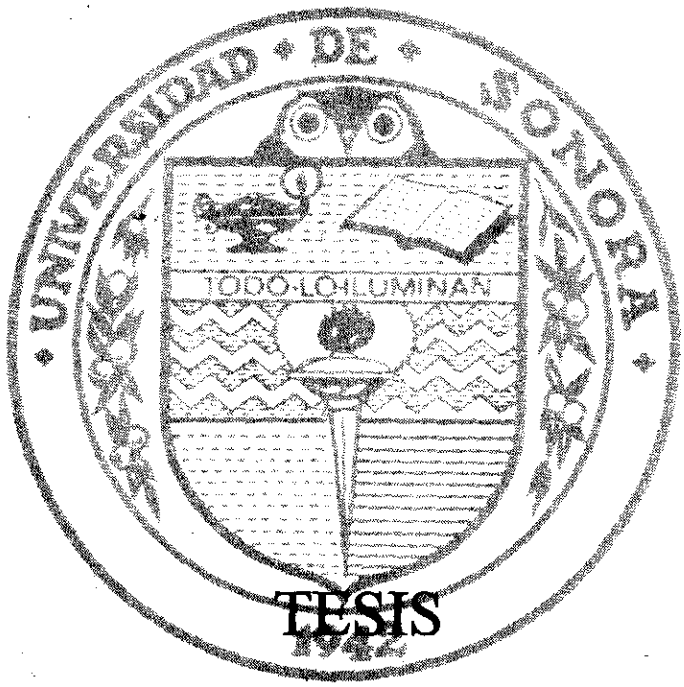
NIVERSIDAD DE SONORA

DEPARTAMENTO DE MATEMATICAS

TEOREMAS DE SYLOW, PRODUCTOS SEMIDIRECTOS
Y CLASIFICACION DE GRUPOS DE ORDEN $pqr < 100$
(p, q, r primos no necesariamente distintos)



TESIS

QUE PARA OBTENER EL TITULO DE
LICENCIADO EN MATEMATICAS

PRESENTA

JESUS MENDIVIL LEON

ERMOSILLO, SONORA **AGOSTO DE 2001**

A mi Familia

...mientos:

...C. Carlos Alberto Robles Corbalá, Director de este trabajo, pero más ...a por ser el primero en tener la suficiente confianza en mi persona para ...lograrlo.

...en C. Gustavo Montaño Bermúdez, quién fungió como asesor de la ... y por las valiosas observaciones que hizo al presente que sin ellas ...mente se hubiera terminado.

...M. en C. Jorge Ruperto Vargas Castro, ante todo por su valiosa ...oración como un real compañero.

...Dr. Martín Eduardo Frías Armenta, uno de los grandes exalumnos que ... presumir que tengo y que para la elaboración de este escrito fue muy ...rtante su participación.

...Dr. Oscar Vega Amaya, quién aunque haya sido por azar el mostrarme el ...rito de donde surgió la idea de escribir este trabajo también es válido ...conocerlo.

...Dr. Jesús Adolfo Minjárez Sosa, quién fue el primero en mostrar un sincero ...erés en que mi persona regresara a este tan buen trabajo el de enseñar y ...ender Matemáticas.

INDICE

INTRODUCCION

El estudio de los grupos finitos aparece en diversas áreas de las ciencias como son: Arqueología, Física, Química, etc. Y dentro de la Matemática podemos encontrar grupos en Teoría de Gráficas, Geometría y Topología Algebraica entre muchas otras.

La importancia de contar con los grupos clasificados permite mayor facilidad en la comprensión de las aplicaciones; por ejemplo, en Topología Algebraica, a un Espacio Topológico se le pueden asignar grupos que ayudan a diferenciar entre espacios, estas tareas se ven sumamente beneficiadas con la clasificación de grupos.

La teoría de grupos de orden finito es un área de las Matemáticas con un rico historial la cual fundamenta el trabajo de muchos grandes matemáticos. De acuerdo con William Burnside, la teoría de grupos finitos tuvo sus orígenes en los intentos del matemático francés A. I. Cauchy (1789-1857), quien en 1815 empezó en forma consistente la teoría de permutaciones, la cual desarrolló después de 1846 en la teoría de grupos de permutaciones, como matemático finalmente empezó a resumir los conceptos originales de grupos teóricos el cual le fué legado a Cauchy por el joven matemático E. Galois (1811-1832). Sobre las bases de Cauchy y Galois podemos empezar a estudiar los grupos finitos, un campo de estudio que fue rápidamente estructurado, con importantes contribuciones al matemático Noruego L. Sylow (1832-1918), y del matemático Alemán L. Kronecker (1823-1891), del cual su famoso teorema probaremos en este escrito. Finalmente con una publicación en 1878 de los escritos sobre la teoría de grupos del matemático Ingles A.

Cayley (1821-1895), la teoría de grupos fue considerada un campo de las matemáticas independiente y auto sostenido. En las décadas pasadas, la clasificación de todos los grupos finitos llevo a muy grandes investigaciones. En la actualidad , ésta es la gran meta de la teoría de grupos finitos.

Para clasificar todos los grupos finitos de orden $n \in \mathrm{N}$, tendríamos que producir una lista de todos los grupos no isomorfos de orden n, para determinar sus tablas de factorizacion únicas. Sin embargo, grupos teóricos han sido determinados como estructuras de grupos en el mayor de los casos probando que el grupo es isomorfo a otro grupo o clase de grupos la cual es fácilmente conocida.

Básicamente podemos dividir la teoría de grupos finitos en la clasificación de tres distintos tipos de grupos finitos (ver Figura 1)

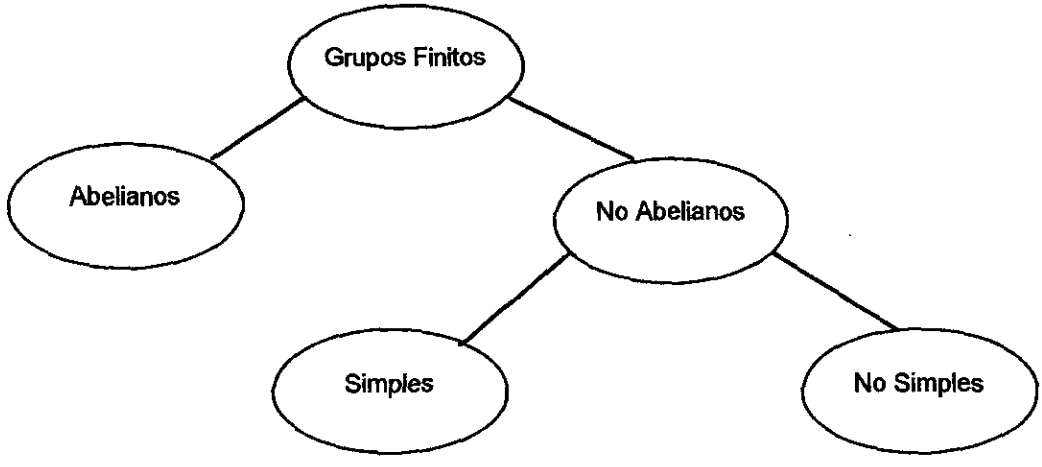


Figura .- Tipos de Grupos Finitos.

Aunque la clasificación de los grupos finitos no simples es un reto hasta ahora, el orden de dos tipos de estos grupos ha sido clasificado; los grupos Abelianos finitos fueron clasificados en 1870 con la ayuda del Teorema de Kronecker, y los grupos Simples finitos

fueron clasificados justamente hace dos décadas. La historia detrás de la clasificación de los grupos simples finitos es de especial significado histórico, esta tarea unió a teóricos de grupos finitos alrededor del mundo durante 30 años que culminaron en 300 a 500 trabajos individuales y alrededor de 5000 a 10,000 paginas en revistas. En este trabajo nuestra modesta meta es la de clasificar de orden menor que 100, con las restricciones de que su orden sea a lo más el producto de tres primos.

En el Capítulo I, se enunciarán y demostrarán sólo algunos teoremas básicos de la teoría de grupos que serán referidos en el desarrollo de los capítulos posteriores, este es material básico de un primer curso de Álgebra Abstracta por lo que su contenido es fácilmente comprendido por estudiantes de matemáticas de los primeros semestres de licenciatura.

En el Capítulo II, se incluye el tema de Acciones de Grupos en Conjuntos con el propósito de dar una demostración compacta del Teorema de Cauchy y de los Teoremas de Sylow que son herramienta fundamental para el propósito del trabajo.

El Capítulo III, contiene una demostración del Teorema Fundamental de los Grupos Abelianos Finitos vía Teoremas de Sylow, como una fuerte herramienta de soporte para la clasificación de grupos finitos. Una demostración muy completa de este teorema y la clasificación general de los grupos abelianos puede verse en la Tesis de Licenciatura ***"Clasificación de Grupos Abelianos"*** del Dr. Martín Eduardo Frías Armenta.[V]

El Capítulo IV, contiene el recurso de los productos semi-directos con el cual principalmente determinaremos los grupos no abelianos no isomorfos que nos hemos propuesto clasificar. Esta es otro de los componentes principales para alcanzar la meta propuesta.

Finalmente en el Capítulo V nos centramos en la clasificación en sí de los grupos finitos que dentro del rango mencionado clasificaremos. La estrategia a seguir en esta tarea será la de establecer las condiciones bajo las cuales se pueda hacer uso de los recursos desarrollados en los capítulos anteriores y dar la clasificación de los grupos hasta donde sea posible, en términos de grupos más conocidos o fáciles de manejar.

CAPITULO I.

PRELIMINARES.

Esta parte del trabajo contiene los conceptos y teoremas básicos de la Teoría de Grupos que se utilizarán en el desarrollo del presente escrito. No se incluyen todas las demostraciones, ya que algunas de ellas son el material clásico en cualquier primer curso de Álgebra Abstracta y por tanto todo estudiante de matemáticas que haya pasado por tal curso es capaz de comprender completamente el contenido del presente.

Iniciaremos con la definición de grupo y algunas de las propiedades elementales de grupos que nos facilitarán el manejo de las demostraciones posteriores.

Definición 1.1.1.- Un conjunto no-vacío G es un ***grupo***, si para sus elementos está definida una operación que cumple con las siguientes propiedades:

1) $\forall\, a, b \in G$, $ab \in G$. (cerradura)

2) $\forall\, a, b, c \in G$, $a(bc) = (ab)c$. (asociatividad)

3) $\exists\, e \in G$, tal que $ae = ea = a$, $\forall\, a \in G$.(elemento identidad)

4) Para cada $a \in G$, $\exists\ a^{-1} \in G$, tal que $aa^{-1} = a^{-1}a = e$.(existencia de inversos)

Cuando en un grupo se cumple la conmutatividad, diremos que el grupo es ***Abeliano***.

Definición 1.1.2.- Un ***subgrupo***, es un subconjunto no-vacío H de un grupo G que es el mismo también un grupo bajo la operación de G. Lo cual denotaremos por $H \leq G$.

El teorema que a continuación se enuncia es uno de los más comunes para demostrar que un subconjunto de un grupo es un subgrupo.

Teorema 1.1.3.- Sea G un grupo, un subconjunto no-vacío H de G, es un subgrupo de G, si:

1) $a, b \in H \rightarrow ab \in H$.

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

Definición 1.1.4.- Un grupo se dice que es ***finito***, si tiene un número finito de elementos.

Definición 1.1.5.- Al número de elementos de un grupo G lo denominaremos el ***orden*** del grupo y se denotará por $|G|$.

Definición 1.1.6.- El ***orden de un elemento*** de un grupo se define, si existe, como el menor entero positivo n tal que $a^n = e$. Si no existe tal entero diremos que el elemento es de ***orden infinito***.

Consecuencias inmediatas de los conceptos anteriores son las propiedades que se expresan en el Lema siguiente.

Lema 1.1.7.- Si G es un grupo, entonces:

1) El elemento identidad es **único**.

2) Todo $a \in G$, tiene un inverso **único** $a^{-1} \in G$.

3) Si $a \in G$, entonces $(a^{-1})^{-1} = a$.

4) $\forall\, a, b \in G$, $(ab)^{-1} = b^{-1} a^{-1}$.

De igual forma también tenemos el siguiente

Teorema 1.1.8.- Para todo $a, b, c \in G$:

1) $ab = ac \Leftrightarrow b = c$

2) $ba = ca \Leftrightarrow b = c$.

Los siguientes son algunos ejemplos de grupos importantes que se citarán posteriormente:

Ejemplo1.1.- Z, el conjunto de los enteros con la suma usual.

Ejemplo 1.2.- $nZ = \{x \in Z$ tales que $x = kz$ con $x \in Z\}$, con la suma usual.

Ejemplo 1.3.- Z_n el conjunto de las clases residuales módulo n con la suma mod n.

Ejemplo 1.4- $U(n) = \{k \in Z$ tales que $(n, k) = 1\}$, con la multiplicación mod n.

Ejemplo 1.5- D_{2n} el conjunto de simetrías del polígono regular de n lados.

El grupo del ejemplo anterior es denominado el ***Grupo Diédrico de orden 2n***.

Ejemplo1.6.- Si A es un conjunto no vacío el conjunto de todas las aplicaciones biyectivas de A en si mismo forman un grupo bajo la composición de funciones denotado S_A.

Ejemplo 1.7.- Si A es el conjunto finito $\{1, 2, 3, \ldots n\}$, entonces el grupo de todas las funciones biyectivas de A en si mismo forman un grupo llamado el ***grupo simétrico de n símbolos*** y se denota por S_n.

Ejemplo 1.8.- Si n es numero natural, el conjunto de las raíces complejas de la unidad: $\left\{ \cos\left(\frac{2\pi k}{n}\right) + i \operatorname{sen}\left(\frac{2\pi k}{n}\right) \text{ con } k = 0, 1, 2, 3, \ldots, n\text{-}1 \right\}$ es un grupo bajo la multiplicación usual de los números complejos.

Los teoremas que a continuación se enuncian, nos proporcionan ejemplos de los subgrupos más importantes.

Teorema 1.1.9.- Si G es un grupo y a es un elemento de G, entonces el conjunto:

$\langle a \rangle = \{a^i$ donde i es un entero$\}$, es un subgrupo de G, llamado el ***subgrupo cíclico generado*** por a. Cuando todo G es generado por alguno de sus elementos se dice que G es ***cíclico*** y lo denotaremos $G = \langle a \rangle$.

Como los grupos cíclicos son una de las parte medulares del presente escrito enunciaremos todas las propiedades que de éstos requeriremos posteriormente.

Teorema 1.1.10.- Si G es un grupo cíclico finito de orden n, entonces es isomorfo a Z_n.

Teorema 1.1.11.- Sea G es un grupo cíclico finito y a es un elemento de G. Si $a^k = e$, entonces $|a|$ divide a k.

Teorema 1.1.12.- Si G es un grupo cíclico finito de orden n, generado por el elemento a, entonces $G = \langle a^k \rangle$ sí, y sólo si $(n, k) = 1$.

En particular si $G = Z_n$ y $a = 1$, en el Teorema anterior obtenemos el siguiente resultado que nos será de bastante utilidad.

Corolario 1.1.13.- (Generadores de Z_n) Un entero k es un generador de Z_n sí, y sólo sí $(n, k) = 1$.

El conjunto de generadores de Z_n, forman un grupo bajo la multiplicación módulo n el cual es llamado el grupo de unidades módulo n citado en el ***Ejemplo 1.4***. El orden de este grupo $U(n)$ es $\phi(n)$ la funcion ϕ de Euler. Cuando $n = p$ primo entonces $U(n)$ es isomorfo a Z_{p-1}.

Teorema 1.1.14.- Todo subgrupo de un grupo cíclico es cíclico. Si $G = \langle a \rangle$ y es de orden n, entonces para cada divisor k de n, el grupo G tiene exactamente un subgrupo de orden k, $\langle a^{n/k} \rangle$.

Teorema 1.1.19.- Si G es un grupo y H un subgrupo de G, entonces el conjunto:

$N[H] = \{x \in G$, tales que $x^{-1}Hx = H\}$, es un subgrupo de G.

Teorema 1.1.20.- Si G es un grupo y H un subgrupo de G, para cada x en G el conjunto: $x^{-1}Hx = \{ x^{-1}hx$, con $h \in H\}$, es un subgrupo de G, llamado el ***conjugado*** de H en G.

El siguiente es el primer resultado realmente importante de la teoría de grupos, aunque su demostración es relativamente fácil, este teorema tiene implicaciones muy fuertes en el estudio de los grupos finitos.

Teorema 1.1.21.- ***(Teorema de Lagrange).*** Si G es un grupo finito y H un subgrupo de G, entonces el orden de H divide al orden de G.

Corolario 1.1.22.- Si G es un grupo finito y a es un elemento de G entonces el orden de a divide al orden de G.

Una implicación importante del ***Corolario 1.1.22*** es que si un grupo finito es de orden primo entonces dicho grupo es cíclico.

Corolario 1.1.23.- Si G es un grupo finito y H un subgrupo de G, entonces el número de clases laterales de H en G es |G| / |H|. A este número de clases laterales se le denomina el ***índice*** de H en G, el cual se denota (G : H).

En la Sección 1.2 nos referiremos principalmente a los subgrupos normales y a los resultados más importantes de éstos, que serán requeridos en los capítulos posteriores.

"Es tributo del genio de Galois es el reconocer que los subgrupos en los cuales las clases laterales derechas e izquierdas coinciden son distinguidos. Frecuentemente en Matemáticas el problema crucial es reconocer y descubrir cuáles son los conceptos relevantes; una vez que esto se ha realizado, más de la mitad del trabajo se ha hecho"

I.N. Herstein, Topics in Álgebra.

Definición 1.2.1.- Un subgrupo N de un grupo G es llamado un ***subgrupo normal*** de G, si $Na = aN$ para todo a en G. Denotaremos esto por $N \lhd G$.

El siguiente teorema es de bastante utilidad a la hora de que se quiere demostrar la normalidad de un subgrupo.

Teorema 1.2.2.- Un subgrupo N del grupo G es normal en G, si, y sólo si, $g^{-1}Ng \subseteq N$ para toda g en G.

Para explicar el especial significado que tienen los subgrupos normales, daremos una simple razón, cuando un subgrupo N es normal en G, entonces el conjunto de las

clases laterales derechas (izquierdas) es él mismo un grupo, llamado el ***grupo cociente*** de G módulo N, denotado G/N, lo cual expresamos en el siguiente:

Teorema 1.2.3.- Sea G un grupo y N un subgrupo normal de G. El conjunto

$G/N = \{Ng, g \in G\}$, es un grupo bajo la operación $(Na)(Nb) = Nab$.

