UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

SOBRE GRUPOS FINITOS SOLUBLES

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

MATEMÁTICO

P R E S E N T A:

ALBERTO ISRAEL INCLÁN MELÉNDEZ

DIRECTOR DE TESIS:
DR. JUAN MORALES RODRÍGUEZ
2011

1.Datos del alumno	1. Datos del alumno
Apellido paterno	Inclán
Apellido materno	Meléndez
Nombre(s)	Alberto Israel
Teléfono	21 56 06 97
Universidad Nacional Autónoma de México	Universidad Nacional Autónoma de México
Facultad de Ciencias	Facultad de Ciencias
Carrera	Matemáticas
Número de cuenta	302141568
2. Datos del tutor	2. Datos del tutor
Grado	Dr
Nombre(s)	Juan
Apellido paterno	Morales
Apellido materno	Rodríguez
3. Datos del sinodal 1	3. Datos del sinodal 1
Grado	M en C
Nombre(s)	Manuel Gerardo
Apellido paterno	Zorrilla
Apellido materno	Noriega
4. Datos del sinodal 2	4. Datos del sinodal 2
Grado	Dr
Nombre(s)	Emilio
Apellido paterno	Lluis
Apellido materno	Puebla
5. Datos del sinodal 3	5. Datos del sinodal 3
Grado	Dr
Nombre(s)	Hugo Alberto
Apellido paterno	Rincón
Apellido materno	Mejía
6. Datos del sinodal 4	6. Datos del sinodal 4
Grado	Dra
Nombre(s)	María del Carmen
Apellido paterno	Gómez
Apellido materno	Laveaga
7. Datos del trabajo escrito.	7. Datos del trabajo escrito
Título	Sobre Grupos Finitos Solubles
Subtitulo	
Número de páginas	44 pp
Año	2011

INTRODUCCIÓN

En el presente trabajo se estudian algunos teoremas clásicos sobre los grupos finitos solubles: teorema de Phillip Hall, teorema de Carter, teorema de Schur-Zassenhaus y algunos teoremas sobre el subgrupo de Frattini y sobre grupos p-nilpotentes.

En el capítulo 1 se aborda un Teorema de Phillip Hall, que data de 1928. Este teorema tiene tres incisos, el primero de los cuales asegura que si el orden de un grupo soluble G es mn, con m y n primos relativos, G tiene subgrupos de orden m. De hecho esta propiedad caracteriza a los grupos finitos solubles. Se hace ver esta última afirmación utilizando el célebre p-q teorema de Burnside.

El capitulo 2 trata sobre los subgrupos de Carter (que son subgrupos nilpotentes y autonormalizantes). Se demuestra que todo grupo finito soluble tiene subgrupos de Carter, así como un teorema que guarda una gran similitud con los teoremas de Sylow. También se da un ejemplo de un grupo finito no soluble que tiene subgrupos de Carter.

En el capítulo 3 se demuestra el resultado conocido como "Teorema de Schur-Zassenhaus" que afirma que si G es un grupo finito y N es un subgrupo de Hall normal, G tiene al menos un complemento de N y que los complementos de N en G forman una clase de conjugación.

El último capítulo trata sobre grupos finitos p-nilpotentes, es decir, grupos finitos que tienen un p-complemento normal. Se da una caracterización de tales grupos y se demuestra que un grupo finito es nilpotente si y sólo si es p-nilpotente para cada primo p que divide al orden de G. A continuación se dan algunas propiedades del subgrupo de Frattini de un grupo finito. Utilizando esta herramienta y el teorema de Schur-Zassenhaus se da una condición suficiente para que un grupo finito sea p-nilpotente.

Los prerrequisitos contienen definiciones y resultados que son necesarios en los capítulos siguientes.

CAPITULO 0
PRERREQUISITOS: DEFINICIONES Y RESULTADOS BÁSICOS

En este trabajo supondremos que se conocen las definiciones y resultados que se presentan en los cursos básicos de Álgebra Abstracta y que se encuentran en los libros de Álgebra Abstracta de J. Rotman [9] y de Teoría de Grupos de W. Lederman [7].

Proposición 1 : Si S, T, R son subconjuntos de G se tiene que $S(TR) = (ST)R$; $(ST)^{-1} = T^{-1}S^{-1}$.

Convención: Si $S = \{a\}$ en lugar de $\{a\}T$ escribimos aT y Ta en vez de $T\{a\}$.

Proposición 2 : Si G es un grupo y $\Phi \neq U \subset G$, U es subgrupo de G si y solo si $UU = U = U^{-1}$.

Proposición 3 : Un subconjunto finito S de un grupo G es un subgrupo de G si y solo si $SS = S$.

Proposición 4 : Sea G un grupo y A, B subgrupos de G. AB es subgrupo de G si y sólo si $AB = BA$.

Demostración:

Supongamos que $AB < G$ entonces, por la proposición 1.1 $AB = (AB)^{-1} = B^{-1}A^{-1} = BA$. Inversamente supongamos que $AB = BA$; $(AB)(AB) = A(BA)B = A(AB)B = (AA)(BB) = AB$ y $(AB)^{-1} = (BA)^{-1} = A^{-1}B^{-1} = AB$ por lo que $AB < G$ ■

Definición: Sea G un grupo y $K \subset G$, se define el *subgrupo generado* por K (y se denota $\langle K \rangle$) como la intersección de todos los $H < G$ tales que $K \subset H$.

Proposición 5 : Sea K un subconjunto de un grupo G. Si $K = \Phi$,

$\langle K\rangle = \{1\}$. Si $K \neq \Phi$,
$\langle K\rangle = \left\{x_1^{\varepsilon_1}x_2^{\varepsilon_2}\ldots x_r^{\varepsilon_r} \mid r \geq 1, x_1,\ldots,x_r \in K, \varepsilon_i = 1 \text{ ó } \varepsilon_i = -1 \text{ para toda } 1 \leq i \leq r\right\}$

Convención: Si $H,K \subset G$ en vez de $\langle H \cup K\rangle$ escribiremos $\langle H,K\rangle$; y si $a_1,a_2,\ldots,a_n \in G$ en lugar de $\langle\{a_1,a_2,\ldots,a_n\}\rangle$ escribiremos $\langle a_1,a_2,\ldots,a_n\rangle$.

Es inmediato que $\langle K\rangle$ es un subgrupo de G, que es el mínimo subgrupo de G que contiene a K y que $\langle K\rangle = K$ si y solo si $K < G$.

Proposición 6 : Sean A,B subgrupos finitos de G entonces $|AB| = \frac{|A||B|}{|A\cap B|}$.

Definicion: Si $S < G$ y $x \in G$, al conjunto $Sx = \{sx \mid s \in S\}$ se le llama *clase derecha* de S en G y análogamente xS se llama *clase izquierda* de S en G.

Proposición 7 : Sea $S < G$ y $x,y \in G$. $Sx = Sy \Leftrightarrow yx^{-1} \in S \Leftrightarrow y \in Sx$. Analogamente $xS = yS \Leftrightarrow y^{-1}x \in S \Leftrightarrow y \in xS$.

Proposición 8 : Si $S < G$ y $x \in G$, las funciones $S \longrightarrow Sx$ y $S \longrightarrow xS$ tales que $t \to tx$ y $t \to xt$ son biyecciones de S en Sx y de S en xS respectivamente, por tanto $|S| = |xS| = |Sx|$.

Proposición 9 : Si $G/_IH$ es el conjunto de clases izquierdas y $G/_DH$ es el conjunto de las clases derechas; $G/_IH$ y $G/_DH$ son particiones de G y $|G/_IH| = |G/_DH|$.

Definición: El *orden de un grupo* G es el cardinal del conjunto G y se denota con $|G|$.

Definición: Si $S < G$ y el conjunto de clases derechas de S en G es finito, el número de clases derechas (o izquierdas) de S en G se llama el *indice de S en G* y se denota $[G : S]$.

Teorema de Lagrange 10 : Si S es un subgrupo de G y G es finito se tiene que $|G| = |S|[G : S]$. Por lo tanto el orden de cualquier subgrupo de G divide al orden de G.

Observación: EL orden de un subgrupo de un grupo finito es un divisor del orden del grupo. Sin embargo el inverso de esta afirmación no es cierta, A_4, el grupo de las permutaciones pares del grupo simétrico S_4 es un grupo de orden 12 y no tiene subgrupos de órden 6.

Teorema 11: Si G es un grupo de orden 12 y no es isomorfo a A_4, G contiene un elemento de orden 6.

Relación de Dedekind 12 : Sea G un grupo finito y X, Y, Z subgrupos de G tales que $Y < X$. Entonces, $X \cap (YZ) = Y(X \cap Z)$.

Teorema 13: Si $A < B < G$ entonces $[G : A] = [G : B][B : A]$.

Definición: Si G es un grupo, $g \in G$; el *centralizador de g en G*, denotado por $C_G(g)$, es el siguiente conjunto $\{x \in G \mid gx = xg\}$ que es un subgrupo de G.

Teorema 14: Si G es un grupo finito, $g \in G$, la clase conjugada de g tiene $[G : C_G(g)]$ elementos, es decir
$|\{xgx^{-1} \mid x \in G\}| = [G : C_G(g)]$.

Definición: Si H un subgrupo del grupo G, se dice que H es *normal* en G y se escribe $H \lhd G$ si para toda $a \in G$, se cumple que $aHa^{-1} \subset H$.

Teorema 15: Si H es un subgrupo de G, las siguientes condiciones son equivalentes:

i) $H \lhd G$

ii) para toda $g \in G \quad gHg^{-1} = H$.

iii) para toda $g \in G \;\; gH = Hg$.

iv) para toda $a, b \in G$ existe $c \in G$ tal que $aHbH = cH$.

v) para toda $a, b \in G \;\; aHbH = abH$.

vi) para toda $a \in G$, $x \in H$ existe $x_1 \in H$ tal que $ax = x_1 a$.

vii) H es el núcleo de un homomorfismo cuyo dominio es G.

Definición: Se dice que un grupo G es *simple* si sus únicos subgrupos normales son $\langle 1 \rangle$ y G.

Ejemplos: $\mathbb{Z}_p$ con p un primo y el grupo alternante A_n sobre un conjunto de n objetos, con $n \geq 5$ son simples.

Definición: Sea G un grupo, y $X \subset G$. El *subgrupo normal de G generado por X* es la intersección de todos los subgrupos normales de G que contienen a X y se denota por X^G.

El subgrupo X^G, también llamado la cerradura normal de X en G, es el mínimo subgrupo normal de G que contiene a X.

Si $X \neq \Phi$, X^G es el subgrupo generado por todos los conjugados de

elementos de X.

Definición: X_G llamado el *interior normal* de X en G es el producto de todos los subgrupos normales de de un grupo finito G contenidos en X.

X_G es el subgrupo normal más grande de G contenido en X. Si $H < G$, $H_G = \bigcap_{g \in G} g^{-1}Hg$.

Definición: Sea G un grupo, $A, B < G$; se dice que G es *producto directo* de A y B si $G = AB$, $A \cap B = \langle 1 \rangle$ y $A, B \lhd G$.

Definición: Sea G un grupo y $H < G$, definimos el *normalizador* de H en G, y lo denotamos como $N_G(H)$, de la siguiente manera $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$.

Teorema 16: Si $H < G$ y $x \in G$, $N_G(xHx^{-1}) = xN_G(H)x^{-1}$.

Definición: Sea G un grupo y $H < G$, definimos el *centralizador de H en G*, y lo denotamos como $C_G(H)$, de la siguiente manera $C_G(H) = \{g \in G \mid ghg^{-1} = h$, para toda $h \in H\}$.

Definición: Sea G un grupo y $A, B < G$, se dice que A *centraliza a* B si $A \subset C_G(B)$.

Definición: Un grupo abeliano, o conmutativo, de orden p^n(con p un primo) es llamado *abeliano elemental* si es producto directo de subgrupos de orden p.

Definición: Sea G un grupo y $H < G$ con $H \neq G$, se dice que H es *maximal* si es un elemento maximal del conjunto de los subgrupos propios de G, esto es, si no existe $K \lneqq G$ tal que $H \lneqq K$.

Definición: Sea G un grupo y $\langle 1 \rangle \neq H \lhd G$, se dice que H es un *subgrupo normal minimal* de G si no existe $K < G$, $K \neq \langle 1 \rangle$ tal que $K \lhd G$ y $K \lneqq H$.

Definición: Sea G un grupo y sean $a, b \in G$; el *conmutador* de a y b es el elemento $a^{-1}b^{-1}ab$ y se denota $[a, b]$. El subgrupo conmutador o subgrupo derivado de G, denotado por G', es el subgrupo generado por los todos los conmutadores $[a, b]$ de G, es decir $G' = \langle [a, b] \mid a, b \in G \rangle$.

Definición: Si $H, K < G$, el subgrupo *interderivado* de H y K, denotado por $[H, K]$, es el subgrupo $[H, K] = \langle [h, k] \mid h \in H, k \in K \rangle$.

Proposición 17: Si G es un grupo, $H < G$, H es normal en G si y

sólo si $[G,H] < H$.

Definición: Si G es un grupo ($G^{(0)} = G$), $G^{(1)}$ es el subgrupo conmutador de G y recursivamente $G^{(n+1)}$ es el subgrupo conmutador de $G^{(n)}$.

$G^{(n)}$ es llamado el n-ésimo conmutador de $\dot{G}$ o el n-ésimo derivado de G.

La cadena $G^{(0)} = G > G^{(1)} > G^{(2)} \ldots > G^{(n)} > G^{(n+1)} > \ldots$ se llama serie derivada de G.

Proposición 18 : Si G es un grupo, el i-ésimo grupo derivado $G^{(i)}$ es un subgrupo normal de G.

Teorema 19: Sea G un grupo, H un subgrupo normal de G y G/H el conjunto de las clases izquierdas (o derechas) de H en G. Se tiene que G/H con la operación $aHbH = abH$ es un grupo, llamado grupo cociente de G módulo H.

Teorema 20: Sea G un grupo, $H \lhd G$. La función $\pi : G \to G/H$ tal que $\pi(a) = aH$ es un homomorfismo suprayectivo, llamado el homomorfismo natural o canónico de G en G/H.

