A LA SOMBRA DE LOS GRUPOS FINITOS

La Teoría de los Grupos Finitos recibe la influencia directa tanto del Algebra Lineal, como de la Cohomología y la Teoría de Módulos, produciendo innumerables aplicaciones tanto sobre la misma Teoría de los Grupos como en ramas diversas de la Matemática, de la Fisica Teórica o de aspectos puntuales de las ciencias básicas.

Las líneas que siguen son una introducción elemental a los conceptos fundamentales de la Teoría de los Grupos Finitos que, por razones de espacio, exponemos en dos partes, mostrando los aspectos generales en una primera parte, que contiene las nociones básicas sobre los grupos finitos cíclicos y los fundamentales teoremas de Lagrange, del Producto y de Fröbenius, para tratar en una segunda parte los grupos de sustituciones, el concepto de subgrupo distinguido y los llamados p-subgrupos de Sylow.

PARTE I: ASPECTOS GENERALES

01. CARACTERIZACIÓN DE LOS GRUPOS FINITOS:

Sabemos que un grupo es simplemente un par (**G, .**) donde es **G** un conjunto que puede ser finito o infinito, y **.** es una ley de composición interna en **G** con las propiedades de ser asociativa, con elemento neutro y tal que todo elemento de **G** tiene un simétrico respecto a ella en **G**.

$$\forall x, y \in G,\ x.y \in G$$
$$\forall x, y, z \in G,\ x.(y.z) = (x.y).z$$
$$\forall x \in G,\ \exists e \in G \,/\, x.e = e.x = e$$
$$\forall x \in G,\ \exists x' \in G \,/\, x.x' = x'.x = e$$

El orden O(G) de un grupo G es el número de sus elementos. Si G es finito, entonces e O(G)=n es un número finito.

Los grupos finitos se pueden caracterizar de una forma muy sencilla. El teorema siguiente nos muestra condiciones mínimas para que un conjunto finito sea un grupo.

Teorema 01.1.

Si es G un conjunto finito y **.** una ley de composición interna en G, asociativa y cerrada en G, admitiendo simplificación bilateral, entonces el par (G,.) es un grupo.

En efecto:

- Al ser interna y asociativa en G solo queda probar que tiene elemento neutro y que todo elemento de G admite un simétrico en G.
- Para todo elemento a de G podemos considerar todos los productos a.x, de forma que x recorra todo G. También los productos a.x recorrerán todo G, por lo que habrá un producto que coincida con el elemento a. Esto es, hay un elemento e de G tal que a.e=a. Análogamente, habrá también un elemento e' de G tal que e'.a=a
- De lo anterior, deducimos, pues, que para todo elemento *a* de G existen dos elementos e, e' de G tales que *a.e=e'.a=a*. Si aplicamos esto a e y e', se tiene que e'.e=e'.e'=e', y también e.e=e'.e=e, por lo que e = e', es el elemento neutro de la ley interna de G.
- En cuanto al elemento simétrico, cualquiera que sea el elemento a de G existe un elemento a' de G tal que a'.a=e, y también existe un elemento a" de G tal que a.a"=e. Entonces, componiendo por la izquierda con a' se tendrá que a'(a.a")=a'.e→(a'.a).a"=a'.e→e.a"=a'.e→a"=a'. Luego este elemento es el simétrico del elemento a de G.

Llamaremos en adelante multiplicación a la ley interna del grupo finito, representaremos por x^{-1} al elemento simétrico de x mediante la multiplicación, llamaremos asimismo complejo a una parte del grupo, y representaremos por Hr al conjunto de los productos de todos los elementos de H por el elemento r (este por la derecha). Asimismo, el producto de r por la izquierda se representará por rH. Si C es

un complejo y H es un subgrupo de G, representaremos por HC y por CH a los productos de los elementos de C por los elementos de H a izquierda y derecha respectivamente.

02. ORDEN DE UN ELEMENTO:

Teorema 02.1.

En todo grupo finito (G,.) se cumple que para todo elemento a de G existe un entero m tal que $a^m = e$.

