Subgrupos Normales.

Consideremos $S_3=\langle \sigma,\pi \mid \sigma^2=e,\ \tilde{\pi}^3=e$ y $\tilde{\pi}\sigma=\sigma\tilde{\pi}^2\rangle=\{e,\sigma,\pi,\pi^2,\sigma\pi,\sigma\pi^2\}$, donde $|\sigma|=|\sigma\pi|=|\sigma\tilde{\pi}^2|=2$ y $|\tilde{\pi}|=|\tilde{\pi}^2|=3$. Sea $H=\langle\sigma\rangle=\{e,\sigma\}$. Veamos que

$$S_3/_D H=\{Hg \mid g\in G\}=\{\underset{\{e,\sigma\}}{\underset{\parallel}{\langle\sigma\rangle}},\ \underset{\{\pi,\sigma\tilde{\pi}\}}{\underset{\parallel}{\langle\sigma\rangle\pi}},\ \underset{\{\pi^2,\sigma\tilde{\pi}^2\}}{\underset{\parallel}{\langle\sigma\rangle\tilde{\pi}^2}}\}$$

y, además:

$$S_3/_I H=\{gH \mid g\in G\}=\{\langle\sigma\rangle,\ \underset{\{\pi,\tilde{\pi}\sigma\}}{\underset{\parallel}{\tilde{\pi}\langle\sigma\rangle}},\ \underset{\{\pi^2,\sigma\tilde{\pi}\}}{\underset{\parallel}{\pi^2\langle\sigma\rangle}}\}$$

observamos que $S_3/_D H\neq S_3/_I H$, más aún $S_3/_D H\not\subset S_3/_I H$, y $S_3/_I H\not\subset S_3/_D H$.
Pero ahora, consideremos

$$N=\langle\tilde{\pi}\rangle=\{e,\tilde{\pi},\tilde{\pi}^2\}$$

Por el teorema de Lagrange, $[G:N]=2$. Veamos que:

$$S_3/_D H=\{Ng \mid g\in G\}=\{\langle\tilde{\pi}\rangle=N,\ \langle\tilde{\pi}\rangle\sigma=\{\sigma,\sigma\pi^2,\sigma\tilde{\pi}\}\}$$

y, por otro lado:

$$S_3/_I H=\{gN \mid g\in G\}=\{\langle\tilde{\pi}\rangle=N,\ \sigma N=\{\sigma,\sigma\tilde{\pi},\sigma\tilde{\pi}^2\}\}$$

vemos que $S_3/_D H=S_3/_I H$. Además:

$$\sigma N=N\sigma$$

El hecho anterior motiva la siguiente definición:

Def. Sea G un grupo y $N<G$. Decimos que **N es un subgrupo normal de G**, a lo que escribimos $N\triangleleft G$, ó $G\triangleright N$, si $G/_I N=G/_D N$.

Obs: Que una clase lateral izquierda sea una clase lateral derecha (de N en G), significa que: dado $g\in G$, $\exists\, x_g\in G \ \ni\ gN=Nx_g$. Como $g=ge\in gN=Nx$, entonces $Nx=Ng \Rightarrow gN=Ng$.

Proposición.

Sea G grupo y $N < G$. Las siguientes condiciones son equivalentes:

i) $N \triangleleft G$.

ii) El producto de dos clases laterales izquierdas (resp. derechas) es una clase lateral izquierda (resp. derecha).

iii) $\forall g \in G$, $gNg^{-1} = N$.

Dem:

(i) $\Rightarrow$ (ii):

Suponga que $N \triangleleft G$. Sean $g, g_1 \in G$, entonces:

$$(Ng)(Ng_1) = (NgN)g_1 = (NN)gg_1 = Ngg_1$$
$$(gN)(g_1N) = (gNg_1)N = gg_1(NN) = gg_1N$$

pues $N < G \Rightarrow NN = N$.

(ii) $\Rightarrow$ (iii):

Sea $g \in G$. Entonces:

$$NgNg^{-1} = Nu, \text{ con } u \in G.$$

como $e = gg^{-1} = eg\,eg^{-1} \in NgNg^{-1} = Nu$, entonces $N = Ne = Nu$. Por lo tanto

$$NgNg^{-1} = N$$

pero $gNg^{-1} \subseteq NgNg^{-1}$, así: $gNg^{-1} \subseteq N$ ... (1).

