UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA-LEÓN

FACULTAD DE CIENCIAS Y TECNOLOGÍA

DEPARTAMENTO DE MATEMÁTICA Y ESTADÍSTICA

APLICACIONES DE LOS TEOREMAS DE SYLOW

MONOGRAFÍA

PARA OPTAR AL TÍTULO DE LICENCIADO EN MATEMÁTICA

PRESENTADA POR

BR. ROMMEL ANTONIO GUIDO CARCACHE

BR. MAYCOL RICARDO SÁNCHEZ MENDOZA

BR. ULISES FRANCISCO SALAZAR GÓMEZ

TUTORA

MSC. ANGELA ALTAMIRANO SLINGER

LEÓN, ABRIL 2012

DEDICATORIA

Dedico este trabajo primeramente a **Dios** por permitirme la vida que es lo más valioso que he necesitado para poder ejercer mis estudios y concluir con mucho éxito mi carrera. A mi madre **Rosario Pérez** por haberme traído a este mundo y apoyarme en lo que más pudo, a mi abuelo **Anastasio Guido** por ser el que me orientó a superarme y sobre todo por su apoyo económico y mi tía **Mayra Guido** por su destacada colaboración económica para completar mi carrera.

Rommel Antonio Guido Carcache

Dedico este trabajo a **Dios**, creador de la vida y fuente de Sabiduría del cual proceden todas las cosas, y por haberme permitido el tiempo necesario para la elaboración de este informe. Quiero dedicar este trabajo de forma especial a mis abuelos **Ricardo Sánchez y Rosa Pérez**, por haberme apoyado siempre en lo bueno y en lo adverso y por esa confianza incondicional depositada en mi la cual me inspiro hasta el día de hoy a ser forjador de un futuro mejor.

Maycol Ricardo Sánchez Mendoza

Dedico de forma especial a **Dios** por haberme brindado buena vida para poder terminar mis estudios universitarios; a mis padres **Ulises Salazar y Haydee Gómez** por apoyarme de forma económica y guiarme por el buen camino para alcanzar lo que hoy he logrado, a la memoria de mis abuelos **Francisco Mairena y Susana del Carmen Soto**, que depositaron en mí la confianza para poder coronar un futuro mejor.

Ulises Francisco Salazar Gómez

AGRADECIMIENTO

Ofrecemos este trabajo **a Dios**, creador de la vida y fuente de Sabiduría del cual proceden todas las cosas, por iluminar nuestros caminos para dar buenos pasos en tierra firme y por habernos permitido el tiempo necesario para la elaboración de nuestro trabajo.

Agradecemos de forma especial al grupo de estudio que conformamos durante los cinco años que con voluntad y dedicación pudimos culminar con éxito nuestros estudios.

A nuestros Maestros, que con ahínco y esmero estimularon nuestra lucha, brindándonos su esmerada paciencia para instruirnos conocimientos que hoy, nos ayudan a la calidad de nuestro triunfo; ya que triunfadores no son aquellos que nunca han caído sino aquellos que caen y se levantan para seguir avanzando.

Agradecemos incondicionalmente a Msc. Ángela Altamirano Slinger, por habernos transmitidos sus conocimientos durante el transcurso de nuestra carrera y por habernos inspirado desde el principio hasta el final con esta tesis; trabajo que finalizamos con éxito.

Agradeciendo también a todo el claustro de maestros que estuvieron pendiente día a día de nuestro aprendizaje.

ÍNDICE

INTRODUCCIÓN

Para que la Teoría de Grupos se usara tal cual hoy la conocemos hubo de pasar mucho tiempo y dar sus aportes muchos matemáticos. Por ejemplo las ideas que contiene la definición de grupo, estaban presentes en algunos trabajos de matemáticos realizados durante la segunda mitad del siglo XVIII y todo el siglo XIX. Todas ellas se referían a casos particulares de grupos, principalmente grupos de permutaciones.

También en el contexto de las permutaciones, el matemático noruego, Mejdell Ludwig Sylow (1832-1918) publicó en 1873 uno de los trabajos que supuso el mayor avance en esta teoría desde los resultados de Cauchy.

Sylow logró demostrar, escrito en lenguaje moderno, que no sólo todo grupo de orden n tiene un subgrupo de orden p si p es primo y divide a n, sino que los tiene de todos los órdenes p^s siempre que p^s divida a n y para el mayor s para el que esto suceda solamente hay uno de ellos. Estos resultados se conocen con el nombre de Teoremas de Sylow. Desde entonces, casi todos los demás resultados y trabajos sobre grupos finitos usan estos teoremas.

Dada la importancia que tienen los Teoremas de Sylow en la teoría de grupos finitos, consideramos de mucho interés el desarrollar una monografía que presente la descripción de estos teoremas, sus demostraciones detalladas y la ilustración de algunas de sus aplicaciones.

Este trabajo monográfico puede ser utilizado por estudiantes o profesores interesados en ampliar sus conocimientos en el campo del Álgebra Abstracta como un material de consulta sobre estos aspectos relevantes de la teoría de grupos finitos.

El presente trabajo consta de tres capítulos. En el primer capítulo se introducen los elementos básicos de la teoría de grupos para estudiar los Teoremas de Sylow, que se muestran en el capítulo dos. En el segundo capítulo se analizan los tres Teoremas de Sylow con sus demostraciones respectivas.

En el capítulo tercero se presentan aplicaciones, con cuatro casos donde se utilizan los Teoremas de Sylow. En los anexos se incluyen una mini biografía de Mejdell Ludwig Sylow, algunas tablas referidas a ejemplos y la descomposición de los números primos. Además añadimos las notaciones usadas y la bibliografía consultada en el presente trabajo.

OBJETIVOS

OBJETIVO GENERAL

- Mostrar la importancia de los Teoremas de Sylow mediante el estudio de algunas de sus aplicaciones.

OBJETIVOS ESPECIFICOS

- Describir los elementos básicos de la Teoría de Grupos que permitan la comprensión de lo establecido en los Teoremas de Sylow.

- Explicar de manera detallada la demostración de los tres Teoremas de Sylow.

- Ilustrar algunas aplicaciones de los Teoremas de Sylow mediante el estudio de casos.

CAPÍTULO I

ELEMENTOS BÁSICOS DE LA TEORÍA DE GRUPOS

1.1 INTRODUCCIÓN

La teoría de grupos tiene su origen en el trabajo de **Evariste Galois** sobre solubilidad por radicales de la ecuación $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x^1 + a_0 = 0$. Dado que el trabajo de Galois citado versa sobre las raíces de polinomios, el concepto de grupo usado por Galois se restringe a lo que hoy llamamos el grupo de permutaciones de n elementos.