Teorema 1.2.4.- El subgrupo N[H] del ***Teorema 1.1.19***, es tal que:

1) Contiene a H.
2) H es normal en N[H].
3) Es el mayor de los subgrupos de G en el que H es normal.

A este subgrupo se le denomina el ***normalizador*** de H en G.

Teorema 1.2.5.- Si H es un subgrupo de G y K es un subgrupo normal de G, entonces el conjunto $HK = \{hk$, donde $h \in H$ y $k \in K\}$, es un subgrupo de G.

La sección que a continuación se exhibirá, contiene el concepto de homomorfismo de grupos, propiedades fundamentales y los teoremas de homomorfismos que se citarán en capítulos posteriores.

Definición 1.3.1.- Un homomorfismo ϕ de un grupo G en un grupo G', es una función

$\phi: G \rightarrow G'$, tal que $\phi(ab) = \phi(a)\phi(b)$ $\forall\, a, b \in G$.

Definición 1.3.2- El ***kernel*** de un homomorfismo $\phi: G \rightarrow G'$, es el conjunto:

$$\textbf{\textit{Ker}}\ \phi = \{ x \in G, \text{ tales que } \phi(x) = e' \}$$

Teorema 1.3.3.- Sea $\phi: G \rightarrow G'$ un homomorfismo con $\textbf{\textit{Ker}}\ \phi = K$, entonces, $\textbf{\textit{Ker}}\ \phi$ es un subgrupo normal de G.

Las propiedades que cumplen los homomorfismos de grupos se expresan en el siguiente teorema.

Teorema 1.3.4.- Sea $\phi: G \rightarrow G'$ un homomorfismo, sea g un elemento de G y H un subgrupo de G, entonces:

1) $\phi(e) = e'$.

2) $\phi(g^n) = [\phi(g)]^n$

3) $\phi(H) = \{\phi(h), \text{ con } h \in H\}$ es un subgrupo de G'.

4) Si H es cíclico, entonces $\phi(H)$ es cíclico.

5) Si H es abeliano, entonces $\phi(H)$ es abeliano.

6) Si H es normal, entonces $\phi(H)$ es normal.

7) Si $|g| = n$, entonces $|\phi(g)|$ divide a n.

8) Si $|H| = n$, entonces $|\phi(H)|$ divide a n.

9) Si K' es un subgrupo de G', entonces $\phi^{-1}(K') = \{k \in K / \phi(k) \in K'\}$, es un subgrupo de G.

10) Si K' es un subgrupo normal de G', entonces $\phi^{-1}(K') = \{k \in K / \phi(k) \in K'\}$, es un subgrupo normal de G.

Definición 1.3.5.- Cuando un homomorfismo $\phi: G \rightarrow G'$, es inyectivo, se dice que es un ***isomorfismo***. En el caso de que ϕ sea suprayectivo diremos que los grupos son ***isomorfos***, es decir: dos grupos son isomorfos si existe un homomorfismo biyectivo definido entre ellos. En tal caso lo denotaremos $G \approx G'$.

Teorema 1.3.6.- ***(Primer Teorema de Homomorfismos)*** Sea ϕ un homomorfismo del grupo G sobre el grupo G', con kernel ***Ker*** $\phi = K$, entonces $G' \approx G/K$, y el isomorfismo entre ellos esta dado por:

$\psi: G/K \rightarrow G'$, definida como $\psi(Kg) = \phi(g)$.

Teorema 1.3.7.- ***(Segundo Teorema de Homomorfismos)*** Sea ϕ un homomorfismo del grupo G sobre el grupo G', con kernel ***Ker*** $\phi = K$ y H' un subgrupo de G', entonces $H = \phi^{-1}(H')$, es tal que:

1) $K \subset H$.

2) $H/K \approx H'$.

3) $H' \triangleleft G' \rightarrow H \triangleleft G$.

Teorema 1.3.8.- ***(Tercer Teorema de Homomorfismos)*** Sea ϕ un homomorfismo del grupo G sobre el grupo G', con kernel ***Ker*** $\phi = K$ y si $N' \triangleleft G'$ y $N = \phi^{-1}(N')$, entonces $G/N \approx G'/N'$, en forma equivalente $G/N \approx (G/K)/(N/K)$.

Definición 1.3.9.- Un isomorfismo de un grupo G en sí mismo es llamado un ***automorfismo*** de G.

Definición 1.3.10.- Sea G un grupo y a un elemento de G, la funcion ϕ_a definida por $\phi_a(x) = axa^{-1} \quad \forall x \in G$, es un automorfismo de G, llamado el ***automorfismo interior*** de G inducido por a.

Al conjunto de todos los automorfismos del grupo G se le denota usualmente como *Aut*(G) y al conjunto de todos los automorfismos interiores de G se denota *Inn*(G).

Teorema 1.3.11.- Si G es un grupo entonces *Aut*(G) e *Inn*(G), son grupos bajo la composición.

Teorema 1.3.12.- Si p es primo entonces $Aut(G) \approx Z_{p-1}$.

Una demostración de este importante resultado puede verse en [VII].

En esta cuarta y ultima sección de este capítulo se abordará el tema de los Productos Directos, mismos que serán de bastante utilidad para obtener la meta propuesta en el presente trabajo.

Definición 1.4.1.- Sean H y K subgrupos del grupo G. Diremos que G es el producto directo de H y K, lo cual denotaremos por $G = H \times K$, si:

1) $G = HK$,

2) $H \cap K = \{ e \}$,

3) $hk = kh$, $\forall\, h \in H$ y $k \in K$.

La condición 3) de la definición anterior implica la normalidad de H y K, probaremos en el siguiente lema el recíproco de esta implicación, es decir, que si dos subgrupos normales cumplen las condiciones 1) y 2) entonces la condición 3) se cumple y por tanto G es el producto directo de estos dos subgrupos normales.

Lema 1.4.2.- Sea G un grupo. $H \lhd G$ y $K \lhd G$ tales que cumplen las siguientes condiciones:

1) $G = HK$,

2) $H \cap K = \{ e \}$,

entonces $hk = kh$ $\forall\ h \in H$ y $k \in K$ y por tanto $G = H \times K$.

Demostración.- Consideremos el elemento $a = hkh^{-1}k^{-1}$, con $h \in H$ y $k \in K$. Asociando podemos expresar a a como $a = (hkh^{-1})k^{-1}$, de la normalidad de K se tiene que $hkh^{-1} \in K$, lo cual implica que $a \in K$; análogamente re-expresando a $a = h(kh^{-1}k^{-1})$, de la normalidad de H se tiene que $a \in H$, de donde $a \in H \cap K$, pero por la condición 2) tenemos que $H \cap K = \{ e \}$, así que $a = e$, de donde obtenemos que $hk = kh \ \forall \ h \in H$ y $k \in K$. ■

La condición 1) de la ***Definición 1.4.1*** establece que todo elemento de $g \in G$, puede ser expresado de la forma $g = hk$, con $h \in H$ y $k \in K$, demostraremos en la siguiente Teorema que esta expresión es <u>única</u>.

Teorema 1.4.3.- Si G es el producto directo de los subgrupos H y K entonces para cada $g \in G$, existen únicos $h \in H$ y $k \in K$, tales que $g = hk$.

Demostración.- La condición 1) de la ***Definición 1.4.1*** establece la existencia de los elementos $h \in H$ y $k \in K$, tales que $g = hk$, supongamos que existen $h' \in H$ y $k' \in K$, tales que $g = h'k'$, entonces $hk = h'k'$ de donde $kk'^{-1} = h^{-1}h'$, de donde $kk'^{-1} \in H \cap K$, pero por la condición 2) tenemos que $H \cap K = \{ e \}$, de donde $kk'^{-1} = e$, así que $k = k'$; análogamente $h = h'$. ■

La mayor parte del contenido de este capítulo puede referirse a [I], [III], [VI] y [VII]

CAPITULO II.

2.1.- *ACCIONES DE GRUPOS EN CONJUNTOS.*

En esta parte del trabajo se abordará el Tema de las Acciones de un Grupo en un Conjunto, herramienta con la cual como se verá se demostrarán los Teoremas de Sylow de una forma muy compacta ya que las demostraciones originales de dichos teoremas en los textos tradicionales son algunas veces por demás demasiado extensas. También en esta sección se obtendrán algunos resultados como la Ecuación de Clase, el Normalizador, el Teorema de Cauchy como aplicaciones de la Teoría desarrollada en esta parte.

Iniciamos el Capítulo con algunas definiciones y resultados importantes.

Definición 2.1.1.- Sea X un conjunto y G un grupo. Una acción de G en X es una función $\phi : X \times G \to X$ tal que:

1.- $\phi(x, e) = x \ \forall\, x \in X$ y e es el elemento neutro de G.

2.- $\phi(x, g_1g_2) = \phi[\phi(x, g_1), g_2] \ \forall\, x \in X$ y $g_1, g_2 \in G$.

Bajo estas condiciones diremos que X es un G-conjunto.

Cuando X es un G-conjunto distinguiremos por el momento dos conjuntos especiales, primero el subconjunto de X de todos los elementos x, tales que $\phi(x, g) = x$ para alguna $g \in G$ fija, y en segundo término a el subconjunto de G que consiste en todos los elementos de G que dejan fijo a un $x \in X$ en particular. En símbolos, sean:

$X_g = \{x \in X / \phi(x, g) = x\}$ y $G_x = \{g \in G / \phi(x, g) = x\}$ tales subconjuntos.

Teorema 2.1.2.- Sea X un G-conjunto. Entonces, para cada $x \in X$, G_x es un subgrupo de G.

Demostración.- G_x es no vacío ya que por la parte 1 de la ***Definición 2.1.1***, al menos tenemos que $e \in G_x$ para cada $x \in X$. Ahora bien sean $g_1, g_2 \in G_x$, es decir: $\phi(x, g_1) = x$ y $\phi(x, g_2) = x$, de donde: $\phi(x, g_1g_2) = \phi[\phi(x, g_1), g_2] = \phi(x, g_2) = x$, lo cual implica que g_1g_2 está en G_x, de donde G_x es cerrado. Además para todo $g \in G_x$, tenemos que: $x = \phi(x, e) = \phi(x, gg^{-1}) = \phi[\phi(x, g), g^{-1}] = \phi(x, g^{-1})$, lo cual implica que $g^{-1} \in G_x$. De aquí que por la ***Teorema 1.1.3***, G_x es un subgrupo de G. Es decir este subgrupo de G asociado al elemento x, consiste en todos los elementos del grupo G que al actuar sobre x no lo modifican, a tal subgrupo lo denominaremos el ***Subgrupo de Isotropía de*** **x**. ■

Teorema 2.1.3.- Sea X un G-conjunto. Para $x_1, x_2 \in X$, definamos la relación $x_1 \sim x_2$, sí, y sólo sí, existe algún $g \in G$ tal que $\phi(x_1, g) = x_2$. Entonces $\sim$ es una relación de equivalencia.

Demostración.- Para toda $x \in X$, se tiene que $\phi(x, e) = x$, de donde $x \sim x$, así $\sim$ es reflexiva. Supongamos que $x_1 \sim x_2$, es decir existe algún $g \in G$ tal que $\phi(x_1, g) = x_2$, consideremos $\phi(x_2, g^{-1})$; $\phi(x_2, g^{-1}) = \phi[\phi(x_1, g), g^{-1}] = \phi(x_1, gg^{-1}) = \phi(x_1, e) = x_1$, de aquí que $x_2 \sim x_1$, de donde $\sim$ es simétrica. Por último, supongamos que $x_1 \sim x_2$ y que $x_2 \sim x_3$,

es decir existen g_1, $g_2 \in G$ tales que $\phi(x_1, g_1) = x_2$ y $\phi(x_2, g_2) = x_3$, consideremos: $\phi(x_1, g_1g_2)$; $\phi(x_1, g_1g_2) = \phi[\phi(x_1, g_1), g_2] = \phi(x_2, g_2) = x_3$, de donde $x_1 \sim x_3$, por tanto $\sim$ es transitiva y esto lo hace una relación de equivalencia.■

Como toda relación de equivalencia, esta nos proporciona una partición de X en clases de equivalencia ajenas y cuya unión es todo X. En particular cada $x \in X$ pertenece a una y solo una clase de equivalencia a la que llamaremos la **órbita** de x y la denotaremos xG.

El siguiente resultado nos muestra como están relacionados las órbitas de los elementos con los correspondientes subgrupos de isotropía.

Teorema 2.1.4.- Sea X un G-conjunto y $x \in X$. Entonces:

$$| xG | = (G: G_x)$$

Demostración.- Sea $\Re$ el conjunto de las clases laterales derechas de G_x en G. Como el número de estas clases laterales derechas es precisamente el índice de G_x en G, se exhibirá una función φ de xG en $\Re$ biyectiva para la demostración de este teorema. Sea $x_1 \in xG$, entonces existe $g \in G$, tal que $\phi(x, g) = x_1$, sea $\varphi(x_1) = G_x g$. Probaremos primero que $\varphi(x_1)$ es independiente de la selección de g, para esto supongamos que g' en G es tal que $\phi(x, g') = x_1$. Pero $\phi(x, g) = x_1$ implica que $\phi(x_1, g^{-1}) = x$, de donde:

$x = \phi(x_1, g^{-1}) = \phi[\phi(x, g'), g^{-1}] = \phi(x, g'g^{-1})$, de esto se tiene que $g'g^{-1} \in G_x$, por tanto $g' \in G_x g$, así se tiene que $G_x g = G_x g'$, lo que nos dice que φ está bien definida.

Supongamos ahora que $x_1, x_2 \in xG$, entonces existen $g_1, g_2 \in G$ tales que $\phi(x, g_1) = x_1$ y $\phi(x, g_2) = x_2$, además supongamos también que $\varphi(x_1) = \varphi(x_2)$ esto implica que $G_x g_1 = G_x g_2$ de aquí que $g_1 \in G_x g_2$, lo cual nos dice que $g_1 = gg_2$ para algún $g \in G_x$, de esto se tiene que: $x_1 = \phi(x, g_1) = \phi(x, gg_2) = \phi[\phi(x, g), g_2] = \phi(x, g_2) = x_2$, lo cual implica que φ es uno-a-uno.

Por último, sea $G_x g_1 \in \Re$ una clase lateral derecha de G_x en G, sea $x_1 = \phi(x, g_1)$, entonces $x_1 \in xG$, además $\varphi(x_1) = G_x g_1$ de donde φ es sobre. Por tanto φ es una función biyectiva de xG en $\Re$, de donde $|xG| = |\Re| = (G: G_x)$ para cada $x \in X$. ■

Es decir el número de elementos que tiene la órbita a la que pertenece x es igual al índice de su correspondiente subgrupo de isotropía. Vale la pena aclarar que con este resultado estamos "contando" los elementos de un conjunto en términos de índices de subgrupos.

Antes de continuar con más resultados puramente teóricos, veamos un ejemplo concreto.

Consideremos $G = D_4$, el grupo de simetrías cuadrado llamado también el grupo octal o bien el grupo Diédrico de orden 8 en el cual definiremos sus elementos como sigue:

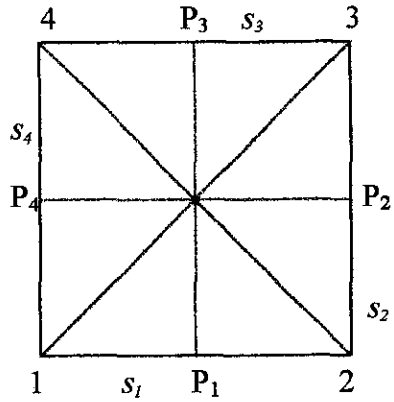
ρ_0 = la rotación de 0° $\quad\quad$ μ_1 = la reflexión con respecto a la mediatriz m_1

ρ_1 = la rotación de 90° $\quad\quad$ μ_2 = la reflexión con respecto a la mediatriz m_2

ρ_2 = la rotación de 180° δ_1 = la reflexión con respecto a la diagonal d_1

ρ_1 = la rotación de 270° δ_2 = la reflexión con respecto a la diagonal d_2

Y en el cuadrado distinguiremos sus elementos como sigue:



los vértices del cuadrado:1, 2, 3, 4; los lados: s_1, s_2, s_3, s_4; las diagonales: d_1, d_2; las mediatrices vertical y horizontal: m_1, m_2; al centro C; P_i los puntos medios de los lados s_i.

$$\text{Sea } X = \{1, 2, 3, 4, s_1, s_2, s_3, s_4, m_1, m_2, d_1, d_2, C, P_1, P_2, P_3, P_4\}$$

En este sentido podemos considerar a X como un D_4-conjunto, como se describe en la siguiente tabla, la totalidad de la acción de D_4 en X.

	1	2	3	4	s_1	s_2	s_3	s_4	m_1	m_2	d_1	d_2	C	P_1	P_2	P_3	P_4
ρ_0	1	2	3	4	s_1	s_2	s_3	s_4	m_1	m_2	d_1	d_2	C	P_1	P_2	P_3	P_4
ρ_1	2	3	4	1	s_2	s_3	s_4	s_1	m_2	m_1	d_2	d_1	C	P_2	P_3	P_4	P_1
ρ_2	3	4	1	2	s_3	s_4	s_1	s_2	m_1	m_2	d_1	d_2	C	P_3	P_4	P_1	P_2
ρ_3	4	1	2	3	s_4	s_1	s_2	s_3	m_2	m_1	d_2	d_1	C	P_4	P_1	P_2	P_3
μ_1	2	1	4	3	s_1	s_4	S_3	s_2	m_1	m_2	d_2	d_1	C	P_1	P_4	P_3	P_2
μ_2	4	3	2	1	s_3	s_2	s_1	s_4	m_1	m_2	d_2	d_1	C	P_3	P_2	P_1	P_4
δ_1	3	2	1	4	s_2	s_1	s_4	s_3	m_2	m_1	d_1	d_2	C	P_2	P_1	P_4	P_3
δ_2	1	4	3	2	s_4	s_3	s_2	s_1	m_2	m_1	d_1	d_2	C	P_4	P_3	P_2	P_1

De esta tabla podemos observar por ejemplo que:

$$X\rho_0 = X,\ X\rho_1 = \{C\},\ X\mu_1 = \{s_1, s_3, m_1, m_2, C, P_1, P_3\}$$

Además:

$$G_1 = \{ \rho_0, \ \delta_2 \}, G_{s_3} = \{ \rho_0, \mu_1 \}, \ G_{d_1} = \{ \rho_0, \rho_2, \delta_1, \delta_2 \},$$

Por ultimo algunos ejemplos de órbitas:

$s_1G = \{ s_1, s_2, s_3, s_4 \}$, $P_3G = \{ P_1, P_2, P_3, P_4 \}$, $d_1G = \{ d_1, d_2 \}$, etc.

