Daniel Vázquez Lago

# Teoría de Grupos

PUBLISHED BY PUBLISHER

TEMPLATE-WEBSITE



*First printing, July 2023*

# Índice

# I

# Introducción y Grupos Discretos

# 1. Introducción a la Teoría de Grupos

## 1.1 Definición de Grupo

**Definición 1.1 — Grupo.** Un grupo es un conjunto de elementos $\{g_1, g_2\}$ dotados de una ley de composición (multiplicación) que a cada par ordenado $g_i, g_j \in G$ le asigna otro elemento $g_i g_j$ de forma que se satisfacen las siguientes propiedades:

- **Cierre**: la ley de composición es interna, es decir, si $g_i, g_j \in G$, entonces $g_i \cdot g_j \in G$
- **Asociatividad**: la ley de composición es interna, es decir, si:
$$g_i \cdot (g_j \cdot g_k) = (g_i \cdot g_j) g_k \tag{1.1}$$
- **Elemento Unidad**: existe un único elemento, denotado usualmente $e$, con la propiedad de que $\forall g_i \in G$:
$$e g_i = g_i e = g_i \tag{1.2}$$
- **Elemento Inverso**: para cada $g_i$ existe un único elemento $g_i^{-1}$ tal que
$$g_i^{-1} g_i = g_i g_i^{-1} = e \tag{1.3}$$

En general la multiplicación no es *conmutativa*, tal que $g_i \cdot g_j \neq g_j \cdot g_i$. Cuando es conmutativa, decimos que el grupo es **abeliano**. El número de elementos de $F$ se denomina *orden* de $F$, y se designa como $\mathcal{O}(G)$. Si el orden es finito, decimos que $G$ es un *grupo finito*.

Dado un grupo, podemos ampliar siempre a un álgebra. Un álgebra es un conjunto de elementos que forman un espacio vectorial sobre un cuerpo (como $\mathbb{R}$ o $\mathbb{C}$), de forma que, junto a la edición se define una operación de multiplicación que verifica los postulados que definen un grupo, excepto que el cero del álgebra no tiene inverso. Así por ejemplo, dado un grupo $G$ con elementos $g_{i(i=1,\dots,h)}$ las combinaciones lineales $\sum_{i=1}^{h} c_i g_i$, de elementos del grupo con coeficientes en el cuerpo, forman el álgebra del grupo. El producto se define por distributividad como

$$\left(\sum_{i=1}^{h} c_i g_i\right)\left(\sum_{j=1}^{h} c_j g_j\right) = \sum_{i=1}^{h}\sum_{j=1}^{h} c_i c_j g_i g_j \tag{1.4}$$

que por ser $g_i g_j$ un elemento del grupo, es un nuevo elemento del álgebra.

### 1.1.1 Ejemplos

Vamos a enucniar algunos ejemplos a título ilustrativo.

1. $Q_+$, El conjunto de todos los números reales estricatavemnte positivos con la ley de composición siendo la multiplicación ordinaria forma un grupo. Este grupo es abeliano y de orden infinito.
2. $S_n$. Permutaciones de $n$ objetos donde la multiplicación es la simple composición de permutaciones sucesivas. Es uno de los grupos más importantes, y es no abeliano.
3. $GL(N, \mathrm{R})$. El grupo lineal $GL(N, \mathrm{R})$ tiene por elementos todas las matrices de orden $N \times N$ con valores reales y deeterminante no nulo. Análogamente, se define el grupo $GL(N, \mathrm{C})$ como el grupo de matrices complejas.

## 1.2 Clase de Conjugación

**Definición 1.2 — Elementos Conjugados.** Dos elementos $g_1$ y $g_2$ de un grupo $G$ son conjugados si existe un tercer elemento tal que $g_2 = gg_1g^{-1}$. Decimos entonces que $g$ es el elemento conjugante.

En los casos en que se definen los elementos de un grupo como transformaciones lineales sonbre un cierto espacio vectorial, la equialencia bajo conjugación surge de la ambigüedad que existe a la hora de escoger la base de dicho espacio vectorial. Precisaremos este comentario en el capítulo siguiente, con un ejemplo explícito en el grupo $S_n$.