Actualmente la teoría de grupos es una de las áreas de las matemáticas que más aplicaciones tiene. Estas van desde las ciencias exactas hasta la música. En las ciencias exactas, las aplicaciones incluyen áreas tales como geometría algebraica, teoría de números y topología algebraica; en física y química su aplicación tiene lugar en el estudio de simetrías de las estructuras moleculares.

En este primer capítulo presentamos los conceptos fundamentales y teoremas básicos de la Teoría de Grupos, la presentación de los temas está acompañada con ejemplos, que tienen la finalidad de auxiliar en la comprensión de los contenidos para lograr un entendimiento de los aspectos básicos de la teoría de grupos.

También se incluyen las definiciones y algunos teoremas de los G-Conjuntos, Órbitas y los P-grupos; que serán de mucha utilidad en el desarrollo del presente trabajo. No se incluyen las demostraciones de los teoremas presentados.

1.2 GRUPOS Y SUBGRUPOS

Comenzaremos presentando el concepto de grupo, para ello necesitamos definir previamente el concepto de operación binaria.

Definición 1.1

Una **operación binaria** $*$ en un conjunto A, es una regla que asigna a cada par ordenado de elementos de A, algún elemento del conjunto A.

El elemento asignado al par (a, b) de elementos de A por $*$ se denota por $a * b$.

Definición 1.2

Una **operación binaria** $*$ en un conjunto A es conmutativa si y sólo si $a* b=b* a$ para todo a, b $\in$ A. La operación binaria $*$ es asociativa si y sólo si $(a*b)*c=a*(b*c)$ para toda a, b, c $\in$ A.

Por ejemplo, en el conjunto de los enteros Z, tanto la suma como la multiplicación usuales son operaciones binarias conmutativas y asociativas. También lo son en el conjunto de los números racionales Q y en el conjunto de los números reales R.

Definición 1.3

Un**grupo** $<G, *>$ es un conjunto G, junto con una operación binaria $*$ en G tal que se satisface los siguientes axiomas:

1. Dados a, b, c$\in$G, se tiene que $a* (b* c)=(a* b)*c$.
   (Esto se describe diciendo que es válida la ley asociativa en G.)
2. Existe un elemento especial e$\in$G tal que $a* e=e* a=a \ \forall \ a\in G$.
   (e se llama elemento identidad de G.)
3. Para todo a$\in$G existe un elemento $a^{-1}\in G$ talque $a* a^{-1}=a^{-1}*a=e$.
   (Este elemento a^{-1} se llama inverso de a en G.)

Cuando el conjunto G tiene un número finito de elementos, entonces el grupo $<G, * >$ es un grupo finito.

Son ejemplos de grupos: <Z,+>, <Q, + >, < R, +>, $<Q^+, \cdot>$, <Q-{0}, ·>, $<R^+, \cdot>$ y <R-{0}, ·>. Si G= {1,-1} entonces < G, ·> es un grupo finito.

Por facilidad en la notación, se denota al grupo $<G,* >$ sólo por la letra G. Se acostumbra denotar el inverso de un elemento **a** en un grupo, con $\mathbf{a}^{-1}$ en notación multiplicativa y con **–a** en notación aditiva.

Definición 1.4

Si G es un grupo finito, entonces el **orden** de G, denotado por |G|, es el número de elementos en G.

Es importante mencionar como especiales aquellos grupos G en los cuales $a*b=b*a$ para todo a, b$\in$G.

Definición 1.5

Un grupo G es **abeliano** o **conmutativo** si su operación binaria $*$ es conmutativa.

Ejemplo:

Los grupos$<Z,+>$, $<Q, + >$, $< R, +>$, $<Q^+, \cdot>$, $<Q-\{0\}, \cdot>$, $<R^+, \cdot>$ y $<R- \{0\}, \cdot>$ son grupos abelianos.

Definición 1.6

Si H es un subconjunto no vacío de un grupo G cerrado bajo la operación de grupo de G y si H es él mismo un grupo bajo esta operación inducida, entonces H es un **subgrupo** de G.

Denotaremos por $H \leq G$ ó $G \geq H$ el hecho de que H es un subgrupo de G, y $H < G$ ó $G > H$ significa que $H \leq G$, pero $H \neq G$.

Ejemplo:

1. $<Z,+>$ es un subgrupo de $< R, +>$

2. $<Q^+,\cdot>$ es un subgrupo de $<R^+, \cdot>$

3. $<Q^+,\cdot>$no es un subgrupo de $<R, +>$

El teorema que a continuación se enuncia es uno de los más comunes que se utilizan como criterio para establecer si un subconjunto de un grupo es un subgrupo del grupo.

Teorema 1.7

Sea G un grupo y H un subconjunto no vacío de G, H es un subgrupo de G si y sólo si:

1. $a, b \in H \rightarrow ab \in H$.
2. La identidad e de G está en H.
3. $a \in H \rightarrow a^{-1} \in H$.

Cada grupo G tiene como subgrupo a G mismo y {e}, donde e es el elemento identidad de G.

Definición 1.8

Si G es un grupo, entonces G es el **subgrupo impropio** de G. Todos los otros subgrupos son subgrupos propios. Además {e} es el subgrupo trivial de G. Todos los otros subgrupos son no triviales.

Ejemplo:

Sea V el 4-grupo de Klein cuya tabla de grupo se describe a continuación. Los subgrupos propios no triviales de V son {e, a}, {e, b} y {e, c}.

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Ejemplo:

El conjunto Z_4= {0,1, 2, 3} bajo la suma módulo 4, es un grupo cuya tabla es la siguiente:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Aquí el único subgrupo propio no trivial de Z_4 es {0,2}. Nótese que {0,3} no es un subgrupo de Z_4, pues {0,3} no es cerrado bajo +. Por ejemplo, 3+3=2 y $2 \notin \{0,3\}$.

A continuación se enuncian los conceptos fundamentales sobre los grupos de permutaciones, los cuales dieron origen a los famosos teoremas de Sylow y que además serán las bases para el desarrollo del presente trabajo.

1.3 GRUPO DE PERMUTACIONES

Estos grupos nos proporcionan los primeros ejemplos de grupo, que no son abelianos y nos familiarizan con la idea de permutación de conjunto, como arreglo de elementos de este mismo conjunto.

Definición 1.9

Una **permutación** de un conjunto A es una función de A en A que es tanto uno a uno como sobre. En otras palabras, una permutación de A es una función uno a uno de A sobre A.

