\mathbb{Z}_n : \langle k \rangle] = \frac{|\mathbb{Z}_n|}{|\langle k \rangle|} = \frac{n}{|k|}.$$

Recordemos que, en \mathbb{Z}_n , $|k| = \frac{n}{\text{mcd}(k,n)}$. Por lo tanto, el índice de arriba se simplifica a

$$[\mathbb{Z}_n : \langle k \rangle] = \text{mcd}(k, n).$$

Por lo tanto,

$$c(q, n) = \frac{1}{n} \sum_{k=1}^n q^{\text{mcd}(k, n)}.$$

□

Ejemplo 3.38. El número de collares no equivalentes bajo rotaciones que pueden fabricarse con 2 colores y 4 piedras es

$$\begin{aligned} c(2, 4) &= \frac{1}{4} \left(2^{\text{mcd}(1,4)} + 2^{\text{mcd}(2,4)} + 2^{\text{mcd}(3,4)} + 2^{\text{mcd}(4,4)} \right) \\ &= \frac{1}{4} (2 + 2^2 + 2 + 2^4) = \frac{1}{4} (24) = 6. \end{aligned}$$

Esto coincide con lo obtenido en la Figura 3.1.

Palabras clave: acción de grupo, kernel, acción fiel, teorema de Cayley, órbita, estabilizador, Teorema Órbita-Estabilizador, Teorema de Cauchy-Frobenius, puntos fijos, conteo de collares.

3.1.4. Ejercicios

Ejercicio 3.1. Sea G un grupo que actúa en X . Demuestra que la relación \sim sobre X , definida por $x \sim y$ si y solo si existe $g \in G$ tal que $y = g \cdot x$, es una relación de equivalencia cuyas clases de equivalencia son las órbitas de la acción

Ejercicio 3.2 (1 pt). Sea $\rho : G \rightarrow \text{Sym}(X)$ una acción de G en X . Demuestra que

$$\ker(\rho) = \bigcap_{x \in X} \text{Stab}(x).$$

Ejercicio 3.3. Teniendo una acción izquierda $G \times X \rightarrow X$ dada por $(g, x) \mapsto g \cdot x$, podemos definir una *acción derecha* $X \times G \rightarrow X$ vía $x \bullet g := g^{-1} \cdot x$. Verifica que esto es una acción.

Ejercicio 3.4. Sea H un subgrupo de G . Para toda $g \in G$, demuestra que gHg^{-1} es un subgrupo de G .

Ejercicio 3.5. Sea G un grupo que actúa en un conjunto X . Demuestra que la acción es fiel si y solo si $g_1 \cdot x = g_2 \cdot x, \forall x \in X$, implica que $g_1 = g_2$.

Ejercicio 3.6. Sea G un grupo que actúa en un conjunto X y sea $Y \subseteq X$. Definimos al *estabilizador puntual* de Y como $\text{Stab}(Y) = \{g \in G : g \cdot y = y, \forall y \in Y\}$ y al *estabilizador global* de Y como $\text{Stab}[Y] = \{g \in G : g \cdot y \in Y, \forall y \in Y\}$. Demuestra que $\text{Stab}(Y)$ y $\text{Stab}[Y]$ son subgrupos de G .

Ejercicio 3.7. Sea $\mathbb{R}[x_1, x_2, \dots, x_n]$ el conjunto de polinomios en n variables con coeficientes en \mathbb{R} . Para cualquier $\alpha \in S_n$ y $f(x_1, x_2, \dots, x_n) \in \mathbb{R}[x_1, x_2, \dots, x_n]$, definimos

$$\alpha \cdot f(x_1, x_2, \dots, x_n) = f(x_{\alpha(1)}, x_{\alpha(2)}, \dots, x_{\alpha(n)}).$$

Responde lo siguiente:

1. Esto define una acción de S_n en $\mathbb{R}[x_1, x_2, \dots, x_n]$.
2. Encuentra un polinomio cuyo estabilizador sea igual a S_n , y otro cuyo estabilizador sea el subgrupo trivial $\{(1)\}$ de S_n .

Ejercicio 3.8. Sea A cualquier conjunto y $A^n = \{(a_1, a_2, \dots, a_n) : a_i \in A\}$. Para cualquier $\alpha \in S_n$ y $(a_1, a_2, \dots, a_n) \in A^n$ definimos

$$\alpha \cdot (a_1, a_2, \dots, a_n) = (a_{\alpha^{-1}(1)}, a_{\alpha^{-1}(2)}, \dots, a_{\alpha^{-1}(n)}).$$

Responde lo siguiente:

1. Demuestra que esto define una acción de S_n en A^n .
2. Para el caso $A = \{0, 1, 2\}$ y $n = 3$, encuentra las órbitas $\text{Orb}(0, 1, 2)$, $\text{Orb}(1, 1, 2)$ y $\text{Orb}(0, 0, 0)$.

Ejercicio 3.9. Sea $G := S_n$ y $X := [n]^2 = \{(a, b) : a, b \in [n]\}$, donde $[n] = \{1, 2, \dots, n\}$. Para cualquier $\sigma \in S_n$, $(a, b) \in X$, definimos

$$\sigma \cdot (a, b) := (\sigma(a), \sigma(b)).$$

Responde lo siguiente:

1. Demuestra que esto define una acción de S_n en X . ¿Cuál es el kernel de la acción?
2. Para $n = 4$, encuentra las órbitas $\text{Orb}(2, 2)$ y $\text{Orb}(1, 2)$, así como los estabilizadores $\text{Stab}(2, 2)$ y $\text{Stab}(1, 2)$. En estos casos, verifica que se cumple el Teorema Órbita-Estabilizador.

Ejercicio 3.10. Sea G un grupo que actúa en X . Sean $x, y \in X$ tales que $y = g \cdot x$, para algún $g \in G$. Demuestra que $\text{Stab}(y) = g\text{Stab}(x)g^{-1}$.

Ejercicio 3.11. Sea G un grupo que actúa en X . Decimos que un subconjunto $Y \subseteq X$ es *invariante* si $g \cdot y \in Y$ para toda $g \in G$, $y \in Y$. Demuestra que un subconjunto $Y \subseteq X$ es invariante si y solo si Y es igual a la unión de algunas órbitas de la acción.

Ejercicio 3.12. Sea G un grupo finito que actúa transitivamente en un conjunto X . Demuestra que X debe ser finito y que $|X|$ divide a $|G|$.

Ejercicio 3.13. Sea G un grupo y H un subgrupo de G . Consideremos la acción de G en las clases laterales G/H dada por $g \cdot (aH) := gaH$. Sea $K := \ker(\rho) = \bigcap_{a \in G} aHa^{-1}$ el kernel de la acción. Demuestra que K es el subgrupo normal de G más grande contenido en H (i.e. si K' es un subgrupo normal de G contenido en H , entonces $K' \subseteq K$).

Ejercicio 3.14. Sea G un grupo finito y H un subgrupo de G tal que $[G : H] = n$. Demuestra que existe un subgrupo normal K de G tal que $K \leq H$ y $[G : K]$ divide a $n!$. (*Sugerencia: Usa el ejercicio anterior.*)

Ejercicio 3.15 (*). Sea G un grupo que actúa en un conjunto X y sea H un subgrupo de G . Demuestra que H actúa transitivamente en X si y solo si G actúa transitivamente en X y $G = H\text{Stab}(x)$, para algún $x \in X$.

Ejercicio 3.16. Encuentra el número de órbitas de la acción natural del grupo de permutaciones $G = \langle (1, 3), (2, 4, 6) \rangle$ sobre el conjunto $\{1, 2, 3, 4, 5, 6, 7\}$.

Ejercicio 3.17. Encuentra el número de collares no equivalentes bajo rotaciones que pueden fabricarse con 6 piedras y 3 colores.

Ejercicio 3.18. ¿Cuántos collares no equivalentes pueden fabricarse con 2 colores y 5 piedras? ¿Y con 2 colores y 7 piedras? Encuentra una fórmula sencilla para determinar el número de collares no equivalentes que pueden fabricarse con q colores y p piedras, donde p es un número primo.

Ejercicio 3.19 (★). Sea G un grupo y A un conjunto tal que $|A| \geq 2$. Demuestra que la acción de traslación de G en A^G es fiel.

3.2. Teoría de Sylow

En esta sección estudiaremos tres teoremas nombrados en honor al matemático noruego Peter Ludwig Sylow que nos proveen de información detallada sobre la estructura de subgrupos de un grupo finito.

