# 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.**

**Por razones de espacio, exponemos los aspectos generales en una primera parte, que contiene 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 II: CIERTOS SUBGRUPOS FINITOS

## 01. GRUPOS DE SUSTITUCIONES. TEOREMA DE CAYLEY:

### Definición 08.1.

Una sustitución de orden n es una aplicación biyectiva s:A $\to$A, donde A={$a_1$,...,$a_n$} es un conjunto de n elementos. Sea $S_n$ el conjunto de todas las sustituciones de orden n. Podemos representar las sustitución $s_i : A \to A$ por la matriz de dos filas siguiente, en donde la primera fila representa los elementos originales de $s_i$, y la segunda las correspondientes imágenes.

$$s_i = \begin{Bmatrix} q_1 & ,\dots, & q_r \\ q_{i1} & ,\dots, & q_{ir} \end{Bmatrix}, \text{ donde } s_i(q_j) = q_{ij};\ j = 1,2,\dots,r$$

### Definición 08.2.

Se llama transposición, en $S_n$, a una sustitución de orden n que cambia entre sí dos elementos dejando fijos a los restantes. Llamaremos $T_n$ al conjunto de todas las transposiciones en $S_n$. Evidentemente $T_n \subset S_n$.

Si representamos por $t_{kl}=(k,l)$ la transposición que cambia el elemento $q_k$ en el $q_l$ y viciversa, se puede expresar por

$$t_{kl} = (k,l) = \begin{Bmatrix} q_1 & ,\dots, & q_k & q_l & ,\dots, & q_r \\ q_1 & ,\dots, & q_l & q_k & ,\dots, & q_r \end{Bmatrix},$$
$$t_{kl}(q_k) = q_l,\ t_{kl}(q_l) = q_k,\ t_{kl}(q_j) = q_j \ \ si\ \ j \neq k \wedge j \neq l$$

### Teorema 08.1.

1) El número de sustituciones sobre un conjunto de orden n es n!. Esto es, el orden del conjunto $S_n$ es o($S_n$)=n!.
2) ($S_n$,°) es un grupo no conmutativo que llamaremos Grupo de las Sustituciones de orden n, o Grupo Simétrico.

En efecto:

1) El número total de biyecciones de A en A, siendo A un conjunto de n elementos, viene dado por todas las maneras posibles de ordenar los n elementos de A. Por tanto, $S_n$=n!.
2) El par ($S_n$,°) donde ° es la composición de biyecciones, f y g, definida por la condición $\forall q \in A, (f \circ g)(q) = f[g(q)] \in A$, es asociativa, no conmutativa, con elemento neutro (la identidad), y todo elemento f tiene un simétrico (la biyección inversa $f^{-1}$).

**Teorema 08.2.**

1) Las transposiciones $t_{ij}$ son elementos involutivos, es decir, $t_{ij}^2$=e, y su número es n(n-1)/2.
2) El conjunto de las transposiciones es un sistema de generadores del grupo $S_n$.
3) Las n-1 transposiciones (1,2), (2,3), ... ,(n-1,n) son también un sistema de generadores de Sn.

En efecto:

1) Sea, por ejemplo, $t_{ij}(q_j) = q_i$, $t_{ij}(q_i) = q_j$, se tendría:

$$t_{ij}^2(q_j) = (t_{ij} \circ t_{ij})(q_j) = t_{ij}(t_{ij}(q_j)) = t_{ij}(q_i) = q_j$$

Habrá tantas transposiciones $t_{ij} : A \to A$ como maneras de ordenar de dos en dos todos los elementos de A, sin que el orden tenga significación, es decir, se trata de las combinaciones de n elementos con orden 2:

$$o(t_n) = \binom{n}{2} = \frac{n!}{2!.(n-2)!} = \frac{n.(n-1)}{2}$$

2) Veamos la demostración por recurrencia:

- Si el conjunto tiene solo dos elementos, $A_2 = \{q_1, q_2\}$, todas las sustituciones del grupo $S_2$ son la identidad e y las transposiciones $t_{12}$ y $t_{21}$. Por lo cual, cualquier sustitución s$\in S_2$ es generada por estos elementos: $s = \prod t_{jk}$ .
- Si suponemos que las sustituciones s de $S_{n-1}$ están generadas por las transposiciones de $T_{n-1}$, esto es, si $\forall s' \in S_{n-1}$, $s' = \prod t'_{jk}$ entonces, podemos considerar las transposiciones de $S_n$ definidas por

$$t_{jk}(q_i) = t'_{jk}(q_k), \quad si\ k < n$$
$$t_{jk}(q_k) = q_k, \quad si\ k = n$$

y las sustituciones de $S_n$ se pueden expresar por

$$\forall s \in S_n,\ s = t_{ni}.s' = t_{ni} \prod t'_{jk} = \prod t_{jk}$$

3) Vemos que para i<j se verifica que (i,j)=(i,i+1)(i+1,i+2)...(j-1,j), se deduce que cualquiera de las trasposiciones tij puede expresarse como este producto, por lo cual, siendo tij sistema de generadores del grupo simétrico, también lo serán los pares (1,2), ..., (n-1,n), es decir, la familia $\{(i, i+1) / i = 1, \ldots, n-1\}$

**Definición 08.3.**

Un k-ciclo $q=(a_{i1}, ...a_{ik})$ es una sustitución de $S_n$ tal que

$$q(a_{i1}) = a_{i2},\ q(a_{i2}) = a_{i3},\ ...,q(a_{ik-1}) = a_{ik}, q(a_{ik}) = a_{i1} \quad \text{y}$$
$$\forall i \notin \{i_1, i_2, ..., i_k\},\ q(a_i) = a_i$$

dos ciclos, $q_1$ y $q_2$ se dice que son disjuntos, si siendo $I_1$, $I_2$ las familias de los índices sustituidos por $q_1$ y $q_2$, respectivamente, se tiene que es $I_1 \cap I_2 = \phi$ .

**Teorema 08.3.**

1) Cualquier sustitución puede expresarse como producto de ciclos disjuntos.
2) Un ciclo de longitud k engendra un subgrupo cíclico de longitud k.

En efecto:

1) Sea s una sustitución cualquiera sobre un conjunto A de n elementos expresado por $A = \{q_1, ..., q_n\}$ y tomemos un elemento cualquiera para hallar su imagen por s, haremos lo mismo con la imagen y así sucesivamente hasta que aparezca el primer elemento sustituido, esto es, se complete un ciclo. Si el ciclo contiene a todos los n elementos del conjunto A sobre el que actúa la sustitución ya hemos terminado, caso contrario haremos lo mismo con los elementos que restan hasta completar otro ciclo con ellos. Si entre ambos ciclos hemos sustituido a todos los n elementos del conjunto A ya hemos terminado y la sustitución dada es el producto de ambos ciclos. Caso contrario seguiríamos el proceso hasta que no quedasen elementos sin sustituir, proceso que tendrá fin por tratarse de un conjunto finito. La sustitución elegida, cualquiera que sea, es, pues, producto de ciclos que son disjuntos pues los índices de los elementos sustituidos son diferentes.

2) Trivialmente.

**Definición 08.4.**

Si es $s \in S_n$ definimos el número de inversiones de s, $\sqrt{s}$ como el número de pares (i,j) i<j, tales que

$$\frac{s(j) - s(i)}{j - 1} < 0$$

Se llama signatura de s al número $\sigma(s) = (-1)^{\sqrt{s}} = \pm 1.$ Se dice que es par si es +1 y que es impar si es –1.

**Teorema 08.4.**

1) Una transposición es impar.

2) La signatura de un producto de sustituciones es igual al producto de las signaturas.