También escribimos: $\varphi: A \overset{1-1}{\underset{\text{sobre}}{\rightarrow}} B$.

En las permutaciones de un conjunto puede definirse una operación binaria, la multiplicación de permutaciones, que no es más que la composición de funciones.

Ejemplo:

Sea A= {1, 2, 3, 4, 5} y las permutaciones de A, $\sigma=\begin{pmatrix}1&2&3&4&5\\4&2&5&3&1\end{pmatrix}$ y $\tau=\begin{pmatrix}1&2&3&4&5\\3&5&4&2&1\end{pmatrix}$

Entonces $\sigma\,\tau=\begin{pmatrix}1&2&3&4&5\\4&2&5&3&1\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\3&5&4&2&1\end{pmatrix}=\begin{pmatrix}1&2&3&4&5\\2&5&1&4&3\end{pmatrix}$

El siguiente teorema muestra que la colección de todas las permutaciones de un conjunto A no vacío forma un grupo bajo esta multiplicación de permutaciones.

Teorema 1.10 (Grupo de Permutaciones)

Sea A un conjunto no vacío y sea S_n la familia de todas las permutaciones de A, entonces S_n es un grupo bajo la multiplicación de permutaciones.

Existe otra notación para permutaciones, la notación cíclica.

Definición 1.11

Una permutación σ de un conjunto A es un **ciclo** de longitud n si existen $a_1, a_2,..., a_n \in A$, tales que $\sigma(a_1)=a_2$, $\sigma(a_2)=a_3$, …, $\sigma(a_{n-1})=a_n$, $\sigma(a_n)=a_1$ y $\sigma(x)=x$ para toda $x \in A$ tal que $x \notin \{a_1, a_2,..., a_n\}$. Escribimos $\sigma= (a_1, a_2,..., a_n)$.

Ejemplo:

Si A= {1, 2, 3, 4, 5}, entonces $(1, 3, 5, 4)=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 3 & 2 & 5 & 1 & 4\end{pmatrix}$

Observe que

(1, 3, 5, 4)=(3,5,4,1)=(5,4,1,3)=(4,1,3,5)

Puesto que los ciclos son tipos particulares de permutaciones, pueden multiplicarse como cualesquiera dos permutaciones. Sin embargo, el producto de dos ciclos no necesariamente es un ciclo.

Definición 1.12

Un **ciclo** de longitud 2 es una transposición. De este modo, una transposición deja fijos todos los elementos excepto dos y lleva a cada uno de estos en el otro.

Cualquier ciclo es producto de transposiciones. Esto es,

$$(a_1, a_2,...,a_n)= (a_1, a_2)(a_1, a_3)\ldots(a_1,a_n).$$

Ejemplo:

Dada la permutación $\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 6 & 5 & 2 & 4 & 3 & 1\end{pmatrix}$, entonces como producto de dos ciclos ajenos tenemos que $\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 6 & 5 & 2 & 4 & 3 & 1\end{pmatrix}$= (1,6) (2, 5, 3).

En una colección de ciclos, los ciclos son ajenos cuando ningún elemento de A aparece en las notaciones de dos ciclos diferentes de la colección. Hay que convenir que cualquier ciclo de longitud uno representa la permutación identidad. Cualquier permutación es el producto de un número impar de transposiciones o bien el producto de un número par de transposiciones.

Definición 1.13

Una permutación de un conjunto finito es **par o impar** de acuerdo con que pueda expresarse como el producto de un número par de transposiciones o como el producto de un número impar de transposiciones, respectivamente.

Ejemplo:

Dado el conjunto A= {1, 2, 3} y el grupo S_3= $\{\rho_0, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3\}$ de las permutaciones de A. Se tiene que

ρ_0= $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$= (1,2) (1,2)

ρ_1=$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$= (1,2 ,3)= (1,2) (1,3)

ρ_2=$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$= (1,3 ,2)= (1,3) (1,2)

μ_1=$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$= (2,3)

μ_2=$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$= (1,3)

μ_3=$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$= (1,2)

Luego ρ_0, ρ_1, ρ_2 son permutaciones pares y μ_1, μ_2, μ_3 son permutaciones impares.

Teorema 1.14

Si n≥2, la colección de todas las permutaciones pares de {1,2,3,…, n} forman un subgrupo de orden n!/2 del grupo simétrico S_n.

Definición 1.15

El subgrupo de S_n que consta de las permutaciones pares de n letras es el **grupo alternante** A_n de n letras.

Por tanto el grupo alternante A_3= $\{\rho_0, \rho_1, \rho_2\}$ es el grupo de las permutaciones pares de S_3.

Nos referiremos al producto directo de grupos, a los resultados que presentaremos en capítulos posteriores que serán de gran utilidad al momento de estudiar dichos grupos.

1.4 PRODUCTOS DIRECTOS DE GRUPOS

Se pueden obtener nuevos grupos a partir del producto cartesiano de grupos dados.

Definición1.16

El producto cartesiano de los conjuntos $S_1, S_2,\ldots,S_n$ es el conjunto de todas las n-adas ordenadas $(a_1, a_2,\ldots, a_n)$, donde $a_i \in S_i$. El producto cartesiano se denota por $S_1 x S_2 x \ldots x S_n$ ó por $\prod_{i=1}^{n} S_i$.

Teorema 1.17

Sean los grupos $G_1, G_2, \ldots, G_n$ para $(a_1, a_2,\ldots, a_n)$ y $(b_1, b_2,\ldots,b_n)$ en $\prod_{i=1}^{n} G_i$ defínase la operación binaria $(a_1, a_2, \ldots,a_n)(b_1, b_2, \ldots,b_n)$ como $(a_1b_1, a_2b_2, \ldots,a_nb_n)$. Entonces, $\prod_{i=1}^{n} G_i$ es un grupo, el producto directo externo de los grupos G_i, bajo esta operación binaria.

Ejemplo:

Sea el grupo $Z_2 = \{0, 1\}$ y $Z_3 = \{0, 1, 2\}$, entonces el producto directo externo $Z_2 x Z_3 = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}$ consta de 6 elementos.

.

En caso de que la operación en cada grupo G_i sea conmutativa, usaremos, algunas veces la notación aditiva y nos referiremos a $\prod_{i=1}^{n} G_i$ como la suma directa externa de los grupos G_i.

En el estudio de grupos, un problema de gran importancia es la “descomposición” de un grupo como “producto” de subgrupos. Este resulta ser un problema de gran dificultad, sin embargo, bajo buenas hipótesis (abeliano y finito) la respuesta es satisfactoria.

