Subgrupos

Def. Sea G un grupo y $H \subset G$. Decimos que H es un subgrupo de G, a lo que se escribe $H < G$, si

i) $H \neq \phi$.

ii) La operación de G inducida en H es cerrada en H, y hace de H un grupo.

Esto es: $\cdot|_{H\times H} : H \times H \to H$ es cerrada para que $H < G$. La asociatividad en H se cumple siendo $\cdot|_{H\times H}$ cerrada.

Proposición.

Sea G un grupo y $H \subset G$ no vacío. Entonces $H < G \Leftrightarrow \forall\, a,b \in H$:

i) $ab \in H$.

ii) $a^{-1} \in H$.

Dem:

$\Rightarrow$) Supongamos que $H < G$, entonces H es grupo con la operación de G. Bajo estas condiciones se tiene por definición, que la operación de G inducida en H es cerrada.

Sea $e' \in H$ la identidad en H, y sea $a \in H$. Entonces como H es un grupo, $\exists\, u \in H$ tal que $ua = au = e'$. Entonces:

$$e' = au = aue = au(aa^{-1}) = a((ua)a^{-1}) = a(e'a^{-1}) = aa^{-1} = e$$

Luego $e \in H$, así $au = e = ua$, luego por unicidad $u = a^{-1} \in H$.

En resumen:

(i) Como $\cdot|_{H\times H}$ es cerrada en H, entonces $a,b \in H \Rightarrow ab \in H$.

(ii) $a \in H \Rightarrow a^{-1} \in H$.

$\Leftarrow$) Supongamos que se cumplen (i) y (ii). Probaremos que $H < G$.

Claramente $H \neq \phi$.

a) Por (i), la operación $\cdot|_{H\times H}$ es asociativa por ser la operación cerrada.

b) Sea $a\in H$, por (ii) $a^{-1}\in H$, luego por (i) $aa^{-1}\in H$, esto es: $e=aa^{-1}=a^{-1}a\in H$, así: $\exists\ e\in H$ tal que $aa^{-1}=e=a^{-1}a$ $\forall\ a\in H$, i.e H tiene identidad.

c) $\forall\ a\in H$ $\exists\ a^{-1}\in H$ tal que $aa^{-1}\in H$, y $aa^{-1}=e=a^{-1}a$, i.e cada elemento tiene inverso.

Por a), b) y c) H es un grupo con la operación inducida por G, i.e $H<G$.

q.e.d.

Obs: Las condiciones (i) y (ii) de la prop. anterior equivalen a la condición (iii)

(iii) $\forall\ a,b\in H$, $ab^{-1}\in H$.

Dem:

(i) y (ii) $\Rightarrow$ (iii)

Sean $a,b\in H$. Como $b\in H$ entonces $b^{-1}\in H$ por (ii), luego con $b\in H$, por (i) se sigue que $ab^{-1}\in H$.

(iii) $\Rightarrow$ (i) y (ii)

Sean $a,b\in H$. Como $a\in H$ y $a\in H$ entonces $e=aa^{-1}\in H$, luego con $a\in H \Rightarrow ea^{-1}=a^{-1}\in H$.

Por lo anterior, $b\in H \Rightarrow b^{-1}\in H$, con $a\in H$ se sigue que $a(b^{-1})^{-1}=ab\in H$.

Así, se cumplen (i) y (ii).

q.e.d.

Proposición.

Sea G un grupo y $H\subset G$ con $H\neq\emptyset$. Si H es finito, entonces $H<G \iff \forall\ a,b\in H$, $ab\in H$.

Dem:

$\Rightarrow$) Suponga que $H<G$, por la proposición anterior $a,b\in H\Rightarrow ab\in H$.

$\Leftarrow$) Basta con probar que $a^{-1}\in H$ $\forall\ a\in H$, pues $a,b\in H \Rightarrow ab\in H$.