En efecto:

1) Sea la transposición $t_{jk}$. Se tiene:

$$t_{jk}(j) = k, t_{jk}(k) = j, \frac{t_{jk}(j) - t_{jk}(k)}{j - k} = \frac{k - j}{j - k} = -1 \Rightarrow t_{jk} \text{ impar}$$

2) Si s es una sustitución de $S_n$, se tendrá:

$$\sigma(s) = \prod \frac{s(j) - s(i)}{j - i}$$, extendido a los $\frac{1}{2}n(n-1)$ pares no ordenados (i,j)

si s' es otra sustitución de $S_n$, y teniendo en cuenta que el producto anterior es independiente del orden de los factores, se puede escribir, el siguiente producto, también extendido a los $\frac{1}{2}n(n-1)$ pares (i,j):

$$\sigma(s) = \prod \frac{s(s'(j)) - s(s'(i))}{s'(j) - s'(i)}$$

por tanto, se tiene:

$$\sigma(s).\sigma(s') = \prod \frac{s(s'(j)) - s(s'(i))}{s'(j) - s'(i)} . \prod \frac{s'(j) - s'(i)}{j - i} = \prod \frac{s(s'(j)) - s(s'(i))}{j - i} =$$

$$= \prod \frac{s.s'(j) - s.s'(i)}{j - i} = \sigma(s.s')$$

**Corolario 08.1.**

1) Una sustitución par es igual al producto de un número par de sustituciones.
2) La familia de las sustituciones pares es un subgrupo de $S_n$, que se denomina *grupo alternado.*

En efecto:

1) Es inmediato, de la proposición 08.5. 2).
2) Por corolario 03.2, si $P_n$ es el subconjunto de $S_n$ formado por las sustituciones pares, se tiene que $P_n^{\,2} \subseteq P_n$.

**Teorema 08.5. (Teorema de Cayley)**

Todo grupo finito G de orden n es isomorfo a un subgrupo de $S_n$.

En efecto:

Sea $G = \{q_1,...,q_n\}$ y sea la aplicación de G en $S_n$ definida por:

$$\forall q_i \in G,\ f(q_i) = s_i \in s_n \,/\, s_i(q_r) = q_i.q_r$$

o bien, se puede expresar también asi:

$$\forall q_i \in G,\ f(q_i) \in s_n \,/\, f(q_i)(q_r) = q_i.q_r$$

Veamos que f es un isomorfismo:

- Es f homomorfismo, pues teniendo en cuenta la propiedad asociativa en G

$$(q_i.q_j).q_k = q_i.(q_j.q_k),\ \forall q_i, q_j, q_k \in G$$

ya que

$$\forall q_i, q_j \in G,\ f(q_iq_j) \in S_n \,/\, f(q_iq_j)(q_r) = q_iq_jq_r = q_if(q_j)(q_r) =$$
$$= f(q_i)[f(q_j)(q_r)] = (f(q_i).f(q_j))(q_r),\ \forall q_r \in G$$

O sea:

$$\forall q_i, q_j \in G,\ f(q_iq_j) = f(q_i).f(q_j)$$

- Es homomorfismo inyectivo, pues si $f(q_i) = f(q_j) \Rightarrow q_iq_r = q_jq_r \Rightarrow q_i = q_j$

Por tanto, f es un isomorfismo de G en un subgrupo f(G) del Grupo simétrico $S_n$.

$$G \approx f(G) \subseteq S_n$$

## 09. SUBGRUPOS INVARIANTES O DISTINGUIDOS:

Vamos a estudiar en este apartado las formas en las que ciertas operaciones o manipulaciones en los elementos de un grupo finito dejan invariantes a estos elementos. Tales propiedades son fundamentalmente la conjugación y la conmutatividad, ambas fuertemente relacionadas.

Definiremos primero la conjugación y a continuación expondremos la conmutatividad como una forma de conjugación, que en realidad es lo que podemos llamar autoconjugación.

### Definición 09.1.

Dado un grupo finito (G,.), se definen los elementos conjugados del modo siguiente:

$$q_1, q_2 \in G \text{ conjugados} \Leftrightarrow \exists x \in G / x^{-1} q_1 . x = q_2$$

El elemento x, no necesariamente único, se denomina *elemento transformador.*

Trivialmente, esta relación de conjugación es reflexiva, simétrica y transitiva, esto es, se trata de una relación de equivalencia, si representamos por $[q_1]$, $[q_2]$, ..., los elementos del conjunto cociente, clases de equivalencia, representará cada clase [l] el conjunto de todos los elementos conjugados con l, que se denomina *órbita de l.* El cardinal h de la orbita [l] es el número de elementos que están conjugados con l.

