Capítulo

3

Teorema de Lagrange

3.1 Introducción

En este capítulo estudiaremos uno de los teoremas más importantes de toda la teoría de grupos como lo es el Teorema de Lagrange. Daremos en primer lugar una serie de resultados básicos que se derivan de la definición de grupos. Posteriormente se introduce el concepto de subgrupo y en especial se estudian las propiedades de los grupos ciclícos.

Si H es un subgrupo de un grupo finito G, entonces el Teorema de Lagrange establece que el orden de H es un divisor del orden de G. Este resultado genera una serie de propiedades interesantes de los grupos finitos de tipo estructural. Finalizamos el capítulo con el estudio de las clases laterales de un subgrupo H de G.

3.2 Resultados Preliminares

En esta sección demostramos algunos hechos básicos sobre grupos, que se pueden deducir de la definición 1.3.1.

Lema 3.2.1 *Si G es un grupo entonces*
a) El elemento identidad es único.
b) Todo $a \in G$ tiene un inverso único en G.
c) Para todo $a \in G$, $(a^{-1})^{-1} = a$.
d) Para todo $a, b \in G$, $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

Demostración: *a)* Sean e y f dos elementos identidad en G. Entonces se tiene la ecuación.

$$e = e \cdot f = f,$$

de donde

$$e = f$$

b) Supongamos que un elemento $a \in G$ posee dos inversos x e y.

Luego

$$x \cdot a = a \cdot x = e$$
$$y \cdot a = a \cdot y = e$$

Luego

$$\begin{aligned} y(a \cdot x) &= y \cdot e = y \\ (y \cdot a) \cdot x &= y \\ e \cdot x &= y \\ x &= y \end{aligned}$$

c) Para $a \in G$, se tiene

$$a^{-1} \cdot a = e$$
$$a \cdot a^{-1} = e$$

Luego a es el inverso de a^{-1}, único, y por lo tanto $(a^{-1})^{-1} = a$.

d) Sean $a, b \in G$. Luego

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

Similarmente

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

Por lo tanto

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

♠

Proposición 3.2.1 *Sean a y b en el grupo G. Entonces las ecuaciones*

$$a\cdot x = b \tag{3.1}$$
$$y\cdot a = b, \tag{3.2}$$

poseen solución única: $x = a^{-1}\cdot b$; $y = b\cdot a^{-1}$.

Demostración: Multiplicando (**??**) por a^{-1} a la izquierda tenemos

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

Similarmente, multiplicando (**??**) por a^{-1} a la derecha tenemos

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

♠

Lema 3.2.2 *Sean a, u, w elementos en G. Entonces valen las siguientes* **leyes de cancelación** *en G.*

$$a \cdot u = a \cdot w \quad \text{implica} \quad u = w \tag{3.3}$$
$$u \cdot a = w \cdot a \quad \text{implica} \quad u = w \tag{3.4}$$

Demostración: La ecuación

$$a \cdot u = a \cdot w$$

posee solución única

$$\begin{aligned}u &= a^{-1}(a \cdot w) \\ &= (a^{-1} \cdot a)w \\ &= e \cdot w \\ &= w\end{aligned}$$

Similarmente, la ecuación

$$u \cdot a = w \cdot a$$

posee solución única

$$\begin{aligned} u &= (w \cdot a)(a^{-1}) \\ &= w(a \cdot a^{-1}) \\ &= w \cdot e \\ &= w \end{aligned}$$

Ejercicios

1) Sea m un entero positivo fijo. Diremos que dos enteros a y b son **congruentes módulo m** y lo denotamos por:

$$a \equiv b \; mod \; m,$$

si m divide a $b - a$

Probar que la relación de congruencia módulo m en el conjunto $\mathbb{Z}$ es una relación de equivalencia.

2) Para cada entero a en $\mathbb{Z}$, se define su **clase de congruencia módulo** m, como el conjunto formado por su clase de equivalencia

$$[a] = \{x \in \mathbb{Z} | x \equiv a \; mod \; m\}$$

El conjunto formado por todas estas clases se llaman **Enteros módulo** m y se denota por $\mathbb{Z}_m$.

Probar que $\mathbb{Z}_m$ es un grupo, bajo la operación de suma módulo m, definida por:

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

¿Cuál es el elemento neutro de este grupo? Construya una tabla para la operación de suma módulo 7.

3) Demuestre que todo grupo de orden ≤ 5 debe ser abeliano.

4) Probar que si G es un grupo abeliano y a, b pertenecen a G, entonces

$$(ab)^n = a^n b^n$$

para todo entero $n \geq 0$.

5) Sea G un conjunto no vacío cerrado con una operación asociativa, tal que

i) Existe un elemento $e \in G$ tal que

$$ae = a$$

para todo $a \in G$.

ii) Para todo $a \in G$ existe un elemento a', tal que

$$a'a = e$$

probar que G es un grupo con esta operación.