3.2.1. La ecuación de clase

En todo este capítulo, G siempre será un grupo finito. Recordemos que la clase de conjugación de $x \in G$ es el conjunto $\text{Cl}(x) := \{g x g^{-1} : g \in G\}$. Como vimos en la Sección 3.1.2, las clases de conjugación son las órbitas de la acción de conjugación de G sobre sí mismo.

Teorema 3.39 (ecuación de clase). Sea G un grupo finito. Entonces,

$$|G| = |Z(G)| + \sum_{i=1}^r |\text{Cl}(x_i)|,$$

donde $Z(G)$ es el centro de G y $\text{Cl}(x_1), \dots, \text{Cl}(x_r)$ son las clases de conjugación de G con más de un elemento.

Demostración. Sean $\text{Cl}(x_1), \dots, \text{Cl}(x_s)$ la lista de todas las clases de conjugación de G . Al ser órbitas de la acción por conjugación, forman una partición de G , por lo que

$$|G| = \sum_{i=1}^s |\text{Cl}(x_i)|.$$

Supongamos que $\text{Cl}(x_1), \dots, \text{Cl}(x_r)$ son las clases de conjugación con más de un elemento y $\text{Cl}(x_{r+1}), \dots, \text{Cl}(x_s)$ son las clases de conjugación con exactamente un elemento.

Afirmación. $Z(G) = \bigcup_{i=r+1}^s \text{Cl}(x_i)$.

Demostración. Sea $z \in Z(G)$. Observemos que

$$\text{Cl}(z) = \{g z g^{-1} : g \in G\} = \{z g g^{-1} : g \in G\} = \{z\}.$$

Entonces $|\text{Cl}(z)| = 1$, lo que implica que $\text{Cl}(z) = \text{Cl}(x_i)$ para algún $i \in \{r+1, \dots, s\}$. Así, $z \in \bigcup_{i=r+1}^s \text{Cl}(x_i)$.

Por otro lado, sea $z \in \bigcup_{i=r+1}^s \text{Cl}(x_i)$. Entonces $z \in \text{Cl}(x_i)$, para algún $i \in \{r+1, \dots, s\}$. Por el Lema 3.19, $\text{Cl}(z) = \text{Cl}(x_i)$, así que $|\text{Cl}(z)| = 1$. Luego $g z g^{-1} = z$ para toda $g \in G$, lo que implica que $z \in Z(G)$. \square

Usando la afirmación anterior, concluimos que

$$|G| = \sum_{i=1}^r |\text{Cl}(x_i)| + \sum_{i=r+1}^s |\text{Cl}(x_i)| = \sum_{i=1}^r |\text{Cl}(x_i)| + |Z(G)|.$$

□

Observación 3.40. Aplicando el Teorema Órbita-Estabilizador a la acción por conjugación de G sobre G , podemos escribir la ecuación de clase de una forma alternativa. Dicho teorema establece que, para toda $x \in G$, $|\text{Cl}(x)| = [G : C(x)]$, donde $C(x) = \{g \in G : gxg^{-1} = x\}$ es el centralizador de x . Por lo tanto,

$$|G| = |Z(G)| + \sum_{i=1}^r [G : C(x_i)],$$

donde los $x_i \in G$ son representantes de las clases de conjugación de G con más de un elemento.

Observación 3.41. Cuando G es un grupo finito, el Corolario 3.29 implica que para toda $x \in G$, $|\text{Cl}(x)|$ divide a $|G|$. En otras palabras, la cardinalidad de cualquier clase de conjugación siempre divide a la cardinalidad de G .

Definición 3.42 (p -grupo). Sea p un número primo. Un grupo finito G es un p -grupo si $|G| = p^k$, para algún $k \geq 1$.

Proposición 3.43 (centro de un p -grupo). Sea G un p -grupo. Entonces $Z(G) \neq \{e\}$.

Demostración. Supongamos que $|G| = p^k$ y $|Z(G)| = 1$. Por la ecuación de clase,

$$p^k = 1 + \sum_{i=1}^r |\text{Cl}(x_i)|,$$

donde $\text{Cl}(x_1), \dots, \text{Cl}(x_r)$ son las clases de conjugación de G con más de un elemento. Por la Observación 3.41, $|\text{Cl}(x_i)|$ divide a $|G| = p^k$, así que $|\text{Cl}(x_i)| = p^{k_i}$, para algunos $k_i \geq 0$. Como $|\text{Cl}(x_i)| > 1$, debemos tener que $k_i > 0$. Sustituyendo en la ecuación de arriba,

$$p^k = 1 + \sum_{i=1}^r p^{k_i}$$

$$p \left(p^{k-1} - \sum_{i=1}^r p^{k_i-1} \right) = 1$$

Esto implica que $p \mid 1$, lo cual es imposible. Por lo tanto, $|Z(G)| \neq 1$. □

Corolario 3.44. Sea G un grupo de orden p^2 , donde p es un número primo. Entonces G es abeliano.

Demostración. Por el Teorema de Lagrange, $|Z(G)| \mid |G| = p^2$. La proposición anterior implica que $|Z(G)| \neq 1$, así que $|Z(G)| = p^2$ ó p .

Caso 1 $|Z(G)| = p^2$. En este caso, $Z(G) = G$, lo que implica que G es abeliano.

Caso 2 $|Z(G)| = p$. Recordemos que $Z(G)$ siempre es un subgrupo normal de G . Por el Teorema de Lagrange, $|G/Z(G)| = p$, por lo que $G/Z(G)$ es un grupo cíclico. Por la Proposición 1.97, G debe ser abeliano. Esto implica que $Z(G) = G$, lo cual contradice que $|Z(G)| = p$. Luego, el Caso 2 no puede ocurrir.

□

3.2.2. Teoremas de Sylow

Sea G un grupo finito de orden n . Un corolario del Teorema de Lagrange es que el orden de cualquier elemento de G divide a n . Sin embargo, el recíproco no es verdad; es decir, si d es un divisor de n , no necesariamente existe $g \in G$ tal que $|g| = d$.

Ejemplo 3.45. El grupo alternante A_4 tiene orden 12, pero no tienen ningún elemento de orden 6.

Sin embargo, si p es un divisor primo de n , sí es verdad que debe existir un $g \in G$ tal que $|g| = p$. Comenzamos demostrando este resultado para el caso abeliano.

Teorema 3.46 (Cauchy). Sea G un grupo abeliano de orden n . Si p es un divisor primo de n , entonces G tiene un elemento de orden p .

Demostración. Haremos la demostración por inducción sobre n .

1. *Caso base.* Si $n = 2$, entonces G es cíclico y tiene un elemento de orden 2.
2. *Hipótesis de inducción.* Supongamos que si H es un grupo abeliano tal que $p \mid |H|$ y $|H| < n$, entonces H tiene un elemento de orden p .
3. *Paso de inducción.* Consideremos un elemento no trivial $g \in G$, $g \neq e$. Sea $k := |g|$. Si $p \mid k$, entonces el elemento $g^{k/p}$ tiene orden p . En otro caso, supongamos que $p \nmid k$. Consideremos al grupo abeliano $\overline{G} := G/\langle g \rangle$ (claramente $\langle g \rangle \trianglelefteq G$ porque G es abeliano). Observemos que

$$|\overline{G}| = \frac{n}{k} < n, \quad \text{porque } k \neq 1.$$

Además, como $p \mid n$ y $p \nmid k$, entonces $p \mid \frac{n}{k} = |\overline{G}|$. Por hipótesis de inducción, \overline{G} tiene un elemento de orden p , digamos $a\langle g \rangle \in \overline{G}$. Sea $r := |a|$. Como $(a\langle g \rangle)^r = a^r\langle g \rangle = e\langle g \rangle$, entonces $p \mid r$ (por el Lema 1.25). Por lo tanto, el elemento $a^{r/p} \in G$ tiene orden p .

□

El siguiente teorema se conoce como el Primer Teorema de Sylow, y establece la existencia de p -subgrupos en todo grupo finito.

Teorema 3.47 (Primer Teorema de Sylow). Sea G un grupo finito de orden n y sea p^k una potencia de un primo tal que $p^k \mid n$. Entonces G tiene un subgrupo de orden p^k .

Demostración. Nuevamente, haremos la demostración por inducción sobre n .

