21

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

SOBRE GRUPOS FINITOS NO CICLICOS CON TODOS SUS SUBGRUPOS NORMALES PROPIOS CICLICOS.

T E S I S

QUE PARA OBTENER EL TITULO DE

M A T E M A T I C A

P R E S E N T A :

ROCIO LEONEL GOMEZ

DIRECTOR DE TESIS: DR. JUAN MORALES RODRIGUEZ

2001

21

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

SOBRE GRUPOS FINITOS NO CICLICOS CON TODOS SUS SUBGRUPOS NORMALES PROPIOS CICLICOS.

T E S I S

QUE PARA OBTENER EL TITULO DE

M A T E M A T I C A

P R E S E N T A :

ROCIO LEONEL GOMEZ

DIRECTOR DE TESIS: DR. JUAN MORALES RODRIGUEZ

2001

VNIVERSIDAD NACIONAL
AVTONOMA DE
MEXICO

M. EN C. ELENA DE OTEYZA DE OTEYZA
Jefa de la División de Estudios Profesionales de la
Facultad de Ciencias
Presente

Comunicamos a usted que hemos revisado el trabajo de Tesis:
Sobre grupos finitos no cíclicos con todos sus subgrupos normales propios cíclicos.

realizado por Rocío Leonel Gómez.

con número de cuenta (95543518) , pasante de la carrera de Matemáticas.

Dicho trabajo cuenta con nuestro voto aprobatorio.

Atentamente

Director de Tesis DR. Juan Morales Rodríguez.
Propietario

Propietario Dr. Adalberto García Maynez.

Propietario Dr. Bertha Tomé Arreola

Suplente Dr. Edith Corina Sáenz Valadez.

Suplente Dr. Alejandro Alvarado García.

Consejo Departamental de Matemáticas.

M. en C. Alejandro Bravo Mojica.

FACULTAD DE CIENCIAS

A Genoveva

Marco

Ale

y

Miriam

Al presentar este trabajo, quiero manifestar mi gratitud muy especial a quienes me brindaron su valiosa colaboración con sus comentarios, criticas y sugerencias. En particular a las profesoras; Bertha Tomé y Edith Corina Sáenz.

Con mucho cariño y respeto para Dr. Juan Morales Rodríguez por su interés y valiosa orientación.

A todas aquellas personas que de alguna u otra manera, me motivaron para que pudiera concluir mis estudios en forma satisfactoria. Gracias.

0.1 INDICE

0.2 INTRODUCCION.

En este trabajo siguiendo a *Mariagrazia Bianchi* en [1], presentamos una clasificación de los grupos finitos, solubles no cíclicos con todos sus subgrupos normales propios cíclicos, los cuales son llamados $Nc-$ grupos finitos.

En el capítulo 1, mencionamos conceptos y resultados básicos en Teoria de Grupos, necesarios para la elaboración del presente trabajo.

En el capítulo 2, que está dedicado a los grupos cíclicos finitos, se dan dos caracterizaciones de ellos, una de ellas no usual en la literatura, con la que se prueban algunos resultados ya conocidos.

En el capítulo 3, estudiaremos los grupos de orden p, p^2, p^3 y pq con p y q primos, entre los cuales se encuentran: el grupo de los Cuaternios y el grupo de las Simetrias del Cuadrado, destacan en particualr estos grupos, porque los cuaternios es un $Nc-$ grupo y el grupo de las simetrias del cuadrado nos hace ver que la normalidad no es una propiedad transitiva.

En el capítulo 4, el cual trata sobre $p-$ grupos finitos, destaca lo siguiente: Si un grupo finito G de orden p^n tiene un único subgrupo de orden p, entonces G es cíclico o G es un grupo cuaternio generalizado. Resultado que usaremos en el último capítulo.

En el capítulo 5, se definen los $Nc-$ grupos y se da una clasificación de los $Nc-$ grupos finitos solubles.Veremos que entre los p-grupos abelianos sólo los p-grupos abeliano elemental de orden p^2 son $Nc-$grupos. Entre los p-grupos no abelianos, sólo el grupo de los cuaternios es un $Nc-$grupo. En este mismo capítulo presentamos algunos resultados sobre los $Nc-$ grupos finitos solubles no nilpotentes.

Todas las definiciones y demostraciones de los teoremas que se mencionan en este trabajo o aquellas que se usan y en forma involuntaria no se enuncian explicitamente, se pueden consultar en los libros de los profesores Rotman, Zappa y Zassenhaus que se encuentran en la bibliografia.

Capítulo 1

Preliminares.

Definición 1 *Un grupo G es un conjunto con una operación binaria $*$ en G que cumple las siguientes propiedades:*

(1) *La operación binaria $*$ es asociativa.*

(2) *Existe $e \in G$ que cumple con $e * x = x * e$ para todo $x \in G$.*

(3) *Para cada $a \in G$ existe $a' \in G$ tal que $a * a' = a' * a = e$.*

Se prueba que el elemento e que cumple con la propiedad (2) es único y se le llama *elemento identidad.* Si $a \in G$ el elemento $a' \in G$ que satisface la propiedad (3) es único y se le llama el *inverso* de a.

En lugar de escribir $a * b$, escribiremos ab.

Definición 2 *El orden de un grupo G es el número de elementos de G y es denotado por $|G|$.*

Si G_1 y G_2 son grupos, $G_1 \times G_2$ es un grupo con la siguiente operación binaria; si $x = (m_1,\ m_2) \in G_1 \times G_2$, $y = (n_1,\ n_2) \in G_1 \times G_2$, entonces $xy = (m_1 n_1,\ m_2 n_2)$.

Definición 3 *Una función φ de un grupo G_1 en un grupo G_2 es un homomorfismo si*

$$\varphi(ab) = \varphi(a)\,\varphi(b)$$

para todos los elementos a y b de G.

Teorema 4 *Si G_1 y G_2 son grupos y $\varphi : G_1 \longrightarrow G_2$ es un homomorfismo de grupos, entonces se cumple lo siguiente:*

1. $\varphi(e) = e'$, *donde* e *y* e' *son las identidades en* G_1 *y* G_2 *respectivamente.*
2. *Si* $a \in G_1$, *entonces* $\varphi(a^{-1}) = \varphi(a)^{-1}$.
3. *Si* $a \in G_1$ *y* $n \in Z$, *entonces* $\varphi(a^n) = \varphi(a)^n$.

Definición 5 *Un homomorfismo φ de un grupo G_1 en un grupo G_2 se llama:*
a) Monomorfismo si φ es inyectiva.
b) Epimorfismo si φ es sobre.
c) Isomorfismo si φ es inyectiva y sobre.

Definición 6 *Si G_1 y G_2 son grupos y existe un isomorfismo entre ellos, se dice que los grupos G_1, G_2 son isomorfos y se denota por $G_1 \simeq G_2$.*

Definición 7 *Un automorfismo de un grupo G es un isomorfismo de G en G.*

Los automorfismos de un grupo G forman un grupo bajo la operación de composición de funciones que se denota por $Aut(G)$.

Definición 8 *Si φ es un homomorfismo de G_1 en G_2, el núcleo de φ, denotado por $N(\varphi)$ se define por*

$$N(\varphi) = \{a \in G_1 \mid \varphi(a) = e' \text{ con } e' \text{ la identidad en } G_2\}.$$

Definición 9 *Un grupo G que satisface que $ab = ba$ para todo $a,b \in G$, se llama un grupo abeliano. Este nombre es en memoria del matemático Niels Henrik Abel.*

El conjunto Z de los enteros con la operación binaria de suma de enteros es un grupo abeliano.

Recordemos que si $n \geq 2$ y a, b son enteros, entonces a congruente con b módulo n, denotado por $a \equiv b \pmod{n}$, significa que n es un divisor de $b - a$.

Definición 10 *Si* $a \in Z$,

$$[a] = \{b \in Z | b \equiv a \,(\mathrm{mod}\, n)\} = \{a + kn | k \in Z\}\,.$$

$[a]$ se le llama la clase de congruencia de a módulo n.

Al conjunto Z_n de todas las congruencias módulo n, se le llama el conjunto de *enteros módulo* n, y es un grupo abeliano con la siguiente operación $[a] + [b] = [a + b]$, donde $[0]$ es el idéntico y $-[a] = [-a]$ es el inverso de $[a]$. Si en Z_n se define $[a][b] = [ab]$, se prueba fácilmente que esta operación está bien definida, al igual que la operación suma. Además se cumple que si $[a], [b], [c] \in Z_n$, entonces:

1. $([a][b])[c] = [a]([b][c])$.
2. $[a][1] = [a]$.
3. $[a][b] = [b][a]$.
4. $[a]([b] + [c]) = [a][b] + [a][c]$.

Por lo que se dice que Z_n con la operación de suma y multiplicación definidas anteriormente es un anillo conmutativo con identidad.

Si k es un campo, el conjunto de todas las matrices no singulares $n \times n$ con entradas en el campo k es un grupo bajo la operación de multiplicación de matrices, denotado por $GL(n, k)$ y se llama el *grupo lineal general* de tamaño n sobre k.

Si $n \geq 2$, $GL(n, k)$ es un grupo no abeliano; si $n = 1$, $GL(1, k)$ es un grupo abeliano y este es el grupo multiplicativo $k^{\times}$ de K que es el conjunto de todos los elementos no cero en k.

Si R es un anillo con identidad 1, un elemento u es unidad en R si existe $v \in R$ tal que $uv = vu = 1$. Es facil probar que si a y u son unidades, au también es unidad en R. El conjunto de unidades en R, denotado por $U(R)$, es un grupo con respecto al producto de R. Si R es un campo k, $U(k) = k^{\times}$. Si R es el anillo de todas las matrices $n \times n$ sobre un campo k, $U(R) = GL(n, k)$.

Definición 11 *Si G es un grupo y $S_1, S_2 \subset G$, $S_1S_2 = \{xy \mid x \in S_1,\ y \in S_2\}$.*

Si G es un grupo y $S_1, S_2, S_3 \subset G$, entonces $(S_1S_2)\,S_3 = S_1\,(S_2S_3)$.

Definición 12 *Se dice que un subconjunto H de G es un subgrupo de G si H es un grupo con la misma operación de G. Si H es un subgrupo de G escribimos $H < G$.*

Teorema 13 *Si M y N son subgrupos de G, MN es un subgrupo de G si y sólo si $MN = NM$.*

Teorema 14 *Sea G un grupo finito. Si H y K son subgrupos de G, entonces*

$$|HK| = \frac{|H|\,|K|}{|H \cap K|}.$$

Definición 15 *Si $X \subset G$, el subgrupo generado por X es el mínimo subgrupo de G que contiene a X y se denota por $\langle X \rangle$.*

Se prueba fácilmente que si $X \subset G$, $\langle X \rangle$ es la intersección de todos los subgrupos de G que contienen a X. Si $X = \emptyset$, $\langle X \rangle = \{e\}$ y si $\langle X \rangle \neq \emptyset$, $\langle X \rangle = \{a_1^{n_1}a_2^{n_2}\cdots a_s^{n_s} | s \geq 1,\ a_1, a_2, \cdots, a_s \in X$ y $n_1, n_2, \cdots, n_s \in Z\}$. En particular si $X = \{a\}$, $\langle X \rangle = \{a^m \mid m \in Z\}$ y en este caso en lugar de escribir $\langle \{a\} \rangle$ se escribe $\langle a \rangle$.

Definición 16 *Se dice que un grupo G es cíclico si y sólo si existe $a \in G$ tal que $G = \langle a \rangle$. Si $G = \langle a \rangle$ se dice que a genera a G.*

Teorema 17 *Dos grupos cíclicos G_1 y G_2 son isomorfos si y sólo si tienen el mismo orden.*

Teorema 18 *Si G es un grupo cíclico de orden n, $Aut(G) \simeq U(Zn)$. En particular si n es un primo p $Aut(G) \simeq U(Zp)$, el cual es un grupo cíclico de orden p-1.*

Definición 19 *Sea G un grupo y $a \in G$. El orden de a es el orden de $\langle a \rangle$, y se denota por $ord(a)$ o $|a|$.*

Obsérvese que $\langle a \rangle$ es finito o infinito. Si $\langle a \rangle$ es de orden finito e igual a n, $\langle a \rangle$ es isomorfo a Z_n. Si $\langle a \rangle$ es infinito, $\langle a \rangle$ es isomorfo a Z y en este caso se dice que a es de orden infinito.

Teorema 20 *Sea G un grupo y $a \in G$, entonces a tiene orden finito n si y sólo si n es el menor entero positivo tal que $a^n = e$ y si $a^m = e$, se tiene que n divide a m.*

Teorema 21 *Sean G_1, G_2 grupos y $\varphi : G_1 \longrightarrow G_2$ un homomorfismo. Si $a \in G_1$ es de orden finito, entonces el orden de $\varphi(a)$ es finito y divide al orden de a.*

Teorema 22 *Sea G un grupo, a y $b \in G$, tales que $ab = ba$. Si a es de orden m, b es de orden n y $(m,n) = 1$, entonces $c = ab$ tiene orden mn.*

Definición 23 *Si G es un grupo, $H < G$ y $a \in G$, la clase lateral izquierda aH de H en G es el conjunto $\{a\}\, H = \{ah |\ h \in H\}$ y la clase lateral derecha Ha de H en G es el conjunto $H\,\{a\}$.*

Teorema 24 *Si G es un grupo y $H < G$, entonces existe una biyección entre el conjunto de las clases laterales derechas de H en G y el conjunto de las clases laterales izquierdas de H en G.*

Teorema 25 *Si G es un grupo, $H < G$ y $a, b \in G$, entonces existe una biyección de Ha en Hb.*

Teorema 26 *Si G es un grupo, $H < G$ y $a, b \in G$ se tiene que:*

1. *$aH = bH$ si y sólo si $b^{-1}a \in H$.*
   $Ha = Hb$ si y sólo si $ab^{-1} \in H$.
2. *$aH = bH$ o $aH \cap bH = \emptyset$.*
   $Ha = Hb$ o $Ha \cap Hb = \emptyset$.
3. *G es la unión de las clases laterales derechas (o izquierdas) de H en G.*

Nótese que $b \in aH$ si y sólo si $b = ah$ para alguna $h \in H$, o si y sólo si $a^{-1}b \in H$.