6) Sea G un conjunto finito, el cual es cerrado bajo una operación asociativa y tal que valen las dos leyes de cancelación. Es decir, para todos a, b, c en G se tiene

$$ab = ac \Longrightarrow b = c$$

$$ba = ca \Longrightarrow b = c$$

Probar que G es un grupo con esta operación.

7) Hallar los inversos de cada uno de los elementos de S_3.

8) Sea S_7 el grupo de permutaciones de 7 elementos con la composición de aplicaciones, como en S_3. Probar que existe un elemento a, tal que $a^{12} = e$, pero $a^s \neq e$ para $0 < s < 12$.

9) Sea G un grupo. Probar que para cualquier par de enteros m y n se tiene

i) $a^m a^n = a^{m+n}$

ii) $(a^m)^n = a^{mn}$

para todo a en G.

10) Si G es un grupo de orden par, probar que existe un elemento $a \in G$, $a \neq e$ y tal que $a^2 = e$.

11) Hallar todos los elementos de $\mathbb{Z}_{12}$ que satisfacen la ecuación $x^6 = 1$.

12) Sea $G = M_2(\mathbb{R})$ el grupo de matrices invertibles cuadradas de orden 2 sobre $\mathbb{R}$, con la operación producto. Probar que G no es abeliano.

13) Probar que el conjunto de matrices invertibles cuadradas de orden 2 sobre $\mathbb{R}$, con la operación producto y con determinante 1 es un grupo.

14) Demuestre que en los enteros módulo 7, todo elemento $a \neq e$ satisface:

i) $a^7 = e$

ii) $a^s \neq e$, para todo $0 < s < 7$.

15) Sea Q^* el conjunto de los números racionales direrentes de cero. Probar que $(Q^*, .)$ no es un grupo cíclico.

3.3 Subgrupos

Definición 3.3.1 *Sea G un grupo y $H \subseteq G$. Si H es un grupo con la operación definida en G, entonces H se dice* **subgrupo de G.**

Ejemplo: Sea $G = (\mathcal{Q}, +)$ el grupo de los números racionales con la adición y $H = (\mathbb{Z}, +)$ el grupo de los enteros con la adición. Entonces H es subgrupo de G.

Para indicar que H es subgrupo de G, usaremos la notación: $H < G$.

Definición 3.3.2 *Un subgrupo H de G se dice* **subgrupo propio** *si $H < G$ y $H \neq \{e\}$, $H \neq G$.*

Nota: Si G es un grupo, los subgrupos G y $\{e\}$ se llaman **los subgrupos triviales de G.**

Ejemplo 1: Sea G un grupo de orden 3. Entonces G es de la forma $G = \{e, a, a^2\}$. Se puede verificar que G no tiene subgrupos propios.

Ejemplo 2: Sea G el grupo de los enteros módulo 4 con la suma y H formado por los elementos $\bar{0}$ y $\bar{2}$. Entonces H es un subgrupo de G.

Ejemplo 3: Sea V el grupo 4 de Klein, $V = \{e, a, ab\}$ sujeto a las relaciones $a^2 = b^2 = e$. Entonces el conjunto $H = \{e, a\}$ es un subgrupo de G.

Podemos hacer un diagrama de los subgrupos de G, para los dos ejemplos anteriores.

Así tenemos

El siguiente teorema establece un criterio muy útil para determinar cuando un subconjunto H de un grupo G es un subgrupo.

Teorema 3.3.1 *Un subconjunto H de de un grupo G es un subgrupo, si y sólo si*

i) $a \cdot b \in H$ *para todo* $a, b \in H$

ii) $a^{-1} \in H$ *para todo* $a \in H$.

Demostración: Puesto que la operación binaria en G es asociativa, sólo falta verificar que $e \in G$. En efecto, sea $a \in H$, luego $a^{-1} \in H$ (por ii)) y además $a \cdot a^{-1} = e \in H \quad (\text{por } i))$.

Luego H es un grupo, y por lo tanto un subgrupo de G.

♠

Teorema 3.3.2 *Sea G un grupo y $a \in G$. Entonces el conjunto*

$$H = \{a^n \mid n \in \mathbb{Z}\}$$

es un subgrupo de G. Además H es el subgrupo de G más pequeño que contiene a.

Demostración: De acuerdo al teorema anterior, será suficiente con probar:

i) $a^n \cdot a^m \in H$, para $a^n, a^m \in H$
ii) $(a^n)^{-1} \in H$. para $a^n \in H$.

Claramente $a^n \cdot a^m = a^{n+m} = a^z \quad \text{con} \quad z = n + m \in \mathbb{Z}$, y por lo tanto $a^n \cdot a^m \in H$.

También

$$(a^n)^{-1} = a^{-n} \in H$$

Luego $H < G$.