En el estudio y clasificación de los grupos, los más sencillos a considerar son los generados por un elemento, es decir los grupos cíclicos.

1.5 GRUPOS CICLICOS

El entender las propiedades y estructura de éstos es de gran importancia, pues se consideran como una especie de tipos elementales de grupos abelianos.

Definición 1.18

Un elemento **a** de un grupo G genera a G y es generador de G si <**a**>=G. Un grupo G es **cíclico** si existe algún elemento **a**∈G que genere a G.

Ejemplo:

Sea el grupo Z_4, este grupo es cíclico porque 1 y 3 son generadores. Esto es,

<1>= {1, 2, 3, 0}=Z_4 y <3>= {3, 2, 1, 0}=Z_4

En general el conjunto Z_n= {0,1, 2,…,n-1} bajo la suma módulo n es un grupo cíclico.

El teorema siguiente nos muestra que dado un elemento de un grupo G existe un subgrupo asociado a él y que es el menor subgrupo que lo contiene.

Teorema 1.19

Sea G un grupo y sea **a** un elemento de G, entonces H= {$\mathbf{a}^n \mid n \in Z$} es un subgrupo de G y es el menor subgrupo de G que contiene a **a**, esto es, cada subgrupo que contiene a **a** contiene a H.

Al grupo H del teorema 1.19 se le llama **subgrupo cíclico** de G generado por **a**, esto es, H=<**a**>.

Ejemplo:

Sea el grupo Z bajo la suma, entonces el subgrupo <**3**> considerando la notación aditiva debe contener:

3 3+3=6 3+3+3=9 y así sucesivamente.

0 -3 -3+(-3)=-6-3+(-3)+(-3)=-9 y así sucesivamente.

En otras palabras, el subgrupo cíclico generado por 3 consta de todos los múltiplos de 3, positivos, negativos y el cero. Denotamos este subgrupo por 3Z, así como por <**3**>.

Definición 1.20

Sea G un grupo y $\mathbf{a}\in G$; si existe algún $n\in Z^+$ tal que $\mathbf{a}^n=e$, el menor de dichos enteros positivos n es el **orden** de **a**. Si no existe dicho n, **a** es de orden infinito

Si **a** es un elemento de un grupo G, el orden de **a** es igual al orden del subgrupo cíclico generado por **a**.

Ejemplo:

Si consideramos el grupo $Z_3xZ_2xZ_4$ de 24 elementos, entonces el orden del elemento (1,0,0) de este grupo es 3 ya que el subgrupo cíclico generado por (1,0,0), H=<(1,0,0)>= {(1,0,0),(2,0,0),(0,0,0)} es de orden 3.

Dado G un grupo cíclico con generador **a**, $G=\{\mathbf{a}^n \mid n\in Z\}=<\mathbf{a}>$, se puede tener los siguientes dos casos:

Caso I: G tiene un número infinito de elementos, esto es, el orden de G es infinito. Afirmamos que dos exponentes h y k no pueden dar elementos iguales $\mathbf{a}^h$ y $\mathbf{a}^k$, es decir, todas las potencias de **a** son distintas.

Por ejemplo, $G=\{6^n \mid n\in Z\}$ bajo la multiplicación, esto es, $G=<6>=\{\ldots 6^0, 6^1, 6^2, 6^3,\ldots\}$ es un grupo cíclico infinito.

Caso II: G tiene orden finito en este caso no todas las potencias positivas de un generador **a** de G son distintos, así que para algún h y k tenemos $\mathbf{a}^h=\mathbf{a}^k$.

Por ejemplo, $<Z_5,+>$ es un grupo cíclico finito con generadores 1, 2, 3 y 4, esto es, $<\mathbf{1}>=<\mathbf{2}>=<\mathbf{3}>=<\mathbf{4}>=Z_5$.

Un resultado importante acerca de grupos finitos es el teorema de Lagrange, que a continuación se establece.

Teorema 1.21 (Lagrange)

Sea G un grupo de orden finito n y H un subgrupo de G. El orden de H divide al orden de G.

Corolario 1.22

Todo grupo de orden primo es cíclico.

Si hay una idea central común a todos los aspectos del algebra abstracta, tal es la noción de homomorfismo. Indicamos con ello una aplicación de un sistema algebraico a un sistema algebraico equivalente, que preserva la estructura.

1.6 HOMOMORFISMO E ISOMORFISMO

A continuación se presenta el concepto de homomorfismo e isomorfismo de grupos que en cierto sentido son de gran importancia al momento de construir la teoría de grupos.

Definición 1.23

Un **homomorfismo** φ de un grupo G en un grupo G', es una función $\varphi: G \rightarrow G'$, tal que $\varphi(ab) = \varphi(a)\varphi(b) \forall a, b \in G$.

En esta definición el producto ubicado al lado izquierdo de la igualdad en $\varphi(ab)$ es el de G, mientras que el producto $\varphi(a)\,\varphi(b)$ es el de G'.

Ejemplo:

Sea G el grupo de los enteros respecto a la adición y G'= {1,-1} el subgrupo de los reales respecto a la multiplicación. Defínase $\varphi(m)=1$ si m es par, y $\varphi(m)=-1$ si m es impar. La afirmación de que φ es un homomorfismo es simplemente un replanteamiento de: par + par=par, par + impar=impar, impar + impar= par.

El **kernel** de un homomorfismo $\varphi: G \longrightarrow G'$ es el conjunto $\text{Ker}\,\varphi = \{x \in G \mid \varphi(x) = e'\}$ donde e' es el elemento identidad de G'.

Teorema 1.24 (Segundo Teorema de Homomorfismo).

Sea ϕ un homomorfismo del grupo G sobre el grupo G', con Kerϕ=K y H' un subgrupo de G', entonces H =ϕ^{-1}(H'), es tal que:

1. $K \subset H$.
2. $H/K \approx H'$.

Definición 1.25

Un **isomorfismo** entre un grupo G y un grupo G' es una función φ uno a uno, que lleva a G sobre G' y tal que para todas las x e y en G, $\varphi(xy) = \varphi(x)\varphi(y)$. Los grupos G y G' son isomorfos.

La notación usual es $G \cong G'$. A menudo es deseable poder identificar un grupo dado como isomorfo a algún grupo concreto conocido. De esta manera, dos grupos que son isomorfos; aunque no sean necesariamente iguales, son estructuralmente idénticos.

