CURSO DE MÉTODOS DE LA FÍSICA MATEMÁTICA

TEORÍA DE GRUPOS

H. FALOMIR
DEPARTAMENTO DE FÍSICA
FACULTAD DE CIENCIAS EXACTAS - UNLP

NOTAS SOBRE TEORÍA DE GRUPOS

1. Generalidades

Un **grupo** G es un conjunto de elementos sobre los cuales hay definida una ley de composición, $\cdot : G \times G \to G$, que es asociativa, con neutro e inverso, es decir,

a) $f \cdot (g \cdot h) = (f \cdot g) \cdot h, \forall\, f, g, h \in G$,

b) $\exists\, e \in G$, llamado **elemento neutro** o **identidad**, que satisface $e \cdot g = g \cdot e = g, \forall\, g \in G$,

c) $\forall\, g \in G, \exists\, g^{-1} \in G$, llamado su **inversa**, que satisface $g \cdot g^{-1} = g^{-1} \cdot g = e$.

Evidentemente, si $f \cdot g = h \cdot g$ entonces $f = h$. En efecto, $(f \cdot g) \cdot g^{-1} = f \cdot (g \cdot g^{-1}) = (h \cdot g) \cdot g^{-1} = h \cdot (g \cdot g^{-1}) \Rightarrow f = g$.

Similarmente, se puede demostrar que el neutro y el inverso de cualquier elemento son únicos. Por ejemplo, si $g \cdot f = e \Rightarrow g^{-1} \cdot (g \cdot f) = (g^{-1} \cdot g) \cdot f = e \cdot f = g^{-1} \cdot e \Rightarrow f = g^{-1}$. En consecuencia, $(f \cdot g)^{-1} = g^{-1} \cdot f^{-1}$, puesto que $(f \cdot g) \cdot (g^{-1} \cdot f^{-1}) = f \cdot (g \cdot g^{-1}) \cdot f^{-1} = f \cdot f^{-1} = e$.

En general, la ley de composición no es conmutativa: $f \cdot g \neq g \cdot f$. Un grupo G para el cual $f \cdot g = g \cdot f, \forall\, f, g \in G$ se dice **Abeliano**.

Ejemplos:

- el grupo ***aditivo*** de los enteros respecto de la operación de suma usual, $\mathbb{Z}$;
- el conjunto de los racionales no nulos, $\mathbb{Q}\backslash\{0\}$, respecto de la operación usual de multiplicación;
- el conjunto $\{1, -1\}$ respecto de la operación de multiplicación de reales;
- el conjunto de las rotaciones de un cuerpo.

El **orden** de un grupo es el número de elementos que contiene. El orden puede finito o infinito.

2. Grupo de permutaciones

Consideremos una permutación de cinco elementos,

$$\{a_1, a_2, a_3, a_4, a_5\} \to \{a_2, a_3, a_1, a_5, a_4\}\,. \tag{2.1}$$

Independientemente de la naturaleza de esos elementos, esta operación puede ser representada por el siguiente cuadro de números que indica, sobre cada columna, la posición inicial y final de un elemento,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix} \equiv \begin{pmatrix} 2 & 3 & 1 & 5 & 4 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} \tag{2.2}$$

(o bien, con idéntico significado, por cualquier otro cuadro que difiera de los anteriores en una permutación de sus columnas).

La operación de composición de σ con otra permutación

$$\sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 2 & 4 \end{pmatrix} \tag{2.3}$$

se define por

$$\sigma' \cdot \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 2 & 4 \end{pmatrix} \cdot \begin{pmatrix} 2 & 3 & 1 & 5 & 4 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} := \begin{pmatrix} 2 & 3 & 1 & 5 & 4 \\ 5 & 3 & 1 & 2 & 4 \end{pmatrix}. \tag{2.4}$$

Esta operación satisface los axiomas de grupo. En efecto, puede constatarse que esa operación es asociativa, que el elemento neutro está dado por

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} \tag{2.5}$$

y que, por ejemplo, la inversa de σ en (2.2) está dada por el mismo cuadro de números con sus filas intercambiadas,

$$\sigma^{-1} = \begin{pmatrix} 3 & 1 & 2 & 5 & 4 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}. \tag{2.6}$$

Este grupo es **no Abeliano**, como surge de verificar que $\sigma \cdot \sigma' \neq \sigma' \cdot \sigma$.

Generalizando esas definiciones, resulta que el conjunto de las **permutaciones de p elementos** se estructura como un grupo (no Abeliano), denotado por $\mathbf{S_p}$.

Consideremos la permutación $\tau \in \mathbf{S_9}$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 3 & 9 & 6 & 1 & 7 & 5 & 8 & 2 \end{pmatrix}. \tag{2.7}$$

Ella puede ser descompuesta en las **permutaciones cíclicas** independientes

$$\tau \equiv \begin{cases} 1 \to 4 \to 6 \to 7 \to 5 \to 1, \\ 2 \to 3 \to 9 \to 2, \\ 8 \to 8. \end{cases} \tag{2.8}$$

Nótese que cada **ciclo** involucra a un cierto número de elementos que no aparece en los demás ciclos.

La permutación τ puede ser caracterizada mediante su **descomposición en ciclos**, y denotada por

$$\tau = (1\ 4\ 6\ 7\ 5)\ (2\ 3\ 9)\ (8) \equiv (2\ 3\ 9)\ (1\ 4\ 6\ 7\ 5), \tag{2.9}$$

dado que los ciclos independientes conmutan entre sí, como puede verificarse fácilmente.

Los ciclos de un elemento pueden ser descartados del cuadro, ya que no tienen ningún efecto en la permutación. Tampoco importa por cual elemento comienza a describirse cada ciclo, ya que con el mismo significado tenemos

$$\tau = (6\ 7\ 5\ 1\ 4)\ (9\ 2\ 3). \tag{2.10}$$

Un ciclo de dos elementos se llama **transposición simple**. Todo ciclo puede ser descompuesto en un producto de transposiciones simples. Por ejemplo,

$$(1\ 4\ 6\ 7\ 5) = (1\ 5)\ (1\ 7)\ (1\ 6)\ (1\ 4). \tag{2.11}$$

Una permutación se dice **par** o **impar** de acuerdo a que sea posible descomponerla en un número par o impar de transposiciones simples.

También es posible **representar** una permutación de p elementos mediante una matriz cuyos elementos son todos 0 excepto p de ellos iguales a 1, dispuestos de modo tal que sólo aparezca un 1 por fila y por columna. Por ejemplo, para $\sigma \in \mathbf{S_5}$ en (2.2) tenemos

$$\begin{pmatrix} a_2 \\ a_3 \\ a_1 \\ a_5 \\ a_4 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \end{pmatrix} = M(\sigma) \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \end{pmatrix}, \tag{2.12}$$

donde hemos introducido un ***producto*** de elementos a_k por 1 o 0 cuyo significado es, respectivamente, seleccionar o no a dicho elemento.

En esta **representación** del grupo $\mathbf{S_5}$, la operación de composición se reduce simplemente al producto usual de matrices, $M(\sigma'\,\sigma) = M(\sigma')\,M(\sigma)$.

Nótese que la traza de $M(\sigma)$, $\mathrm{tr}\, M(\sigma)$, es el número de elementos que deja invariantes la permutación σ, mientras que su determinante, $\det M(\sigma)$, es igual a $+1$ para permutaciones pares y a -1 para las impares. Por ejemplo, para σ en (2.2) y $M(\sigma)$ en (2.12),

$$\sigma = (1\ 3\ 2)\ (4\ 5) = (4\ 5)\ (1\ 2)\ (1\ 3),$$
$$\mathrm{tr}\, M(\sigma) = 0, \quad \det M(\sigma) = -1. \tag{2.13}$$

Ejemplo: La **tabla** de la operación de composición en el grupo $\mathbf{S_3} = \{e, a = (1\ 2\ 3), b = (1\ 3\ 2), \alpha = (2\ 3), \beta = (3\ 1), \gamma = (1\ 2)\}$ está dada por el cuadro

$\cdot$	e	a	b	α	β	γ
e	e	a	b	α	β	γ
a	a	b	e	γ	α	β
b	b	e	a	β	γ	α
α	α	β	γ	e	a	b
β	β	γ	α	b	e	a
γ	γ	α	β	a	b	e

(2.14)

Si nos restringimos a las entradas correspondientes al neutro e y a una transposición simple, digamos γ, tenemos la tabla de $\mathbf{S_2}$,

$\cdot$	e	γ
e	e	γ
γ	γ	e

(2.15)

que coincide formalmente con la tabla del **grupo aditivo de los enteros módulo 2**, $\mathbb{Z}_2$,

$(+)_{\mathrm{mod}\,2}$	0	1
0	0	1
1	1	0

(2.16)

con la identificación $e \leftrightarrow 0, \gamma \leftrightarrow 1$.