La relación de conjugación entre dos o más elementos es una relación de equivalencia $\sim$. Se verifican las siguietnes propiedades:

1. Reflexiva: $a \sim a$, ya que $a = ea = ae$.
2. Simétrica: $a = gbg^{-1} \Rightarrow b = gag^{-1}$.
3. Transitiva: $a = gbg^{-1}$, $b = hch^{-1}$, $\Rightarrow a = (gh)c(gh)^{-1}$

Dada una relación de equivalencia, la *clase de equivalencia* (conjunto de elementos con relación de equivalencia) de un elemento $a$ escrita como $(a)$ se define como:

$$(a) = \{b|b \sim a\} \tag{1.5}$$

de las propiedades de $\sim$ se sigue que la subdivisión de un conjunto en clases de equivalencia es una *partición en subconjuntos disjuntos*, ya que todo elemento pertenece a alguna calse de equivalencia por la propiedad reflexiva $a \sim a \Rightarrow (a) = \{a\}$. Además, si dos clases $(a)$ y $(b)$ tuvieran algún elemento en común $a \sim c$ y $b \sim c$, por transitividad se verifica que $a \sim b$ y por tanto $(a) = (b)$. Como sabemos, que la propiedad de conjugación es una relación de equivalencia, todo grupo $G$ admite una descomposición en *clases de conjugación*:

$$(g_i) = \left\{g_i \mid g_j = gg_ig^{-1}, \text{para algún } g \in G\right\} \tag{1.6}$$

Lógicamente el número de claes de conjugación es menor que el orden del grupo. Sólo es un grupo abeliano, cada elemento es a la vez toda una clase de conjugación que $a = gbg^{-1} = gg^{-1}b = b$.

## 1.3 Subgrupos

**Definición 1.3 — Subgrupos.** Un subgrupo $H$ de un grupo $G$ es un subconjunto de $G$ que a su vez forma un grupo bajo la misma ley de composición de $G$.

Cuando $G$ es finito, una definición equivalente afirma que $H$ es un subgrupo de $G$ cuando es cerrado (el producto de dos elementos de $H$ generá otro elemento de $H$) bajo la ley de composición de $G$:

$$\forall h_1, h_2 \in H \subset G \Rightarrow h_1 \cdot h_2 \in H \tag{1.7}$$

¿Por qué basta con que se verifique esto? Es obvio que la asociatividad es una propiedad heredada de $G$, y la existencia de identidad y de inverso en $H$ se heredan también. El elemento identidad $e$ debe pertenecer necesariamente a cualquier subgrupo. De hecho, en todo grupo $G$ hay dos ejemplos triviales, a saber, $H = \{e\}$ y $H = G$. Cualquier subgrupo que no sea estos dos se llama **subgrupo propio**.

### 1.3.1 Coset

Dados un elemento $g \in G$ y un subgrupo $H = \{h_1, h_2, ...\}$, de un grupo $G$ el **coset** por la izquierda de $g$ se escribe como $gH$ y consiste en el conjunto de elementos obtenidos al multiplicar $g$ por todos los elementos de $H$:

$$gH \equiv \{gh_1, gh_2, ...\} \tag{1.8}$$

Análogamente se define el coset por la derecha. La pertenencia de dos elementos al mismo coset define una relación de equivalencia

$$a \sim b \text{ si } b \in aH \tag{1.9}$$

y se verifican reflexividad, simetría y transitividad:

1. Reflexiva: $a \in aH$, ya que $a = ae$.
2. Simétrica: $b \in aH \Rightarrow b = ah \Rightarrow a = bh^{-1} \Rightarrow a \in bH$.
3. Transitiva: $b \in aH$, $c \in aH$, $b = ah$, $c = ah'$ así que $c = bh^{-1}h' = bh''$, i.e. $c \in bH$.

En consecuencia, los cosets son *clases de equivalencia*, lo que implica automáticamente que la división en costest es una partición disjunta de $G$. Si $G$ es un grupo finito, podemos enumerar los cosets *distintos* de la forma $\frac{G}{H} = \{g_1H = eH, g_2H, ..., g_sH\}$.

En un grupo finito $G$ de orden $\mathcal{O}(G)$, cada coset $gH$ contiene el mismo número de elementos $r$ que conicide con el orden $\mathcal{O}(H)$ del subgrupo $H$, lo que es evidente ya que $gh_1 = gh_2$ implica necesariamente que $h_1 = h_2$. Como hemos visto que la relación que definen los cosets, produce una partición disjunta de $G$, los elementos de éste se agrupan en $s$ cosets, todos del mismo orden $\mathcal{O}(H)$. Es decir,

$$\mathcal{O}(G) = s\mathcal{O}(H) \tag{1.10}$$

llegando al siguiente teorema:

**Teorema 1.1 — Teorema de Lagrange.** En un grupo finito $G$ el orden de cualquier subgrupo $H \subset G$ es un divisor del orden de $G$.