1. *Caso base.* El resultado es trivialmente verdadero cuando $n = 2$.
2. *Hipótesis de inducción.* Supongamos que si H es un grupo tal que $|H| < n$ y p^r es una potencia de un primo tal que $p^r \mid |H|$, entonces H tiene un subgrupo de orden p^r .
3. *Paso de inducción.* Dividimos este paso en dos casos:

- **Caso 1:** $p \mid |Z(G)|$. Puesto que $Z(G)$ es abeliano, el Teorema de Cauchy implica que existe $z \in Z(G)$ tal que $|z| = p$. Como $\langle z \rangle \triangleleft G$, entonces $\overline{G} := G/\langle z \rangle$ es un grupo. Observemos que

$$|\overline{G}| = \frac{n}{p} < n,$$

y que $p^{k-1} \mid |\overline{G}|$. Por hipótesis de inducción, \overline{G} contiene un subgrupo \overline{H} de orden p^{k-1} . Por el Teorema de Correspondencia (Ejercicio 1.74), existe un subgrupo H tal que $\langle z \rangle \leq H \leq G$ y

$$\overline{H} = H/\langle z \rangle.$$

(De hecho, $H := \{g \in G : g(z) \in \overline{H}\}$). Luego, $|H| = |\overline{H}||\langle z \rangle| = p^{k-1}p = p^k$, y el resultado queda establecido en este caso.

- **Caso 2:** $p \nmid |Z(G)|$. Consideremos la ecuación de clase de G :

$$|G| = |Z(G)| + \sum_{i=1}^r |\text{Cl}(x_i)|,$$

donde $\text{Cl}(x_1), \dots, \text{Cl}(x_r)$ son las clases de conjugación de G con más de un elemento. Si $p \mid |\text{Cl}(x_i)|$ para toda i , entonces

$$p \mid \left(|G| - \sum_{i=1}^r |\text{Cl}(x_i)| \right) = |Z(G)|,$$

lo cual es una contradicción. Luego, debe existir un s tal que $p \nmid |\text{Cl}(x_s)|$. Por el Teorema Órbita-Estabilizador,

$$|\text{Cl}(x_s)| = [G : C(x_s)] \Rightarrow |C(x_s)| = \frac{|G|}{|\text{Cl}(x_s)|}.$$

Como $p^k \mid |G|$ pero $p \nmid |\text{Cl}(x_s)|$, entonces $p^k \mid |C(x_s)|$. Además, $|C(x_s)| < n$ porque $|\text{Cl}(x_s)| > 1$. Por hipótesis de inducción, $C(x_s)$ tiene un subgrupo de orden p^k , el cual también es un subgrupo de G .

□

Corolario 3.48. Sea G un grupo finito de orden n . Si p es un número primo tal que $p \mid n$, entonces G tiene un elemento de orden p .

Demostración. Por el Primer Teorema de Sylow, G tiene un subgrupo de orden p . Como todo grupo de orden primo es cíclico, G tiene un elemento de orden p . □

Ejemplo 3.49. Todo grupo de orden 21 tiene al menos un elemento de orden 3 y al menos un elemento de orden 7.

Ejemplo 3.50. Todo grupo de orden $360 = 2^3 \cdot 3^2 \cdot 5$ tiene subgrupos de los siguientes órdenes: 2, 2^2 , 2^3 , 3, 3^2 y 5.

Definición 3.51 (p -subgrupo de Sylow). Sea G un grupo finito de orden n y p un número primo tal que $p \mid n$. Un p -subgrupo de Sylow de G es un subgrupo de G cuyo orden es igual a la máxima potencia de p que divide a n ; en otras palabras, es un subgrupo H tal que $|H| = p^m$ donde $p^m \mid n$ pero $p^{m+1} \nmid n$.

Ejemplo 3.52. Sea G un grupo de orden $360 = 2^3 \cdot 3^2 \cdot 5$. Entonces, un 2-subgrupo de Sylow de G tiene orden $2^3 = 8$, un 3-subgrupo de Sylow de G tiene orden $3^2 = 9$, y un 5-subgrupo de Sylow de G tiene orden 5.

Observación 3.53. Por el Primer Teorema de Sylow, si p es un primo que divide al orden de G , entonces siempre existe al menos un p -subgrupo de Sylow de G .

Observación 3.54. Sea P un p -subgrupo de Sylow de G . Para cualquier $g \in G$, recordemos que el conjugado gPg^{-1} también es un subgrupo de G (Ejercicio 3.4). Además, puesto que $|P| = |gPg^{-1}|$ (ya que $a \mapsto gag^{-1}$ es una biyección de P a gPg^{-1}), deducimos que gPg^{-1} también es un p -subgrupo de Sylow de G (ya que su orden también es la máxima potencia de p que divide a $|G|$). En conclusión, el conjugado de un p -subgrupo de Sylow siempre es un p -subgrupo de Sylow.

Teorema 3.55 (Segundo Teorema de Sylow). Sea G un grupo finito de orden n y p un número primo tal que $p \mid n$. Sea H un subgrupo de G tal que $|H| = p^k$, para algún $k \geq 1$, y sea P un p -subgrupo de Sylow de G . Entonces existe $g \in G$ tal que $H \leq gPg^{-1}$.

Demostración. Consideremos la acción de H sobre el conjunto de clases laterales $G/P = \{gP : g \in G\}$ por multiplicación izquierda, es decir, $h \cdot gP := hgP$, para toda $h \in H$, $gP \in G/P$. Como las órbitas O_1, \dots, O_r de la acción forman una partición de G/P , tenemos

$$|G/P| = |O_1| + \dots + |O_r|$$

Por el Corolario 3.29, $|O_i|$ divide a $|H| = p^k$ para toda i . Por lo tanto, $|O_i| = p^{m_i}$ para $0 \leq m_i \leq k$. Observemos que $p \nmid |G/P| = \frac{|G|}{|P|}$ porque P es un p -subgrupo de Sylow de G . Si $m_i \geq 1$ para toda i , entonces

$$p = \sum_{i=1}^r p^{m_i} = \sum_{i=1}^r |O_i| = |G/P|,$$

lo cual es una contradicción. Luego, debe existir al menos una órbita O_j con $m_j = 0$, es decir, $|O_j| = p^{m_j} = p^0 = 1$. Así, $O_j = \{gP\}$ para algún $g \in G$. Entonces, para cualquier $h \in H$, $hgP = gP$, así que $hg = ga$ para algún $a \in P$. Esto implica que, para toda $h \in H$,

$$h = gag^{-1} \in gPg^{-1}.$$

Por lo tanto, $H \leq gPg^{-1}$. □

Corolario 3.56. Para cualquier par P_1 y P_2 de p -subgrupos de Sylow de G existe $g \in G$ tal que $P_1 = gP_2g^{-1}$.

Demostración. Aplicamos el Segundo Teorema de Sylow con $H = P_1$ y $P_2 = P$ para obtener $g \in G$ tal que $P_1 \leq gP_2g^{-1}$. Como P_1 y gP_2g^{-1} son p -subgrupos de Sylow (ver Observación 3.54), deben tener el mismo orden, así que $P_1 = gP_2g^{-1}$. □

Observación 3.57. Sea

$$\text{Syl}_p(G) := \{P \leq G : P \text{ es } p\text{-subgrupo de Sylow}\}.$$

Respecto a la acción por conjugación de G sobre sus subgrupos, la Observación 3.54 implica que $\text{Syl}_p(G)$ es invariante (ver Ejercicio 3.11 para la definición de *invariante*), y el corolario anterior muestra que $\text{Syl}_p(G)$ está constituido por una sola órbita; en otras palabras, la acción por conjugación de G sobre $\text{Syl}_p(G)$ es transitiva.

Recordemos que el normalizador de un subgrupo $H \leq G$ es el subgrupo $N(H) := \{g \in G : gHg^{-1} = H\}$.

Teorema 3.58 (Tercer Teorema de Sylow). Sea G un grupo finito de orden n y p un número primo tal que $p \mid n$. Sea $n_p := |\text{Syl}_p(G)|$ el número total de p -subgrupos de Sylow de G . Entonces,

$$n_p = [G : N(P)] \quad \text{y} \quad n_p \equiv 1 \pmod{p},$$

donde P es cualquier p -subgrupo de Sylow de G .

Demostración. Consideremos la acción por conjugación de G sobre $\text{Syl}_p(G)$. Por la Observación 3.57, esta acción es transitiva, así que por el Teorema Órbita-Estabilizador

$$n_p := |\text{Syl}_p(G)| = |\text{Orb}(P)| = [G : N(P)],$$

donde P es cualquier p -subgrupo de Sylow de G .