Similarmente, las entradas de la tabla de $\mathbf{S_3}$ correspondientes a la composición de las permutaciones cíclicas de tres elementos,

$\cdot$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

(2.17)

no involucran a las transposiciones simples, y coinciden formalmente con la tabla del **grupo aditivo de los enteros módulo 3**, $\mathbb{Z}_3$,

$$
\begin{array}{c|ccc}
(+)_{\mathrm{mod}\,3} & 0 & 1 & 2 \\
\hline
0 & 0 & 1 & 2 \\
1 & 1 & 2 & 0 \\
2 & 2 & 0 & 1
\end{array}
\tag{2.18}
$$

con la identificación entre elementos $e \leftrightarrow 0, a \leftrightarrow 1, b \leftrightarrow 2$.

Dos grupos entre cuyos elementos existe una correspondencia biunívoca de modo que sus tablas de composición resulten idénticas, se dicen **isomorfos**.

Un subconjunto $H \subset G$ que contiene a la identidad y a la inversa de cada uno de sus elementos, y que es **cerrado** respecto de la operación de composición en G, constituye un **subgrupo** de G.

Todo grupo G tiene dos **subgrupos impropios**: G y $\{e\}$. Todo otro subgrupo se dice **propio**.

La intersección de subgrupos también constituye un subgrupo, como puede verificarse fácilmente.

Ejemplos:

a) Los enteros $\mathbb{Z}$ forman un subgrupo del grupo aditivo de los reales $\mathbb{R}$.
b) Las rotaciones sobre un plano forman un subgrupo del grupo de rotaciones en el espacio.
c) Las rotaciones alrededor de un eje en ángulos $0, \pi/2, \pi, 3\pi/2$ forman un subgrupo del grupo de rotaciones en el plano.

3. Homomorfismo - Representaciones

Un **homomorfismo** es una aplicación entre grupos, $\phi : G \to H$, que satisface

$$
\phi(g \cdot g') = \phi(g) \cdot \phi(g') \in H, \ \forall\, g, g' \in G. \tag{3.1}
$$

Dos grupos G y H se dicen **isomorfos**, lo que se denota por $G \approx H$, si entre sus elementos existe una aplicación biunívoca (uno a uno y sobreyectiva) que preserva las operaciones de composición como en (3.1). En ese caso la aplicación $\phi : G \leftrightarrow H$ constituye un **isomorfismo**.

Independientemente de la naturaleza de cada grupo, una vez identificados sus elementos mediante el isomorfismo ϕ, grupos isomorfos presentan la misma tabla de composición.

El isomorfismo establece una relación de equivalencia entre grupos. En efecto, es evidente que $G \approx G$; que si $G \approx H \Rightarrow H \approx G$; y que si $G \approx F$ y $F \approx H \Rightarrow G \approx H$.

Esto permite definir **clases de equivalencia**, donde dos grupos están en la misma clase si son isomorfos entre sí. Todos los grupos dentro de una clase presentan la misma tabla de composición, la que entonces caracteriza a la clase de equivalencia o **grupo abstracto**.

Los diversos grupos pertenecientes a una misma clase constituyen distintas **realizaciones** de ese grupo abstracto (cuyos elementos no están especificados). Cada clase de equivalencia puede ser identificada por uno cualquiera de los grupos que contiene.

Ejemplos: Existe un único grupo abstracto de orden 2, denominado $\mathbb{Z}_2$ y caracterizado por la tabla en (2.16). Distintas realizaciones de ese grupo son $\mathbb{Z}_2$, $\mathbf{S_2}$, el grupo $\{+1, -1\}$ respecto del producto de reales, o el grupo

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\} \tag{3.2}$$

respecto del producto usual de matrices.

Similarmente, existe un único grupo abstracto de orden 3, denominado $\mathbb{Z}_3$ y caracterizado por la tabla en (2.18). Distintas realizaciones de este grupo son el propio $\mathbb{Z}_3$ o el subgrupo de $\mathbf{S_3}$ correspondiente a las permutaciones cíclicas de tres elementos, $\{e, a, b\}$, cuya tabla está dada en (2.17).

Para órdenes mayores de 3 es posible construir varias tablas que satisfacen los axiomas de grupo.

Un homomorfismo de un grupo G sobre un grupo de operadores lineales H (definidos sobre cierto espacio lineal $\mathbf{E}$) constituye una **representación lineal** de G. Cuando esta aplicación es un isomorfismo, la representación se dice **fiel**.

Si el **espacio de la representación E** es de dimensión finita, H es un grupo de matrices (cuando los operadores son referidos a cierta base de $\mathbf{E}$). En ese caso se tiene una **representación matricial** de G, donde la operación de composición en el grupo H se reduce al producto usual de matrices.

Ejemplo: La asignación de una matriz $M(\sigma)$ a cada permutación σ, como en (2.12), constituye una representación matricial fiel del grupo $\mathbf{S_p}$, llamada **representación regular**,

$$\phi : \mathbf{S_p} \leftrightarrow \{M(\sigma) \mid \sigma \in \mathbf{S_p}\}\,. \tag{3.3}$$

Por ejemplo, para el grupo $\mathbf{S_3}$ tenemos

$$M(e) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad M(a) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad M(b) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

(3.4)

$$M(\alpha) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad M(\beta) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad M(\gamma) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Todo grupo tiene una **representación trivial**, en la cual todo elemento es representado por el operador identidad. La mínima dimensión posible para el espacio de esta representación es $\dim \mathbf{E} = 1$, en cuyo caso tenemos $\phi : G \to \{1\}$. Esta representación no es fiel (excepto para el grupo trivial $\mathbb{Z}_1 = \{e\}$).

Para los grupos de permutaciones $\mathbf{S_p}$ existe una segunda representación unidimensional, llamada **representación alternada**, en la que cada permutación σ es representada por (la matriz de 1×1) $+1$ ó -1, de acuerdo a que σ sea par ó impar respectivamente.

Esta representación tampoco es fiel, excepto para $\mathbf{S_2}$. Por ejemplo, para $\mathbf{S_3}$ tenemos $\phi(e) = \phi(a) = \phi(b) = +1$ y $\phi(\alpha) = \phi(\beta) = \phi(\gamma) = -1$.

Ejemplo: Las rotaciones en un plano forman un grupo (subgrupo del grupo de las rotaciones en el espacio $\mathbb{R}^3$). Ellas pueden ser representadas como matrices de 2×2 que actúan sobre vectores reales del mismo plano $\mathbb{R}^2$ (espacio de la representación). La rotación en un ángulo $\varphi \in [0, 2\pi)$ alrededor del origen, $R(\varphi)$, corresponde a la acción de la matriz

$$\phi(R(\varphi)) = D(\varphi) = \begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix}. \tag{3.5}$$

Se trata de una representación fiel, puesto que la relación entre $R(\varphi)$ y $D(\varphi)$ es biunívoca, satisfaciendo que

$$\phi\left(R(\varphi_1) \cdot R(\varphi_2)\right) = \phi\left(R\left([\varphi_1 + \varphi_2]_{\mathrm{mod}\, 2\pi}\right)\right) = \phi\left(R(\varphi_1)\right) \cdot \phi\left(R(\varphi_2)\right), \tag{3.6}$$

como se comprueba fácilmente del cálculo del producto de matrices

$$D(\varphi_1)\, D(\varphi_2) = D\left([\varphi_1 + \varphi_2]_{\mathrm{mod}\, 2\pi}\right). \tag{3.7}$$

Por otra parte, todas las matrices $D(\varphi)$ en (3.5) pueden ser simultáneamente diagonalizadas, para llevarlas a la forma

$$D(\varphi) \to \begin{pmatrix} e^{i\varphi} & 0 \\ 0 & e^{-i\varphi} \end{pmatrix}. \tag{3.8}$$

Evidentemente, el conjunto de los bloques diagonales (de 1×1) constituye una representación unidimensional fiel del grupo de rotaciones en el plano,

$$R(\varphi) \leftrightarrow D_{\pm}(\varphi) := e^{\pm i\varphi}, \tag{3.9}$$

que actúa sobre un espacio de representación complejo unidimensional, y en la cual la operación del grupo se reduce al producto usual de complejos.