Cuando G es un grupo finito y X es un G-conjunto finito, podemos afirmar que hay un número finito de órbitas en X. Sea r en este caso el número de órbitas en X. Si elegimos un representante de cada órbita, consideremos el conjunto $\{x_1, x_2, ..., x_r\}$ que tiene a un elemento de cada órbita de X, entonces

$$| X | = \sum_{i=1}^{r} | x_iG | \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Como puede haber órbitas con un solo elemento. Sea

$$X_G = \{x \in X / xg = x, \ \forall g \in G\}$$

El conjunto que contiene a todas las órbitas con un solo elemento, supongamos que hay s de tales órbitas, entonces la ecuación (1) puede escribirse como sigue:

$$|X| = |X_G| + \sum_{i=s+1}^{r} |x_iG| \ldots\ldots\ldots\ldots (2)$$

Observación 2.1.5.- Consideremos en particular el caso en que X = G, G es un grupo finito y la acción de G en X por conjugación de modo que $g \in G$ lleva a $x \in G$ en $g^{-1}xg$, entonces G es un G-conjunto y

$X_G = \{x \in X / g^{-1}xg = x, \ \forall g \in G\} = \{x \in X / gx = xg, \ \forall g \in G\} = Z(G)$ (el centro de G) ahora bien si $x \notin Z(G)$ entonces $|xG| = (G: G_x)$ donde G_x es el subgrupo de Isotropía de x, es decir $G_x = \{g \in G / g^{-1}xg = x\} = \{g \in G / gx = xg\} = C(x)$ (el centralizador de x)

Así la ecuación (2) la podemos escribir como:

$|G| = |Z(G)| + \sum_{x \notin Z(G)} |G : C(x)|$ la cual es la llamada ***Ecuación de Clase***.

El resultado que a continuación se presenta nos permitirá hacer una demostración del ***Teorema de Cauchy*** como se había dicho con anterioridad, muy sencilla e ilustrativa.

Teorema 2.1.6.- Sea G un grupo de orden p^n con p primo y X un G-conjunto finito, entonces: $|X| \equiv |X_G| \pmod{p}$.

Demostración.- Por el ***Teorema 2.1.4*** se tiene que $|xG| = (G: G_x)$ para cada $x \in X$; ahora bien para todos aquellos $(G: G_x)$ que corresponden a elementos cuya órbita tiene mas de un elemento se tiene que estos índices dividen a $|G|$, de donde p divide a: $(G: G_{x_i}) = |x_i G|$ para $s + 1 \leq i \leq r$, de donde p divide a $\sum_{i=s+1}^{r} |x_i G|$ lo cual implica que p divide a $|X| - |X_G|$ por tanto $|X| \equiv |X_G| \pmod{p}$. ■

Teorema 2.1.7.- ***(Teorema de Cauchy).*** Sea G un grupo de orden finito y sea p un primo que divide a $|G|$. Entonces G tiene un elemento de orden p y por tanto un subgrupo de orden p.

Demostración.- Sea X el conjunto:

$$X = \{(g_1, g_2, \ldots, g_p) / \; g_1 g_2 \ldots g_p = e \text{ con } g_i \in G\}$$

Al formar un elemento de X podemos elegir arbitrariamente a las primeras *p-1* componentes y las *p*-ésima componente quedaría determinada de manera única por: $g_p = (g_1 g_2 \ldots g_{p-1})^{-1}$ de donde $|X| = |G|^{p-1}$. Como *p* divide al orden de G, entonces *p* también divide a $|X|$. Sea σ el ciclo (123...*p*) en S_p, hacemos que σ actúe en X mediante: $(g_1, g_2, \ldots, g_p)\,\sigma = (g_{1\sigma}, g_{2\sigma}, \ldots, g_{p\sigma}) = (g_2, g_3, \ldots, g_p, g_1)$ el cual es también un elemento de X, ya que $g_1 = (g_2 g_3 \ldots g_p)^{-1}$ de donde: $g_2 g_3 \ldots g_p g_1 = (g_2 g_3 \ldots g_p)(g_2 g_3 \ldots g_p)^{-1} = e$. Consideremos ahora el subgrupo cíclico generado por σ, $\langle\sigma\rangle$ de S_p y hagamos que actúe sobre X por iteración. Como $|\langle\sigma\rangle| = p$, entonces por el ***Teorema 2.1.6*** se tiene que $|X| \equiv |X_{\langle\sigma\rangle}| \pmod{p}$. De donde *p* divide a $|X_{\langle\sigma\rangle}|$ ya que *p* divide a $|X|$. Como σ y $\langle\sigma\rangle$ deja fijo a $(g_1, g_2, \ldots, g_p) \Leftrightarrow g_1 = g_2 = \ldots = g_p$ y como al menos $(e,e,\ldots,e)$ esta en $X_{\langle\sigma\rangle}$, entonces existe un elemento $a \in G$ tal que $a \neq e$ y $(a,a,\ldots,a) \in X_{\langle\sigma\rangle}$, de donde $a^p = e$, lo cual implica que $|a| = p$, además $\langle a\rangle$ es de orden *p*.■

Los conceptos y teoremas que se exhiben en seguida nos serán muy útiles en la demostración de los ***Teoremas de Sylow***.

Definición 2.1.8.- Un grupo G es un *p*-grupo si todo elemento de G es de orden una potencia de *p*. Un subgrupo de un grupo G es un *p*-subgrupo de G si el subgrupo es un *p*-grupo.

Corolario 2.1.9.- Sea G un grupo finito. Entonces G es un p-grupo sí, y sólo sí, el orden de G es una potencia de p.

Demostración.- Sea G un p-grupo. Supongamos que existe un primo $q \neq p$, tal que q divide al orden de G, entonces por el ***Teorema de Cauchy***, G tiene un elemento de orden q lo cual contradice en hecho de que G es un p-grupo ya que todos sus elementos son de orden una potencia de p, de donde $|G| = p^n$. Para el recíproco, por el ***Corolario 1.1.20***, se tiene que para todo $g \in G$, $|g|$ divide al $|G|$, entonces $|g|$ divide a p^n, lo cual implica que todo elemento de G es de orden una potencia de p. Por tanto G es un p-grupo.■

Observación 2.1.10.- Sea G un grupo y Γ la colección de todos los subgrupos de G. Γ es un G-conjunto, haciendo que G actúe por conjugación en Γ, es decir si $H \in \Gamma$ entonces la acción sería $\phi(H, g) = g^{-1}Hg$. Por el ***Teorema 2.1.2*** se tiene que:

$$G_H = \{g \in G / \phi(H, g) = H\}$$

Es el subgrupo de isotropía de H en G. Pero $\phi(H, g) = H$ implica que $g^{-1}Hg = H$ para aquellas $g \in G_H$. Ahora bien este subgrupo de G relativo a H ya era conocido y no es otro que el ***Normalizador*** de H, de donde $H \lhd G_H$, más aun G_H contiene a cualquier otro subgrupo de G en el que H sea normal. Denotaremos a G_H en la forma usual N[H].

Lema 2.1.11.- Sea H un p-subgrupo del grupo finito G, entonces,

$$(N[H]:H) \equiv (G:H) \pmod{p}$$

Demostración.- Sea $\mathfrak{R}$ el conjunto de todas las clases laterales derechas de H en G, entonces $|\mathfrak{R}| = (G:H)$.

Hagamos que H actúe en $\mathfrak{R}$ mediante la acción $\phi: \mathfrak{R} \times H \to \mathfrak{R}$, la traslación derecha es decir: para $Hx \in \mathfrak{R}$, $\phi(Hx, h) = Hxh$. Entonces $\mathfrak{R}$ es un H-conjunto. Determinemos $\mathfrak{R}_H$ es decir, todas las clases en $\mathfrak{R}$ que dejan fijas todos los elementos de H, o sea aquellas clases tales que $Hx = Hxh$ para toda $h \in H$, pero

$Hx = Hxh \ \forall h \in H \Leftrightarrow H = Hxhx^{-1} \ \forall h \in H \Leftrightarrow xhx^{-1} \in H \ \forall h \in H \Leftrightarrow xHx^{-1} \subset H$, además

$(x^{-1})^{-1}hx^{-1} = xhx^{-1} \in H \ \forall h \in H$, de donde $x^{-1} \in N[H]$, lo cual implica que $x \in N[H]$ de donde todas las clases en $\mathfrak{R}_H$ son aquellas clases de la forma Hx con $x \in N[H]$, de donde $(N[H]:H) = |\mathfrak{R}_H|$. Como H es un p-subgrupo de G entonces, por el ***Corolario 2.1.9*** $|H| = p^n$. Ahora bien por el ***Teorema 2.1.6*** se tiene que: $|\mathfrak{R}| \equiv |\mathfrak{R}_H| \pmod{p}$, de donde $(N[H]:H) \equiv (G:H) \pmod{p}$.■

Bibliografí consultada [III]

2.2.- *TEOREMAS DE SYLOW.*

El objetivo central de esta sección es el de demostrar los ***Teoremas de Sylow***, que podemos considerarlos parcialmente como la parte recíproca del ***Teorema de Lagrange***, es decir mientras el ***Teorema de Lagrange*** establece que el orden de cualquier subgrupo de un grupo finito divide al orden del grupo, su recíproco no es necesariamente cierto, por ejemplo el grupo S_4 tiene orden 24 pero no tiene subgrupo orden 6, y el primer teorema de Sylow establece que si la potencia de un primo p divide al orden de un grupo finito entonces este grupo contiene un subgrupo de ese orden. En particular si el grupo es abeliano finito, este tiene subgrupos de todos los ordenes que dividan al orden del grupo.

También los ***Teoremas de Sylow*** nos proporcionarán información muy importante en la clasificación de los grupos no abelianos.

Las demostraciones de los ***Teoremas de Sylow*** son otra aplicación del tema de Acciones de Grupos en Conjuntos. En las que el G-conjunto en esta ocasión será algunas veces el mismo grupo, otras una colección de clases laterales y en otras más una colección de subgrupos.

El Teorema que a continuación se enuncia y demuestra es conocido como el ***Primer Teorema de Sylow***.

Teorema 2.2.1.-(Primer Teorema de Sylow) Sea G un grupo de orden p^nm, con $n \geq 1$ y p no divide a m, entonces:

1.- G contiene un subgrupo de orden p^i para cada $1 \leq i \leq n$.

2.- Todo subgrupo H de G de orden p^i es normal en algún subgrupo de orden p^{i+1} para $1 \leq i < n$.

Demostración.- Para $n = 1$, por el ***Teorema 2.1.7 (Teorema de Cauchy),*** se tiene que G contiene un subgrupo de orden p, por tanto el teorema se cumple para $n = 1$. Se hará la prueba por inducción sobre n, es decir se demostrará que le existencia de un subgrupo de orden p^i, implica que existencia de un subgrupo de orden p^{i+1}. Sea H un subgrupo de G de orden p^i, con $i < n$, entonces p divide a (G : H), de donde por el ***Lema 2.1.11,*** se tiene que p también divide a (N[H]:H). Ahora bien H es normal en N[H], entonces podemos formar el grupo cociente N[H]/H y tenemos que p también divide al orden de este grupo cociente, ya que el orden de este grupo cociente es precisamente el índice de H en N[H], entonces por el ***Teorema 2.1.7***, N[H]/H tiene un subgrupo K de orden p.

Consideremos ahora el homomorfismo natural γ: N[H] $\rightarrow$ N[H]/H, $\gamma(n) = Hn$ $\forall n \in$ N[H], entonces por el ***Teorema 1.3.7***, la imagen inversa de K, $K\gamma^{-1}$, es un subgrupo de N[H] y por tanto de G, que contiene a H y es de orden p^{i+1}, ya que $Ker\ \gamma =$ H, y como $K\gamma^{-1}$ /H es isomorfo a K, entonces: $|K\gamma^{-1}| = |H|\,|K| = p^i\, p = p^{i+1}$, ya que por la hipótesis de inducción $|H| = p^i$.

Así queda demostrada la primera parte del teorema.

Para la parte 2) se tiene que H es normal en N[H] y $K\gamma^{-1}$ es un subgrupo de N[H] que contiene a H, de donde H es normal en $K\gamma^{-1}$ que es un posiblemente menor que N[H].■

El Teorema anterior garantiza la existencia de subgrupos de orden una potencia de p para cada una de éstas que dividan al orden del grupo.

A continuación se introduce en concepto de ***p*-subgrupo de Sylow** y el ***Segundo Teorema de Sylow*** que establece una característica bastante interesante que tienen estos subgrupos.

Definición 2.2.2.- Un ***p*-subgrupo de Sylow** P de un grupo G es un p-subgrupo maximal de G, esto es un p-subgrupo que no está contenido en un p-subgrupo mayor.

Teorema 2.2.3.- ***(Segundo Teorema de Sylow)***.- Sean P_1 y P_2 ***p*-subgrupos de Sylow** de un grupo finito G, entonces P_1 y P_2 son subgrupos conjugados en G.

Demostración.- Se hará la demostración usando el concepto de acción de grupo, y la estrategia es hacer actuar uno en las clases laterales derechas del otro. Sea $\mathfrak{R}$ el conjunto de todas las clases laterales derechas de P_1, en este sentido los elementos de $\mathfrak{R}$ son subconjuntos de la forma P_1x, con $x \in G$.

Definamos la acción de grupo de P_2 en $\mathfrak{R}$, definida por $\phi(P_1x, g) = P_1xg$, para toda $P_1x \in \mathfrak{R}$ y toda $g \in P_2$, a esta acción es llamada en algunos textos "traslación derecha".

En este sentido hemos convertido a $\mathfrak{R}$ en un P_2-conjunto y por tanto podemos hacer uso de la teoría desarrollada en la Sección 2.1. Haremos uso del ***Teorema 2.1.6*** en el que se tiene que: $|\mathfrak{R}| \equiv |\mathfrak{R}_{P_2}| \pmod{p}$, pero $|\mathfrak{R}| = (G : P_1)$ no es divisible por p ya que P_1 es un ***p*-subgrupo de Sylow** de G y por tanto su orden es la máxima potencia de p que divide al orden de G, de aquí que $|\mathfrak{R}_{P_2}| \neq 0$. Recordemos que $|\mathfrak{R}_{P_2}|$ es el número de orbitas de $\mathfrak{R}$ que constan de un solo elemento. Sea $P_1x \in \mathfrak{R}_{P_2}$ entonces se tiene que $P_1xg = P_1x \ \forall g \in P_2$, de donde tenemos que $P_1xgx^{-1} = P_1 \ \forall g \in P_2$, así $xgx^{-1} \in P_1 \ \forall g \in P_2$, entonces $xP_2x^{-1} \subseteq P_1$ y como $|P_1| = |P_2|$ entontes $xP_2x^{-1} = P_1$ lo cual implica que P_1 y P_2 conjugados. ■

Corolario 2.2.4.- Sea G es un grupo abeliano finito, entonces G contiene un único ***p-subgrupo de Sylow*** para cada p que divida al orden de G.

Antes de hacer la demostración de este corolario, notemos que éste no es válido en el caso de que G no sea abeliano. Para esto basta un ejemplo.

Consideremos el grupo S_3, este grupo tiene un único subgrupo de orden 3, pero tiene 3 subgrupos de orden 2.

Demostración.- Supongamos que G es un grupo abeliano finito y p es un primo que divide al orden de G. El ***Teorema 2.2.1*** nos garantiza que G contiene un subgrupo de orden

una potencia de p para cada una de estas que divida al orden de G. Sean H y K dos ***p-subgrupo de Sylow*** de G. Entonces por el ***Teorema 2.2.3*** éstos han de ser conjugados, es decir $gHg^{-1} = K$ para toda g en G, de donde se tiene que $gH = Kg = gK$, ya que G es abeliano. Pero $gH = gK$ implica que $H = K$. ■

Retomando el ejemplo que se dio anteriormente, el hecho de que el subgrupo de orden 3 sea único nos es casual. En particular sabemos que dicho subgrupo es normal en S_3, este hecho lo estableceremos en el siguiente Lema.

Lema 2.2.5.- Si P es un ***p-subgrupo de Sylow*** de G y P es normal en G, entonces P es el único ***p-subgrupo de Sylow*** de G.

Demostración.- Supongamos que P y Q son ***p-subgrupo de Sylow*** de G y P es normal en G. De la normalidad de P se tiene que $g^{-1}Pg = P$, para toda $g \in G$.

Ahora bien por el ***Teorema 2.2.3*** se tiene que P y Q son conjugados, es decir que existe $x \in G$ tal que $x^{-1}Px = Q$, lo cual implica junto con la normalidad de P que $P = Q$, de donde P es único. ■

El recíproco también es válido y su prueba es inmediata.

El tercer y último de los teoremas de Sylow, nos proporcionará valiosa información sobre el número de subgrupos de Sylow de un grupo arbitrario finito, la cual nos será muy

útil en el Capítulo 5, que es precisamente el que contiene las Técnicas de Clasificación que se desarrollarán en este trabajo.

Teorema 2.2.6.- (Tercer Teorema de Sylow).- Si G es un grupo finito y p un primo que divide al orden de G, entonces el número de ***p-subgrupos de Sylow*** de G es congruente con 1 mod p y divide al orden de G.

Demostración.- La demostración de este teorema será también una aplicación de la acción de un grupo en un conjunto. En este caso el grupo que estará actuando sobre un conjunto será uno de los ***p-subgrupos de Sylow*** de G y el conjunto que consideraremos será una colección de ***p-subgrupos de Sylow*** de G. Sea P un ***p-subgrupo de Sylow*** de G y sea $\mathcal{P}$ la colección de todos los ***p-subgrupos de Sylow*** de G. Consideremos la acción ϕ de P en $\mathcal{P}$ definida por conjugación de manera que $x \in P$ lleva a $T \in \mathcal{P}$ en $x^{-1}Tx$, es decir:

$\phi(T, x) = x^{-1}Tx$, para toda $T \in \mathcal{P}$ y toda $x \in P$.