Definición 27 *Si G es un grupo finito y $H < G$, el índice de H en G es el número de clases laterales izquierdas (o derechas) de H en G y se denota por $[G : H]$.*

Teorema 28 (*Teorema de Lagrange*).
Sea G un grupo finito de orden n y $H < G$, entonces $[G : H] = |G|/|H|$.

Teorema 29 *Si $K \leq H \leq G$ y $[H : K]$, $[G : H]$ son finitos entonces*

$$[G : K] = [G : H]\,[H : K].$$

Corolario 30 *Si G es un grupo finito y $a \in G$, el orden de a divide al orden de G.*

Corolario 31 *Si G es un grupo finito de orden p con p un primo, entonces G no contiene subgrupos propios, es decir, los únicos subgrupos de G son él mismo y la identidad.*

Inversamente, si G es un grupo con más de un elemento y no tiene subgrupos propios, entonces G es un grupo de orden un primo p. En efecto, si existe $e \neq b \in G$, el subgrupo generado por b no es la identidad y en consecuencia $G = \langle b \rangle$; b es de orden finito, ya que de lo contrario b^2 genera un subgrupo propio de G. Si b es de orden n y si n no es primo, $n = rs$ con $1 < r < n$ y $1 < s < n$, y b^r genera un subgrupo propio de G de orden s, lo cual es una contradicción, por lo tanto n es primo.

Los últimos dos resultados se pueden enunciar de la siguiente manera:

Teorema 32 *Sea G un grupo con $|G| > 1$. Los únicos subgrupos de G son él mismo y la identidad si y sólo si G es un grupo de orden primo.*

Teorema 33 *(Teorema de Fermat).*
Si a, $p \in Z$ con p un primo tal que $p \nmid a$, entonces $p \mid (a^{p-1} - 1)$, es decir, $a^p \equiv a \pmod{p}$.

Definición 34 *La función φ de Euler, se define mediante:*

$$\varphi(n) = \left\{ \begin{array}{c} 1 \text{ si } n = 1 \\ |\{k : 1 \leq k \leq n \text{ y } (k,n) = 1\}| \end{array} \right\}.$$

Si p es un primo $\varphi(p) = p - 1$.

Teorema 35 *Si $G = \langle a \rangle$ es de orden rs, donde $(r,s) = 1$, entonces existen $b, c \in G$ únicos de orden r y s respectivamente tales que $a = bc$.*

Teorema 36 *Si $n \in Z$, $n > 0$ y $n = rs$ con $(r,s) = 1$, entonces* $\varphi(n) = \varphi(r)\varphi(s)$.

Demostración. Sea $G = \langle a \rangle$, a de orden n, $n = rs$ con $(r,s) = 1$, entonces $H = \langle a^r \rangle$ es un subgrupo de G de orden s y $H = \langle a^s \rangle$ es un subgrupo de G de orden r y como H tiene $\varphi(s)$ generadores, K tiene $\varphi(r)$ generadores y G tiene $\varphi(n)$ generadores, luego si b genera a H y c genera a K, bc genera a G, por lo tanto $\varphi(r)\varphi(s) = \varphi(n) = \varphi(rs)$. ∎

Definición 37 *Un subgrupo H de G es normal si $gHg^{-1} = H$ para toda $g \in G$, y se denota como $H \lhd G$.*

Teorema 38 *Sea G un grupo y $H < G$. Las siguientes condiciones son equivalentes:*

1. $H \lhd G$.
2. $aH = Ha$ *para toda* $a \in G$.
3. $a^{-1}Ha \subset H$ *para toda* $a \in G$.
4. *Para toda* $a \in G$, $h \in H$ *existe* $h_1 \in H$ *tal que* $ah = h_1 a$.
5. *Para toda* $a, b \in G$, $HaHb = Hc$ *para alguna* $c \in G$.

En particular, si G es un grupo con M y N subgrupos de G y $M \lhd G$ o $N \lhd G$ entonces $MN < G$. Además, si $M \lhd G$ y $N \lhd G$, entonces $MN \lhd G$.

Teorema 39 *Si G es un grupo y $H < G$ de índice 2, entonces $H \lhd G$.*

Definición 40 *Sea G un grupo. El centro de G es el conjunto*

$$Z(G) = \{z \in G \mid zx = xz \text{ para todo } x \in G\}.$$

Obsérvese que $Z(G)$ es un subgrupo normal de G.

Definición 41 *Si $a, b \in G$, el elemento $aba^{-1}b^{-1}$ denotado por $[a,b]$ es llamado el conmutador de los elementos a y b. El subgrupo generado por todos los conmutadores de G es llamado el subgrupo conmutador de G o el subgrupo derivado de G y es denotado por G' o $G^{(1)}$.*

Se sigue de la definición que $G' = \{e\}$ si y solo si G es abeliano.

Definición 42 *Un subgrupo H de un grupo G se llama característico si $\varphi(H) \subset H$ para todos los automorfismos φ de G y escribimos H car G.*

Se prueba que si H car G entonces $H \lhd G$ y si M, N son subgrupos característicos de G, MN car G.

Teorema 43 *Si G es un grupo y G' el subgrupo derivado de G, G' es característico y en consecuencia normal en G.*

Definición 44 *Un grupo G es simple si no tiene subgrupos normales propios no triviales.*

Teorema 45 *Si G es un grupo cíclico finito y $H < G$, H car G.*

Teorema 46 *Sea G un grupo, M y N son subgrupos de G. Si M car N y $N \lhd G$, entonces $M \lhd G$.*

En general si M y N son subgrupos de G, $M \lhd N$ y $N \lhd G$ no necesariamente $M \lhd G$. Adelante daremos un ejemplo.

Si G es un grupo, M y N son subgrupos de G y se tiene que:

1. $M \lhd G$, $N \lhd G$,
2. $MN = G$,
3. $M \cap N = \{e\}$,

entonces G es isomorfo a $M \times N$ y se dice que G es el *producto directo* de los subgrupos M y N.

Inversamente, si G_1 y G_2 son grupos, $G = G_1 \times G_2$, $\overline{G_1} = \{(a, e_2) \,|\, a \in G_1\}$, $\overline{G_2} = \{(e_1, b) \,|\, b \in G_1\}$ y se cumplen:

1. $\overline{G_1} \lhd G, \overline{G_2} \lhd G$,
2. $\overline{G_1}\ \overline{G_2} = G$ y
3. $\overline{G_1} \cap \overline{G_2} = \{(e_1, e_2)\}$, entonces en este caso

G es el *producto directo* de los subgrupos G_1 y G_2.

Definición 47 *Si G es un grupo y $M \lneqq G$, se dice que M es un subgrupo maximal de G si no existe $N \lneqq G$ que contenga propiamente a M.*

Definición 48 *Un subgrupo normal M de un grupo G es normal maximal, si no es igual a G y no existe un subgrupo normal propio N de G que contenga propiamente a M.*

Teorema 49 *Si G es un grupo y $H \lhd G$, el conjunto de las clases laterales derechas (o izquierdas) de H en G es un grupo con respecto a la operación $HaHb = Hab$. A este grupo se le conoce como el grupo cociente de G con respecto de H y se denota por G/H.*

Teorema 50 *Si G es un grupo cíclico y $H \lhd G$, entonces G/H es cíclico.*

Teorema 51 *Si G es un grupo no abeliano, entonces $G/Z(G)$ no es cíclico.*

Definición 52 *Si H es un subgrupo de G el normalizador de H en G es el conjunto*

$$N_G(H) = \left\{a \in G \mid a^{-1}Ha = H\right\}.$$

Nótese que $N_G(H) < G$ y claramente $H \lhd N_G(H)$.

Definición 53 *Sea G un grupo, para $a \in G$ el centralizador de a en G es el conjunto*

$$C_G(a) = \{x \in G \mid ax = xa\}$$

Obsérvese que $C_G(a)$ es un subgrupo de G.

Definición 54 *Sea G un grupo y a, b elementos cualesquiera de G. Se dice que a y b son conjugados si existe x en G tal que $b = x^{-1}ax$.*

Teorema 55 *Sea G un grupo finito y $a \in G$, entonces el número de conjugados distintos de a en G es $[G : C_G(a)] = |G| / |C_G(a)|$.*

Teorema 56 *Sea G un grupo y $N < G$. $N \lhd G$ y G/N es abeliano si y sólo si $G' < N$.*

Teorema 57 *Si G es un grupo y $N \lhd G$, el homomorfismo canónico (o natural) $\varphi : G \longrightarrow G/N$ dado por $\varphi(a) = aN$, es un epimorfismo.*

Teorema 58 *(Primer Teorema de Isomorfismo).*

Sean G y G_1 grupos y $\varphi : G \longrightarrow G_1$ un homomorfismo con nucleo K. Existe un monomorfismo $\gamma : G/K \longrightarrow G_1$ definido por $\gamma(Ka) = \varphi(a)$ y resulta que G/K es isomorfo a la imagen de φ.

Teorema 59 *(Segundo Teorema de Isomorfismos).*

Sea G un grupo, H y N subgrupos de G, con $N \lhd G$. Entonces

$$(HN)/N \simeq H/(H \cap N).$$

Teorema 60 *(Tercer Teorema de Isomorfismos).*

Sea G un grupo, $H \lhd G$, $K \lhd G$ y $K \leq H$. Entonces

$$G/H \simeq (G/K)(H/K).$$

Teorema 61 *(Teorema de la Correspondencia).*

Sea G un grupo, $K \lhd G$ y sea $\gamma : G \longrightarrow G/K$ el homomorfismo natural. Entonces $\varphi : S \longrightarrow \gamma(S) = S/K$ es una biyección de la familia de todos los subgrupos de G que contienen a K a la familia de todos los subgrupos de G/K.

Más aún, si denotamos S/K por S^*, entonces:

(i) $T \leq S$ si y sólo si $T^* \leq S^*$ y en este caso $[S : T] = [S^* : T^*]$.

(ii) $T \lhd S$ si y sólo si $T^* \lhd S^*$ y en este caso $S/T \simeq S^*/T^*$.

Definición 62 *Si p es un número primo, un grupo G se dice que es un p-grupo si cada elemento de G tiene como orden alguna potencia de p. Si $H < G$, H es un p-subgrupo de G si H es un p-grupo.*

Definición 63 *Si G es un grupo abeliano, p un número primo y $x^p = e$ para toda $x \in G$, se dice que G es abeliano elemental.*

Definición 64 *Sea G un grupo. Se dice que H es un subgrupo de Sylow de G si H es un p-subgrupo maximal para algún primo p, es decir, H es un p-subgrupo de G y no existe otro p-subgrupo K de G que contenga propiamente a H.*

Si G es un grupo finito de orden $p^n \cdot s$ y $p \nmid s$, entonces los subgrupos de G de orden p^n son subgrupos de Sylow de G y se les llama *$p-$ subgrupos de Sylow de G.*

Teorema 65 *(Primer Teorema de Sylow).*
Sea G un grupo finito y p un número primo. Si G es de orden $n = p^m s$ donde $p \nmid s$, para cada $i = 1, 2, \cdots, m$ G contiene al menos un subgrupo de orden p^i, y cada subgrupo de orden p^i, $i = 1, 2, \cdots, m-1$, es un subgrupo normal de al menos un subgrupo de orden p^{i+1}.

Teorema 66 *(Segundo Teorema de Sylow).*
Sea G un grupo finito y p un número primo. Los p-subgrupos de Sylow de G son conjugados, es decir si S_1, S_2 son p-subgrupos de Sylow de G, existe $x \in G$ tal que $S_2 = x^{-1} S_1 x$.

Teorema 67 *(Tercer Teorema de Sylow).*
Sea G un grupo finito, p un número primo y r el número de p-subgrupos de Sylow de G, entonces $r \equiv 1 \pmod{p}$ y r es un divisor del orden de G.

Definición 68 *Una serie normal de un grupo G es una sucesión finita de subgrupos normales de G, H_0, H_1, H_2, $H_3, \cdots, H_n$ tal que $H_0 = \{e\}$, $H_n = G$ y $H_i \lhd H_{i+1}$ es decir,*

$$\{e\} = H_0 \lhd H_1 \lhd \cdots \lhd H_n = G.$$

Definición 69 *Un grupo G es soluble si tiene una serie normal*

$$\{e\} = H_0 \lhd H_1 \lhd \cdots \lhd H_n = G$$

con los grupos cocientes H_{i+1}/H_i abelianos para $i = 0, 1, 2, \cdots, n-1$.

Se sigue de la definición que si G es un grupo abeliano, G es soluble.

Teorema 70 *Sea G un grupo soluble, se tiene que:*
a) si $H < G$, entonces H es soluble.
b) si $H \lhd G$, entonces G/H es soluble.