Para probar la segunda afirmación, sea K un subgrupo de G y $a \in K$. Luego $a^0 = e \in K$ por ser K un grupo. También $a^2 \in K$, pues $a \in K$ y K es cerrado bajo la operación en G. De esta forma se concluye $a^n \in K$ para todo $n \geq 0$.

También $a^{-1} \in K$, pues $a \in K$ y su inverso se halla en K. Similarmente $a^{-2} = a^{-1} \cdot a^{-1} \in K$, pues $a^{-1} \in K$ y K es cerrado. Luego $a^{-n} \in K$ para todo $n \geq 0$. Hemos probado entonces que $H \subseteq K$

♠

Definición 3.3.3 *El grupo H, se llama* **subgrupo cíclico** *generado por a. El elemento a se llama el* **generador de** *H. Usaremos la notación:*

$$H =< a > .$$

Definición 3.3.4 *Un grupo G se dice* **cíclico** *si $G =< a >$ para algún $a \in G$.*

Ejemplo 1: Sea G el grupo formado por los enteros con la suma. Entonces $G =< 1 >$.

Ejemplo 2: Sea G el grupo de los enteros módulo 4, luego $G =< \bar{1} >$

Ejemplo 3: Sea $G = S_3$ y $K =< \phi >$, Entonces K es cíclico de orden 2.

3.4 Teorema de Lagrange

En esta sección estudiaremos una condición necesaria necesaria para que un subconjunto de un grupo finito, sea un subgrupo de este.

Teorema 3.4.1 *(Lagrange)*
Sea G un grupo finito y H un subgrupo de G. Entonces el orden de H divide al orden de G.

Demostración: Si $H = \{e\}$ ó $H = G$ no hay nada que probar. Supongamos entonces que $H \neq \{e\}$ y $H \neq G$. Sea

$$H = \{h_1, \ldots, h_r\}$$

donde $r = \circ(H)$.

Luego existe un elemento $a \in G$, tal que $a \notin H$. Entonces tenemos los siguientes elementos en G.

$$h_1, h_2, \ldots, h_r, ah_1, \ldots, ah_r.$$

Afirmamos que hay $2r$ elementos distintos. En efecto:
i)$Si\ ah_i = h_j$, entonces multiplicando por h_i^{-1} a la derecha nos da

$$a = h_j h_i^{-1} \in H$$

Luego $a \in H$, lo cual es una contradicción
ii) Si $ah_i = ah_j$, cancelación por a nos da

$$h_i = h_j$$

lo cual es, nuevamente una contradicción.

Si esos $2r$ elementos son todos elementos de G, entonces

$$\circ(G) = 2r = 2 \circ (H)$$

y entonces $\circ(H)$ divide al orden de G.

Si por el contrario, hay más de $2r$ elementos en G, continuamos el proceso y tendremos que existe un elemento $b \in G$, distinto de los anteriores. Luego tenemos los siguientes elementos en G

$$\begin{array}{cccc} a_0h_1, & \ldots, & a_0h_r \\ a_1h_1, & \ldots, & a_1h_r \\ a_2h_1, & \ldots, & a_2h_r \\ & \vdots & \end{array}$$

donde $a_0 = e$, $a_1 = a$, $a_2 = b$,...etc. y a_i no esta en ninguno de los elementos que forman las filas anteriores a la fila i-ésima. Se puede probar que todos estos elementos que se generan son distintos. En efecto:

i) Si $a_ih_j = a_ih_k$, entonces cancelando se tiene que $h_j = h_k$, lo cual es una contradicción.

ii) Si para $i > l$ se tiene $a_ih_j = a_lh_k$, entonces multiplicando por h_j^{-1} a la derecha se tiene $a_i = a_lh_kh_j^{-1}$. Como H es un grupo , tendremos que $h_kh_j^{-1} \in H$, luego $h_kh_j^{-1} = h_s$, para algún s y por lo tanto $a_i = a_lh_s$. Entonces el elemento a_i pertenece a la l-ésima fila, lo cual es una contradicción.

Puesto que G es un grupo finito, este proceso de formación de filas se detiene despúes de un número finito de pasos, digamos k pasos. Se tendrá entonces que hay $k \circ (H)$ elementos en G. Con esto termina la desmostración.

♠

Definición 3.4.1 *Si G es un grupo y $a \in G$, el* **orden de a** *es el menor entero positivo n tal que*

$$a^n = e.$$

Usamos la notación $\circ(a)$ para indicar el orden de a.

Si ese entero no existe, diremos que a tiene **orden infinito**

Corolario 3.4.1 *Si G es un grupo finito y $a \in G$, entonces $\circ(a)$ es un divisor de $\circ(G)$.*

Demostración: Sea $a \in G$ y consideremos el subgrupo cíclico generado por a, $H =< a >$ el cual consiste en los elementos

$$a^0 = e, a, a^2, \ldots, a^{n-1}$$

donde $a^n = e$.