Ejemplo:

Sea R bajo la suma y R^+ bajo la multiplicación, entonces R es isomorfo a R^+. Si definimos $\varphi: R \to R^+$, $\forall\, x \in X$ con $\varphi(x)=e^x$, se tiene que φ es 1-1, pues $\varphi(x)=\varphi(y)$ implica $e^x=e^y$ así que x=y, también φ es sobre, si $r \in R^+$, $\varphi(x)=e^x=r$ se tiene que $x=\ln r \in R$. Además $\varphi(x+y)=\varphi(x)\ \varphi(y)$, ya que $\varphi\ (x+y)=e^{x+y}=e^x \cdot e^y=\varphi(x)\varphi(y)$. Por tanto R bajo la suma es isomorfo a R^+ bajo la multiplicación.

1.7 SUBGRUPOS NORMALES Y GRUPO FACTOR

Definición 1.26

Sea H un subgrupo de un grupo G y sea $a \in G$. La **clase lateral izquierda** aH de H es el conjunto **{**$ah \mid h \in H$**}. La clase lateral derecha** Ha de H es el conjunto **{**$ha \mid h \in H$**}.**

La notación multiplicativa para la clase lateral izquierda es aH y la notación aditiva es a+H. De manera similar se tiene para la clase lateral derecha.

Ejemplo:

Considerando el grupo <Z, +> y el subgrupo 3Z. Las clases laterales izquierdas de 3Z en notación aditiva son:

0+3Z= {…, -9, -6, -3, 0, 3, 6, 9,…}

1+3Z= {…, -8, -5, -2, 1, 4, 7, 10,…} y

2+3Z= {…, -7, -4, -1, 2, 5, 8, 11,…}

Lema 1.27

Si H es un subgrupo de un grupo G y si la operación inducida de multiplicación de clases laterales en las clases laterales izquierdas (derechas) de H está bien definida, entonces la colección de clases laterales izquierdas (derechas) de H forma un grupo bajo la multiplicación de clases laterales inducida.

Definición 1.28

Sea H un subgrupo de un grupo G, el número de clases laterales izquierdas de H en G es el **índice** (G:H) de H en G.

También se puede definir el índice (G:H) como el número de clases laterales derechas de H en G.

Ejemplo:

El índice del subgrupo H= <6> de Z_{36} es 6, ya que H=<6>= {6, 12, 18, 24, 30, 0} y sus clases laterales son: 0+H, 1+H, 2+H, 3+H, 4+H y 5+H.

Los automorfismos de grupo pueden usarse como procedimiento para la construcción de nuevos grupos partiendo del grupo original.

Definición 1.29

Entenderemos por **automorfismo** de un grupo G a un homomorfismo de G en si mismo que es uno a uno y sobre.

Ejemplo:

Sea G el grupo aditivo de los enteros y definamos ϕ:G→G por $\phi(x)=-x$ $\forall x\in G$. Como $\phi(x+y)= -(x+y)= -x-y=\phi(x)+\phi(y)$, entonces ϕ es un homomorfismo. ϕ es uno a uno, ya que si $\phi(x)= \phi(y)$, entonces $-x=-y$, de donde $x=y$. ϕ es sobre, ya que $\phi(G)=\{ \phi(x) \mid x\in G \}=\{-x: x\in G \}=G$. Luego, ϕ es un automorfismo.

Teorema 1.30

Para cada $g\in G$, la transformación i_g:G →G dada por $i_g(x)=g^{-1}xg$ es un automorfismo de G, el **automorfismo interno** de G bajo la conjugación por g.

Definición 1.31

Dos subgrupos H y K de un grupo G son **conjugados** si $H=a^{-1}Ka$ para alguna $a\in G$, esto es, si uno se transforma en el otro mediante algún automorfismo interno de G.

Ejemplo:

Los subgrupos H= $\{\rho_0,\mu_1\}$ y K= $\{\rho_0,\mu_2\}$ del grupo S_3 son conjugados, puesto que para $\rho_1 \in S_3$ y $\rho_0,\mu_1 \in H$ se tiene que:

$(\rho_1)^{-1}\rho_0\rho_1=\rho_2\rho_0\rho_1=\rho_2\rho_1=\rho_0 \in K$

$(\rho_1)^{-1}\mu_1\rho_1=\rho_2\mu_1\rho_1=\mu_3\rho_1=\mu_2 \in K$

Así el automorfismo interno i_{ρ_1} transformó al subgrupo H= $\{\rho_0,\mu_1\}$ en el subgrupo K= $\{\rho_0,\mu_2\}$.

En el Anexo No.2, se presenta la tabla del grupo S_3 para verificar los cálculos anteriores.

Definición 1.32

Un subgrupo H de un grupo G es un **subgrupo normal** (o invariante) de G si $g^{-1}Hg=H$ para todas las $g\in G$, esto es, si H permanece invariante bajo todo automorfismo interno de G.

Teorema 1.33

Todo subgrupo de un grupo abeliano es un subgrupo normal.

Ejemplo:

El subgrupo 3Z del grupo Z bajo la suma es un subgrupo normal, ya que <Z,+> es un grupo abeliano.

Recientemente se terminó la determinación y clasificación completa de todos los grupos simples finitos. El nuevo conocimiento de todos los grupos simples finitos se puede usar para resolver algunos problemas de la teoría de grupos finitos.

Definición 1.34

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

Ejemplo:

El grupo Z_2 es un grupo simple. También el grupo alternante A_n para $n \geq 5$.

El concepto de grupo factor es muy sutil y de mucha importancia, dado que sucede mediante la formación de un nuevo conjunto a partir de uno anterior utilizando como elementos de dicho conjunto nuevo subconjuntos del anterior.

Definición 1.35

Si N es un subgrupo normal de un grupo G, el grupo de las clases laterales de N bajo la operación inducida es el **grupo factor** de G módulo N y se denota por G/N. Las clases laterales son las clases residuales de G módulo N.

Ejemplo:

Sea el grupo $G=Z_4 \times Z_6$ y $H=<(0,2)>=\{(0,0), (0,2), (0,4)\}$ un subgrupo normal de G. El grupo factor $(Z_4 \times Z_6)/H$ es de orden 8, ya que $Z_4 \times Z_6$ tiene orden 24 y el subgrupo generado por (0,2) es de orden 3. Para saber a qué grupo es isomorfo nuestro grupo factor observemos que el primer factor Z_4 no se altera y el factor Z_6 esencialmente

se colapsa por un subgrupo de orden 3, dando un grupo factor en el segundo factor de orden 2, que debe ser isomorfo a Z_2. Por tanto, $(Z_4 \times Z_6)/\langle(0,2)\rangle$ es isomorfo a $Z_4 \times Z_2$.

El siguiente teorema relaciona los grupos factor con los homomorfismos.