### 1.3.2 Subgrupos Normales

**Definición 1.4 — Subgrupo Normal.** Un subgrupo normal es un subgrupo $H$ que verifica $gHg^{-1} = H \quad \forall g \in G$

A los subgrupos también se les llama *auto-conjugados*. Una definición alternativa es decir que los subgrupos normales están compuestos de *clases de conjugación completas*, ya que $\forall h \in H \Rightarrow$

$ghg^{-1} = h' \in H$. También se puede decir que un subgrupo normal tiene la propiedad de que sus *cosests por la izquierda y derecha coinciden*:

$$gH = Hg \tag{1.11}$$

Cada elemento de un grupo abeliano es una clase de conjugación, lo que nos lleva a decir que todo grupo formado por $\{e, h, h^{-1}\}$ es un subgrupo normal de $G$ ($h \in G$).

> **Definición 1.5 — Grupo Simple.** Decimos que un grupo es simple si no posee ningún subgrupo normal propio. Si ungrupo no posee ningún subgrupo normal aveliano, decimos que es semisimple. Evidentemente todo grupo simple es semisimple.

### 1.3.3 Grupo Cociente

Como sabemos, el *conjunto coset G/H* define una partición disjunta de $G$ cuyos elementos (cosets) denotamos simbólicamente mediante un representatne $g_i H$.Una pregunta natural que podríamos hacernos es si $\frac{G}{H}$ es a su vez un grupo. Para ello debemos diseñar una operación interna que satisfaga los aiomas de grupo $(g_1 H) \cdot (g_2 H) = g_e H$. Si empezamos probando con la simple multiplicación definida en $G$ tal que $(g_1 H) \cdot (g_2 H) = g_1 H g_2 H = g_3 H$ (lógiacamente cada vez que pongamos $H$ nos referimos a cualquier elemento $h \in H$. En general esto no será cierto, salvo en el caso de que $H$ sea un subgrupo normal, ya que entonces por la propia definición de subgrupo normal Ecuación (1.10) se verifica que

$$(g_1 H) \cdot (g_2 H) = g_1 H g_2 H = g_1 g_2 H H = g_3 H \tag{1.12}$$

(aunque no parezca obvio $HH = H$ implica que el producto de *cualquier* elemento de por otro elemento de $H$ lleva a un elemento de $H$, por definición). En consecuencia, podemos concluir que el conjunto de cosets $\{g_i H\}$ admite una estructura de grupo cuando $H$ es un subgrupo normal. Llamamos a este grupo *grupo cociente G/H.*

### 1.3.4 Producto Directo

> **Definición 1.6 — Producto Directo.** Decimos que un grupo $G$ es el producto directo de dos subgrupos $A$ y $B$, $G = A \otimes B$, cuando
> 1. Todos los elementos de $A$ conmutan con todos los de $B$.
> 2. Todo elemento de $G$ admite una expresión única en forma de $g = ab$ donde $a \in A$ y $b \in B$.

De esta definición se generaliza directamente el producto de $n$ subgrupos $G = A \otimes B \otimes ... \otimes J$.

- El único elemento que tienen en común $A$ y $B$ es el elemento neutro/identidad.
- El producto de dos elementos $g_1 = a_1 b_1$ y $g_2 = a_2 b_2$ implica:

  $$g_1 g_2 = (a_1 b_1)(a_2 b_2) = a_1 a_2 b_1 b_2 = (a_1 a_2)(b_1 b_2) \tag{1.13}$$

  donde hemos aplicando la conutación $ba = ab$.
- Los grupos $A$ y $B$ son subgrupos normales. Que sean subgrupos es trivial (ya que $a/b$ puede ser el elemento neutro). Que sean subgrupos normales, no es tan trivial, aunque se pueden ver de que al ser $g = ab$:

  $$gAg^{-1} = (ab)a_i(ab)^{-1} = aba_i a^{-1} b^{-1} = aa_i a^{-1} \tag{1.14}$$

y como $aa_ia^{-1} \in A$, queda demostrado.