Es claro entonces que $n = \circ(H)$ y además $n = \circ(a)$.

De acuerdo al teorema de Lagrange, tendremos que

$$\circ(H) | \circ(G)$$

Luego

$$\circ(a) | \circ(G).$$

♠

Corolario 3.4.2 *Si G es un grupo finito y $a \in G$, entonces*

$$a^{\circ(G)} = e.$$

Demostración: Sabemos que $a^{\circ(a)} = e$, y por el corolario anterior

$$\circ(G) = k \circ (a) \quad \text{para algún } \ k.$$

Luego

$$\begin{aligned} a^{\circ(G)} &= a^{\circ(a)\cdot k} \\ &= \left(a^{\circ(a)}\right)^k \\ &= e^k \\ &= e. \end{aligned}$$

Corolario 3.4.3 *Si G es un grupo finito de orden primo p, entonces G es cíclico.*

Demostración: Sea $a \in G$, $a \neq e$. Entonces $H =< a >$ el subgrupo cíclico generado por a tiene orden un divisor de p. Luego hay dos posibilidades:

i) $\circ(H) = p$, lo cual implica $H = G$ y G es cíclico generado por a

ii) $\circ(H) = 1$, y por lo tanto se tendría $a = e$, lo cual es imposible. Luego G es un grupo cíclico.

♠

Ejercicios

1)Probar que $(\mathbb{Z}_6, +)$ es un grupo cíclico. Hallar todos sus generadores.

2) Demuestre que el grupo 4 de Klein no es cíclico.

3) Hallar el orden de cada uno de los elementos del grupo $(\mathbb{Z}_{10}, +)$.

4) Sea p un número primo. Probar que Q_p el conjunto de números racionales de la forma

$$\frac{a}{p^\alpha}$$

donde a es un entero primo relativo con p, y α es un entero positivo, es un subgrupo de $(Q, +)$.

5) Demuestre que si p es un número primo, entonces el grupo $(\mathbb{Z}_p, +)$ tiene p-1 generadores.

6) Demuestre que el grupo de los enteros módulo m, bajo la suma, es un grupo cíclico, con $\overline{1}$ como generador.

7) Sea $G = \mathbb{Z}x\mathbb{Z}$ con la operación de suma de coordenadas. Demuestre que G no es cíclico.

8) (Teorema de Euler). Probar que si a es un entero positivo primo relativo con n, entonces

$$a^{\phi(n)} \equiv 1 \; mod \; n,$$

donde $\phi(n)$ = número de enteros entre 1 y n primos relativos con n.

9) (Teorema de Fermat). Probar si p es un número primo y a es cualquier entero, entonces

$$a^p \equiv a \ mod \ p$$

10) Usando el problema anterior, demuestre que $2^{30} - 1$ es un número compuesto.

11) Hallar el diagrama de subgrupos para los grupos siguientes
a) $(\mathbb{Z}_6,+)$
b) S_3
c) $(\mathbb{Z}_7,+)$

12) Sea m un entero fijo y $\mathbb{Z}_m$ el conjunto de clases de congruencias módulo m. Se define el producto módulo m en $\mathbb{Z}_m$, mediante

$$[a] \cdot [b] = [a \cdot b]$$

Probar que esta operación esta bien definida ¿Es $(\mathbb{Z}_m, \cdot)$ un grupo?

13) Probar que si p es un número primo, entonces el conjunto de los enteros módulo p, no nulos, forman un grupo bajo el producto.

14) Hallar una tabla para el grupo de los enteros módulo 7 bajo el producto.

15) Demuestre que todo grupo cíclico es abeliano

16) Probar que todo subgrupo de un grupo cíclico es cíclico.

17) ¿Cuantos generadores tiene un grupo cíclico de orden n?

18) Sea m un entero positivo dado, no necesariamente primo. Sea U_m el conjunto de clases de congruencias módulo m, no nulas $\overline{x}$, tales que $(x, m) = 1$. Probar que U_m es un grupo bajo la operación de producto módulo m.

19) Hallar explicitamente U_6 y U_{10}.

20) Demuestre que U_{15} tiene un elemento de orden 4.

21) Hallar un generador de U_{10}

22) Dar un ejemplo de un subgrupo cíclico en el grupo de matrices 2×2, de la forma

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{con} \quad ad - bc \neq 0$$

23) Sea $G = S_4$, hallar el grupo cíclico H generado por el elemento

$$\psi : \begin{array}{l} x_1 \longrightarrow x_2 \\ x_2 \longrightarrow x_3 \\ x_3 \longrightarrow x_1 \\ x_4 \longrightarrow x_1 \end{array}$$

¿Cual es el orden de este grupo?

24) Sean a y b dos elementos en un grupo G, abeliano tal que

$$(\circ(a), \circ(b)) = 1.$$

Probar que:

$$\circ(ab) = \circ(a) \cdot \circ(b)$$

donde (,) denota el máximo común divisor.

