Subgrupos generados y órdenes de elementos en un grupo

Dado G un grupo y $g \in G$. Recordemos que

$$g^n = \begin{cases} g \cdots g \ (n \text{ veces}) & \text{si } n \in \mathbb{Z}^+, \\ e & \text{si } n = 0, \\ g^{-1} \cdots g^{-1} \ (-n \text{ veces}) & \text{si } n \in \mathbb{Z} \setminus \mathbb{N}. \end{cases}$$

Denotamos por $\langle g \rangle$ al siguiente subconjunto de G: (45)

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

Proposición: $\langle g \rangle$ es un subgrupo de $(G, \cdot)$.

- **Demostración:** - $e = g^0 \in \langle g \rangle$, por lo que $\langle g \rangle \neq \emptyset$.

- Sean g^n y g^m en $\langle g \rangle$. Veamos que $g^n \cdot g^m \in \langle g \rangle$.

i) $n, m > 0$: En este caso, $g^n \cdot g^m = g^{n+m} \in \langle g \rangle$.

ii) $m = 0$: $g^n \cdot g^m = g^n \cdot e = g^n \in \langle g \rangle$.

iii) $n > 0$ y $m < 0$: $g^n \cdot g^m = g^n \cdot (g^{-1})^{|m|} = g^{n-|m|} \in \langle g \rangle$.
$n \geq |m|$

iv) $n > 0$ y $m < 0$: $g^n \cdot g^m = g^n \cdot (g^{-1})^{|m|} = (g^{-1})^{|m|-n}$
$n < |m|$
$= g^{n-|m|} \in \langle g \rangle$.

En cualquier caso, vemos que $g^n \cdot g^m = g^{n+m} \in \langle g \rangle$.

- Finalmente, para $g^n \in \langle g \rangle$ tenemos que

i) $(g^n)^{-1} = (g^{-1})^n = g^{-n}$ si $n > 0$

ii) $(g^0)^{-1} = e^{-1} = e = g^0$

iii) $(g^n)^{-1} = [(g^{-1})^{-n}]^{-1} = [(g^{-1})^{-1}]^{-n} = g^{-n}$ si $n < 0$

En cualquier caso, $(g^n)^{-1} \in \langle g \rangle$.

■

Definición: Al subgrupo $\langle g \rangle$ de G se le llama **subgrupo generado por** g.

Si existe $g \in G$ tal que $G = \langle g \rangle$, entonces diremos que G es un **grupo cíclico** generado por g.

Ejemplos:

1) $(\mathbb{Z}, +)$ es cíclico ya que $\mathbb{Z} = \langle 1 \rangle$.

Por ejemplo, $5 = 5 \cdot 1 = 1+1+1+1+1$ y

$$-3 = (-1)+(-1)+(-1).$$

2) $(\mathbb{R}^*, \cdot)$ no es cíclico.

Supongamos lo contrario: $\mathbb{R}^* = \langle r \rangle$ para algún $r \in \mathbb{R}$ con $r \neq 0$. Luego, como $-1 \in \mathbb{R}^+$, existe $n \in \mathbb{Z}$ tal que $-1 = r^n$, de donde

$$1 = (-1)(-1) = r^{2n}.$$

Note que $n \neq 0$ pues $-1 = r^n$. Entonces, $1 = r^{2n}$ solo puede ocurrir si $r = 1$, de donde

$$\mathbb{R}^* = \langle 1 \rangle = \{1\},$$

y esto es una contradicción.

3) En S_n (no cíclico), tenemos los subgrupos generados $\langle \sigma_1 \rangle = \{id, \sigma_1\}$, $\langle \sigma_2 \rangle = \{id, \sigma_2\}$ y $\langle \sigma_3 \rangle = \{id, \sigma_3\}$

4) D_4 tampoco es cíclico, pero $Rot = \langle R \rangle$, siendo R la rotación de $90°$.

5) $\mathbb{Z}_{12}$ es cíclico, ya que

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

De manera más general, $\bar{a}$ es un generador de $\mathbb{Z}_m$ si y solamente si $mcd(a, m) = 1$.

En efecto, si $\bar{a}$ genera a $\mathbb{Z}_m$,

$$\mathbb{Z}_m = \langle \bar{a} \rangle,$$

entonces $\bar{1} = k\bar{a}$ para algún $k \in \mathbb{Z}$. Luego,

$$\bar{1} = k\bar{a} \Longrightarrow m \mid (1 - ka).$$

Por otro lado, sea $d = mcd(a, m)$. Como $d \mid m$, tenemos que $d \mid (1 - ka)$. Además, $d \mid a$, por lo cual $d \mid 1$. Por lo tanto $d = 1$.