Si descomponemos el grupo G en clases se tiene $G = [q_1] + [q_2] + \ldots + [q_r]$, y si es $h_i$ el cardinal de $[q_i]$, se tendrá que el orden de G es $g = h_1 + h_2 + \ldots + h_r$.

Cuando un elemento está conjugado consigo mismo se dice *autoconjugado*. Se debe cumplir, por tanto:

$$q \in G \text{ autoconj} \Leftrightarrow \exists x \in G / x^{-1} . q . x = q$$

que es lo mismo que decir

$$q \in G \text{ autoconj} \Leftrightarrow \exists x \in G / q . x = x . q$$

Esto es, si en un grupo G hay elementos q autoconjugados, esto quiere decir que existen elementos x de G que conmutan con q. El conjunto de estos elementos que conmutan con el elemento q se llama *normalizador de q.* Representaremos por $N_q$ al normalizador de q.

En general, diremos que q conmuta con x, si q.x=x.q, y, en general, q conmuta con el complejo $C \subseteq G$, si qC=Cq.

Si el normalizador de q es todo el grupo G, quiere decir esto que todos los elementos del grupo conmutan con q. Se dice, entonces, que q es un elemento invariante o autoconjugado en todo G.

Si q es un elemento autoconjugado en G quiere decir esto que es el mismo q el único elemento de G conjugado con q, o sea, que la órbita de q está constituida por un solo elemento, el mismo q, por lo que el cardinal h de la órbita de q es precisamente h=1.
Si en lugar de tomar un elemento q del grupo tomamos una parte o complejo C del mismo, podemos definir los mismos conceptos. Así, para dos complejos C y C' se define la relación de conjugación:

$$C, C' \text{ conjugados} \Leftrightarrow \exists t \in G / t^{-1}Ct = C'$$

relación de equivalencia que parte al conjunto potencia de G, P(G), en clases de equivalencia.

También aquí el conjunto de los elementos de G que conmutan con C se denomina *normalizador de C*, y es también un subgrupo del grupo G.

Si el complejo C es un subgrupo de G, entonces hay h subgrupos de G conjugados con el complejo C. Cuando el único subgrupo conjugado con C es el mismo C, esto es, cuando h=1, se da el caso de autoconjugación.

**Teorema 09.1.**

1) El normalizador, Nq, de un elemento q es un subgrupo.
2) Si es g el orden del grupo G y es n el orden del normalizador de q, esto es, si g=n.h, se verifica que cada clase [q] contiene h elementos distintos, o sea, su cardinal es precisamente el índice en G del normalizador del elemento q.

En efecto:

1) Veamos que efectivamente Nq es un subgrupo de G, probando que para dos elementos a,b cualesquiera de Nq se verifica que $a.b^{-1}$ pertenece también a Nq:

$$\forall a, b \in Nq,\ q.(a.b^{-1}) = a.q.b^{-1} = a.b^{-1}q \Rightarrow a.b^{-1} \in Nq$$

la conmutatividad de q con el inverso $b^{-1}$ se comprueba fácilmente, pues

$$q.b = b.q \Rightarrow b^{-1}.q = q.b^{-1}$$

2) Para probar que todos los elementos de cada clase [q] son distintos, veamos que si consideramos descompuesto G en clases a la derecha de la forma

$$G = N_q t_1 + \ldots + N_q t_h$$

entonces cada elemento $N_q t_i$ genera por conjugación el mismo elemento que genera $t_i$:

$$(N_q t_i)^{-1}.q.(N_q t_i) = t_i^{-1}.q.t_i$$

por otra parte, cada uno de los elementos $N_q t_i$ genera elementos distintos, pues caso contrario se daría una contradicción:

$$\text{si } t_i^{-1}qt_i = t_j^{-1}qt_j \Rightarrow q.t_i.t_j^{-1} = t_i.t_j^{-1}.q \Rightarrow t_i.t_j^{-1} \in N_q \Rightarrow N_q t_i = N_q t_j$$

(lo cual es contradictorio)

**Teorema 09.2.**

Si $O(G)=p^m$ (p primo), esto es, si el grupo G es p-primario, el número de sus elementos autoconjugados es múltiplo de p, es decir, su centro no se reduce al elemento neutro.