Entonces $\mathcal{P}$ es un P-conjunto, como P es un ***p-subgrupo de Sylow*** de G entonces es de orden una potencia de p y por el ***Teorema 2.1.6*** se tiene que:

$$|\mathcal{P}| \equiv |\mathcal{P}_P| \pmod{p},$$

Determinemos $\mathcal{P}_P$. Si $T \in \mathcal{P}_P$, entonces $x^{-1}Tx = T \ \forall x \in P$, de esto se sigue que $P \leq N[T]$. Como también $T \leq N[T]$, y ambos son ***p-subgrupos de Sylow*** de G, también son ***p-subgrupos de Sylow*** de N[T], entonces P y T son conjugados en N[T], como T es

normal en N[T], entonces T es su único conjugado en N[T], de donde P = T. Entonces $\mathcal{P}_P = \{P\}$, de donde $|\mathcal{P}| \equiv 1 \pmod{p}$, con lo cual tenemos la primera parte del teorema.

Para la segunda parte consideremos a G actuando por conjugación en $\mathcal{P}$, en este sentido tendríamos que $\phi(T, g) = g^{-1}Tg$, para todo T en $\mathcal{P}$ y toda g en G.

Como todos los ***p-subgrupos de Sylow*** de G son conjugados, según el ***Teorema 2.2.3*** entonces hay una sola órbita en $\mathcal{P}$ bajo G. De esto se sigue el número de elementos de $\mathcal{P}$ es igual al número de elementos que tenga esa órbita de $\mathcal{P}$. Además se tiene que si T es un elemento de $\mathcal{P}$, por el ***Teorema 2.1.4***, el número de elementos de su órbita es igual al índice del correspondiente subgrupo de Isotropía de T en G. En particular tenemos que éste subgrupo de isotropía $G_T = N[T]$, y su índice $(G : G_T)$ es un divisor del orden de G. De aquí que $|\mathcal{P}|$ es un divisor del orden de G. ■

Bibliografía consultada [III]

CAPITULO III.

GRUPOS ABELIANOS FINITOS

En esta parte del trabajo se abordará el Tema de los Grupos Abelianos Finitos los cuales son grupos que tienen una estructura más manejable que los grupos en general. Como se verá los Grupos Abelianos no son mas complicados que los grupos cíclicos, de hecho el objetivo central de este capítulo es el de exhibir, demostrar y aplicar el Teorema Fundamental de los Grupos Abelianos Finitos como una herramienta a utilizar en la clasificación de grupos finitos.

Antes de entrar en detalle, primero se hará un pequeño bosquejo de lo que será el contenido de esta parte. El Teorema Fundamental de los Grupos Abelianos finitos, afirma que todo grupo abeliano finito se puede expresar como el producto directo de grupos cíclicos, este resultado junto con los Teoremas de Sylow, nos proporcionarán la información suficiente para determinar todos los grupos abelianos no isomorfos que de determinado orden pueden existir, es decir la clasificación de los grupos abelianos finitos.

La estrategia que se seguirá para alcanzar la meta de este capítulo, será la de primero probar que todo grupo abeliano finito es el producto directo de sus p-subgrupos de Sylow; y cada p-subgrupos de Sylow es el producto directo de grupos cíclicos. Y con esto probar el Teorema Fundamental de Grupos Abelianos Finitos.

Teorema 3.1.- Sea G un grupo abeliano finito. Entonces G es el producto directo de sus p-subgrupos de Sylow.

Demostración.- Consideremos el orden de G expresado por el Teorema Fundamental de la Aritmética como el producto de potencias de primos, es decir:

$$| G | = p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k}$$

Donde los p_i son primos distintos. Por el ***Teorema 2.2.1.-(Primer Teorema de Sylow)***, G tiene un subgrupo de orden $p_i^{n_i}$ para cada $p_i^{n_i}$ que divida al orden de G y por el ***Corolario 2.2.4*** estos subgrupos son únicos. Sean $S_1, S_2, S_3, \ldots, S_k$, los ***p-subgrupos de Sylow*** de G de órdenes $p_1^{n_1}, p_2^{n_2}, \ldots, p_k^{n_k}$ respectivamente. Se hará la prueba del teorema por inducción sobre k. Es claro que el teorema es válido en el caso de que k sea igual a 1. Supongamos que el teorema se cumple para $k-1$, y a partir de esta hipótesis demostraremos que el teorema se cumple para k. Sea $A_0 = S_1S_2S_3 \ldots S_{k-1}$, como G es abeliano cada S_i es normal en A_0 y además cada S_i es también un p_i -subgrupo de Sylow de A_0 para $1 \leq i \leq k-1$. Entonces por la Hipótesis de Inducción A_0 es el producto directo de los $S_1, S_2, S_3, \ldots, S_{k-1}$. Demostraremos que G es el producto directo de $A_0 \times S_k$. Como los ordenes de A_0 y S_k son primos relativos, entonces $A_0 \cap S_k = \{ e \}$, de aquí que A_0S_k tiene tantos elementos como los que tiene G ya que:

$$|A_0S_k| = |A_0|\,|S_k| = \left[\,|S_1|\,|S_2| \ldots |S_{k-1}|\,\right]|S_k| = p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k} = |G|$$

cual implica que $G = A_0S_k$, de donde por el ***Lema 1.4.2*** se sigue que G es el producto

ecto de: $S_1, S_2, S_3, \ldots, S_k$ ■

Ahora demostraremos un teorema que nos asegura que todo *p*-grupo abeliano finito puede expresar como el producto directo de un subgrupo cíclico de máximo orden y gún otro subgrupo (llamado el complemento directo), con lo cual podremos demostrar el orema Fundamental de Grupos Abelianos Finitos de una forma por demás sencilla.

eorema 3.2.- Sea G un grupo abeliano finito de orden p^n, y a un elemento de G de orden máximo de todos los elementos de G, entonces $G \approx A \times Q$, donde $A \approx \langle a \rangle$ y Q es un subgrupo de G.

Demostración.- Por Inducción sobre n. Es claro que si $n = 1$, el teorema es válido ya ue G sería de orden p, por lo tanto cíclico generado por cualquier $a \neq e$, de donde endríamos que $G \approx \langle a \rangle \times \{ e \}$.

Supongamos que el teorema se cumple para todo *p*-grupo de orden menor que p^n. Sea a un elemento de G de orden máximo de todos los elementos de G, como G es un *p*-grupo entonces a es de orden p^s con $s \leq n$. En el caso de que $s = n$, el teorema se cumple al ya que $G \approx \langle a \rangle$ y en este caso podemos expresar a $G \approx \langle a \rangle \times \{ e \}$.

Consideremos el caso de que $s < n$. En este sentido $G - \langle a \rangle \neq \phi$ y basaremos la eba en la existencia en $G - \langle a \rangle$ de un elemento de orden p. Sea $x \in G - \langle a \rangle$, como G es to podemos elegir a x de orden mínimo, en tal caso el orden de x^p es menor que el orden x, entonces $x^p \in \langle a \rangle$, por tanto: $x^p = a^i$ para algún i. Si p no divide a i entonces i y el en de a son primos relativos de donde a^i es también un generador de $\langle a \rangle$, de donde el en de x^p sería igual al orden de a y por tanto el orden de x sería $p|a|$, lo cual es una tradicción con la elección de a.

Por lo anterior $p \mid i$, entonces $i = pt$ de donde $x^p = a^i = a^{pt} = (a^t)^p$. Bajo estas diciones consideremos $b = xa^{-t}$. Por tanto b es de orden p y es tal que no está en $\langle a \rangle$ ya e $x \notin \langle a \rangle$.

Sea $B = \langle b \rangle$. Se sigue de esto que $A \cap B = \{ e \}$. Sea $\hat{G} = G/B$, como $B \neq \{e\}$, an ntonces el orden de $\hat{G}$ es menor que el orden de G y para utilizar la hipótesis de inducción ecesitamos de un elemento de $\hat{G}$ de orden máximo. Como a es de orden máximo en G, obaremos que Ba es de orden máximo en $\hat{G}$. Para esto denotemos con $\bar{a} = Ba$. En este ntido tenemos que: $(\bar{a})^{|a|} = (Ba)^{|a|} = Ba^{|a|} = Be = B = \bar{e}$, de aquí que el orden de $\bar{a}$ divida l orden de a. Por otro lado $(\bar{a})^{|\bar{a}|} = \bar{e} = (Ba)^{|\bar{a}|} = Ba^{|\bar{a}|} = B$, implica que $a^{|\bar{a}|} \in B$, pero $a^{|\bar{a}|}$ es un elemento de A, de donde $a^{|\bar{a}|} \in A \cap B = \{ e \}$, de aquí que $a^{|\bar{a}|} = e$, lo cual implica que el orden de a divide al orden de $\bar{a}$, por lo que tenemos que $|a| = |\bar{a}|$. Así pues $\bar{a}$ es

bién de orden máximo en $\hat{G}$. De lo anterior $\hat{G} = \hat{A} \times U$, donde $\hat{A}$ es el subgrupo ico de $\hat{G}$ generado por $\bar{a}$ y U es un subgrupo de $\hat{G}$. Por el Segundo Teorema de omomorfismos se tiene que $U \approx Q/B$ donde Q es un subgrupo de G. Afirmaremos que e subgrupo Q es el complemento directo de A, para esto supongamos que:

$\cap Q \neq \{ e \}$, es decir supongamos que existe $u \in Q$ tal que $u = a^i$ para algún entero i. este sentido la clase $Ba^i \in U$ y también pertenece a $\hat{A}$, de donde $Ba^i \in \hat{A} \cap U$, pero $\cap U = \{\bar{e}\} = B$, entonces a^i está en B y además en A, de donde $u = a^i = e$ ya que: $\cap B = \{ e \}$. Es claro que todo elemento de A conmuta con cualquier elemento de Q que G es abeliano por lo que falta según el ***Lema 1.4.2***, mostrar que todo elemento de se puede expresar como el producto de un elemento de A y un elemento de Q.

Sea g un elemento arbitrario de G. Consideremos la clase $\hat{g} = Bg$, esta clase es un lemento de $\hat{G}$, de aquí que se pueda expresar como el producto de un elemento de $\hat{A}$ por n elemento de U, es decir $\hat{g} = \bar{a}^i\bar{u}$, de donde $\hat{g}\bar{a}^{-i} \in U$, por tanto $ga^{-i} \in Q$, así $ga^{-i} = q$, ara algún $q \in Q$, de donde $g = a^i q \in A \times Q$. Por tanto $G \approx A \times Q$.■

Corolario 3.3.- Si G es p-grupo abeliano finito, entonces G es el producto directo de subgrupos cíclicos.

Demostración.- Por el ***Teorema 3.2***, se tiene que G se puede expresar como el producto directo de un grupo cíclico de orden maximal en G y algún otro subgrupo Q de G llamado el complemento directo del subgrupo maximal. Este subgrupo Q es también un p-

upo, por tanto también lo podemos expresar como el producto directo de un subgrupo clico maximal de Q y algún otro subgrupo de Q. Podemos repetir el proceso a Q hasta gar a un complemento directo que sea un subgrupo cíclico, y con esto expresar a G como producto directo de subgrupos cíclicos. ■

Del ***Corolario 3.3,*** se sigue que si G es un *p*-grupo abeliano entonces G es el oducto directo de subgrupos cíclicos, pero el orden de dichos subgrupos es una potencia de *p* de donde si G es de orden p^n entonces $G = H_1 \times H_2 \times H_3 \times \ldots \times H_s$, donde cada H_i de orden p^{n_i}, de donde: $n = n_1 + n_2 + n_3 + \ldots + n_s$, a estos n_1, n_2, n_3, . . . ,n_s se les noce como los invariantes de G y estos son forman una partición de *n* y afirmaremos sin emostrarlo que una condición necesaria y suficiente para que dos *p*-grupos abelianos sean omorfos es que tengan los mismos invariantes. Una demostración de este resultado se uede ver en [II].

Para destacar la importancia del ***Corolario 3.3,*** consideremos el caso de determinar odos los grupos abelianos de orden p^3 para cualquier primo *p*. Como las posibles particiones de 3 son: 3 = 3, 3 = 2 + 1 y 3 = 1 + 1 + 1, entonces tendríamos que G puede ser: Z_{p^3}, si G tiene algún elemento de orden p^3, $Z_{p^2} \times Z_p$, si G tiene algún elemento de orden p^2, o bien $Z_p \times Z_p \times Z_p$, si todo elemento de G diferente de *e* es de orden *p*.

Teorema 3.4.- ***(Teorema Fundamental de Grupos Abelianos Finitos).*** Todo grupo abeliano finito es el producto directo de grupos cíclicos.

Demostración.- Como por el ***Teorema 3.1***, se tiene que si G es un grupo abeliano finito entonces es el producto directo de sus *p*-subgrupos de Sylow y por el ***Corolario 3.3***, cada *p*-subgrupo de Sylow es el producto directo de grupos cíclicos, el teorema se cumple.

Argumentemos un poco más este resultado. Sea G abeliano finito de orden $p_1^{n_1}p_2^{n_2}\ldots p_k^{n_k}$ donde los p_i son primos distintos. Sean S_1, S_2, S_3,..., S_k, los *p*-subgrupos de Sylow de G de órdenes $p_1^{n_1}, p_2^{n_2}, \ldots, p_k^{n_k}$ respectivamente, entonces G es el producto directo de: S_1, S_2, S_3,..., S_k. Ahora bien por el ***Corolario 3.3*** cada S_j es el producto directo de $H_{j_1} \times H_{j_2} \times H_{j_3} \times \ldots \times H_{j_s}$, donde cada H_{j_i} es cíclico de orden $p^{n_{ji}}$, y $n_j = n_{j1} + n_{j2} + n_{j3} + \ldots + n_{js}$, de donde:

$$G \approx (Z_{p_{11}} \times Z_{p_{12}} \times \ldots \times Z_{p_{1s1}}) \times (Z_{p_{21}} \times Z_{p_{22}} \times \ldots \times Z_{p_{2s2}}) \times \ldots \times (Z_{p_{j1}} \times Z_{p_{j2}} \times \ldots \times Z_{p_{jsj}}) \blacksquare$$

Bibliografía consultada [I], [II] y [V]

CAPITULO IV

PRODUCTOS SEMI-DIRECTOS.

En este capítulo se abordará el tema de los Productos Semi-Directos, herramienta que nos permitirá principalmente determinar a los grupos no abelianos que de orden dado pueden existir.

La principal característica que tienen los productos semi-directos es que tienen condiciones más débiles que los productos directos, pero con ellos podemos reconstruir grupos a partir de la existencia de algunos de sus subgrupos bajo ciertas condiciones. También veremos que los productos directos son casos particulares de los productos semi-directos.

Antes de entrar en detalle del tema, resolveremos el problema de determinar todos los grupos de orden 6 que existen, dicho problema es muy ilustrativo y contiene gran parte de la teoría que se desarrollara en este capítulo con la cual podremos alcanzar la meta que se ha propuesto en el presente trabajo.

Consideremos G un grupo de orden 6. Por la teoría de Sylow se tiene que este grupo contiene un único subgrupo A de orden 3 el cual es normal en G, además por el Teorema de Cauchy G contiene al menos un subgrupo B de orden 2, y por el tercer teorema de Sylow, el número de estos subgrupos puede ser 1 o 3. Como A y B son de orden primo, son cíclicos, e isomorfos a Z_3 y Z_2, respectivamente. Sea a un generador de A y b un

enerador de B. De lo anterior se sigue que $A \cap B = \{ e \}$, de aquí que $G = AB$, es ecir que podemos ver que todos los elementos de G son $\{ e, a, a^2, b, ab, a^2b \}$ y precisamente la forma de operar con ellos es la que nos determina los diferentes grupos de rden 6 que pueden existir.

Del hecho de que $A \lhd G$, se tiene que $bab^{-1} \in A$, para todo $a \in A$ y $b \in B$, pero uál elemento de A puede ser bab^{-1}. Es claro que no puede ser e ya que esto implicaría por ncelación que $a = e$, lo cual contradice el hecho de que a es un generador de A. Así pues ab^{-1} puede ser a o bien a^2.

De la primera opción se sigue que $ba = ab$ de donde G es abeliano y es en particular producto directo de $Z_3 \times Z_2 \approx Z_6$. Si consideramos la segunda opción, $bab^{-1} = a^2 = a^{-1}$, sigue que G es $S_3 \approx D_3$. Así pues los únicos subgrupos no isomorfos de orden 6 que ueden existir son: Z_6 ó S_3.

Retomando la argumentación anterior cabe resaltar los siguientes hechos:

i) Cuando en un grupo G se puede asegurar que existen subgrupos A y B con las características anteriores (normalidad de A, $A \cap B = \{e\}$ y $G = AB$), siempre podremos reconstruir a G en base a estos subgrupos.

ii) La reconstrucción cuando se puede realizar, depende de la asignación que elijamos para $bab^{-1} \in A$.

iii) En ambos casos Z_6 y S_3 tienen subgrupos con características similares (A y B), pero nos son isomorfos, lo cual nos lleva a considerar otro tipo de producto interior.

De ii) tenemos que si analizamos esta asignación para todos los elementos de A esto no es otra cosa que un automorfismo de A, para cada b en B. Por otro lado, si esta asignación la consideramos para los elemento de B, como a cada elemento de B le está asignando un automorfismo de A y estos forman un grupo bajo la composición, entonces al menos ésta debe preservar las propiedades de B como grupo, lo cual nos exige que sea un homomorfismo de B en *Aut*(A).

La definición y el lema siguientes formalizan lo dicho anteriormente.

Definición 4.1.- Un grupo G es un producto semi-directo de A por B, en el caso de que G contenga subgrupos A y B tales que:

a) $A \lhd G$.

b) $G = AB$ y

c) $A \cap B = \{ e \}$

El siguiente lema nos proporciona una característica fundamental de los productos semi-directos.