Teoremas de isomorfismo 21: Sean G y H grupos:

1)Sea $f : G \to H$ un homomorfismo de grupos, entonces $(G/\ker f) \simeq \operatorname{Im} f$.

2) Si N es un subgrupo normal de un grupo G y H es un subgrupo cualquiera de G, entonces $H \cap N \lhd H$ y $H/(H \cap N) \simeq NH/N$.

3) Si N y H son dos subgrupos normales en un grupo G, con $N < H$, entonces $H/N \lhd G/N$ y $G/H \simeq (G/N)/(H/N)$.

Teorema de la correspondencia 22: Sea G un grupo, $H \lhd G$ y $\pi : G \to G/H$ el homomorfismo natural o canónico. $S \rightarrowtail \pi(S) = S/H$ es una biyección entre Sub(G;H), la familia de todos los subgrupos S de G que contienen a H y, Sub(G/H), la familia de todos los subgrupos de G/H. Si denotamos S/H por S^*, $T < S$ si y solamente si $T^* < S^*$, en este caso $[S : T] = [S^* : T^*]$; $T \lhd S$ si y solamente si $T^* \lhd S^*$ y se tiene que $S/T \cong S^*/T^*$.

Teorema 23: Si G es un grupo y $N < G$ las siguientes dos condiciones son equivalentes:

i) $N \lhd G$ y G/N es abeliano.

ii) $G' < N$.

Corolario 24: Si G es un grupo, G' es normal en G y G/G' es abeliano.

Definición: Si G es un grupo, el *centro de* G, denotado por $Z(G)$, es el subgrupo formado por todas las $x \in G$ tales que $xy = yx$ para toda $y \in G$.

Ejemplos:

i) Si G es un grupo abeliano, $Z(G) = G$.

ii) Si $n \geq 3$ el grupo simétrico S_n tiene centro trivial, es decir $Z(S_n) = \{1\}$ y si $n \geq 4$ el grupo alternante A_n tiene centro trivial.

iii) Si n es par, el centro del grupo diédrico $D_{2(n)}$ tiene orden 2. Si n es impar el centro de $D_{2(n)}$ es trivial.

Observación: El centro de un grupo es un subgrupo normal.

Teorema 25: Si G es un grupo no abeliano, el grupo $G/Z(G)$ no es cíclico.

Teorema 26: Sea G un grupo finito y $H \triangleleft G$. Si $([G : H], |H|) = 1$ se tiene que H es el único subgrupo de G de orden $|H|$ y para toda $\varphi \in aut(G)$ tenemos que $\varphi(H) = H$.

Demostración:

Supongase que $K < G$ y $|K| = |H|$:

$KH/H \simeq K/H \cap K$ de donde $[KH : H] = [K : H \cap K] = \frac{|K|}{|H \cap K|}$ y tenemos que $|H| = |K| = |H \cap K|\,[KH : H]$ entonces $[KH : H]$ divide a $|H|$, por otro lado $[G : H] = [G : KH][KH : H]$ lo que implica que $[KH : H]$ divide a $[G : H]$ y como $([G : H], |H|) = 1$ tenemos que $[KH : H] = 1$ y $KH = H$ de donde $K < H$ y se tiene que $K = H$.

Si $\varphi \in aut(G)$, $|\varphi(H)| = |H|$ y por tanto $\varphi(H) = H$■

A continuación presentamos una demostración diferente del teorema anterior:

Sea $K < G$ tal que $|K| = |H|$ demostraremos que $K = H$:

Sea $a \in K$; $aH \in G/H$, $|aH|$ divide a $|G/H|$ lo que implica que $|aH|$ divide a $[G : H]$. Por otro lado $|aH|$ divide a $|a|$, como $|a|$ divide a $|K|$ tenemos que $|aH|$ divide a $|K|$ y por ende $|aH|$ divide a $|H|$. Como

$([G:H],|H|)=1$, $|aH|=1$ por lo que $aH=H$, esto implica que $a\in H$ y por tanto $K\subset H$, por lo que concluimos que $H=K$■

Definición: Un subgrupo H de un grupo G es *característico* si para toda $\varphi\in aut(G)$ se tiene que $\varphi(H)\subset H$.

Definición: Si G es un grupo finito y $H<G$ se dice que H es un *subgrupo de Hall* de G si $(|H|,[G:H])=1$.

El teorema anterior asegura que en un grupo finito G, si H es un subgrupo de Hall y $H\triangleleft G$ entonces H es un subgrupo caracteristico de G.

Definición: Sea G un grupo, $H\lneqq G$, decimos que H es un *subgrupo normal maximal* de G si $H\triangleleft G$ y no existe K tal que $K\triangleleft G$ y $H\lneqq K\lneqq G$.

Definición: Una *serie de composición* de un grupo G es una cadena de subgrupos $\langle 1\rangle=G_r<G_{r-1}<\cdots<G_1<G_0=G$, tal que G_i es subgrupo normal maximal de G_{i-1} para cada $i=1,2,\ldots,r$.

Proposición 27: Todo grupo finito tiene una serie de composición.

Demostración:

Sea G un grupo finito. Si G es simple entonces $1\subset G$ y esa es una serie de composición de G. En otro caso, G tiene un subgrupo normal maximal G_1 y otra vez hay dos casos, que G_1 sea simple o no, si es simple la cadena $1\subset G_1\subset G_0=G$ es una serie de composición, si no es simple entonces existe G_2 tal que es subgrupo maximal normal de G_1 de esta manera y teniendo en uenta que G es finito, concluimos que $1\subset G_r\subset\cdots\subset G_1\subset G_0=G$ es una serie de composición de G■

Definición: Una *serie principal* de un grupo finito G es una cadena de subgrupos $\langle 1\rangle=G_r\subset G_{r-1}\subset\cdots\subset G_1\subset G_0=G$, tal que $G_i\triangleleft G$ y no existe $K\triangleleft G$ tal que $G_i\subsetneqq K\subsetneqq G_{i-1}$ con $i=1,2\ldots r$.

Teorema 28: Todo grupo finito tiene una serie de principal.

La demostración es análoga a la del teorema anterior.

Definición: En los casos de las 2 definiciones anteriores, llamaremos factores de composición o factores principales a los cocientes G_{i-1}/G_i segun sea el caso.

Definición: Si G_{i-1}/G_i es un *factor principal* de G, se dice que G_{i-1}/G_i es central si está contenido en el centro de G/G_i.

Teorema de Jordan-Hölder 29: Sean $G = H_0 \supsetneq H_1 \supsetneq \cdots \supsetneq H_r = \langle 1 \rangle$ y $G = L_0 \supsetneq L_1 \supsetneq \cdots \supsetneq L_s = \langle 1 \rangle$ dos series de composición (o dos series principales) de G. Entonces $r = s$ y existe una función biyectiva φ del conjunto $\{H_0/H_1, H_1/H_2, \ldots, H_{r-1}/H_r\}$ sobre el conjunto $\{L_0/L_1, L_1/L_2, \ldots, L_{r-1}/L_r\}$ tal que los factores H_i/H_{i+1} y $\varphi(H_i/H_{i+1})$ son isomorfos para toda $r = 1, 2, \ldots, (r-1)$.

Definición: Sea G un grupo finito. Se dice que G es *soluble* si existe algún entero positivo n tal que $G^{(n)} = \langle 1 \rangle$.

Un ejemplo de grupos solubles son los grupos abelianos, porque si G es abeliano tenemos para toda $a, b \in G,\ [a, b] = 1$ y por consiguiente $G^{(1)} = \langle 1 \rangle$.

Algunas propiedades elementales de los grupos solubles:

Teorema 30: Si G un grupo soluble y $H < G$, H es soluble. Y si $H \triangleleft G,\ G/H$ es soluble.

Teorema 31: Sea G un grupo y $N \triangleleft G$. Si N y G/N son solubles, entonces G es soluble.

Teorema 32: Sea G un grupo finito y $A, B \triangleleft G$ tales que A, B son solubles; entonces AB también es soluble.

Definición: A la serie de subgrupos $G = G_0 > G_1 > G_2 > \ldots > G_r > \ldots$ de un grupo G se le llama *serie subnormal* si $G_{i+1} \triangleleft G_i$ para cada i. Y una serie subnormal de G es llamada *serie normal* si $G_i \triangleleft G$ para cada $1 \leq i$. Los grupos cocientes G_i/G_{i+1} son llamados factores de la serie.

Teorema 33: Si G es un grupo, las siguientes afirmaciones son equivalentes:

a) G es soluble.

b) G tiene una serie normal que termine en $\langle 1 \rangle$ con sus factores abelianos.

c) G tiene una serie subnormal que termine en $\langle 1 \rangle$ con sus factores abelianos.

Teorema 34: Los subgrupos minimales normales de un grupo finito soluble son abelianos elementales.

Teorema 35: Sea G un grupo finito, entonces las siguientes afirmaciones son equivalentes:

a) G es soluble.

b) Los factores de cualquier serie de composición tienen orden primo.

c) Los factores de cualquier serie principal de G son abelianos elementales.

Definición: Se dice que si p es un número primo y G un grupo finito, G es un *p-grupo* si $|G| = p^n$ para algun entero no negativo n.

Teorema 36: Si G es un p-grupo finito entonces.

a) $Z(G) \neq \{1\}$.

b) Si $\langle 1\rangle \neq N \triangleleft G$, $N \cap Z(G) \neq \langle 1\rangle$.

Teorema 37: Si G es un p-grupo finito no trivial (con p un número primo) y H/K es un factor principal de G, H/K es de orden p.

Teorema 38: Si G es un p-grupo finito cada serie principal de G es una serie central.

Corolario 39: Si G es un p-grupo finito no trivial (con p un número primo), G es soluble.

Teorema de Cauchy 40: Si G es un grupo finito y p un primo que divide al orden de G, G tiene un elemento de orden p.

Definición: Si G es un grupo finito de orden $p^k m$, p un primo tal que no divide a m, un subgrupo de G de orden p^k se llama *p-subgrupo* de Sylow de G.

Ejemplos:

i) Si $G = S_3$, A_3 es un 3-subgrupo de Sylow de S_3 y $H = \langle(12)\rangle$ es un 2-subgrupo de Sylow de S_3.

ii) Si $G = Q \times \mathbb{Z}_{3^2}$ con Q el grupo de cuaterniones de orden 8, $|G| = 2^3 * 3^2$, Q es un 2-subgrupo de Sylow de G y $\mathbb{Z}_{3^2}$ es un 3-subgrupo de Sylow de G.

Teoremas de Sylow 41: Si G es un grupo finito y p divide al orden de G, se tiene que:

a) G tiene p-subgrupos de Sylow.

b) Si Q es un p-subgrupo de G y P es un p-subgrupo de Sylow de G, existe $x \in G$ tal que $Q < xPx^{-1}$, en particular, si Q es subgrupo

de Sylow de G, P y Q son conjugados.

c) Si r_p es el número de subgrupos de Sylow de G, $r_p \equiv 1(\mathrm{mod}\, p)$ y $r_p \mid [G : P]$, de hecho $r_p = [G : N_G(P)]$.

Corolario 42: Sea G un grupo finito. Si existe un p-subgrupo de Sylow P de G que sea normal entonces P es el único p-subgrupo de Sylow de G, e inversamente, si P es el único p-subgrupo de Sylow de G, entonces P es normal en G.

Demostración:

Sea S un p-subgrupo de Sylow de G. Entonces existe $x \in G$ tal que $x^{-1}Px = S$, pero P es normal, por tanto $P = x^{-1}Px = S$.

E inversamente, si P es el único p-subgrupo de Sylow de G entonces para toda $x \in G$ $x^{-1}Px$ es un p-subgrupo de Sylow de G y por consiguiente $P = x^{-1}Px$, i.e. P es normal en G■

Proposición 43: El grupo de cuaterniones de orden 8 no es un subgrupo de S_4 ni de S_5.

Demostración:

$$|S_4| = 4 * 3 * 2 = 2^3 * 3\ ,\ |S_5| = 5 * 4 * 3 * 2 = 5 * 2^3 * 3$$

El grupo diédrico $D_{2(4)}$ es un 2-subgrupo de Sylow de S_4 y de S_5 y como $D_{2(4)}$ y Q no son isomorfos, no son conjugados y Q no es un subgrupo de S_4 ni de S_5■

Teorema 44: Sea G un grupo finito:

i) Si Q es un p-subgrupo de Sylow de G y $N_G(Q) < H < G$, entonces $N_G(H) = H$.

ii) Si N es normal en G y Q es un p-subgrupo de Sylow de G, se tiene que :

a) $P \cap N$ es un p-subgrupo de Sylow de N.

b) PN/N es un p-subgrupo de Sylow de G/N.

Argumento de Frattini 45: Sea G un grupo finito, $N \triangleleft G$ y sea P un subgrupo de Sylow de N. Entonces $G = N_G(P)N$.

Demostración:

Para todo $x \in G$ tenemos que $x^{-1}Px < x^{-1}Nx = N$ y de aquí se sigue que $x^{-1}Px$ y P son subgrupos de Sylow de N, esto implica que existe

$z \in N$ tal que $x^{-1}Px = z^{-1}Pz$ de donde $P = zx^{-1}Pxz^{-1} = (xz^{-1})^{-1}P(xz^{-1})$, es decir, $n = xz^{-1} \in N_G(P)$ de donde obtenemos $x = nz \in N_G(P)N$ y por tanto $G < N_G(P)N$. De lo anterior concluimos que $G = N_G(P)N$ y la prueba está concluida■

Definición: Una *serie central* de G es una serie normal $H_1 = G > H_2 > \cdots > H_{r-1} > H_r > \ldots$ tal que para toda $i \geq 1$ $H_i/H_{i+1} < Z(G/H_{i+1})$.

Teorema 46: La serie normal $G = H_1 > H_2 > \ldots > H_r > \ldots$ es central si y sólo si $[G, H_i] < H_{i+1}$ para toda $i \geq 1$.

Demostración:

Inmediata■

Definición: Un grupo G es nilpotente si y solo si tiene una serie central que termine en $\langle 1 \rangle$.

Ejemplos:

Los grupos abelianos y los p-grupos finitos son nilpotentes.