Para demostrar la segunda igualdad, fijamos $P \in \text{Syl}_p(G)$ y consideramos la acción por conjugación de P sobre $\text{Syl}_p(G)$. Claramente $aPa^{-1} = P$, para toda $a \in P$, así que $\{P\}$ es una órbita de cardinalidad 1.

Afirmación. En la acción por conjugación de P sobre $\text{Syl}_p(G)$, $\{P\}$ es la única órbita de cardinalidad 1.

Demostración. Supongamos que $\{S\}$ es otra órbita con un elemento. Luego, $aSa^{-1} = S$ para toda $a \in P$, lo que implica que $P \leq N(S)$. También es claro que $S \leq N(S)$, lo que muestra que P y S son p -subgrupos de Sylow de $N(S)$. Por el corolario del Segundo Teorema de Sylow, existe $h \in N(S)$ tal que $P = hSh^{-1}$. Pero $hSh^{-1} = S$, por definición del normalizador de S , lo que demuestra que $P = S$. \square

Sean $O_1 = \{P\}, O_2, \dots, O_r$ las órbitas de la acción por conjugación de P sobre $\text{Syl}_p(G)$. Entonces,

$$n_p := |\text{Syl}_p(G)| = 1 + \sum_{i=2}^r |O_i|,$$

Para toda $i = 2, \dots, r$, sabemos que $|O_i| \neq 1$ y el Corolario 3.29 implica que $|O_i| \mid |P| = p^m$. Luego, $p \mid |O_i|$ para toda $i = 2, \dots, r$. Por lo tanto,

$$p \mid \sum_{i=2}^r |O_i| = n_p - 1,$$

lo que implica que $n_p \equiv 1 \pmod{p}$. \square

Corolario 3.59. El grupo G tiene un único p -subgrupo de Sylow P si y solo si $P \trianglelefteq G$.

Demostración. El subgrupo P es único si y solo si $n_p = 1$. Por el Tercer Teorema de Sylow, $n_p = [G : N(P)]$. Luego, $n_p = 1 = [G : N(P)]$ si y solo si $N(P) = G$, lo cual se cumple si y solo si $P \trianglelefteq G$ (ver Ejercicio 1.51). \square

Observación 3.60. Sea n_p el número de p -subgrupos de Sylow de G y sea P un p -subgrupo de Sylow de G . El Tercer Teorema de Sylow establece que $n_p = [G : N(P)]$, por lo que el Teorema de Lagrange implica que

$$n_p \mid |G|.$$

Además, como $P \leq N(P)$, deducimos que

$$\frac{|G|}{|N(P)|} \leq \frac{|G|}{|P|} \Rightarrow n_p \leq [G : P].$$

Ejemplo 3.61. Sea G un grupo de orden 48 y sea P un 2-subgrupo de Sylow de G . Entonces, $|P| = 2^4 = 16$. Sea n_2 el número total de 2-subgrupos de Sylow de G . Por la observación anterior, $n_2 \leq \frac{|G|}{|P|} = \frac{48}{16} = 3$ y $n_2 \mid 48$. Luego, $n_2 \in \{1, 2, 3\}$. Además, por el Tercer Teorema de Sylow, $n_2 \equiv 1 \pmod{2}$. Por lo tanto, G puede tener un único 2-subgrupo de Sylow o exactamente tres 2-subgrupos de Sylow.

3.2.3. Aplicaciones de la teoría de Sylow

Como una primera aplicación, usaremos la teoría de Sylow para demostrar que grupos de ciertos órdenes no pueden ser *simples*.

Definición 3.62 (grupo simple). Un grupo G es *simple* si sus únicos subgrupos normales son $\{e\}$ y G mismo.

En otras palabras, un grupo es simple si y solo si no tiene subgrupos normales propios no triviales.

Proposición 3.63. Ningún grupo de orden 15 es simple.

Demostración. Sea G un grupo de orden 15 y sea P un 5-subgrupo de Sylow de G , así que $|P| = 5$. Sea n_5 el número de 5-subgrupos de Sylow de G . Por el Tercer Teorema de Sylow y la Observación 3.60,

$$n_5 \mid |G| = 15, \quad n_5 \leq [G : P] = 3 \quad \text{y} \quad n_5 \equiv 1 \pmod{5}.$$

Las primeras dos igualdades implican que $n_5 = 1$ o $n_5 = 3$, pero como $3 \not\equiv 1 \pmod{5}$, concluimos que $n_5 = 1$. Por el Corolario 3.59, P es normal en G , por lo que G no es simple. \square

Proposición 3.64. Ningún grupo de orden 30 es simple.

Demostración. Sea G un grupo de orden 30, y sean P_3 y P_5 unos 3- y 5-subgrupos de Sylow de G , respectivamente. Luego, $|P_3| = 3$ y $|P_5| = 5$. Por la Observación 3.60,

$$n_3, n_5 \mid 30, \quad n_3 \leq [G : P_3] = 10, \quad n_5 \leq [G : P_5] = 6.$$

Así, $n_3 \in \{1, 2, 3, 5, 6, 10\}$ y $n_5 \in \{1, 2, 3, 5, 6\}$. Por el Tercer Teorema de Sylow, $n_3 \equiv 1 \pmod{3}$ y $n_5 \equiv 1 \pmod{5}$, así que

$$n_3 \in \{1, 10\} \quad \text{y} \quad n_5 \in \{1, 6\}.$$

Si $n_3 = 1$ ó $n_5 = 1$, el Corolario 3.59 establece que P_3 o P_5 son normales en G , respectivamente, por lo que G no es simple. Supongamos que $n_3 \neq 1$ y $n_5 \neq 1$, así que $n_3 = 10$ y $n_5 = 6$. Esto significa que G tiene 10 subgrupos de orden 3 y 6 subgrupos de orden 5. Todos esos subgrupos de G son cíclicos y la intersección entre cualquier par distinto de ellos es trivial (por el Teorema de Lagrange). Por lo tanto, G tiene $6 \times (5 - 1) = 24$ elementos de orden 5 y $10 \times (3 - 1) = 20$

elementos de orden 3, lo cual es imposible, pues G tiene 30 elementos en total. \square

La teoría de Sylow nos permite describir completamente la estructura de algunos grupos por el solo hecho de conocer su orden. Para lograr esto, primero es importante poder reconocer cuándo un grupo es isomorfo a la suma directa de dos de sus subgrupos.

Recordemos que si $H, K \leq G$ son subgrupos de un grupo G , su producto es $HK := \{hk : h \in H, k \in K\}$, el cual no necesariamente es un subgrupo de G . Sin embargo, si H o K son normales en G , entonces $HK = KH$ y HK es un subgrupo de G (ver Ejercicio 1.53).

Teorema 3.65 (suma directa interna). Sea G un grupo y $H, K \leq G$ subgrupos que satisfacen lo siguiente:

1. $H \trianglelefteq G$ y $K \trianglelefteq G$.
2. $G = HK$.
3. $H \cap K = \{e\}$.

Entonces,

$$G \cong H \oplus K.$$

Demostración. Definimos una función $\beta : G \rightarrow H \oplus K$ como

$$\beta(hk) = (h, k), \quad \forall hk \in G.$$

Esta función está definida en todo G porque $G = HK$ por el punto (2.) de la hipótesis. Demostraremos que β es un isomorfismo.

1. *Está bien definida.* Supongamos que $h_1k_1 = h_2k_2$, para algunos $h_i \in H$, $k_i \in K$. Por el punto (3.),

$$h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K = \{e\},$$

lo que implica que $h_2^{-1}h_1 = e$ y $k_2k_1^{-1} = e$. Luego, $h_1 = h_2$ y $k_1 = k_2$. Por lo tanto, $\beta(h_1k_1) = (h_1, k_1) = (h_2, k_2) = \beta(h_2k_2)$.

2. *Es un homomorfismo.* Consideremos el conmutador $[h, k] := hkh^{-1}k^{-1}$ de cualquier par de elementos $h \in H$, $k \in K$. Como H y K son subgrupos normales por el punto (1.):

$$[h, k] = \underbrace{(hkh^{-1})}_{\in K} k^{-1} \in K,$$

$$[h, k] = h \underbrace{(kh^{-1}k^{-1})}_{\in H} \in H.$$

Así, $[h, k] \in K \cap H = \{e\}$, por el punto (3.). Despejando, obtenemos que

$$hk = kh, \quad \forall h \in H, k \in K.$$

Con esto podemos demostrar que β es un homomorfismo:

$$\begin{aligned}\beta((h_1k_1)(h_2k_2)) &= \beta(h_1h_2k_1k_2) \\ &= (h_1h_2, k_1k_2) \\ &= (h_1, k_1)(h_2, k_2) \\ &= \beta(h_1k_1)\beta(h_2k_2),\end{aligned}$$

para toda $h_i \in H, k_i \in K$.