25) Sean a y b dos elementos en grupo abeliano G. Probar que:

$$\circ(ab) = [\circ(a), \circ(b)],$$

donde [,] denota el mínimo común múltiplo.

26) Demuestre que si un elemento a en un grupo G satisface:

$$a^k = e, \quad \text{entonces} \quad \circ(a) | k$$

27) Hallar todos los subgrupos de $(\mathbb{Z}_{10}, +)$.

28) Hallar todos los subgrupos del grupo de simetrías del cuadrado.

3.5 Operaciones con los Subgrupos

Cuando se tiene un grupo G, es posible conocer parte del mismo si se conoce un subgrupo H de G. Si G tiene varios subgrupos diferentes, entonces cada uno de ellos es una pieza dentro de una gran maquinaria: cada una cumple una función específica en G. Cuando se conocen todos los subgrupos de G entonces se tiene un conocimiento total del grupo G, en cierto sentido.

Si queremos mirar como se multiplican dos elementos dentro de G, y estos dos elementos están dentro de un subgrupo H, el cual ha sido determinado de antemano, entonces el problema estará resuelto porque sabemos como se ejecuta la multiplicación dentro de H.

Si por el contrario un elementos está en un subgrupo H, y otro elemento esta fuera de H y dentro otro subgrupo K, entonces el producto de ambos elementos estará en un conjunto L contenido en G. Nos preguntamos: ¿Cómo podríamos garantizar que L sea un subgrupo de G? ¿Cuál es el orden de L?

Definición 3.5.1 *Sea G un grupo y H, K dos subgrupos de G. Entonces la* **intersección** *de H y K, es el conjunto*

$$H \cap K = \{x \in G \mid x \in H, \text{ y } x \in K\}$$

Proposición 3.5.1 *La intersección de dos subgrupos de G es un subgrupo de G.*

Demostración Sean $x,\ y \in H \cap K$. Entonces $xy \in H$, y además $xy \in K$, pues H y K son grupos. Luego $xy \in H \cap K$.

Por otro lado, si $x \in H \cap K$, entonces $x^{-1} \in H$, y $x^{-1} \in K$, pues H y K son grupos. Luego $x^{-1} \in H \cap K$.

Mas generalmente, se tiene

Proposición 3.5.2 *Sea G un grupo y $\{H_i\}$, $i \in I$ una familia de subgrupos de G. Entonces el conjunto*

$$H = \bigcap_{i \in I} H_i$$

es un subgrupo de G.

La **unión de dos subgrupos** no es un grupo en general, por ejemplo, sea $G = (\mathbb{Z}_6, +)$ enteros módulo 6, y

$$H = \{\bar{e}, \bar{2}, \bar{4}\} \quad \text{y} \quad K = \{\bar{e}, \bar{3}\}.$$

Sabemos que H y K son subgrupos de G. Sin embargo

$$H \cup K = \{\bar{e}, \bar{2}, \bar{3}, \bar{4}\}$$

no es un subgrupo, pues

$$\bar{2} + \bar{3} = \bar{5} \notin H \cup K.$$

Definición 3.5.2 *Sea G un grupo y H, K subgrupos de G. Entonces el* **producto de H y K**, *se define por:*

$$HK = \{hk \mid h \in H \text{ y } k \in K\}.$$

Observación El producto de dos subgrupos no es un subgrupo en general. Afortunadamente, existe un criterio muy útil, para determinar cuando esto es cierto.

Teorema 3.5.1 *Sea G un grupo. Entonces HK es un subgrupo de G si y sólo si*

$$HK = KH.$$

Demostración: Sea $HK = KH$ y sean $h_1, h_2 \in K$ y $k_1, k_2 \in K$. Luego debemos probar:

i) $(h_1k_1)(h_2k_2) \in HK$

ii) $(h_1k_1)^{-1} \in HK$

Para probar *i*) notemos que

$$k_1h_2 \in KH = HK,$$

luego existen h_3, k_3 tal que

$$k_1 h_2 = h_3 k_3,$$

por lo tanto

$$\begin{aligned}(h_1k_1)(h_2k_2) &= h_1(k_1h_2)k_2 \\ &= h_1(h_3k_3)k_2 \\ &= (h_1h_3)(k_3k_2) \in HK\end{aligned}$$

Para probar $ii)$ vemos que

$$(h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH = HK$$

Recíprocamente, si HK es un subgrupo de G probaremos que

$$HK = KH$$

En efecto, sea $kh \in KH$. Luego existe el inverso de $hk : h^{-1}k^{-1} \in HK$, y por lo tanto $h = (h^{-1}k^{-1})^{-1} \in HK$.