Recíprocamente, si $mcd(a, m) = 1$, para $R \in \{0, 1, \ldots, m-1\}$ la ecuación

$$ak \equiv R \pmod{m}$$

tiene solución $k \in \mathbb{Z}$, es decir, existe $k \in \mathbb{Z}$ tal que

$$\bar{R} = \overline{ka} = k\bar{a}.$$

En los ejemplos de grupos cíclicos finitos con generador g, notamos que existe $k \in \mathbb{Z}^+$ tal que $g^k = e$. Esto da lugar al siguiente concepto.

Definición: Sea $(G, \cdot)$ un grupo y $g \in G$.

- Si $g^n \neq e$ para todo $n \in \mathbb{Z}^+$, diremos que g tiene orden infinito.

$$o(g) = \infty.$$

- Si $g^n = e$ para algún $n \in \mathbb{Z}^+$, diremos que g tiene orden finito.

$$o(g) := \min \{ n \in \mathbb{Z}^+ / \; g^n = e \}.$$

Ejemplo:

1) Para todo grupo $(G, \cdot)$, $o(e) = 1$.

2) En S_n, si σ es una trasposición, se tiene

$$o(\sigma) = 2.$$

Para el caso particular $n = 3$:

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

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

$o(\sigma_4) = 3$. De manera similar, $o(\sigma_5) = 3$.

3) En D_4, $o(r) = 4$, $o(s) = 2$.

Más aún, $o(r^2) = 2$, $o(r^3) = 3$, $o(sr) = 2$,

$o(sr^2) = 2$, $o(sr^3) = 2$.

Propiedades del orden de un elemento:

Sea $(G, \cdot)$ un grupo y $g \in G$.

1) Si $n \in \mathbb{Z}^+$, entonces

$o(g) = n$ si y solamente si $g^n = e$ y $n \mid m$ para todo $m \in \mathbb{Z}$ tal que $g^m = e$.

- Demostración: ($\Rightarrow$) Supongamos $o(g) = n$. Entonces $g^n = e$ se sigue de la definición de orden. Ahora, sea $m \in \mathbb{Z}$ tal que $g^m = e$. Veamos que $n \mid m$, es decir, que el resto de dividir m por n es cero. Por el Teorema de la División Entera, existen $q, r \in \mathbb{Z}$ con $0 \leq r < n$ tales que $m = q \cdot n + r$. Luego,

$$e = g^m = g^{q \cdot n} \cdot g^r = (g^n)^q \cdot g^r = e^q \cdot g^r = g^r.$$

Como n es el menor entero positivo que cumple $g^n = e$, y $r \in \{0, 1, \ldots, n-1\}$, tenemos que $r = 0$. Por lo tanto, $n \mid m$.

($\Leftarrow$) Ahora supongamos que $g^n = e$ y que

$$g^m = e \Rightarrow n \mid m.$$

Sea $m \in \{ m \in \mathbb{Z}^+ / g^m = e \}$. Luego, $n \mid m$ por hipótesis, de donde $0 < m \leq m$.

Por lo tanto, $o(g) = n$. ■

2) Si $o(g) < \infty$, entonces

$g^m = g^k$ si y solamente si $m \equiv k \pmod{o(g)}$

· Demostración: ($\Rightarrow$) Supongamos $g^m = g^k$ con $m \geq k$. Luego, $g^{m-k} = e$ de donde $o(g) \mid (m-k)$, es decir,

$$m \equiv k \pmod{o(g)}.$$

($\Leftarrow$) Supongamos que $m \equiv k \pmod{o(g)}$. Luego, $o(g) \mid (m-k)$, de donde $g^{m-k} = e$. Multiplicamos por g^k para obtener

$$g^m = g^k.$$ ■

3) Si $o(g) = \infty$ y $m \neq k$, entonces $g^m \neq g^k$.

· Demostración: Supongamos $g^m = g^k$. Luego, $g^{m-k} = e$ con $m - k > 0$ ya que $m \neq k$ (podemos tomar m más grande que k). Entonces, $g^{m-k} = e$ implica que el orden de g es finito, lo cual contradice la hipótesis

4) Si $o(g) < \infty$ y $k \in \mathbb{Z}$, entonces

$$o(g^k) = \frac{o(g)}{\text{mcd}(k, o(g))}$$

· Demostración: $o(g) = o(g)' \cdot mcd(k, o(g))$.

$$(g^k)^{o(g)'} = g^{k \cdot o(g)'} = g^{k \cdot \frac{o(g)}{mcd(k, o(g))}}$$

$$= g^{\frac{k}{1} \cdot o(g)} = (g^{o(g)})^{\frac{k}{1}} = e^{\frac{k}{1}} = e$$

$$(g^k)^{o(g)'} = e.$$

Ahora, sea $m \in \mathbb{Z}^+$ tal que $(g^k)^m = e$.