Definiciónes: Sea G un grupo,

i) Sean $Z_1 = Z(G), \ldots, \frac{Z_{n+1}}{Z_n} = Z\left(\frac{G}{Z_n}\right)$ para toda $n \geq 1$. La cadena $Z_0 = \langle 1 \rangle \subset Z_1 \subset Z_2 \subset \ldots \subset Z_n \subset \ldots$ es llamada la *serie central ascendente* de G.

ii) Sean $G_1 = G, \ldots, G_{n+1} = [G_n, G]$ para toda $n \geq 1$. La cadena $G = G_1 \supset G_2 \supset \ldots \supset G_n \supset \ldots$ es llamada la *serie central descendente* de G.

Observación 1: Se prueba facilmente por inducción que $G_i \supset G_{i+1}$ para toda $i \geq 1$.

Observación 2: $G_2 = G'$, donde G' es el subgrupo derivado de G.

Observación 3: En virtud de la proposición 17 y el teorema 46, la serie central descendente es central.

Teorema 47: Sea G un grupo. Entonces las siguientes afirmaciones son equivalentes:

a) G es nilpotente.

b) La serie central descendente de G alcanza $\langle 1 \rangle$.

c) La serie central ascendente de G alcanza G.

Teorema 48: Las siguientes afirmaciones acerca de un grupo finito G son equivalentes:

a) G es nilpotente.

b) Ningun subgrupo propio de G es el normalizador de si mismo, i.e. si $H \lneqq G$, entonces $H \lneqq N_G(H)$.

c) Todo subgrupo de Sylow de G es normal en G.

d) G es producto directo de sus subgrupos de Sylow.

e) Todo subgrupo maximal de G es normal en G.

Teorema 49: Sea G un grupo finito nilpotente. Entonces todo subgrupo de G es nilpotente y si $N \lhd G,\ G/N$ es también nilpotente.

Teorema 50: Sea G un grupo y A, B subgrupos normales nilpotentes de G. Entonces AB también es nilpotente.

Teorema 51: Sean $G \neq \langle 1 \rangle$ un grupo finito nilpotente y $\langle 1 \rangle \neq N \lhd G$. Entonces $N \cap Z(G) \neq \langle 1 \rangle$. En particular $Z(G) \neq \langle 1 \rangle$, y si $|N| = p$, $N \subset Z(G)$.

CAPÍTULO 1
UNA CARACTERIZACIÓN DE LOS GRUPOS FINITOS SOLUBLES

El presente capítulo inicia enunciando el célebre p-q teorema de Burnside como preámbulo de un teorema de P. Hall, que se enuncia y demuestra. Posteriormente se presentan ejemplos que hacen ver la necesidad de la hipótesis de solubilidad en el teorema de Hall y por último se da un resultado que caracteriza a los grupos finitos solubles utilizando los dos resultados antes mencionados.

El primer resultado que demostraremos (usando un teorema que sólo enunciaremos) en esta sección es el clásico e importante

Teorema 1.1 (W. Burnside, 1904): Si G es un grupo finito de orden $p^a q^b$, con p y q primos, G es soluble.

Este resultado es conocido como el p-q Teorema de Burnside. La demostración original se basa en otro resultado clásico, también debido a él, que asegura que si un grupo finito G tiene una clase conjugada de orden p^m con p un primo y $m \geq 1$, G no es simple.

En la demostración de éste último teorema se usan métodos de la teoría de caracteres así como resultados sobre números algebraicos.

Demostración del p-q Teorema de Burnside:

Inducción sobre $a + b$:

Si $a + b = 1$, G es de orden primo y G es soluble.

Supongamos que $a + b \geq 2$ y que si H es un grupo de orden $p^r q^s$ con $r + s < a + b$, H es soluble.

Podemos suponer que G no es abeliano. Sea Q un q-subgrupo de

Sylow de G, si Q es de orden 1, G es un p-grupo y por lo tanto es soluble. Supongamos que $Q \neq \langle 1 \rangle$, se tiene que $Z(Q) \neq \langle 1 \rangle$ y consideremos $1 \neq g \in Z(Q)$, $Q < C_G(g)$.

$p^a = [G : Q] = [G : C_G(g)][C_G(g) : Q]$

$[G : C_G(g)] = p^m$ con $0 \leq m \leq a$. Si $[G : C_G(g)] = 1$, $G = C_G(g)$; lo que dice que $g \in Z(G)$ y $Z(G)$ es un subgrupo normal de G y G no es simple.

Si $[G : C_G(g)] = p^m$ con $m \geq 1$, G no es simple en virtud del teorema de Burnside citado anteriormente y también en este caso existe $1 \neq N \lhd G$ tal que $N \neq G$, como el orden de N y de G/N son de la forma $p^r q^s$ con $r + s < a + b$, N y G/N son solubles, lo que implica que G es soluble■

Hasta principios de la década de los setenta del siglo pasado no se conocía una demostración de este teorema que evitara el uso de caracteres de grupos. H. Bender [2] dio una demostración de este teorema en 1972 sin usar la teoría de caracteres.

Ahora enunciaremos y demostraremos un teorema de Philip Hall (1928) que generaliza el teorema de Sylow para grupos finitos solubles.

Teorema 1.2 (P. Hall): Sea G un grupo soluble de orden $l = mn$, con $(m, n) = 1$. Entonces:

a) G tiene subgrupos de orden m.

b) Si $M, K < G$ tales que $|M| = m$ y $|K|$ divide a m, entonces existe $x \in G$ tal que $K \subset x^{-1}Mx$

c) Si H_1, H_2 son subgrupos de G de orden m entonces existe $y \in G$ tal que $y^{-1}H_1y = H_2$

Demostración de a) y b):

Si l es primo entonces $m = 1$ o $n = 1$ y el teorema es trivial. Procedemos por inducción sobre el número de divisores primos de l.

Caso 1) Existe un subgrupo normal minimal U tal que $|U|$ divide a m.

Como G es soluble, $|U| = p^\alpha$ con p un primo ($p \mid m$), G/U es soluble y $|G/U| = \frac{m}{p^\alpha} n$, $\left(\frac{m}{p^\alpha}, n\right) = 1$. Por inducción G/U tiene un subgrupo M/U de orden $\frac{m}{p^\alpha}$ y M es un subgrupo de G de orden m y a) se cumple.

Ahora probemos b):

Sea $M < G$ de orden m y $K < G$ de orden m' que divide m. Como $U \lhd G$, $UM < G$, $|UM| = \frac{|U||M|}{|U \cap M|}$; ya que $(|M|, n) = (m, n) = 1$, $(|U|, n) = 1$. Si q es un primo que divide a $|UM|$ se sigue que $q \mid \frac{|M|}{|U \cap M|}$ o $q \mid |U|$, en cualquiera de los casos q no divide a n, y por consiguiente $(|MU|, n) = 1$ y como $|MU|$ divide a mn tenemos que $|MU|$ es divisor de m pero $M < MU$, lo que implica que $M = MU$ y $U < M$. Tenemos que $|M/U| = \frac{m}{p^\alpha}$ y que $|KU/U|$ divide a $\frac{m}{p^\alpha}$ ya que $KU/U < G/U$.

G/U es soluble $|G/U| = \frac{m}{p^\alpha} n$, $\left(\frac{m}{p^\alpha}, n\right) = 1$ por inducción existe $xU \in G/U$ tal que $KU/U \subset (xU)^{-1} M/U (xU) = x^{-1} U (M/U) xU$. Para todo $k \in K$, $kU = x^{-1} U y U x U = x^{-1} y x U$ con $y \in M$, por lo que $k = x^{-1} y x u_1 = x^{-1} y u_2 x = x^{-1} y_2 x$ de donde $K \subset x^{-1} M x$ y se cumple b).

Caso 2) No existen subgrupos normales minimales de G con orden divisor de m.

Sea $V \lhd_{\min} G$, $|V| = q^\beta$, para algun primo q que no divide a m, $q^\beta \mid n$. $|G/V| = \frac{|G|}{|V|} = m \frac{n}{q^\beta}$. Se distinguen dos casos:

Caso 2.1) $q^\beta < n$

Por inducción G/V tiene un subgrupo H/V de orden m, $|H| = m|V| = mq^\beta$. H es soluble, $|H| < |G|$, $|H| = mq^\beta$ $(m, q^\beta) = 1$.

Por inducción H tiene un subgrupo M de orden m y se cumple a).

Probamos que en este caso también se cumple b):

Sea M un subgrupo de G de orden m y K un subgrupo de G tal que el orden de K divide a m. $|MV/V| = m$, $|KV/V|$ divide a m y por inducción existe $xV \in G/V$ tal que $KV/V \subset x^{-1} V (MV/V) xV$. Para toda $k \in K$, $kV = x^{-1} V y V x V = x^{-1} y x V$, $k = x^{-1} y x v_1 = x^{-1} y v_2 x$ $(v_1, v_2 \in V, y \in M)$ lo que implica que $K \subset x^{-1} MV x$.

Ya que $|x^{-1} MV x| = |MV| = mq^\beta < t$ y como $x^{-1} M x < x^{-1} MV x$, por inducción se tiene que existe $y \in x^{-1} MV x$ tal que $K \subset y^{-1} (x^{-1} M x) y = (xy)^{-1} M x y$ y se cumple b)

Caso 2.2) $q^\beta = n$

Sea R/V un subgrupo normal minimal de G/V que es de orden $|R/V| = r^c$ con r un primo que divide a m, lo que implica que $r \neq q$. R es un subgrupo normal de G, $|R| = r^c q^\beta = r^c n$.

Sea S un r-subgrupo de Sylow de R, como $R \triangleleft G$, en virtud del argumento de Frattini $G = RN_G(S)$; como $V < R$ y $|V| = q^\beta$ y $|R| = r^c q^\beta$, se tiene $R = SV$ y por consiguiente $G = SVN_G(S) = VN_G(S)$ ya que $S \subset N_G(S)$.

$N_G(S) \lneqq G$ porque hemos supuesto que G no tiene subgrupos normales minimales de orden un divisor de m.

$mq^\beta = |G| = |V||N_G(S)|\frac{1}{|V \cap N_G(S)|}$; $\frac{|N_G(S)|}{|V \cap N_G(S)|} = m$, $|N_G(S)| = m|V \cap N_G(S)|$ $(m, |V \cap N_G(S)|) = 1$ y por inducción $N_G(S)$ tiene un subgrupo de orden m, así que se cumple a).

También en este caso probaremos que se cumple b) y tendremos completa la demostración de los incisos a) y b) del teorema.

Sean M y K subgrupos de G, M de orden m y K de orden un divisor de m. Demostremos que existe $t \in G$ tal que $K < t^{-1}Mt$. MR es un subgrupo de G porque $R \triangleleft G$. Siendo M un subgrupo de MR, el orden de M divide a $|MR|$, analogamente el orden de R divide a $|MR|$, lo que implica que q^β divide a $|MR|$ y siendo $(q^\beta, m) = 1$, entonces $q^\beta m = nm$ divide a $|MR|$ y se tiene que $G = MR$.

$|M \cap R| = \frac{|M||R|}{|G|} = \frac{r^c q^\beta m}{q^\beta m} = r^c$, lo que nos dice que $M \cap R$ es un r-subgrupo de Sylow de R y como $K \cap R$ es un r-subgrupo de R existe $y \in R$ tal que $K \cap R \subset y^{-1}(M \cap R)y$.

Ya que R es normal en G, $M \cap R$ es normal en M, luego $M < N_G(M \cap R)$ y $m \mid |N_G(M \cap R)|$. Además $N_G(M \cap R) \neq G$ porque G no tiene subgrupos normales minimales de orden un divisor de m.

$|N_G(M \cap R)| = mt$ y $mtk = |G| = mn$ de donde $n = tk$ lo que implica que $(m, t) = 1$. Por inducción el teorema se cumple en $N_G(M \cap R)$ y $y^{-1}N_G(M \cap R)y$.

Como $M < N_G(M \cap R)$, $y^{-1}My < y^{-1}N_G(M \cap R)y$; también se tiene que $K < N_G(K \cap R)$. Recordemos que $|K| \mid |M|$, si $|K| = |M|$ por un razonamiento análogo al de un parrafo anterior $KR = G$ y entonces $|K \cap R| = \frac{r^c q^\beta m}{q^\beta m} = r^c = |M \cap R|$ y como hemos visto que $K \cap R \subset y^{-1}(M \cap R)y$, tenemos que $K \cap R = y^{-1}(M \cap R)y$.

$K < N_G(K \cap R) = N_G(y^{-1}(M \cap R)y) = y^{-1}N_G(M \cap R)y$; sucede que $y^{-1}My \subset y^{-1}N_G(M \cap R)y$ y $|K| = m = |y^{-1}My|$, por inducción existe $z \in y^{-1}N_G(M \cap R)y$ tal que $K < z^{-1}y^{-1}Myz = (yz)^{-1}Myz$.

Supongase ahora que $|K| \lneqq |M|$. Entonces $KV \lneqq G$, $(|K|, |V|) = 1$ y

como $(KV)M = G$, se tiene que $|G| = \frac{|KV||M|}{|KV \cap M|} = \frac{|K||V||M|}{|KV \cap M|}$;
$|KV \cap M| = \frac{|K||V||M|}{|G|} = |K|$, $KV \cap M < KV$ de orden $|K|$, $K < KV$, por inducción existe $t \in KV$ tal que $K < t^{-1}(KV \cap M)t < t^{-1}Mt$

Demostración de c):

Como $|H_1|$ divide a $|H_2|$ y viceversa, entonces existe $y \in G$ que cumple $y^{-1}H_1y < H_2$, pero $|H_1| = |y^{-1}H_1y|$. Por tanto $|y^{-1}H_1y| = |H_2|$, es decir $y^{-1}H_1y = H_2$ ■

Observaciones:

La hipótesis de solubilidad del grupo G es una condición necesaria en las tres afirmaciones del teorema anterior:

En efecto, A_5 es un grupo no soluble de orden $60 = 4 * 15$ y no tiene subgrupos de orden 15.

A_5 es de orden $60 = 12 * 5$ y tiene un subgrupo H de orden 6 generado por (123) y $(12)(45)$ y H no está contenido en un subgrupo de orden 12 ya que los únicos subgrupos de A_5 de orden 12 son isomorfos a A_4 que no tiene subgrupos de orden 6. (Si H es un subgrupo de A_5 y $|H| = 12$, H no puede tener elementos de orden 6 y por lo tanto debe ser isomorfo a A_4).