En efecto:

Si G es finito y consideramos los productos a, a^2, a^3, ..., estos no pueden ser todos distintos, por lo que hay enteros h<k tales que $a^h=a^k$. Esto quiere decir que $a^{k-h}=e$, y, por tanto existe un m=k-h tal que $a^m=e$.

Definición 02.1.

Se llama orden, característica o periodo de un elemento a de un grupo finito G al mínimo entero positivo m tal que $a^m=e$. Se puede representar por O(a)=m.

Teorema 02.2.

1) Si es $a^m=e$, entonces m es múltiplo del orden de a.
2) Si O(a)=1, entonces a=e.
3) $O(a)=O(a^{-1})$
4) $\forall p \in G,\ b = p^{-1}.a.p \Rightarrow O(b) = O(a)$
5) Para todo entero z, es $O(a^z) \le O(a)$. Si z es primo, entonces $O(a^z) = O(a)$

En efecto:

1) Dividiendo m entre el orden del elemento a, se tiene que m=O(a).q+r, siendo r menor que o(a), pero r ha de ser nulo, pues caso contrario será
$$a^m = a^{O(a).q+r} = a^{O(a).q}.a^r = e.a^r = a^r = e$$
y no sería O(a) el orden de a.
2) En este caso es $a^1=a=e$.
3) Los elementos a y a^{-1} son simétricos. Si es O(a)=h y $O(a^{-1})=h'$, tenemos que es
$$a^h = e \to a^{h-h} = e.a^{-h} \to e = a^{-h} \to \left(a^{-1}\right)^h = e \Rightarrow h' \ \ divide\ h$$
análogamente, por ser a también el simétrico de a^{-1}: h divide a h', por lo que concluimos en que h= h', esto es $O(a)=O(a^{-1})$
4) Si es O(b)=h, se tiene que $b^h = (p^{-1}.a.p)^h = p^{-h}.a^h.p^h = e \to a^h.p^h = p^h$, es decir: $a^h = p^{h-h} = e \to O(a) = h$
5) – Probemos la primera parte llamando $b=a^z$: $b^h = a^{zh} = (a^h)^z = e^z = e \Rightarrow o(b) \le o(a)$
o sea: $o(a^z) \le o(a)$
- En cuanto a la segunda parte, si z y h son primos, $\exists x, y \in Z / xz + hy = 1 \Rightarrow$
$\Rightarrow b^x = a^{xz} = a^{1-hy} = a.a^{-hy} = a.e = a$, es decir a es una potencia de b. Y como también es b una potencia de a, ambos tienen el mismo orden

Teorema 02.3

Si c es de orden *m.n*, tales que *mcd(m,n)=1*, entonces c puede expresarse unívocamente por el producto de dos elementos conmutativos *a*, y *b* de G tales que sus órdenes respectivos son *m* y *n*.

$$O(c) = m.n \Rightarrow c = a.b = b.a \wedge O(a) = m, O(b) = n$$

En efecto:

- Llamando $x=c^n$, $y=c^m$, se tiene que *x.y=y.x*, pues $c^{m+n} = c^{n+m}$.

- Por otra parte: $x^m = \left(c^n\right)^m = c^{n.m} = e,\ \ y^n = \left(c^m\right)^n = c^{m.n} = e$
  Y serán m y n los ordenes respectivos de x e y, pues, caso contrario, si existiese por ejemplo un h<m tal que $x^h=e$, entonces $(c^n)^h = c^{nh} = e$, y el orden de c no sería m.n, sino m.h.

- Por ser *mcd(m,n)=1* existen $u, v \in Z$ tales que *un+vm=1*, con lo cual se tiene que $c = c^{un+vm} = \left(c^n\right)^u \left(c^m\right)^v = x^u.y^v$, y son x^u, y^v conmutables, por serlo *x* e *y*.