Pueden construirse otras representaciones unidimensionales no fieles de este grupo mediante la asignación $R(\varphi) \to D_m(\varphi) = e^{im\varphi}$, con $m \in \mathbb{Z}$ y $m \neq \pm 1$. En efecto, $D_m(\frac{2\pi}{m}) = e^{im\frac{2\pi}{m}} = 1 = D_m(0)$, con $\frac{2\pi}{m} \neq 0 \bmod 2\pi$.

4. Subgrupos

Recordemos que un subconjunto $H \subset G$ es un **subgrupo** de G si

- el elemento identidad $e \in H$,
- si $h \in H \Rightarrow h^{-1} \in H$,
- $\forall\, h_1, h_2 \in H$, se tiene que $h_1 \cdot h_2 \in H$.

Con esas propiedades, H se estructura como un grupo respecto de la misma ley de composición del grupo G. En efecto, H es cerrado respecto de una ley de composición asociativa, con neutro e inverso.

Teorema 4.1. *El subconjunto $H \subset G$ es un subgrupo del grupo G si y sólo si $\forall\, a, b \in H$ resulta que $a \cdot b^{-1} \in H$.*

Demostración: Por una parte, resulta evidente que si H es un subgrupo de G, entonces $a \cdot b^{-1} \in H, \forall\, a, b \in H$.

Supongamos ahora que $\forall\, a, b \in H$ resulta que $a \cdot b^{-1} \in H$. Entonces,

- Como H no es vacío, si $a \in H \Rightarrow a \cdot a^{-1} = e \in H$.
- Además, si $e, a \in H \Rightarrow e \cdot a^{-1} = a^{-1} \in H$.
- Finalmente, si $a, b \in H \Rightarrow a, b^{-1} \in H \Rightarrow a \cdot (b^{-1})^{-1} = a \cdot b \in H$.

Por lo tanto, H es un subgrupo de G. □

El **núcleo** (o **kernel**) de un homomorfismo $\phi : G \to H$, denotado por $\phi^{-1}(e_H)$, es el conjunto de los elementos de G que tienen por imagen al elemento neutro en

H,

$$\phi(g) = e_H,\ \forall\, g \in \phi^{-1}(e_H)\,. \tag{4.1}$$

El núcleo de un homomorfismo $\phi : G \to H$ es un subgrupo de G. En efecto, si $a, b \in \phi^{-1}(e_H) \Rightarrow \phi(a) = e_H$ y $\phi(b^{-1}) = \phi(b)^{-1} = e_H^{-1} = e_H \Rightarrow \phi(a \cdot b^{-1}) = \phi(a) \cdot \phi(b^{-1}) = e_H \cdot e_H = e_H$. Por lo tanto, $a \cdot b^{-1} \in \phi^{-1}(e_H)$ que, en consecuencia, es un subgrupo.

Sea H un subgrupo propio del grupo G, y sea $a_1 \notin H$. Consideremos el subconjunto de G formado por los elementos de la forma $a_1 \cdot h$, con $h \in H$, que denotamos por $a_1 \cdot H$. Si $\exists\, a_2 \notin H \cup a_1 \cdot H$, formamos el subconjunto $a_2 \cdot H = \{a_2 \cdot h,\ \text{con } h \in H\}$, y así siguiendo hasta agotar los elementos del grupo.

El subgrupo H puede denotarse como $e \cdot H$.

Los subconjuntos de G así construidos, llamados **cosets izquierdos**[1] del subgrupo H, son disjuntos. En efecto, si dos de ellos tuvieran un elemento en común, $a_i \cdot h_1 = a_k \cdot h_2$, con $h_1, h_2 \in H$. Entonces, $a_k = (a_i \cdot h_1) \cdot h_2^{-1} = a_i \cdot (h_1 \cdot h_2^{-1}) = a_i \cdot h_3$, donde $h_3 = h_1 \cdot h_2^{-1} \in H \Rightarrow a_k \in a_i \cdot H$, lo que (por construcción) no puede ocurrir si $a_k \neq a_i$. Por lo tanto, $a_i \cdot H \cap a_k \cdot H = \emptyset$ para $k \neq i$.

Por otra parte, los cosets $a \cdot H$ son independientes del elemento $a = a \cdot e \in a \cdot H$ que se emplea en su construcción. En efecto, supongamos que $b \in a \cdot H \Rightarrow b = a \cdot h$, para algún $h \in H$. Pero entonces, $a = b \cdot h^{-1} \in b \cdot H$. Sea ahora $c = a \cdot h_1 \in a \cdot H \Rightarrow c = b \cdot h^{-1} \cdot h_1 \in b \cdot H$. En esas condiciones, $a \cdot H \subset b \cdot H$. Se prueba de manera similar que $b \cdot H \subset a \cdot H$. En consecuencia, $a \cdot H = b \cdot H$.

En esas condiciones, el conjunto G puede expresarse como la unión de los conjuntos disjuntos correspondientes a los cosets izquierdos de H,

$$G = \bigcup_k a_k \cdot H\,. \tag{4.2}$$

En particular, si G es de orden finito, $\#G = n$, también lo es $H \subset G$, y los cosets tienen todos el mismo número de elementos que H, $\#H = m$. Como los cosets son disjuntos, los hay en un número finito k tal que $n = m\,k$. Con esto queda establecido el siguiente teorema.

Teorema 4.2. (de Lagrange) *El orden de un subgrupo H de un grupo de orden finito G es un divisor del orden de G,*

$$\frac{\#G}{\#H} = k \in \mathbb{N}\,. \tag{4.3}$$

[1] De manera similar se definen los **cosets derechos** de H.

Una consecuencia inmediata de este teorema es que un grupo de orden primo sólo tiene subgrupos impropios.

Sea G un grupo de orden finito, y sea $a \in G$ uno de sus elementos. Consideremos el conjunto de elementos de G de la forma $e, a, a^2 = a \cdot a, \ldots, a^{k+1} = a \cdot a^k, \ldots$. Como $\#G < \infty$, los elementos a^k no pueden ser todos distintos. Supongamos que $a^p = a^q$, con $p > q$; entonces $a^{p-q} = e$. Sea n el menor número natural para el cual $a^n = e$. En ese caso, el elemento a se dice de orden n.

En esa condiciones, el conjunto $\{e, a, a^2, \ldots, a^{n-1}\}$ forma un grupo llamado **grupo cíclico de orden** n, que es isomorfo a $\mathbb{Z}_n$. En efecto, $a^k \cdot a^l = a^{k+l|_{\mathrm{mod}\, n}}$.

Teorema 4.3. (de Cayley) *Todo grupo de orden n es isomorfo a un subgrupo regular de* $\mathbf{S_n}$.

Demostración: Consideremos la tabla de la ley de composición en un grupo G de orden n,

(4.4)

$\cdot$	a_1	a_2	$\ldots$	a_k	$\ldots$	a_n
a_1	a_1	a_2	$\ldots$	a_k	$\ldots$	a_n
a_2	$a_2 \cdot a_1$	$a_2 \cdot a_2$	$\ldots$	$a_2 \cdot a_k$	$\ldots$	$a_2 \cdot a_n$
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
a_l	$a_l \cdot a_1$	$a_l \cdot a_2$	$\ldots$	$a_l \cdot a_k$	$\ldots$	$a_l \cdot a_n$
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
a_n	$a_n \cdot a_1$	$a_n \cdot a_2$	$\ldots$	$a_n \cdot a_k$	$\ldots$	$a_n \cdot a_n$

donde $a_1 = e$.