En efecto:

Sea la clase $[p_j]$. Si no es autoconjugada entonces su cardinal, $h_j$, divide al orden del grupo, esto es, divide a $p^m$, lo que nos indica que es $h_j = p^s$ (s<m). Esto quiere decir que si llamamos u a la suma de todos los elementos autoconjugados, se puede expresar el orden g del grupo como suma de todos los elementos autoconjugados más los cardinales de las clases que no son autoconjugadas, potencias del primo p:

$$g = p^m = u + p^{s_1} + \ldots + p^{s_k}$$

y de aquí podemos despejar el número de elementos autoconjugados:

$$u = p^m - p^{s_1} - \ldots - p^{s_k} = p.\lambda$$

El número u de elementos autoconjugados es, en definitiva, un múltiplo de p.

**Definición 09.2.**

Un subgrupo S de G se dice que es invariante, normal o distinguido, si su normalizador N es igual a *G (N=G),* o si *h=1*, donde es *h=i($N_S$).*

**Teorema 09.3.**

1) Un subgrupo de índice 2 es siempre invariante.
2) Si por Z denotamos la familia de elementos autoconjugados de G, o centro de G, se tiene que Z es un subgrupo abeliano e invariante de G.
3) Si $O(G)=g=p^2$ (p primo) entonces G es abeliano.

En efecto:

1) si i(H)=2, entonces g=h.2, siendo *h=O(H)*. Descompongamos el grupo G en clases a la derecha respecto del subgrupo H:

$$G = \{H, Hr\}$$

siendo r un elemento de G que no está en H. Es inmediato que las dos clases, H y Hr son disjuntas, pues caso contrario se daría una contradicción:

$H \cap Hr \neq \phi \Rightarrow \exists h_1, h_2 \in H / h_1 r = h_2 \Rightarrow r = h_1^2.h_2 \in H$ , y esto implica que *r.H=H.r*

Entonces, $\forall x \in Hr / x = h.r$ *cumple* : $H.x = H.h.r = H.r = r.H = r.h.H = x.H$

Por lo que, $\forall x \in G, x.H = H.x$ , de lo que se deduce que todos los elementos de G conmutan con H, o bien que el normalizador de H es el grupo G, $N_H$=G. H es, por tanto, subgrupo distinguido de G.

2) Para probar que es un grupo abeliano y distinguido probemos simplemente que se trata de un grupo, pues que es conmutativo y distinguido es evidente.

   Por el teorema 03.1, bastará probar que U es cerrado para la ley interna del grupo:

$$\forall u_1, u_2 \in U \Rightarrow \forall t \in G, t^{-1}u_1u_2t = t^{-1}u_1t.t^{-1}u_2t = u_1u_2 \Rightarrow u_1u_2 \in U$$

3) Sea U el centro del grupo G. Por el Teorema 09.2, el orden de U es multiplo de p y además ha de ser divisor de $p^2$, por lo cual:

$$O(U) = p \wedge O(U) = p^2$$

Si $O(U) = p^2$ entonces hemos terminado. En este caso es U=G y siendo U abeliano esto implica que G es abeliano.

Si $O(U) = p$ en este caso el grupo cociente G/U es de orden p primo, y por tanto G es cíclico, lo que quiere decir que existe en G un elemento generador q:

$$\exists q \in G / G = U + Uq + ... + Uq^{p-1}$$

y dos elementos distintos cualesquiera $x_1$, $x_2$, de G, pueden escribirse de la forma

$$x_1 = u_1q^r, \quad x_2 = u_2q^s$$

por lo cual

$$x_1.x_2 = u_1.u_2q^{r+s} = u_1u_2q^{s+r} = x_2.x_1 \Rightarrow G \text{ abeliano}$$

## 10. SUBGRUPOS DE SYLOW:

### Definición 10.1. (Grupo que opera sobre un conjunto)

Se dice que un grupo T opera sobre un conjunto cualquiera E sii existe un homomorfismo $\Phi$ de T en el grupo S(E) de las biyecciones de E.