Lema 4.2.- Sea G un producto semi-directo de A por B. Entonces, existe un homomorfismo $\theta : B \rightarrow Aut(A)$, definido por: $b \mapsto \theta_b$ con

$$\theta_b(a) = bab^{-1}, \text{ para todas } a \text{ en } A.$$

emostración.- Es claro que para cada b en B, $\theta_b(a) = bab^{-1}$ considerándola como na función en la variable a, define un automorfismo de A, ya que A es normal en G, este es el llamado el automorfismo interior inducido por b. Además, si la consideramos como na función que a cada elemento b de B, le asocia el automorfismo lo que a final de uentas estamos haciendo es el de determinar que elemento de A le corresponde a: $\theta_b(a) = bab^{-1}$, entonces, para b y b' en B, se tiene:

$$\theta_{bb'}(a) = (bb')a(bb')^{-1}$$

$$= (bb')a(b'^{-1}b^{-1})$$

$$= b(b'ab'^{-1})b^{-1}$$

$$= b(\theta_{b'}(a))b^{-1}$$

$$= \theta_b(\theta_{b'}(a)),$$

lo cual no dice que θ es un homomorfismo de B $\rightarrow$ *Aut*(A) ■

El lema anterior nos garantiza la existencia de un homomorfismo de B $\rightarrow$ *Aut*(A) ya que *Aut*(A) $\neq \phi$, pues la función identidad siempre está en *Aut*(A), pero el objetivo central de este capítulo es el de reconstruir a G como un producto semi-directo de A por B, a partir solamente de A y B, y algún homomorfismo de B $\rightarrow$ *Aut*(A). Que bien podemos pensarlo como el recíproco del ***Lema 4.2.*** En este sentido convenimos en:

Definición 4.3.- Dados los subgrupos A y B de G y un homomorfismo $\theta : B \rightarrow$ *Aut*(A), entonces, un producto semi-directo G de A por B es realizado por θ, sí: $\theta_b(a) = bab^{-1}$, *para todas a en* A.

Definición 4.4.- Dados los grupos A y B y un homomorfismo $\theta : B \rightarrow$ *Aut*(A), entonces, $A \times_\theta B$ es el conjunto de pares ordenados $(a, b) \in A \times B$ y para estos definimos la operación binaria:

$$(a, b)(a', b') = (a\theta_b(a'), bb')$$

Teorema 4.5.- Sean A y B grupos y $\theta : B \rightarrow$ *Aut*(A) un homomorfismo dados, entonces, $G = A \times_\theta B$ es un producto semi-directo de A por B realizado por θ.

Demostración.- Primero demostraremos que G es un grupo. El que la operación sea cerrada se sigue de las definiciones anteriores. Para verificar asociatividad, consideremos:

$$[(a, b)(a_1, b_1)](a_2, b_2) = [a\theta_b(a_1), bb_1](a_2, b_2)$$

$$= (a\theta_b(a_1)\theta_{bb_1}(a_2), bb_1b_2)$$

$$= (a\theta_b(a_1)(\theta_b(\theta_{b_1}(a_2)), bb_1b_2)$$

$$= (a\theta_b(a_1\theta_{b_1}(a_2)), bb_1b_2)$$

$$= (a, b)[(a_1\theta_{b_1}(a_2), b_1b_2]$$

$$= (a, b)[(a_1, b_1)(a_2, b_2)].$$

El elemento (e_A, e_B), actúa como elemento identidad, lo cual es sencillo verificar, pero como el inverso de (a, b) viene dado por $(\theta_b^{-1}(a^{-1}), b^{-1})$, no es inmediato que cumpla con la propiedad requerida, por lo tanto hagamos dicha verificación:

$$(a, b)\,(\theta_b^{-1}(a^{-1}), b^{-1}) = (a\theta_b\,(\theta_b^{-1}(a^{-1}), b\,b^{-1})$$

$$=(a(\theta_{bb}{}^{-1}(a^{-1}), e_B)$$

$$=(a(\theta_e(a^{-1}), e_B)$$

$$=(a(a^{-1}), e_B)$$

$$=(e_A, e_B)$$

De donde G es un grupo. Podemos identificar a A como el subconjunto de G que consiste en todos los pares de la forma *(a, e)*, y la función $\pi : G \to B$ dada por $\pi\,(a, x) = x$, el cual es un homomorfismo de G en B con *ker* π = A, de donde A es normal en G. Identificando también a los elementos de B como las parejas de la forma *(e, b)*, entonces B es un subgrupo de G y es tal que $A \cap B = \{\ (e, e)\ \}$, además G = AB, así G es un producto semi-directo de A por B.

Para verificar que G es realizado por θ, calculemos:

$(e, b)\,(a, e)\,(e, b)^{-1} = (e\theta_b(a), be)(e, b^{-1}) = (\theta_b(a), b)(e, b^{-1}) = (\theta_b(a), e)$ ■

Como se había anticipado el ***Teorema 4.5***. exhibe como construir un grupo a partir de dos grupos y un homomorfismo de $\theta : B \to Aut(A)$. Cabe hacer la observación de que

en las hipótesis del teorema los grupos en cuestión, pueden ser arbitrarios, en este sentido podemos como sucede con los productos directos, distinguir los productos semi-directos internos y los productos semi-directos externos.

Teorema 4.6.- Si G un producto semi-directo de A por B. Entonces, $G \approx A \times_\theta B$, para algún homomorfismo $\theta : B \to Aut(A)$.

Demostración.- Como el ***Lema 4.2*** se define $\theta_b(a) = bab^{-1}$. Ahora bien del hecho de que G es un producto semi-directo de A por B se tiene que G = AB entonces cada elemento $g \in G$, tiene una expresión única de la forma $g = ab$ con $a \in A$ y $b \in B$ ya que $A \cap B = \{ e \}$, y la multiplicación en G satisface:

$$(ab)(a_1b_1) = a(b\, a_1b^{-1})\, bb_1 = a\theta_b(a_1)\, bb_1$$

Ahora bien si consideramos el mapeo $\Psi : A \times_\theta B \to G$, dado por $\Psi(a, b) = ab$, es claro que es un isomorfismo de grupos. ■

Como hemos observado los productos semi-directos cuando existen, están determinados por algún homomorfismo, veremos ahora cuando dos productos semi-directos dan lugar al mismo grupo.

Teorema 4.7.- Sean $\theta, \theta' : B \to Aut(A)$ homomorfismos. Si $\theta = \theta'\beta$ para algún $\beta \in Aut(B)$, entonces:

$$A \times_\theta B \approx A \times_{\theta'} B.$$

Demostración.- Sea π: $A \times_{\theta'} B \to A \times_\theta B$, dado por $\pi(a, b) = (a, \beta(b))$, entonces:

$\pi[(a_1, b_1)(a_2, b_2)] = \pi[a_1 \theta'_{b_1}(a_2), b_1 b_2] = [a_1 \theta'_{b_1}(a_2), \beta(b_1 b_2)] =$

$[a_1 \theta'_{b_1}(a_2), \beta(b_1)\beta(b_2)] = (a_1, \beta(b_1))(a_2, \beta(b_2)) = \pi(a_1, b_1)\pi(a_2, b_2)$.

De donde π es un homomorfismo, el cual es biyectivo β lo es, por tanto π es un isomorfismo, así $A \times_\theta B \approx A \times_{\theta'} B$. ■

Teorema 4.8.- $A \times_\theta B = A \times B \Leftrightarrow \theta$ es el homomorfismo trivial.

Demostración.-

$\Rightarrow$) Si $A \times_\theta B = A \times B$, entonces tenemos que $\forall a \in A$ y $b \in B$ tenemos que $ab=ba$, lo cual implica que $a = bab^{-1} = \theta_b(a)$ de donde $\theta_b(a)$ es el automorfismo identidad de *Aut*(A), por tanto θ asigna a todo elemento de B el elemento identidad de *Aut*(A), de donde θ sea el homomorfismo trivial.

$\Leftarrow$) Si θ es el homomorfismo trivial de $B \to Aut(A)$, entonces $\forall b \in B$, tenemos que el homomorfismo θ le asigna el automorfismo identidad de *Aut*(A), entonces:

$\theta_b(a) = a = bab^{-1}$ $\forall a \in A$ de donde $ab=ba$ $\forall a \in A$ y $b \in B$, por tanto la ***Definición 1.4.1***, tenemos que $A \times_\theta B = A \times B$.■

Bibliografía consultada [IV], [VI] y [VII]

CAPITULO V

ALGUNAS TÉCNICAS DE CLASIFICACIÓN DE GRUPOS FINITOS

En esta última parte del trabajo se exhibirá un conjunto de técnicas para clasificar grupos finitos, cuyo orden sea menor que 100 y dicho orden sea a lo más el producto de tres primos, no necesariamente distintos.

La estrategia a seguir, será la de primero establecer bajo que condiciones un grupo finito es abeliano, ya que como se vio en el Capítulo III, éstos están completamente caracterizados por el Teorema Fundamental de los Grupos Abelianos Finitos y después con la herramienta de los productos semi-directos determinaremos los no abelianos.

Cada una de las secciones de este capítulo las denominaremos "casos" pues en realidad son los posibles casos de ordenes de los grupos que vamos a contemplar.

En algunos de estos casos se exhibirá un ejemplo concreto de la técnica desarrollada, para los que su aplicación no sea demasiado obvia.

En toda esta sección denotaremos con p, q, r números primos tales que $p \leq q < r$.

Caso 1.- ***Grupos de orden p.***

Teorema 5.1.1.- Si G es un grupo de orden p, entonces G es isomorfo a Z_p.

Demostración.- Por el ***Teorema 2.1.7 (Teorema de Cauchy)***, G tiene un elemento de *a* orden *p*. Sea A = $\langle a \rangle$, como |A| = |G|, entonces A = G, de donde G es cíclico. Claramente la función $\psi : Z_p \rightarrow$ A, definida como $\psi(k) = a^k \; \forall \, k \in Z_p$, es un isomorfismo de grupos, por tanto A = G $\approx Z_p$.■

Los grupos que se incluyen en este caso son aquellos cuyo orden es: 1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 y 97.

Caso 2.- ***Grupos de orden p^2.***

Teorema 5.2.1.- Si G es un grupo de orden p^2, entonces G es isomorfo a uno de los grupos Z_{p^2} ó $Z_p \times Z_p$.

Demostración.- En este caso G es un *p*-grupo. Si G tiene un elemento de orden p^2, entonces G es cíclico y por tanto abeliano isomorfo a Z_{p^2}. En el caso de que G no tenga elemento de orden p^2, entonces por el ***Teorema 2.1.7 (Teorema de Cauchy)*** se tiene que contiene un elemento *a* de orden *p*. Sea A el subgrupo cíclico generado por *a*. De aquí A sea de orden *p*, por lo que A no es todo G, además por el ***Teorema 2.2.1 (Primer Teorema de Sylow*** es normal en G. Sea *b* un elemento de G tal que $b \notin$ A. El orden de elemento divide al orden de G y no es p^2, por tanto es también de orden *p*. Denotemos B al subgrupo cíclico generado por *b*, análogamente B también es normal en G.

Entonces A ∩ B = { e }, ya que si no fuera así un elemento $c \in$ A ∩ B, distinto de e generaría tanto a A como a B de donde A = B. Así tenemos que AB es un subgrupo de G y su orden es p^2, por lo que AB = G. Además por el , estos subgrupos son normales en G. Por tanto estos subgrupos cumplen con las hipótesis del ***Lema 1.4.2***, de donde G es el producto directo de A y B, por tanto isomorfo a $Z_p \times Z_p$; pero por el mismo ***Lema 1.4.2*** entonces G es abeliano.■

Una forma de representar a estos grupos es:

G = $\langle a,b \rangle$, donde $a^p = b^p = e$, con la relación $ab = ba$. Los grupos incluidos en este caso son los de orden: 4, 9, 25 y 49.

Caso 3.- Grupos de orden pq, con p ∤ q-1.

Teorema 5.3.1.- Si G es un grupo de orden pq con $p \nmid q-1$, entonces G es isomorfo a Z_{pq}.

Demostración.- En este caso por el ***Teorema 2.2.6 (Tercer Teorema de Sylow)*** , tenemos que los respectivos subgrupos de Sylow de orden p y q, son únicos, y por el ***Lema 2.2.5*** son normales. Denotemos con B el p-subgrupo de Sylow y con A el q-subgrupo de Sylow de G. Como p y q son distintos entonces A ∩ B = { e }, si no fuera así el elemento x en la intersección sería tal que su orden dividiría tanto a p como a q, lo cual implica que es 1, por tanto $x = e$. Además por la normalidad de A se tiene que AB es un subgrupo de G que tiene orden |AB| = |A||B| = pq, por tanto tenemos que G = AB, de donde por el ***Lema***

1.4.2, G es el producto directo de A por B. Y como p y q son primos relativos G es isomorfo a Z_{pq}, por tanto abeliano. ■

Este caso abarca los grupos de orden: 15, 33, 35, 51, 65, 77, 85, 87, 91 y 95.

El caso que a continuación se aborda es el primero en el que haremos uso de la teoría desarrollada en el Capítulo IV, es decir los Productos Semi-Directos. Posteriormente de dará una caracterización completa de los grupos de orden pq, que tiene a este caso como un caso particular, pero no deja de ser bastante ilustrativo de el uso de los productos semi-directos.

Caso 4.- ***Grupos de orden 2p.***

Teorema 5.4.1.- Si G es un grupo de orden $2p$, entonces G es isomorfo a Z_{2p} ó D_{2p}.

Demostración.- Como el caso p^2, incluye el caso $2p$, con $p = 2$, consideremos en este apartado que p es un primo mayor o igual que 3.

En esta situación tenemos por el ***Teorema 2.2.6 (Tercer Teorema de Sylow),*** que el número de p-subgrupos de Sylow de G es 1 y el número de 2-subgrupos de Sylow de G, es o p.

Como el p-subgrupo de Sylow es único, por el ***Lema 2.2.5***, éste es normal en G. En caso de que el numero de 2-subgrupos de Sylow de G, también sea 1, entonces por el mismo ***Lema 2.2.5*** este 2-subgrupo de Sylow es normal en G. Sea B el 2-subgrupo de

Sylow de G y A el p-subgrupo de Sylow de G. De esto se sigue que A es isomorfo a Z_p y B es isomorfo a Z_2.

De nuevo tenemos que $A \cap B = \{ e \}$, lo cual implica $|AB| = |A|\,|B| = 2p$, por tanto $G = AB$, de donde por el ***Lema 1.4.2***, G es el producto directo de A por B, así tenemos que $G \approx Z_2 \times Z_p \approx Z_{2p}$.

Supongamos que el 2-subgrupo de Sylow de G no es único. En tal caso denotemos por B, alguno de los subgrupos de orden 2 de G. De nuevo tenemos que $A \cap B = \{ e \}$, por tanto $|AB| = |A||B|$ de donde $G = AB$ y A es normal en G, así estos subgrupos cumplen con las condiciones de la ***Definición 4.1***, por tanto G es el producto semi-directo de A por B.

Aplicando el ***Teorema 4.6*** tenemos que $G \approx A \times_\theta B$ donde θ es algún homomorfismo de $B \rightarrow Aut(A)$. Determinaremos estos homomorfismos no triviales, si existen, ya que este como se vio en el ***Teorema 4.8***, el homomorfismo trivial produce en correspondiente producto directo, ya considerado.

Como $B \approx Z_2$ podemos presentarlo como $B = \langle b \rangle$ donde $b^2 = e$ y $A \approx Z_p$ podemos presentarlo como $A = \langle a \rangle$ donde $a^p = e$. Para determinar los homomorfismos de B en $Aut(A)$, necesitamos solo determinar la imagen de b ante este homomorfismo ya que B es cíclico y la imagen de los demás elementos de B se obtiene por composiciones repetidas

del homomorfismo θ. Como una característica de los homomorfismos de grupos es la de que el orden de la imagen homomorfica de un elemento divide al orden del elemento y en este caso b es de orden 2, entonces el automorfismo que corresponda a la imagen de b, es de orden 1 o 2. Pero si un automorfismo de A es de orden 1, entonces es el automorfismo identidad, que es el que nos define el homomorfismo trivial.

Pasemos al caso de determinar los automorfimos de A que son de orden 2. Primero consideremos su existencia, como $A \approx Z_p$, entonces $Aut(A) \approx Z_{p-1}$, y como para todo primo p que es mayor o igual que 3, 2 divide a $p-1$, tenemos que por el ***Teorema 2.1.7 (Teorema de Cauchy),*** $Aut(A)$ tiene un elemento de orden *2*.

Como cualquier automorfismo α de $A \approx Z_p$, está completamente determinado si conocemos la imagen del generador de A, entonces tenemos que: $\alpha(a)$ puede ser cualquier a^k con $1 \leq k \leq p-1$, ya que todos ellos son primos relativos con p, así que: $\alpha(a) = a^k$ de donde: $\alpha^2(a) = \alpha(a^k) = a^{k^2}$, por tanto si α es de orden 2 entonces $\alpha^2(a) = a$, lo cual implica que: $a^{k^2} = a$, de donde: $k^2 \equiv 1 (mod\, p)$.

Así tenemos que p divide a $k^2 - 1 = (k-1)(k+1)$ por tanto se tiene que $k = 1$ o bien $k = p - 1$. La opción en la que $k = 1$, nos lleva al automorfismo identidad . Y con la otra opción tenemos que $\alpha(a) = a^k = a^{q-1} = a^{-1}$. De aquí que tenemos dos opciones para determinar la imagen homomorfica de b: α_0 (el automorfismo identidad) o bien α, es decir tenemos dos homomorfismos θ y ψ de $B \rightarrow Aut(A)$, definidos como:

$\theta_b(a) = bab^{-1} = \alpha_0(a) = a$ y $\psi_b(a) = bab^{-1} = \alpha(a) = a^{-1}$.

Con el primero de ellos obtenemos el grupo G en el para todo a en A y b en B se tiene que $bab^{-1} = a$ por tanto G es abeliano, isomorfo a Z_{2p} como ya lo habíamos considerado.

Con el segundo producimos un grupo G en el que para todo $a \in$ A y $b \in$ B se tiene que $bab^{-1} = a^{-1}$, que representado con generadores y relaciones es:

G = $\langle a,b \rangle$, donde $a^p = b^2 = e$, con la relación $bab^{-1} = a^{-1}$.

El cual es el grupo Diédrico de orden $2p$ al que denotaremos D_{2p}. ■

Los grupos de este tipo contemplados en este trabajo son los de orden: 6, 10, 14, 22, 26, 34, 38, 46, 58, 62, 74, 82, 86 y 94.