Primero señalemos que los elementos no se repiten en la filas ni en las columnas de esa tabla. En efecto, si, por ejemplo, un elemento se repitiera en la i-ésima fila, $a_i \cdot a_k = a_i \cdot a_l \Rightarrow a_k = a_l$, lo que no puede ser dado que los elementos de G tienen una única entrada en la tabla para la multiplicación a derecha.

En consecuencia, la l-ésima fila (que corresponde a la multiplicación a izquierda por a_l, y en la que aparecen los n elementos del grupo) se obtiene de la primera

mediante una **permutación regular** (es decir, una permutación que no deja invariante ningún elemento):

$$\phi(a_l) = \pi_l = \begin{pmatrix} 1 & 2 & \dots & k & \dots & n \\ \pi_l(1) & \pi_l(2) & \dots & \pi_l(k) & \dots & \pi_l(n) \end{pmatrix} =$$

$$\begin{pmatrix} \pi_l^{-1}(1) & \pi_l^{-1}(2) & \dots & \pi_l^{-1}(k) & \dots & \pi_l^{-1}(n) \\ \pi_l(\pi_l^{-1}(1)) & \pi_l(\pi_l^{-1}(2)) & \dots & \pi_l(\pi_l^{-1}(k)) & \dots & \pi_l(\pi_l^{-1}(n)) \end{pmatrix} = \tag{4.5}$$

$$= \begin{pmatrix} \pi_l^{-1}(1) & \pi_l^{-1}(2) & \dots & \pi_l^{-1}(k) & \dots & \pi_l^{-1}(n) \\ 1 & 2 & \dots & k & \dots & n \end{pmatrix},$$

donde $\pi_l : \{1, 2, \dots, n\} \leftrightarrow \{1, 2, \dots, n\}$ es una aplicación biunívoca que no tiene puntos fijos.

Esta correspondencia es uno a uno, puesto que si $\phi(a_l) = \pi_l = \pi_k = \phi(a_k)$, entonces las filas l-ésima y k-ésima son idénticas $\Rightarrow a_l = a_k$.

Dada la asociatividad del producto, la fila correspondiente al elemento $a_k \cdot a_l$ se obtiene de multiplicar a izquierda por a_k los elementos en la fila $a_l \cdot a_1, \dots, a_l \cdot a_n$. Para poder describir esta operación en términos de la permutación π_k, esa l-ésima fila debe ser primero llevada al orden correspondiente a la primera fila, $a_1, \dots, a_n$:

$$\phi(a_k) \cdot \phi(a_l) =$$

$$= \begin{pmatrix} 1 & 2 & \dots & n \\ \pi_k(1) & \pi_k(2) & \dots & \pi_k(n) \end{pmatrix} \begin{pmatrix} \pi_l^{-1}(1) & \pi_l^{-1}(2) & \dots & \pi_l^{-1}(n) \\ 1 & 2 & \dots & n \end{pmatrix} = \tag{4.6}$$

$$= \begin{pmatrix} 1 & 2 & \dots & n \\ \pi_k(\pi_l(1)) & \pi_k(\pi_l(2)) & \dots & \pi_k(\pi_l(n)) \end{pmatrix} = \phi(a_k \cdot a_l)\,.$$

Por lo tanto, $\phi : G \leftrightarrow \{\pi_1, \dots, \pi_n\}$ es un isomorfismo. El rango de este isomorfismo es un **subgrupo regular de $\mathbf{S_n}$** (cuyos elemento son permutaciones que no dejan posiciones invariantes, a excepción del elemento identidad π_1). □

Siendo $\mathbf{S_n}$ un grupo de orden finito, resulta que el número de subgrupos que contiene es necesariamente finito. Esto implica que hay sólo un número finito de grupos de orden $n \in \mathbb{N}$ que no son isomorfos entre sí.

5. Clases de elementos conjugados

Dos elementos $a, b \in G$ se dicen **conjugados** si existe un tercer elemento $g \in G$ tal que $a = g \cdot b \cdot g^{-1}$.

Esta definición establece una relación de equivalencia. En efecto,

a) todo elemento es conjugado de sí mismo: $a = e \cdot a \cdot e^{-1}$;
b) si a es conjugado de b, entonces b es conjugado de a: $a = g \cdot b \cdot g^{-1} \Rightarrow b = g^{-1} \cdot a \cdot (g^{-1})^{-1}$;
c) si a es conjugado de b, y b lo es de c, entonces el primero es conjugado del último: $a = g \cdot b \cdot g^{-1},\ b = h \cdot c \cdot h^{-1} \Rightarrow a = (g \cdot h) \cdot c \cdot (g \cdot h)^{-1}$.

Mediante esta relación pueden organizarse los elementos del grupo G en clases de equivalencia, llamadas **clases de elementos conjugados**.

Algunas consecuencias:

- El elemento neutro forma una clase por sí solo: si $a = g \cdot e \cdot g^{-1} \Rightarrow a = e$.
- Si G es un grupo Abeliano, cada elemento forma una clase por sí mismo: $a = g \cdot b \cdot g^{-1} = b \cdot g \cdot g^{-1} = b$.
- Todos los elementos de una clase son del mismo orden: Supongamos que b es de orden n y que $a = g \cdot b \cdot g^{-1}$; entonces $a^n = g \cdot b^n \cdot g^{-1} = g \cdot e \cdot g^{-1} = e$.

Ejemplo: Para determinar las clases de elementos conjugados del grupo $\mathbf{S_n}$, consideremos dos permutaciones

$$\sigma = \begin{pmatrix} 1 & 1 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 1 & \dots & n \\ \tau(1) & \tau(2) & \dots & \tau(n) \end{pmatrix}. \tag{5.1}$$

La inversa de τ está dada por

$$\tau^{-1} = \begin{pmatrix} \tau(1) & \tau(2) & \dots & \tau(n) \\ 1 & 1 & \dots & n \end{pmatrix}, \tag{5.2}$$

de modo que

$$\tau \cdot \sigma \cdot \tau^{-1} = \begin{pmatrix} 1 & 1 & \dots & n \\ \tau(1) & \tau(2) & \dots & \tau(n) \end{pmatrix} \cdot \begin{pmatrix} \tau(1) & \tau(2) & \dots & \tau(n) \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

$$= \begin{pmatrix} \sigma(1) & \sigma(2) & \dots & \sigma(n) \\ \tau(\sigma(1)) & \tau(\sigma(2)) & \dots & \tau(\sigma(n)) \end{pmatrix} \cdot \begin{pmatrix} \tau(1) & \tau(2) & \dots & \tau(n) \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix} \tag{5.3}$$

$$= \begin{pmatrix} \tau(1) & \tau(2) & \dots & \tau(n) \\ \tau(\sigma(1)) & \tau(\sigma(2)) & \dots & \tau(\sigma(n)) \end{pmatrix}.$$

Este resultado corresponde a realizar la misma permutación de elementos que σ, pero a partir de un ordenamiento distinto, dado por $\tau(1)\ \tau(2)\ \dots\ \tau(n)$. Esto puede

verse fácilmente si se considera, por ejemplo, una transposición simple, $\sigma = (1\ 2)$; en ese caso,

$$\tau \cdot \sigma \cdot \tau^{-1} = \begin{pmatrix} \tau(1) & \tau(2) & \tau(3) & \dots & \tau(n) \\ \tau(2) & \tau(1) & \tau(3) & \dots & \tau(n) \end{pmatrix} = (\tau(1)\ \tau(2))\,. \tag{5.4}$$

En el caso general, se puede comprobar que σ y $\tau \cdot \sigma \cdot \tau^{-1}$ se descomponen en ciclos de la misma longitud, si bien los elementos involucrados por ellos en uno y otro caso son, en general, diferentes.

Recíprocamente, se puede mostrar que dos permutaciones que presentan la misma estructura en ciclos son conjugadas una de la otra.