### Teorema 10.1

Sea (G, .) un grupo finito y sea T=G y también sea G=E. Si asociamos a cada elemento g de G la correspondencia $f_g$ de G en G definida por

$$\forall x \in G,\ f_g(x) = gx \in G$$

Se cumple:

1) fg es una biyección.
2) La correspondencia $\Phi$ de G en el grupo simétrico de G, S(G), es un homomorfismo

En efecto:

1)
- Es aplicación: $x_1 = x_2 \Rightarrow g.x_1 = g.x_2 \Rightarrow f_g(x_1) = f_g(x_2)$
- Es inyectiva: $f_g(x_1) = f_g(x_2) \Rightarrow g.x_1 = g.x_2 \Rightarrow x_1 = x_2$
- Es sobreyectiva: $\forall g.x \in G \Rightarrow \exists f_g : G \to G \,/\, f_g(x) = gx$

Es, por consiguiente, una biyección.

2) Para ver que se trata de un homomorfismo, veamos que

$$\forall g_1, g_2 \in G,\ \Phi(g_1.g_2) = \Phi(g_1).\Phi(g_2)$$

pues siendo $\Phi(g_1.g_2) = f_{g_1g_2} \quad \wedge \quad \Phi(g_{g_1}).\Phi(g_2) = f_{g_1}.f_{g_2}$

se tiene que

$$\forall x \in G,\ f_{g_1g_2}(x) = g_1g_2x = g_1(g_2x) = g_1(f_{g_2}(x)) = f_{g_1}\left[f_{g_2}(x)\right] = (f_{g_1}.f_{g_2})(x)$$

por tanto: $\forall g_1, g_2 \in G,\ \Phi(g_1.g_2) = f_{g_1g_2} = f_{g_1}.f_{g_2} = \Phi(g_1).\Phi(g_2)$. En realidad $\Phi$ es un isomorfismo: $\Phi(G) \approx G$.

### Corolario 10.1

Todo grupo G opera sobre sí mismo por las traslaciones a la izquierda.

En efecto:

Inmediato, del teorema 10.1.

**Definición 10.2. (Estabilizador de una parte de un grupo)**

La relación R, definida en G por la condición

$$x_1, x_2 \in G,\ x_1 R x_2 \Leftrightarrow \exists y \in G / y.x_1 = x_2$$

es una relación de equivalencia, y como todos los elementos del grupo G están relacionados por ella, la única clase de equivalencia es el mismo grupo G.

Si la relación anterior se define sobre el conjunto de las partes del grup G, P(G), esto es:

$$P_1, P_2 \in G,\ P_1 R_p P_2 \Leftrightarrow \exists P' \in G / P'.P_1 = P_2$$

entonces tal relación de equivalencia $R_p$ tiene más de una clase de equivalencia.

Cuando en esta relación de equivalencia hay una única clase de equivalencia, se dice que *G opera transitivamente en G.* Cuando hay más de una clase de equivalencia se dice que *G opera intransitivamente en G*.

La relación de equivalencia $R_p$ en el conjunto potencia P(G) nos indica, pues, que G opera por ella intransitivamente sobre G. Cada una de las clases de equivalencia en las que tal relación parte el conjunto potencia P(G) se denomina *clase de transitividad u órbita*.

Se define *estabilizador* de una parte $X \in P(G)$ del modo siguiente:

$$G_X \text{ estabilizador de } X \Leftrightarrow \forall b \in G_X, b.X = X$$

**Teorema 10.2.**

1) El estabilizador $G_x$ de $X \in P(G)$ es un subgrupo de G.
2) Si $O(G)=g$ y $O(G_x)=h$, entonces la órbita de X consta de g/h elementos de P(G), todos con el mismo cardinal que X.

En efecto:

Trivial. Es proposición análoga al teorema 09.1 y 09.2, sobre el normalizador de un grupo.

**Definición 10.3. (p-subgrupo de Sylow)**

Si es (G, .) un grupo finito cuyo orden es $O(G)=m.p^r$ donde es p primo no divisor de m, se llama *subgrupo de Sylow* a un subgrupo $H_s$ de G cuyo orden es $O(H_s)=p^r$.

**Teorema 10.3. (Primer Teorema de Sylow)**

a) Un grupo finito (G,.) cuyo orden es divisible exactamente por $p^r$ (p primo, r≥1) admite, para todo entero a tal que 1≤a≤r, por lo menos un subgrupo de orden $p^a$.
b) El número de subgrupos de orden $p^a$ es congruente con 1 módulo p.