3. *Es inyectiva.* Supongamos que $\beta(h_1k_1) = \beta(h_2k_2)$. Entonces $(h_1, k_1) = (h_2, k_2)$, por lo que $h_1 = h_2$ y $k_1 = k_2$. Por lo tanto, $h_1k_1 = h_2k_2$.
4. *Es sobreyectiva.* La preimagen de cualquier $(h, k) \in H \oplus K$ bajo β es $hk \in G$.

□

Corolario 3.66 (suma directa interna). Sea G un grupo y H_1, H_2, \dots, H_m subgrupos de G que satisfacen lo siguiente:

1. $H_i \trianglelefteq G$, para toda $i = 1, \dots, m$.
2. $G = H_1H_2 \dots H_m$.
3. $(H_1H_2 \dots H_i) \cap H_{i+1} = \{e\}$, para toda $i = 1, \dots, m-1$.

Entonces,

$$G \cong H_1 \oplus H_2 \oplus \dots \oplus H_m.$$

Demostración. Haremos la demostración por inducción sobre m .

1. *Caso base.* Si $m = 2$, el resultado queda establecido por el teorema anterior.
2. *Hipótesis de inducción.* Supongamos que el resultado se cumple para $m-1$.
3. *Paso de inducción.* Aplicamos el teorema anterior con $H := H_1H_2 \dots H_{m-1}$ y $K := H_m$. Es fácil verificar que $H \trianglelefteq G$. Además, por hipótesis del corolario, $K \trianglelefteq G$, $G = HK$ y $H \cap K = \{e\}$. Por hipótesis de inducción, $H \cong H_1 \oplus \dots \oplus H_{m-1}$. Por lo tanto,

$$G \cong H \oplus K \cong H_1 \oplus H_2 \oplus \dots \oplus H_{m-1} \oplus H_m.$$

□

Proposición 3.67. Si G es un grupo de orden 15, entonces G es cíclico.

Demostración. Por el Primer Teorema de Sylow, G tiene un 3-subgrupo de Sylow H de orden 3 y un 5-subgrupo de Sylow K de orden 5. Luego, $H \cong \mathbb{Z}_3$ y $K \cong \mathbb{Z}_5$. Usaremos el Teorema 3.65 para probar que

$$G \cong H \oplus K \cong \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{15},$$

donde la última isomorfía se da porque $\text{mcd}(3, 5) = 1$. Verificamos que se cumplen las hipótesis del Teorema 3.65:

1. Sea n_3 el número de 3-subgrupos de Sylow de G y n_5 el número de 5-subgrupos de Sylow de G . Por la Observación 3.60,

$$n_3 = \frac{|G|}{|N_G(H)|} \leq \frac{|G|}{|H|} = 5 \quad \text{y} \quad n_3 \mid 15,$$

$$n_5 = \frac{|G|}{|N_G(K)|} \leq \frac{|G|}{|K|} = 3 \quad \text{y} \quad n_5 \mid 15.$$

Luego, $n_3 \in \{1, 3, 5\}$ y $n_5 \in \{1, 3\}$. Además, por el Tercer Teorema de Sylow debemos tener que

$$n_3 \equiv 1 \pmod{3} \quad \text{y} \quad n_5 \equiv 1 \pmod{5}.$$

Entonces $n_3 = 1$ y $n_5 = 1$. Por el Corolario 3.59, $H \triangleleft G$ y $K \triangleleft G$.

2. Como $H \cap K$ es un subgrupo de ambos H y K , su orden debe dividir $|H| = 3$ y $|K| = 5$. Entonces, $|H \cap K| = 1$ y $H \cap K = \{e\}$.
3. Para demostrar que $G = HK$ usamos la fórmula para $|HK|$ dada por el Ejercicio 1.42

$$|HK| = \frac{|H||K|}{|H \cap K|} = \frac{3 \cdot 5}{1} = 15.$$

Por lo tanto, $|G| = |HK|$ y $G = HK$ (pues $HK \subseteq G$ y G es finito).

□

La demostración puede generalizarse para demostrar que si G un grupo de orden pq donde p y q son números primos, $p < q$ y p no divide a $q - 1$, entonces G debe ser cíclico (Ejercicio 3.28).

Palabras clave: ecuación de clase, p -grupo, Teorema de Cauchy, Teoremas de Sylow, p -subgrupo de Sylow, grupo simple, producto directo interno.

3.2.4. Ejercicios

Ejercicio 3.20. Sea H un subgrupo normal de G . Muestra que si ambos H y G/H son p -grupos, entonces G es un p -grupo.

Ejercicio 3.21. Encuentra todos los 3-subgrupos de Sylow de \mathbb{Z}_{18} y todos los 3-subgrupos de Sylow de S_4 .

Ejercicio 3.22. Sea G un grupo abeliano finito. Muestra que G tiene un único p -subgrupo de Sylow para cada divisor primo p de $|G|$.

Ejercicio 3.23. Sea G un grupo de orden 1925. Si G tiene más de un 5-subgrupo de Sylow, entonces ¿exactamente cuántos 5-subgrupos de Sylow tiene?

Ejercicio 3.24. Supongamos que G es un grupo de orden $p^k m$, donde p es un primo y $p > m$. Demuestra que cualquier p -subgrupo de Sylow de G debe ser normal en G .

Ejercicio 3.25. Sea G un grupo finito. Para cada divisor primo p_i de $|G|$, sea P_i un p_i -subgrupo de Sylow de G . Demuestra que G es generado por la unión $\bigcup_i P_i$; en otras palabras,

$$G = \left\langle \bigcup_i P_i \right\rangle.$$

Ejercicio 3.26. Demuestra que si un grupo finito G tiene un único p -subgrupo de Sylow para cada divisor primo p de $|G|$, entonces G es isomorfo a la suma directa de sus subgrupos de Sylow.

Ejercicio 3.27. Sea K un p -subgrupo de Sylow de G . Demuestra que si $g \in N_G(K)$ y el orden de g es una potencia de p , entonces $g \in K$.

Ejercicio 3.28 (2 pts). Sea G un grupo de orden pq donde p y q son números primos, $p < q$ y p no divide a $q - 1$. Demuestra que G debe ser cíclico. (*Sugerencia: Usa el Teorema de la Suma Directa Interna.*)

Ejercicio 3.29. Sea G un grupo que actúa en un conjunto finito X . Generaliza la ecuación de clase para la acción de G en X , y úsala para demostrar que si G es un p -grupo, entonces

$$|X| \equiv |\text{Fix}(G)| \pmod{p}.$$

Ejercicio 3.30. Describe todos los 3-subgrupos de Sylow de A_4 y todos los 3-subgrupos de Sylow de S_4 .

Ejercicio 3.31. Sea G un grupo de orden 36 no abeliano. Demuestra que G tiene más de un 2-subgrupo de Sylow o más de un 3-subgrupo de Sylow.

Ejercicio 3.32. Sea G un grupo finito. Para cada divisor primo p_i de $|G|$, sea P_i un p_i -subgrupo de Sylow de G . Demuestra que G es generado por la unión $\bigcup_i P_i$; es decir,

$$G = \left\langle \bigcup_i P_i \right\rangle.$$

Ejercicio 3.33. Demuestra que si un grupo finito G tiene un único p -subgrupo de Sylow para cada divisor primo p de $|G|$, entonces G es isomorfo a la suma directa de sus subgrupos de Sylow.

Ejercicio 3.34. Sea G un grupo de orden 2907. Demuestra que G no es simple.

Ejercicio 3.35 (*). Sea H un subgrupo de G y P un subgrupo de Sylow de G . Demuestra que si $N_G(P) \leq H$, entonces $H = N_G(H)$.

Ejercicio 3.36 (*). Sea K un p -subgrupo de Sylow de G . Demuestra que si $g \in N(K)$ y el orden de g es una potencia de p , entonces $g \in K$.