De ese modo, la descomposición en ciclos permite caracterizar las clases de elementos conjugados en el grupo $\mathbf{S_n}$. Por ejemplo,

$$\mathbf{S_2}: \left\{ \begin{array}{l} e = (1)\,(2) \\ \gamma = (1\ 2) \end{array} \right\} \Rightarrow 2 \text{ clases}, \tag{5.5}$$

$$\mathbf{S_3}: \left\{ \begin{array}{l} e = (1)\,(2)\,(3) \\ a = (1\ 2\ 3),\ b = (1\ 3\ 2) \\ \alpha = (2\ 3),\ \beta = (3\ 1),\ \gamma = (1\ 2) \end{array} \right\} \Rightarrow 3 \text{ clases}, \tag{5.6}$$

$$\mathbf{S_4}: \left\{ \begin{array}{l} e \\ (1\ 2),\ (1\ 3),\ \dots \\ (1\ 2)\,(3\ 4),\ (1\ 3)\,(2\ 4),\ \dots \\ (1\ 2\ 3),\ (1\ 2\ 4),\ \dots \\ (1\ 2\ 3\ 4),\ (1\ 3\ 2\ 4),\ \dots \end{array} \right\} \Rightarrow 5 \text{ clases} \tag{5.7}$$

(donde hemos omitido los ciclos de longitud uno).

También se ve que el número de clases de $\mathbf{S_n}$ es igual al número de particiones de n. Por ejemplo, para $\mathbf{S_4}$

$$\begin{aligned} 4 &= 1+1+1+1, \\ 4 &= 2+1+1, \\ 4 &= 2+2, \\ 4 &= 3+1, \\ 4 &= 4. \end{aligned} \tag{5.8}$$

Esto permite representar gráficamente las clases mediante **diagramas de Young**, en los que cada ciclo es representado por un número de cuadros contiguos, dispuestos horizontalmente, igual a su longitud.

$$\{e\} \to \begin{array}{|c|}\hline\ \\\hline\ \\\hline\ \\\hline\ \\\hline\end{array}\ , \quad \{(1\ 2)\,(3)\,(4),\ \dots\} \to \begin{array}{|c|c|}\hline\ &\ \\\hline\ \\\cline{1-1}\ \\\cline{1-1}\end{array}\ ,$$

(5.9)

$$\{(1\ 2)\,(3\ 4),\ \dots\} \to \begin{array}{|c|c|}\hline\ &\ \\\hline\ &\ \\\hline\end{array}\ , \quad \{(1\ 2\ 3)(4),\ \dots\} \to \begin{array}{|c|c|c|}\hline\ &\ &\ \\\hline\ \\\cline{1-1}\end{array}\ ,$$

$$\{(1\ 2\ 3\ 4),\ \dots\} \to \begin{array}{|c|c|c|c|}\hline\ &\ &\ &\ \\\hline\end{array}\ .$$

También podemos calcular el número de permutaciones en cada clase considerando las posibles disposiciones de los cuatro elementos en los cuadros del correspondiente diagrama, teniendo en cuenta que disposiciones que difieren en una permutación cíclica de los elementos de un ciclo, o en el intercambio de los elementos de dos ciclos de la misma longitud, corresponden a la misma permutación:

$$\#\left(\begin{array}{|c|}\hline\ \\\hline\ \\\hline\ \\\hline\ \\\hline\end{array}\right) = \frac{4!}{4!} = 1, \quad \#\left(\begin{array}{|c|c|}\hline\ &\ \\\hline\ \\\cline{1-1}\ \\\cline{1-1}\end{array}\right) = \frac{4!}{2\times 2!} = 6,$$

(5.10)

$$\#\left(\begin{array}{|c|c|}\hline\ &\ \\\hline\ &\ \\\hline\end{array}\right)\frac{4!}{2^2\times 2!} = 3, \quad \#\left(\begin{array}{|c|c|c|}\hline\ &\ &\ \\\hline\ \\\cline{1-1}\end{array}\right) = \frac{4!}{3} = 8,$$

$$\#\left(\begin{array}{|c|c|c|c|}\hline\ &\ &\ &\ \\\hline\end{array}\right) = \frac{4!}{4} = 6,$$

cuya suma corresponde al orden del grupo, $\#G = 4!$.

La generalización al caso de $\mathbf{S_n}$ es inmediata: si en un diagrama se tienen r_1 ciclos de longitud 1, r_2 ciclos de longitud 2, etc, el orden de la clase es

$$\#(\dots) = \frac{n!}{1^{r_1}\times 2^{r_2}\times\cdots\times r_1!\times r_2!\dots}\,. \tag{5.11}$$

6. Subgrupos invariantes

Se llama **subgrupo conjugado** de un subgrupo $H \subset G$ a aquel subgrupo de G cuyos elementos se obtienen de los de H por conjugación con un elemento fijo

$g \in G$,

$$H' = g \cdot H \cdot g^{-1} = \{h' \in G \mid h' = g \cdot h \cdot g^{-1}, \text{ con } h \in H\}. \tag{6.1}$$

Este conjunto constituye efectivamente un subgrupo: sean $h'_1, h'_2 \in H'$, entonces $h'_{1,2} = g \cdot h_{1,2} \cdot g^{-1} \Rightarrow h'_1 \cdot (h'_2)^{-1} = g \cdot h_1 \cdot (h_2)^{-1} \cdot g^{-1} \in H'$, dado que $h_1 \cdot (h_2)^{-1} \in H$.

Un subgrupo se dice **invariante** si contiene a todos sus subgrupos conjugados, $g \cdot H \cdot g^{-1} \subset H$, $\forall\, g \in G$.

Si H es invariante, entonces contiene a sus elementos en clases completas: $h \in H \Rightarrow g \cdot h \cdot g^{-1} \in H,\ \forall\, g \in G$.

Ejemplos:

- Los subgrupos impropios $\{e\}$ y G, así como la intersección de subgrupos invariantes, son invariantes.
- Todo subgrupo de un grupo Abeliano es invariante.
- El núcleo $\phi^{-1}(e_H)$ de un homomorfismo $\phi : G \to H$ es un subgrupo invariante. En efecto, supongamos que $a \in \phi^{-1}(e_H) \Rightarrow \phi(a) = e_H$. Entonces, $\forall\, g \in G$ tenemos que $\phi(g \cdot a \cdot g^{-1}) = \phi(g) \cdot \phi(a) \cdot \phi(g^{-1}) = \phi(g) \cdot e_H \cdot \phi(g)^{-1} = e_H$. En consecuencia, el subgrupo $\phi^{-1}(e_H)$ (ver Sec. 4) contiene a sus elementos en clases completas.
- El conjunto de las **matrices regulares** (con inversa) de $n \times n$ forman el **grupo lineal** $GL(n)$ (respecto del producto usual de matrices). El conjunto de las matrices de $n \times n$ con determinante igual a 1 constituye el **subgrupo especial lineal** $SL(n)$, que es invariante. En efecto, si $M \in SL(n)$, $\det(N\, M\, N^{-1}) = \det N\ \det M\ (\det N)^{-1} = 1,\ \forall\, N \in GL(n)$.

Si H es un subgrupo invariante de G, entonces sus cosets izquierdos coinciden con los cosets derechos. En efecto, sea $a \cdot H = \{a \cdot h \,|\, h \in H\}$, entonces $a \cdot h = (a \cdot h \cdot a^{-1}) \cdot a = h' \cdot a \in H \cdot a,\ \forall\, h \in H$, puesto que $h' = a \cdot h \cdot a^{-1} \in H$. En consecuencia, $a \cdot H \subset H \cdot a$. De manera similar se demuestra que $H \cdot a \subset a \cdot H$. Por lo tanto, si H es invariante $\Rightarrow a \cdot H = H \cdot a,\ \forall\, a \in G$.

Un grupo se dice **simple** si no contiene subgrupos propios invariantes.

Un grupo se dice **semi-simple** si no contiene subgrupos propios Abelianos invariantes.

Ejemplo: los únicos grupos Abelianos simples son los grupos cíclicos de orden primo, que no tienen subgrupos propios.

7. El grupo cociente

Sea H un subgrupo invariante de G. Podemos descomponer a G en cosets izquierdos de H, de modo que $G = e\cdot H \cup a_1\cdot H \cup a_2\cdot H \ldots$, donde $a_k \notin H,\ \forall\, k$.