Por último el grupo $GL(3,2) \cong SL(3,2) \cong PSL(3,2)$ es un grupo simple de orden $168 = 24 * 7$, y tiene subgrupos de orden 24 que no son conjugados [cfr [7, pp154]].

Recordemos la siguiente

Definición: Sea G un grupo finito, $H < G$. Se dice que H es un *subgrupo de Hall* de G si $(|H|, [G : H]) = 1$

Ejemplos:

i) Si G es un grupo finito y P es un p-subgrupo de Sylow de G, P es un subgrupo de Hall de G

ii) El subgrupo $S_5^{(5)}$ formado por los elementos de S_5 que dejan fijo al elemento 5, es un subgrupo de Hall de S_5 ya que $S_4 \simeq S_5^{(5)}$ es de orden 24 y $\left[S_5 : S_5^{(5)}\right] = 5$.

Definición: Si G es un grupo finito y $|G| = p^a m$ con p un primo tal que $p \nmid m$, un *p-complemento* de G es un subgrupo C de G de orden m.

Sean G un grupo y p un primo, un p-complemento C de G es un

subgrupo de Hall de G ya que $([G : C], |C|) = 1$.

Inversamente, si H es un subgrupo de Hall de G con $[G : H] = p^t$ con $t \geq 1$, se tiene que $p \nmid |H|$ y como $|G| = |H|[G : H] = |H|p^t = mp^a$, se tiene que $p^a = p^t$, $|H| = m$ y por consiguiente H es un p-complemento de G.

Proposición 1.3 : Si S es un p-subgrupo de Sylow de un grupo finito G y H es un p-complemento de G, entonces $SH = G$, $S \cap H = \langle 1 \rangle$.

Demostración:

$|G| = p^a m$, p un primo que no divide a m. $|S| = p^a$, $|H| = m$. Tenemos que $S \cap H < S$ y $|S \cap H| = p^r$ con $0 \leq r \leq a$, además $S \cap H < H$ por lo que $p^r \mid m$ pero $p \nmid m$ por lo tanto $r = 0$ y se tiene que $S \cap H = \langle 1 \rangle$.

$|SH| = \frac{|S||H|}{|S \cap H|} = |S||H| = p^a m = |G|$ por lo que $G = SH$■

Teorema 1.4 : Si G es un grupo finito de orden $g = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$ con $p_1, p_2, \ldots, p_r$ primos diferentes, las siguientes tres afirmaciones son equivalentes:

a) G es soluble

b) si $|G| = mn$ con $(m, n) = 1$, G tiene un subgrupo de orden m.

c) G tiene un p_i-complemento para cada $i = 1, 2, \ldots, r$

Demostración:

a) implica b) es parte del teorema 1.1

b) implica c) es inmediata

c) implica a):

Supongamos que existen grupos finitos que tienen p-complemento para cada primo p que divide al orden del grupo y que no son solubles. De estos grupos escojamos uno de orden mínimo y lo llamamos G.

Demostraremos que existe $\langle 1 \rangle \neq M \lhd G$ tal que M y G/M son solubles, lo que implicará que G es soluble, obteniendo de ahí una contradicción.

Si $|G| = g = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$ con $p_1, p_2, \ldots, p_r$ primos diferentes, por el p-q teorema de Burnside se tiene que $r > 2$. Probaremos primero que si C_i es un p_i-complemento de G con $1 \leq i \leq r$ es decir si $C_i < G$,

$|C_i| = gp_i^{-a_i}$, C_i tiene p_j-complemento para toda $1 \leq j \leq r,\ j \neq i$ y como G es un contraejemplo de orden mínimo, C_i es soluble.

Si $1 \leq j \leq r$ y C_j es un p_j-complemento de G, $C_i \cap C_j$ es un p_j-complemento de C_i, en efecto, $|C_iC_j| = \frac{|C_i||C_j|}{|C_i \cap C_j|}$ lo cual implica que tanto $|C_i| = gp_i^{-a_i}$ como $|C_j| = gp_j^{-a_j}$ son divisores de $|C_iC_j|$ de ahí que $|C_i|$ y $p_i^{a_i}$ son divisores de $|C_iC_j|$, por lo que $C_iC_j = G$.

$|G| = \frac{|C_i||C_j|}{|C_i \cap C_j|}$, $|C_i \cap C_j| = \frac{gp_i^{-a_i}gp_j^{-a_j}}{g} = gp_i^{-a_i}p_j^{-a_j}$ lo que nos dice que $C_i \cap C_j$ es un p_j-complemento de C_i. Se tiene pues que C_i es soluble, en particular C_1 es soluble.

Sea N un subgrupo normal minimal de C_1, $|N| = p_i^{t_t}$ para algun primo p_i, $1 < i \leq r$.

Sea S_i un p_i-subgrupo de Sylow de C_1 conteniendo a N, $|S_i| = p_i^{a_i}$. Sean $1 < j \leq r$ con $j \neq i$ (tal j existe porque r>2) y C_j un p_j-complemento de G i.e. $C_j < G$ y $|C_j| = gp_j^{-a_j}$; si Q es un p_i-subgrupo de Sylow de C_j y por consiguiente de G, para alguna $x \in G$, $S_i = x^{-1}Qx \subset x^{-1}C_jx = \bar{C}j$, es decir S_i está contenido en un p_j-complemento de C_j conjugado en G.

Como $N < S_i < C_1$, $N < C_1 \cap \bar{C}_j$ y habíamos visto que $G = C_1\ \bar{C}_j$, si $h \in G\ h = kl$ con $k \in C_1$ y $l \in \bar{C}_j$ y tenemos $h^{-1}Nh = l^{-1}k^{-1}Nkl = l^{-1}Nl \subset l^{-1}S_il \subset \bar{C}_j$ es decir, $\bar{C}_j$ contiene a todo subgrupo conjugado de N y por consiguiente a la cerradura normal de N en G, que llamaremos M. Se tiene que $M \triangleleft G$ y $M < \bar{C}j$. Como $\bar{C}j$ es soluble, M es soluble.

Demostraremos ahora que G/M es soluble:

Como $|G/M|$ divide a $|G|$ y $|G/M| < |G|$ si hacemos ver que para cada t con $1 \leq t \leq r$, G/M tiene un p_t-complemento, se tendrá que G/M es soluble, ya que G es un contraejemplo de orden mínimo.

Haremos notar que si C_t es un p_t-complemento de G, C_tM/M es un p_t-complemento de G/M.

$|G/M| = |C_tM/M|[G/M : C_tM/M] = |C_tM/M|[G : C_tM]$

$p_t^{a_t} = [G : C_t] = [G : C_tM][C_tM : C_t]$

lo que implica que $[G/M : C_tM/M] = p_t^{b_t}$. Por otro lado $C_tM/M \simeq C_t/(M \cap C_t)$ por lo tanto p_t no divide a $|C_tM/M|$. Y si $|C_tM/M| = c$, $|G/M| = cp_t^{b_t}$ y C_tM/M es un p_t-complemento de G/M y G/M es soluble.

CAPÍTULO 2

TEOREMAS DE CARTER

En este capítulo son presentados dos de los teoremas de Carter (que guardan una gran similitud con los teoremas de Sylow). Se dan algunos ejemplos de estos subgrupos y en la última proposición se demuestra que la solubilidad no es una condición necesaria para que en un grupo finito existan los subgrupos de Carter.

Teorema 2.1 : Sea G un grupo finito soluble, H un subgrupo de Hall de G, y K un subgrupo de G que contiene a $N_G(H)$. Entonces $N_G(K) = K$.

Demostración:

Sea $g \in N_G(K)$. Por demostrar que $g \in K$. Entonces: $g^{-1}Hg \subset g^{-1}Kg = K$ y $H \subset N_G(H) \subset K$ y $(|H|, [G : H]) = 1$ implica que $(|H|, [K : H]) = 1$ ya que $[G : H] = [G : K][K : H]$ es decir, H y $g^{-1}Hg$ son subgrupos de Hall de K.

Pero K es soluble, entonces por el teorema 1.2 H y $g^{-1}Hg$ son conjugados en K, es decir, existe $k \in K$ tal que $H = k^{-1}g^{-1}Hgk$. Entonces $gk \in N_G(H) \subset K$; pero $k \in K$, entonces $g \in K$ y por tanto $N_G(K) = K$■

Definición: Sea G un grupo finito. Un subgrupo H de G es llamado un *subgrupo de Carter* si H es nilpotente y $N_G(H) = H$.

Ejemplos de subgrupos de Carter:

i) Si G es nilpotente y finito, G es su único subgrupo de Carter.

G es de Carter por ser nilpotente y $N_G(G) = G$. Supongamos que H es un subgrupo propio de G, como G es nilpotente $H \subsetneq N_G(H)$ y por

tanto H no es subgrupo de Carter de G.

ii) Si G es un grupo no trivial i.e. $G \neq \langle 1 \rangle$, el subgrupo $\langle 1 \rangle$ no es subgrupo de Carter de G porque $N_G(\langle 1 \rangle) = G$.

iii) Consideremos $G = S_3$. Si H es un subgrupo de G de orden 2, H es nilpotente, y es conocido que H no es normal en G i.e. $N_G(H) \lneqq G,\ H < N_G(H) \lneqq G$, como $N_G(H)$ es de orden múltiplo de 2 y divisor de 6 (sin poder ser 6) entonces $N_G(H) = H$. Esto impica que H es un subgrupo de Carter de G. Si K es un subgrupo de G no trivial y no es de orden 2, K es de orden 3, por consiguiente K es normal en G y K no es subgrupo de Carter de G; por tanto los únicos subgrupos de Carter de G son sus 2-subgrupos de Sylow.

iv) Ahora veremos que S_4 tiene subgrupos de Carter:

Los subgrupos de S_4 son $\langle 1 \rangle, C_2, C_3 \simeq A_3, C_4, V, S_3, D_{2(4)}, A_4, S_4$. Como ya es sabido $\langle 1 \rangle$ no es de Carter, S_3, A_4, S_4 no son nilpotentes por que tienen centro trivial y por tanto no son de Carter.

Los subgrupos de orden 2 y 4 son subgrupos de un 2-subgrupo de Sylow de orden 8 que es nilpotente y en los grupos nilpotentes tenemos que si $H \lneqq G$, $H \subsetneqq N_G(H)$ por tanto los subgrupos de orden 2 y 4 no son de Carter.

Para el caso de C_3 tenemos que $C_3 = \langle abc \rangle$ y $C_3 < \langle (abc)(ab) \rangle = N \simeq S_3$, y como $C_3 \lhd N$ tenemos que C_3 no es subgrupo de Carter de S_4.

$D_{2(4)}$ es un 2-subgrupo de Sylow de S_4 y por tanto es nilpotente y S_4 tiene tres 2-subgrupos de Sylow, así que $3 = [S_4 : D_{2(4)}] = [S_4 : N_{S_4}(D_{2(4)})][N_{S_4}(D_{2(4)}) : D_{2(4)}] = 3 * [N_{S_4}(D_{2(4)}) : D_{2(4)}]$ por que $[S_4 : N_{S_4}(D_{2(4)})]$ es el número de 2-subgrupos de Sylow de S_4 y por tanto $N_{S_4}(D_{2(4)}) = D_{2(4)}$, es decir $D_{2(4)}$ es un subgrupo de Carter de S_4. En conclusión S_4 tiene subgrupos de Carter y todos son conjugados.

v) Ahora veremos cómo son los subgrupos de Carter de A_4:

Los subgrupos de A_4 son $\langle 1 \rangle$, los grupos de orden 2 formados por $\langle 1 \rangle$ y una permutación de la forma $(ab)(cd)$, los subgrupos de orden 3 generados por un 3-ciclo, el subgrupo de orden 4 isomorfo al 4-grupo de Klein y A_4.

El 2-subgrupo de Sylow de A_4 (de orden 4) es normal, y por tanto no es de Carter. Los subgrupos de orden 2 son subgrupos normales del 2-subgrupo de Sylow de A_4 y no son de Carter.

A_4 no es nilpotente por tanto no es subgrupo de Carter de si mismo.

Los subgrupos de orden 3 son los 3-subgrupos de Sylow de S_4 y existen 4 de ellos, sea P un 3-subgrupo de Sylow de A_4 tenemos que $[A_4 : N_{A_4}(P)][N_{A_4}(P) : P] = [A_4 : P] = 4$ y como $[A_4 : N_{A_4}(P)] = 4$, $P = N_{A_4}(P)$ y por tanto P es subgrupo de Carter de A_4.

Observación:

Si S es un subgrupo de Carter de G, S es maximal en la clase de los subgrupos nilpotentes de G pero no todo subgrupo maximal en la clase de los subgrupos nilpotentes de G es subgrupo de Carter.

Teorema 2.2 (Primer teorema de Carter): Todo grupo finito soluble tiene un subgrupo de Carter.

Demostración:

Usando inducción sobre el orden de G, si H es subgrupo de G tal que $|H| \lneqq |G|$ entonces H tiene un subgrupo de Carter. Sea N un subgrupo minimal normal de G; entonces $|N| = p^r$ (con p un primo y $r \geq 1$). G/N tiene un subgrupo de Carter, digamos K/N, que, al ser nilpotente, su p-subgrupo de Sylow S/N es normal en K/N. Como N es un p-grupo, S también es un p-grupo, entonces un p-subgrupo de Sylow de K. Además S es normal en K porque S/N es normal en K/N. El subgrupo K, al ser soluble, por el teorema 1.2, tiene un p-complemento, al que llamaremos R. Sea H el normalizador de R en K. Ahora demostremos que H es un subgrupo de Carter de G.

Como $K = SR$ (porque S es un p-subgrupo de Sylow de K y R es un p-complemento de K) y S es normal en K, por la relación de Dedekind obtenemos que $H = H \cap K$ (porque $H \subset K$) entonces $H = H \cap K = H \cap SR = R(H \cap S)$.