Teorema 1.36 (Homomorfismo canónico)

Si N es un subgrupo normal de un grupo G, entonces la transformación canónica (o natural) $\gamma: G \to G/N$ dada por $\gamma(a)=aN$ para $a \in G$, es un homomorfismo.

Definición 1.37

Un **subgrupo normal maximal** de un grupo G es un subgrupo normal M que no es igual a G y tal que ningún subgrupo normal propio N de G contiene propiamente a M.

Teorema 1.38

M es un subgrupo normal maximal de G si y sólo si G/M es simple.

Ejemplo:

Como el grupo factor S_n/A_n es isomorfo a Z_2 que es un grupo simple, también lo es el grupo factor. De donde A_n es un subgrupo normal maximal de S_n.

1.8 G-CONJUNTOS

Una aplicación al conteo se puede tener con los G-conjuntos.

Definición 1.39

Sea X un conjunto y G un grupo. Una acción de G en X es una transformación $*$**:** X x G→X tal que:

1. xe=x para todas las x∈X.
2. x(g_1g_2)=(xg_1)g_2 para todas las x∈ X y todas las g_1 y g_2 ∈ G.

Bajo estas condiciones, X es un **G-conjunto**.

Ejemplo:

Todo grupo G en sí mismo es un G-conjunto, donde la acción de g_2 ∈G sobre g_1 ∈ G está dada por la multiplicación derecha. Esto es, $*(g_1, g_2)=g_1g_2$. Si H es un subgrupo de G, también podemos considerar G como un H-conjunto donde $*$(g,h)=gh.

Cuando X es un G-conjunto distinguiremos por el momento dos conjunto especiales, primero el subconjunto de X de todos los elementos x, tales que xg= x para alguna g∈G fija, y en segundo término el subconjunto de G que consiste en todos los elementos de G que dejan fijo a un x∈X en particular. En símbolos, sean: X_g= {x∈X│xg=x} y G_x= {g∈G│xg=x} tales subconjuntos.

Teorema 1.40

Sea X un G-conjunto. Entonces, G_x es un subgrupo de G para cada x∈X.

Definición 1.41

Sea X un G-conjunto y sea x∈X. El subgrupo G_x= {g∈G│xg=x} es el subgrupo de isotropía de x.

G_x es el subconjunto de G que consiste en todos los elementos de G que dejan fijo a un x∈X.

1.9 Órbitas

El siguiente resultado nos muestra que es posible particionar todo G-conjunto X en subconjuntos de este tipo.

Teorema 1.42

Sea X un G-conjunto. Para x_1, x_2∈X, sea la relación x_1~x_2 si y sólo si existe g∈G tal que x_1g= x_2. Entonces ~ es una relación de equivalencia en X.

En particular cada $x \in X$ pertenece a una y sólo una clase de equivalencia o celda a la que llamaremos la órbita de x.

Definición 1.43

Sea X un G-conjunto. Cada celda en la partición de la relación de la equivalencia, descrita en el teorema 1.42, es una **órbita** en X bajo G. Si $x \in X$, la celda que contiene a x es la órbita de x y la denotaremos por xG.

El siguiente teorema nos proporciona herramientas para determinar el número de órbitas en un G-conjunto de X bajo G.

Teorema 1.44

Sea G un grupo finito y X un G-conjunto finito, si r es un número de órbitas en X bajo G, entonces $r\,|G| = \sum_{g \in G} |X_g|$.

Corolario 1.45

Si G es un grupo finito y X es un G-conjunto finito, entonces el número de órbitas en X bajo G, es $r = \frac{1}{|G|} \sum_{g \in G} |X_g|$.

Ejemplo:

Sea X el conjunto de las 720 marcaciones distintas de las caras de un cubo, usando de uno hasta seis puntos. Sea G el grupo de las 24 rotaciones del cubo, ahora bien |G|=24. Para $g \in G$ donde $g \neq e$, tenemos $|X_g|=0$ porque cualquier rotación diferente a la identidad cambia cualquiera de las 720 marcas por otra distinta. Sin embargo, $|X_e|=720$ pues la identidad deja fijas las 720 marcaciones. Entonces, por el corolario 1.45 tenemos que:

(Número de órbitas)=1/24 (720)=30. Así que hay 30 dados distintos.

La relación entre las órbitas de X y la estructura de grupo de G es central en las aplicaciones que aparecerán en el capitulo siguiente. Esta relación se expone mediante el teorema siguiente.

Teorema 1.46

Sea X un G-conjunto y sea x∈X. Entonces |xG|=(G:G_x).

Ejemplo:

Sea G el grupo D_4=$\{\rho_0, \rho_1, \rho_2, \rho_3, \mu_1, \mu_2, \delta_1, \delta_2\}$, el grupo de simetrías del cuadrado o grupo octal. En anexo No.3, mostramos el cuadrado con vértice 1, 2, 3, 4. Además, denominamos a los lados por S_1, S_2, S_3, S_4 , a las diagonales por d_1, d_2, y a los ejes vertical y horizontal por m_1, m_2 , al centro por C y a los puntos medios de los lados s_i y P_i. Usemos ρ_i, el cual corresponde a rotar el cuadrado en sentido contrario al que giran las manecillas del reloj en $\pi i/2$ radianes, μ_i corresponde a voltear el cuadrado alrededor del eje m_i, y δ_i a voltear el cuadrado alrededor de la diagonal d_i.

Sea X= {1,2,3,4,$S_1, S_2, S_3, S_4, m_1, m_2, d_1, d_2$,C,$P_1, P_2, P_3, P_4$ }.

Entonces, X puede considerarse como un D_4–conjunto. En anexo No.4 se describe en su totalidad la acción de D_4 en X. Ahora bien, como X es el D_4–conjunto con G=D_4, entonces tenemos 1G= {1,2,3,4} y G_1= $\{\rho_0, \delta_2\}$. Como |G|= 8 tenemos que |1G|= (G:G_1)=4.

1.10 P-GRUPOS

El principal objetivo de esta sección es mostrar que un grupo finito G tiene un subgrupo de todo orden la potencia de un primo, que a su vez divide a |G|. Además la mayoría de los resultados de esta sección proceden de una ecuación que cuenta el número de elemento de un G-conjunto.

Definición 1.47

Un grupo G es un **p-grupo** si todo elemento en G tiene orden alguna potencia del primo p. Un subgrupo de un grupo G es un p-subgrupo de G si el subgrupo es él mismo un p-grupo.

Una herramienta que será de mucha utilidad en el estudio y comprensión de los resultados de Sylow, es el teorema de Cauchy que enunciamos a continuación.