Ejercicio 3.37. Demuestra que todo grupo no abeliano de orden 10 es isomorfo a D_{10} . (Sugerencia: Usa la teoría de Sylow y el hecho de que $D_{10} = \langle a, b : a^2 = b^5 = e, aba = b^{-1} \rangle$).

3.3. Demostración del Teorema Fundamental de Grupos Abelianos Finitos

Nuestro objetivo en esta sección es demostrar el siguiente teorema.

Teorema 3.68 (Teorema Fundamental de Grupos Abelianos Finitos). Todo grupo abeliano finito es isomorfo a una suma directa de grupos cíclicos.

Sea G un grupo abeliano finito. Por el Ejercicio 3.26, sabemos que G es isomorfo a la suma directa de sus subgrupos de Sylow; es decir,

$$G = P_1 \oplus P_2 \oplus \cdots \oplus P_r,$$

donde P_i es el p_i -subgrupo de Sylow de G . Por lo tanto, para demostrar el Teorema 3.68, debemos estudiar más a fondo la estructura de los p -grupos abelianos finitos, y demostrar que todo p -grupo abeliano es isomorfo a una suma directa de grupos cíclicos.

Lema 3.69. Sea G un p -grupo abeliano finito. Si G tiene un único subgrupo de orden p , entonces G es cíclico.

Demostración. Supongamos que $|G| = p^n$, y procederemos por inducción sobre n .

Caso base: Si $n = 1$, entonces G es cíclico.

Hipótesis de inducción: Supongamos que el lema se cumple para todo p -grupo abeliano de orden p^k con $k < n$.

Paso de inducción: Consideremos el endomorfismo

$$\phi : G \rightarrow G \quad \text{dado por} \quad \phi(g) = g^p, \quad \forall g \in G.$$

Sea $K := \ker(\phi) = \{g \in G : g^p = e\}$. Usando la hipótesis del lema, sea $H \cong \mathbb{Z}_p$ el único subgrupo de G de orden p . Claramente, $H \leq K$, porque todos los elementos de H tienen orden p . Por otro lado, para cualquier $k \in K$, el subgrupo $\langle k \rangle$ tiene orden p , así que $\langle k \rangle = H$ por unicidad. Luego $k \in H$, lo que demuestra que $K = H$. Si $G = K$, entonces $G \cong \mathbb{Z}_p$ es cíclico, como se quería demostrar. Por otro lado, si $K < G$, entonces $\phi(G) \cong G/K$ es un subgrupo propio no trivial de G . Por el Teorema de Cauchy, $\phi(G)$ tiene un subgrupo de orden p , y como todo subgrupo de $\phi(G)$ es subgrupo de G , sabemos que $\phi(G)$ tiene un único subgrupo de orden p (que es K). Por hipótesis de inducción, $\phi(G) \cong G/K$ es cíclico, así que digamos que $G/K = \langle gK \rangle$. Demostraremos que $G = \langle g \rangle$. De nuevo por el Teorema de Cauchy, $\langle g \rangle$ tiene un subgrupo de orden p , el cual, por unicidad, debe ser K ; es decir, $K \leq \langle g \rangle$. Así, para cualquier $a \in G$ existe $i \in \mathbb{Z}$ tal que $aK = g^iK$. Pero esto implica que $a = g^ik$, para algún $k \in K \leq \langle g \rangle$, así que nuevamente existe $j \in \mathbb{Z}$ tal que $k = g^j$. Luego, $a = g^{i+j} \in \langle g \rangle$, lo que demuestra que $G = \langle g \rangle$.

□

Lema 3.70. Sea G un p -grupo abeliano finito y sea $a \in G$ un elemento de orden máximo. Entonces existe $H \leq G$ tal que

$$G \cong \langle a \rangle \oplus H.$$

Demostración. Procederemos nuevamente por inducción sobre $|G|$.

Caso base: Si $n = 1$, entonces G es cíclico y $G \cong \langle a \rangle \oplus \langle e \rangle$.

Hipótesis de inducción: Supongamos que el lema se cumple para todo p -grupo abeliano \bar{G} de orden $|\bar{G}| < |G|$.

Paso de inducción: Si G es cíclico no hay nada que hacer, así que supongamos que G no es cíclico. Por el lema anterior, G tiene más de un subgrupo de orden p , mientras que $A := \langle a \rangle$ tiene un único subgrupo de orden p . Luego, sea $K \leq G$ el subgrupo de orden p que no está contenido en A . Luego, $K \cap A = \{e\}$. Por el Segundo Teorema de Isomorfía (Ejercicio 1.72),

$$\frac{AK}{K} \cong \frac{A}{K \cap A} \cong A.$$

Como A es un subgrupo cíclico de G de orden máximo, entonces $AK/K \cong A$ es un subgrupo cíclico de G/K de orden máximo. Aplicando la hipótesis de inducción a G/K , deducimos que existe $\bar{H} \leq G/K$ tal que

$$G/K = (AK/K) \oplus \bar{H}.$$

Sea $H \leq G$ la preimagen de \bar{H} bajo el homomorfismo natural de G a G/K ; es decir, $H = \{g \in G : gK \in \bar{H}\}$, el cual cumple que $K \leq H \leq G$. Por la igualdad de arriba, para toda $g \in G$, existen $a^i \in A$ y $h \in H$ tales que

$$gK = (a^i K)(hK) = a^i hK \implies g = a^i h k, \text{ para algún } k \in K.$$

Como $hk \in H$ porque $K \leq H$, esto demuestra que $G = AH$. Además, $(AK/K) \cap \bar{H} = \{eK\}$ implica que $(AK) \cap H = K$, y por lo tanto $A \cap H = \{e\}$ (ya que $K \cap A = \{e\}$). Por el Teorema de la Suma Directa Interna concluimos que $G = A \oplus H$.

□

Corolario 3.71. Todo p -grupo abeliano finito es isomorfo a una suma directa de grupos cíclicos.

A

Apéndice A: Prerrequisitos

En esta sección enunciamos algunas definiciones y teoremas importantes que son necesarios para comprender la parte principal del texto. Omitimos la mayoría de las demostraciones, las cuales pueden consultarse en [1].

A.1. Teoría de números elemental

Sea $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ el conjunto de los *números enteros* y sea $\mathbb{N} = \{0, 1, 2, \dots\}$ el conjunto de los *números naturales*.

Definición A.1 (Divisor). Sean $a, b \in \mathbb{Z}$, con $a \neq 0$. Decimos que a es divisor (o factor) de b si existe $t \in \mathbb{Z}$ tal que $b = at$. Escribimos $a \mid b$ si a es divisor de b , y $a \nmid b$ si a no es divisor de b .

Si $a \mid b$, también decimos que b es *múltiplo* de a , o que b es *divisible* entre a .

La definición de divisor involucra a la multiplicación y no a la división, como su podría sugerir. La razón de esto es que la división no es una operación bien definida en \mathbb{Z} ; es decir, la división de dos números enteros no siempre es un entero. De cualquier forma, en ocasiones podría resultar cómodo pensar que a es divisor de b , si división a/b pertenece a \mathbb{Z} . Por ejemplo, 5 es divisor de 10 porque $10 = 5 \cdot 2$, o, equivalentemente, porque $10/5 = 2$ es un entero.

Ejemplo A.2. Consideremos los siguientes ejemplos.

1. $1 \mid n$ para toda $n \in \mathbb{Z}$, porque $n = 1 \cdot n$.
2. $n \mid 0$ para toda $n \in \mathbb{Z}$, porque $0 = 0 \cdot n$.
3. Si $2n \in 2\mathbb{Z}$ es un número par, claramente $2 \mid 2n$.

Definición A.3 (Número Primo). Sea $p \in \mathbb{Z}$, $p > 1$. Decimos que p es un *número primo* si sus únicos divisores positivos son 1 y él mismo.

Definición A.4 (Compuesto). Si $t \in \mathbb{Z}$, $t > 1$, no es un número primo, decimos que t es un *número compuesto*.

Las siguientes son algunas propiedades básicas de la divisibilidad.

Lema A.5 (Divisibilidad). Sean $a, b, c \in \mathbb{Z}$.

1. Si $a \mid b$ y $b \mid c$, entonces $a \mid c$
2. Si $c \mid a$ y $c \mid b$ entonces $c \mid (au + bv)$ para todo $u, v \in \mathbb{Z}$
3. $a \mid b$ y $b \mid a$ si y solo si $a = \pm b$

El siguiente es un resultado importante, cuya demostración se estudia normalmente en un curso de teoría de números elemental.