Pero R es normal en H; además $H \cap S$ es normal en H por que S es normal en K. Como $R \cap (H \cap S) \subset R \cap S = \langle 1 \rangle$ (porque S es p-subgrupo de Sylow de K y R es p-complemento de K), se sigue que $H = R \times (H \cap S)$. Pero R es isomorfo a K/S porque $K/S = SR/S$. Por el tercer teorema de isomorfismo se tiene que $SR/S \simeq R/S \cap R = R/\langle 1 \rangle = R$. Además K/S es imagen homomorfa del grupo nilpotente K/N. Por tanto R es nilpotente. También $H \cap S$ es nilpotente, porque S es un p-grupo. Se sigue que $H = R \times (H \cap S)$ es nilpotente (porque además ambos son normales en H).

Demostremos ahora que $N_G(H) = H$. Como H es el normalizador en K de R (subgrupo de Hall de K), y NH es un subgrupo de K que

contiene a H, por el teorema 4.1, $N_K(NH) = NH$, y esto implica que $N_{K/N}(NH/N) = NH/N$. Además K/N es nilpotente, entonces, si $NH/N \subsetneq K/N$ se tendría que $NH/N \subsetneq N_{K/N}(NH/N)$, lo cual es una contradicción. Por tanto $NH/N = K/N$, es decir $NH = K$.

Ahora sea $z \in N_G(H)$ y por demostrar que $z \in K$. Entonces, como N es normal en G tenemos que $z^{-1}NHz = z^{-1}Nzz^{-1}Hz = NH = K$ y así $z \in N_G(K)$ y $zN \in N_{G/N}(K/N)$; pero $N_{G/N}(K/N) = K/N$. Por tanto $zN \in K/N$, es decir $z \in K$. Como $z \in N_G(H)$, se sigue que $z \in N_K(H)$. Además como H es el normalizador de R (subgrupo de Hall de K), por el teorema 4.1 $N_K(H) = H$. Esto implica que $z \in H$, es decir $N_G(H) = H$, y H es un subgrupo de Carter de G■

Teorema 2.3 (Segundo Teorema de Carter): Sea G un grupo finito soluble. Entonces:

a) Si H es un subgrupo de Carter de G y K es un subgrupo de G que contiene a H, entonces $N_G(K) = K$.

b) Si H es un subgrupo de Carter de G y N es un subgrupo normal de G, entonces NH/N es un subgrupo de Carter de G/N

c) Si H_1, H_2 son subgrupos de Carter de G, entonces existe $g \in G$ tal que $g^{-1}H_1g = H_2$.

Nótese la similitud existente entre los teoremas de Sylow y este teorema.

Demostración:

Si G es nilpotente, G es el único subgrupo de Carter de G y el teorema se cumple trivialmente. Usamos inducción sobre el orden de G, es decir, si A es subgrupo de G y $|A| \lneq |G|$ entonces el teorema se cumple en A.

Primero probemos a). Si $K = G$, el teorema se cumple; por tanto podemos suponer que $K \neq G$. Por demostrar que $N_G(K) \subset K$. Sea $x \in N_G(K)$, entonces $x^{-1}Hx \subset x^{-1}Kx = K$.

$x^{-1}Hx$ es subgrupo de Carter porque al ser isomorfo a H, es nilpotente y $N_K(x^{-1}Hx) = x^{-1}N_K(H)x = x^{-1}Hx$

Entonces, por inducción (como $K \neq G$) tenemos que existe $k \in K$ tal que $k^{-1}(x^{-1}Hx)k = H$. Entonces $xk \in N_G(H) = H \subset K$, y como $k \in K$, también $x \in K$. Esto implica que $N_G(K) = K$ y a) está probado.

Probemos b). Sea N un subgrupo normal de G. Como H es nilpotente, también HN/N lo es porque N es normal en HN y

$HN/N \simeq H/(H \cap N)$ que es nilpotente por que H lo es. Sea $xN \in N_{G/N}(HN/N)$ y $a \in HN$.

Tenemos que $(xN)^{-1}(aN)(xN) = x^{-1}axN$ y así $x^{-1}HNx = HN$; es decir $x \in N_G(HN)$ pero $H \subset HN$, entonces por el inciso a), $N_G(HN) = HN$. De ahí $x \in HN$ y $xN \in HN/N$ y por tanto $N_{G/N}(HN/N) = HN/N$.

De lo anterior podemos concluir que HN/N es un subgrupo de Carter de G/N, es decir b) fue probado.

Ahora probamos c). Sea N un subgrupo normal minimal de G. Entonces, por b), si H_1, H_2 son subgrupos de Carter de G tenemos que H_1N/N y H_2N/N son subgrupos de Carter de G/N; entonces, por inducción, existe $xN \in G/N$ tal que $(xN)^{-1}(H_1N/N)(xN) = H_2N/N$, es decir $x^{-1}H_1Nx = H_2N$. Se sigue que $x^{-1}H_1x \subset H_2N$ por que $H_1 \subset H_1N$, entonces $x^{-1}H_1x \subset x^{-1}H_1Nx = H_2N$

De lo anterior tenemos que $x^{-1}H_1x$ y H_2 son subgrupos de Carter de H_2N. Si $H_2N \neq G$, por indución, existe $y \in H_2N$ tal que $y^{-1}x^{-1}H_1xy = H_2$ y c) está probado. Por tanto podemos suponer que $G = H_2N$. Denotando $x^{-1}H_1x = H_3$, tenemos que $H_3N = H_2N = G$.

El subgrupo $N \cap H_2$ es normal en N, porque sabemos que $N \lhd_{\min} G$ y además G es soluble, entonces N es abeliano.

Pero $N \cap H_2$ también es normal en H_2, porque N es normal en G; por tanto $N \cap H_2$ es normal en $H_2N = G$. Como $N \cap H_2 \subset N$ y N es normal minimal, tenemos que $N \cap H_2 = N$ ó $N \cap H_2 = \langle 1 \rangle$. Si $N \cap H_2 = N$, entonces $N \subset H_2$, es decir $G = H_2$, G es nilpotente, y c) está probada. Por tanto podemos suponer que $N \cap H_2 = N \cap H_3 = \langle 1 \rangle$.

Sea p^r (p un primo y $r \geq 1$) el orden de N. El subgrupo $H_2(H_3)$, al ser nilpotente tiene un único p-complemento $R_2(R_3)$ por que si L es un p-complemento y q es un primo tal que $p \neq q$ y q divide a $|H_2(H_3)|$, podemos tomar L_q un q-subgrupo de Sylow de L y R_q un q-subgrupo de Sylow de $R_2(R_3)$ y observar que L_q y R_q son q-subgrupos de Sylow del grupo nilpotente $H_2(H_3)$, así que $L_q = R_q$. Basta ahora notar que L y $R_2(R_3)$ son nilpotentes por ser subgrupos de $H_2(H_3)$, por lo que cada uno de ellos es producto directo de sus subgrupos de Sylow, y entonces, como $|L| = |R_2(R_3)|$, tenemos que $L = R_2(R_3)$.

Ahora verifiquemos que $[G : R_2]$ y $[G : R_3]$ son potencia de p:

Tenemos que $[G : R_2] = [H_2N : H_2][H_2 : R_2] = |H_2N|/|R_2| = (|H_2|/|R_2|)|N|$ y eso es potencia de p porque R_2 es p-complemento de H_2. Análogamente

$[G : R_3]$ es potencia de p.

Por tanto, como $|G| = |H_2(H_3)||N|$, y $[G : R_2]$, $[G : R_3]$ son potencia de p, entonces R_2 y R_3 son p-complementos de G. Por tanto, por el teorema 1.2, existe $z \in G$ tal que $z^{-1}R_3z = R_2$. Se sigue que R_2 es normal en H_2 y en $z^{-1}H_3z$ porque $R_2 = z^{-1}R_3z \subset z^{-1}H_3z$. En efecto sea $x \in z^{-1}H_3z$; esto implica que $x^{-1}(R_2)x = x^{-1}(z^{-1}R_3z)x$; pero $x = z^{-1}yz$, con $y \in H_3$, entonces $x^{-1}(R_2)x = x^{-1}(z^{-1}R_3z)x = (z^{-1}yz)^{-1}(z^{-1}R_3z)(z^{-1}yz) = z^{-1}y^{-1}R_3yz$. Además $z^{-1}y^{-1}R_3yz = z^{-1}R_3z = R_2$ porque R_3 es normal en H_3 y $y \in H_3$; por tanto R_2 es normal en $z^{-1}H_3z$.

Entonces, como R_2 es nomal en H_2 y en $z^{-1}H_3z$, también lo es en $U = \langle H_2, z^{-1}H_3z \rangle$.

Pero H_2 es subgrupo de Carter de G, entonces lo es de U porque es nilpotente y $N_G(H_2) = H_2 \subset N_U(H_2) \subset N_G(H_2)$, por lo que $N_U(H_2) = H_2$; de donde H_2 es subgrupo de Carter de U.

Por tanto, por b), H_2/R_2 es subgrupo de Carter de U/R_2. Pero U/R_2 es p-subgrupo porque R_2 es p-complemento de G.

Entonces U/R_2 es un p-grupo, entonces es nilpotente, y esto implica que es el único subgrupo de Carter de si mismo. Por tanto $H_2/R_2 = U/R_2$, es decir $U = H_2$ y así $H_2 = z^{-1}H_3z = z^{-1}x^{-1}H_1zx$. Esto implica que c) está probado■

Dado que en un grupo finito soluble, existen subgrupos de Carter, es natural preguntarse si la solubilidad en una condición necesaria.

El grupo alternante con 5 objetos A_5 es el grupo no soluble de orden menor. ¿A_5 tiene subgrupos de Carter?

A_5 es un grupo simple y no tiene subgrupos de orden 15, 20 o 30; por lo que los posibles órdenes de subgrupos no triviales de A_5 son 2, 3, 4, 5, 6, 10 y 12.

A_5 no tiene elementos de orden 10, por lo que los únicos subgrupos de orden 10 son isomorfos al diédrico $D_{2(5)}$, que no es nilpotente porque su centro es trivial. Por lo tanto, A_5 no tiene subgrupos de Carter de orden 10.

Es conocido que si G es un grupo de orden 12 y no es isomorfo al grupo alternante de 4 elementos A_4 tiene un elemento de orden 6 pero A_5 no tiene elementos de orden 6, se tiene que si H es un subgrupo de A_5 de orden 12 H es isomorfo a A_4 que no es nilpotente por tener centro trivial, por tanto A_5 no tiene subgrupos de

Carter de orden 12.

Como A_5 no tiene elementos de orden 6, si H es un subgrupo de orden 6, H es isomorfo a S_3 que no es nilpotente por tener centro trivial, por lo que A_5 no tiene subgrupos de Carter de orden 6.

Si H es un subgrupo de A_5 de orden 5, H está generado por un 5-ciclo $(abcde) = \alpha$, si $\beta = (be)(cd)$ y $K = \langle \alpha, \beta \rangle$ es un subgrupo isomorfo a $D_{2(5)}$ de orden 10, por lo que $H \lhd K$, lo que implica que $H \lneqq N_{A_5}(H)$ y H no es subgrupo de Carter de A_5.

Si H es un subgrupo de A_5 de orden 3, H está generado por un 3-ciclo $\alpha = (abc)$. Si $\beta = (ab)(de)$ con $d, e \notin \{a, b, c\}$, $K = \langle \alpha, \beta \rangle$ es un subgrupo isomorfo a S_3 de orden 6, por lo que $H \lhd K$ y $H \neq N_{A_5}(H)$. Y H no es subgrupo de Carter de A_5.

Si H es un subgrupo de A_5 de orden 2, H está contenido en un subgrupo K de orden 4, H es normal en K y $N_{A_5}(H) > K > H$ y por consiguiente H no es subgrupo de Carter de A_5.

Por último si H es subgrupo de A_5 de orden 4, $H = \{(1), (ab)(cd), (ac)(bd), (ad)(bc)\}$ con $a, b, c, d \in \{1, 2, 3, 4, 5\}$, H es un subgrupo del subgrupo $A_5^{(e)} \simeq A_4$ que consiste en todas las permutaciones pares de S_5 que dejan fijo al objeto e, se tiene que $H \lhd A_5^{(e)}$ y $H \lneqq N_{A_5}(H)$ por lo que H no es subgrupo de Carter de A_5. Concluimos que A_5 no tiene subgrupos de Carter■

S_5 no es soluble porque A_5 tampoco lo es. Veamos que S_5 sí tiene subgrupos de Carter demostrando el siguiente resultado.

Proposición 2.4 : Si P es un 2-subgrupo de Sylow de S_5, P es un subgrupo de Carter de S_5.

Demostración:

Si r es el número de 2-subgrupos de Sylow de S_5 $r \equiv 1 (\mathrm{mod}\, 2)$ y $r = [S_5 : N_{S_5}(P)]$.

Como $[S_5 : N_{S_5}(P)][N_{S_5}(P) : P] = [S_5 : P] = \frac{120}{8} = 15$, entonces $r = 1, 3, 5$ o 15. Tenemos que $r \neq 1$ porque P no es normal en S_5 (es conocido que el único subgrupo normal no trivial de S_5 es A_5). Haremos ver que $r > 5$ lo que implicará que $r = 15$.

Si $r = 15$ tenemos que $[N_{S_5}(P) : P] = 1$ lo que implica que $P = N_{S_5}(P)$ y siendo P un 2-subgrupo, es nilpotente y por consiguiente es subgrupo de Carter de S_5.

Demostremos pues que $r > 5$.

Para cada $1 \leq i \leq 5$ tenemos que $S_5^{(i)}$ es un subgrupo de S_5 isomorfo a S_4. Como $|S_4| = 2^3 * 3$ y $|S_5| = 2^3 * 3 * 5$ cada 2-subgrupo de Sylow de $S_5^{(i)}$ es subgrupo de Sylow de S_5.

Si t es el número de 2-subgrupos de Sylow de S_4, $t \equiv 1(\mathrm{mod}\, 2)$ y $t \mid 3$ por lo tanto $t = 1$ o $t = 3$, pero $t \neq 1$ porque si $t = 1$ y Q es el 2-subgrupo de Sylow de S_4, Q sería normal en S_4 pero los únicos subgrupos normales no triviales de S_4 son A_4 y el grupo de Klein V, por tanto $t = 3$.

Hemos visto que por cada $1 \leq i \leq 5$, $S_5^{(i)}$ tiene tres 2-subgrupos de Sylow y por consiguiente S_5 también.