Teorema 71 *Si G es un grupo y $H \lhd G$, entonces G es soluble si tanto H como G/H son solubles.*

Teorema 72 *Si G es un grupo con $M \lhd G$, $N \lhd G$, M y N solubles, entonces MN es soluble.*

Teorema 73 *Si N y M son dos grupos solubles, entonces $M \times N$ es soluble.*

Definición 74 *Un grupo finito G es nilpotente si es producto directo de sus subgrupos de Sylow.*

Teorema 75 *Si un grupo G es abeliano, entonces G es nilpotente.*

Teorema 76 *Sea G un grupo nilpotente, se tiene que:*
a) si $H < G$, entonces H es nilpotente,
b) si $H \lhd G$, entonces G/H es nilpotente,
c) si $G \neq 1$, entonces $Z(G) \neq 1$,
d) G es soluble.

Teorema 77 *Si G es un grupo nilpotente, entonces cada subgrupo maximal H de G es normal y tiene índice un primo p.*

Teorema 78 *Sea G un grupo nilpotente, si $H \lhd G$, no trivial, entonces $H \cap Z(G) \neq 1$, y si $A \lhd G$ maximal y abeliano , entonces $A = C_G(A)$.*

Teorema 79 *Si G es un grupo con $M \lhd G$, $N \lhd G$, N y M nilpotentes entonces MN es nilpotente.*

Teorema 80 *Si M y N son dos grupos nilpotentes, entonces $M \times N$ es nilpotente.*

Definición 81 *Un grupo G es supersoluble si tiene una serie normal*
$G = A_0 \rhd A_1 \rhd \cdots \rhd A_n = \langle 1 \rangle$ tal que $A_i \,/\, A_{i+1}$ es cíclico para $i = 0, 1, \cdots, (n-1)$.

Teorema 82 *Si G es un grupo supersoluble y*
a) si $H < G$, entonces H es supersoluble,
b) si $H \lhd G$, entonces G/H es supersoluble.

Teorema 83 *Si G es un grupo, con $M \lhd G$, M es cíclico y G/M es supersoluble, entonces G es supersoluble.*

Teorema 84 *Si G es un p-grupo, entonces G es supersoluble.*

Teorema 85 *Si G es un grupo nilpotente, entonces G es supersoluble.*

Teorema 86 *Si G es un grupo finito supersoluble y p un divisor primo del orden de G, entonces G tiene al menos un subgrupo de índice p.*

Teorema 87 *Si G es un grupo finito supersoluble de orden n y si m es un divisor de n, entonces G contiene al menos un subgrupo normal de orden m.*

Teorema 88 *Si G es un grupo finito supersoluble de orden $p_1^{r_1}p_2^{r_2}\cdots p_k^{r_k}$ con $p_1 > p_2 > \cdots > p_k$ números primos, entonces G tiene al menos un subgrupo normal de orden $p_1^{r_1}$.*

Teorema 89 *Sea G un grupo finito, p el menor primo que divida al orden de G y H un subgrupo de G de índice p. Entonces H es normal en G.*

Capítulo 2

Grupos cíclicos finitos.

Teorema 90 *Sea G un grupo cíclico. Si $H < G$, entonces H es cíclico.*

Teorema 91 *Sea G un grupo finito de orden n, $G = \langle a \rangle$. Entonces se cumple lo siguiente:*

(1) *si $1 \leq r$ y $r \mid n$, entonces a^r es de orden n/r,*

(2) *si $k \in Z$ y $d = (n,\ k)$, entonces $\langle a^k \rangle = \langle a^d \rangle$, con a^k de orden $n/d = n/(n,k)$,*

(3) *si $s \mid n$ con $1 \leq s$, entonces G tiene uno y sólo un subgrupo de orden s,*

(4) *el número de generadores de G es $\varphi(n)$, con φ la función de Euler.*

Demostración.

Demostración de (1). Como $n = rs$, $n/r = s$ y a^r tiene orden s, en efecto $(a^r)^s = a^{rs} = a^n = e$, si $(a^r)^t = e$, entonces $rs \mid rt$ y $s \mid t$ lo que implica que el orden de a^r es $n/r = s$.

Demostración de (2). Sea $k = dk_1$, $a^k = a^{dk_1} = \left(a^d\right)^{k_1}$, por consiguiente $\langle a^k \rangle < \langle a^d \rangle$, como $d = nu + kv$ con $u,\ v \in Z$, $a^d = a^{nu+kv} = a^{nu} \cdot a^{kv} = a^{kv} = \left(a^k\right)^v$, lo que implica que $\langle a^d \rangle < \langle a^k \rangle$, por lo tanto $\langle a^k \rangle = \langle a^d \rangle$, y $|a^k| = |a^d| = n/d$.

Demostración de (3). Como $s \mid n$, $n = rs$ con $1 \leq s$ y $1 \leq r$, por (1) a^r genera un subgrupo de G de orden s. Supóngase que $H < G$ de orden s, $H = \langle a^k \rangle$ para alguna $k \in Z$. Si $d = (n,k)$ por (2), $\langle a^k \rangle = \langle a^d \rangle$, pero a^d es

de orden $n/d = s$, por lo tanto $n = ds$, $rs = ds$ y $r = d$, por consiguiente $H = \langle a^k \rangle = \langle a^d \rangle = \langle a^r \rangle$.

Demostración de (4). Si $1 = d = (n,k)$, entonces $|a^k| = |a^d| = n/(n,k) = n$, en consecuencia a^k genera a G, y como $\varphi(n) = \{k : 1 \leq k \leq n \text{ y } (k,n) = 1\}$, se tiene que el número de generadores de G es $\varphi(n)$. ■

Lema 92 *Si G es un grupo, $\mathbf{C}$ la colección de todos los subgrupos cíclicos de G y para cada $C \in \mathbf{C}$ $genC = \{x \in G | \langle x \rangle = C\}$, entonces $\{genC | C \in \mathbf{C}\}$ es una partición de G.*

Demostración. Por demostrar que $G = \bigcup_{C \in \mathbf{C}} genC$. Si $x \in G$, $x \in genC$ lo que implica que$x \in \bigcup_{C \in \mathbf{C}} genC$ y $G \subset \bigcup_{C \in \mathbf{C}} genC$.

Inversamente si $x \in \bigcup_{C \in \mathbf{C}} genC$, $x \in G$, y $G = \bigcup_{C \in \mathbf{C}} genC$.

Si $x \in genC_1 \cap genC_2$, $\langle x \rangle = C_1$ y $\langle x \rangle = C_2$, por lo tanto $C_1 = C_2$, en consecuencia $genC_1 = genC_2$ y $\{genC | C \in \mathbf{C}\}$ es una partición de G. ■

Teorema 93 *Si n es un entero positivo, entonces $n = \sum_{d/n} \varphi(d)$, donde la suma es sobre todos los divisores d de n con $1 \leq d \leq n$, y φ la función de Euler.*

Demostración. Sea G un grupo cíclico de orden n, por cada divisor d de n, G tiene sólo un subgrupo cíclico de orden d y cada subgrupo de G tiene $\varphi(d)$ generadores, si $\mathbf{C}$ es la colección de subgrupos cíclicos de G, como $\{genC | C \in \mathbf{C}\}$ es una partición de G, $n = |G| = \sum_{C \in \mathbf{C}} |genC| = \sum_{d/n} \varphi(d)$. ■

Corolario 94 *Si F es un campo y G es un subgrupo finito de F^x, entonces G es cíclico.*

Demostración. Sea $|G| = n$ y $d \mid |G|$, G tiene a lo más un subgrupo de orden d, porque el polinómio $x^d = 1$ tiene a lo más d raíces en F^x, lo que implica que G es cíclico. ■

Corolario 95 *Si F es un campo finito, entonces F^x es cíclico.*

2.1 Una caracterización de los grupos cíclicos.

Teorema 96 *Sea G un grupo finito de orden n, si por cada divisor d de n G tiene sólo un subgrupo de orden d, entonces G es cíclico.*

Demostración. Por cada divisor d de n, G tiene sólo un subgrupo de orden d. Si para algún divisor d de n, G no tuviera un subgrupo cíclico de orden d y considerando que $G = \bigcup_{C \in \mathbf{C}} genC$, entonces

$$n = |G| = \sum_{C \in \mathbf{C}} |genC| < \sum_{d/n} \varphi(d) = n,$$

lo que es un absurdo, por lo tanto G tiene un subgrupo cíclico por cada divisor de n, en particualr para n y se tiene que G es cíclico. ■

Teorema 97 *Sea p un primo, un grupo G de orden p^n es cíclico si y sólo si G es abeliano con un único subgrupo de orden p.*

Demostración. Supóngase que G es un grupo cíclico de orden p^n, entonces existe un único subgrupo de orden d para cada divisor d de n, en particular para $d = p$, por lo tanto G es abeliano y tiene un único subgrupo de orden p.

Inversamente, sea G un grupo abeliano de orden p^n con un único subgrupo H de orden p y $a \in G$ un elemento de orden máximo en G, digamos p^k, entonces $g^{p^k} = 1$ para todo $g \in G$. Si $\langle a \rangle$ fuera un subgrupo propio de G, existe $x \in G$ tal que $x \notin \langle a \rangle$, $\langle x \rangle \cap \langle a \rangle \neq \{e\}$ ya que G tiene sólo un subgrupo de orden p, de donde $x^s \in \langle a \rangle$. Sea r el entero positivo más grande tal que $y = x^r \notin \langle a \rangle$ como $r < pr$, $y^p = x^{pr} \in \langle a \rangle$, por lo tanto existe $y \in G - \langle a \rangle$ tal que $y^p \in \langle a \rangle$, si $k = 1$, $y^p = a^l = 1$ y $y \in H$ pero $H < \langle a \rangle$ entonces $y \in \langle a \rangle$, lo cual es una contradicción, así $k > 1$ y $1 = y^{p^k} = (y^p)^{p^{k-1}} = \left(a^l\right)^{p^{k-1}}$. Como a es de orden p^k, p^k divide a lp^{k-1} y $p^k m = lp^{k-1}$ para algun entero m por lo que $l = pm$ y $y^p = a^{mp}$. Por ser G abeliano, $1 = y^{-1}a^{mp} = (y^{-1}a^m)^p$, lo cual implica que $y^{-1}a^m \in H < \langle a \rangle$ y se tiene que $y \in \langle a \rangle$ lo cual es un absurdo. Por lo tanto $G = \langle a \rangle$ es cíclico. ■

Se puede observar que si G es un grupo cíclico de orden pq con p y q primos diferentes, entonces existen subgrupos H y K de G de orden p y q

respectivamente. Entonces en el teorema anterior la hipótesis que G sea de orden p^n es necesaria, ya que existen grupos cíclicos que tiene dos subgrupos de orden primo.

2.2 Otra caracterización de los grupos cíclicos.

Teorema 98 *Sea G un grupo finito y $G \neq \{e\}$. G es cíclico si y sólo si existe un subgrupo cíclico A de G que satisface las siguientes tres condiciones:*

(1) Para cada $y \in G$ el orden de y divide al orden de A.

(2) $\langle y \rangle \cap A \neq \{e\}$ para cada $y \in G$, con $y \neq e$.

(3) $A \subset Z(G)$.

Demostración. Si G es cíclico, $A = G$ cumple con (1), (2) y (3).

Inversamente, supóngase que existe $A < G$ tal que A es cíclico y se cumplen (1), (2) y (3). Se demostrará que $G = A$.

Supóngase que $G - A \neq \emptyset$. Sea $x \in G - A$ de orden mínimo en G. Se afirma que x no es de orden primo. En efecto, ya que $\{e\} \neq \langle x \rangle \cap A \subsetneq \langle x \rangle$, se tiene que el orden de $(\langle x \rangle \cap A)$ divide al orden de x donde el orden de $(\langle x \rangle \cap A)$ es distinto de uno y del orden de $\langle x \rangle$.

Sea p un primo que divida al orden de x. Como el orden de x divide al orden de a, p divide al orden de A, además $e \neq x^p \in A = \langle a \rangle$ porque el orden de x^p es menor que el orden de x, por lo tanto $x^p = a^r$ para alguna r, $1 \leq r < |A| = m$.

Como el orden de x divide a m, $e = (x^p)^{m/p} = (a^r)^{m/p} = a^{r(m/p)}$, lo que implica que $|A|$ divide a $r(m/p)$, esto es $mt = r(m/p)$ y $pt = r$.

Sea $y = xa^{-t}$, como $x \notin A$, $y \notin A$, por lo tanto $\langle y \rangle \cap A \subsetneq \langle y \rangle$ y el orden de $(\langle y \rangle \cap A)$ divide al orden de y. Como $\{e\} \neq \langle y \rangle \cap A$, el orden de $(\langle y \rangle \cap A)$ divide al orden de y, por lo que el orden de $(\langle y \rangle \cap A)$ es distinto de uno y del orden de $\langle y \rangle$. Ya que el orden de $\langle y \rangle \cap A$ divide al orden de y, se tiene que y no es de orden primo.

Por otro lado se tiene que $y^p = x^p (a^{pt})^{-1} = x^p (a^r)^{-1} = a^r (a^r)^{-1} = e$, es decir, y es de orden primo y se tiene una contradición. Por lo tanto $G - A = \emptyset$, $G = A$ y G es cíclico. ∎

Veamos que con esta caracterización de los grupos cíclicos, podemos dar otra demostración del teorema 94.

Corolario 99 *(Teorema 94) Sea p un primo, un grupo G de orden p^n es cíclico si y sólo si G es abeliano con un único subgrupo de orden p.*

Demostración. Si G es cíclico, G es abeliano y por el teorema 95 G tiene sólo un subgrupo de orden p.