Sea $a\in H$, construimos el conjunto

$$A = \{a^m \mid m \in \mathbb{Z}\}$$

Claramente $A < H$, luego A es finito. Por tanto, $\exists\, m, l \in \mathbb{Z}$ $\ni$ $a^m = a^l$ con $m < l$, luego $a^{l-m} = e$ con $l-m > 0$. Por tanto:

$$a^{l-m} = a^{l-m-1} \cdot a = e = a \cdot a^{l-m-1}$$

donde $l-m-1 \geq 0$, así $a^{-1} = a^{l-m-1} \in A < H$. Claramente si $l-m-1 = 0$, entonces $a^{-1} = e \in H$, en otro caso se sigue teniendo el resultado.

q.e.d.

Obs: Sea G un grupo. La relación $<$ "ser subgrupo de" es una relación transitiva. Es decir, si $K < H$ y $H < G$, entonces $K < G$.

Def. Sea G un grupo y $H < G$. En G definimos la siguiente relación: para cada $a, b \in G$, a es congruente con b por la derecha módulo H, a lo que se escribe $a \equiv_D b \bmod H$ si $ab^{-1} \in H$, i.e:

$$a \equiv_D b \bmod H \Leftrightarrow ab^{-1} \in H$$

Esta relación sobre G es una relación de equivalencia. En efecto:

(i) $\forall\, a \in G$, $a \equiv_D a \bmod H$ pues $aa^{-1} = e \in H$.

(ii) Sean $a, b \in G$ $\ni$ $a \equiv_D b \bmod H$, entonces $ab^{-1} \in H$. Como $e \in H$ se sigue que $e(ab^{-1})^{-1} = ba^{-1} \in H$, luego $b \equiv_D a \bmod H$.

(iii) Sean $a, b, c \in G$ $\ni$ $a \equiv_D b \bmod H$ y $b \equiv_D c \bmod H \Rightarrow ab^{-1} \in H$ y $bc^{-1} \in H \Rightarrow$
$ac^{-1} = a(ec^{-1}) = a((b^{-1}b)c^{-1}) = (ab^{-1})(bc^{-1}) \in H \Rightarrow a \equiv_D c \bmod H$.

Por (i), (ii) y (iii), $\equiv_D \bmod H$ es una relación de equivalencia.

Nota: Denotamos $a \equiv_I b \bmod H \Leftrightarrow a^{-1}b \in H$ (Congruencia izquierda).

Denotamos de manera estándar a las clases de equivalencia de $a \in G$ como $[a]_D$. Afirmamos que:

$$[a]_D = Ha = \{ha \mid h \in H\}$$

En efecto:

a) Sea $x \in [a]_D$, entonces $x \equiv_D a \bmod H$, luego $xa^{-1} \in H$. Tome $h = xa^{-1} \in H$, entonces $x = (xa^{-1})a = ha$, luego $x \in Ha$.

b) Sea $x \in Ha$, entonces $\exists\ h \in H$ tal que $x = ha \Rightarrow h = xa^{-1} \in H \Rightarrow x \equiv_D a \bmod H$ $\Rightarrow x \in [a]_D$.

Por (a) y (b), $[a]_D = Ha$.

Al conjunto de clases de equivalencia bajo la congruencia por la derecha módulo H, la denotamos por $G/\equiv_D \bmod H = G/_D H = \{Ha \mid a \in G\}$. H induce conjuntos en G, todos disjuntos. $G/_D H$ es una partición de G.

En general:

$$G/_D H = \{Ha \mid a \in R\}$$

donde R es un conjunto completo de representantes donde:

$$|G/_D H| = |R|$$

Ejemplos:

Proposición:

Sea G un grupo y $H < G$. Toda clase lateral por la derecha Ha bajo la congruencia módulo H ($\equiv_D \bmod H$), tiene una misma cardinalidad, a saber:

$$|Ha| = |H| \ \forall a \in G.$$

Dem:

Sea $f: H \to Ha$, donde $f(h) = ha$, $\forall\ h \in H$. Claramente:

a) f es inyectiva.

Sean $h, h' \in H$ tales que $f(h) = f(h')$, entonces $ha = h'a \Rightarrow h = h'$ por Ley de cancelación, luego f es inyectiva.

b) f es suprayectiva.