Si Q es un 2-subgrupo de Syow de $S_5^{(j)}$ con $1 \leq j \leq 5$ con $j \neq i$, Q no es 2-subgrupo de Sylow de $S_5^{(i)}$, en efecto, supongase que $Q \subset S_5^{(i)}$, entonces $Q \subset S_5^{(i)} \cap S_5^{(j)}$ lo que implica que $\left|S_5^{(i)} \cap S_5^{(j)}\right| \geq 8$.

Por otro lado $S_5^{(i)} \cap S_5^{(j)} = \left\{\alpha \in S_5 \mid \alpha(i) = i\,,\, \alpha(j) = j\right\}$ es isomorfo al grupo simétrico S_3. Bajo el supuesto de que $Q \subset S_5^{(i)}$ se tiene que $6 = \left|S_5^{(i)} \cap S_5^{(j)}\right| \geq 8$ lo que es una contradicción. Por lo tanto S_5 tiene al menos seis 2-subgrupos de Sylow (los 3 de $S_5^{(i)}$ y los 3 de $S_5^{(j)}$ y por consiguiente $r = 15$■

CAPÍTULO 3

TEOREMA DE SCHUR-ZASSENHAUS

En este tercer capítulo se enuncia y demuestra el teorema de Schur-Zassenhaus, que es uno de los más representativos en el estudio de los grupos finitos, ya que uno de los principales problemas ha sido el de encontrar complementos en estos grupos y ése es precisamente el objeto de este teorema.

Sea G un grupo finito, N un subgrupo normal y abeliano de G, y sea $G/N = H$. Para cada elemento $h_i \in H$ fijamos un representante $r(h_i)$ de la clase lateral h_i de N en G. Para cada $h_i, h_j \in H$ tenemos:

$$r(h_i)r(h_j) = r(h_ih_j)c(h_i, h_j)$$

con $c(h_i, h_j) \in N$. Como N es abeliano, todos los elementos pertenecientes a una clase lateral dada h_j de N en G inducen el mismo automorfismo en N. Si $c \in N$, denotamos por c^{h_i} a la imagen de c bajo ese automorfismo.

En particular $c^{h_i} = (r(h_i))^{-1}cr(h_i)$.

Ahora probamos que si $h_i, h_j, h_k \in H$, entonces

(1)

$$c(h_ih_j, h_k)[c(h_i, h_j)]^{h_k} = c(h_i, h_jh_k)c(h_j, h_k).$$

Sabemos que $[r(h_i)r(h_j)]r(h_k) = r(h_ih_j)c(h_i, h_j)r(h_k)$; ahora $[c(h_i, h_j)]^{h_k} = (r(h_k))^{-1}c(h_i, h_j)r(h_k)$, entonces $r(h_k)[c(h_i, h_j)]^{h_k} = c(h_i, h_j)r(h_k)$ y sustituyendo tenemos que $r(h_ih_j)c(h_i, h_j)r(h_k) = r(h_ih_j)r(h_k)[c(h_i, h_j)]^{h_k} = r(h_ih_jh_k)c(h_ih_j, h_k)[c(h_i, h_j)]^{h_k}$.

Por otro lado $r(h_i)[r(h_j)r(h_k)] = r(h_i)r(h_jh_k)c(h_j, h_k) = r(h_ih_jh_k)c(h_i, h_jh_k)c(h_j, h_k)$ y como $[r(h_i)r(h_j)]r(h_k) = r(h_i)[r(h_j)r(h_k)]$ tenemos que $r(h_ih_jh_k)c(h_ih_j, h_k)[c(h_i, h_j)]^{h_k} = r(h_ih_jh_k)c(h_i, h_jh_k)c(h_j, h_k)$. Por tanto $c(h_ih_j, h_k)[c(h_i, h_j)]^{h_k} = c(h_i, h_jh_k)c(h_j, h_k)$ y (1) está

demostrado■

Definición: Sea G es un grupo y $H < G$. Un *complemento* de H en G es un subgrupo C tal que $G = HC$ y $H \cap C = \langle 1 \rangle$.

Teorema 3.1 : Sea G un grupo finito y N un subgrupo de Hall de G normal y abeliano. Entonces existe, en G, al menos un complemento de N, y los complementos de N en G son conjugados en G.

Demostración:

Sea $G/N = H$. Como N es un subgrupo de Hall de G, tenemos que $(|N|, |H|) = 1$ porque $|H| = [G : N]$, y así existe $z \in \mathbb{Z}$ tal que $|H|z \equiv 1 \pmod{|N|}$. Llamemos m al orden de H y denotemos por $h_1, \ldots, h_m$ los elementos de H, escribimos para toda $h_i \in H$

(2)

$$c(h_i) = \Pi_{t=1}^{m}[c(h_t, h_i)]^{-z}$$

Mostremos que el conjunto $C = \{r(h_i)c(h_i) \mid i = 1, \ldots, m\}$ es un complemento de N en G. En primer lugar, en una clase lateral dada h_i de N en G hay un sólo un elemento de C, es decir $r(h_i)c(h_i)$, y así, ya que veamos que $C < G$, tendriamos que $N \cap C = \langle 1 \rangle$ y que $NC = G$, . Por tanto es suficiente probar que C es subgrupo de G, o como G es finito, que, si $h_i, h_j \in H$,

$$r(h_i)c(h_i)r(h_j)c(h_j) = r(h_ih_j)c(h_ih_j).$$

Como N es abeliano, tenemos que $[c(h_i)]^{h_j} = (r(h_j))^{-1}c(h_i)r(h_j)$, es decir $r(h_j)[c(h_i)]^{h_j} = c(h_i)r(h_j)$; además sabemos que $r(h_i)c(h_i)r(h_j)c(h_j) = r(h_i)r(h_j)[c(h_i)]^{h_j}c(h_j)$, pero $r(h_i)r(h_j) = r(h_ih_j)c(h_i, h_j)$ por tanto $r(h_i)c(h_i)r(h_j)c(h_j) = r(h_ih_j)c(h_i, h_j)[c(h_i)]^{h_j}c(h_j)$.

De aquí bastará probar que:

(3)

$$c(h_ih_j) = c(h_i, h_j)[c(h_i)]^{h_j}c(h_j)$$

De (1), como N es abeliano, se sigue que $\Pi_{i=1}^{m}c(h_ih_j, h_k)[\Pi_{i=1}^{m}c(h_i, h_j)]^{h_k} = \Pi_{i=1}^{m}\left(c(h_ih_j, h_k)[c(h_i, h_j)]^{h_k}\right)$ ya que c^{h_k} es imagen de c bajo un automorfismo, es decir $[\Pi_{i=1}^{m}c(h_i, h_j)]^{h_k} = \Pi_{i=1}^{m}\left[c(h_i, h_j)^{h_k}\right]$, entonces $\Pi_{i=1}^{m}\left\{c(h_ih_j, h_k)[c(h_i, h_j)]^{h_k}\right\} = \Pi_{i=1}^{m}[c(h_i, h_jh_k)c(h_j, h_k)]$. Pero $\Pi_{i=1}^{m}[c(h_i, h_jh_k)c(h_j, h_k)] = [\Pi_{i=1}^{m}c(h_i, h_jh_k)][c(h_j, h_k)]^m$; por tanto $\Pi_{i=1}^{m}c(h_ih_j, h_k)[\Pi_{i=1}^{m}c(h_i, h_j)]^{h_k} = \Pi_{i=1}^{m}c(h_i, h_jh_k)[c(h_j, h_k)]^m$

Elevando ambos lados de la igualdad a la z-ésima potencia tenemos

que

$[\prod_{t=1}^{m} c(h_t, h_k)]^z \left[\prod_{t=1}^{m} (c(h_t, h_j))^{h_k}\right]^z = [\prod_{t=1}^{m} c(h_t, h_j h_k)]^z [c(h_j, h_k)]^{mz}$; pero $mz \equiv 1 \left(\mathrm{mod}\ |N|\right)$,
por tanto $[\prod_{t=1}^{m} c(h_t, h_k)]^z \left[\prod_{t=1}^{m} (c(h_t, h_j))^{h_k}\right]^z = [\prod_{t=1}^{m} c(h_t, h_j h_k)]^z c(h_j, h_k)$.

Esto es, de acuerdo con (2),
$[c(h_k)]^{-1}\left[(c(h_j))^{-1}\right]^{h_k} = [c(h_j h_k)]^{-1} c(h_j, h_k)$ o equivalentemente:
$c(h_j h_k) = c(h_j, h_k)[c(h_j)]^{h_k} c(h_k)$.

Escribiendo i, j en vez de j, k; obtenemos (3). Esto implica que C es subgrupo de G y así C es complemento de N en G. Ahora sean C, C' complementos de N en G. Si $h_i \in H$, en la clase lateral h_i hay un y solo un elemento $r(h_i)$ de C ($r'(h_i)$ de C').

Como $r(h_i)$ y $r'(h_i)$ están en la misma clase lateral de N en G, $r(h_i)a(h_i) = r'(h_i)$ con $a(h_i) \in N$. Además tenemos que , si $h_i, h_j \in H$

$$r'(h_i h_j) = r(h_i h_j) a(h_i h_j).$$

Por otro lado

$$r'(h_i h_j) = r'(h_i) r'(h_j) = r(h_i) a(h_i) r(h_j) a(h_j) = r(h_i) r(h_j) [a(h_i)]^{h_j} a(h_j) = r(h_i h_j) [a(h_i)]^{h_j} a(h_j)$$

Se sigue que

$$a(h_i h_j) = [a(h_i)]^{h_j} a(h_j)$$

y así

$$\prod_{i=1}^{m} a(h_i h_j) = \prod_{i=1}^{m} ([a(h_i)]^{h_j} a(h_j))$$
$$\text{pero } \prod_{i=1}^{m} ([a(h_i)]^{h_j} a(h_j)) = [\prod_{i=1}^{m} a(h_i)]^{h_j} [a(h_j)]^m$$
$$\text{por tanto } \prod_{i=1}^{m} a(h_i h_j) = [\prod_{i=1}^{m} a(h_i)]^{h_j} [a(h_j)]^m.$$

Pero

$$\prod_{i=1}^{m} a(h_i h_j) = \prod_{i=1}^{m} a(h_j)$$

por tanto

$$\prod_{i=1}^{m} a(h_i) = [\prod_{i=1}^{m} a(h_i)]^{h_j} [a(h_j)]^m.$$

Escribiendo $b = [\prod_{i=1}^{m} a(h_i)]^z$ tenemos que
$b^{-1} r(h_j) b = [\prod_{i=1}^{m} a(h_i)]^{-z} r(h_j) [\prod_{i=1}^{m} a(h_i)]^z$. Pero
$\prod_{i=1}^{m} a(h_i) = [\prod_{i=1}^{m} a(h_i)]^{h_j} [a(h_j)]^m$; entonces

$$[\prod_{i=1}^{m} a(h_i)]^{-z} r(h_j) [\prod_{i=1}^{m} a(h_i)]^z = [\prod_{i=1}^{m} a(h_i)]^{-z} r(h_j) [[\prod_{i=1}^{m} a(h_i)]^{h_j} [a(h_j)]^m]^z$$

$$[\prod_{i=1}^{m} a(h_i)]^{-z} r(h_j) [[\prod_{i=1}^{m} a(h_i)]^{h_j} [a(h_j)]^m]^z = [\prod_{i=1}^{m} a(h_i)]^{-z} r(h_j) [[\prod_{i=1}^{m} a(h_i)]^{h_j}]^z [a(h_j$$

pero $mz \equiv 1 (\mathrm{mod}\ |N|)$, así obtenemos que

$$[\prod_{i=1}^{m} a(h_i)]^{-z} r(h_j) [[\prod_{i=1}^{m} a(h_i)]^{h_j}]^z [a(h_j)]^{mz} = [\prod_{i=1}^{m} a(h_i)]^{-z} r(h_j) [[\prod_{i=1}^{m} a(h_i)]^z]^{h_j} a(h_j$$

$$[\prod_{i=1}^{m} a(h_i)]^{-z} r(h_j) [[\prod_{i=1}^{m} a(h_i)]^z]^{h_j} a(h_j) = [\prod_{i=1}^{m} a(h_i)]^{-z} r(h_j) \left(r(h_j)^{-1}\right) [\prod_{i=1}^{m} a(h_i)]^z r($$

y cancelando obtenemos que

$[\prod_{i=1}^{m} a(h_i)]^{-z} r(h_j)[[\prod_{i=1}^{m} a(h_i)]^{h_j}]^{z} a(h_j) = r(h_j)a(h_j) = r'(h_j)$.

Esto implica que $b^{-1}Cb = C'$, lo que prueba el teorema■

Teorema 3.2 (Schur-Zassenhaus): Sea G un grupo finito y N un subgrupo de Hall normal de G. Entonces existe en G al menos un complemento de N. Además, si al menos uno de los grupos N, G/N es soluble, entonces los complementos de N en G son conjugados.

Demostración:

La prueba es por inducción sobre el orden de G. Primero probamos que existe un complemento de N en G. Consideramos dos casos:

Caso 1) N no es soluble. Entonces al menos un subgrupo de Sylow de S en N no es normal en N. Por el argumento de Frattini (45), $G = N_G(S)N$.

Entonces $N_G(S) \cap N$ es normal en $N_G(S)$ y $|G/N| = |N_G(S)N/N| = |N_G(S)||N|/|N_G(S) \cap N||N| = |N_G(S)|/|N_G(S) \cap N|$ es decir $[G : N] = [N_G(S) : N_G(S) \cap N]$.

Consecuentemente $N_G(S) \cap N$ es un subgrupo de Hall de $N_G(S)$, porque $|N_G(S) \cap N|$ divide a $|N|$; entonces $|N_G(S) \cap N|$ y $[G : N]$ son primos relativos, pero $[G : N] = [N_G(S) : N_G(S) \cap N]$ por tanto $(|N_G(S) \cap N|, [N_G(S) : N_G(S) \cap N]) = 1$.

