En caso de que tengamos $X=\{x\}$ y $Y\subseteq G$, escribimos xY o Yx omitiendo las llaves.

Def: Sea $H\leq G$ un subgrupo de G. Dado $g\in G$, la clase lateral izquierda de H determinada por g es el conjunto $gH=\{gh \mid h\in H\}$. De manera analoga se define la clase lateral derecha de H determinada por g, Hg.

Si $g\notin H$, ent. $g^{-1}\notin H$. Así $e\notin gH$ (ni en Hg). En general las clases laterales NO son subgrupos.

Si $g\in H$, entonces $gH\subseteq H$. Si $h\in H$, ent $h=g(g^{-1}h)$ con $g^{-1}h\in H$, es decir, $H\subseteq gH$. Por lo tanto $gH=H=Hg$

Para todo $g\in G$, $g=ge\in gH$. Analogamente, $g\in Hg$

Lema: Sea $H \leq G$.

i) $G = \bigcup_{g \in G} Hg = \bigcup_{g \in G} gH$.

ii) Si $Hx \cap Hy \neq \emptyset$, entonces $Hx = Hy$.

iii) Si $xH \cap yH \neq \emptyset$, entonces $xH = yH$.

Dem:

(i) Tenemos que $G \subseteq \bigcup_{g \in G} Hg \subseteq G$.

(ii) Sea $g \in Hx \cap Hy$. Entonces $g = h_1 x$ y $g = h_2 y$ con $h_1, h_2 \in H$. Por lo tanto

$Hg = Hh_1 x = Hx$ y $Hg = Hh_2 y = Hy$.

(iii) Es analogo a (ii).

Cor. Sea $H \leq G$. Entonces G es la union disjunta de las distintas clases laterales derechas de H. Lo mismo se tiene para las clases laterales izquierdas.

Ejemplo. Dado $H \leq G$ y $g \in G$, en general $gH \neq Hg$. Sea $G = D_8$, $H = \langle v \rangle$ $= \{Id, v\}$ y $g = d$.

$gH = d\langle v \rangle = \{d, dv\}$, $Hg = \langle v \rangle d = \{d, vd\}$

pero $dv = 90° \neq vd = 270$

Lema. Sea $H \leq G$. Para cada $g \in G$ tenemos que $|gH| = |H| = |Hg|$.

Dem:

Sea $\varphi : H \longrightarrow Hg$ definida como $\varphi(h) = hg$. Es claro que φ es una función suprayectiva. Ahora

Si $h_1 g = h_2 g$, ent $(h_1 g)g^{-1} = (h_2 g)g^{-1}$, ie, $h_1 = h_2$.

Por lo tanto, φ es inyectiva. $\therefore |H| = |Hg| = |gH|$.

Lema: Sea $H \leq G$. Entonces $Hg = Hk$ si y solo si $gk^{-1} \in H$. Análogamente, $gH = kH$ si y solo si $k^{-1}g \in H$.

Dem:

$Hg = Hk \iff g = hk \iff gk^{-1} = h \in H$.

Lema. Sea $H \leq G$. Sean $\mathcal{R}$ y $\mathcal{L}$ los conjuntos de clases laterales derechas e izquierdas respectivamente. Entonces existe una biyección entre $\mathcal{R}$ y $\mathcal{L}$.

Dem:

Sea $\varphi : \mathcal{R} \longrightarrow \mathcal{L}$ definida como $\varphi(Hg) = g^{-1}H$

Esta función es suprayectiva.

Supongamos que $\varphi(Hg_1) = \underbrace{g_1^{-1}H = g_2^{-1}H}_{} = \varphi(Hg_2)$

Por el lema anterior $(g_2^{-1})^{-1} g_1^{-1} = g_2 g_1^{-1} \in H$ y

Por el mismo lema, esto implica que $Hg_1 = Hg_2$. Por lo tanto φ es inyectiva.

$\therefore$ φ es una biyección.

Def. Sea $H \leq G$. El índice de H en G denotado $[G:H]$ es el número de clases laterales izquierdas (ó derechas) distintas de H.

Teorema (Lagrange).
Sean G un grupo y H un subgrupo de G. Entonces $|G| = |H| \cdot [G:H]$. En particular, si G es finito, entonces $|H|$ divide a $|G|$ y $[G:H] = \frac{|G|}{|H|}$.

Dem:
El grupo G es la union disjunta de las distintas clases laterales derechas, que son tantas como $[G:H]$ y además cada una de ellas es de tamaño $|H|$

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

Cor. Sea G un grupo finito y $g \in G$. Entonces $o(g) \mid |G|$ y $g^{|G|} = e$.

Dem:

Si $g \in G$, $o(g) = |\langle g \rangle|$. Por Lagrange $o(g) \mid |G|$

y así $g^{|G|} = e$.

Cor. (Euler). Sean $a, n \in \mathbb{Z}$ tales que $\text{mcd}(a,n) = 1$. Entonces $a^{\varphi(n)} \equiv 1 \bmod n$.

Dem:

$$U_n = \{ 0 \leq r < n \mid \text{mcd}(r,n) = 1 \} \hookrightarrow \mathbb{Z}/n\mathbb{Z}$$

U_n son las unidades de $\mathbb{Z}/\mathbb{Z}_n$, así U_n es un grupo. Por el cor. $a \in U_n$, $a^{\varphi(n)} = 1$ en $\mathbb{Z}/n\mathbb{Z}$.