Teorema:

Las siguientes condiciones son equivalentes para un subgrupo $H \leq G$:

(a) $H \trianglelefteq G$

(b) $Hg = gH$ para todo $g \in G$.

(c) Toda clase lateral izq. de H en G es una clase lateral derecha.

(d) El conjunto de clases laterales derechas de H en G es cerrado bajo el producto de subconjuntos.

Dem:

(a) $\Rightarrow$ (b) Tenemos que $H = H^g = g^{-1}Hg$ para todo $g \in G$. Entonces $gH = g(g^{-1}Hg) = Hg$. para todo $g \in G$.

(b) $\Rightarrow$ (c) Es obvio

(c) $\Rightarrow$ (d) Sean Hg_1 y Hg_2 dos clases laterales derechas de H. Por hipótesis existe

$k \in G$ tal que $g_1 H = Hk$. Así

$$Hg_1 Hg_2 = H(g_1 H) g_2 = H(Hk) g_2 = Hg_3 \quad \text{con} \quad g_3 = kg_2.$$

Por lo tanto el producto vuelve a ser una clase lateral derecha.

(d) $\Rightarrow$ (a) Sea $g \in G$. Por (d) $Hg^{-1}Hg$ es una clase lateral derecha que contiene a $g^{-1}g = e$. Entonces:

$$g^{-1}Hg \subseteq Hg^{-1}Hg = He = H.$$

Por un lema anterior, H es normal en G. $\blacksquare$

Notemos que la condición (b) del teorema anterior es simetrica, entonces en los incisos (c) y (d) podemos intercambiar las palabras "derecha" e "izquierda":

Cor. Las siguientes condiciones son equivalentes para un subgrupo $H \leq G$:

(a) $H \trianglelefteq G$

(b) Toda clase lateral derecha de H en G es una clase lateral izquierda.

(c) El conjunto de las clases laterales izq. de H en G es cerrado bajo el producto de subconjuntos.

Dado $H \trianglelefteq G$ al conjunto $\{Hg \mid g \in G\}$ lo denotamos G/H y lo leemos como "G módulo H". Por el teorema anterior, G/H es cerrado bajo la multiplicación de subconjuntos.

Teorema.

Si $H \trianglelefteq G$, entonces G/H es un grupo. En este caso el producto está dado por

$$(Hx)(Hy) = Hxy \quad \text{para cualesquiera } x, y \in G.$$

Dem:

Por el teorema anterior $(Hx)(Hy)=H(xH)y=H(Hx)y=H(xy)$. Si $Hx=Hz$, entonces $zx^{-1}\in H$. Así $z(yy^{-1})x^{-1}\in H$ que es lo mismo que $zy(xy)^{-1}\in H$. Por lo tanto

$$HzHy=H(zy)=H(xy)=HxHy$$

Es decir, la operación está bien definida.

El neutro es la clase lateral H, ya que:

$$Hx(H)=HHx=H=H(Hx).$$

Dada $Hx\in G/H$, se tiene que $(Hx)Hx^{-1}=Hxx^{-1}=H=Hx^{-1}x=(Hx^{-1})Hx$. Por lo tanto $(Hx)^{-1}=Hx^{-1}$.

Def: Sea $H\trianglelefteq G$. Al grupo G/H se le llama el grupo cociente de G por H.

Por el Teorema de Lagrange, si G es finito, entonces $|G/H| = [G:H]$.

Por ejemplo: En $(\mathbb{Z},+)$, el grupo cociente de $\mathbb{Z}$ por $n\mathbb{Z}$ es $\mathbb{Z}/n\mathbb{Z} = \{a+n\mathbb{Z} \,/\, a\in\mathbb{Z}\}$

Las clases residuales módulo n.

Cor. Sea $N \triangleleft G$ y $H \leq G$. Entonces $NH = HN$ es un subgrupo y es normal si $H \trianglelefteq G$.

Dem:

Se tiene que:

$$HN = \bigcup_{h\in H} hN = \bigcup_{h\in H} Nh = NH. \quad \text{Por lo tanto } NH \leq G.$$

Si $g\in G$, por el automorfismo interior que define se tiene que:

$$(HN)^g = H^g N^g = H^g N. \text{ Si } H \trianglelefteq G, \text{ ent } (HN)^g = HN \text{ y así } HN \trianglelefteq G.$$