Inversamente, supóngase que $|G| = p^n$, G abeliano y G sólo tiene un subgrupo de orden p, veamos que se cumplen las tres condiciones del Teorema 95.

Sea $a \in G$, de orden máximo y $A = \langle a \rangle$, tal que el orden de a sea p^m, si $y \in G$ y el orden de y es p^k con $k \leq m$, se tiene que $k + s = m$ con $s \geq 0$, entonces $p^k p^s = p^m$ y el orden de y divide al orden de a, por lo tanto se cumple (1).

Sea $y \in G$, $y \neq e$, tal que el orden de y es p^kcon $0 < k$ y $H = \langle y \rangle$, sea $K < H$ de orden p, como G sólo tiene un subgrupo de orden p, $K \subset A$, por lo que $\langle y \rangle \cap A \neq e$, y se cumple (2).

Por último como $Z(G) = G$, por ser G abeliano se tiene que $A \subset Z(G)$, y se cumple (3). ■

Teorema 100 *Sea G un grupo abeliano de orden p^n con p un número primo, $a \in G$ de orden máximo en G, $A = \langle a \rangle$. Entonces $G = A \times Q$ para algún subgrupo Q de G.*

Demostración. Inducción sobre n.

Es claro que el teorema es cierto para $n = 1$ y $n = 2$.

Supóngase entonces que $2 < n$ y que el teorema es cierto para $m < n$.

Caso 1.

Para cada $y \in G$, con $y \neq e$ se tiene que $\langle y \rangle \cap A \neq \{e\}$. Como el orden de y divide al orden de A y $A \subset Z(G)$, entonces G es cíclico, de hecho $G = A$ y se tiene que $G = A \times \{e\}$.

Caso 2.

Para alguna $y \in G$, con $y \neq \{e\}$ se tiene que $\langle y \rangle \cap A = \{e\}$. Sea $H = \langle y \rangle$, $\bar{a} = aH$. Probaremos que $\bar{a}$ es de orden máximo en G/H.

Sea $m = |\bar{a}|$ y $k = |a|$. Es conocido que el orden de $\bar{a}$ divide al orden de a. Por otro lado, se tiene que $\bar{a}^m = H$, esto es $a^m H = H$ lo que implica que $a^m \in H \cap A$ y como $H \cap A = \{e\}$, $a^m = e$, por consiguiente k divide a m y $k = m$.

Si $gH \in G/H$ para alguna $g \in G$, el orden de gH divide al orden de g y como el orden de g es menor o igual k, el orden de $gH \leq k = m$

Es claro que $1 < |H| < |G|$ y consecuentemente $1 < |G/H| < |G|$.

G/H es un grupo abeliano de orden p^r, $\bar{a} = aH$ es de orden máximo en G/H, como $r < n$, si $A_1 = \langle \bar{a} \rangle$ se tiene por hipótesis de inducción que $G/H = A_1 \times T$ con $T < G/H$.

Como $T < G/H$, $T = Q/H$ con $H < Q < G$. Se puede probar fácilmente que $G = A \times Q$. ■

Teorema 101 *Si G es un grupo abeliano de orden p^n con p un número primo, entonces G es producto directo de subgrupos cíclicos.*

Demostración. Inducción sobre el orden de G.

Supóngase que G no es cíclico. Sea $a \in G$ de orden máximo y $A = \langle a \rangle$. Por el teorema anterior $G = A \times Q$ para algún subgrupo propio Q de G y por hipótesis de inducción $Q = A_1 \times A_2 \times \cdots \times A_s$ con $A_1, A_2, \cdots, A_s$ cíclicos.

Por lo tanto G es producto directo de subgrupos cíclicos. ■

Teorema 102 *Si G es un grupo abeliano finito, entonces G es producto directo de grupos cíclicos.*

Demostración. Si $\mid G \mid = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$ con p_i primos diferentes y $H_i = \{x \in G \mid x$ tiene orden alguna potencia de $p_i\}$, $H_i < G$ y resulta que $G = H_1 H_2 \cdots H_r$ y $H_i \cap H_1 H_2 \cdots H_{i-1} = \{e\}$ para toda $i = 2, 3, \cdots, r$, por lo que G es producto directo de $H_1, H_2, \cdots, H_r$ y como cada H_i es producto directo de subgrupos cíclicos, se tiene que G es producto directo de grupos cíclicos. ■

Corolario 103 *Si G es un grupo abeliano finito y $m \mid |G|$, entonces G tiene un subgrupo de orden m.*

Capítulo 3

Grupos de orden p, p^2, p^3 y pq.

3.1 Grupos de orden p y p^2.

Teorema 104 *Si G es un grupo finito de orden p, G es cíclico e isomorfo a Z_p.*

Demostración. Como G no tiene subgrupos propios, G es cíclico e isomorfo a Zp. ■

Teorema 105 *Si p es un número primo, entonces cada grupo de G de orden p^2 es abeliano, e isomorfo a $Z_p \times Z_p$ ó Z_{p^2}.*

Demostración. Sea G un grupo de orden p^2, supóngase que G no es abeliano, como $Z(G) \neq 1$, $|Z(G)| = p$, y $|G/Z(G)| = p$ por lo tanto $G/Z(G)$ es cíclico, lo cual no puede ser ya que G no es abeliano. Por lo que G es abeliano. Si G tiene un elemento a de orden p^2, entonces $G = \langle a \rangle$ y es isomorfo a Z_{p^2}. Si G no tiene ningún elemento de orden p^2, sean $a, b \in G$ de orden p, tales que $b \notin \langle a \rangle$. Si $H = \langle a \rangle$ y $K = \langle b \rangle$, $H \lhd G$, $K \lhd G$, $HK = G$ y $H \cap K = \{e\}$. Por lo tanto G es isomorfo a $H \times K$ que es isomorfo a $Z_p \times Z_p$. ■

3.2 Grupo de los Cuaternios.

Sea Q el conjunto de los elementos (x, y) tales que x pertenezca a las clases de congruencia módulo 4, y pertenezca a las clases de congruencia módulo 2.

Las clases de congruencia módulo 4 sólo contiene cuatro elementos y la indicaremos mediante los simbolos $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, las clases de congruencia módulo 2, sólo contiene dos elementos y los indicaremos mediante los simbolos $\overline{0}$, $\overline{1}$. Por tanto Q consta de los siguientes elementos:

$$\{(\overline{0},\overline{0}),\ (\overline{1},\overline{0}),\ (\overline{2},\overline{0}),\ (\overline{3},\overline{0}),\ (\overline{0},\overline{1}),\ (\overline{1},\overline{1}),\ (\overline{2},\overline{1}),\ (\overline{3},\overline{1})\}.$$

Definamos ahora en Q el producto de la siguiente manera:

$$(x_1,y_1)(x_2,y_2) = (x_1+x_2, y_1+y_2) \qquad \text{si } y_1 = \overline{0}.$$

$$(x_1,y_1)(x_2,y_2) = (x_1-x_2, y_1+y_2) \qquad \text{si } y_1 = \overline{1},\ y_2 = \overline{0}.$$

$$(x_1,y_1)(x_2,y_2) = (x_1-x_2+\overline{2}, y_1+y_2) \qquad \text{si } y_1 = \overline{1},\ y_2 = \overline{1}.$$

Probemos que Q es un grupo bajo la operación definida anteriormente.

Sean $(x_1,y_1),(x_2,y_2),(x_3,y_3)$, tres elementos de Q, veamos que

$$[(x_1,y_1)(x_2,y_2)](x_3,y_3) = (x_1,y_1)[(x_2,y_2)(x_3,y_3)]$$

Si $y_1 = y_2 = \overline{0}$ se verifica la igualdad, ya que de ambos lados es igual a $(x_1+x_2+x_3, y_1+y_2+y_3)$.

Si $y_1 = y_2 = \overline{1}$ también se verifica la igualdad, ya que de ambos lados es igual a $(x_1-x_2+x_3+\overline{2},\ y_1+y_2+y_3)$.

Si $y_1 = \overline{1}$, $y_2 = \overline{0}$,

$$\begin{aligned}[(x_1,y_1)(x_2,y_2)](x_3,y_3) &= (x_1-x_2-x_3, y_1+y_2+y_3)\\ &= (x_1,y_1)[(x_2,y_2)(x_3,y_3)] \ \textit{si}\ y_3 = \overline{0}.\end{aligned}$$

$$\begin{aligned}[(x_1,y_1)(x_2,y_2)](x_3,y_3) &= (x_1,y_1)[(x_2,y_2)(x_3,y_3)]\\ &= (x_1-x_2-x_3+\overline{2}, y_1+y_2+y_3) \ \textit{si}\ y_3 = 1.\end{aligned}$$

Si $y_1 = \overline{0}$, $y_2 = \overline{1}$

$$\begin{aligned}[(x_1, y_1)(x_2, y_2)](x_3, y_3) &= (x_1 + x_2 - x_3, y_1 + y_2 + y_3) \\ &= (x_1, y_1)[(x_2, y_2)(x_3, y_3)] \ \textit{si}\ y_3 = \overline{0}.\end{aligned}$$

$$\begin{aligned}[(x_1, y_1)(x_2, y_2)](x_3, y_3) &= (x_1 + x_2 - x_3 + \overline{2}, y_1 + y_2 + y_3) \\ &= (x_1, y_1)[(x_2, y_2)(x_3, y_3)] \ \textit{si}\ y_3 = \overline{1}\end{aligned}$$

$\therefore$ se cumple la igualdad.

Sea (x, y) un elemento de Q, se tiene que

$$(x, y)(\overline{0}, \overline{0}) = (x, y) = (\overline{0}, \overline{0})(x, y)$$

en consecuencia Q tiene un elemento unidad que es $(\overline{0}, \overline{0})$. Además, dado cualquier elemento (x, y) de Q siempre podremos encontrar otro elemento (x', y') de Q tal que $(x, y)(x', y') = (\overline{0}, \overline{0})$. Si $y = \overline{0}$, $(x', y') = (-x, y)$ y si $y = \overline{1}$, $(x', y') = (x + 2, y)$

Como Q cumple con (1), (2) y (3) de la definición 1, tenemos que Q es un grupo.

Q no es un grupo abeliano ya que si $a = (\overline{1}, \overline{0})$ y $b = (\overline{1}, \overline{1})$ se tiene:

$$ab = (\overline{1}, \overline{0})(\overline{1}, \overline{1}) = (\overline{2}, \overline{1}) \neq (\overline{0}, \overline{1}) = (\overline{1}, \overline{1})(\overline{1}, \overline{0}) = ba.$$

Si $H = \langle a \rangle$, $[Q : H] = 2$ por lo tanto $H \lhd Q$ y $b^{-1}ab \in H$ es de orden 4. Como $b^{-1}ab \neq a$, tendremos que $b^{-1}ab = a^3 = a^{-1}$; por otro lado $ab = ba^3 = (ba)a^2 = a^2ba$, $b = (ab)a$, $ba = (ab)a^2$ y $ba^2 = (ab)a^3$.

Así G consta de los siguientes elementos:

$$\{e,\ a,\ a^2,\ a^3,\ b,\ ab,\ a^2b,\ a^3b\}$$

Obsérvese que G está generado por los elementos a y b, los cuales cumplen las siguientes relaciones:

$$a^4 = b^4 = e,\ bab^{-1} = a^{-1} \text{ y } b^2 = a^2,$$

Como $b^2 = a^2$ conmuta con a y b, $a^2 \in Z(Q)$, por otro lado como $ab = a^2ba$, $(ab)^2 = (ab)(ab) = a(a^3b)b = b^2$ por lo tanto ab es de orden 4, como $a^2b = ba^2$, $(a^2b)^2 = b^2$ y a^2b también es de orden 4, por último como $(a^3b)^2 = (a^2(ab))^2 = (ab)^2 = b^2$, a^3b es también de orden 4.

Por lo tanto de los ocho elementos de Q, $\{a, b, b^{-1}ab, ab, a^2b, a^3b\}$ son de orden 4 y a^2 de orden 2.

Si $S < Q$ y $|S| = 4$, S es cíclico porque en caso contrario S tendría dos elementos de orden 2. Cada subgrupo S de Q es normal porque si $|S| = 4$, $[Q : S] = 2$ y en consecuencia $S \lhd Q$. Si $|S| = 2$, $S = \{e, a^2\} \subset Z(Q)$. Como Q no es abeliano $G/Z(Q)$ no es cíclico y $|Q/Z(Q)| = 4$ lo cual implica que $|Z(Q)| = 2$ por lo tanto $Z(Q) = \{1, a^2\}$. Como $G/Z(Q)$ es abeliano, $G' \leq Z(Q)$ y ya que $Q' \neq e$ porque Q no es abeliano, $Q' = Z(Q)$.

Si S, T son dos subgrupos de Q tales que $|S| = |T| = 4$ y por consiguiente maximales $ST = Q$ y $|ST| = |S|\,|T|/|S \cap T|$ entonces $|S \cap T| = 2$ y por lo tanto $S \cap T = Z(Q)$.

Entonces Q es un grupo no abeliano (no cíclico) de orden ocho con todos sus subgrupos normales propios cíclicos.

A este grupo se le conoce como el *Grupo de los cuaternios.*

Se prueba fácilmente que si G es un grupo generado por dos elementos x y z que satisfacen las relaciones $x^4 = z^4 = e$, $x^2 = z^2$, $z^{-1}xz = x^3$, entonces G es isomorfo al grupo de los cuaternios.