- También, por ser *mcd(u,m)=1* se tiene, del teorema 02.1, 5):

$$O(x) = O(x^u) = m$$
$$O(y) = O(y^v) = n$$

por lo que se tiene que si llamamos $a=x^u$, $b=u^v$, será:

$$c=a.b \quad y \quad O(a)=m,\ O(b)=n$$

- La unicidad de esta descomposición se comprueba fácilmente, pues si fuera *C = a.b = a'.b'* se tendría, elevando a *nu*:

$$a^{nu}.b^{nu} = a'^{nu}.b'^{nu} \Rightarrow a^{nu} = a'^{nu}.b'^{nu} \Rightarrow a = a'$$

  y, en consecuencia, también es *b=b'.*

03. SUBGRUPOS:

Teorema 03.1.

Una parte H de un grupo finito (G,.) es un subgrupo de G sii es cerrado para la ley interna del grupo.

En efecto:

Trivialmente, pues la parte H verifica las condiciones del Teorema 01.1

Corolario 03.1.

Un complejo $H \subseteq G$, no vacío, será un subgrupo de G sii $H^2 \subseteq H$.

En efecto:

Trivialmente.

Teorema 03.2.

Sea H subgrupo de G.

a) Si h es un elemento de H, entonces se verifica que $Hh = H = hH$.
b) Si C es una parte de H, entonces se verifica que HC=H=CH.

En efecto:

a) Si $x_i H = x_j H \Rightarrow x_i = x_j \Rightarrow x_i.H$ recorre todo *H* cuando x_i recorre todo *H* $\Rightarrow$ *H.h=H*. Análogamente, *h.H=H.*
b) $C \subseteq H \Rightarrow C = \{x_1,...,x_r\} \wedge HC = \{Hx_1,...,Hx_2\} = \{H,...,H\} = H.$ Análogamente, es también $CH = H$

Corolario 03.2.

Un complejo no vacío $H \subseteq G$ es un subgrupo de G sii $H^2 = H$

En efecto:

Trivialmente, por Corolario 03.1 y Teorema 03.2.

Teorema 03.3.

Si H es un subgrupo del grupo finito (G,.), y p es un elemento cualquiera de G, entonces el complejo $H' = p^{-1}Hp$ es un subgrupo isomorfo a H.

En efecto:

1) Veamos que H' es un subgrupo, comprobando que cumple la condición del Corolario 03.2:

$$H' = p^{-1}Hp \Rightarrow H'^2 = \left(p^{-1}Hp\right)^2 = p^{-1}H^2p = p^{-1}Hp = H \Rightarrow H'^2 = H' \Rightarrow H' \; subgr \; de \; G$$

2) Veamos que H' y H son isomorfos:

Sea *f:H* $\rightarrow$ *H'* definido por la condición de que $\forall h \in H,\ f(h) = p^{-1}hp = h' \in H'$. Entonces, se tiene:

$$\forall h_1, h_2 \in H,\ f(h_1h_2) = p^{-1}h_1h_2p = p^{-1}h_1p.p^{-1}h_2p = f(h_1).f(h_2) \Rightarrow$$
$$\Rightarrow f : H \rightarrow H' \quad \text{es homomorfismo}$$

Veamos que f es inyectivo:

$$f(h_1) = f(h_2) \Rightarrow p^{-1}h_1p = p^{-1}h_2p \Rightarrow h_1 = h_2 \Rightarrow \text{ f es inyectivo}$$

Por tanto *f:H* $\rightarrow$ *H* es isomorfismo, esto es, H' y H son isomorfos.

04. LOS GRUPOS FINITOS CÍCLICOS:

Definición 04.1.

Un grupo finito (G,.) es cíclico si existe en G un elemento a tal que cualquier otro elemento de G es de la forma a^n, $n \in Z^+$. Se dice que a es elemento generador del grupo.

Teorema 04.1.

Si es (G,.) un grupo cíclico finito de orden n, se cumple:

1) (G,.) es conmutativo.
2) Si es a generador de G y es O(G)=n, entonces O(a)=n.
3) Todo subgrupo de G es también cíclico finito.
4) Si es (a^h) un grupo cíclico generado por a^h, entonces $(a^h) = (a^d)$, d=mcd(h,n)

Entonces:

1) Sea *G=(a),* $\forall x, y \in G, \exists h, k \in Z \,/\, x = a^h, y = a^k \Rightarrow x.y = a^{h+k} = a^{k+h} = y.x$
2) Si a es el generador de G y es o(G)=n, entonces es $G = \{a, a^2, ..., a^n\}$ donde son todos los elementos distintos, por lo que el orden del elemento generador a es también n.
3) Sea G=(a), y sea el subgrupo S de G tal que es a^h la menor potencia de a contenida en S. Si fuera también $a^m \in S$, *con* $m > h$, se tendría:
$$a^m = a^{hq+r} = a^{hq}.a^r \Rightarrow a^r \in S,$$
por lo que h no sería la menor potencia de a contenida en S, luego ha de ser r=0, lo cual indicaría que todos los elementos del subgrupo S son de la forma $(a^h)^q$, es decir, $S = (a^h)$ y es, por tanto, cíclico.
4) Veamos que (a^h) está contenido en (a^d), y, al revés, que (a^d) está contenido en (a^h):

   Si mcd(h,n)=d, entonces es $(a^h) \subseteq (a^d)$. Por otra parte, se cumple que

$$\exists u, v \in Z \,/\, uh + vn = d \Rightarrow a^d = a^{uh+vn} = (a^h)^u.(a^n)^v = (a^h)^u \Rightarrow$$
$$\Rightarrow a^d \in (a^h) \Rightarrow (a^d) \subseteq (a^h)$$

   En definitiva, pues, se cumple que $(a^h) = (a^d)$, si d=mcd(h,n).

Corolario 04.1.

Para que una potencia de a, a^h, genere a un grupo G debe ser mcd(h,n)=1. Los elementos h que cumplen esta condición son los enteros menores que n y primos con n, este conjunto se denomina *indicador de Euler* de n.

En efecto,

Trivialmente, de la proposición anterior, teorema 04.1. 4)

Teorema 04.2.

1) Si f:G→H es homomorfismo sobreyectivo del grupo cíclico (G,.) en H, entonces f(G)=H es cíclico finito.
2) Dos grupos cíclicos del mismo orden son isomorfos.

En efecto:

1) Sea G=(a) y f(a)=z∈H. Se tiene:
$$\forall x \in H, \exists m \in Z / a^m = x \Rightarrow \forall x \in H, x = z^m \Rightarrow H = (z)$$
Por tanto, es H un grupo cíclico finito generado por z.

2) Sean dos grupos cíclicos finitos (a) y (b) ambos de orden n.
La aplicación f: (a)→(b) tal que f(a)=b es un isomorfismo.

Corolario 04.2.

Todo grupo cíclico finito de orden n es isomorfo a Z/nZ, grupo finito de las clases de restos módulo n.

En efecto:

Puesto que el conjunto Z/nZ de las clases de restos módulo n es un grupo cíclico finito para la adición, resulta, pues que todo grupo cíclico finito de orden n es isomorfo a Z/nZ.

05. TEOREMA DE LAGRANGE:

Teorema 05.1.

Si H es un subgrupo del grupo finito (G,.), y r,s son elementos de G, entonces se verifica que

$$H.r = H.s \Leftrightarrow r.s^{-1} \in H.$$ Caso contrario es $H.r \cap H.s = \phi$

o bien

$$r.H = s.H \Leftrightarrow s^{-1}.r \in H.$$ Caso contrario es $r.H \cap s.H = \phi$

En efecto:

Si $h = rs^{-1} \in H$, por teorema 03.2. se tiene que $H.rs^{-1} = H \Rightarrow Hr = Hs$

Si $Hr = Hs \Rightarrow H.rs^{-1} = H \Rightarrow rs^{-1} \in H$

Si $h = rs^{-1} \notin H$ entonces $Hr \cap Hs = \phi$, pues, caso contrario, si existieran $h, h' \in H$ tales que $hr = h's \Rightarrow rs^{-1} = hh'^{-1} \in H,$ lo cual contradice la hipótesis.

La segunda parte es de demostración análoga, trivialmente.