Como el g fue arbitrario, se cumple para g^{-1}, así:

$$g^{-1}Ng \subseteq N \Rightarrow gg^{-1}Ngg^{-1} \subseteq gNg^{-1}$$
$$\Rightarrow N \subseteq gNg^{-1} \text{ ... } (2)$$

Por (1) y (2), $gNg^{-1} = N$.

(iii) $\Rightarrow$ (i):

Sea $g \in G$. Como $gNg^{-1} = N \Rightarrow gN = Ng$. Así:

$gN = Ng \in G/_D N \Leftrightarrow Ng = gN \in G/_I N$. Por tanto $G/_D N = G/_I N \Rightarrow N \lhd G$.

q.e.d.

Corolario.

Sea G grupo y $N < G$. Las siguientes condiciones son equivalentes:

i) $N \lhd G$.

ii) $\forall g \in G$, $gNg^{-1} \subseteq N$.

iii) $\forall g \in G$ y $\forall n \in N$, $gng^{-1} \in N$.

Observaciones:

1) Si G es abeliano, todos los subgrupos de G son normales.

2) Si G no es abeliano y todos sus subgrupos son normales, entonces se dice que G es Hamiltoneano.

3) Los subgrupos triviales de un grupo G son subgrupos normales de G. En el caso que G tenga como subgrupos normales únicamente a los subgrupos triviales, decimos que G es simple.

4) Si $N < G$ tal que $[G : N] = 2$, entonces $N \lhd G$.

Dem:

En efecto, sea $g \in G$. Si $g \in N \Rightarrow gN = N = Ng$. Si $g \notin N$, entonces $gN \neq N$. también $Ng \neq N$. Como $[G:N]$, entonces debe pasar que $gN = Ng$.

q.e.d.

5) Sea $\{N_i\}_{i \in I}$ una familia de subgrupos normales de un grupo G. Entonces $N = \bigcap_{i \in I} N_i$ es un subgrupo normal de G

Dem:

Como $N_i \lhd G$ $\forall i \in I \Rightarrow \bigcap_{i \in I} N_i < G$. Sea $g \in G$ y $n \in N$ entonces $gng^{-1} \in N_i$ $\forall i \in I$ (pues $n \in N_i$ $\forall i \in I$). Por tanto $gng^{-1} \in N \Rightarrow N \lhd G$.

q.e.d.

Proposición.

Sea G un grupo, $H < G$ y $N \triangleleft G$. Entonces:

i) $H \cap N \triangleleft H$.

ii) $NH < G$ y $N \triangleleft NH$.

iii) Si $H \triangleleft G$, entonces $NH \triangleleft G$.

Dem:

De (i):

Como $H, N < G$, entonces $H \cap N < G$. Además $H \cap N \subseteq H \Rightarrow H \cap N < H$. Sea $h \in H$ y $n \in H \cap N$. Probaremos que $hnh^{-1} \in H \cap N$. Como $h, n, h^{-1} \in H \Rightarrow hnh^{-1} \in H$, además $h \in G$ y $n \in N \Rightarrow hnh^{-1} \in N$, por tanto $hnh^{-1} \in N$.

Así $hnh^{-1} \in H \cap N \Rightarrow H \cap N \triangleleft H$.

De (ii):

Para la primera parte basta probar que $NH = HN$. Sea $nh \in NH$, como $N \triangleleft G$ y $h \in H \subseteq G \Rightarrow h^{-1}nh \in N \Rightarrow nh = h(h^{-1}nh) \in HN$. Por tanto $NH \subseteq HN$.

Sea $hn \in HN$, de manera similar $hnh^{-1} \in N \Rightarrow hn = (hnh^{-1})h \in NH$. Así $HN \subseteq NH$.

Por tanto $NH = HN$. Para la segunda parte, claramente $N < NH$. Sea $n \in N$ y $n_1 h \in NH$. Veamos que

$$(n_1 h)^{-1} n (n_1 h) = h^{-1}(n_1^{-1} n n_1)h$$

como $n_1 \in G \Rightarrow n_1^{-1} n n_1 \in N$, así con $h \in G \Rightarrow h^{-1}(n_1^{-1} n n_1) h \in N$. Por tanto $N \triangleleft NH$.