Teorema A.6 (Algoritmo de la División). Sean $a, b \in \mathbb{Z}$, $b > 0$. Entonces existen únicos enteros q y r tales que

$$a = bq + r$$

donde $0 \leq r < b$.

En el algoritmo de la división, el entero q es llamado el *cociente* de a entre b , mientras que r es llamado el *residuo*.

Ejemplo A.7. Consideremos los siguientes ejemplos.

1. Si $a = -5$ y $b = 2$, entonces $a = -3b + 1$.
2. Si $a = 0$ y $b = 250$, entonces $a = 0b + 0$.
3. Si $a = 23$ y $b = 5$, entonces $a = 4b + 3$.

Definición A.8 (Máximo Común Divisor). Sean $a, b \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$. Decimos que $d \in \mathbb{Z}$, $d > 1$, es el máximo común divisor de a y b , si se cumplen las siguientes propiedades:

1. Es divisor común: $d \mid a$ y $d \mid b$.
2. Si c es un entero tal que $c \mid a$ y $c \mid b$, entonces $c \mid d$.

Denotamos al máximo común divisor de a y b como $\text{mcd}(a, b)$.

Definición A.9 (Primos Relativos). Decimos que $a, b \in \mathbb{Z}$ son *primos relativos* si $\text{mcd}(a, b) = 1$.

Una forma de obtener el máximo común divisor de dos números es escribir todos los divisores de ambos números, y observar cuál es el mayor de los divisores comunes. Por ejemplo, para encontrar $\text{mcd}(12, 18)$ vemos que

Divisores de 12 : 1, 2, 3, 4, 6, 12.

Divisores de 18 : 1, 2, 3, 6, 9, 18.

El máximo de los divisores comunes es 6, así que $\text{mcd}(12, 18) = 6$. Sin embargo, este procedimiento puede ser muy lento si se usan números más grandes. Un método computacionalmente más eficiente para obtener el máximo común divisor entre dos números es el famoso *algoritmo de Euclides*.

Teorema A.10 (Bézout). Para toda $a, b \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$, existen $s_1, s_2 \in \mathbb{Z}$ tales que

$$\text{mcd}(a, b) = as_1 + bs_2.$$

El Teorema de Bézout también se demuestra normalmente en un curso de teoría de números elemental.

Corolario A.11. Sean $a, b \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$. Entonces $\text{mcd}(a, b) = 1$ si y solo si existen $s_1, s_2 \in \mathbb{Z}$ tales que $as_1 + bs_2 = 1$.

Demostración.

(\Rightarrow) Si $\text{mcd}(a, b) = 1$, entonces $as_1 + bs_2 = 1$ para algunos $s_1, s_2 \in \mathbb{Z}$ por el Teorema de Bézout.

(\Leftarrow) Supongamos que $1 = as_1 + bs_2$ para algunos $s_1, s_2 \in \mathbb{Z}$. Sea $d = \text{mcd}(a, b)$. Como $d \mid a$ y $d \mid b$, el Lema A.5 (2.) implica que

$$d \mid (as_1 + bs_2) \implies d \mid 1.$$

Claramente, $1 \mid d$ por el Ejemplo A.2 (1.), así que el Lema A.5 (3.) implica que $d = \pm 1$. Por definición, el máximo común divisor es positivo, así que $d = 1$.

□

Lema A.12. Si $a = qb + r$, entonces $\text{mcd}(a, b) = \text{mcd}(b, r)$.

Demostración. Sean $c = \text{mcd}(a, b)$ y $d = \text{mcd}(b, r)$. El Lema A.5 (2.) implica que

$$d \mid (qb + r) = a \quad \text{y} \quad c \mid (a - qb) = r.$$

Por definición de máximo común divisor, tenemos que

$$\begin{aligned} d \mid a \quad \text{y} \quad d \mid b &\implies d \mid \text{mcd}(a, b) = c, \\ c \mid b \quad \text{y} \quad c \mid r &\implies c \mid \text{mcd}(b, r) = d. \end{aligned}$$

Por el Lema A.5 (3.), obtenemos que $d = \pm c$, lo que implica que $d = c$, ya que el máximo común divisor siempre es positivo. □

Además del algoritmo, el siguiente lema lleva el nombre de Euclides.

Lema A.13 (Euclides). Sean $a, b \in \mathbb{Z}$. Si p es un primo tal que $p \mid ab$ entonces $p \mid a$ o $p \mid b$.

Demostración. Supongamos que $p \nmid a$. Demostraremos que $p \mid b$. Como $p \nmid a$, tenemos que $\text{mcd}(p, a) = 1$, y por el Teorema de Bézout, existen $s_1, s_2 \in \mathbb{Z}$ tales que

$$1 = ps_1 + as_2.$$

Multiplicando por b , obtenemos que

$$b = ps_1b + abs_2.$$

Como $p \mid abs_2$ y $p \mid ps_1b$, tenemos que $p \mid b$ por el Lema A.5 (2.). \square

Es un error pensar que el Lema de Euclides se cumple si p no es un número primo. Por ejemplo, $6 \mid 3 \cdot 4$ pero $6 \nmid 3$ y $6 \nmid 4$.

Por fin, el siguiente teorema revela la gran importancia de los números primos.

Teorema A.14 (Teorema Fundamental de la Aritmética). Cualquier entero mayor que 1 es un número primo o un producto de números primos. Además, este producto es único excepto por el orden de los factores.

Ejemplo A.15. La factorización de 30 en números primos es

$$30 = 2 \cdot 3 \cdot 5.$$

Esta factorización es única excepto por el orden de los factores.

A.2. Relaciones de equivalencia

Sean A y B conjuntos. Recordemos que una relación R de A en B es un subconjunto del producto cartesiano $A \times B$. Escribimos aRb si $(a, b) \in R$.

Ejemplo A.16. Sea $f : A \rightarrow B$ cualquier función entre los conjuntos A y B . La siguiente relación se llama *la gráfica de la función*:

$$R := \{(a, b) \in A \times B \mid f(a) = b\}.$$

Una relación *sobre* A es simplemente una relación de A en A .

Definición A.17 (relación de equivalencia). Una relación R sobre un conjunto A es una *relación de equivalencia* si se cumplen las siguientes propiedades:

(E1) R es *reflexiva*: aRa para toda $a \in A$.

(E2) R es *simétrica*: aRb implica bRa .

(E3) R es *transitiva*: aRb y bRc implican aRc .

Ejemplo A.18. Sea \mathbb{Z} el conjunto de los números enteros y sea $n \geq 1$ un número entero. La relación

$$R_n = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : n \mid (a - b)\}$$

es una relación de equivalencia llamada la *congruencia módulo n* . Si $(a, b) \in R_n$ escribimos

$$a \equiv b \pmod{n}.$$

Es necesario demostrar que las propiedades (E1), (E2) y (E3) se cumplen:

- (E1) Para cualquier $a \in \mathbb{Z}$, $n \mid (a - a) = 0$, así que $a \equiv a \pmod{n}$.
- (E2) Si $n \mid (a - b)$, entonces $n \mid (b - a)$. Por lo tanto, $a \equiv b \pmod{n}$ implica $b \equiv a \pmod{n}$.
- (E3) Sean $a, b, c \in \mathbb{Z}$ tales que $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m}$. Entonces se cumple que $a - b = k_1m$ y $b - c = k_2m$ para algunos $k_1, k_2 \in \mathbb{Z}$. Sumando las ecuaciones anteriores obtenemos que $a - c = (k_1 + k_2)m$, lo que implica que $a \equiv c \pmod{m}$.

Observación A.19. Veamos que $a \equiv b \pmod{n}$ si y solo si $a = b + kn$ para algún $k \in \mathbb{Z}$. En particular, $a \equiv 0 \pmod{n}$ si y solo si a es un múltiplo de n .

Definición A.20 (clase de equivalencia). Sea R una relación de equivalencia sobre A . La *clase de equivalencia* de un elemento $a \in A$, denotada como $[a]$, es el subconjunto de A definido como

$$[a] = \{x \in A : xRa\}.$$

Al conjunto de todas las clases de equivalencia de los elementos de A se le llama el *conjunto cociente* de A por R , y se denota como A/R . En símbolos,

$$A/R = \{[a] : a \in A\}.$$

Ejemplo A.21. Sea R_n la relación de congruencia módulo n . Para cualquier $a \in \mathbb{Z}$, la clase de equivalencia módulo n de a es

$$[a] = \{x \in \mathbb{Z} : x \equiv a \pmod{n}\}.$$

El conjunto cociente \mathbb{Z}/R_n , denotado en este caso simplemente como \mathbb{Z}_n , es

$$\mathbb{Z}_n := \mathbb{Z}/R_n = \{[a] : a \in \mathbb{Z}\} = \{[0], [1], [2], \dots, [n-1]\}.$$

Es posible demostrar esta última igualdad usando el algoritmo de la división.