Luego, $g^{mk} = e$, de donde $o(g) \mid mk$.

$$\frac{mk}{o(g)} = \frac{mk \, mcd(k, o(g))}{o(g) \cdot mcd(k, o(g))} = \frac{mk}{o(g)'}$$

Así, $\frac{mk}{o(g)'} = \frac{mk}{o(g)} \in \mathbb{Z}$, de donde $o(g)' \mid mk$.

Como $mcd(k, o(g)') = 1$, por el Lema de Euclides se tiene que $o(g)' \mid m$.

Por lo tanto, $o(g^k) = o(g)'$ ■

5) Si $o(g) < \infty$ y $k \in \mathbb{Z}$, entonces

$o(g) = o(g^k)$ si y solamente si $mcd(k, o(g)) = 1$.

· Demostración: ($\Rightarrow$) Supongamos $o(g) = o(g^k)$. Por la fórmula anterior,

$$o(g^k) = o(g) / mcd(k, o(g))$$

Como $o(g^k) = o(g)$, nos queda $mcd(k, o(g)) = 1$.

($\Leftarrow$) Análogo a la implicación anterior. ■

El orden de un elemento de un grupo coincide justamente con la cardinalidad del subgrupo generado por dicho elemento, por lo que no hay ambigüedad con el término "orden".

Proposición: Dado un grupo $(G, \cdot)$ y $g \in G$, se tiene que

$$o(g) = o(\langle g \rangle).$$

· **Demostración**: Si $o(g) = \infty$, entonces $\langle g \rangle$ posee infinitos elementos. De lo contrario, existirían $m, k \in \mathbb{Z}$ tales que $g^m = g^k$, de donde se tendría que $o(g) < \infty$.

Ahora supongamos $o(g) < \infty$, digamos $o(g) = n$. Como $g^m = g^k$ si y solamente si $m \equiv k \pmod{n}$, se tiene que $\langle g \rangle$ se puede escribir como

$$\langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}.$$

Así, $o(\langle g \rangle) = n = o(g)$. ∎

Finalizamos esta sección estudiando propiedades de los grupos cíclicos.

Proposición: Sea $(G, \cdot)$ un grupo finito.

1) G es cíclico si y solamente si existe $g \in G$ tal que $o(g) = o(G)$.

· **Demostración**: ($\Rightarrow$) Si $G = \langle g \rangle$, se tiene por la proposición anterior que $o(G) = o(\langle g \rangle) = o(g)$.

($\Leftarrow$) Ahora supongamos que $o(G) = o(g)$ para algún $g \in G$.

Consideremos $\langle g \rangle$. Luego, $\langle g \rangle < G$ con $o(\langle g \rangle) = o(g) = o(G)$.

Es decir, $\langle g \rangle$ es un subgrupo de G con la misma cantidad (finita) de elementos de G. Por lo tanto, $G = \langle g \rangle$. ∎

2) Si $G = \langle g \rangle$, entonces $G = \langle g^k \rangle$ si y solamente si $mcd(k, o(G)) = 1$.

· Demostración: Supongamos $G = \langle g^k \rangle$. Luego,

$$o(g) = o(\langle g \rangle) = o(G) = o(\langle g^k \rangle) = o(g^k).$$

Además, $o(g) = o(g^k) \cdot mcd(k, o(g))$, de donde

$mcd(k, o(g)) = 1$ pues $o(g) = o(g^k)$.

Ahora supongamos que $mcd(k, o(g)) = 1$. Por la fórmula anterior, $o(g) = o(g^k)$. Luego,

$$o(g^k) = o(G),$$

de donde $\langle g^k \rangle$ es un subgrupo de G con la misma cardinalidad de G. Por lo tanto, $G = \langle g^k \rangle$. ∎

3) Si $G = \langle g \rangle$, entonces G tiene $\varphi(o(G))$ generadores distintos.

· Demostración: Sea $n = o(G) = o(g)$. Como

$$g^m = g^k \text{ si y solamente si } m \equiv k \pmod{n},$$

tenemos que G es de la forma

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

Por la parte 2., g^k (con $0 \leq k < n$) es un generador de G si y solamente si $mcd(k, n) = 1$. Como la cantidad de tales k es $\varphi(n)$, tenemos que G tiene $\varphi(n)$ generadores. ■

El atributo de ser cíclico se "hereda" a nivel de subgrupos.