Teorema 106 *Si* $A = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in GL(2, C)$ *y* $G = \langle A, B \rangle$, *entonces* G *es isomorfo a* Q, *el grupo de los cuaternios.*

Demostración. G no es un abeliano ya que

$$AB = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} \neq \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = BA.$$

$$A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \text{ y } A^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I.$$

$$B^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = A^2 \text{ y } B^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = A^4 = I$$

$$A \cdot B^3 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = BA$$

Como $A \cdot B^3 = BA$ y $B^2 = A^2$, $B^{-1}AB \cdot A^2 = A$ y $B^{-1}AB = A^{-1} = A^3$. Sean $H = \langle A \rangle$ y $K = \langle B \rangle$. Entonces $HK = \{I, A, A^2, A^3, B, AB, A^2B, A^3B\}$ y $KH = \{I, B, B^2, B^3, A, BA, B^2A, B^3A\}$ veamos que $HK = KH$. Como $A^2 = B^2$, $A^3 = A^2A = B^2A$, $A^2B = B^2B = B^3$, por otro lado $B^{-1}AB = A^3$, lo cual implica que $AB = BA^3 = BB^2A = B^3A$ y$B^2AB = B^2B^3A = BA$. Por lo tanto $HK = KH$ es un grupo y $G = HK$.

Entonces $G = \{I,\ A,\ A^2,\ A^3,\ B,\ B^3,\ AB,\ BA\}$ es un grupo no abeliano, generado por A y B, los cuales satisfacen las siguientes relaciones: $A^4 = I$, $A^2 = B^2$ y $BAB^{-1} = A^3 = A^{-1}$. Por consiguiente G es isomorfo al grupo de los cuaternios. ■

3.3 Generalización de los Cuaternios.

Si M es un grupo cíclico de orden 2^{n-1} con $n \geq 3$ y $M = \langle a \rangle$. Por un teorema de *Hölder* sobre extensiones de grupos, se tiene que existe un único grupo Q_n de orden 2^n con $M < Q_n$ y necesariamente $M \lhd Q_n$. Además $Q_n/M = \langle bM \rangle$ y se cumplen las siguientes relaciones:

$$a^{2^{n-1}} = 1,\ b^2 = a^{2^{n-2}} \text{ y } bab^{-1} = a^{-1}.$$

Como $Q_n = M \cup Mb$, entonces cada elemento de Q_n es de la forma a^ib^j con $0 \leq i \leq 2^{n-1} - 1$ y $0 \leq j < 2$.

$$\left(b^2\right)^2 = \left(a^{2^{n-2}}\right)^2 = a^{2 \cdot 2^{n-2}} = a^{2^{n-1}} = 1,$$

es decir b^2 es de orden 2.

Si $x = a^ib$, $x^2 = (a^ib)^2 = a^ib \cdot a^ib = a^ib^2b^{-1}a^ib = a^ib^2a^{-i} = b^2$, lo que implica que cada elemento de Q_n que no está en M es de orden 4, por lo tanto $b^2 = a^{2^{n-2}}$ es el único elemento de Q_n de orden 2.

Para cada $n \geq 3$ el grupo anterior Q_n se llama *Grupo de los Cuaternios Generalizados.* Los elementos $a^{2^{n-2}}$ y b generan un grupo isomorfo a los cuaternios.

Si $n = 3$, $Q_3 = Q$ que es el grupo de los cuaternios.

En virtud de las observaciones anteriores podemos enunciar el siguiente teorema.

Teorema 107 *Para* $n \geq 3$, *el grupo* Q_n *de los cuaternios generalizados de orden* 2^n *tiene un único subgrupo de orden 2. Si* $n > 3$, Q_n *sólo tiene un subgrupo cíclico de orden* 2^{n-1} *y los elementos de* Q_n *que no pertenecen a M tienen orden 4.*

Se probará más adelante que si G es un $p-$ *grupo* finito con un único subgrupo de orden p, entonces G es cíclico o G es un grupo cuaternio generalizado.

3.4 Grupo de las Simetrías del cuadrado.

Si a es la rotación del plano alrededor del centro del cuadrado con $H = \langle a \rangle$ y b es la reflexión del plano sobre $\mathcal{L}_1$ con $K = \langle b \rangle$ (figura 3.1), se puede probar que HK son todos los movimientos rigidos del plano que dejan fijo al cuadrado.

$D_8 = HK$ es un grupo de orden 8, llamado el *Grupo Diedrico de orden* 8.

Como $|H| = 4$, $[D_8 : H] = 2$ en consecuencia $H \lhd D_8$ y $H \cap K = \{e\}$, donde e es la identidad en R^2. Siendo a la rotación del plano alrededor del centro del cuadrado y b la reflexión del plano sobre $\mathcal{L}_1$, entonces $ab \neq ba$ por lo tanto el grupo diedrico de orden 8 no es un grupo abeliano.

Se cumple también que $a^4 = b^2 = e$, $b^{-1}ab$ y $a \in H$ tienen el mismo orden y como $b^{-1}ab \neq a$, $b^{-1}ab = a^3$ y $ab = ba^3$, por otro lado $b^{-1} = b$ entonces $bab = a^3$ y $ba = a^3b$. Entonces D_8 está formado por los siguientes ocho elementos:

$$\left\{e,\ a,\ a^2,\ a^3,\ b,\ ab,\ a^2b,\ a^3b\right\}.$$

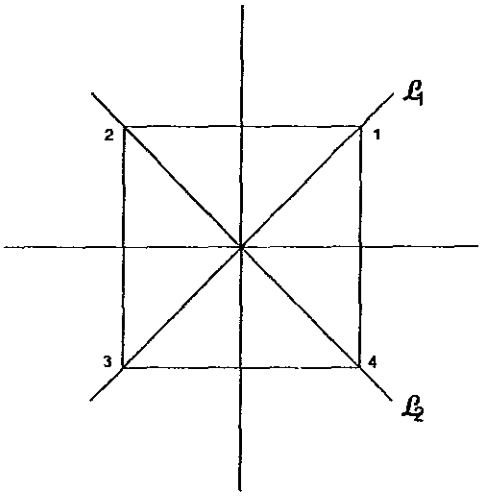

Figura 3.1:

Como a^2 conmuta con a y b, entonces $a^2 \in Z(D_8)$ y $\{e, a^2\} \subset Z(D_8)$. Razonando como en el caso de los cuaternios se tiene que $\{e, a^2\} = Z(D_8)$ y $Z(D_8) = D_8'$, y si S, T son dos subgrupos de D_8 de orden 4, $S \cap T = Z(D_8)$ y a^2, b, ab, a^2b, a^3b son elementos de orden 2, y $(ab)^2 = (ab)(ab) = aa^3b^2 = a^4b^2 = e$, por otro lado $a^3b = a^2(ab) = (ab)a^2$ en consecuencia a^3b es de orden 2. Entonces en D_8 hay cinco elementos de orden 2 y dos de orden 4.

Por lo tanto D_8 es un grupo no abeliano, generado por los elementos a y b, con a de orden 4 y b de orden 2, los cuales cumplen las siguientes relaciones $a^4 = b^2 = e$ y $b^{-1}ab = bab = a^3$.

Si $S = \{e, a^2\}$ y $T = \{e, b\}$ como $S = Z(D_8)$, ST es un subgrupo de orden 4 con $ST = \{e,\ a^2,\ b,\ a^2b\}$ que resulta normal en D_8, además $T \lhd ST$ y T no es normal de D_8, porque $a^{-1}ba = a^3ba = ba^2 \notin T$. Por lo tanto D_8 tiene subgrupos que no son normales y subgrupos normales que no son cíclicos ST.

Se puede mostrar fácilmente que si G es un grupo generado por los elementos x, z tales que $x^4 = z^2 = 1$ y $z^{-1}xz = x^3$, entonces G es isomorfo a D_8.

D_8 es un ejemplo que hace ver en general que no se cumple que si M, N son subgrupos de G tal que $N \lhd M$ y $M \lhd G$, no necesariamente $N \lhd G$.

3.5 Grupos de orden p^3.

Teorema 108 *Cualquier grupo G no abeliano de orden 2^3 es isomorfo a Q o a D_4.*

Demostración. Sea G un grupo no abeliano de orden 8. Si G tiene al menos un subgrupo S cíclico de orden 4, $S = \langle a \rangle$, sea $b \notin S$ tal que $T = \langle b \rangle$.

Si para todo elemento $b \notin S$, el orden de b es 2, y $a^4 = e$, $b^2 = e$ asi e, a, a^2, a^3, b, ab, a^2b, a^3b, son ocho elementos diferentes de G, por lo tanto $ST = G = \{e,\ a,\ a^2,\ a^3,\ b,\ ab,\ a^2b,\ a^3b\}$, como $S \lhd G$, si $ba = ab$, $b \in Z(G)$, $a \in Z(G)$ y G resultaría abeliano, lo cual no puede ser, entonces $ba \neq ab$ y en consecuencia $b^{-1}ab = a^3$. Tenemos por lo tanto que:

1. G es un grupo no abeliano de orden 8.
2. G está generado por los elementos a y b.
3. $a^4 = b^2 = 1$ y $b^{-1}ab = a^3$.

Por consiguiente G es isomorfo a D_4.

Si existe $b \in S$, tal que b es de orden 4, se tiene que G tiene dos subgrupos S y T de orden 4, con $S = \langle a \rangle$ y $T = \langle b \rangle$, tales que $a^4 = 1$, $b^4 = 1$ y $G = ST = \{e,\ a,\ a^2,\ a^3,\ b,\ ab,\ a^2b,\ a^3b\}$. Como $S \lhd G$, $b^{-1}ab = a$ o $b^{-1}ab = a^3$, si $b^{-1}ab = a$, $ab = ba$ y G resultaría abeliano, lo cual es una contradicción, por lo tanto $b^{-1}ab = a^3$.

Por otro lado $|Z(G)| = 2$ y $G/Z(G)$ no es cíclico, ya que de lo contrario G resultaría abeliano, como $|G/Z(G)| = 4$, cada elemento de $G/Z(G) \neq Z(G)$ es de orden 2, como a es de orden 4, $a \notin Z(G)$ y $aZ(G) \neq Z(HG)$, entonces $(aZ(G))^2 = Z(G)$ por lo que $a^2 \in Z(G)$. Como b^2 es de orden 2 y el único elemento de G de orden 2 es a^2 esto implica que $b^2 = a^2$. Por lo tanto:

1. G es un grupo no abeliano de orden 8.
2. G está generado por a y b.

3. $a^4 = e$, $b^4 = e$, $a^2 = b^2$ y $b^{-1}ab = a^3$.

Por consiguiente G es isomorfo a los cuaternios. ∎

Consideremos ahora G un grupo no abeliano de orden p^3, con p un primo impar. G no contiene ningún elemento de orden p^3 ya que de lo contrario G sería cíclico y en consecuencia abeliano, supongamos que G tiene un elemento a de orden p^2, asi $a^{p^2} = 1$. Si $A = \langle a \rangle$, $A \lhd G$. Como $|A| = p^2$, se tiene que $|G/A| = p$. Sea $b \in G$ tal que $b \notin A$, luego $G/A = \langle GAb \rangle$ y $(bA)^p = A$, entonces $b^p \in A$, como $[G : A] = p$ y A, Ab, Ab^2, $Ab^3, \cdots, Ab^{p-1}$, son las diferentes clases laterales derechas de A en G, G se puede ver como la unión de estas clases laterales derechas, si $x \in G$, $x \in Ab^j$ para alguna j, con $0 \leq j \leq p-1$, lo cual implica que $x = a^i b^j$, por lo tanto a y b generan a G.

Como $A \lhd G$, $b^{-1}ab = a^r$ con $1 < r \leq p^2 - 1$ ya que G no es abeliano, continuando por inducción $b^{-j}ab^j = a^{r^j}$ y $b^{-p}ab^p = a^{r^p}$, como $b^p \in A$, $b^{-p}ab^p = a$ de donde $a^{r^p} = a$ en consecuencia $r^p \equiv 1 \pmod{p^2}$ y $r^p \equiv 1 \pmod{p}$. Considerando el teorema de Fermat $r^p \equiv r \pmod{p}$ por lo que $r \equiv 1 \pmod{p}$, para alguna s, escribamos $r = 1 + sp < p^2$ entonces $0 < s < p$ y $p \nmid s$, por lo tanto $(s, p) = 1$. Como la siguiente congruencia $sx \equiv 1 \pmod{p}$ tiene solución, tomemos $j > 1$, tal que $js \equiv 1 \pmod{p}$, y

$$b^{-j}ab^j = a^{r^j} = a^{(1+sp)j}$$

Como $p > j \geq 2$, $(1 + sp)^j = 1 + jsp + p^2 m$,

$$b^{-j}ab^j = a^{r^j} = a^{(1+sp)j} = a^{1+jsp+p^2 m} = a^{1+jsp} = a^{1+p}$$

Como $(j, p) = 1$, $c = b^j \notin A$, con $c^{-1}ac = a^{1+p}$ asi G está generado por a y c y se tiene que $c^p \in A$. Como c^p está en A, $c^p = a^t$, y como c no es de orden p^3, c^p es de orden p, por lo tanto $c^p = a^{up}$.

Por otro lado a es de orden p^2 y $|Z(G)| = p$, por lo que $a \notin Z(G)$ lo cual implica que $aZ(G) \neq Z(G)$ y $(aZ(G))^p = Z(G)$, por lo tanto $a^p \in Z(G)$.

