Sea G un grupo y $H \leq G$
Definimos 2 relaciones

$$g_1 \sim_{L} g_2 \iff g_1^{-1} g_2 \in H.$$

left

$$g_1 \sim_{R} g_2 \iff g_2 g_1^{-1} \in H.$$

right

$\sim_{L,R}$ es de equivalencia, las clases de equivalencia se llaman laterales izquierdo y derechos.

Prop: Sea $H \leq G$, sea $x \in G$, el lateral izquierdo de x es:

$$xH = \{xh,\ h \in H\}$$

el lateral der:

$$Hx = \{hx,\ h \in H\}$$

Dem:

$$y \in [x]_{\sim_L} \iff x \sim_L y \iff x^{-1} y \in H$$

$$\iff \exists\, h \in H : x^{-1} y = h$$

$$\iff y = xh. \quad \blacksquare$$

(el otro sentido es tarea)

$\boxed{\text{Ej:}}$

$G = S_3 = \{ (1), (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2) \}$

$H = \{ (1), (1\ 3) \}$

Calculamos laterales izq. y derecho:

I	D
$(1)H = \{(1), (1\ 3)\}$	$H(1) = \{(1), (1\ 3)\}$
$(1\ 2)(1\ 3) = (1\ 3\ 2)$	$(1\ 3)(1\ 2) = (1\ 2\ 3)$
$(12)H = \{(1\ 2), (1\ 3\ 2)\}$	$H(12) = \{(1\ 2), (1\ 2\ 3)\}$
$(2\ 3)H = \{(2\ 3), (1\ 2\ 3)\}$	$H(2\ 3) = \{(1\ 3), (1\ 3\ 2)\}$

Por equivalencia de clases solo hay esta cantidad de clases para este grupo

→ en general $xH \neq Hx$.

→ todos los laterales tienen la misma card. y es la cardinalidad de H (o el grupo con el que estamos operando).

→ en general el único lateral que es un grupo es $(1)H$, $H(1)$, o lo que es lo mismo H.

Lema: hay tantos laterales derechos cuantos laterales izquierdos.

Dem: Sea $X \subseteq G$, definimos

$$X^{-1} = \{ x^{-1},\ x \in X \}$$

Tenemos $(X^{-1})^{-1} = X$, es decir,

$$\mathcal{P}(G) \longrightarrow \mathcal{P}(G)$$
$$X \longmapsto X^{-1}$$

es biyección.

En particular sea $H \leq G$ tenemos:

$$H^{-1} \subseteq H$$

$$H = (H^{-1})^{-1} \subseteq H^{-1}$$

$$\Rightarrow H = H^{-1}.$$

Sea xH un lateral izquierdo luego $xH \subseteq G$ y

$$(xH)^{-1} = H^{-1}x = Hx$$

Def: • Cuando tenemos un grupo su cardinalidad se llama orden.

• Si $H \leq G$, el número de laterales se llama índice H a G y se denota $[G : H]$.

Teorema (Lagrange): Sea G grupo finito, sea $H \leq G$ luego

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

En particular, el orden de un subgrupo divide el orden del grupo.

es condición necesaria para ser subgrupo pero no suficiente.

Dem: es suficiente mostrar que cada lateral tiene $|H|$ elementos.

Sea $g \in G$, $g \notin H$

Consideremos

$$\varphi : H \to gH$$
$$h \to gh$$

(es biyectiva porque tiene inversa)

• es sobreyectiva por def. de lateral (Por lema de laterales)

• Si $\varphi(h_1) = \varphi(h_2) \Leftrightarrow gh_1 = gh_2 \Leftrightarrow h_1 = h_2$

entonces es inyectiva.

Alternativamente se puede decir φ es invertible.

$$\varphi^{-1}: gH \to H$$
$$gh \to h.$$

Def [orden de un elemento]:

Dado un grupo G, $g \in G$, el orden de g es el menor entero positivo t.q.

$$g^n = 1$$

Si no existe g tiene orden ∞.

Prop: Sea G un grupo, $g \in G$

$$\langle g \rangle = \{ g^n, n \in \mathbb{Z} \} \leq G$$

subgrupo cíclico generado por g.

$|\langle g \rangle|$ es igual al orden de g.

Por teorema de Lagrange

• el orden de g divide $|G|$.

• Si g tiene orden $n < \infty$, $g^m = 1$

sii $n | m$.

Dem: Sean $g^{m_1}, g^{m_2} \in \langle g \rangle$

$$g^{m_1}(g^{m_2})^{-1} = g^{m_1} \cdot g^{-m_2} = g^{m_1 - m_2} \in \langle g \rangle$$

Por el test $\langle g \rangle \leq G$.

- Si g tiene orden ∞, mostramos que $|\langle g \rangle| = \infty$.

  Si $g^n = g^k$, puedo multiplicar por g^{-k}, $g^{n-k} = 1$.

  en contradicción con ord. ∞ de g.

- Sea, ahora, $n < \infty$ el orden de g.

$$g^{nk} = (g^n)^k = 1^k = 1.$$

- Sea $g^m = 1$, Podemos escribir $m = nq + r$, $0 \leq r < n$.

$$1 = g^m = g^{nq+r} = g^{nq} \cdot g^r$$
$$= g^r$$

$\Rightarrow r = 0$

$$\langle g \rangle = \{ 1 = g^0, g, g^2, \dots, g^{n-1} \}$$

$\blacksquare$