De (iii):

Suponga que $H \triangleleft G$. Por (ii) $NH < G$. Sea $nh \in NH$ y $g \in G$. Entonces

$$gnhg^{-1} = gng^{-1}ghg^{-1}, \text{ donde } gng^{-1} \in N \text{ y } ghg^{-1} \in H$$

pues $N \triangleleft G$ y $H \triangleleft G$. Así $gnhg^{-1} \in NH$. Por tanto $NH \triangleleft G$.

q.e.d.

Proposición.
Sean $N, M \triangleleft G$ tales que $N \cap M = \{e\}$. Entonces $\forall\, n \in N$ y $\forall\, m \in M$, $nm = mn$.

Dem:
Como $m^{-1}nm \in N$ y $nmn^{-1} \in M$, pues $N, M \triangleleft G$, entonces $m^{-1}nmn^{-1} \in N$ y $m^{-1}n$ $mn^{-1} \in M$, así $m^{-1}nmn^{-1} \in N \cap M = \{e\} \Rightarrow m^{-1}nmn^{-1} = e \Rightarrow nm = mn$.

q.e.d.

EJEMPLOS:

1) Como $\mathbb{Z}$ es abeliano, todos sus subgrupos son normales, luego
$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/_I n\mathbb{Z} = \mathbb{Z}/_D n\mathbb{Z}$$
por lo cual, para $a \in \mathbb{Z}$,
$$[a] = a + n\mathbb{Z} = n\mathbb{Z} + a$$

Def. Sea G un grupo y $N \triangleleft G$. Denotamos por
$$G/N = G/_I N = G/_D N$$
y, definimos la función $\psi : G/N \times G/N \to G/N$ como:
$$\forall\, a, b \in G,\ \psi(Na, Nb) = Nab$$
Afirmamos que ψ está bien definida. En efecto, sean $a, b, a_1, b_1 \in G$ m $a_1 \in Na$ y $b_1 \in Nb$. Como:
$$(ab)(a_1b_1)^{-1} = abb_1^{-1}a_1^{-1}$$
$$= (aa_1^{-1})(a_1 bb_1^{-1} a_1^{-1})$$
como $a \in Na_1$, $b \in Nb_1 \Rightarrow aa_1^{-1}, bb_1 \in N$. Además, N es normal en G, así $a_1bb_1^{-1}a_1^{-1} \in N$. Luego como $N < G$:
$$(ab)(a_1b_1)^{-1} \in N \Rightarrow Nab = Na_1b_1$$
Así, la operación ψ está bien definida, dada por:
$$\psi(Na, Nb) = Nab = Na\,Nb$$

Con esta operación, G/N es un grupo, con identidad N y, $\forall\, a \in G$, $(Na)^{-1} = Na^{-1}$.

Así, G/N es llamado el grupo cociente ó grupo factor de G por N. Además, si G es finito: $|G/N| = \frac{|G|}{|N|}$.

EJEMPLOS.

1) Tomando a $\mathbb{Z}$ como grupo aditivo, por ser abeliano y cíclico $(\mathbb{Z} = \langle 1 \rangle)$, entonces todo subgrupo de él es normal y cíclico, i.e son de la forma $n\mathbb{Z}$ con $n \in \mathbb{N} \cup \{0\}$.
Así, el grupo cociente $\mathbb{Z}/n\mathbb{Z}$ es el grupo abeliano de clases bajo la congruencia módulo n.

2)

Def. Sea G grupo, y $a,b\in G$. Se define el conmutador de a y b, denotado por $[a,b]$, como:

$$[a,b] := aba^{-1}b^{-1}$$

Proposición.

Sean $a,b\in G$. Entonces:

a) $[a,b]^{-1}=[b,a]$ (anticonmutatividad).

b) $\forall\, g\in G$, $g[a,b]g^{-1}=[gag^{-1},gbg^{-1}]$.

Dem:

De a):

$$[a,b]^{-1}=(aba^{-1}b^{-1})^{-1}=(bab^{-1}a^{-1})=[b,a]$$

De b):

$$g[a,b]g^{-1}=g(aba^{-1}b^{-1})g^{-1}=(gag^{-1})(gb^{-1}g)=(gag^{-1})(gbg^{-1})^{-1}=[gag^{-1},gbg^{-1}]$$

q.e.d.

Nota: Si $g,a\in G$, al elemento gag^{-1} se le llama conjugado de a. De manera similar, si $H<G$ y $g\in G$, entonces gHg^{-1} es subgrupo de G.