Luego

$$KH \subseteq HK$$

Para demostrar la inclusión en el otro sentido, sea $x \in HK$, entonces

$$x^{-1} = hk \in HK,$$

luego

$$\begin{aligned}x &= (x^{-1})^{-1} \\ &= (hk)^{-1} \\ &= k^{-1}h^{-1} \in KH\end{aligned}$$

Por lo tanto hemos demostrado

$$HK \subseteq KH$$

♠

Pregunta : ¿Cuantos elementos tiene HK?

Teorema 3.5.2 *Sea G un grupo finito y H, K subgrupos de G. Entonces*

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

Demostración: Los elementos de HK son la forma hk con $h \in H$ y $h \in K$. Entonces hay $\circ(H)\ \circ(K)$ elementos de este tipo. Sin embargo puede haber repeticiones, es decir

$$h_1 k_1 = h_2 k_2$$

para algunos $h_1, h_2 \in H$, $k_1, k_2 \in K$.

Pero entonces $h_2^{-1} h_1 = k_2 k_1^{-1}$, y por lo tanto se tiene un elemento $x = h_2^{-1} h_1 = k_2 k_1^{-1}$ en la intersección de H y K.

Es decir cada vez que hay una repetición de dos elementos, se produce un elemento en la intersección $H \cap K$.

Recíprocamente, si $x \in H \cap K$, se tiene

$$hk = hx^{-1}xk = h_1 k_1$$

es decir, x genera un duplicado de hk en el conjunto HK.

Así pues el número de veces que un elemento hk aparece repetido es igual al orden de intersección $\circ(H \cap K)$.

Luego

$$|HK| = \frac{\circ(H) \circ (K)}{\circ(H \cap K)}$$

♠

Corolario 3.5.1 *Si H y K son subgrupos de G y*

$$\circ(H) > \sqrt{\circ(G)} \quad \text{y} \quad \circ(K) > \sqrt{\circ(G)}$$

Entonces

$$H \cap K \neq \{e\}$$

Demostración: Como $|HK| \leq \circ(G)$ tenemos

$$\begin{aligned} \circ(G) &\geq |HK| \\ &= \frac{\circ(H) \circ (K)}{\circ(H \cap K)} \\ &> \frac{\sqrt{\circ(G)}\sqrt{\circ(G)}}{\circ(H \cap K)} \\ &= \frac{\circ(G)}{\circ(H \cap K)} \end{aligned}$$

Luego

$$\circ(H \cap K) > 1$$

por lo cual

$$H \cap K \neq \{e\}$$

♠

Como aplicación de esto tenemos lo siguiente

Ejemplo: Sea G un grupo finito, con $\circ(G) = 15$, entonces G tiene a lo sumo un subgrupo de orden 5.

Solución: Si H y K son subgrupos de orden 5, entonces

$$\circ(H) > \sqrt{\circ(G)} \quad \text{y} \circ (K) > \sqrt{\circ(G)},$$

luego por el corolario anterior

$$H \cap K \neq \{e\}.$$

Pero $H \cap K < H$, y por el teorema de Lagrange se tiene $\circ(H \cap K)|5$

Luego la única posibilidad es:

$$\circ(H \cap K) = 5.$$

Por lo tanto

$$H \cap K = H.$$

Usando la misma técnica se prueba $H \cap K = K$. Luego H=K.

Definición 3.5.3 *Sea G un grupo y S un subconjunto de G, diferente del vacío. Entonces el* **grupo generado por** *S viene dado por*

$$< S >= \bigcap \{H \mid \ H \text{ subgrupo de } G \text{ y } S \subseteq H\}$$

Observación Es claro que $< S >$ es un subgrupo de G. Además es el menor subgrupo de G que contiene a S. Esto es simple consecuencia de la definición.

Definición 3.5.4 *Sea G un grupo, y H, K subgrupos de G. Entonces* **el grupo generado por** *H* **y** *K es el conjunto $< H \cup K >$.*

3.6 Clases Laterales

Cuando estudiamos la relación de congruencias módulo m en el conjunto de los números enteros, vimos que esta se define para dos enteros a y b

$$a \equiv b \ mod \ m,$$

si y sólo si m divide a $a - b$.

Es posible definir esta relación en términos de grupos. Si m es un entero positivo, entonces el conjunto de todos los multiplos de m, $H = m\mathbb{Z}$ es un subgrupo del grupo aditivo de $\mathbb{Z}$. Entonces se tiene que

$$a \equiv b \ mod \ m,$$

si y sólo si $a - b \in H$.

En esta sección daremos una generalización del concepto de congruencia módulo m, al considerar dentro de un grupo G la congruencia módulo H, donde H es un subgrupo de G.

Esta relación tiene propiedades muy similares a la congruencia de los números enteros. Una de las ventajas es que nos proporciona una partición del grupo en clases de equivalencias. Bajo ciertas condiciones sobre H, este conjunto de clases de equivalencias módulo H se le podrá dotar de una estructura de grupo.