Como S no es normal en G (si lo fuera, también lo sería en N) tenemos que $N_G(S) \neq G$; esto implica que, por inducción, existe un complemento C de $N_G(S) \cap N$ en $N_G(S)$. Entonces tenemos que $|N_G(S)| = |N_G(S) \cap N||C|$ de donde $|C| = |N_G(S)|/|N_G(S) \cap N| = |G|/|N|$, es decir $|G| = |C||N|$. Consideremos $|CN| = |C||N|/|C \cap N| = |G|/|C \cap N|$, pero $N_G(S) = (N_G(S) \cap N)C$; entonces como C es complemento de $N_G(S) \cap N$ tenemos que $N_G(S) \cap N \cap C = \langle 1 \rangle$ y como $C \subset N_G(S)$, tenemos que $|C \cap N| = 1$ y $|CN| = |G|$.

Así podemos concluir que $G = CN$ y que C es un complemento de N en G.

Caso 2) N es soluble. Sea M un subgrupo normal minimal de G contenido en N. Por tanto M es p-grupo abeliano elemental (p primo). Sea $|M| = p^r$ y $|G/N| = l$. Se sigue que N/M es un subgrupo normal de Hall de G/M porque $[G/M : N/M] = |G|/|N| = [G : M] = l$, y como $|N/M|$ divide a $|N|$ y $(|N|, l) = 1$ concluimos que $(|N/M|, l) = 1$. Entonces por inducción, existe un complemento D/M de N/M es G/M.

Como $|G/M| = |D/M||N/M|$ tenemos que $|D/M| = |G|/|N| = l$; por tanto D es un subgrupo de G de orden $p^r l$ con $(p^r, l) = 1$ porque p^r divide a

$|N|$ y $(|N|, l) = 1$. Entonces M es un subgrupo de Hall de D, normal en D porque $[D : M] = l$ y $|M|$ divide a $|N|$ por tanto $([D : M], |M|) = 1$ y la normalidad se da porque M es normal en G.

Como M es abeliano, por el teorema 5.1, existe en D un complemento C de M. Entonces $|D| = |C||M|$, de donde $|C| = |D|/|M| = l$.

Observemos ahora que CN es un subgrupo de G porque N es normal en G, entonces $|CN| = |C||N|/|C \cap N| = l|N|/|C \cap N|$; pero $|C \cap N|$ divide a $|N|$ y a $|C|$ que son primos relativos, por tanto $|C \cap N| = 1$. Y de ahí concluimos que $|G| = |CN|$. Esto implica que C es complemento de N en G.

Entonces hemos probado que, en ambos casos, existe un complemento de N en G. Ahora sean C_1, C_2 dos complementos de N en G. Tenemos que demostrar que son conjugados si al menos uno de los siguientes dos casos ocurre: a) N es soluble; b) G/N es soluble.

Caso a): Sea M un subgrupo normal minimal de G contenido en N. Entonces $|M| = p^r$ (con p primo). Además N/M es un subgrupo normal de Hall de G/M y C_1M/M, C_2M/M son complemento de N/M en G/M ya que como N/M es subgrupo de G/M al ser N/M normal en G/M tendremos que, si $i = 1, 2$

$|(C_iM/M)(N/M)| = |C_iM/M||N/M|/|C_iM/M \cap N/M| = (|C_i||N|/|M|)/|C_iM/M \cap N/M|$ ya que $|C_i \cap M| = 1$ porque $M < N$ y $C_i \cap M < C_i \cap N = \langle 1 \rangle$.

Pero $C_iM \cap N = M$ porque $M \subset C_iM$ y $M < N$; además si $y \in C_iM \cap N$ tenemos que $y \in C_iM$, de donde $y = cm$ con $c \in C_i$ y $m \in M$. Como $M < N$, $m \in N$ y esto implica que $c \in N$; de aquí $c \in C_i \cap N = \langle 1 \rangle$ pr tanto $c = 1$, es decir $y = m \in M$ y podemos concluir que $C_iM \cap N = M$; entonces $C_iM/M \cap N/M = \langle 1 \rangle$, en otras palabras $|(C_iM/M)(N/M)| = |G|/|M|$.

Entonces por inducción, existe un elemento $xM \in G/M$ tal que $(xM)^{-1}C_1M/M(xM) = C_2M/M$; es decir $(xM)^{-1}C_1M(xM) = C_2M$. Nótese que $x^{-1}C_1x \subset C_2M$ porque $C_1 \subset$, entonces $x^{-1}C_1x \subset x^{-1}C_1Mx = C_2M$; y así $x^{-1}C_1x$ y C_2 son complementos de M en C_2M (porque $|x^{-1}C_1x| = |C_1|$), mientras que M es un subgrupo normal de Hall de C_2M porque $[C_2M : M] = (|C_2||M|)/(|C_2 \cap M||M|) = |C_2|$ ya que $|C_2 \cap M| = 1$, y esto se da porque $|C_2 \cap M|$ divide a $|M|$ y a $|C_2|$ aunado a que $|M|$ divide a $|N|$ y $(|N|, |C_2|) = 1$ (ya que $G = C_2N$). Por tanto $(|C_2|, |M|) = 1$.

Observemos que como M es abeliano; existe, por el teorema 5.1,

una $y \in C_2M$ tal que $y^{-1}(x^{-1}C_1x)y = C_2$. Por tanto C_2 es conjugado de C_1 en G.

Caso b) Sea $H/N <_{\min} G/N$. Entonces como G/N es soluble, H/N es abeliano elemental y $|H/N| = q^s$ (q primo). Sea $|N| = n$ y $|H| = q^s n$ con $(n, q^s) = 1$ (porque $|H/N|$ divide a $|G/N| = [G : N]$ y N es subgrupo de Hall de G).

Como H es normal en G, $H \cap C_i$ $(i = 1, 2)$, es normal en C_i, con $|HC_i| = |H||C_i|/|C_i \cap H|$ entonces $|H \cap C_i| = |H||C_i|/|HC_i|$; pero $|HC_i|$ divide a $|G|$ y además como $N \triangleleft G$ también es normal en HC_i, es decir NC_i es subgrupo de HC_i. De aquí $|NC_i| = |G|$, de donde $|G| = |HC_i|$ y al sustituir obtenemos $|H \cap C_i| = |H||C_i|/|G| = (nq^s|C_i|)/(n|C_i|)$. Esto implica que $|H \cap C_i| = q^s$.

Por tanto $H \cap C_1$ y $H \cap C_2$ son q-subgrupos de Sylow de H, entonces existe $h \in H$ tal que $h^{-1}(H \cap C_1)h = H \cap C_2$, es decir $H \cap (h^{-1}C_1h) = H \cap C_2$ porque se ve fácilmente que $h^{-1}(H \cap C_1)h = H \cap (h^{-1}C_1h)$.

Observemos que $H \cap C_2$ es normal en $h^{-1}C_1h = C_3$. En efecto, si $x \in h^{-1}C_1h$ hay que ver que $x^{-1}(H \cap C_2)x = H \cap C_2$. Tenemos que $x^{-1}(H \cap C_2)x = x^{-1}(H \cap (h^{-1}C_1h))x$ y sabemos que $x^{-1}(H \cap (h^{-1}C_1h))x = (x^{-1}Hx) \cap (x^{-1}(h^{-1}C_1h)x)$; pero como H es normal en G entonces $x^{-1}Hx = H$, además $x \in h^{-1}C_1h$, $x^{-1}(h^{-1}C_1h)x = h^{-1}C_1h$. Por tanto $x^{-1}(H \cap C_2)x = x^{-1}(H \cap (h^{-1}C_1h))x = H \cap C_2$. Entonces, $C_3 \leq N_G(H \cap C_2)$.

Sea $j = 2, 3$. De acuerdo con la relación de Dedekind tenemos que $N_G(H \cap C_2) = N_G(H \cap C_2) \cap G = N_G(H \cap C_2) \cap NC_j = C_j(N \cap N_G(H \cap C_2))$, ya que $NC_j = C_jN$ y $C_j \subset N_G(H \cap C_2)$.

Pero como N es normal en G, $N \cap N_G(H \cap C_2)$ es normal y de Hall en $N_G(H \cap C_2)$ y como C_2, C_3 son complementos de $N \cap N_G(H \cap C_2)$ en $N_G(H \cap C_2)$ porque $N_G(H \cap C_2) = C_j(N \cap N_G(H \cap C_2))$ para $j = 2, 3$.

Además $N_G(H \cap C_2)/(N \cap N_G(H \cap C_2))$ es soluble porque es subgrupo de G/N, y este último lo es. Si $N_G(H \cap C_2) \neq G$, por inducción existe $k \in N_G(H \cap C_2)$ tal que $k^{-1}C_3k = C_2$, es decir $k^{-1}(h^{-1}C_1h)k = C_2$, y esto implica que C_1 y C_2 son conjugados en G.

Por el contrario si $N_G(H \cap C_2) = G$, $H \cap C_2$ es normal en G. Es facil verificar que $N(H \cap C_2)/(H \cap C_2)$ es un subgrupo normal y de Hall de $G/(H \cap C_2)$, en donde $C_2/(H \cap C_2)$ y $C_3/(H \cap C_2)$ son complementos suyos. Por inducción, existe $x(H \cap C_2)$ tal que

$x(H \cap C_2)^{-1}(C_3/(H \cap C_2))x(H \cap C_2) = C_2/(H \cap C_2)$ y esto implica que $x^{-1}(h^{-1}C_1h)x = x^{-1}C_3x = C_2$ y también en este caso C_1 y C_2 son conjugados■

El teorema de Schur-Zassenhaus aparece por primera vez en el libro [22] de Zassenhaus. La primera parte de este teorema es atribuida por Zassenhaus a Schur. La segunda seguramente se debe a Zassenhaus.

Un célebre teorema de Feit-Thompson establece que un grupo de orden impar es soluble. De acuerdo con este teorema, la hipótesis "N es soluble o G/N es soluble" puede ser removida del enunciado del teorema de Schur-Zassenhaus, ya que como N es subgrupo de Hall de G, $(|N|, |G/N|) = 1$, así que al menos uno de N ó G/N es de orden impar y éste es soluble.

Observaciones:

i) Consideremos $G = A_5$, el orden de G es $2^2 * 15$ con $(2^2, 15) = 1$. G tiene un subgrupo N de orden 4 que no es normal (porque A_5 es simple) y A_5 no tiene subgrupos de orden 15.

ii) Consideremos $G = S_3$, $|S_3| = 2 * 3$. Si N es un 2-subgrupo de Sylow de G, N no es normal pero G sí tiene un subgrupo de orden 3.

En la observación *ii* se hace notar que en el teorema de Schur-Zassenhaus la normalidad del subgrupo N no es una condición necesaria.

CAPÍTULO 4
GRUPOS P-NILPOTENTES Y EL SUBGRUPO DE FRATTINI

En este último capitulo se presenta un resultado que caracteriza a los grupos nilpotentes, a saber, que un grupo finito es nilpotente si y sólo si es p-nilpotente para todo primo p que divida a su orden. También se demuestran algunos resultados sobre el subgrupo de Frattini de un grupo finito para finalmente relacionar este concepto con el de p-nilpotencia.

En este capítulo sólo consideramos grupos finitos.

Definición: Sea G un grupo y p un primo. Una cadena de subgrupos normales $G = H_0 \geq H_1 \geq H_n \geq \ldots$ es una serie *p-central* si para cada i tal que p divida a $|H_{i-1}/H_i|$ se tiene que $H_{i-1}/H_i \subset Z(G/H_i)$ o equivalentemente $[G, H_{i-1}] \subset H_i$.

Observación: Una serie normal es central si y sólo si es p-central para cada primo p que divide al orden de G.

Recordemos que un grupo G se llama nilpotente si tiene una serie central que alcanza $\langle 1 \rangle$.

Definición: Sea p un primo, un grupo G se llama *p-nilpotente* si tiene una serie p-central que alcanza $\langle 1 \rangle$.

Ejemplo: S_3 es un grupo 2-nilpotente porque la serie $S_3 > A_3 > \langle 1 \rangle$ es una serie 2-central. S_3 no es 3-nilpotente porque 3 divide al orden de $A_3/\langle 1 \rangle$ y $A_3/\langle 1 \rangle$ no está contenido en $Z(S_3/\langle 1 \rangle)$.

Teorema 4.1: Sea G un grupo finito y p un primo, G es p-nilpotente si y sólo si G tiene un p-complemento normal.

Demostración:

Supongamos que G tiene un p-complemento normal C, $|G| = p^n m$ con p primo, $n \geq 0$ y $|C| = m$. Es decir $|G/C| = p^n$. G/C es nilpotente porque es p-grupo, por tanto la serie central ascendente $\langle 1 \rangle \leq Z_0 \leq Z_1 \leq \ldots \leq Z_i \leq \ldots$ de G/C alcanza a G/C, esto es $Z_t = G/C$ para alguna t. Sea H_i la imagen inversa bajo el homomorfismo canónico de G sobre G/C, entonces $G = H_t > H_{t-1} > \ldots > H_0 = C > \langle 1 \rangle$ es una serie p-central de G que alcanza $\langle 1 \rangle$, en efecto: p no divide a $|C|$, mientras que $H_i/H_{i-1} \subset Z(G/H_{i-1})$ porque $Z_i/Z_{i-1} \subset Z[(G/C)/Z_{i-1}]$ y entre G/H_{i-1} y $(G/C)/Z_{i-1}$ existe un isomorfismo φ tal que $gH_{i-1} \overset{\varphi}{\to} (gC)Z_{i-1}$.

Inversamente, supongamos que G es p-nilpotente y sea $G = H_0 \gneqq H_1 \gneqq \ldots \gneqq H_s = \langle 1 \rangle$ una serie p-central que alcanza a $\langle 1 \rangle$.

Demostración por inducción sobre el orden de G:

Distinguimos 2 casos

a) p no divide al orden de H_{s-1}:

G/H_{s-1} es también p-nilpotente porque $G/H_{s-1} \geq H_1/H_{s-1} \geq \ldots \geq H_{s-1}/H_{s-1} = \langle 1 \rangle$ es una serie p-central de G/H_{s-1} ya que si $H_{i-1}/H_i \subset Z(G/H_i)$, $(H_{i-1}/H_{s-1})/(H_i/H_{s-1}) \simeq H_{i-1}/H_i$ debe estar en el centro de $(G/H_{s-1})/(H_i/H_{s-1})$, por lo tanto G/H_{s-1} tiene un p-complemento normal C/H_{s-1} y por lo tanto $G/C \simeq (G/H_{s-1})/(C/H_{s-1})$ es un p-grupo, además $|C| = [C : H_{s-1}]|H_{s-1}|$ no es divisible por p ya que p no divide a $|H_{s-1}|$ y p no divide a $|C/H_{s-1}|$.