Ya que $c^{-1}ac = a^{1+p}$, $c^{-1}a^u c = a^{u(1+p)}$, esto es $a^u c = ca^{u(1+p)} = ca^u a^{up}$, y considerando que $a^p \in Z(G)$ obtenemos:

$$(ca^u)^2 = (ca^u)(ca^u) = c(a^u c)a^u = cca^{u(1+p)}a^u = c^2 a^{2u} a^{up}$$

y

$$\begin{aligned}(ca^u)^3 &= (ca^u)^2(ca^u) = c^2a^ua^ua^{up}ca^u = c^2a^ua^uca^ua^{up}\\ &= c^2a^uca^ua^ua^{up}a^{up} = c^3a^{u(1+2)}a^{3up}\end{aligned}$$

continuando por inducción,

$$(ca^u)^p = c^pa^{u(1+2+\cdots+(p-1))}a^{up^2} = c^pa^{u\frac{p(p-1)}{2}} = c^pa^{up}$$

ya que $1+2+3+\cdots+p-1 = \frac{p(p-1)}{2}$ es un múltiplo de p puesto que p es impar.

Por lo tanto $(ca^{-u})^p = c^pa^{-up} = 1$. Además, como $b_1^{-1}ab_1 = a^u(b^{-1}ab)a^{-u}$, se tiene que si G es un grupo no abeliano de orden p^3, con p un primo y $a \in G$, de orden p^2, G está generado por los elementos a y b los cuales cumplen que: $a^{p^2} = 1$, $b_1^p = 1$ y $b_1^{-1}ab_1 = a^{1+p}$.

Como un último caso supongamos que G no tiene ningún elemento de orden p^2. Como $Z(G)$ es de orden p, pues de lo contrario, si fuera de orden p^2 o mayor, el grupo sería abeliano, $G/Z(G)$ es un grupo de orden p^2, (necesariamente abeliano) y no cíclico, por lo que $G/Z(G)$ está generado por dos elementos x, y de orden p. Si en el homomorfismo canónico $\psi : G \longrightarrow G/Z(G)$ se tiene que $\psi(a) = x$, y $\psi(b) = y$, entonces $a^p = 1$, $b^p = 1$, $a^{-1}b^{-1}ab = [a,b] = c \in Z(G)$.

$G = \langle\{a,b\} \cup Z(G)\rangle$ de hecho si $g,h \in G$, $g = a^rb^sz$ con $z \in Z(G)$ y $h = a^{r'}b^{s'}z'$ con $z' \in Z(G)$, tendremos que $gh = a^rb^sa^{r'}b^{s'}zz'$, si $c = 1$, $gh = hg$ y G resultaría abeliano, entonces $c \neq 1$ y $c^p = 1$

Como $G/Z(G)$ es abeliano $aZhZ = hZaZ$, y $ahZ = haZ$ si y sólo si $a^{-1}b^{-1}ab \in Z$ por lo que $c \in Z(G)$ y como $|Z(G)| = p$, $\langle c\rangle = Z(G)$ por lo tanto $G = \langle a,b,c\rangle$ y tendremos las siguientes relaciones:

$$a^p = 1,\ b^p = 1,\ c^P = 1,\ ab = bac,\ ca = ac,\ cb = bc.$$

Teorema 109 *Sean H y K grupos y φ un homomorfismo de K en $Aut(H)$, si $k \in K$, $h \in H$ y denotamos $\varphi(k)h = h^k$ y definimos en $G = H \times K$ el producto $(h_1,k_1)(h_2,k_2) = \left(h_1 h_2^{k_1}, k_1 k_2\right)$, G resulta un grupo con (e,e) como idéntico y $\left((h^{-1})^{h^{-1}}, k^{-1}\right)$ el inverso de (h,k).*

El grupo G del teorema anterior se llama el *producto semidirecto* de H por K realizado por φ y se denota como $H \rtimes_\varphi K$.

Siguiendo la notación del teorema anterior, si $h \in H$, $k \in K$ e identificamos $(h,1)$ con h y $(1,k)$ con k se tiene que $khk^{-1} = h^k$.

Se puede observar que si φ es el homomorfismo trivial, es decir si $h^k = h$, para toda $h \in H$, entonces el producto $(h_1,k_1)(h_2,k_2) = (h_1h_2, k_1k_2)$, y $H \rtimes_\varphi K = H \times K$.

Teorema 110 *Dados K, Q grupos y $\varphi : Q \longrightarrow Aut(K)$ un homomorfismo, entonces $G = K \rtimes_\varphi Q$ es un producto semidirecto de K por Q realizado por φ.*

Construcción de grupos de orden p^3 con p un impar.

Sea p un primo, $K = \langle a,c\rangle$ un grupo abeliano elemental de orden p^2, sea $Q = \langle b\rangle$ un grupo cíclico de orden p. Sea $\varphi : Q \longrightarrow Aut(k) \simeq GL(2,p)$ un homomorfismo definido por $\varphi(b^i) = \begin{bmatrix} 1 & 0 \\ i & 1 \end{bmatrix}$.

Se tiene entonces que $a^b = ac$ y $c^b = c$, el conmutador $a^b a^{-1}$ es c y $G = K \rtimes_\varphi Q$ es un grupo de orden p^3 con $G = \langle a,b,c\rangle$, donde a, b y c, cumplen las siguientes relaciones:

$$a^p = 1,\ b^p = 1,\ c^p = 1,\ c = [a,b],\ \text{y}\ [a,b] = 1 = [c,b].$$

Si p es un primo impar, G es un grupo no abeliano de orden 8 isomorfo a D_8.

Sea p un primo impar, $K = \langle a\rangle$ un grupo cíclico de orden p^2, $Q = \langle x\rangle$ un grupo cíclico de orden p.

El grupo $Aut(K)$ es el producto directo de los subgrupos $\langle\beta\rangle$ y $\langle\alpha\rangle$ de orden $(p-1)$ y p respectivamente con $\alpha(a) = a^{1+p}$. (Ver [7], Teorema 7.3)

Si $\varphi : Q \longrightarrow Aut(k)$ es el homomorfismo tal que $\varphi(x) = \alpha$, entonces el grupo $G = K \rtimes_\varphi Q$ es no abeliano de orden p^3 y tiene las siguientes relaciones: $x^P = 1$, $a^{p^2} = 1$ y $xax^{-1} = a^x = a^{1+p}$.

3.6 Grupos de orden pq.

Teorema 111 *Si G es un grupo de orden pq, con p y q primos y $p < q$, entonces G es cíclico ó G no es abeliano*

Demostración. Supóngase que G es un grupo abeliano, sean $b \in G$ de orden p y $a \in G$ de orden q, entonces $c = ab$ es de orden pq y G resulta ser un grupo cíclico. ■

Teorema 112 *Sean p y q primos con $p < q$ y G un grupo no abeliano de orden pq. Sean $a \in G$ de orden p y $b \in G$ de orden q, si $K = \langle a \rangle$ y $H = \langle b \rangle$, entonces:*

1. $H \lhd G$.
2. $G = HK$
3. $H \cap K = \{e\}$.
4. $a^p = e$, $b^q = e$.
5. $a^{-1}ba = b^r$ *con* $1 < r \leq q-1$.
6. $r^p \equiv 1 \pmod{q}$ *y en este caso* $p|(q-1)$.

Demostración. Sean $a, b \in G$, a de orden p y b de orden q, como $H = \langle b \rangle$, $H \lhd G$. Es claro que $G = HK$, como $(p, q) = 1$, $H \cap K = \{e\}$. Ya que $H \lhd G$, $a^{-1}ba = b^r$ para alguna r con $0 \leq r \leq q-1$, si $r = 0$, b sería la identidad, si $r = 1$, $ba = ab$ y el grupo resultaria abeliano, por lo tanto $1 < r \leq q-1$.

Demostremos por inducción sobre m, que $a^{-m}ba^m = b^{r^m}$. Para $m = 2$:

$$a^{-2}ba^2 = a^{-1}\left(a^{-1}ba\right)a = a^{-1}b^r a = \left(a^{-1}ba\right)^r = (b^r)^r = b^{r^2}.$$

Si $a^{-m}ba^m = b^{r^m}$,

$$a^{-m-1}ba^{m+1} = a^{-1}\left(a^{-m}ba^m\right)a = a^{-1}b^{r^m}a = \left(a^{-1}ba\right)^{r^m} = (b^r)^{r^m} = b^{r^{m+1}}.$$

Por lo tanto ya que el orden de a es p, para $m = p$. $b = a^{-p}ba^p = b^{r^p}$ lo cual implica que $b^{r^p}b^{-1} = e$ y como el orden de b es q, $q \mid r^p - 1$ entonces $r^p \equiv 1 \pmod{q}$ y $p \mid (q-1)$. ■

Corolario 113 *Sean p y q primos con $p < q$. Si G es un grupo de orden pq y $p \nmid (q-1)$, entonces G es abeliano y por lo tanto cíclico.*

Si $G = H \bowtie_\varphi K$ y $\overline{H} = H \times \{e\}$, $\overline{K} = K \times \{e\}$ entonces se tiene que

1. $\overline{H} \lhd G$, $\overline{K} \lhd G$,
2. $\overline{H}\,\overline{K} = G$,
3. $\overline{H} \cap \overline{K} = \{e\}$.

Inversamente si G es un grupo, H y K son subgrupos de G y se cumple:

1. $H \lhd G$, $HK = G$ y $H \cap K = \{e\}$,
2. Si $\varphi : K \longrightarrow Aut(H)$ es tal que $\varphi(k)$ es la conjugación en H por k, es decir $\varphi(k)\,h = k^{-1}hk$ para cada $h \in H$, entonces φ es un homomorfismo, y
3. Si $\overline{G} = H \bowtie_\varphi K$.
   $\overline{G} \simeq G$ y se dice que G es producto semidirecto de H y K.

En virtud del teorema anterior si p y q son primos con $p < q$ y $p \mid (q-1)$, podemos construir un grupo no abeliano de orden pq.

Teorema 114 *Sean p y q primos, tal que $p < q$ y $p \mid (q-1)$. Entonces existe un grupo no abeliano de orden pq.*

Demostración. Sean $K = \langle a \rangle$ es un grupo de orden p y $H = \langle b \rangle$ un grupo de orden q, entonces los $Aut(H)$ es un grupo cíclico de orden $(q-1)$. Sea $f \in Aut(H)$ tal que $f(b_i) = b^{ir}$ con $1 < r \leq q-1$ y $r^p \equiv 1 \pmod{q}$, entonces es claro que f es de orden p.

Sea $\varphi : K \longrightarrow Aut(H)$ tal que $\varphi(a^s) = f^s$, entonces φ es un homomorfismo y $G = H \bowtie_\varphi K$ es un grupo no abeliano de orden pq. ∎

Se puede probar si G_1 es un grupo no abeliano de orden pq, entonces G_1 es isomorfo a G.

Capítulo 4

p-Grupos.

Teorema 115 *Sea G un grupo finito y p un número primo. G es un p-grupo si y sólo si el orden de G es una potencia de p.*

Teorema 116 *Si G es un grupo abeliano de orden $|G|$ y p un primo que divide a $|G|$, entonces G tiene un elemento de orden p.*

Demostración. Sea G un grupo abeliano y p un primo tal que $|G| = pm$ para algún m, con $1 \leq m \in Z$. La demostración es por inducción sobre m. Es claro que el primer paso de la inducción es cierto. Tomemos $x \in G$ de orden $t > 1$. Si $p \mid t$, entonces $x^{t/p}$ tiene orden p y el teorema se cumple. Si $p \nmid t$, por ser G un grupo abeliano y $\langle x \rangle \lhd G$, $G/\langle x \rangle$ es un grupo abeliano de orden $|G|/t = pm/t$ y m/t debe ser un entero ya que $p \nmid t$. Por hipótesis de inducción $G/\langle x \rangle$ contiene un elemento z de orden p. Como el homomorfismo natural $\varphi : G \longrightarrow G/\langle x \rangle$ es un epimorfismo, existe $y \in G$ tal que $\varphi(y) = z$, de donde el orden de y es un multiplo de p, esto es, $ord(y) = k = ps$ para alguna $s \in Z$. Por lo tanto $y^{k/p}$ tiene orden p y en consecuencia G tiene un elemento de orden p. ■

Si G es un grupo $a \in G$, el subconjunto $[a] = \{xax^{-1} | x \in G\}$ se llama la clase de conjugación de a en G. El conjunto formado por todas las clases de conjugación es una partición de G, entonces $G = \bigcup_{a \in G} [a]$. Si a es finito y C es el subconjunto de G formado por un elemento de cada clase de conjugación en G, entonces

$$|G| = \sum_{a \in C} |[a]| = \sum_{a \in C} [G : C_G(a)].$$

Teorema 117 *(De Cauchy). Si G es un grupo finito, y p un primo que divide al orden de G, entonces G tiene un elemento de orden p.*

Demostración. Podemos suponer que G no es abeliano. $|G| = pm$.

La demostración es por inducción sobre m. Si $m = 1$, el teorema es cierto.