Consideremos dos elementos cualesquiera $a_i\cdot h_1 \in a_i\cdot H$ y $a_k\cdot h_2 \in a_k\cdot H$. Su composición es

$$(a_i\cdot h_1)\cdot(a_k\cdot h_2) = (a_i\cdot a_k)\cdot(a_k^{-1}\cdot h_1\cdot a_k)\cdot h_2 \in (a_i\cdot a_k)\cdot H, \tag{7.1}$$

puesto que $(a_k^{-1}\cdot h_1\cdot a_k)\in H,\ \forall\, h_1, h_2 \in H$.

Entonces resulta natural definir una operación entre cosets de modo que

$$(a_i\cdot H)\cdot(a_k\cdot H) = (a_i\cdot a_k)\cdot H\,. \tag{7.2}$$

Puesto que ella se basa en la composición en G, esta operación es asociativa. Existe un elemento neutro que corresponde a $H = e\cdot H$, y todo coset $a_k\cdot H$ tiene un inverso correspondiente al coset que contiene al elemento a_k^{-1}, $a_k^{-1}\cdot H$

$$\begin{aligned}(a\cdot H)\cdot(e\cdot H) &= (a\cdot e)\cdot H = (a\cdot H)\,,\\ (a\cdot H)\cdot(a^{-1}\cdot H) &= (a\cdot a^{-1})\cdot H = (e\cdot H)\,.\end{aligned} \tag{7.3}$$

Así estructurado, el conjunto de cosets del subgrupo invariante H conforma un grupo llamado **grupo cociente**, y denotado por G/H.

Es posible establecer un homomorfismo $\phi : G \to G/H$, cuyo núcleo es $\phi^{-1}(e_{G/H}) = H$. En efecto, sea ϕ una aplicación que asigne a cada elemento de G el coset que lo contiene,

$$\phi(h) := e\cdot H,\ \ \phi(a\cdot h) := a\cdot H,\ \ \forall\, h\in H,\ \ \forall\, a\notin H\,. \tag{7.4}$$

Entonces,

$$\begin{aligned}\phi(a_i\cdot h_1)\cdot\phi(a_k\cdot h_2) = (a_i\cdot H)\cdot(a_k\cdot H) = (a_i\cdot a_k)\cdot H =\\ = \phi((a_i\cdot a_k)\cdot h_3) = \phi((a_i\cdot h_1)\cdot(a_k\cdot h_2))\,,\end{aligned} \tag{7.5}$$

donde $h_3 = a_k^{-1}\cdot h_1\cdot a_k\cdot h_2 \in H$. Entonces ϕ es un homomorfismo de núcleo H.

Teorema 7.1. *Sea $\phi : G \to G'$ un homomorfismo sobreyectivo y de núcleo $\phi^{-1}(e') = H \subset G$. Entonces, H es un subgrupo invariante de G, y el grupo cociente G/H es isomorfo a G'.*

Demostración: Ya sabemos que el núcleo de un homomorfismo es un subgrupo invariante, respecto del cual podemos construir el grupo cociente G/H.

Definamos ahora una aplicación $\overline{\phi} : G/H \to G'$ de modo que $\overline{\phi}(a \cdot H) = \phi(a)$. Dado que dos elementos en $a \cdot H$ difieren en la composición con un elemento de H, esta asignación es independiente del elemento empleado para caracterizar el coset: $\phi(a \cdot h) = \phi(a) \cdot \phi(h) = \phi(a) \cdot e' = \phi(a),\ \forall\, h \in H$.

Entonces,

$$\overline{\phi}((a \cdot H) \cdot (b \cdot H)) = \overline{\phi}((a \cdot b) \cdot H) = \phi(a \cdot b) = \tag{7.6}$$
$$= \phi(a) \cdot \phi(b) = \overline{\phi}(a \cdot H) \cdot \overline{\phi}(b \cdot H)\,.$$

Por lo tanto, $\overline{\phi} : G/H \to G'$ es un homomorfismo.

Como el rango de $\phi(g)$ es todo G', $\forall\, g' \in G'\ \exists\, g \in G$ tal que $\overline{\phi}(g \cdot H) = \phi(g) = g'$. Por lo tanto, $\overline{\phi} : G/H \to G'$ también es sobreyectivo.

Finalmente, si $\overline{\phi}(a \cdot H) = \overline{\phi}(b \cdot H) \Rightarrow \phi(a) \cdot \phi(b)^{-1} = \phi(a \cdot b^{-1}) = e'$. Entonces, $a \cdot b^{-1} \in H \Rightarrow a = h \cdot b \in H \cdot b = b \cdot H$, por ser H invariante. Pero entonces $a \cdot H = b \cdot H$, y el homomorfismo es uno a uno (es decir, es un isomorfismo).

Por lo tanto, $G/H \approx G'$. □

8. Producto directo de grupos

A partir de dos grupos G_1 y G_2 es posible construir un tercer grupo $G = G_1 \times G_2$, llamado **producto directo**, de la siguiente manera.

Sean $a_1, b_1, c_1, \cdots \in G_1$ y $a_2, b_2, c_2, \cdots \in G_2$. El grupo $G_1 \times G_2$ es el conjunto de los pares ordenados $\langle g_1, g_2 \rangle$ estructurado con la ley de composición

$$\langle a_1, a_2 \rangle \cdot \langle b_1, b_2 \rangle := \langle a_1 \cdot a_2, b_1 \cdot b_2 \rangle\,. \tag{8.1}$$

Puede verificarse que esta ley es asociativa, tiene por elemento neutro al par $\langle e_1, e_2 \rangle$, y el inverso de $\langle g_1, g_2 \rangle$ es el par $\langle g_1^{-1}, g_2^{-1} \rangle$.

Si G_1 y G_2 son de orden finito, $\#G = \#G_1\, \#G_2$.

Los elementos de la forma $\langle e_1, g_2 \rangle$ forman un subgrupo invariante $\widetilde{G_2}$ de $G_1 \times G_2$, isomorfo a G_2. Similarmente, los pares de la forma $\langle g_1, e_2 \rangle$ forman un subgrupo invariante $\widetilde{G_1}$ de $G_1 \times G_2$, isomorfo a G_1. Evidentemente, elementos de esos subgrupos conmutan entre sí,

$$\langle e_1, g_2 \rangle \cdot \langle g_1, e_2 \rangle = \langle g_1, g_2 \rangle = \langle g_1, e_2 \rangle \cdot \langle e_1, g_2 \rangle\,, \tag{8.2}$$

y todo elemento de $G_1 \times G_2$ puede escribirse en la forma de un producto como en (8.2).

Puede verificarse fácilmente que $G/\widetilde{G_2} \approx G_1$, y que $G/\widetilde{G_1} \approx G_2$.

Recíprocamente, si un grupo G tiene dos subgrupos invariantes G_1 y G_2 tales que

$$G_1 \cap G_2 = \{e\}\,,$$

$$g_1 \cdot g_2 = g_2 \cdot g_1,\ \forall\, g_1 \in G_1\,, g_2 \in G_2\,, \tag{8.3}$$

y si todo elemento $g \in G$ tiene una descomposición (única[2]) como un producto de la forma $g = g_1 \cdot g_2$, con $g_1 \in G_1\,, g_2 \in G_2$, entonces $G = G_1 \times G_2$. También en este caso $G/G_2 \approx G_1$ y $G/G_1 \approx G_2$.

9. Automorfismo - Centro de un grupo

Un **automorfismo** es un isomorfismo de un grupo en sí mismo, $\phi : G \leftrightarrow G$. El conjunto de todos los automorfismos forma un grupo respecto de la composición usual de aplicaciones. Su elemento neutro es la aplicación identidad.

Ejemplo: Para el grupo cíclico $\{e, a, a^2\}$, la aplicación

$$\phi(e) = e\,,\ \phi(a) = a^2\,,\ \phi(a^2) = a\,, \tag{9.1}$$

es un automorfismo.