Definición 3.6.1 *Sea G un grupo y H un subgrupo de G. Si $a \in G$, entonces la* **clase lateral derecha de a en H** *es el conjunto*

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

Ejemplo: Sea $G = S_3$ el grupo simetrico de orden 6. Sea $H = \{I, \phi\}$ entonces las clases laterales derechas son:

$$\begin{aligned} H\psi &= \{\psi, \phi\psi\} \\ H\psi^2 &= \{\psi^2, \phi\psi^2\} \\ H\phi\psi &= \{\phi\psi, \psi\} \\ H\phi\psi^2 &= \{\phi\psi^2, \psi^2\} \\ HI &= \{\psi, \phi\psi\} \\ H\phi &= \{\phi, I\} \end{aligned}$$

Definición 3.6.2 *Sea $a \in G$, entonces la* **clase lateral izquierda de** *a es el conjunto*

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

Ejemplo: Las clases laterales izquierdas de H en S_3 son:

$$\begin{aligned} \psi H &= \{\psi, \phi\psi^2\} \\ \psi^2 H &= \{\psi^2, \phi\psi\} \\ \phi\psi H &= \{\phi\psi, \psi^2\} \\ \phi\psi^2 H &= \{\phi\psi^2, \psi\} \\ IH &= \{I, \phi\} \\ \phi H &= \{\phi, I\} \end{aligned}$$

Definición 3.6.3 *Sea G un grupo y H un subgrupo de G. Sean a y b dos elementos de G. Diremos que a* **es congruente a** *b módulo H y lo denotamos*

$$a \equiv b \ mod \ H$$

si y sólo si $ab^{-1} \in H$.

Ejemplo 1: Sea $G = (\mathbb{Z}, +)$ y $H = (3\mathbb{Z}, +)$, entonces

$$a \equiv b \ mod \ H,$$

significa que

$$a - b \in H,$$

luego

$$a - b = 3k, \quad \text{para algún} \ \ k \in \mathbb{Z}$$

Luego se tiene la misma relación de congruencia de números enteros

$$a \equiv b \ mod \ 3$$

Teorema 3.6.1 *Sea G un grupo y $H < G$, entonces la relación de congruencia módulo H, determina una relación de equivalencia en G.*

Demostración:
1) **Reflexiva:** Sea $a \in G$, entonces

$$aa^{-1} = e \in H,$$

luego

$$a \equiv a \ mod \ H$$

2) **Simétrica:** Supongamos que $a \equiv b \ mod \ H$, entonces $ab^{-1} \in H$.

Ahora bien, como H es un grupo, se tiene

$$(ab^{-1})^{-1} = ba^{-1} \in H$$

luego

$$b \equiv a \ mod \ H$$

3) **Transitiva:** Supongamos que $a \equiv b \ mod \ H$ y $b \equiv c \ mod \ H$.

Luego

$$ab^{-1} \in H \quad \text{y} \quad bc^{-1} \in H.$$

Como H es un subgrupo de G, se debe tener

$$ac^{-1} = (ab^{-1})(bc^{-1}) \in H$$

Luego

$$a \equiv c \ mod \ H$$

Teorema 3.6.2 *Para todo $a \in G$, sea*

$$[a] = \{x \in G \mid x \equiv a \ mod \ H\}$$

Entonces

$$[a] = Ha.$$

Demostración: Sea $x \in [a]$, entonces

$$x \equiv a \ mod \ H,$$

luego

$$xa^{-1} \in H$$

por lo tanto existe $h \in H$ tal que $xa^{-1} = h$, lo cual implica $x = ha$. Por lo tanto $x \in Ha$.

Recíprocamente, supongamos que $x \in Ha$. Luego existe $h \in H$, tal que $x = ha$. Luego $xa^{-1} = h$ y por ende $x \equiv a \ mod \ H$. Con esto se prueba que $x \in [a]$, lo cual da fin a la demostración.

♠

Observación Si a es un elemento de G, el conjunto $[a]$ se llama **la clase de congruencia módulo H**. El teorema anterior nos dice entonces, que toda clase lateral es igual a una clase de congruencia.

Seguidamente, probaremos que todas las clases laterales tienen el mismo número de elementos.

Teorema 3.6.3 *Sean a y $b \in G$. Entonces*

$$|Ha| = |Hb|.$$

Demostración: Consideremos la función

$$\begin{aligned} \phi \ : \ & Ha \longrightarrow hb \\ & ha \longrightarrow hb \end{aligned}$$

Entonces probaremos que ϕ es inyectiva.

Sean $h_1, h_2 \in H$. Si suponemos $\phi(h_1 a) = \phi(h_2 a)$, se tiene que $h_1 b = h_2 b$, y luego $h_1 = h_2$.

Claramente ϕ es sobreyectiva y por lo tanto ϕ es biyectiva.