Si $x \in Z(G)$, la clase de conjugación de x en G es $[x] = \{x\}$. Si C es el subconjunto de G formado por un elemento de cada clase de conjugación de G y C' es el subconjunto de G formado por un elemento de cada clase de conjugación con más de un elemento, $C = Z(G) \cup C'$ y $Z(G) \cap C' = \emptyset$. Por lo tanto $|G| = |Z(G)| + \sum_{a \in C'} [G : C_G(a)]$. Si $x \in C'$, $1 < |C_G(x)|$ porque 1, $x \in C_G(x)$ y $x \neq 1$, además como $C_G(x) \lneq G$ porque $x \notin Z(G)$ se tiene que $1 < |C_G(x)| < |G|$. Si $p \mid |C_G(x)|$, $|C_G(x)| = pk$ con $k < m$ y por hipótesis de inducción $C_G(x) \subset G$ tiene un elemento de orden p. Supóngase que para toda $x \in C'$, $p \nmid |C_G(x)|$ como $|G| = [G : C_G(x)]\,|C_G(x)|$ y $p \nmid |C_G(x)|$, entonces $p \mid [G : C_G(x)]$ para toda $x \in C'$. Como

$$|G| = |Z(G)| + \sum_{x \in C'} [G : C_G(x)]$$

y $|G|$, $|C_G(x)|$ son divisibles por p, entonces el $|Z(G)|$ también, por lo tanto por el teorema anterior el $Z(G) \subset G$ contiene un elemento de orden p. ■

Teorema 118 *Si $G \neq 1$ es un p-grupo finito, entonces $Z(G) \neq 1$.*

Demostración. Considerando que $|G| = |Z(G)| + \sum [G : C_G(x_i)]$, $|G| = p^m$ para alguna $m \geq 1$ y que $p \mid [G : C_G(x_i)]$ entonces $p \mid |Z(G)|$ y dado que $|Z(G)| \geq 1$, $|Z(G)|$ es por lo menos p, por lo que debe haber un elemento $x \neq e$ tal que $x \in Z(G)$. Por lo tanto $Z(G) \neq 1$. ■

Teorema 119 *Sea G un p-grupo finito. Si $H \lneq G$ entonces $H \lneq N_G(H)$ y cada subgrupo maximal de G es normal y tiene índice p.*

Teorema 120 *Si G es un p-grupo finito con p un número primo, si $H \lhd G$ y tiene orden p, entonces H está contenido en el centro de G.*

Demostración. Como $|H| = p$, $H = \langle a \rangle$ para algún $a \in G$, sabemos que el número de conjugados de a es el índice de su centralizador y es uno o una potencia de p. Pero en este caso el número de conjugados de a es cuando más $p - 1$. Por tanto la única posibilidad es el uno. Entonces $a \in Z(G)$ y por lo tanto $H \subset Z(G)$. ■

Teorema 121 *Sea G un grupo y $H \lhd G$. Si tanto H como G/H son p-grupos entonces G es un p-grupo.*

Teorema 122 *Sea G un p-grupo finito de orden p^n.*

a) Si $0 \leq k \leq n$, entonces G contiene un subgrupo normal de orden p^k.

b) Si $H < G$ tal que $|H| = p^s$, entonces existe un subgrupo de orden p^{s+1} el cual contiene a H.

Demostración. (Demostración de (a) por inducción sobre n.

Si $n = 1$, G es de orden p y $\{1\}$ es el subgrupo de orden p^0. Supongamos que para alguna $k > 1$ todo subgrupo de orden p^k tiene un subgrupo normal de orden p^{k-1}. Sea G de orden p^{k+1}, como $Z(G) \neq 1$ existe un elemento x de orden p en $Z(G)$. Si $\langle x \rangle = H$, entonces $H \lhd G$ de orden p, por lo tanto podemos considerar el grupo cociente G/H y

$$|G/H| = |G|/|H| = p^{k+1}/p = p^k,$$

por hipótesis de inducción G/H tiene un subgrupo normal M de orden p^{k-1}. Dado que $\varphi : G \longrightarrow G/H$ es un homomorfismo, entonces por el Teorema de la Correspondencia existe un subgrupo N de G tal que $H \subset N \lhd G$ y $N/H = M$ pero

$$p^{k-1} = |M| = |N|/|H| = |N|/p$$

entonces $|N| = p^k$ por lo tanto N es el subgrupo normal de G de orden p^k.

(b) Si $H < G$ tal que $|H| = p^s$, entonces por el primer teorema de Sylow H es un subgrupo normal de al menos un subgrupo de orden p^{s+1}. ■

Lema 123 *Sean $x, y \in G$. Si tanto x como y conmutan con $[x, y]$, entonces:*

a) $[x,\ y]^n = [x^n,\ y] = [x,\ y^n]$ para toda $n \in Z$.

b) $(xy)^n = [y,\ x]^{n(n-1)/2} x^n y^n$ para toda $n \geq 0$.

Teorema 124 *Si G es un p-grupo finito con sólo un subgrupo de orden p y más de un subgrupo cíclico de índice p, entonces G es isomorfo a Q, el grupo de los cuaternios.*

Demostración. Supongamos que G tiene más de dos subgrupos cíclicos de índice p. Sea $A < G$, de índice p, entonces $A \lhd G$. Por consiguiente si $x \in G$, $Ax \in G/A$ que es un grupo de orden p y se tiene que $x^p \in A$. Sean $A = \langle a \rangle$ y $B = \langle b \rangle$ distintos subgrupos de G de índice p. Como A y B son normales en G, entonces $A \cap B = D$ es un subgrupo normal de G.

Como A y B son distintos subgrupos normales maximales de G, se tiene que $AB = G$, de donde $[G : D] = |A||B|/|A \cap B||A \cap B| = p^2$. Entonces G/D es abeliano y $G' < D$.

Como $G = AB$, si $x \in G$, $x = a^r b^s$ para alguna $r, s \in Z$, pero si $y \in D$, $y = a^{r_1} = b^{s_1}$, $yx = xy$ para cada $x \in G$, y $G' \leq D \leq Z(G)$. Entonces para cada $x,\ y \in G,\ [y,\ x]^p = [y^p,\ x]$, pero $y^p \in D \leq Z(G)$, por lo que $[y, x]^p = 1$, y se tiene que $(xy)^p = [y,\ x]^{p(p-1)/2} x^p y^p$. Si p es impar, p divide $p(p-1)/2$ y $(xy)^p = x^p y^p$. Por otro lado si $G[p] = \{x \in G : x^p = 1\}$ y $G^p = \{x^p : x \in G\}$, entonces ambos son subgrupos y $[G : G[p]] = |G^p|$.

Por consiguiente $|G[p]| = [G : G^p] = [G : D][D : G^p] \geq p^2$, y $G[p]$ contiene un subgrupo E de orden p^2; que es abeliano elemental, entonces G contiene más de un subgrupo de orden p, lo cual no puede ser, por lo tanto $p = 2$.

Si $p = 2$, tenemos que $D = \langle a^2 \rangle = G^2 \leq Z(G)$, $[G : D] = 4$ y $[y, x]^2 = 1$ para toda $x,\ y \in G$, $(xy)^4 = [y, x]^6 x^4 y^4$.

Como $D = \langle a^2 \rangle$ y $G^4 = \langle a^4 \rangle$, $|G[2]| = [G : G^4] = [G : D][D : G^4] = 8$. Si $G[2]$ tiene sólo un subgrupo cíclico de orden 4, entonces contendría más de un elemento de orden 2, lo cual no puede ser, hay por consiguiente dos subgrupos cíclicos $\langle u \rangle$ y $\langle v \rangle$ de orden 4 en $G[2]$. Si $a^4 \neq 1$, podriamos tomar $\langle u \rangle \leq \langle a^2 \rangle \leq Z(G)$, y $\langle u \rangle \langle v \rangle$ sería un subgrupo abeliano de G, pero $\langle u \rangle \langle v \rangle$ contiene al menos dos elementos de orden 2, lo cual es una contradicción, por lo que $a^4 = 1$, se sigue que como $|D| = 2$ y $|G| = 8$, G es isomorfo a D_8 o Q, pero Q el grupo de los cuaternios tiene más de un subgrupo de índice 2, por lo tanto G es isomorfo a los cuaternios. ■

Teorema 125 *Sea* $U(Z_{2^m}) = \{[a] \in Z_{2^m} | a \text{ es impar}\}$. *Si* $m \geq 3$, *entonces*

$$U(Z_{2^m}) = \langle [-1], [5] \rangle \simeq Z_2 \times Z_{2^{m-2}}.$$

Corolario 126 *Sea* G *un grupo con elementos* $x,\ y$ *tales que* x *tenga orden* 2^m *con* $m \geq 3$. $y^2 = x^{2r}$, $yxy^{-1} = x^t$, *entonces* $t = \pm 1$ *o* $t = \pm 1 + 2^{m-1}$.

Teorema 127 *Si un p-grupo finito* G *de orden* p^n *tiene un único subgrupo de orden* p, *entonces* G *es cíclico o* G *es un grupo cuaternio generalizado.*

Demostración. (Por inducción sobre n).

Sea p^n el orden de G es claro que si $n = 1$ G es un grupo cíclico. Consideremos entonces $n > 1$ y p un primo impar. Por inducción un subgrupo H de índice p es cíclico y no puede haber otro subgrupo de índice p, al menos que G sean los cuaternios, el cual es un 2-grupo, por lo tanto G sólo tiene un subgrupo de índice p, el cual es maximal, si G no fuese cíclico, $\langle x \rangle$ es un subgrupo propio de G para cada $x \in G$ y $\langle x \rangle < H$, por lo que $G \leq H$ lo cual es una contradicción.

Sea G un 2-grupo. Si G es abeliano con un único subgrupo de orden p, se tiene que G es cíclico.

Supongamos que G no es abeliano y sea A un subgrupo normal maximal de G. Como A tiene sólo un elemento de orden dos, A es cíclico con $A = \langle a \rangle$. Además A tiene índice 2 ya que de lo contrario si $|G/A| \geq 4$ y si $Ab \in G/A$ tal que $(Ab)^2 \neq e$, entonces $b^2 \notin A$. Consideremos $H = \langle a, b^2 \rangle < \langle a, b \rangle \leq G$. Si H es abeliano, entonces b^2 centraliza A, lo cual es una contradicción, entonces H no es abeliano y por hipótesis de inducción debe ser la generalización de los cuaternios. Podemos por consiguiente asumir que $b^2ab^{-2} = a^{-1}$. Como $\langle a \rangle \lhd G$, $bab^{-1} = a^i$ para alguna i, y se tiene que:

$$a^{-1} = b^2ab^{-2} = b\left(bab^{-1}\right)b^{-1} = ba^ib^{-1} = \left(bab^{-1}\right)^i = \left(a^i\right)^i = a^{i^2},$$

con $i^2 \equiv -1 \pmod{2^e}$ donde 2^e es el orden de a. Nótese que $e \geq 2$, para $A \lneq Z(G)$. Pero no existe tal congruencia; si $e \geq 3$ por el teorema anterior esta congruencia no tiene solución; si $e = 2$, entonces -1 no es un cuadrado módulo 4, por lo que $(Ab)^2 = e$ para todo $Ab \in G/A$. Si $|G/A| \geq 4$, existen elementos c y d con c, d, $c^{-1}d \notin A$ y con $\langle a, c \rangle$, $\langle a, d \rangle$ y $\langle a, c^{-1}d \rangle$ subgrupos propios de G, ninguno de ellos puede ser abeliano, porque de lo contrario c, d o $c^{-1}d$ centralizarían a A, entonces los tres grupos son la generalización de los cuaternios y como $cac^{-1} = a^{-1} = dad^{-1}$, $c^{-1}d \in C_G(A)$, lo cual es una contradición, por lo tanto $A = \langle a \rangle$ tiene índice dos en G.

Tomemos $b \in G$, tal que $b^2 \in \langle a \rangle$, entonces existe $r \leq n - 2$ tal que $b^2 = a^{2r}$, si es necesario cambiemos a por otro generador de $\langle a \rangle$ para obtener el resultado que deseamos.

Como $\langle a \rangle \lhd G$, $bab^{-1} = a^t$ para alguna t, pero G sólo tiene un elemento de orden 2, entonces por el corolario anterior $t = \pm 1$, si $t = 1$, $ab = ba$, G sería abeliano y en consecuencia cíclico, por lo tanto $t = -1$ y $G = \langle a, b \rangle$, donde:

$$a^{2^{n-1}} = 1, \quad bab^{-1} = a^{-1}, \quad b^2 = a^{2r}.$$

Sólo falta probar que $r = n-2$, pero $t = -1$, entonces $2^r \equiv -2^r \pmod{2^{n-1}}$, lo cual implica que $2^{r+1} \equiv 0 \pmod{2^{n-1}}$, por lo que $r = n-2$. ∎

Teorema 128 *Sea G un grupo finito de orden p^n, con p un primo y $n \geq 3$. Si para alguna $m \in Z$, con $1 < m < n$, G tiene sólo un subgrupo de orden p^m, entonces G es cíclico.*

Demostración. Sea $U < G$ único de orden p^m, $1 < m < n$. Si $m = n-1$ cada subgrupo propio de G está contenido en un subgrupo máximal y como G sólo tiene un subgrupo máximal si $x \notin U$, $\langle x \rangle = G$, ya que si $\langle x \rangle \subsetneq G$, entonces $\langle x \rangle \subset U$ lo cual es una contradicción, por lo tanto G es cíclico. Esto prueba el teorema para $n = 3$ y para $n > 3$ con $m = n-1$. Procedamos ahora por inducción sobre n. Supongamos que $2 \leq m < n-1$, sea U_1 un subgrupo de G de orden p^{m+1} que contenga a U, como U es el único subgrupo de orden p^m en U_1 por hipótesis de inducción, U_1 es cíclico en consecuencia U es cíclico.