Sea $x \in Ha$, entonces $\exists\ h \in H$ tal que $x = ha$, luego $\exists\ h \in H \ni f(h) = ha$, así f es suprayectiva.

Por a) y b), f es biyectiva, luego $|Ha| = |H|$.

q.e.d.

Obs: También existe la congruencia por la izquierda módulo H, dada por:

$$\forall\ a, b \in G, \quad a \equiv_I b \bmod H \iff a^{-1} b \in H$$

y las clases de equivalencia son de la forma:

$$[a]_I = aH = \{ah \mid h \in H\}$$

Nota: En general $Ha \neq aH$, pero si G es abeliano entonces $Ha = aH$, $\forall\ a \in G$, i.e $\equiv_D \bmod H = \equiv_I \bmod H$. Los subgrupos en los que sucede esto son llamados subgrupos normales.

El conjunto cociente de congruencias por la izquierda módulo H se denota por:

$$G/_I H = \{aH \mid a \in G\}$$

Proposición.

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

$$|G/_D H| = |G/_I H|$$

Dem:

Sea $\varphi : G/_D H \to G/_I H$ dada como sigue:

$$\forall a \in G, \quad \varphi(Ha) = a^{-1}H$$

Primero probaremos que φ está bien definida.

a) Sean $a,b \in G$ tales que $b \in Ha$.

$$\begin{aligned} b \in Ha &\Rightarrow b \equiv_D a \bmod H \\ &\Rightarrow a \equiv_D b \bmod H \\ &\Rightarrow ab^{-1} \in H \\ &\Rightarrow (ab^{-1})^{-1} \in H \\ &\Rightarrow (b^{-1})^{-1} a^{-1} \in H \\ &\Rightarrow b^{-1} \equiv_I a^{-1} \bmod H \\ &\Rightarrow b^{-1} \in a^{-1}H \end{aligned}$$

Luego $Hb = Ha \Rightarrow b^{-1}H = a^{-1}H \Rightarrow \varphi(Hb) = \varphi(Ha)$. Por tanto, φ está bien definida.

b) φ es inyectiva.

Sean $a,b \in G$ tales que $\varphi(Ha) = \varphi(Hb)$, entonces:

$$\begin{aligned} \varphi(Ha) = \varphi(Hb) &\Rightarrow a^{-1}H = b^{-1}H \\ &\Rightarrow a^{-1} \in b^{-1}H \\ &\Rightarrow a^{-1} \equiv_I b^{-1} \bmod H \\ &\Rightarrow ab^{-1} \in H \\ &\Rightarrow (ab^{-1})^{-1} \in H \\ &\Rightarrow ba^{-1} \in H \end{aligned}$$

$$\Rightarrow b \equiv_D a \bmod H$$
$$\Rightarrow a \equiv_D b \bmod H$$
$$\Rightarrow Ha = Hb$$

Luego, φ es inyectiva.

c) φ es suprayectiva.

Sea $c \in G$, entonces para cH $\exists$ Hc^{-1} tal que $\varphi(Hc^{-1}) = (c^{-1})^{-1}H = cH$.

Por b) y c), φ es biyectiva, luego:
$$|G/_D H| = |G/_I H|$$

q.e.d.

Nota: Al cardinal común $|G/_D H| = |G/_I H|$ se le llama índice de H en G.

Teorema (de Lagrange).

Sea G un grupo finito y $H < G$, entonces $|H| \mid |G|$. Más aún:
$$|G| = |H| \cdot [G : H]$$

Dem:

Sea R un conjunto de representantes por la derecha módulo H, entonces:
$$G = \dot{\bigcup_{a \in R}} Ha$$

$$\begin{aligned} \Rightarrow |G| &= \left|\dot{\bigcup_{a\in R}} Ha\right| \\ &= \sum_{a \in R} |Ha| \\ &= \sum_{a \in R} |H| \\ &= |H| \cdot |R| \end{aligned}$$

Pero $|R| = [G : H]$, entonces:
$$|G| = |H| \cdot [G : H].$$

q.e.d.