Teorema 1.48 (Cauchy)

Sea G un grupo finito y p un primo que divide a $|G|$. Entonces G tiene algún elemento de orden p y, por tanto, un subgrupo de orden p.

Corolario 1.49

Sea G un grupo finito. Entonces, G es un p-grupo si y sólo si $|G|$ es una potencia de p.

De manera análoga al corolario anterior si $|G|=p^n$, entonces para todo $g \in G$ como el orden de g divide a $|G|=p^n$, entonces el orden de g es una potencia de p. El cual se ilustra en el ejemplo siguiente.

Ejemplo:

El grupo Z_4 es un 2-grupo ya que $Z_4= \{0, 1, 2, 3\}$ es de orden $4=2^2$ aquí p=2. Los órdenes de los elementos 0, 1, 2 y 3 son 1, 4, 2 y 4 respectivamente, que son potencias de 2.

Definición 1.50

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

Ejemplo:

Los 2-subgrupos de Sylow de S_3 tienen orden 2. Los subgrupos de orden 2 de S_3 son: $\{\rho_0, \mu_1\}$, $\{\rho_0, \mu_2\}$, $\{\rho_0, \mu_3\}$.

.

El teorema que se enuncia a continuación constituye una herramienta muy poderosa, aunque no sea precisamente un teorema de conteo pero si concibe una conclusión numérica sobre todo cuando se escoge adecuadamente el conjunto y la acción de grupo.

Teorema 1.51

Sea G un grupo de orden p^n, p un primo y sea X un G-conjunto finito. Entonces,

$|X| \equiv |X_G|$ (mod p).

El resultado siguiente nos muestra que si tenemos un grupo G y Ω que es la colección de todos los subgrupos de G y si convertimos Ω en un G-conjunto, haciendo que G actué en Ω por conjugación. Esto es, si $H \in \Omega$ de modo que $H \leq G$, y $g \in G$, entonces la acción de g en H produce el subgrupo conjugado $g^{-1}Hg$.

Ahora bien, $H_G = \{g \in G \mid g^{-1}Hg = H\}$ es un subgrupo de G, de modo que H es un subgrupo normal de H_G. Como H_G consta de todos los elementos de G que dejan invariante a H bajo la conjugación, H_G es el mayor subgrupo de G que tiene a H como subgrupo normal,

Definición 1.52

El subgrupo H_G, es el **normalizador** de H en G y se denotará por N[H].

Ejemplo:

El normalizador de cualquier subgrupo es el grupo completo. En particular N[<e>] y N[G] son ambos iguales a G.

Lema 1.53

Sea H un p-subgrupo del grupo finito G, entonces $(N[H]:H) \equiv (G:H) \pmod p$.

Concluimos este capítulo afirmando que “La Teoría de Grupos” es una herramienta muy poderosa y que constituye la base para cualquier estudio referido a una estructura algebraica.

CAPITULO II

Los Teoremas de Sylow

2.1 INTRODUCCION

El objetivo central de este capítulo 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 de orden 6, y el primer teorema de Sylow establece que si la potencia de un primo pdivide 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 órdenes que dividan al orden del grupo.

Las demostraciones de los Teoremas de Sylowson 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.

Los Teoremas de Sylow nos proporcionan información muy importante en la clasificación de los grupos no abelianos, también acerca de los grupos finitos no conmutativos. Nos dicen, entre otras cosas, que si la potenciade un primo divide al orden de un grupo este posee un subgrupo con ese orden.

2.2 PRIMER TEOREMA DE SYLOW

El Teorema que a continuación se enuncia y que se demostrará más tarde, es conocido como el Primer Teorema de Sylow.

Teorema 2.1

Sea G un grupo finito y sea $|G| = p^n m$ donde $n \geq 1$, p un número primo y donde p no divide a m. Entonces,

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

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

Antes de comenzar con la demostración es necesario analizarla estructura que ésta tiene. El procedimiento que se utiliza es el método de la prueba por inducción el cual consiste en probar dos argumentos: el primero, que se cumple para n=1 y la segunda si se cumple para n, entonces se cumple para n+1 conocido como el paso inductivo. Además en la demostración nos apoyamos principalmente en el teorema de Cauchy, así como también en la noción del normalizador.

Cabe señalar que en el desarrollo de dicha demostración la presencia de algunos resultados de la teoría de grupo, fue de gran importancia para la elaboración de la misma.

2.2.1 DEMOSTRACIÓN DEL PRIMER TEOREMA DE SYLOW

Para n=1, por el Teorema1.48 (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 la existencia de un subgrupo de orden p^i, implica la existencia de un subgrupo de orden p^{i+1}.

Sea H un subgrupo de G de orden p^i, con i <n, entonces pdivide a (G:H), de donde por el Lema 1.53 se tiene que p también divide a (N[H]:H). Ahora bien H es normal en N[H], entonces podemos formar el grupo factor N[H]/H y tenemos que p también divide al orden de este grupo factor, ya que el orden de este grupo factor es precisamente el índice de H en N[H], entonces por el Teorema de Cauchy, N[H]/H tiene un subgrupo K de orden p.

Consideremos ahora el homomorfismo natural γ:N[H]→N[H]/H dado por $\gamma(n)= H_n$ $\forall n \in N[H]$, entonces por el Teorema 1.24, 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 Kerγ = H, y como $\gamma^{-1}(K)$/H es isomorfo a K, entonces: $|\gamma^{-1}(H)|=|H||K|=p^ip=p^{i+1}$ ya que por la hipótesis de inducción $|H|=p^i$. Así queda demostrada la primera parte del teorema.

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

2.3 SEGUNDO TEOREMA DE SYLOW

Procedemos a enunciar el Segundo Teorema de Sylowel cual establece una característica bastante interesante que tienen estos subgrupos.

Teorema 2.2

Sean P_1 y P_2 son p-subgrupos de Sylow de un grupo finito G. Entonces, P_1 y P_2 son subgrupos conjugados de G.

Para dar inicio a la demostración siguiente es importante mencionar que el procedimiento a utilizar es el método de la prueba directa el cual consiste en tomar como hipótesis un argumento dado y probar que la conclusión se infiere a partir de dicho argumento. Además, se hace uso de la teoría desarrollada de órbitas y los p-grupos.

Aclaramos que para este teorema y su debida demostración, también se hará uso de algunos resultados de la teoría de grupos.

2.3.1DEMOSTRACIÓN DEL SEGUNDO TEOREMA DE SYLOW

Se hará la demostración usando el concepto de acción de grupo, y la estrategia es hacer actuar uno de los p-subgrupos en las clases laterales derechas del otro.