- Los grupos cocientes $\frac{G}{B}$ y $\frac{G}{A}$ son isomorfos a $A$ y $B$ respectivamente. Esto es trivial si pensamos que $\frac{G}{B} = \{g_iB \quad \forall g_i \in G\}$, que al ser $g = ab$, $\frac{G}{B} = \{a_iB \quad \forall a_i \in A\}$. Evidentemente todos los cosets son distintos, ya que si suponemos que $a_1b_1 = a_2b_2$, entonces estaríamos violando la definición de *producto directo*. Entonces es evidente que existe una aplicación 1:1 entre $\frac{G}{B}$ y $A$, tal que $a_iB \longmapsto a_i$ es un *homomorfismo*, y esto se basa en la propiedad de subgrupo normal de $B$, que implica la ley de multiplicación $(a_1B)(a_2B) = a_1a_2N \longmapsto a_1a_2$.

Con frecuencia haremos también el producto directo de dos grupos $G \otimes G'$. Para obtenerlo basta con formar todas las parejas posibles de la forma $(g, g')$. Si $e$ y $e'$ son las identidades respectivas, $(e, e')$ es la identidad del producto directo. Vemos por tanto, qeu el orden del producto directo es el producto de los órdenes. El producto de pares se define mediante

$$(f, f')(g, g') = (fg, f'g') \tag{1.15}$$

Los elementos $(g, e')$ forman un subgrupo $\Gamma$ que es isomorfo a $G$, y lo mismo de $(e, g') \in \Gamma' \sim G$. Entonces el grupo de pares de elementos definido es el producto directo de $\Gamma$ y $\Gamma'$.

### 1.3.5 Centro de un grupo

**Definición 1.7 — Centro.** El centro $Z$ de un grupo $G$ se define como el subconjunto de elementos $z$ que conmutan con todos los elementos del grupo $Z = \{z \in G \quad | \; zg = gz \quad \forall \in G\}$

Claramente $Z$ es un subgrupo abeliano; además la propiedad que define el centro implica que es un subgrupo normal, puesto que cada elemento $z \in Z$ es una clase de conjugación completa $z = gzg(-1)$.

## 1.4 Ejercicios

**Ejercicio 1.1** Sea $G$ un grupo y considérese el centralizador asociado a un elemento $g \in G$. Demostrar qeu dicho centralizador es un subgrupo de $G$.

**Ejercicio 1.2** Demuéstrese que si $G = H_1 \otimes H_2$, entonces $\frac{G}{H} \simeq H_2$ y que $\frac{G}{H_2} \simeq H_1$ donde $\simeq$ significa isomorfo.

# 2. Homomorfismos y Reducibilidad

## 2.1 Homomorfismos

Un homomorfismo es una aplicación $f$ de un conjunto $A$ en otro $B$ (escribimos $f : A \longmapsto B$) que preserva alguna estructura interna. En particular estamos interesados en la estructura de grupo de $A$ y $B$.

**Definición 2.1 — Homomorfismo.** sean $A$ y $B$ dos grupos y $f : A \to B$ una aplicación. Decimos enton es que $f$ es un homomorfismo cuando verifica que para cualesquiera $a_1, a_2 \in A$:

$$f(a_1 a_2) = f(a_1) f(a_2) \tag{2.1}$$

Cuando $B$ coincide con $A$ decimos que $f$ es un **endomorfismo**. Recordemos la definición de imagen y kernel de una aplicación:

$$\text{Im } f := \{b \in B \mid b = f(a) \text{ para algún } a \in A\} \tag{2.2}$$

$$\text{Ker } f := \{a \in A \mid f(a) = e_B \in B\} \tag{2.3}$$

Una aplicación es **inyecta** cuando Ker $f = e_A$. Si además Im $f = B$, $f$ es **suprayectiva**. Si es biyectiva y suprayectiva a la vez decimos que es la aplicaicón es **biyectiva** o 1:1. Si además $f$ es un homomorfismo (Ecuación (2.1)) es decimos que constituye un *isomorfismo*. Un *isomorfismo* $f : A \longmapsto A$ de un grupo en sí mismo se llama *automorfismo*.

## 2.2 Ejercicios

# 3. Grupos finitos

## 3.4 Ejercicios

# II

# Grupos Continuos

# 4. Grupos de Lie

## 4.1 Definición y Ejemplos

## 4.2 Ejercicios