Caso 5.- ***Grupos de orden pq con p | q-1.***

Teorema 5.5.1.- Si G es un grupo de orden pq, en el que p divide a q –1, entonces G es isomorfo a uno de los grupos Z_{pq} ó $Z_q \times_\theta Z_p$

Demostración.- En este caso como en el anterior tenemos que el número de p-subgrupos de Sylow, puede ser 1 o q, y el número de q-subgrupos de Sylow es 1. Por tanto el q-subgrupo de Sylow es único, de donde es normal en G, por el ***Lema 2.2.5***. En el caso de que el número de p-subgrupos de Sylow de G, sea 1, entonces este p-subgrupo es también normal

en G. De nuevo tenemos que estos subgrupos tienen solo el elemento identidad en común, de donde por el ***Lema 1.4.2***, G es el producto directo de estos subgrupos, Z_p y Z_q por lo tanto es Z_{pq}.

Consideremos el caso en que el número de p-subgrupos es distinto de 1. Denotemos por A el q-subgrupo de Sylow de G y B alguno de los subgrupos de G de orden p. Así tenemos que $A \cap B = \{ e \}$, y además $|G| = |AB|$, de nuevo como en el caso $2p$, G cumple con los requisitos de la ***Definición 4.1*** para ser un producto semi-directo de A por B, es decir que también por el ***Teorema 4.6***, en este caso tenemos que $G \approx A \times_\theta B$ donde θ es algún homomorfismo $B \rightarrow Aut(A)$, y el caracterizar a todos estos grupos, consiste en determinar todos los homomorfismos θ, que dan lugar a diferentes grupos de orden pq.

Para facilitar el manejo de la notación, identificaremos al subgrupo A como el subgrupo de G generado por un elemento a de orden q, y B el subgrupo de G generado por un elemento b de orden p, es decir: $A = \langle a \rangle$, con $a^q = e$ y $B = \langle b \rangle$, con $b^p = e$.

De manera análoga a la que se utilizó en el caso anterior, nuestra labor será la de determinar los homomorfismos de $B \rightarrow Aut(A)$, que sean de orden p, ya que el orden de la imagen homomorfica del generador b de B, ha de dividir a $|be = p$.

Pero $Aut(A) \approx Z_{q-1}$ y como p divide a $q - 1$, entonces $Aut(A)$ tiene un elemento de orden p, por el ***Teorema 2.1.7(Teorema de Cauchy)*** y por tanto un único subgrupo de

orden p, ya que $Aut(\mathrm{A})$ es cíclico, que consiste en automorfismos de $Aut(\mathrm{A})$ que sean de orden p. Ahora bien, como A es cíclico, tenemos que si α es un automorfismo de A, entonces $\alpha(a) = a^i$, con $1 \leq i \leq q-1$, ya que cada uno de estos a^i, es un generador de A, y α es de orden p si cumple la condición adicional: $i^p \equiv 1 (mod_q)$.

Denotemos con $\bar{\mathrm{A}}$ el conjunto que contiene los automorfismos de A que son de orden p.

Claramente $\bar{\mathrm{A}}$ es cíclico, ya que es un subgrupo de $Aut(\mathrm{A}) \approx Z_{q-1}$, lo cual implica que es generado por cualquier elemento que no sea la identidad del grupo, ya que es de orden p.

De lo anterior se sigue que tenemos orden $\bar{\mathrm{A}}$ alternativas de homomorfismos θ. Pero demostraremos mediante el ***Teorema 4.7***, que todas las que no sean triviales, dan lugar al mismo producto semi-directo.

Sean $\theta, \psi : \mathrm{B} \rightarrow Aut(\mathrm{A})$ homomorfismos de orden p. De nuevo basta determinar la imagen del generador b de B, para que el homomorfismo quede completamente definido.

En otras palabras:

θ es tal que $b \rightarrow \alpha_i \in \bar{\mathrm{A}}$ y ψ es tal que $b \rightarrow \alpha_j \in \bar{\mathrm{A}}$, más explícitamente:

$\theta_b(a) = \alpha_i(a) = a^i$ con i tal que $i^p \equiv 1 (mod\ q)$ y

$\psi_b(a) = \alpha_j(a) = a^j$ con j tal que $j^p \equiv 1 (mod\ q)$.

Para poder utilizar el ***Teorema 4.7***, lo que requerimos es de un automorfismo β de B, tal que $\psi = \theta\beta$. Para este propósito, utilizaremos a los automorfismos α_i y $\alpha_j \in \bar{A}$, que definieron a los homomorfismos θ y ψ, para determinar a β.

Como α_i y $\alpha_j \in \bar{A}$ y como ninguno de ellos es el neutro del grupo, entonces cualquiera de ellos es generador del grupo, así que sin pérdida de generalidad, consideremos a α_i el generador de $\bar{A}$. Entonces existe algún entero s tal que $(\alpha_i)^s = \alpha_j$, con $1 < s < p - 1$, ya que $\alpha_j \in \bar{A}$, donde el exponente s indica el número de veces que se compone α_i consigo mismo. En este sentido tenemos que: $(\alpha_i)^s (a) = a^{i^s} = \alpha_j(a) = a^j$.

Consideremos el automorfismo $\beta \in Aut(B)$, dado por $\beta(b) = b^s$, por tanto tenemos que:

$$\theta_{\beta(b)}(a) = \theta_{b^s}(a) = b^s (a^i) b^{-s} = a^{i^s} = a^j = \alpha_j(a) = \psi_b(a)$$

Por lo anterior, todos los homomorfismos de $B \rightarrow Aut(A)$, que no sean el trivial, dan lugar al mismo producto semi-directo, así que sin pérdida de generalidad, podemos considerar al homomorfismo $\theta_b(a) = bab^{-1} = a^i$, con $i^p \equiv 1 (mod_q)$, para identificar a este grupo. así $G = \langle a,b \rangle$, donde $a^p = b^p = e$, con la relación $bab = a^i$ e $i^p \equiv 1 (mod_q)$. ■

Ejemplo 5.4.2.- Sea G un grupo de orden 21. Analizaremos el caso en el que el número de los *3*-subgrupos de Sylow no es 1, (el otro caso es el producto directo). Consideremos: A el *7*-subgrupo de Sylow de G, y B alguno de los subgrupos de orden 3.

Como el grupo de automorfismos de A es isomorfo a Z_6 y este solo tiene dos elementos de orden tres, por tanto hay solo dos automorfismos de A que sean de orden 3. Estos son:

$$\alpha_1(a) = a^2 \text{ y } \alpha_2(a) = a^4$$

Supongamos que el homomorfismo θ le asigna a b el generador de B el automorfismo α_1.En este sentido tenemos que $\theta_b(a) = bab^{-1} = a^2$.

Pero $\theta_b{}^2\ (a) = b^2 ab^{-2} = b(bab^{-1})b^{-1} = b(\theta_b(a)b^{-1} = b(a^2)b^{-1} = \theta_b(a^2) = a^4 = \alpha_2(a)$

Que correspondería al homomorfismo que asignaría a *b* el automorfismo α_2.

De aquí que sólo existe un grupo no abeliano de orden 21, que expresado en términos de generadores y relaciones es: $G \approx \langle a,b \rangle$, $a^7=b^3=e$, $bab^{-1}=a^2$.

Con esto los grupos que de este tipo contempla el trabajo son los de orden:21, 39, 55, 57 y 93.

Caso 6.- ***Grupos de orden p^2q con $p \mid q-1$.***

Los grupos que son de este tipo que caen dentro del rango que nos hemos propuesto caracterizar, son de la forma 2^2q o bien 3^2q, los consideraremos por separado.

En el caso de los grupos de orden 2^2q, el grupo de orden 12 es un caso especial ya que es en la única situación en donde el q-subgrupo de Sylow puede no ser único por lo cual será analizado aparte de los demás.

Teorema 5.6.1.- Si G es un grupo de orden 2^2q y 2^2 no divide a $q-1$, entonces G es isomorfo a alguno de los siguientes grupos:

$Z_2 \times Z_{2q}, Z_{4q}, Z_q \times_\theta Z_4, D_{4q}, D_{2q} \times_\psi Z_2, D_{2q} \times Z_2.$

Demostración.- Sea G un grupo de orden 2^2q y 2^2 no divide a $q-1$. En este tipo de grupos tenemos que por el ***Teorema 2.2.6 (Tercer Teorema de Sylow)*** el número n_q de q-subgrupos de Sylow es 1, por tanto este q-subgrupo es normal en G. El numero n_2 de subgrupos de Sylow, puede ser 1 o q. En caso de que n_2 sea 1, entonces el 2-subgrupo de Sylow de G también es normal en G, de aquí que G es el producto directo de sus subgrupos de Sylow.

Para este caso el 2-subgrupo de Sylow es de orden 4, de donde por ***Teorema Fundamental de Grupos Abelianos Finitos***, tenemos que este 2-subgrupo es Z_4 o $Z_2 \times Z_2$. Por tanto tenemos como era de esperarse que G puede ser $Z_2 \times Z_2 \times Z_q$ o bien $Z_4 \times Z_q$,

que son los posibles grupos abelianos no isomorfos que de este orden pueden existir. Cabe hacer la observación de que $Z_2 \times Z_2 \times Z_q$ es isomorfo a $Z_2 \times Z_{2q}$ y $Z_4 \times Z_q$ es isomorfo a Z_{4q}.

Supongamos que el *2*-subgrupo de Sylow, no es único. Sea A el *q*-subgrupo de Sylow de G, que por ser de orden *q*, es cíclico, al cual lo identificaremos como $A = \langle a \rangle$ donde $a^q = e$. Sea B alguno de los *2*-subgrupos de G. Como ya lo habíamos mencionado anteriormente B es Z_4 o bien $Z_2 \times Z_2$.

En cualesquiera de los dos casos podemos reconstruir a G, como veremos mediante un producto semi-directo de A por B por el ***Teorema 4.6***. ya que en ambos casos estos subgrupos cumplen con las condiciones de la ***Definición 4.1***.

Sea B isomorfo a Z_4, es decir $B = \langle b \rangle$ con $b^4 = e$. Determinemos ahora los homomorfismos de B en *Aut*(A). Como *b* es de orden 4, y *Aut*(A) es isomorfo a Z_{q-1}, y como en este tipo de grupos estamos considerando que *4* no divide a *q-1*, entonces sólo requerimos determinar los automorfismos de A que sean de orden 2, que si existen en *Aut*(A), ya que 2 divide a todo primo mayor que 2 como lo es *q*. Pero estos automorfismos ya los determinamos en el ***Caso 4 (2p)***, y este es único y es de la forma $\alpha(a) = a^{-1}$. Por tanto el homomorfismo no trivial $\theta : B \rightarrow Aut(A)$, es $\theta_b(a) = bab^{-1} = a^{-1}$. Por tanto el grupo producido por este producto semi directo es $Z_q \times_\theta Z_4$, , el que podemos presentar en términos de generadores y relaciones como $\langle a,b \rangle$, $a^q = b^4 = e$, $bab^{-1} = a^{-1}$.

Consideremos ahora el caso en el que B es isomorfo a $Z_2 \times Z_2$. En tal caso y para facilitar la clasificación de este tipo de grupos consideraremos a B presentado en términos de generadores y relaciones, es decir: $B = \langle x, y \rangle$, $x^2 = y^2 = e$, $xy = yx$. Denotemos por $X = \langle x \rangle$ y $Y = \langle y \rangle$. De la normalidad de A se sigue que AX es un subgrupo de G. También tenemos que $A \cap X = \{ e \}$, ya que A no tiene elementos de orden 2, por tanto el orden de AX es $2q = |G| / 2$, lo cual implica que AX es normal en G. También tenemos que los subgrupos AX y Y solo tienen al elemento identidad en común ya que si no fuera así entonces $a^k x = y$, para algún $1 \leq k \leq p-1$, lo cual implica que $a^k = yx^{-1} \in A \cap B = \{ e \}$, lo cual es una contradicción ($x \neq y$), de donde de nuevo tenemos que (AX)Yes un subgrupo de G, pero como su orden es $4q$, entonces es todo G. Ahora bien los subgrupos AX y Y cumplen con las condiciones establecidas en la ***Definición 4.1***, do donde G es el producto semi-directo de estos dos subgrupos.

En tal caso por el ***Teorema 4.6***, necesitamos determinar los homomorfismos de Y en $Aut(AX)$. Pero como AX es de orden $2q$, entonces por el análisis hecho en el Caso 2, entonces AX es isomorfo a Z_{2q} o bien a D_{2q}.

Consideremos en primera instancia el caso en que AX es isomorfo a Z_{2q}. Un homomorfismo no trivial α: $Y \rightarrow Aut(AX)$, es como en el Caso 2, $t \in AX$, con el cual producimos el grupo $Z_{2q} \times_{\alpha} Z_{2^s} \cong D_{4q}$.

Ahora bien cuando AX es D_{2q}, también el homomorfismo no trivial es el que asigna al generador y de Y, el automorfismo de $\psi(d) = ydy^{-1} = d^{-1}$ de D_{2q}. Con el cual el grupo producido es $D_{2q} \times_{\psi} Z_2$. En este mismo ámbito el homomorfismo trivial también produce un grupo no considerado, que es el producto directo $D_{2q} \times Z_2$. ■

Los grupos que se incluyen en este caso son los de orden: 28, 44, 76 y 92.

Teorema 5.6.2.- Si G es un grupo de orden 2^2q y 2^2 divide a $q-1$, entonces G es isomorfo a alguno de los siguientes grupos:

$Z_2 \times Z_{2q}$, Z_{4q}, $Z_q \times_{\theta} Z_4$, D_{4q}, $D_{2q} \times_{\psi} Z_2$, $D_{2q} \times Z_2$, $Z_q \times_{\lambda} Z_4$.

Demostración.- Como en el caso analizado anteriormente tenemos que el q-subgrupo de Sylow es único, mientras que el número n_2 de 2-subgrupos de Sylow puede ser 1 o q. De donde la única diferencia con respecto al caso anterior es aquella en la que el 2-subgrupo de Sylow es isomorfo a Z_4, y en este caso si podemos asegurar la existencia de automorfismos de A el q-subgrupo de Sylow que sean de orden 4, ya que en este tipo de grupos 4 si divide a $q-1$, el cual es el orden del grupo $Aut(A) \approx Z_{q-1}$. De donde por la ***Teorema 1.1.14*** $Aut(A)$ tiene un único subgrupo cíclico de orden 4 y por tanto dos elementos de orden 4. así que solo agregaremos esta situación a la antes considerada. Sean τ y π tales automorfismos de A de orden 4, es decir: $\tau(a) = a^m$ con $1 < m \leq q-1$ y $m^4 \equiv 1$(mód q) y $\pi(a) = a^n$ con $1 < n \leq q-1$ y $n^4 \equiv 1$(mód q). De esto se sigue que $\tau^3 = \pi$. Consideremos ahora γ y λ los correspondientes homomorfismos de $B \rightarrow Aut(A)$ que definen estos automorfismos, $\gamma_b(a) = bab^{-1} = \tau(a) = a^m$ y $\lambda_b(a) = bab^{-1} = \pi(a) = a^n$.

Sea $\beta \in Aut(B)$ definido por $\beta(b) = b^3$ donde B es el 2-grupo de Sylow de G, presentado como: $B = \langle b \rangle$ con $b^4 = e$. De donde:

$$\gamma_{\beta(b)}(a) = \gamma_{b^3}(a) = b^3 ab^{-3} = a^{m^3} = \tau^3(a) = \pi(a) = \lambda_b(a)$$

De donde por el ***Teorema 4.7***, todos estos homomorfismos describen el mismo grupo G como el producto semi-directo de A por B. Es decir:

$$G \approx A \times_\lambda B \approx Z_q \times_\lambda Z_4. \blacksquare$$

Los grupos que de este tipo son contemplados en el trabajo son los de orden: 20, 52 y 68.

Teorema 5.6.3.- Si G es un grupo de orden 12, entonces G es isomorfo a alguno de los siguientes grupos:

$$Z_2 \times Z_6,\ Z_{12},\ Z_3 \times_\theta Z_4,\ D_6 \times_\theta Z_2,\ (Z_2 \times Z_2) \times_\theta Z_3$$

Demostración.- En este caso especial tenemos que el número n_2 de *2*-subgrupos de Sylow puede ser 1 o 3, y el número n_3 de los *3*-subgrupos de Sylow, es 1 o 4. Supongamos que $n_2 = 3$ y $n_3 = 4$, en esta situación tendríamos que los 3 *2*-subgrupos aportarían aparte del elemento identidad, cada uno tres elementos diferentes, es decir 9 en total para estos *2*-subgrupos; por otro lado la cantidad de elementos en los 4 *3*-subgrupos serían otros 8 elementos diferentes a los anteriores, en esta situación G tendría 17 elementos diferentes lo cual es una contradicción.

La anterior argumentación nos lleva a concluir que:

i) $n_2 = 1$ y $n_3 = 1$,

ii) si $n_2 = 3$ entonces $n_3 = 1$ o bien

iii) si $n_3 = 4$ entonces $n_2 = 1$.

Consideremos el tipo i) ambos grupos de Sylow son únicos por lo tanto son normales por tanto G es el producto directo de sus subgrupos de Sylow, lo cual nos lleva al caso abeliano, es decir el caso en que G puede ser:

$Z_2 \times Z_2 \times Z_3 \approx Z_2 \times Z_6$ o bien $Z_3 \times Z_4 \approx Z_{12}$.

Para ii) tenemos que el *3*-subgrupo es único, por tanto normal en G. Denotemos por A a este *3*-subgrupo de Sylow. Ahora bien, sea B alguno de los *2*-subgrupos, en tal caso A y B cumplen con las condiciones para reconstruir a G como un producto semi-directo de A por B.

Como el orden de B es 4, B es Z_4 o bien $Z_2 \times Z_2$; consideremos en primer lugar el caso en que B es Z_4, por lo que hay que determinar los homomorfismos no triviales de B en *Aut*(A). Primero su existencia, como *Aut* (A) es isomorfo a Z_2, solo existe un automorfismo distinto del automorfismo identidad, que es el definido por $\alpha(a) = a^2$, donde a es el generador de A. así que sólo tenemos un homomorfismo no trivial de B $\rightarrow$ *Aut*(A) que es el definido por $\theta_b(a) = bab^{-1} = a^2$. El cual nos produce el grupo $Z_3 \times_\theta Z_4$ que en términos de generadores y relaciones es $\langle a,b \rangle$ con $a^3 = b^4 = e$ y $bab^{-1} = a^2 = a^{-1}$.

Cuando B es $Z_2 \times Z_2$, tenemos una situación muy similar a la contemplada en ***Teorema 6.1.1*** por tanto para no ser repetitivo, afirmaremos por el análisis ya hecho en ese

caso que los grupos no abelianos que se producen en este caso son los productos semi-directos de Z_6 por $Z_2 = D_{12}$ y el de D_6 por Z_2.