Teorema 05.2. (Teorema de Lagrange)

Si es H un subgrupo del grupo finito (G,.) y si son h y g sus ordenes respectivos, entonces h, orden del subgrupo, es factor de g, orden del grupo, de modo que si g= h.n, el entero n=i(H) se denomina *índice del subgrupo H con respecto al grupo G.*

Existen además sendos conjuntos de n elementos $\{r_1, r_{2,\ldots,} r_n\}$ y $\{s_1, s_2, \ldots, s_n\}$ tales que $G = \{H.r_1, H.r_2, \ldots, H.r_n\}$ y $G = \{s_1.H, s_1.H, \ldots, s_n.H\}$.

En efecto:

Sea r_1=e el elemento neutro. Si Hr_1=G hemos terminado. En este caso es O(G)= =O(h)=h y es n=i(H)=1 el índice de H respecto de G.

En cambio, si $Hr_1 \neq G$, existe un $r_2 \in G\text{-}hr_1$ tal que, por teorema 05.1., es $Hr_1 \cap Hr_2 = \phi$. Si $\{Hr_1, Hr_2\} = G$ hemos terminado. En este caso es O(G)=2.O(h)=2h y es n=i(H)=2 el índice de H respecto de G.

En cambio si $\{Hr_1, Hr_2\} \neq G$, existe un $r_3 \in G\text{-}\{Hr_1, Hr_2\}$ tal que, por Teorema 05.1., es $Hr_1 \cap Hr_2 = \phi$ y $Hr_3 \cap Hr_2 = \phi$. Si $\{Hr_1, Hr_2, Hr_3\} = G$ hemos terminado. En este caso es O(G)=3.O(H)=3h y es n=i(H)=3 el índice de H respecto de G.

El proceso continuará al cabo de n etapas, por tratarse de un grupo finito, en donde será $\{Hr_1, \ldots, Hr_n\} = G$. La familia $\{Hr_1, \ldots, Hr_n\}$ se denomina familia de clases a la derecha de H.

Análogamente se prueba para el caso de $\{s_1H,...,s_nH\}$, familia de clases a la izquierda de H.

Corolario 05.1.

1) Si G es un grupo de orden g, el orden de cada elemento de G es factor de g.
2) Un grupo de orden primo no tiene subgrupos propios y es necesariamente cíclico.

En efecto:

1) Si el elemento a$\in$G es de orden h, entonces los elementos $\{a,a^2,...,a^h\}$ forman un subgrupo cíclico de orden h, por lo que h divide a g.

2) Por el apartado anterior, si el orden de G es un número primo p, entonces los subgrupos cíclicos posibles son de orden 1 o p, que son impropios y es, además, $G=\{a,a^2,...,a^p\}$. Por tanto, G es cíclico.

Teorema 05.3.

Todo grupo finito G de orden compuesto tiene subgrupos propios.

En efecto:

- Si G no es un grupo cíclico, se tiene que cualquier elemento a$\neq$e genera un subgrupo (a) de G que es cíclico y (a) $\neq$ G. Luego (a) es subgrupo propio de G.

- Si G es cíclico y su orden g puede factorizarse de la forma g=n.h, entonces (a^h) es un subgrupo cíclico de G de orden n. Luego, en este caso, también, G tiene subgrupos propios.

06. TEOREMA DEL PRODUCTO:

Teorema 06.1. (Teorema del Producto)

Si A y B son subgrupos del grupo finito G con ordenes a y b, respectivamente, y consideramos el complejo producto A.B, se tiene:

1) El orden de A.B es a.b/d, donde d es el orden el subgrupo intersección de A y B.
2) El complejo A.B es un grupo sii A.B=B.A

En efecto:

Sean, pues, a=O(A), b=O(B), d=O(A∩B).

1) Veamos en primer lugar que O(A.B)=O(B.A)=a.b/d:

Sea, por ejemplo, el subgrupo B descompuesto en clases a la derecha respecto del subgrupo D= A∩B:

$$B = \{Db_1, \ldots, Db_n\}, \quad con\ n = \frac{b}{d}$$

Si multiplicamos a izquierda por A:

$$A.B = \{ADb_1, \ldots, ADb_n\} = \{Ab_1, \ldots, Ab_n\}$$

en donde cada elemento Ab_i tiene a elementos, por lo que o(AB)=a.n=a.b/d

Si repetimos el proceso para el subgrupo A, se tiene:

$$A = \{Da_1, \ldots, Da_m\}, \quad con\ m = \frac{a}{d}$$

y, por tanto:

$$B.A = \{BDa_1, \ldots, BDa_m\} = \{Ba_1, \ldots, Ba_m\}$$

y cada elemento Ba_i tiene b elementos, por lo que o(BA)=b.m=b.a/d

en definitiva, es $o(A.B) = o(B.A) = \frac{ab}{d}$

Comprobemos también que los elementos de A.B (por analogía los de B.A) son todos distintos, es decir, que $Ab_i \cap Ab_j = \phi$, $si\ i \neq j$, pues, caso contrario, habría elementos tales que $a_i b_i = a_j b_j$, $con\ a_i, a_j \in A$, $b_i, b_j \in B$, lo cual indicaría que es $a_j^{-1} a_i = b_j b_i^{-1}$, con lo que $a_j^{-1} a_i = b_j b_i^{-1} \in D$ y por tanto $D(b_j b_i^{-1}) = D$ y de aquí se deduciría que $Db_j = Db_i$, que es contradictorio.

Del mismo modo se deduce que todos los elementos de B.A son distintos.

Los complejos A.B y B.A contienen el mismo número de elementos, aún cuando en general, pueden ser distintos (AB≠BA).

2) Veamos ahora la condición de conmutatividad:

- Comprobemos que si A.B es grupo, entonces A.B=B.A:

Si A.B es grupo tenemos que $\forall q_a \in A, \forall q_b \in B \Rightarrow q_a^{-1} \in A, q_b^{-1} \in B$ y también

$$q_a.q_b \in A.B \Rightarrow (q_a q_b)^{-1} = q_b^{-1} q_a^{-1} \in A.B$$

también $q_a \in A, q_b \in B \Rightarrow q_a^{-1}.q_b^{-1} \in A.B \Rightarrow (q_a^{-1}.q_b^{-1})^{-1} = q_b.q_a \in A.B$

Es decir, $q_b.q_a \in B.A \Rightarrow q_b.q_a \in A.B \Rightarrow B.A \subseteq A.B$

Y como tienen el mismo orden, ha de ser A.B=B.A

- Comprobemos ahora que si A.B=B.A, entonces A.B es un grupo:

Bastará aplicar el corolario 03.2, pues,

$$(A.B).(A.B) = A.(B.A).B = A.(A.B).B = (A.A).(B.B) = A^2.B^2 = A.B$$

07. TEOREMA DE FRÖBENIUS:

Teorema 07.1. (Teorema de Fröbenius)

Sean A y B subgrupos del grupo finito (G,.), entonces existen $\{p_1, p_2, \ldots, p_r\}$ elementos de G tales que

$$G = \{Ap_1B, Ap_2B, \ldots, Ap_rB\} \quad y \quad Ap_iB \cap Ap_jB = \phi, \quad i \neq j$$

En efecto:

Elegimos un primer elemento p_i. Puede ocurrir que pertenezca o no a ambos subgrupos.

Si $p_i \in A \; v \; p_i \in B$, *entonces* $Ap_iB = G$, con lo que hemos terminado.

Si $p_i \notin A \wedge p_i \notin B$, *entonces* $p_i \in G - A.B$. En este caso $A.B \cap Ap_iB = \phi$, pues si hubieran elementos $q_a, q_a^{'} \in A, \; q_b, q_b^{'} \in B$ *tales que* $q_a.q_b = q_a^{'}p_iq_b^{'}$, con lo que $q'^{-1}_a \, q_a.q_bq'^{-1}_b = p_i \in AB$, lo cual sería contradictorio.

Si $\{AB, Ap_iB\} = G$ hemos terminado.

Caso contrario, existe un $p_j \in G - \{AB, Ap_iB\}$, y así sucesivamente.

Puesto que G es finito, el proceso ha de terminar, por lo que existirá un conjunto de elementos

$\{p_1, p_2, \ldots, p_r\}$ tal que $G = \{Ap_1B, Ap_2B, \ldots, Ap_rB\} \quad y \quad Ap_iB \cap Ap_jB = \phi, \quad i \neq j$