Proposición.

Sea G un grupo y $K, H < G$ tales que $K < H$. Entonces:

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

Siendo G un grupo finito.

Dem:

Sean I y J conjuntos completos de representantes de las clases laterales derechas H en G y K en H, respectivamente. Claramente:

$$I \subset H \text{ y } J \subset K$$

Además:

$$|I| = |G/_D H| = [G:H] \quad \text{y} \quad |J| = |H/_D K| = [H:K]$$

Como:

$$G = \dot{\bigcup_{a \in I}} Ha \quad \text{y} \quad H = \dot{\bigcup_{b \in J}} Kb$$

Sea

$$A = \{ K_{ba} \mid (a,b) \in I \times J \}$$

probaremos que:

$$A = G/_D K$$

En efecto, claramente $A \subset G/_D K$. Probaremos la otra contención. Sea $u \in G$, entonces $Ku \in G/_D K$. Probaremos que $\exists (a,b) \in I \times J$ tal que $u = ba$. Como $u \in G$, $\exists a \in I \ni u \in Ha$, luego $\exists h \in H \ni u = ha$. Como $h \in H$, $\exists b \in J \ni h \in Kb$, así $\exists k \in K \ni h = Kb$, por tanto $u = Kba$, entonces $u \in Kba$. Por tanto $\exists (a,b) \in I \times J$ tal que $Ku = Kba$.

Veamos ahora que $K_{ba} = K_{dc} \Leftrightarrow (a,b) = (c,d)$

$\Leftarrow$) Es inmediata.

$\Rightarrow$) Suponga que $K_{ba} = K_{dc}$, entonces $ba \in Kdc \Rightarrow \exists k \in K \ni ba = Kdc \Rightarrow b = Kd(ca^{-1})$ como $K, d \in H$, pues $K \in K \subset H$ y $d \in J \subset H$, entonces $Kd \in H$. Además $ca^{-1} \in H$, pues $c, a \in I \subset H$ y $H < G$. Por tanto, $ca^{-1} = (Kd)^{-1}b$, donde $(Kd)^{-1}b \in H$, pues $b \in J$

$\subset K \subset H$, así $c \equiv_D a \bmod H \Rightarrow Hc = Ha$, pero $a, c \in I \Rightarrow a = c \Rightarrow ba = Kdc \Rightarrow$
$b = Kd \Rightarrow b \in Kd \Rightarrow Kb = Kd$, como $b, d \in J \Rightarrow b = d$.
Por tanto, $(a,b) = (c,d)$.

Así, $I \times J$ es un conjunto completo de representantes, por lo tanto:

$$[G:K] = |G/_D K| = |A| = |I \times J| = |I| \cdot |J|$$
$$= [G:H] \cdot [H:K]$$

q.e.d.

Def. Sea G grupo y $A, B \subset G$. Definimos

$$AB = \{ab \mid a \in A \text{ y } b \in B\}$$
$$A^{-1} = \{a^{-1} \mid a \in A\}$$
$$AB^{-1} = \{ab^{-1} \mid a \in A \text{ y } b \in B\}$$

Así pues, las siguientes condiciones son equivalentes. Para $H \subset G$, $H \neq \emptyset$:

i) $H < G$.
ii) $HH \subset H$ y $H^{-1} \subset H$.
iii) $HH^{-1} \subset H$.

Dem: es inmediato. q.e.d.

También, si $|H| < \infty$, entonces:

$$H < G \Leftrightarrow HH \subset H.$$

Si $H < G$, entonces:

$$HH = H, \; H^{-1} = H \text{ y } HH^{-1} = H$$

Veamos que, si $H, K < G$, entonces HK no es necesariamente subgrupo de G. Por ejemplo:

$$S_3 = \{e, \pi, \sigma, \pi^2, \sigma\pi, \sigma\pi^2\}$$

donde $|\sigma|=2$, $|\pi|=3$ y $\pi\sigma=\sigma\pi^2$. Consideremos

$$H=\{e,\sigma\} \text{ y } K=\{e,\sigma\pi\}$$

claramente $H, K < S_3$, pero

$$HK=\{e,\sigma,\sigma\pi,\sigma^2\pi=\pi\} \not< S_3$$

pues $|HK| \nmid |G|$.