En efecto, sean $ghg^{-1}, gh_1g^{-1}\in gHg^{-1}$, entonces

$$(ghg^{-1})\cdot(gh_1g^{-1})^{-1}=ghg^{-1}\cdot gh_1^{-1}g^{-1}= ghh_1^{-1}g^{-1}\in gHg^{-1}$$

pues $H<G$, así $hh_1^{-1}\in H$. gHg^{-1} es llamado conjugado de H.

Def. Sea G grupo. Se define el derivado ó subgrupo conmutador de G, denotado G', $G^{(1)}$, DG, dG o $[G,G]$, como:

$$G^{(1)}=\langle [a,b]\mid a,b\in G\rangle$$

De manera más general, si $A,B\subseteq G$ son no vacíos, se define el subgrupo conmutador de A y B, como $[A,B]=\langle [a,b]\mid a\in A \text{ y } b\in B\rangle$.

Obs: de la anticonmutatividad probada anteriormente, se tiene que:

$$G^{(1)} = \{[a_1,b_1]\cdot\ldots\cdot[a_r,b_r] \mid a_i,b_i \in G,\ \forall i=1,2,\ldots,r;\ r\in\mathbb{N}\}$$

Además $G^{(1)} \triangleleft G$. En efecto, sea $x \in G^{(1)}$, entonces $\exists$ $r\in\mathbb{N}$ y $a_1,b_1,\ldots,a_r,$ $b_r \in G$ m

$$x = [a_1,b_1]\cdot\ldots\cdot[a_r,b_r]$$

Sea $g\in G$. Entonces:

$$\begin{aligned} gxg^{-1} &= g[a_1,b_1]\cdot\ldots\cdot[a_r,b_r]g^{-1} \\ &= g[a_1,b_1]g^{-1}\cdot g[a_2,b_2]g^{-1}\cdot\ldots\cdot g[a_r,b_r]g^{-1} \\ &= [ga_1g^{-1},gb_1g^{-1}]\cdot\ldots\cdot[ga_rg^{-1},gb_rg^{-1}] \in G^{(1)} \end{aligned}$$

pues, $ga_ig^{-1}, gb_ig^{-1} \in G$, $\forall i=1,2,\ldots,r$. Por tanto, $G^{(1)} \triangleleft G$.

Proposición.

Sea G un grupo. Entonces:

i) G es abeliano $\Leftrightarrow G^{(1)} = \langle e\rangle$.

ii) Si $N \triangleleft G$, entonces G/N es abeliano $\Leftrightarrow G^{(1)} < N$.

Dem:

De (i):

G es abeliano $\Leftrightarrow \forall a,b\in G,\ ab=ba \Leftrightarrow \forall a,b\in G,\ aba^{-1}b^{-1}\in\{e\}=\langle e\rangle$
$\Leftrightarrow \forall a,b\in G,\ [a,b]\in\langle e\rangle \Leftrightarrow G^{(1)}=\langle e\rangle$.

De (ii):

G/N es abeliano $\Leftrightarrow \forall a,b\in G,\ NaNb=NbNa \Leftrightarrow \forall a,b\in G.\ Nab=Nba \Leftrightarrow \forall a,b$ $\in G,\ aba^{-1}b^{-1}\in N \Leftrightarrow \forall a,b\in G,\ [a,b]\in N \Leftrightarrow G^{(1)}\subseteq N \Leftrightarrow G^{(1)}<N$.

q.e.d.

Obs: $G/G^{(1)}$ siempre es abeliano, pues $G^{(1)}\triangleleft G$ y $G^{(1)}<G^{(1)}$.

Def. Sea G un grupo y $A\subseteq G$ no vacío. Se definen:

i) El centralizador de A en G, como:

$$Z(A) = \{x\in G \mid xa=ax,\ \forall a\in A\} = Z_G(A)$$

ii) El normalizador de A en G, como

$$N(A)=\{x\in G \mid xA=Ax\}=N_G(A)$$

Proposición.

Sean $A,B\subseteq G$ no vacíos, y G grupo. Entonces:

i) $Z(A)<G$.

ii) $N(A)<G$

iii) $Z(A)\triangleleft N(A)$.

Dem:

De (i):

Sean $x,y\in Z(A)$, entonces $xa=ax$ y $ya=ay$, $\forall a\in A \Rightarrow ay^{-1}=y^{-1}a$, $\forall a\in A$. Por tanto:

$$xy^{-1}a=xay^{-1}=axy^{-1},\ \forall a\in A.$$

así, $xy^{-1}\in Z(A)\Rightarrow Z(A)<G$.