Analicemos ahora iii), el cual es el caso en que el *2*-subgrupo es único. Denotemos por A a éste *2*-subgrupo de Sylow de G. Como A es de orden 4, entonces por el ***Teorema 5.2.1*** A es Z_4 o bien $Z_2 \times Z_2$. Sea B alguno de los *3*-subgrupos de G, $B = \langle x \rangle$ con $x^3 = e$.

Para la primera de estas opciones el caso en que $A = Z_4$ tenemos que solo existe el homomorfismo trivial, ya que *Aut*(A) es isomorfo a Z_2 por tanto no tiene elementos de orden 3, los cuales se requieren para reconstruir a G como un producto semi-directo de A por B, así que de este caso solo obtenemos el grupo abeliano $Z_4 \times Z_3$, que ya ha sido contemplado.

Así que solo nos resta considerar el caso cuando $A \approx Z_2 \times Z_2$, y para exhibir explícitamente los automorfismos de A que sean de orden 3, denotaremos a A como sigue:

$$A = \{e, a, b, ab\}, \text{ donde } a^2 = b^2 = e,\ ab = ba.$$

Pero *Aut*(A) es isomorfo a S_3 el cual tiene un único subgrupo de orden 3, el cual contiene a los dos automorfismos no triviales de orden 3.

Entonces los automorfismos de A que son de orden 3 son permutaciones de los 3 elementos distintos del idéntico del grupo que son ciclos de longitud 3, es decir:
$\alpha_1 = (a, b, ab)$ o bien $\alpha_2 = (a, ab, b)$, de donde $(a, b, ab)^2 = (a, ab, b)$. De donde tenemos dos homomorfismos no triviales θ y $\psi : B \to Aut(A)$, definidos por:

$$\theta_x(y) = xyx^{-1} = \alpha_1(y) \text{ y } \psi_x(y) = xyx^{-1} = \alpha_2(y)$$

Consideremos ahora el automorfismo de B definido por: $\beta(x) = x^2$. De esto tenemos que:

$$\theta_{\beta(x)}(y) = \theta_x^2(y) = x(xyx^{-1})x^{-1} = x[\alpha_1(y)]x^{-1} = \alpha_1^2(y) = \alpha_2(y) = \psi_x(y).$$

De donde estos dos homomorfismos producen el mismo producto semi-directo. Entonces G es $(Z_2 \times Z_2) \times_\theta Z_3$, el cual es un grupo con no abeliano con 8 elementos distintos del elemento identidad de orden 3 y tres elementos distintos del elemento identidad los cuales son de orden 2, por tanto este grupo nos describe el grupo A_4. ■

Los grupos de orden 3^2q con en los que 3 divide a $q-1$ que quedan dentro del rango son los de orden 63, nos concretaremos a clasificar a este tipo de grupos.

Teorema 5.6.4.- Si G es un grupo de orden 63, entonces G es isomorfo a alguno de los siguientes grupos:

$$Z_3 \times Z_{21}, Z_7 \times Z_9, Z_7 \rtimes Z_9, Z_7 \rtimes (Z_3 \times Z_3), Z_{21} \rtimes Z_3.$$

Demostración.- Como el único grupo que del tipo 3^2q y 3 divide a $q-1$, que queda dentro del rango propuesto es el de orden 63, nos concretaremos a dar la clasificación de este tipo de grupos. Si G es un grupo de orden 63, entonces $n_3 = 1$ o 7, y $n_7 = 1$. De donde el 7-subgrupo de Sylow es único, por tanto normal en G. Sea $A = \langle a \rangle$, con $a^7 = e$, el 7-subgrupo de Sylow de G, y B alguno de los 3-subgrupos de G.

En el caso de que $n_3 = 1$, B también es normal en G, de donde G es el producto directo de A por B, y por el análisis hecho en el ***Caso 2***, tenemos que B es $Z_3 \times Z_3$ o bien Z_9, de donde $G \approx Z_3 \times Z_3 \times Z_7 \approx Z_3 \times Z_{21}$ o bien $G \approx Z_9 \times Z_7 \approx Z_{63}$.

Supongamos que $n_3 \neq 1$, en tal caso G es el producto semi-directo de A por B, ya que estos subgrupos cumplen con las condiciones de la ***Definición 4.1***.

Consideremos primero el caso en el que B es el cíclico de orden 9, es decir: $B=\langle b \rangle$, con $b^9 = e$. Como *Aut*(A) es isomorfo a Z_6, y este no tiene elementos de orden 9, entonces solo determinaremos los automorfismos no triviales de *Aut*(A) que sean de orden 3. Sean ρ y π, estos dos automorfismos de A, de orden 3, es decir: $\rho(a) = a^2$ y $\pi(a) = a^4$ los cuales habíamos determinado en el ***Ejemplo 5.4.2***. y en forma análoga tenemos que $\rho^2 = \pi$. Por tanto con el automorfismo β de *Aut*(B), $\beta(b) = b^2$ y el ***Teorema 4.7***, los grupos realizados por estos homomorfismos son isomorfos. Por tanto el grupo que es realizado por ρ es el grupo $Z_7 \times_\rho Z_9$.

Consideremos ahora cuando B es isomorfo a $Z_3 \times Z_3$ que para facilitar su manejo lo presentaremos en términos de generadores y relaciones, es decir:

$$B = \langle x, y \rangle, \text{ donde } x^3 = y^3 = e, \text{ con la relación } xy = yx.$$

Como todo elemento de B que no es el elemento identidad es de orden 3, entonces el orden de su imagen homomorfica ha de ser 1 o 3. De donde los automorfismos de A que

requerimos son los de orden 3, que ya hemos identificado anteriormente en el ***Ejemplo 5.1***, sean: $\alpha_1(a) = a^2$ y $\alpha_2(a) = a^4$, los automorfismos de A de orden 3 y $\alpha_0(a) = a$ el automorfismo identidad de $Aut(\mathrm{A})$.

Por otro lado un homomorfismo de B queda completamente definido si conocemos la imagen de los generadores de B, entonces tenemos las siguientes opciones para definir estos homomorfismos no triviales de $\mathrm{B} \to Aut(\mathrm{A})$:

θ_1 $x \to \alpha_1$ $y \to \alpha_1$	θ_2 $x \to \alpha_2$ $y \to \alpha_2$	θ_3 $x \to \alpha_1$ $y \to \alpha_2$	θ_4 $x \to \alpha_2$ $y \to \alpha_1$
θ_5 $x \to \alpha_1$ $y \to \alpha_0$	θ_6 $x \to \alpha_0$ $y \to \alpha_1$	θ_7 $x \to \alpha_2$ $y \to \alpha_0$	θ_1 $x \to \alpha_0$ $y \to \alpha_2$

1) Con θ_1, producimos el grupo que presentado en términos de generadores y relaciones es:

$$G_1 = \langle a, x, y \rangle \text{ con } a^7 = x^3 = y^3 = e,\ xax^{-1} = a^2,\ yay^{-1} = a^2.$$

2) Con θ_2, producimos el grupo que presentado en términos de generadores y relaciones es:

$$G_2 = \langle a, x, y \rangle \text{ con } a^7 = x^3 = y^3 = e,\ xax^{-1} = a^4,\ yay^{-1} = a^4.$$

3) Con θ_3, producimos el grupo que presentado en términos de generadores y relaciones es:

$$G_3 = \langle a, x, y \rangle \text{ con } a^7 = x^3 = y^3 = e,\ xax^{-1} = a^2,\ yay^{-1} = a^4.$$

4) Con θ_4, producimos el grupo que presentado en términos de generadores y relaciones es:

$$G_4 = \langle a, x, y \rangle \text{ con } a^7 = x^3 = y^3 = e,\ xax^{-1} = a^4,\ yay^{-1} = a^2.$$

5) Con θ_5, producimos el grupo que presentado en términos de generadores y relaciones es:

$$G_5 = \langle a, x, y \rangle \text{ con } a^7 = x^3 = y^3 = e,\ xax^{-1} = a^2,\ yay^{-1} = a.$$

6) Con θ_6, producimos el grupo que presentado en términos de generadores y relaciones es:

$$G_6 = \langle a, x, y \rangle \text{ con } a^7 = x^3 = y^3 = e,\ xax^{-1} = a,\ yay^{-1} = a^2.$$

7) Con θ_7, producimos el grupo que presentado en términos de generadores y relaciones es:

$$G_7 = \langle a, x, y \rangle \text{ con } a^7 = x^3 = y^3 = e,\ xax^{-1} = a^4,\ yay^{-1} = a.$$

8) Con θ_8, producimos el grupo que presentado en términos de generadores y relaciones es:

$$G_8 = \langle a, x, y \rangle \text{ con } a^7 = x^3 = y^3 = e,\ xax^{-1} = a,\ yay^{-1} = a^4.$$

a) $G_1 \approx G_2$ por el Teorema 4.7 con $\beta_1 \in Aut(B)$ definido por $\beta_1(x, y) = (x^2, y^2)$.

b) $G_3 \approx G_4$ por el Teorema 4.7 con $\beta_2 \in Aut(B)$ definido por $\beta_2(x, y) = (y, x)$.

c) $G_5 \approx G_6$ por el Teorema 4.7 con $\beta_2 \in Aut(B)$ definido por $\beta_2(x, y) = (y, x)$.

d) $G_7 \approx G_8$ por el Teorema 4.7 con $\beta_2 \in Aut(B)$ definido por $\beta_2(x, y) = (y, x)$.

e) $G_1 \approx G_3$ por el Teorema 4.7 con $\beta_3 \in Aut(B)$ definido por $\beta_3(x, y) = (x, y^2)$.

f) $G_5 \approx G_7$ por el Teorema 4.7 con $\beta_4 \in Aut(B)$ definido por $\beta_4(x, y) = (x^2, y)$.

Por lo que solo tenemos dos grupos no isomorfos con estos productos semi-directos: el G_1 y el G_5, el primero de ellos corresponde al producto semi-directo $Z_7 \rtimes (Z_3 \times Z_3)$ y el G_5 en el cual la segunda relación implica que el generador y conmuta con el generador a, por lo que por la ***Definición 1.4.1***, G tiene un subgrupo que es el producto directo de A y $\langle y \rangle$, de donde este subgrupo es isomorfo a Z_{21}, de donde G_5 es el producto semi-directo de $Z_{21} \rtimes Z_3$.■

Caso 7.- ***Grupos de orden p^2q con $p \nmid q-1$.***

Los grupos que de esta clase nos hemos propuesto clasificar son los de orden:45 y 99, son de la forma 3^2q, sólo consideraremos grupos de este orden en este caso.

Teorema 5.7.1.- Si G es un grupo de orden 3^2q con $3 \nmid q-1$, entonces G es isomorfo a alguno de los siguientes grupos: $Z_3 \times Z_{3q}$ ó Z_{9q}.

Demostración.- Cuando un grupo G es de orden 3^2q y 3 no divide a $q-1$, entonces tenemos que como q es un primo mayor que 3, entonces el número n_q de q-subgrupos de Sylow es 1 y del hecho de que 3 no divide a $q-1$ el número n_3 de 3-subgrupos de Sylow también es 1, de donde en éste tipo de grupos los correspondientes subgrupos de Sylow son únicos, por tanto normales por el ***Lema 2.2.5*** lo cual implica que G es el producto directo de sus subgrupos de Sylow.

Como el 3-subgrupo es de orden 9, entonces es Z_9 o bien $Z_3 \times Z_3$ y el q-subgrupo es Z_q, de donde G es $Z_3 \times Z_3 \times Z_q \approx Z_3 \times Z_{3q}$ o el grupo Z_{9q} .■

Los grupos considerados de este tipo, son los de orden: 45 y 99.

Caso 8.- ***Grupos de orden pq^2 con $p \mid q-1$.***

En esta clase de grupos tenemos que el q-subgrupo de Sylow es único ya que por ser de índice 2 es normal en G y por el ***Lema 2.2.5*** tenemos la unicidad, pero también por el

Tercer Teorema de Sylow tenemos que el número n_q de q-subgrupos de Sylow es 1, ya que 1 es el único divisor del orden de G que es congruente con 1 mod q, y el número n_2 de 2-subgrupos de Sylow, puede ser 1, q ó q^2. Estos grupos son el producto semi-directo de el q-subgrupo de Sylow por alguno de los 2-subgrupos de Sylow, pero su caracterización queda fuera del alcance del presente trabajo, pero es un excelente motivo de continuar el estudio y caracterización de éstos grupos.

Caso 9.- ***Grupos de orden pqr con*** $q \nmid r-1$.

Los grupos que de este tipo quedan dentro del rango a clasificar son los de orden 30, 66 y 70, todos ellos son de la forma $2qr$, por lo que sólo determinaremos la clasificación de este tipo de grupos. Como en los grupos de orden 30 no tenemos directamente un subgrupo normal, su clasificación se hará en forma separada de los de orden 66 y 70.

Teorema 5.9.1.- Si G es un grupo de orden 30, entonces es isomorfo a alguno de los siguientes grupos: Z_{30}, D_{30}, $G_1 = \langle a,b \rangle$ con $a^{15} = b^2 = e$, con la relación $bab^{-1} = a^4$, $G_2 = \langle a,b \rangle$ con $a^{15} = b^2 = e$, con la relación $bab^{-1} = a^{11}$.

Demostración.- Sea G es un grupo de orden 30. Por el ***Tercer Teorema de Sylow***, tenemos que los números de los respectivos p-subgrupos de Sylow son: $n_2 = 1, 3, 5$ o 15; $n_3 = 1$ o 10; $n_5 = 1$ o 6. Pero n_3 y n_5 no pueden ser simultáneamente diferentes de 1, ya que si así fuera, tendríamos en los 10 3-subgrupos 20 elementos distintos y en los 6 5-subgrupos, 24

elementos distintos así G tendría al menos 44 elementos distintos del elemento identidad, lo cual es una contradicción. De donde ; $n_3 = 1$ o $n_5 = 1$, por tanto en cualesquiera de las dos opciones tenemos que n_p es 1 si $p=3$ *o* 5. Por tanto tenemos que el p-subgrupo de Sylow es normal en G. Si denotamos por H a este p-subgrupo y por K a alguno de los otros subgrupos de Sylow de que no sean de orden 2 o p, tenemos que HK es un subgrupo de G, de orden 15, lo cual implica que es de índice 2, por tanto normal en G. Denotemos por A este subgrupo normal de G de orden 15, que por el análisis hecho en el ***Caso 3***, este subgrupo es isomorfo a Z_{15}. Sea B uno de los 2-subgrupos de G, por tanto isomorfo a Z_2. De esto se sigue que $A \cap B = \{ e \}$, por tanto $|AB| = |A|\,|B| = (15)(2) = |G|$ lo cual implica que G = AB, de aquí que G es el producto semi-directo de A por B.

Ahora bien hay que determinar los homomorfismos no triviales de $B \rightarrow Aut(A)$, que sean de orden 2, ya que B es isomorfo a Z_2. Por tanto los automorfismos de A que no son el automorfismo identidad son de la forma $\alpha(a) = a^k$ con $1 < k \leq 14$, $(k, 15) = 1$, y son de orden 2, si además cumplen la condición de que k^2 sea congruente con 1 módulo 15, de donde $k = 4$, 11 o 14.

a) $k = 4$.- Para $k = 4$, el homomorfismo de $B \rightarrow Aut(A)$, queda definido como: $\theta_b(a) = bab^{-1} = a^4$, el cual nos determina un grupo que en términos de generadores y relaciones es tal que: $G_1 = \langle a, b \rangle$ con $a^{15} = b^2 = e$, con la relación $bab^{-1} = a^4$

b) $k = 11$.- Para $k = 11$, el homomorfismo de B $\rightarrow Aut$(A), queda definido como: $\theta_b(a)=bab^{-1}=a^{11}$, el cual nos determina un grupo que en términos de generadores y relaciones es tal que: $G_2 = \langle a,b \rangle$ con $a^{15} = b^2 = e$, con la relación $bab^{-1} = a^{11}$.

c) $k = 14$.- Para $k = 14$, el homomorfismo de B$\rightarrow Aut$(A), queda definido como: $\theta_b(a)=bab^{-1}=a^{14} = a^{-1}$, el cual nos determina un grupo que en términos de generadores y relaciones es tal que: $G = \langle a,b \rangle$ con $a^{15} = b^2 = e$, con la relación $bab^{-1} = a^{-1}$, el cual es el D_{30}.■

Teorema 5.9.2.- Si G es un grupo de orden 66, entonces es isomorfo a alguno de los siguientes grupos: Z_{66}, D_{66}, $G_1 = \langle a,b \rangle$ con $a^{33} = b^2 = e$, con la relación $bab^{-1} = a^{10}$, $G_2 = \langle a,b \rangle$ con $a^{33} = b^2 = e$, con la relación $bab^{-1} = a^{23}$.

Demostración.- Sea G un grupo de orden 66, entonces por el ***Tercer Teorema de Sylow***, tenemos que los respectivos números de p-subgrupos de Sylow son: $n_2 = 1, 3, 11$ o 33; $n_3 = 1$ o 22; $n_{11} = 1$. Por tanto el ***Lema 2.2.5***, el 11-subgrupo de Sylow es normal en G. En el caso de que $n_2 = n_3 = 1$, entonces G es el producto directo de sus subgrupos de Sylow, por tanto $G \approx Z_{66}$.

Sean H el *11*-subgrupo de Sylow de G, K alguno de los *3*-subgrupo de Sylow de G y B alguno de los *2*-subgrupos de G. De la normalidad de H, se sigue que HK es un subgrupo de G, de orden 33, por lo que es de índice 2, lo cual implica que es normal en G. Como HK es de orden 33, entonces por el ***Teorema 5.3.1***, HK es cíclico. Para facilitar el manejo de estos subgrupos identificaremos a HK = A = $\langle a \rangle$ con $a^{33} = e$ y B = $\langle b \rangle$ con $a^2 = e$. Entonces A∩B = { e }, por tanto tenemos que |AB| = |A| |B| = (33)(2) = |G|, lo cual implica que G = AB, de aquí que G es el producto semi-directo de A por B.