En efecto:

a) Si es O(G)=n=m.$p^r$ donde p no divide a m. Y hemos visto que el grupo G opera sobre la familia $P_a(G)$ de las partes de G con exactamente $p^a$ elementos ($1 \le a \le r$). Este conjunto $P_a(G)$ queda descompuesto en clases de transitividad u órbitas $\{C_k : k \in K\}$, siendo $G_k$ el estabilizador de una parte cualquiera $A_k$ de $C_k$. Supongamos que sea $n_a$ el número de elementos distintos de $P_a(G)$. Se tiene que:

$$n_a = \sum_{k \in K} card\ C_k$$

Ahora bien, por el teorema 10.2 sabemos que $card\ C_k = i(G_k) \Rightarrow n_a = \sum_{k \in K} i(G_k)$. Y también es $n_a = \binom{n}{p^a}$, por lo cual:

$$n_a = \frac{mp^r}{p^a}.\frac{mp^r-1}{1}....\frac{mp^r-(p^a-1)}{p^a-1} = mp^{r-a}\binom{mp^r-1}{p^a-1} =$$

$$= mp^{r-a}.w = mp^{r-a}\left(-1+\frac{mp^r}{1}\right)...\left(-1+\frac{mp^r}{p^a-1}\right)$$

donde hemos llamado $w = \prod_{s=1}^{p^a-1}\left(-1+\frac{mp^r}{s}\right)$

De acuerdo con las desigualdades a ≤1, s ≤ $p^a$-1, la potencia más alta de p que divide a s es más pequeña que $p^r$. Cada uno de los factores del segundo miembro es, pues, de la forma

$$-1+\frac{mp^{r'}}{s'},\ con\ r'>0\ y\ mcd(s',p)=1$$

De lo que deducimos $w = (-1)^{p^a-1} + p.\frac{u}{\prod s'}$, (u entero)

Si p ≠ 2, entonces $p^a$-1 es par, y puesto que $\prod s$ es primo con p esto implica que w=1+hp, para un cierto h entero.

Si p = 2, se tiene que w= -1+hp, pero reemplazando h por h+1, queda también de la forma anterior: w=1+h'p.

Por lo cual siempre es $n_a = mp^{r-a}(1+hp)$ $\quad [10.1]$

Hemos visto antes que $card\ C_k = i(G_k) = \frac{O(G)}{O(G_k)} = \frac{mp^r}{O(G_k)}$. Pero de [10.1] se deduce que existe un card($C_k$) divisible como máximo por $p^{r-a}$. En consecuencia será $O(G_k)$ divisible por lo menos por $p^a$, lo cual implica que $O(G_k) \geq p^a$.

Como $G_k$ es el estabilizador de par parte $X \in C_k$, $\forall x \in X$, $G_k x \subseteq X$. Por lo cual:

$$O(G_k) = card(G_k x) \leq cardX = p^a$$

Y de ambas desigualdades: $O(G_k) = p^a$. Se ha construido, en definitiva un subgrupo de orden $p_a$, y además es $G_k.x=X$.

b) Observamos que la clase $C_k$ de X contiene a toda parte aX, en particular:

$$S = x^{-1}G_k x = x^{-1}.X \in C_k$$

siendo S un subgrupo con $p^a$ elementos.

Resulta en definitiva que $C_k$ es el conjunto de las clases por la izquierda con respecto a este subgrupo S (pues $C_k$ es la órbita de X), que, por ello, es el único subgrupo de $C_k$. En consecuencia $C_k$, que es una clase de transitividad cualquiera tal que card($C_k$) sea divisible como máximo por $p^{r-a}$, verifica:

$$card(C_k) = i(G_k) = \frac{mp^r}{O(G_k)} = mp^{r-a}$$

Y, recíprocamente, para todo subgrupo S de orden $p^a$ el conjunto $\{x \in S / x \in G\}$, de clases a la izquierda, es una órbita $C_k$ de este tipo.