De (ii):

Sean $x,y\in N(A)$, entonces $xA=Ax$ y $yA=Ay\Rightarrow Ay^{-1}=y^{-1}A$. Por tanto:

$$xy^{-1}A=xAy^{-1}=Axy^{-1}$$

por tanto, $xy^{-1}\in N(A)\Rightarrow N(A)<G$.

De (iii):

Claramente $Z(A)<N(A)$, pues $\forall x\in Z(A)$:

$$ax=xa,\ \forall a\in A$$
$$\Rightarrow Ax=xA$$
$$\Rightarrow x\in N(A).$$

luego $Z(A)\subseteq N(A)\Rightarrow Z(A)<N(A)$. Sea $x\in Z(A)$ y $g\in N(A)$, probaremos que $gxg^{-1}\in Z(A)$. En efecto, sea $a\in A$. Como $g\in N(A)$, $\exists a_1\in A$ m $g^{-1}a=a_1g^{-1}$.

Veamos que:

$$gxg^{-1}a = (gx)(g^{-1}a) = (gx)(a_1 g^{-1}) = g(xa_1)g^{-1} = ga_1 x g^{-1} = agxg^{-1}$$

por tanto $gxg^{-1} \in Z(A) \Rightarrow Z(A) \lhd N(A)$.

q.e.d.

Def. Sea G grupo. Se define el centro de G, como $Z_G(G)$ y, se denota por Z_G ó Z.

Corolario.

Si G es grupo, entonces $Z \lhd N(G) = G$.

Dem:

Es inmediata de la proposición anterior y del hecho que $N(G) = G$.

q.e.d.

Proposición.

Sea G grupo y $H < G$. Entonces:

i) $H \lhd N(H) < G$.

ii) $N(H)$ es el máximo subgrupo de G en el cual H es normal, i.e si $K < G$ $\ni$ $H \lhd K$, entonces $K \subseteq N(H)$.

iii) $H \lhd G \Leftrightarrow N(H) = G$.

Dem:

De (i):

Sea $x \in H$. Probaremos que $x \in N(H)$. Como $x \in H$: $x = e^{-1}x \in H$, y $xe^{-1} \in H$, así $xH = eH = H = He = Hx$. Por tanto, $x \in N(H)$. Luego $H < N(H)$.

Sea ahora $x \in H$ y $g \in N(H)$. Entonces $gH = Hg \Rightarrow gHg^{-1} = H \Rightarrow ghg^{-1} \in H$. Por tanto, $H \lhd N(H)$.

De (ii):

Suponga que $\exists$ $K < G$ $\ni$ $H \lhd K$. Sea $k \in K$, como $H \lhd K$, $kH = Hk \Rightarrow k \in N(H)$.

Luego $K \subseteq N(H)$.

De (iii):

$\Rightarrow$) Suponga que $H \trianglelefteq G$. Como $G < G$ y $H \trianglelefteq G$, por la parte (ii), $G \subseteq N(H)$. Además $N(H) \subseteq G$, así $N(H) = G$.

$\Leftarrow$) Suponga que $N(H) = G$, entonces por (i), $H \trianglelefteq G$.

q.e.d.

Obs: Sea $A \subseteq G$, $A \neq \emptyset$. Si $A = \{a\}$, escribimos $Z(a)$ y $N(a)$, respectivamente para $Z(A)$ y $N(A)$. En este caso, notemos que

$$Z(a) = N(a)$$

Pues:

$$x \in Z(a) \Leftrightarrow a'x = xa',\ \forall a' \in A = \{a\} \Leftrightarrow ax = xa \Leftrightarrow \{xa\} = \{ax\}$$
$$\Leftrightarrow x\{a\} = \{a\}x \Leftrightarrow x \in N(a)$$

Proposición.

Sea G grupo, y $a \in A \subseteq G$ arbitrario. Entonces $a \in Z \Leftrightarrow N(a) = G$.

Dem:

$$a \in Z \Leftrightarrow ax = xa,\ \forall x \in G \Leftrightarrow \{a\}x = x\{a\},\ \forall x \in G \Leftrightarrow N(a) = G.$$

q.e.d.

EJEMPLOS.

1)