Lema A.22 (propiedades básicas de las clases de equivalencia). Sea R una relación de equivalencia sobre A .

- (1) $a \in [a]$ para toda $a \in A$.
- (2) $[a] = [b]$ si y solo si aRb .
- (3) Si $[a] \neq [b]$, entonces $[a] \cap [b] = \emptyset$.
- (4) $A = \bigcup_{a \in A} [a]$.

Ejemplo A.23. Hay dos clases de equivalencia en la relación módulo 2 sobre \mathbb{Z} . Una de estas clases contiene a los números divisibles entre 2 (los pares)

y la otra contiene a los números que no son divisibles entre 2 (los impares). Explícitamente,

$$\begin{aligned} [0] &= \{0, \pm 2, \pm 4, \dots\} = \{2n : n \in \mathbb{Z}\}, \\ [1] &= \{\pm 1, \pm 3, \pm 5, \dots\} = \{2n + 1 : n \in \mathbb{Z}\}. \end{aligned}$$

Por lo tanto, el conjunto cociente es

$$\mathbb{Z}_2 = \{[0], [1]\}.$$

Ejemplo A.24. En este ejemplo, encontraremos \mathbb{Z}_3 . Si $a \in \mathbb{Z}$, el algoritmo de la división implica que existen enteros q y r tales que

$$a = 3q + r,$$

donde $0 \leq r < 3$. Por lo tanto, $3 \mid a - r$ y

$$a \equiv r \pmod{3}, \text{ donde } 0 \leq r < 3.$$

Esto significa que cualquier número entero siempre es congruente módulo 3 con 0, 1 o 2. Por lo tanto, \mathbb{Z}_3 contiene exactamente tres clases de equivalencia:

$$\mathbb{Z}_3 = \{[0], [1], [2]\},$$

donde

$$\begin{aligned} [0] &= \{\dots, -6, -3, 0, 3, 6, \dots\}, \\ [1] &= \{\dots, -5, -2, 1, 4, 7, \dots\}, \\ [2] &= \{\dots, -4, -1, 2, 5, 8, \dots\}. \end{aligned}$$

Observación A.25. En general, dado cualquier número $a \in \mathbb{Z}$ es posible encontrar, usando el algoritmo de la división, un entero r , $0 \leq r < m$ tal que $a \equiv r \pmod{m}$. Esto significa que las clases de equivalencia módulo m siempre tienen representantes $0, 1, 2, \dots, m - 1$.

Ejemplo A.26. Consideremos la clase de equivalencia de 243 en la relación módulo 11. Para empezar, podemos sumar y restar múltiplos de 11 para obtener otros números en la misma clase:

$$[243] = [254] = [265] = [232].$$

Esto es válido ya que $11k \equiv 0 \pmod{11}$ para cualquier $k \in \mathbb{Z}$, así que

$$243 \equiv 243 + 11 \equiv 243 + 22 \equiv 243 - 11 \pmod{11}.$$

Para encontrar un representante menor que 11, usamos el algoritmo de la división:

$$243 = 11 \cdot 22 + 1.$$

Por lo tanto, $1 \equiv 243 \pmod{11}$, y $[243] = [1]$.

B

Apéndice B: Proyectos Finales

La siguiente es una lista de temas sugeridos para desarrollar un proyecto final en un curso de Teoría de Grupos.

1. **Generalizaciones de grupos:** estudiar diversas generalizaciones de grupos como subgrupos, monooides, cuasigrupos, lazos, etc.
2. **Grupos y música:** investigar las conexiones entre la teoría de grupos y la teoría musical.
3. **Grupos y criptografía:** investigar las conexiones entre la teoría de grupos y la criptografía.
4. **Grupos y física:** investigar las conexiones entre la teoría de grupos y la física teórica.
5. **Grupos y química:** investigar las conexiones entre la teoría de grupos y la química teórica.
6. **Grupo del cubo de Rubik:** explicar al grupo del cubo de Rubik, el cual es un subgrupo de S_{48} .
7. **Grupos diédricos:** estudiar más a fondo la estructura de los grupos diédricos: sus subgrupos, presentaciones, generalizaciones, etc.
8. **Grupos lineales:** estudiar más a fondo la estructura del grupo general lineal y del grupo especial lineal.
9. **Grupo de cuaternios:** definir al grupo de cuaternios como el grupo de las 8 unidades del álgebra de cuaternios; presentar propiedades y generalizaciones.
10. **Software GAP:** aprender a usar el software libre *Groups, Algorithms, Programming* (GAP), y presentar algunas de sus funciones básicas sobre grupos.

11. **Producto semidirecto:** definir al producto semidirecto externo de dos grupos; demostrar la equivalencia de la definición anterior con el producto semidirecto interno.
12. **Grupos nilpotentes:** definir a los grupos nilpotentes por medio de las series centrales; presentar ejemplos y propiedades básicas.
13. **Grupos solubles:** definir a los grupos solubles por medio de las series subnormales, y por medio de las series derivadas; presentar ejemplos, contraejemplos y propiedades básicas.
14. **Grupos topológicos:** definir y estudiar propiedades básicas de los grupos topológicos.
15. **Presentaciones de grupos:** definir la presentación de un grupo como un conjunto de generadores y relaciones; definir a los grupos libres y su propiedad universal.
16. **Gráficas de Cayley:** definir a la gráfica de Cayley de un grupo respecto a un subconjunto; presentar ejemplos y propiedades básicas.
17. **Grupos finitamente generados:** presentar ejemplos y propiedades básicas de grupos finitamente generados; demostrar que ser numerable es una condición necesaria, pero no suficiente, para ser finitamente generado.
18. **Grupos afines:** definir al grupo afín como el grupo de transformaciones afines invertibles de un espacio afín; examinar su estructura y propiedades básicas.
19. **Grupos primitivos:** definir qué es un grupo primitivo de permutaciones, por medio de una acción primitiva; desarrollar ejemplos y propiedades básicas.
20. **Representaciones de grupos:** definir representaciones de grupos como homomorfismos al grupo general lineal de un espacio vectorial; desarrollar ejemplos; demostrar el Teorema de Maschke y Lema de Schur.
21. **Extensiones de grupos:** definir extensiones de grupos mediante sucesiones exactas cortas y estudiar sus propiedades básicas.
22. **Grupos de Galois (\star):** definir grupos de Galois de extensiones de campos y polinomios, y estudiar sus propiedades básicas.
23. **Grupos de Lie (\star):** explicar en términos generales qué es un grupo de Lie; desarrollar ejemplos de grupos matriciales de Lie como los grupos unitarios y ortogonales.
24. **Grupos simples (\star):** demostrar que el grupo alternante A_5 es simple; enunciar y explicar el Teorema de Clasificación de Grupos Simples Finitos.

Bibliografía

- [1] A. Castillo Pérez, A. Castillo Ramírez, E. L. De la Cruz García, y A. M. Hernández Magdaleno, *Conjuntos y Números*, Editorial Universitaria, Centro Universitario de Ciencias Exactas e Ingenierías, Universidad de Guadalajara, 2014.
- [2] J. B. Fraleigh, *Algebra Abstracta: Primer Curso*, Addison-Wesley Iberoamericana, 1982.
- [3] J. A. Gallian, *Contemporary Abstract Algebra*, Séptima edición, Brooks/Cole, Cengage Learning, 2010.
- [4] D.S. Dummit y R.M. Foote, *Abstract Algebra*, Tercera edición, John Wiley and Sons, Inc., 2004.
- [5] K. Conrad, *Expository Papers: Group Theory*, Disponible en: <https://kconrad.math.uconn.edu/blurbs/>.
- [6] J. J. Rotman, *An Introduction to the Theory of Groups*, Cuarta edición, Springer-Verlag, 1995.
- [7] S. Roman, *Fundamentals of Group Theory: An Advanced Approach*, Birkhauser, Springer Science+Business Media, 2012.
- [8] H. E. Rose, *A Course on Finite Groups*, Universitext, Springer-Verlag, 2009.