Un **endomorfismo** es un automorfismo definido mediante la conjugación por un elemento fijo del grupo,

$$\phi_a : G \leftrightarrow G \mid \phi_a(g) = a \cdot g \cdot a^{-1},\ \forall\, g \in G\,. \tag{9.2}$$

El conjunto de los endomorfismos sobre G forma un subgrupo del grupo de los automorfismos, que resulta ser homomorfo al propio grupo G. En efecto,

$$(\phi_a \circ \phi_b)(g) = \phi_a\left(\phi_b(g)\right) = \phi_a\left(b \cdot g \cdot b^{-1}\right) =$$

$$= \phi_a(b) \cdot \phi_a(g) \cdot \phi_a(b^{-1}) = a \cdot b \cdot g \cdot b^{-1} \cdot a^{-1} = \tag{9.3}$$

$$= (a \cdot b) \cdot g \cdot (a \cdot b)^{-1} = \phi_{a\cdot b}(g),\ \forall\, g \in G\,.$$

Por lo tanto $\phi_a \circ \phi_b = \phi_{a\cdot b}$, y la aplicación $a \mapsto \phi_a$ es un homomorfismo. En particular, $e \mapsto \phi_e$, la identidad en el grupo de automorfismos.

[2]En efecto, si un elemento de G puede expresarse como $g = g_1 \cdot g_2$, y también como $g = g_1' \cdot g_2'$, donde $g_1, g_1' \in G_1$ y $g_2, g_2' \in G_2$, entonces $(g_1')^{-1} \cdot g_1 = g_2' \cdot g_2^{-1} = e$, de donde resulta que la descomposición es única.

El núcleo de este homomorfismo está constituido por los elementos de G para los cuales $a \mapsto \phi_a = \phi_e$, es decir, tales que

$$\phi_a(g) = a \cdot g \cdot a^{-1} = \phi_e(g) = g \Rightarrow a \cdot g = g \cdot a, \ \forall\, g \in G\,. \tag{9.4}$$

Esto corresponde al **centro** del grupo G, es decir, al conjunto C de aquellos elementos que conmutan con todo otro elemento de G.

Por ser el núcleo de un homomorfismo, C es un subgrupo invariante de G, y entonces el grupo de endomorfismos es isomorfo a G/C (ver Teorema 7.1).

10. Espacios clásicos

En lo que sigue estaremos interesados en representaciones matriciales de grupos, es decir, en homomorfismos con grupos de operadores lineales definidos sobre espacios de dimensión finita.

En un espacio euclídeo de dimensión n, $\mathbf{E}$, generado por la base $\{e_1, e_2, \ldots, e_n\}$, los vectores tienen desarrollos de la forma

$$x = \sum_{k=1}^{n} x_k\, e_k\,, \quad y = \sum_{k=1}^{n} y_k\, e_k\,, \tag{10.1}$$

y el producto escalar (hermítico y positivo definido) puede escribirse como

$$(x, y) = \sum_{k,l=1}^{n} x_k^*\, (e_k, e_l)\, y_l = \sum_{k,l=1}^{n} x_k^*\, g_{kl}\, y_l\,, \tag{10.2}$$

donde $g_{kl} = (e_k, e_l) = g_{lk}^*$.

En esas condiciones, la **métrica** del espacio $g = (g_{kl})$ define una ***forma cuadrática, hermítica y positiva definida,*** sobre $\mathbb{C}^n$,

$$\overline{x}^\dagger g\, \overline{y} = (x, y) = \left(\overline{y}^\dagger g\, \overline{x}\right)^*, \tag{10.3}$$

donde $\overline{x}, \overline{y} \in \mathbb{C}^n$ tienen por componentes a los coeficientes de Fourier en (10.1).

Como la métrica es una matriz autoadjunta, $g^\dagger = g$, ella puede ser diagonalizada para llevarla a la forma $\mathrm{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n)$, con los $\lambda_k > 0$. Un cambio adecuado en las escalas de los vectores de la base permite reducirla a la matriz identidad, $g = \mathbf{1_n}$ (lo que corresponde a adoptar una base ortonormal para $\mathbf{E}$).

En el caso de espacios euclídeos reales, la métrica g define una ***forma bilineal, simétrica y positiva definida*** sobre $\mathbb{R}^n$,

$$\overline{x}^t\, g\, \overline{y} = (x, y) = \overline{y}^t\, g\, \overline{x}\,, \tag{10.4}$$

donde $\overline{x}, \overline{y} \in \mathbb{R}^n$, y $g^t = g$.

Ahora bien, en la Física también tienen aplicación espacios lineales más generales que los espacios euclídeos. Por ejemplo, el espacio de Minkowsky $\mathbf{M}_4$, que es un espacio real con métrica simétrica pero no positiva definida, $g = \mathrm{diag}(+1, -1, -1, -1)$.

Un espacio $\mathbf{E}$ con un producto interior hermítico que no es positivo definido es llamado **pseudo-euclídeo**. También en este caso puede elegirse una base para $\mathbf{E}$ formada por vectores ***unitarios*** ortogonales, $\{e_1, e_2, \ldots, e_n\}$ con $(e_k, e_l) = 0$, para $k \neq l$. Pero como la ***norma*** no es positiva definida se tiene que

$$(e_k, e_l) = (e_l, e_k)^* = g_{kl} = \begin{cases} +\delta_{kl}, \ 1 \leq k \leq p\,, \\ -\delta_{kl}, \ p+1 \leq k \leq p+q = n\,, \end{cases} \tag{10.5}$$

donde el par de enteros $\langle p, q\rangle$, cuya suma es la dimensión de $\mathbf{E}$, es la **signatura** del espacio. Esta signatura es una propiedad del espacio, y no depende de la elección de un sistema ***ortonormal*** en $\mathbf{E}$.

La métrica de los espacios pseudo-euclídeos, dada por la matriz autoadjunta $g = (g_{kl}) = g^\dagger = g^{-1}$, define una forma hermítica sobre $\mathbb{C}^n$, que no es positiva definida:

$$\overline{x}^\dagger g\, \overline{y} = (x, y) = \left(\overline{y}^\dagger g\, \overline{x}\right)^*. \tag{10.6}$$

En estos espacios existen vectores no nulos que tienen ***norma*** nula.

En espacios pseudo-euclídeos reales de dimensión n, la métrica $g = g^t$ es una matriz real y simétrica que define una ***forma cuadrática bilineal simétrica***, no positiva definida, sobre $\mathbb{R}^n$,

$$\overline{x}^t g\, \overline{y} = (x, y) = \overline{y}^t g\, \overline{x}\,. \tag{10.7}$$

Si en un espacio lineal (real o complejo) se tiene un producto interior ***bilineal y antisimétrico***,

$$(a\,x, b\,y) = a\,b\,(x, y)\,, \quad (x, y) = -\,(y, x)\,, \tag{10.8}$$

se está en presencia de un **espacio simpléctico**.

Se puede mostrar (ver más adelante) que estos espacios tienen dimensión par, y que en ellos siempre puede seleccionarse un sistema completo de vectores ***unitarios*** de la forma $\{e_1, e_2, \ldots, e_n, f_1, f_2, \ldots, f_n\}$, los que satisfacen

$$\begin{aligned} &(e_k, e_l) = 0 = (f_k, f_l)\,, \\ &(e_k, f_l) = \delta_{kl} = -(f_l, e_k)\,, \end{aligned} \tag{10.9}$$

para $k, l = 1, 2, \ldots, n$. Desarrollando los vectores respecto de esa base tenemos

$$(x, y) = \overline{x}^t g\, \overline{y} = -\overline{y}^t g\, \overline{x}\,, \tag{10.10}$$

donde la métrica

$$g = \begin{pmatrix} \mathbf{0} & \mathbf{1_n} \\ \mathbf{-1_n} & \mathbf{0} \end{pmatrix} = -g^t \tag{10.11}$$

define una ***forma bilineal antisimétrica*** sobre $\mathbb{R}^n$ ó $\mathbb{C}^n$, según el caso.

Todo vector de un espacio simpléctico tiene ***norma*** nula,

$$\overline{x}^t g\, \overline{x} = -\overline{x}^t g\, \overline{x} = 0\,. \tag{10.12}$$

11. Operadores isométricos

Un operador lineal que conserva los productos interiores en un espacio clásico **E**,

$$(A\,x, A\,y) = (x, y)\,,\ \forall\, x, y \in \mathbf{E}\,, \tag{11.1}$$

se dice **isométrico**.