Determinaremos los homomorfismos no triviales de B→*Aut*(A), y con esto determinar los grupos que estos realizan. Como el generador de B es de orden 2, solo nos interesarán los automorfismos de A que sean de orden 2, es decir aquellos de la forma:

$\alpha(a) = a^k$ con $1 < k \leq 32$, $(k, 33) = 1$, $k^2 \equiv 1 \pmod{33}$, de donde $k = 10, 23$ o 32.

a) Para $k = 10$, θ: B →*Aut*(A), queda definido como: $\theta_b(a) = bab^{-1} = a^{10}$, el cual nos determina un grupo que en términos de generadores y relaciones es tal que: $G_1 = \langle a, b \rangle$ con $a^{33} = b^2 = e$, con la relación $bab^{-1} = a^{10}$.

b) Para $k = 23$, θ: B →*Aut*(A), queda definido como: $\theta_b(a) = bab^{-1} = a^{23}$, el cual nos determina un grupo que en términos de generadores y relaciones es tal que: $G_2 = \langle a, b \rangle$ con $a^{33} = b^2 = e$, con la relación $bab^{-1} = a^{23}$.

c) Para $k = 23$, θ: B →*Aut*(A), queda definido como: $\theta_b(a) = bab^{-1} = a^{23}$, el cual nos determina un grupo que en términos de generadores y relaciones es tal que:

$G_3 = \langle a,b \rangle$ con $a^{33} = b^2 = e$, con la relación $bab^{-1} = a^{32} = a^{-1}$. Lo cual implica que $G_3 = D_{66}$. ■

Teorema 5.9.3.- Si G es un grupo de orden 70, entonces es isomorfo a alguno de los siguientes grupos: Z_{70}, D_{70}, $G_1 = \langle a,b \rangle$ con $a^{70} = b^2 = e$, con la relación $bab^{-1} = a^6$, $G_2 = \langle a,b \rangle$ con $a^{70} = b^2 = e$, con la relación $bab^{-1} = a^{29}$.

Demostración.- Sea G un grupo de orden 70, entonces por el ***Tercer Teorema de Sylow***, tenemos que los respectivos números de *p*-subgrupos de Sylow son: $n_2 = 1, 5, 7$ o 35; $n_5 = 1$; $n_7 = 1$. Por tanto el ***Lema 2.2.5***, el 7-subgrupo de Sylow y el 5-subgrupo de Sylow son normales en G. En el caso de que $n_2 = n_5 = 1$, entonces G es el producto directo de sus subgrupos de Sylow, por tanto $G \approx Z_{70}$.

Sean H el *7*-subgrupo de Sylow de G, K alguno de los *3*-subgrupos de Sylow de G y B alguno de los *2*-subgrupos de G. De la normalidad de H, se sigue que HK es un subgrupo de G, de orden 35, por lo que es de índice 2, lo cual implica que es normal en G. Como HK es de orden 35, entonces por el ***Teorema 5.3.1***, HK es cíclico. Para facilitar el manejo de estos subgrupos identificaremos a $HK = A = \langle a \rangle$ con $a^{35} = e$ y $B = \langle b \rangle$ con $a^2 = e$. Entonces $A \cap B = \{ e \}$, por tanto tenemos que $|AB| = |A|\,|B| = (35)(2) = |G|$, lo cual implica que $G = AB$, de aquí que G es el producto semi-directo de A por B.

Determinaremos los homomorfismos no triviales de $B \to Aut(A)$, y con esto determinar los grupos que estos realizan. Como el generador de B es de orden 2, solo nos interesarán los automorfismos de A que sean de orden 2, es decir aquellos de la forma:

$\alpha(a) = a^k$ con $1 < k \leq 34$, $(k, 35) = 1$, $k^2 \equiv 1 \pmod{35}$, de donde $k = 6$, 29 o 34.

d) Para $k = 6$, $\theta: B \to Aut(A)$, queda definido como: $\theta_b(a) = bab^{-1} = a^6$, el cual nos determina un grupo que en términos de generadores y relaciones es tal que: $G_1 = \langle a, b \rangle$ con $a^{35} = b^2 = e$, con la relación $bab^{-1} = a^6$.

e) Para $k = 29$, $\theta: B \to Aut(A)$, queda definido como: $\theta_b(a) = bab^{-1} = a^{29}$, el cual nos determina un grupo que en términos de generadores y relaciones es tal que: $G_2 = \langle a, b \rangle$ con $a^{35} = b^2 = e$, con la relación $bab^{-1} = a^{29}$.

f) Para $k = 34$, $\theta: B \to Aut(A)$, queda definido como: $\theta_b(a) = bab^{-1} = a^{34}$, el cual nos determina un grupo que en términos de generadores y relaciones es tal que: $G_3 = \langle a, b \rangle$ con $a^{35} = b^2 = e$, con la relación $bab^{-1} = a^{34} = a^{-1}$. Lo cual implica que $G_3 = D_{70}$. ■

Caso 10.- ***Grupos de orden pqr con q | r-1.***

Los grupos que de este tipo quedan dentro del rango a clasificar son los de orden 42 y 78.

Teorema 5.10.1.- Si G es un grupo de orden 42, entonces es isomorfo a alguno de los siguientes grupos: Z_{42}, D_{42}, $(Z_7 \rtimes Z_3) \times Z_2$, $(Z_7 \rtimes Z_3) \rtimes Z_2$,

$G_1 = \langle c,k \rangle$ con $c^{21} = k^2 = e$ y $kck^{-1} = c^8$; $G_2 = \langle c,k \rangle$ con $c^{21} = k^2 = e$ y $kck^{-1} = c^{13}$.

Demostración.- Sea G es un grupo de orden 42. Por el ***Tercer Teorema de Sylow***, tenemos que los números de los respectivos *p*-subgrupos de Sylow son: $n_2 = 1, 3, 7$ o 21; $n_3 = 1$ o 7; $n_7 = 1$. De donde el 7-subgrupo de Sylow, es único, por tanto, normal en G. Sea A este 7-subgrupo de Sylow.

Así que tenemos que analizar las opciones siguientes:

1) $n_3 = 1$ y $n_2 = 1$,
2) $n_3 = 1$ y $n_2 \neq 1$,
3) $n_3 \neq 1$ y $n_2 = 1$.
4) $n_3 \neq 1$ y $n_2 \neq 1$.

Para 1) tenemos que tanto el 2-subgrupo como el 3-subgrupo de Sylow, son únicos, de donde por el **Lema 2.2.5**, éstos subgrupos son también normales en G, de aquí que G sea el producto directo de sus *p*-subgrupos de Sylow, por tanto es $Z_7 \times Z_3 \times Z_2 \approx Z_{42}$.

Para 2) tenemos que el 3-subgrupo es único, por tanto normal en G. Sea H este 3-subgrupo de Sylow y K uno de los 2-subgrupos de G y A el 7-subgrupo de Sylow que por ser único es normal en G. De la normalidad de H y A se sigue que AH es un subgrupo de G de orden 21. Denotemos por C = AH, por ser de orden 21 es de índice 2 por tanto normal en G. Pero en tal caso tenemos que C es el producto directo de H y A, de donde C

es isomorfo a Z_{21}, de donde G es el producto semi-directo de C y K. Por lo que hay que determinar los homomorfismos no triviales de orden 2, $\theta : K \rightarrow Aut(C)$, para facilitar el manejo de éstos sea $C = \langle c \rangle$ con $c^{21} = e$. De donde tenemos que:

$\alpha_1(c) = c^8$; $\alpha_2(c) = c^{13}$ y $\alpha_3(c) = c^{20}$; son los automorfismos de C de orden 2.

Con éstos automorfismos determinamos los grupos que presentados con generadores y relaciones son:

$G_1 = \langle c,k \rangle$ con $c^{21} = k^2 = e$ y $kck^{-1} = c^8$.

$G_2 = \langle c,k \rangle$ con $c^{21} = k^2 = e$ y $kck^{-1} = c^{13}$.

$G_3 = \langle c,k \rangle$ con $c^{21} = k^2 = e$ y $kck^{-1} = c^{20} = c^{-1}$.

De esto se sigue que G_3 es D_{42}.

Para 3) tenemos que el 3-subgrupo de Sylow no es único pero el 2-subgrupo de Sylow si lo es, por lo tanto normal en G. Sea K este 2-subgrupo de Sylow y H uno de los 3-subgrupos Sylow de G. Por lo tanto tenemos que AH es un subgrupo no abeliano de G de orden 21, por tanto normal en G. Esto implica que G es el producto directo de AH y K, por ser normales y $AH \cap K = \{ e \}$. Y $|(AH)K| = |AH||K| = (21)(2) = 42$, por lo que $(AH)K = G$. Pero el gruopo no abeliano de orden 21 ya ha sido determinado en el ***Ejemplo 5.4.2***, el cual es el grupo $\langle a,h \rangle$ con $a^7 = h^3 = e$, $hah^{-1} = a^2$. De donde G es $(Z_7 \rtimes Z_3) \times Z_2$.

Para 4) Tenemos los 3-subgrupos y 2-subgrupos no son únicos. Sea H uno de los 3-subgrupos de G y K uno de los 2-subgrupos de G. De esto tenemos que AH es un

subgrupo de G debido a la normalidad de A. AH es no abeliano de orden 21, por lo que es de índice 2, lo cual implica que es normal en G. Además $AH \cap K = \{ e \}$ y $|(AH)K| = |AH||K| = (21)(2) = 42$, por lo que $(AH)K = G$. De donde G es el producto semi-directo de AH por K. Es decir G es $(Z_7 \rtimes Z_3) \rtimes Z_2$. Omitimos la determinación completa de este producto semi-directo ya que el grupo de automorfismos de AH es un grupo no abeliano de orden 42, que queda fuera del alcance de la teoría desarrollada en este escrito. ■

Teorema 5.10.2.- Si G es un grupo de orden 78, entonces es isomorfo a alguno de los siguientes grupos: Z_{78}, D_{78}, $Z_{13} \rtimes Z_6$, $(Z_{13} \rtimes Z_3) \times Z_2$, $(Z_{13} \rtimes Z_3) \times Z_2$,

$G_1 = \langle c,k \rangle$ con $c^{39} = k^2 = e$ y $kck^{-1} = c^{14}$; $G_2 = \langle c,k \rangle$ con $c^{39} = k^2 = e$ y $kck^{-1} = c^{25}$.

Demostración.- Sea G es un grupo de orden 78. Por el ***Tercer Teorema de Sylow***, tenemos que los números de los respectivos *p*-subgrupos de Sylow son: $n_2 = 1, 3, 13$ o 39; $n_3 = 1$ o 13; $n_{13} = 1$. De donde el 13-subgrupo de Sylow, es único, por tanto, normal en G. Sea A este 13-subgrupo de Sylow.

Así que tenemos que analizar las opciones siguientes:

1) $n_3 = 1$ y $n_2 = 1$,

2) $n_3 = 1$ y $n_2 \neq 1$,

3) $n_3 \neq 1$ y $n_2 = 1$.

4) $n_3 \neq 1$ y $n_2 \neq 1$.

Para 1) tenemos que tanto el 2-subgrupo como el 3-subgrupo de Sylow, son únicos, de donde por el **Lema 2.2.5**, éstos subgrupos son también normales en G, de aquí que G sea el producto directo de sus p-subgrupos de Sylow, por tanto es $Z_{13} \times Z_3 \times Z_2 \approx Z_{78}$.

Para 2) tenemos que el 3-subgrupo es único, por tanto normal en G. Sea H este 3-subgrupo de Sylow y K uno de los 2-subgrupos de G y A el 13-subgrupo de Sylow que por ser único es normal en G. De la normalidad de H y A se sigue que AH es un subgrupo de G de orden 39. Denotemos por C = AH, por ser de orden 39 es de índice 2 por tanto normal en G. Pero en tal caso tenemos que C es el producto directo de H y A, de donde C es isomorfo a Z_{39}, de donde G es el producto semi-directo de C y K. Por lo que hay que determinar los homomorfismos no triviales de orden 2, $\theta : K \rightarrow Aut$ (C), para facilitar el manejo de éstos sea C = $\langle c \rangle$ con $c^{21} = e$. De donde tenemos que:

$\alpha_1(c) = c^{14}$; $\alpha_2(c) = c^{25}$ y $\alpha_3(c) = c^{38}$; son los automorfismos de C de orden 2.

Con éstos automorfismos determinamos los grupos que presentados con generadores y relaciones son:

$G_1 = \langle c,k \rangle$ con $c^{39} = k^2 = e$ y $kck^{-1} = c^{14}$.

$G_2 = \langle c,k \rangle$ con $c^{39} = k^2 = e$ y $kck^{-1} = c^{25}$.

$G_3 = \langle c,k \rangle$ con $c^{39} = k^2 = e$ y $kck^{-1} = c^{38} = c^{-1}$.

De esto se sigue que G_3 es D_{78}.

Para 3) tenemos que el 3-subgrupo de Sylow no es único pero el 2-subgrupo de Sylow si lo es, por lo tanto normal en G. Sea K este 2-subgrupo de Sylow y H uno de los

3-subgrupos Sylow de G. Por lo tanto tenemos que AH es un subgrupo no abeliano de G de orden 39, por tanto normal en G. Esto implica que G es el producto directo de AH y K, por ser normales y $AH \cap K = \{ e \}$. Y $|(AH)K| = |AH||K| = (39)(2) = 78$, por lo que $(AH)K = G$. Pero el gruopo no abeliano de orden 39 es el grupo $\langle a,h \rangle$ con $a^{13} = h^3 = e$, $hah^{-1} = a^3$. De donde G es $(Z_7 \rtimes Z_3) \times Z_2$.

Para 4) Tenemos los 3-subgrupos y 2-subgrupos no son únicos. Sea H uno de los 3-subgrupos de G y K uno de los 2-subgrupos de G. De esto tenemos que AH es un subgrupo de G debido a la normalidad de A. AH es no abeliano de orden 39, por lo que es de índice 2, lo cual implica que es normal en G. Además $AH \cap K = \{ e \}$ y $|(AH)K| = |AH||K| = (39)(2) = 78$, por lo que $(AH)K = G$. De donde G es el producto semi-directo de AH por K. Es decir G es $(Z_{13} \rtimes Z_3) \rtimes Z_2$. Omitimos la determinación completa de este producto semi-directo ya que el grupo de automorfismos de AH es un grupo no abeliano de orden 78, que queda fuera del alcance de la teoría desarrollada en este escrito.■

Caso 11.- ***Grupos de orden p^3.***

Como los grupos que dentro del rango a clasificar de este tipo de grupos son los de orden 8 y 27, sólo consideraremos tales grupos.

Teorema 5.11.1.- Si G es un grupo de orden 8, entonces es isomorfo a uno y sólo uno de los siguientes grupos:

1) Si G es abeliano

$$Z_8;\ Z_4 \times Z_2; Z_2 \times Z_2 \times Z_2.$$

2) Si G es no abeliano

$$H_2(cuaternios);\ D_8.$$

Demostración.- 1) Si G es abeliano de orden 8, por el ***Teorema Fundamental de Grupos Abelianos Finitos***, tenemos que G es isomorfo a: Z_8 ó $Z_4 \times Z_2$ ó $Z_2 \times Z_2 \times Z_2$.

2) Supongamos que G de orden 8 es no abeliano, en tal caso G no tiene elemento de orden 8, ya que esto implicaría que G es cíclico y por consiguiente abeliano. Tampoco puede tener todos sus elementos de orden 2, ya que tabién en este caso G sería abeliano. Por el ***Teorema de Lagrange*** debe existir $a \in G$, tal que su orden sea 4; consideremos $A = \langle a \rangle$. Como el índice de A es 2, entonces A es normal en G. Como A es de orden 4, entonces $A \neq G$. Sea $b \in G$, tal que $b \notin A$; por tanto $A \neq Ab$, de donde $G = A \cup Ab$, además también tenemos que $A \cap Ab = \phi$. Como $b^2 \in G$ y $b^2 \notin Ab$, ya que esto implicaría que $b \in A$, entonces $b^2 \in A$. Si $b^2 = a$ o bien $b^2 = a^3$, entonces b sería de orden 8, lo cual es una contradicción para el supuesto de G. De donde $b^2 = a^2$, o bien $b^2 = e$, por otro lado de la normalidad de A se tiene que el orden de bab^{-1} tiene que ser el mismo de a, de donde $bab^{-1} = a$, o bien $bab^{-1} = a^3$. Si $bab^{-1} = a$, entonces G sería abeliano, lo cual contradice

nuestra hipótesis de que G es no abeliano. De donde sólo tenemos dos grupos no abelianos de orden 8 determinados por:

$\langle a,b / a^4 = e, a^2 = b^2, bab^{-1} = a^3 \rangle$ y $\langle a,b / a^4 = b^2 = e, bab^{-1} = a^3 \rangle$

los cuales definen a H_2 y D_8, respectivamente. Ver [VII]■

Teorema 5.11.2.- Si G es un grupo de orden 27, entonces es isomorfo a uno y sólo uno de los siguientes grupos:

2) Si G es abeliano

$$Z_{27};\ Z_9 \times Z_3; Z_3 \times Z_3 \times Z_3.$$

2) Si G es no abeliano

$G_1 = \langle a,b / a^9 = b^3 = e, bab^{-1} = a^4 \rangle$

$G_2 = \langle a,b,c / a^3 = b^3 = c^3 = e, ab = bac, ac = ca, bc = cb \rangle$

Demostración.- 1) Si G es abeliano de orden 27, por el ***Teorema Fundamental de GruposAbelianos Finitos***, tenemos que G es isomorfo a: Z_{27} ó $Z_9 \times Z_3$ ó $Z_3 \times Z_3 \times Z_3$.

Para 2) puede verse [VII] págs. 43 y 44, en el cual tenemos una demostración completa de este resultado pero con herramientas diferentes a las expuestas en este trabajo.■

BIBLIOGRAFIA

[I] *Abstract Algebra 2nd Edition*
I.N. Herstein
Macmillan Publishing Company 1990

[II] *Abstract Algebra: A first Course*
L.J. Goldstein
Prentice Hall 1973

[III] *A First Course in Abstract Algebra 3rd Edition*
John B. Fraleigh
Addison-Wesley Publishing Company, Inc. 1982

[IV] *An Introduction to the Theory of Groups 3rd Edition*
J.J. Rotman
Wm. C. Brown Publishers 1988

[V] *Clasificación de Grupos Abelianos*
Martín Eduardo Frías Armenta
Universidad de Sonora 1994

[VI] *Contemporany Abstract Algebra*
Joseph A. Gallian
D.C. Heath Company 1986

[VII] *Estructuras Algebraicas III*
Horacio Hernán O'brein
OEA 1973