Luego, si $s_a$ es el número de subgrupos de orden $p^a$, podemos escribir:

$$n_a = mp^{r-a}.(1+hp) = s_a.mp^{r-a} + t.p^{r-a+1} \Rightarrow m.(1-s_a) = (t-mh).p \quad \text{(t entero)}$$

y, puesto que p es primo con m, se tiene que $s_a \equiv 1 \pmod{p}$

**Corolario 10.2.**

1) Todo grupo finito (G,.) tiene un subgrupo de Sylow para cada número primo p que divida a O(G).
2) Todo grupo finito (G,.) cuyo orden es multiplo del número primo p, contiene al menos un elemento de orden p. (Cayley)

En efecto:

Resulta trivial, por el teorema 10.1.

**Teorema 10.4. (Segundo Teorema de Sylow)**

a) En todo grupo finito G cuyo orden es divisible exactamente por $p^r$ (p primo), todo subgrupo de orden $p^a$ ($1 \le a \le r$) está contenido en un p-subgrupo de sylow.
b) Todos los p-subgrupos de Sylow son conjugados de uno de ellos, y su número (que es congruente con 1 módulo p, por teorema 10.2) es divisor de O(G).

En efecto:

a) Sea H un subgrupo cualquiera, S un p-subgrupo de Sylow de G y H el conjunto de las clases por la izquierda de G respecto a S: $M = \{x_1.S,...,x_m.S\}$, y sea $\{D_i\}$ la familia de clases en que se descompone M bajo la acción de H, cuando tomamos como operadores los elementos de H y decimos que dos elementos X, Y de M son conjugados sii $\exists a \in H / a.X = Y$ . Se tiene que $card\ M = m = \sum_i card\ D_i$ .

   Al ser m primo con p, al menos una de estas clases, sea D, cumple que card D no es múltiplo de p, pero por el teorema 10.2, es card D=$i_H$(E) = índice en H del estabilizador E de un representante K de D. Así, pues, p no divide a $i_H$(E).

   Tomamos como H un subgrupo de orden pa ($1 \le a \le r$): $i_H$(E) divide a O(H)=$p^a$ y como no es múltiplo de p esto quiere decir que $i_H$(E)=1, es decir, card D =1.

   Luego D={K}, ed decir, la clase D consta de un solo elemento: K. Esta clase K=k.S, elemento único de su clase de transitividad D, es, pues, invariante por H:

$$HkS = kS \Rightarrow HkSk^{-1} = kSk^{-1}$$

   Pero $T=K.S.K^{-1}$ es, como S, un subgrupo de orden pr y la igualdad precedente se escribe H.T=T, lo cual implica que $H \subseteq T$ donde es T p-subgrupo de Sylow.

b) Si a= r, H= T, luego es un conjugado de S.

   Por el teorema 09.2, el número de conjugados de S, igual al índice del normalizador de S, es un divisor del orden de G.

## 11. Bibliografía:

**Alperin, J.L; Bell, Rowen B**. Groups and Representations. Graduate Texts in Mathematics 162, Springer-Verlag New York Inc., New York, 1995
**Anzola, M.; Caruncho, J.; Pérez-Canales, G.,** Problemas de álgebra, Alef (1981)
**Burnside, W.**, *Theory of Groups of Finite Order*, 2nd edition, Dover, New York, 1955.
**Dixon, J. D.,** Problems in group theory, Dover Publications (1973).
**Dorronsoro, J.; Hernández, E**., Números, grupos y anillos, Ed. Addison-Wesley Iberoamericana - U.A.M. (1996).
**Fraleigh, J.B**., Álgebra Abstracta, Ed. Addison-Wesley Iberoamericana (1987).
**Godement, R.**, Álgebra, Tecnos (1978).
**Humphreys, ] John F.** A Course in Group Theory. Oxford Science Publications, Oxford University Press Inc., New York, 1996
**Hungerford, T.W**., Algebra, Springer-Verlag (1974).
**Kerber, A.** Aplied Finite Group Actions, 2nd edition, Springer 1999.
**Lang, Serge.** Algebra. Addison-Wesley Publishing Company Inc., Reading, Massachusetts, 3rd edition, 1993,
**Robinson, Derek J. S.,** A Course in the Theory of Groups, Springer, New York, 1995.