Un operador isométrico es llamado **unitario, pseudo-unitario o simpléctico** según que el espacio sea euclídeo, pseudo-euclídeo o simpléctico respectivamente.

De la definición del operador adjunto tenemos que

$$(A\,x, A\,y) = \left(A^\dagger A\,x, y\right)\,,\ \forall\, x, y \in \mathbf{E}\,, \tag{11.2}$$

de donde resulta que $A^\dagger = A^{-1}$ (en dimensión finita, el inverso a izquierda es también el inverso a derecha).

El conjunto de los operadores isométricos (o **isometrías**) sobre un espacio **E** forma un grupo respecto de la composición usual de operadores. En efecto, tenemos que

- el operador identidad es una isometría,
- cada isometría tiene una inversa dada por su adjunto, que es también isométrico:

$$\left(A^\dagger\, x, A^\dagger\, y\right) = \left(AA^\dagger\, x, AA^\dagger\, y\right) = (x, y)\,,\ \forall\, x, y \in \mathbf{E}\,, \tag{11.3}$$

- si A y B son isométricos, entonces AB es también una isometría:

$$\begin{aligned} \left((AB)\,x, (AB)\,y\right) &= \left(A(B\,x), A(B\,y)\right) = \\ &= (B\,x, B\,y) = (x, y)\,,\ \forall\, x, y \in \mathbf{E}\,. \end{aligned} \tag{11.4}$$

Referido a una base de $\mathbf{E}$, el operador A está descrito por una matriz $\mathcal{A} = (A_{kl})$. Si la métrica es hermítica, tenemos

$$(A\,x, A\,y) = (A_{ki}\,x_i)^*\,g_{kl}\,(A_{lj}\,y_j) = \\ = \overline{x}^\dagger\,\mathcal{A}^\dagger\,g\,\mathcal{A}\,\overline{y} = \overline{x}^\dagger\,g\,\overline{y},\ \forall\,\overline{x},\overline{y}\in\mathbb{C}^n\ (\text{ó }\mathbb{R}^n) \Rightarrow \mathcal{A}^\dagger\,g\,\mathcal{A} = g\,, \tag{11.5}$$

En consecuencia, las isometrías preservan la métrica del espacio. En términos de la matriz adjunta, la inversa está dada por $\mathcal{A}^{-1} = g^{-1}\,\mathcal{A}^\dagger\,g$.

De esa relación se deduce inmediatamente que

$$\det\left(\mathcal{A}^\dagger\,g\,\mathcal{A}\right) = \det\mathcal{A}^\dagger\,\det g\,\det\mathcal{A} = \det g \neq 0 \Rightarrow |\det\mathcal{A}|^2 = 1\,, \tag{11.6}$$

es decir, $\det\mathcal{A} = e^{i\theta}$ si el espacio es complejo, o $\det\mathcal{A} = \pm 1$ si el espacio es real.

Si la métrica es bilineal y antisimétrica,

$$(A\,x, A\,y) = (A_{ki}\,x_i)\,g_{kl}\,(A_{lj}\,y_j) = \\ = \overline{x}^t\,\mathcal{A}^t\,g\,\mathcal{A}\,\overline{y} = \overline{x}^t\,g\,\overline{y},\ \forall\,\overline{x},\overline{y}\in\mathbb{C}^n\ (\text{ó }\mathbb{R}^n) \Rightarrow \mathcal{A}^t\,g\,\mathcal{A} = g\,. \tag{11.7}$$

También en los espacios simplécticos las isometrías preservan la métrica. La matriz inversa está dada por $\mathcal{A}^{-1} = g^{-1}\,\mathcal{A}^t\,g$.

Además

$$\det\left(\mathcal{A}^t\,g\,\mathcal{A}\right) = (\det\mathcal{A})^2\,\det g = \det g \neq 0 \Rightarrow (\det\mathcal{A})^2 = 1\,, \tag{11.8}$$

pero en este caso se puede mostrar que $\det\mathcal{A} = 1$.

En particular, el operador correspondiente a la matriz $\mathcal{M} = g^{-1}\,g^t$ es una isometría en los espacios simplécticos. En efecto,

$$\mathcal{M}^t\,g\,\mathcal{M} = g\left(g^{-1}\right)^t\,g\,g^{-1}\,g^t = g\,. \tag{11.9}$$

Esta matriz es también **unimodular**,

$$\det\mathcal{M} = \det\left(g^{-1}g^t\right) = (\det g)^{-1}\det g = 1\,. \tag{11.10}$$

Pero como la métrica es antisimétrica, $\mathcal{M} = g^{-1}g^t = -g^{-1}g = -\mathbf{1}_{\dim\mathbf{E}} \Rightarrow \det\mathcal{M} = (-1)^{\dim\mathbf{E}}$. En consecuencia, la dimensión de los espacios simplécticos es necesariamente par.

12. Principales grupos de matrices

Ya hemos mencionado anteriormente al **grupo general lineal** $GL(n, \mathbb{R}$ ó $\mathbb{C})$, formado por las matrices (reales o complejas) regulares de $n \times n$, y a su subgrupo **especial lineal** $SL(n, \mathbb{R}$ ó $\mathbb{C})$, de matrices unimodulares.

De acuerdo a los resultados de la sección anterior, podemos introducir distintos grupos de isometrías.

En un espacio euclídeo complejo de dimensión n y métrica $g = \mathbf{1_n}$, las matrices **unitarias**[3], $U^\dagger U = \mathbf{1_n}$ forman el grupo $U(n)$. Si $U \in U(n) \Rightarrow |\det U| = 1$.

Este grupo contiene un subgrupo (invariante) unimodular $SU(n)$, formado por las matrices unitarias de determinante igual a 1.

En un espacio euclídeo real de dimensión n, el conjunto de las matrices **ortogonales** de $n \times n$, $R^t R = \mathbf{1_n}$ conforman el grupo $O(n)$. Si $R \in O(n) \Rightarrow \det R = \pm 1$.

Este grupo contiene un subgrupo (invariante) $SO(n)$, formado por las matrices ortogonales de determinante igual a 1.

En el caso de espacios pseudo-euclídeos con métrica

$$g = \begin{pmatrix} \mathbf{1_p} & \mathbf{0} \\ \mathbf{0} & -\mathbf{1_q} \end{pmatrix}, \tag{12.2}$$

el grupo de isometrías corresponde al de las matrices **pseudo-unitarias** $U(p, q)$ o **pseudo-ortogonales** $O(p, q)$, según sea el espacio complejo o real,

$$\begin{aligned} U^\dagger g\, U = g \Rightarrow |\det U| = 1\,, \\ R^t g\, R = g \Rightarrow \det R = \pm 1\,. \end{aligned} \tag{12.3}$$

Esos grupos contienen subgrupos unimodulares invariantes, denotados por $SU(p, q)$ y $SO(p, q)$ respectivamente.

Finalmente, en un espacio simpléctico de dimensión $2n$ con métrica

$$g = \begin{pmatrix} \mathbf{0} & \mathbf{1_n} \\ -\mathbf{1_n} & \mathbf{0} \end{pmatrix}, \tag{12.4}$$

---

[3]La aplicación **exponencial** de una matriz M se define por la serie

$$e^M = \sum_{n=0}^{\infty} \frac{M^n}{n!}, \tag{12.1}$$

que converge en el sentido de la norma de los operadores.

Si $A = A^\dagger$ es una matriz autoadjunta, entonces e^{iA} es unitaria. En efecto, $\left(e^{iA}\right)^\dagger = e^{-iA^\dagger} = \left(e^{iA}\right)^{-1}$.

Similarmente, si $K = -K^t$ es antisimétrica, entonces e^K es una matriz ortogonal: $\left(e^K\right)^t = e^{-K} = \left(e^K\right)^{-1}$.

el grupo de isometrías corresponde al grupo de matrices **simplécticas** $Sp(2n, \mathbb{R}$ ó $\mathbb{C})$, $M^t\, g\, M = g$, las que (como se dijo) tienen determinante $\det M = 1$.

Bibliografía:

- H. Bacry, *Leçons sur la Théorie des Groupes et les Symmétries des Particules Elémentaires.*
- M. Hammermesh, *Group Theory and its Applications to Physical Problems.*