Además $C \lhd G$ porque $C/H_{s-1} \lhd G/H_{s-1}$.

b) p divide al orden de H_{s-1}:

$H_{s-1} = H_{s-1}/\langle 1 \rangle = H_{s-1}/H_s \subset Z(G/H_s) = Z(G)$ por lo que H_{s-1} es abeliano.

Sea P el único p-subgrupo de Sylow de H_{s-1}, P *car* H_{s-1} pues si $\varphi \in aut(H_{s-1})$ se tiene que $\varphi(P) < H_{s-1}$ de orden $|P|$ por tanto $\varphi(P) = P$.

Siendo $H_{s-1} \lhd G$ y P *car* H_{s-1} entonces $P \lhd G$ y por tanto $G = H_0 \geq H_1 \geq \ldots \geq H_{s-1} \geq P \geq H_s = \langle 1 \rangle$ es también una serie p-central y G/P es p-nilpotente y por hipótesis de inducción G/P tiene un p-complemento normal S/P. $|S/P| = l$ con $(l, |P|) = 1$.

Entonces $|S| = |P|l$ y como $G/S \simeq (G/P)/(S/P)$, G/S es un p-grupo (S/P es un p-complemento de G/P). Como $P \lhd S$ y $(|P|, [S : P]) = 1$,

entonces por el teorema de Schur-Zassenhaus, se tiene un p-complemento C en S, como $P \subset Z(S)$ también $P \subset C_G(C)$.

$S = PC$ y si $x \in S$ tenemos que $x = p_1 c_1$ y si $c \in C$, $x^{-1}cx = c_1^{-1}p_1^{-1}cp_1c_1 = c_1^{-1}cc_1 \in C$ por tanto $C \lhd S$ y por el teorema de Schur-Zassenhaus C es el único p-complemento de S es decir C es característico en S. Como $C\ car\ S$ y $S \lhd G$ tenemos que $C \lhd G$.

Como $|C| = l$ y $[G : C] = [G : S][S : C]$ con $[G : S]$ y $[S : C]$ potencias de p se tiene que C es un p-complemento normal de G ya que $|G| = [G : C]|C| = p^a l$■

Teorema 4.2: Sea G un grupo finito. G es nilpotente si y sólo si G tiene un p-complemento normal para cada primo p que divida al orden de G.

Demostración:

Sea $|G| = p_1^{n_1} \dots p_s^{n_s}$, con p_i primos diferentes. Supongamos que G es nilpotente, para cada $1 \leq i \leq s$, si Q_i es un p_i-subgrupo de Sylow, Q_i es normal en G. $C_i = \prod_{1 \leq j \leq s,\ j \neq i} Q_j$ Es un p_i –complemento normal de G.

(Observese que esta implicación puede probarse también usando la definición de p-nilpotencia y el teorema 4.1)

Inversamente si $C_1, C_2, \dots C_s$ son los p_i-complementos normales de G y $Q_i = \bigcap_{1 \leq j \leq s,\ j \neq i} C_i$ es un p_i-subgrupo de Sylow normal de G. En efecto, Q_i es normal en G, además si $i \neq j$ tenemos que $|C_i \cap C_j| = |C_i||C_j|/|C_iC_j| = |C_i||C_j|/|G| = (|G|p_i^{-n_i}|G|p_j^{-n_j})/|G| = |G|p_i^{-n_i}p_j^{-n_j}$ e inductivamente se puede probar que $\left| \bigcap_{1 \leq j \leq s,\ j \neq i} C_j \right| = |G| \prod_{1 \leq j \leq s,\ j \neq i} p_j^{n_j}$. Por lo tanto $|Q_i| = p_i^{n_i}$ para toda i, de donde se sigue que G es nilpotente■

Nota: compare este resultado con 1.4.

En virtud de 6.1 y 6.2, se tiene que un grupo G es nilpotente si y sólo si G es p-nilpotente para todo primo p que divide al orden de G

Definición: $M \lneqq G$ es *maximal* si no existe H tal que $M < H < G$. Y escribimos $M <_{\max} G$.

Definición: Sea $G \neq \langle 1 \rangle$ el *subgrupo de Frattini* de G, $\phi(G)$ es la intersección de todos los subgrupos maximales de G.

Si $G = \langle 1 \rangle$, $\phi(G) = \langle 1 \rangle$. Si $M <_{\max} G$ y $\varphi \in aut(G)$ entonces

$\varphi(M) <_{\max} G$ y por tanto $\varphi(\phi(G)) = \phi(G)$.

Tenemos entonces el

Teorema 4.3: El subgrupo de Frattini es característico en G.

Recordemos el Argumento de Frattini (45):

Sea G un grupo, $H \lhd G$ y P un p-subgrupo de Sylow de H entonces $G = HN_G(P)$.

El argumento usado en esta demostración se conoce como "El argumento de Frattini" y su sencillez a veces enmascara su gran utilidad.

Teorema 4.4: Sea P un p-subgrupo de Sylow de G y sea $K = N_G(P)$, si $K < H$ entonces $H = N_G(H)$.

Demostración: (usando el argumento de Frattini)

Sea $g \in N_G(H)$ entonces $g^{-1}Pg \subset g^{-1}Kg \subset g^{-1}Hg = H$ es decir que P y $g^{-1}Pg$ son dos p-subgrupos de Sylow de H y por tanto existe $h \in H$ tal que $h^{-1}Ph = g^{-1}Pg$. Entonces $P = (gh^{-1})^{-1}P(gh^{-1})$ i.e. $gh^{-1} \in N_G(P) = K \subset H$, por tanto $g \in H$■

Teorema 4.5: Sea G un grupo y $H < G$ tal que $G = H\phi(G)$, entonces $H = G$.

Demostración:

Supongamos que $H \lneqq G$ entonces existe $M <_{\max} G$ tal que $H \leq M$. $G = H\phi(G) \leq M\phi(G) = M$ por tanto $G = M$. Esto contradice que $M <_{\max} G$. ■

Definición: $g \in G$ es un *no-generador* de G si y solo si para todo $X \subset G$ que cumpla $\langle X \cup \{g\} \rangle = G$ se tiene que $\langle X \rangle = G$.

Teorema 4.6: $\phi(G) = \left\{ g \in G \mid g \text{ es un no-generador de } G \right\}$.

Demostración:

Sea $g \in \phi(G)$ y $X \subset G$ tal que $\langle X \cup \{g\} \rangle = G$. Supongamos que $\langle X \rangle \lneqq G$. Sea $M <_{\max} G$ tal que $X \subset M$. Por tanto $G = \langle X \cup \{g\} \rangle \subset \langle M, g \rangle = M$. Por tanto $G = \langle X \rangle$.

Inversamente, sean g un no-generador de G y $M <_{\max} G$. Por demostrar que $g \in M$.

Supongamos que $g \notin M$. Dado que $M \lneqq \langle M, g \rangle$, se sigue que

$\langle M,g\rangle = G$ pero como g es un no-generador $\langle M\rangle = G$ y como $M < G$, tenemos que $M = \langle M\rangle = G$ lo cual es una contradicción■

Teorema 4.7: Cada p-subgrupo de Sylow P de $\phi(G)$ es normal en G y $\phi(G)$ es nilpotente.

Demostración:

$\phi(G)$ *car* G entonces $\phi(G) \lhd G$. Como P es un p-subgrupo de Sylow de $\phi(G)$ entnoces $G = \phi(G)N_G(P)$ lo que implica que $G = N_G(P)$ entonces $P \lhd G$ y $P \lhd \phi(G)$, por tanto $\phi(G)$ es nilpotente■

Teorema 4.8: Sea G un grupo nilpotente entonces $G' < \phi(G)$.

Basta demostrar que $G' < M$ para todo $M <_{\max} G$. Como G es nilpotente si $H \lneqq G$ se tiene que $H \lneqq N_G(H)$ por consiguiente siendo M maximal, entonces $M \lhd G$.

Como G es soluble (por ser nilpotente) y G/M es simple, entonces G/M es de orden primo y por ser abeliano $G' < M$■

Teorema 4.9: Sea G un grupo, $N \lhd G$ tal que $\phi(G) \subset N$, si $N/\phi(G)$ es p-nilpotente, entonces N es p-nilpotente.

Demostración:

Siendo $N/\phi(G)$ p-nilpotente, tiene un p-complemento normal $K/\phi(G)$. $K/\phi(G)$ es un subgrupo normal de Hall de $N/\phi(G)$ y en consecuencia $K/\phi(G)$ es caracteristico en $N/\phi(G)$ por 26 y como $N/\phi(G) \lhd G/\phi(G)$, $K/\phi(G) \lhd G/\phi(G)$. Así, $K \lhd G$. Sea P un p-subgrupo de Sylow de $\phi(G)$ (puede que $P = \langle 1\rangle$) como $K/\phi(G)$ es un p-complemento de $N/\phi(G)$ p no divide a $|K/\phi(G)|$ y por lo tanto $\phi(G)$ contiene a todos los p-elementos de K y por consiguiente P es un p-subgrupo de Sylow de K.

Siendo P un p-subgrupo de Sylow de $\phi(G)$ es normal en G (por 6.7) y por consiguiente en K y por el teorema de Schur-Zassenhaus en K existe un p-complemento B y entonces $K = PB$.

Si $g \in G$, $g^{-1}Bg < g^{-1}Kg = K$ ($K \lhd G$), $g^{-1}Bg$ es también un p-complemento de K y $h^{-1}Bh = g^{-1}Bg$ para alguna $h \in K$ (porque los p-complementos de K son conjugados) por tanto $B = (gh^{-1})^{-1}B(gh^{-1})$ entonces $gh^{-1} \in N_G(B)$, $g \in N_G(B)K$.

$N_G(B)K = N_G(B)PB = N_G(B)P \leq N_G(B)\phi(G)$ por tanto $G \leq N_G(B)\phi(G)$, $G = N_G(B)\phi(G)$ y $G = N_G(B)$ y $B \lhd G$, por lo tanto $B \lhd N$. Si demostramos que B es un p-complemento de N, se tendrá

que N es p-nilpotente:

$[N : B] = [N : K][K : B]$ es una potencia de p porque $|N/K| = |(N/\phi(G))/(K/\phi(G))|$ es potencia de p porque $K/\phi(G)$ es un p-complemento de $N/\phi(G)$.

$\left|K/B\right|$ también es potencia de p porque B es un p-complemento de K. $|N| = [N : B]|B|$, B es un p-complemento de N.

Teorema 4.10: Si G es un grupo y p divide al orden de G, entonces p divide al orden de $|G/\phi(G)|$.

Demostración:

Supóngase que $p \nmid |G/\phi(G)|$, como $|G| = |\phi(G)|[G : \phi(G)]$ y $p \nmid |G/\phi(G)|$ entones $\phi(G)$ contiene a los p-subgrupos de Sylow de G, si P es un p-subgrupo de Sylow de G también lo es de $\phi(G)$ y por tanto $P \triangleleft G$ (por 6.7).

Por el teorema de Schur-Zassenhaus G tiene un p-complemento C. Sea $M <_{\max} G$ tal que $C < M < G$, como $[G : C] = [G : M][M : C]$ y $[G : C]$ es potencia de p, entonces $[G : M]$ es una potencia de p y como $\phi(G) < M < G$ y $[G : \phi(G)] = [G : M][M : \phi(G)]$ entonces p divide a $[G : \phi(G)]$ lo cual es una contradicción■

ÍNDICE DE SIMBOLOS

$A \subset B$ A es subconjunto de B

$A \subsetneq B$ A es subconjunto propio de B

$H < G$ H es subgrupo de G

$H \lneqq G$ H es subgrupo propio de G

Φ El conjunto vacío

$A \times B$ Producto directo de A y B

$A \lhd B$ A es subgrupo normal de B

$|A|$:= cardinalidad del conjunto A.

$AB = \{ab \mid a \in A, b \in B\}$ con A, B subconjuntos de un grupo G.

$a^b = b^{-1}ab$

$A^b = b^{-1}Ab$

$A^B = \{b^{-1}ab \mid a \in A, b \in B\}$

$A^{-1} = \{a^{-1} \mid a \in A\}$

$[G : S]$ El indice del subgrupo S en el grupo G

$G <_{\max} H$ G es subgrupo maximal de H

$G <_{\min} H$ G es subgrupo minimal de H

$G \lhd_{\max} H$ G es subgrupo normal maximal de H

$G \lhd_{\min} H$ G es subgrupo normal minimal de H

xH clase lateral izquierda de H que contiene a x

G/H grupo cociente G entre H

G'	El subgrupo conmutador o derivado de G
$G^{(n)}$	El n-ésimo subgrupo derivado de G
$Z(G)$	El centro del grupo G
$Aut(G)$	El conjunto de automorfismos del grupo G
$\mathbb{Z}_n$	Las clases residuales de los enteros modulo n

Bibliografía

[1] Alperin, J. L. - Bell Rowen B., *Groups and Representations*, Springer, 1995.

[2] Bender, H., A group Theoretic proof of Burnside's $p^a q^b$-theorem, Math. Z.126,327-338, 1972.

[3] Carter, R., *Nilpotent Self-normalizing Subgroups of Soluble Groups,* Math. Z., 1961.

[4] Hall, P., *A Note on Soluble Groups,* J. London Math. Soc., 1928.

[5] Hall, P., *A Characteristic Property of Soluble Groups,* J. London Math. Soc., 1937.

[6] Lederman, W., *Introduction to Group Theory,* Longman, London, 1973.

[7] Marshall Hall, Jr.,*Teoría de los Grupos*, Trillas, México, 1973.

[8] Robinson, Derek J. S., *A course in the Theory of Groups*, Springer-Verlag, 1982 (reimpreso 1994).

[9] Rotman, Joseph J., *A Introduction to the Theory of Groups,* Springer-Verlag, 1995.

[10] Zappa, G., *Topics on Finite Solvable Groups,* Istituto Nazionale di Alta Matematica Francesco Severi, Roma, 1982