♠

Definición 3.6.4 *Sea G y H un subgrupo de G, entonces el número de clases laterales de H en G se llama el* **índice de H en G** *y lo denotamos por $[G : H]$.*

Corolario 3.6.1 *Sea G un grupo, H un subgrupo de G. Entonces*

$$|G| = [G : H]|H| \tag{3.5}$$

Demostración: Notar que todas las clases laterales derechas de G tiene el mismo número de elementos, en particular H mismo es una clase lateral derecha pues

$$H = He$$

De aquí se deduce

$$\begin{aligned} |G| &= \text{número de clases laterales} \times \text{número de elementos en } H \\ &= [G : H] \cdot |H| \end{aligned}$$

♠

Nota: Si G es finito, entonces se tiene

$$[G : H] = \frac{\circ(G)}{\circ(H)} \tag{3.6}$$

Observación: La fórmula (**??**) nos proporciona otra demostración del teorema de Lagrange.

Ejercicios

1)Sea $G = (\mathbb{Z}_{12}, +)$ y $H =< \overline{3} >$, $K =< \overline{6} >$. Hallar el orden de HK.

2) Sea G un grupo finito. Sean H y K subgrupos de G de ordenes m y n, respectivamente. Probar que $H \cap K = \{e\}$.

3) Sea G un grupo de orden 21 y H y K subgrupos de ordenes 3 y 7 respectivamente. Probar que $HK = KH$.

4) Sea G un grupo, S un n subconjunto no vacío de G, y consideremos

$$S_0 = \{s_1 \dots s_n \mid s_i \in S,\ o\ s_i^{-1} \in S,\ n \in N\}$$

Probar que S_0 es subgrupo de G que contiene S y además $S_0 =< S >$.

5)Sea G el grupo $(\mathbb{Z}, +)$ y $S = \{2, 5\}$. Hallar el grupo generado por S en G.

6) Hallar las clases laterales de $H =< 2 >$ en $(\mathbb{Z}, +)$.

7) Hallar las clases laterales de $H = \{1, -1\}$ en $(\mathcal{Q}, \cdot)$

8) Demuestre que si m y n son enteros primos relativos, entonces el grupo generado por ellos en $(\mathbb{Z}, +)$ es todo $\mathbb{Z}$.

9) Sea m un entero positivo, y $H =< m >$. Hallar el índice de H en $(\mathbb{Z}, +)$.

10) Hallar un subgrupo de índice 2 en $(\mathcal{Q}^*, \cdot)$.

11) Sea $G = S_4$ y

$$\begin{aligned} H &= \{\sigma \in S_4 \mid \sigma(x_1) = x_1\} \\ H &= \{\psi \in S_4 \mid \psi(x_2) = x_2\} \end{aligned}$$

a) Probar que: H y K son subgrupos de S_4
b) Hallar: $\circ(H)$ y $\circ(K)$
c) Hallar: $H \cap K$ y $\circ(H \cap K)$
d) Calcule: $\#HK$
e) Deduzca de d) que HK no es un subgrupo de G.

12) Sea $G = S_4$ y

$$\theta : \begin{array}{l} x_1 \longrightarrow x_3 \\ x_2 \longrightarrow x_1 \\ x_3 \longrightarrow x_2 \\ x_4 \longrightarrow x_4 \end{array} \qquad \psi : \begin{array}{l} x_1 \longrightarrow x_2 \\ x_2 \longrightarrow x_3 \\ x_3 \longrightarrow x_4 \\ x_4 \longrightarrow x_1 \end{array}$$

a) Calcular: $\circ(\theta)$ y $\circ(\psi)$
b) Calcular: $\circ(< \theta\psi >)$

13) Sea G un grupo abeliano y g_1, g_2 elementos de G de orden 3 y 4 respectivamente ¿Cuál es el orden de $g_1 \cdot g_2$?

14) Hacer el diagrama de subgrupos para $\mathbb{Z}_{12}$

15) Demuestre que todo grupo de orden 9 debe ser abeliano.

Ayuda:

i) Considere un elemento $g \in G$ ¿Cual es su orden?

ii) Demuestre que $G = HK$, donde H y K son subgrupos de orden 3, de la forma $H =< g_1 >$, $K =< g_2 >$.

iii) Demuestre que $g_1 g_2 = g_2 g_1$ y por lo tanto todos los elementos de G conmutan.

16) ¿Cuantos grupos abelianos de orden 9 se pueden construir?

17) Sea $G = (\mathbb{C}^*, \cdot)$ el grupo de los números complejos con el producto. Sea $W_n = e^{2\pi i/n}$ y $H_n =< W_n >$

a) Hallar el orden de H_n.

b) Representar H_6 en el plano complejo.

c) Represente el diagrama de subgrupo de H_6

18) Demuestre que un conjunto finito H, en un grupo G, es un grupo si y sólo si H es cerrado bajo la operación establecida en G.