Proposición.

Sean $H, K < G$, entonces HK es un subgrupo de $G \Leftrightarrow HK=KH$.

Nota: en un grupo abeliano, HK siempre es subgrupo de G.

Dem:

$\Rightarrow$) Suponga que $HK<G$. Probaremos que $HK=KH$.

Sea $x\in HK$, entonces $\exists\ h_1\in H$ y $k_1\in K$ $\ni$ $x=h_1k_1$. Como $HK<G$, entonces $k_1^{-1}h_1^{-1} = (h_1k_1)^{-1}\in HK$, así: $\exists\ h_2\in H$ y $k_2\in H$ $\ni$ $k_1^{-1}h_1^{-1}=h_2k_2 \Rightarrow h_1k_1=k_2^{-1}h_2^{-1}$, luego como $H,K<G$, entonces $h_2^{-1}\in H$ y $k_2^{-1}\in K$. Por tanto, $x\in KH$.

Así, $HK\subset KH$.

Recíprocamente, sea $x\in KH$, entonces $\exists\ k_1\in K$ y $h_1\in H$ $\ni$ $x=k_1h_1$, entonces $x^{-1}= h_1^{-1}k_1^{-1}\in HK$, pues $H,K<G$. Como $x^{-1}\in HK$, como $HK<G$ se tiene que $x\in HK$.

Así, $KH\subset HK$. Luego $HK=KH$.

$\Leftarrow$) Supongamos que $HK=KH$. Probaremos que $HK<G$. Sean $x,y\in HK$, con $x=h_1k_1$ y $y=h_2k_2$, donde $h_1,h_2\in H$ y $k_1,k_2\in K$. Veamos que

$$xy^{-1}=h_1k_1k_2^{-1}h_1^{-1}$$

como $k_1k_2^{-1}\in K$ y $h_1^{-1}\in H$, entonces $k_1k_2^{-1}h_1^{-1}\in KH=HK$, luego $\exists\ h_3\in H$ y $k_3\in H$ tales que $k_1k_2^{-1}h_1^{-1}=h_3k_3$, luego:

$$xy^{-1}=h_1h_3k_3\in HK$$

pues $h_1,h_3\in H$. Por lo tanto, $HK<G$.

q.e.d.

Teorema

Sean $H, K < G$. Entonces:

$$|HK| \cdot |H \cap K| = |H| \cdot |K|$$

en particular, si H y K son finitos se cumple que:

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$$

Dem:

En $H \times K$ definimos la relación $\sim$ dada por: Para cada $(h,k),(h_1,k_1) \in H \times K$, $(h,k) \sim (h_1,k_1) \Leftrightarrow hk = h_1k_1$. Probaremos que $\sim$ es relación de equivalencia.

a) Reflexiva:

Sea $(h,k) \in H \times K$, como $hk = hk$, entonces $(h,k) \sim (h,k)$.

b) Simétrica:

Sean $(h,k),(h_1,k_1) \in H \times K$ tales que $(h,k) \sim (h_1,k_1)$, entonces $hk = h_1k_1 \Rightarrow h_1k_1 = hk \Rightarrow (h_1,k_1) \sim (h,k)$.

b) Transitiva:

Sean $(h,k),(h_1,k_1),(h_2,k_2) \in H \times K$ tales que $(h,k) \sim (h_1,k_1)$ y $(h_1,k_1) \sim (h_2,k_2)$, entonces $hk = h_1k_1$ y $h_1k_1 = h_2k_2 \Rightarrow hk = h_2k_2 \Rightarrow (h,k) \sim (h_2,k_2)$.

Afirmamos ahora que toda clase de equivalencia de $H \times K$ bajo la relación $\sim$ tiene cardinal $|H \cap K|$. En efecto, sea $\mathcal{C}$ una clase de equivalencia de $H \times K$ bajo la relación $\sim$ con representante (h,k). Definimos $f: \mathcal{C} \to H \cap K$ como sigue $f(x,y) = h^{-1}x$, $\forall (x,y) \in \mathcal{C}$. Tenemos lo siguiente:

d) f está bien definida.