Luego cada subgrupo de G de orden p o p^2 esta contenido en un subgrupo de orden p^m, como U es el único subgrupo de ese orden y es cíclico, entonces G sólo tiene un subgrupo de orden p y uno de orden p^2, pero un $p-grupo$ que contenga sólo un subgrupo de orden p es cíclico o un cuaternio generalizado, y este último tiene más de un subgrupo de orden 2^2, por lo tanto G es cíclico. ∎

Teorema 129 *Sea G un $p-$ grupo. Cada subgrupo de G de orden p^2 es cíclico si y sólo si G tiene sólo un subgrupo de orden p.*

Demostración. Supongamos que cada subgrupo de G de orden p^2 es cíclico y que G tiene dos subgrupos de orden p, como el centro de G es no trivial uno de los subgrupos de orden p está contenido en el centro de G, y el producto de estos dos subgrupos es un subgrupo no cíclico de orden p^2, lo cual es una contradicción. Por lo tanto G tiene sólo un subgrupo de orden p.

Inversamente, supongamos que G sólo tiene un subgrupo de orden p.

Si G tuviera algún subgrupo no cíclico de orden p^2, entonces G tendría al menos dos subgrupos de orden p, contradiciendo que G sólo tiene uno, por lo tanto cada subgrupo de G de orden p^2 es cíclico. ∎

Teorema 130 *Si G es un grupo de orden p^n con p un primo y para algún m, con $1 < m < n$, todos los subgrupos de G de orden p^m son cíclicos, entonces G es cíclico, excepto cuando $p = 2$, $m = 2$. En este último caso G también puede ser un grupo cuaternio generalizado.*

Demostración. Si $m > 2$, como cada subgrupo de G de orden p^m es cíclico, entonces todo subgrupo de G de orden p^2 es cíclico. Por lo tanto G sólo tiene un subgrupo de orden p, lo cual implica que G es cíclico o un grupo cuaternio generalizado; pero un cuaternio generalizado es un 2-grupo, por lo tanto si $p > 2$, G es cíclico. ■

Capítulo 5

Nc-grupos finitos .

Definición 131 *Un grupo G es un $Nc-$ grupo si G no es cíclico y todos sus subgrupos normales propios son cíclicos.*

En este capítulo estudiaremos la clase de los $Nc-$*grupos* solubles finitos.

Teorema 132 *Sea G un Nc-grupo finito. Si G es nilpotente, entonces G es un p-grupo.*

Demostración. Supóngase que $|G| = p_1^{n_1} p_2^{n_2} \cdots p_s^{n_s}$ con $p_1, p_2, \cdots, p_s$ primos diferentes y $s > 1$.

Por cada $1 \leq i \leq s$ el p_i subgrupo de Sylow de G es normal y por lo tanto cíclico.

Como G es producto directo de sus subgrupos de Sylow, G resulta ser un grupo cíclico lo que es un absurdo, por lo tanto $s = 1$ y G es un p-grupo. ∎

Corolario 133 *Si G es un Nc-grupo finito, entonces G es un p-grupo o G no es nilpotente.*

Un $Nc-$*grupo* finito y soluble pertenece a alguna de las siguientes clases:

$C_1 =$ La clase de los $p-$*grupos* abelianos.

$C_2 =$ La clase de los $p-$*grupos* no abelianos.

$\mathcal{C}_3 =$ La clase de los grupos no nilpotentes.

Teorema 134 *Si G es un Nc-grupo finito y soluble, entonces G' es cíclico.*

Demostración. Como G es soluble, existe $N \underset{\neq}{\lhd} G$ tal que G/N es abeliano lo que implica que $G' \lneqq G$ y como G' es normal en G, entonces G' es cíclico. ∎

Teorema 135 *Sea G un $Nc-$ grupo finito. Si $G \in \mathcal{C}_1$ entonces G es isomorfo a $Z_p \times Z_p$ para algún primo p.*

Demostración. Como G es producto directo de subgrupos cíclicos, se tiene que G es isomorfo a $Z_p \times Z_p$, porque en caso contrario G tendría un subgrupo normal propio isomorfo a $Z_p \times Z_p$ que no es cíclico. ∎

El teorema anterior nos dice que los únicos $p-$ *grupos abelianos* finitos que son $Nc-$ *grupos* son los *grupos abeliano elemental* de orden p^2.

Teorema 136 *Sea G un $Nc-$grupo finito Si $G \in \mathcal{C}_2$ entonces G es isomorfo al grupo de los cuaternios.*

Demostración. Sea $|G| = p^n$ con $n \geq 3$. Como G no es cíclico, tiene al menos dos subgrupos de orden p^{n-1}, que resultan normales en G y por consiguiente cíclicos.

G tiene sólo un subgrupo de orden p. En efecto, ya que cada subgrupo H de G de orden p está contenido en un subgrupo maximal M de orden p^{n-1} que es normal y por consiguiente cíclico, se tiene que $H \lhd G$ porque H es característico en M y $M \lhd G$.

Entonces si G tuviera dos subgrupos de orden p, G tendría un subgrupo normal de orden p^2 isomorfo a $Z_p \times Z_p$ que no es cíclico. lo que contradice que G es un $NC-$ *grupo.*

Como G tiene sólo un subgrupo de orden p y al menos dos subgrupos de orden p^{n-1}, G resulta isomorfo al grupo de los cuaternios. ∎

Teorema 137 *Si G es un Nc-grupo finito no nilpotente, entonces G tiene sólo un subgrupo normal maximal.*

Demostración. Supongamos que G tenga dos subgrupos normales maximales N_1 y N_2, entonces $G = N_1N_2$ y como N_1 y N_2 son nilpotentes por ser cíclicos, se tiene que G es nilpotente, lo cual es una contradicción, por lo tanto G tiene sólo un subgrupo normal maximal. ∎

Teorema 138 *Si G es un Nc-grupo finito y $G \in C_3$, entonces G/G' es un $p-$ grupo cíclico o abeliano elemental de orden p^2, para algún primo p.*

Demostración. Supóngase que G/G' no es cíclico. Sea H/G' un subgrupo no trivial de G/G', $H/G' \lhd G/G'$ lo que implica que $H \overset{\neq}{\lhd} G$ y como H es cíclico, H/G' es cíclico, por consiguiente G/G' es un $Nc-$ *grupo* finito y abeliano, por lo tanto G/G' es isomorfo a $Z_p \times Z_p$.

Supóngase que G/G'es cíclico y sea N el único subgrupo normal maximal de G, $G' \leq N < G$ y $[G:N] = p$, para algún primo p.

Como $|G/G'| = |G/N|\,|N/G'|$, $p \mid |G/G'|$. Si un primo q divide a $|G/G'|$, existe $H/G' < G/G'$ tal que $[G/G' : H/G'] = q$. Como $H/G' \lhd G/G'$, entonces $H \lhd G$ y $[G:H] = q$, lo que implica que H es normal maximal en G, por lo tanto $H = N$, $p = q$ y G/G' resulta un $p-$ *grupo*. ∎

Teorema 139 *Si G es un Nc-grupo soluble no nilpotente, entonces G es supersoluble.*

Demostración. Como G' es cíclico y G/G' es supersoluble porque es abeliano, entonces G es supersoluble. ∎

Teorema 140 *G es un Nc-grupo finito, soluble no nilpotente si y sólo si G es una extension no nilpotente de un grupo cíclico finito N mediante un grupo cíclico de orden p y N el único subgrupo normal maximal de G.*

Demostración. Supóngase que G es un $Nc-$ *grupo* finito, soluble no nilpotente. Sea N el único subgrupo normal maximal de G. Como G es soluble, $|G/N| = p$ con p un primo. Si $T = G/N$, G resulta ser una extensión

no nilpotente de un grupo cíclico finito N mediante el grupo cíclico T de orden p y N el único subgrupo normal maximal.

Inversamente, supóngase que N es un grupo cíclico, H un grupo de orden p con p un primo y sea G un grupo no nilpotente tal que $N \lhd G$, $G/N \simeq H$ y que N sea el único subgrupo normal maximal de G.

Como G/N y N son solubles, se tiene que G es soluble.

Si $R \overset{\neq}{\lhd} G$, entonces $R < N$ y en consecuencia R es cíclico, por lo tanto G es un $Nc - grupo$ finito, soluble no nilpotente. ■

Teorema 141 *Si G es un Nc-grupo finito, soluble no nilpotente y N el único subgrupo normal maximal de G, entonces $|G/N|$ es un primo p y p es menor o igual a todos los divisores primos de $|N|$ y menor o igual a todos los divisores de $|G|$.*

Demostración. Como G es soluble, $|G/N| = p$ con p un primo. Como G es supersoluble, si p_s es el menor primo que divide al orden de G, entonces G tiene un subgrupo M de índice p_s que resulta normal en G.

Como $[G : M] = p_s$ entonces M es normal maximal, por lo tanto $M = N$ y $p_s = p$ ■

Teorema 142 *G es un Nc-grupo finito, soluble no nilpotente si y sólo si se cumplen las siguientes dos condiciones:*

(*i*) *G es producto semidirecto de un grupo cíclico M (no trivial que coincide con el G'), con un p-grupo cíclico H y p es un primo tal que $p \nmid |M|$.*

(*ii*) *$H^p < Z(G)$, $N = MH^p = M \times H^p$ y N es el único subgrupo normal maximal de G.*

Demostración. Sea N el único subgrupo normal maximal de G, se tiene que:

(1) $[G : N] = p$ con p un primo.

(2) G/G' es un p-grupo (*Teorema* 135).

(3) $p \nmid |G'|$.

Supongamos que $p \mid |G'|$. $|G'| = p^t k$, $p \nmid k$ y $k > 1$. G' tiene un subgrupo M de orden k, porque G' es cíclico lo que implica que $[G' : M] = p^t$. $M \lhd G$ porque M car G' y $G' \lhd G$.

Como $G/G' \simeq G/M/G'/M$ y tanto G/G' como G'/M son p–grupos se tiene que G/M es un p-grupo.

Ya que G/M tiene un único subgrupo normal maximal, G/M es cíclico lo que implica que $G' < M$ y $M = G'$.

Como $k = |M| = |G'|$ y $p \nmid k$, es decir, $p \nmid |G'|$ se tiene una contradicción porque habíamos supuesto que $p \mid |G'|$.

(4) $G = G'H$.

Sea H un p–subgrupo de Sylow de G. Como $|G/G'| = p^t$, $|G| = |G'|p^t$ y como $p \nmid |G'|$, $G = G'H$. Ya que $G' \lhd G$ y $G' \cap H = \{1\}$, G es el producto semidirecto de G' por H.

(5) H es un p–grupo cíclico.

Como G/G' es cíclico y

$$\frac{G}{G'} = \frac{G'H}{G'} \simeq \frac{H}{G' \cap H} = H,$$

se tiene que H es cíclico.

(6) $H^p < Z(G)$.

En efecto como H es cíclico, $H^p < C_G(H)$, además, $H^p < N$ porque $[G : N] = p$, y como $G' < N$ por ser N el único subgrupo normal maximal de G, se tiene que $H^p < C_G(G')$. Como $G = G'H$, entonces $H^p < C_G(G) = Z(G)$.

(7) $N = G'H^p = G' \times H^p$.

Como G' y H^p son normales en G, entonces $G'H^p \lhd G$ y ya que $G' \cap H = \{1\}$,

$$|\frac{G'H}{G'H^p}| = \frac{|G'H|}{|G'H^p|} = \frac{|H|}{|H^p|} = |\frac{H}{H^p}| = p,$$

porque H es cíclico, por lo tanto $[G : G'H^p] = p$ y como $G'H^p < N$, entonces $N = G'H^p = G' \times H^p$.

Hemos demostrado que si G es un Nc-grupo finito, soluble no nilpotente, entonces se cumple (i) y (ii).

Inversamente, supongamos que se cumplen (i) y (2).

Como el p-subgrupo de Sylow H de G no está contenido en N, H no es normal en G y por lo tanto G no es nilpotente.

Como G/N y N son solubles. G es soluble.

Sea $R \lhd G$, entonces $R < N$ ya que N es el único subgrupo normal maximal de G y como $N = G' \times H^p$, se tiene que R es cíclico, por lo tanto G es un Nc-grupo. ∎

Un ejemplo de un Nc-grupo finito, soluble no nilpotente es el grupo de todas las permutaciones del conjunto $A = \{1, 2, 3\}$, denotado por S_3. De hecho si p y q son primos con $p > q$ y $q \nmid (p-1)$, el grupo no abeliano de orden pq es un $Nc - grupo$.

BIBLIOGRAFIA

[1] BIANCHI, M. G., Sui Gruppi a Sottogruppi Normale Ciclici. Instituto Lombardo, Rendiconti di Scienze (*A*). Vol. 112, (1978).

[2] FRALEIGH, B. J., Algebra Abstracta. Addison-Wesley Iberoamérica, (1987).

[3] HERSTEIN, I. N., Algebra Abstracta. Grupo Editorial Iberoamérica, (1988).

[4] MARSHALL, H, J., Teoria de los Grupos. Editorial Trillas, México, (1973).

[5] MORALES RODRÍGUEZ JUAN. Una caracterización de los grupos cíclicos. Aportaciones Matemáticas. Comunicaciones. Vol. 25, (1999).

[6] MORALES RODRÍGUEZ JUAN. Sui gruppi finiti non abeliani a sottogruppi normali propri abeliani. Accademia Nazionale dei Lincei, Rendiconti della Classe di Scienze fisiche, matematiche e naturali. Vol.LXXIV, (1983).

[7] ROTMAN, J. J., An Introduction to the Theory of Groups. Springer-Verlag, (1995).

[8] ZAPPA, G., Fondamenti di Teoria dei Gruppi. Vol. II Edizioni Cremonese, Roma (1970).

[9] ZASSENHAUS, H., The Theory of Groups. Chelsea, (1956).