Proposición: Si G es un grupo cíclico, entonces todo subgrupo de G es cíclico.

- Demostración: Sea $H < G$, donde $G = \langle g \rangle$. Si $H = \{e\} = \langle e \rangle$ o $H = G = \langle g \rangle$, no hay nada que demostrar.

Supongamos entonces $H \neq \langle e \rangle$ y sea $h \in H$ con $h \neq e$. Como $G = \langle g \rangle$, existe $m \neq 0$ en $\mathbb{Z}$ tal que $h = g^m$. Podemos asumir que m es el menor entero positivo tal que $h = g^m$ (ya que si $m < 0$, podemos reescribir h como $h = (g^{-1})^{-m}$).

Ahora, sea $h' \in H$. Luego, existe $n \in \mathbb{Z}$ tal que

$$h' = g^n.$$

Por el Teorema de la División Entera, existen $q, r \in \mathbb{Z}$ con $0 \leq r < m$ tales que

$$n = q \cdot m + r.$$

Luego,

$$h' = g^m = g^{q \cdot m + r} = (g^m)^q \cdot g^r = h^q \cdot g^r$$

$$g^r = h' \cdot (h^{-1})^q \in H \quad (\text{ya que } H < G).$$

Como m es el menor entero positivo que cumple con $g^m \in H$, y como $g^r \in H$ con $0 \leq r < m$, debe ocurrir que $r = 0$.

Así, $h' = h^q = (g^m)^q \in \langle g^m \rangle$.

Por lo tanto, $H = \langle g^m \rangle$. ■

Teorema de Lagrange

Dado un grupo cíclico $G = \langle g \rangle$ de orden finito, sabemos que cualquier $H < G$ es cíclico, de donde H es de la forma

$$H = \langle g^k \rangle$$

para algún $g^k \in G$. Sabemos además que $o(G) = o(g)$, $o(H) = o(g^k)$ y que

$$o(g^k) = o(g) / \text{mcd}(k, o(g)).$$

Es decir, $o(G) = mcd(k, o(g)) \cdot o(H)$. Tenemos así que $o(H) \mid o(G)$.

Esto último no es exclusivo de los grupos finitos cíclicos. Por ejemplo, para $G = D_4$ y $H = \{id, r, r^2, r^3\}$ (subgrupo de rotaciones) se tiene que $o(H) = 4 \mid 8 = o(G)$.

Esto que estamos notando será siempre el caso respecto a grupos finitos y subgrupos de éste.

<u>Teorema de Lagrange</u>: Si $(G, \cdot)$ es un grupo finito y $H < G$, entonces

$$o(H) \mid o(G)$$

Antes de dar una demostración, nos va a ser útil generalizar el concepto de congruencia modular.

Dados $a, b \in G$, diremos que

$$a \equiv b \pmod{H}$$

si $a \cdot b^{-1} \in H$ (no necesariamente ocurre que $a \in H$ o $b \in H$).

<u>Ejemplo</u>: $G = (\mathbb{Z}, +)$, $H = n\mathbb{Z}$

$$a \equiv b \pmod{n\mathbb{Z}} \Leftrightarrow a + (-b) \in n\mathbb{Z} \Leftrightarrow n \mid (a-b)$$
$$\Leftrightarrow a \equiv b \pmod{n}.$$

Proposición: $\equiv \pmod{H}$ es una relación de equivalencia.

· **Demostración**:

- Reflexividad: Sea $a \in G$.

$$a \cdot a^{-1} = e \in H.$$

Luego, $a \equiv a \pmod{H}$.

- Simetría: Sean $a, b \in G$ tales que $a \equiv b \pmod{H}$

Luego, $a \cdot b^{-1} \in H$. Como $H < G$, tenemos $(a \cdot b^{-1})^{-1} \in H$.

Es decir,

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

Entonces, $b \equiv a \pmod{H}$.

- Transitividad: Sean $a, b, c \in G$ tales que

$$a \equiv b \pmod{H} \quad y \quad b \equiv c \pmod{H}.$$

Luego, $a \cdot b^{-1} \in H$ y $b \cdot c^{-1} \in H$. Como $H < G$, se tiene

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

Entonces, $a \equiv c \pmod{H}$. ∎

Denotemos por el momento a la clase de $a \in G$ por $\bar{a}$.

$$\bar{a} = \{ b \in G \mid b \equiv a \pmod{H} \}.$$