Sea $(x,y) \in \mathcal{C}$, como $(x,y) \sim (h,k)$, entonces $xy = hk \Rightarrow yk^{-1} = hx^{-1}$. Como $h, x \in H$ y $y, k \in K$, entonces $hx^{-1} \in H$ y $yk^{-1} \in K$, luego $hx^{-1} = f(x,y) \in H \cap K$.

e) f es inyectiva.

Sean $(x,y),(u,v)\in\mathcal{C}$ tales que $f(x,y)=f(u,v)$, entonces $hx^{-1}=hu^{-1}\Rightarrow x=u$.
Como $(x,y)\sim(u,v)\Rightarrow xy=uv\Rightarrow y=v$, luego $(x,y)=(u,v)$.

f) f es suprayectiva.

Sea $z\in H\cap K$. Tomemos $x=hz\in H$ y $y=z^{-1}k\in K$, claramente $xy=hk$ y, además $(x,y)\in\mathcal{C}$ con $f(x,y)=hx^{-1}=hh^{-1}z=z$.

Por lo tanto, $|\mathcal{C}|=|H\cap K|$.

Además, se cumple que $|(H\times K)/\sim|=|HK|$. Para probarlo, definimos $\varphi: HK\to (H\times K)/\sim$ dada por $\varphi(xy)=[(x,y)]$, $\forall\,(x,y)\in H\times K$. Tenemos lo siguiente:

g) φ está bien definida.

Sean $(x,y),(u,v)\in H\times K$ m $xy=uv$. Entonces $(x,y)\sim(u,v)$, luego $[(x,y)]=[(u,v)]$, así $\varphi(xy)=\varphi(uv)$.

h) φ es inyectiva.

Sean $(x,y),(u,v)\in H\times K$ tales que $\varphi(xy)=\varphi(uv)$, entonces $[(x,y)]=[(u,v)]$ así $(x,y)\sim(u,v)\Rightarrow xy=uv$.

i) φ es suprayectiva.

Sea $[(x,y)]\in(H\times K)/\sim$, entonces $\varphi(xy)=[(x,y)]$.

Así, $|(H\times K)/\sim|=|HK|$. Finalmente, sea R un conjunto completo de representantes de $H\times K$ bajo $\sim$, tenemos:

$$|H|\cdot|K|=|H\times K|=\Big|\dot{\bigcup_{(x,y)\in R}}[(x,y)]\Big|$$

$$=\sum_{(x,y)\in R}|[(x,y)]|=\sum_{(x,y)\in R}|H\cap K|=|R|\cdot|H\cap K|=|(H\times K)/\sim|\cdot|H\cap K|$$

$$=|HK|\cdot|H\cap K|$$

q.e.d.

Corolario.

Sean H y $K<G$, G un grupo finito tales que $|H|,|K|>\sqrt{|G|}$. Entonces $\exists\, x\in H\cap K$

tal que $x \neq e$.

Dem:

Tenemos que:

$$|G| \geq |HK| = \frac{|H|\cdot|K|}{|H\cap K|} > \frac{|G|}{|H\cap K|}$$

$$\Rightarrow |H\cap K| > 1$$

q.e.d.

Corolario.

Sean p y q primos con $p<q$ tales que G es un grupo de orden pq. Si G tiene un subgrupo de orden q, entonces este es el único.

Dem:

Sea K un subrugupo de G de orden q. Entonces $|H| = q = \sqrt{q^2} > \sqrt{pq} = \sqrt{|G|}$. Similarmente se tiene que $|K| > \sqrt{|G|}$. Por el corolario anterior, $|H\cap K| > 1$. Como $H\cap K$ es subgrupo de H, así $|H\cap K| \mid |H|$, como q es primo, entonces $|H\cap K| = q = |K| = |H|$, luego $H = H\cap K = K$.

q.e.d.