Sea $\Re$ el conjunto de todas las clases laterales derechas de P_1, en este sentido los elementos de $\Re$ son subconjuntos de la forma P_1x, con $x \in G$.

Definamos la acción de grupo de $P_2 \in \Re$, por $\varphi(P_1x,g)=P_1xg$, para toda $P_1x \in \Re$ y toda $g \in P_2$, a esta acción es llamada en algunos textos "traslación derecha".

En este sentido hemos convertido a $\Re$ en un P_2-conjunto y por tanto podemos hacer uso de la teoría desarrollada en la Sección 1.9 y 1.10.

Haremos uso del Teorema 1.51 en el que se tiene que: $|\Re| \equiv |\Re_{P_2}| (\text{mod} p)$, pero $|\Re| = (G:P_1)$ 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 $|\Re_{P_2}| \neq 0$. Recordemos que $|\Re_{P_2}|$ es el número de orbitas de $\Re$ que constan de un solo elemento.

Sea $P_1x \in \Re_{P_2}$, 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 son conjugados■

2.4 TERCER TEOREMA DE SYLOW

Este teorema nos proporcionará valiosa información sobre el número de subgrupos de Sylow de un grupo arbitrario finito, el cual nos será muy útil precisamente en las aplicaciones que se desarrollarán en el siguiente capítulo.

Teorema 2.3

Si G es un grupo finito, p un primo y p divide a $|G|$, entonces el número de p-subgrupos de Sylow es congruente con 1 módulo p y divide a $|G|$.

Ahora podemos observar que para el desarrollo de la demostración se tomaran algunos elementos de la teoría de grupos; además se incluirán resultados previos de orbitas, así como el segundo teorema de Sylow.

2.4.1 DEMOSTRACIÓN DEL TERCER TEOREMA DE SYLOW

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 Sylowde G.

Sea P un p-subgrupo de Sylowde 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 $T\in P$ en $x^{-1}Tx$, es decir, $\varphi(T,x)=x^{-1}Tx$, 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 1.51 se tiene que $|P|\equiv|\mathcal{P}_p|(\text{mod}p)$. 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 $|\mathcal{P}|\equiv 1(\text{mod}p)$, 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 $\varphi(T, g) = g^{-1}Tg$, para todo T en $\mathcal{P}$ y toda *g* en G.

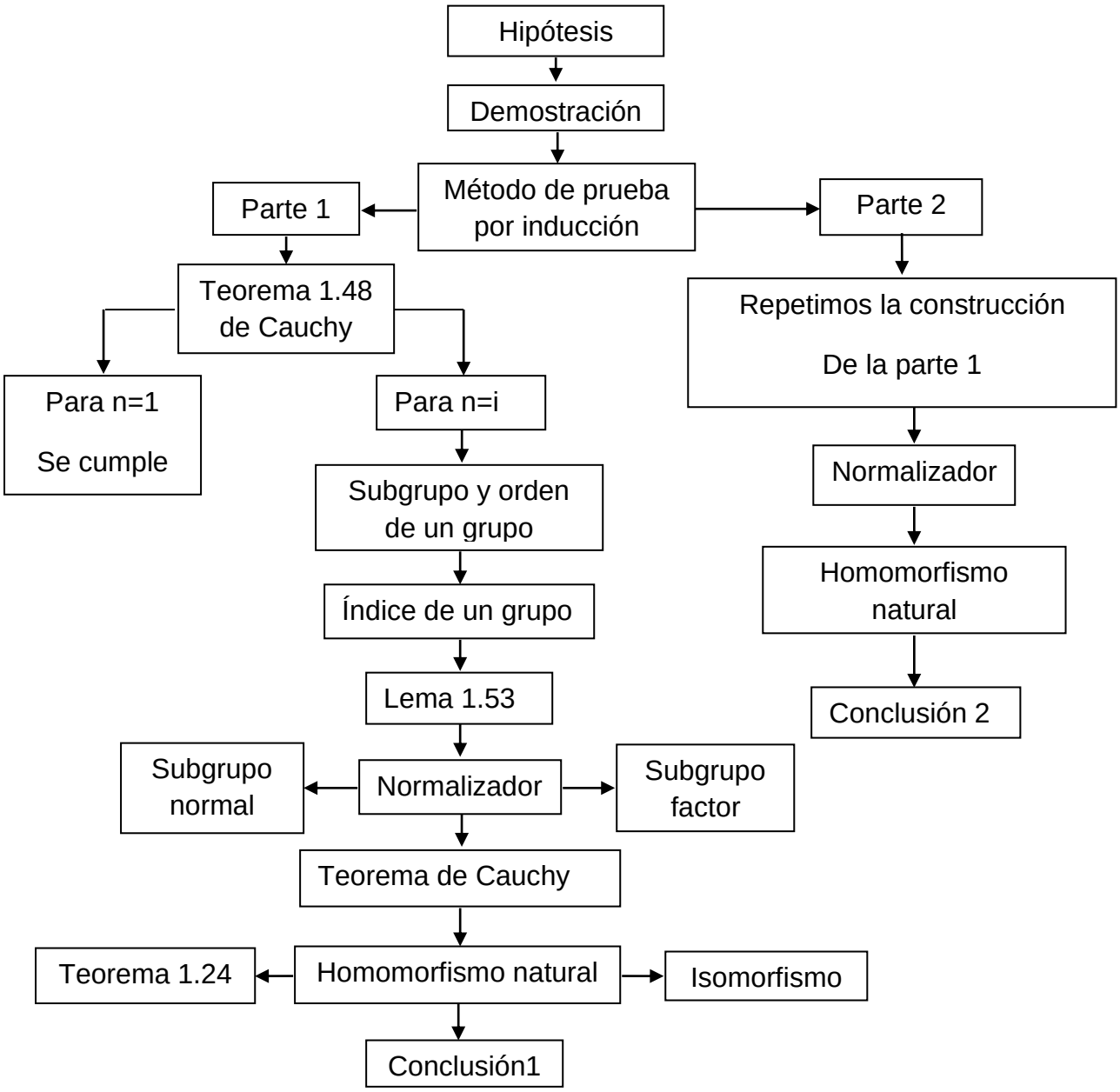
Como todos los p-subgrupos de Sylow de G son conjugados, según el Teorema 2.3 entonces hay una sola órbita en $\mathcal{P}$ bajo G. De esto se sigue el número de elementos de $\mathcal{P}$ es igual al número de elementos que tenga esa órbita de $\mathcal{P}$.

Además se tiene que si T es un elemento de $\mathcal{P}$, por el Teorema 1.46, 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■

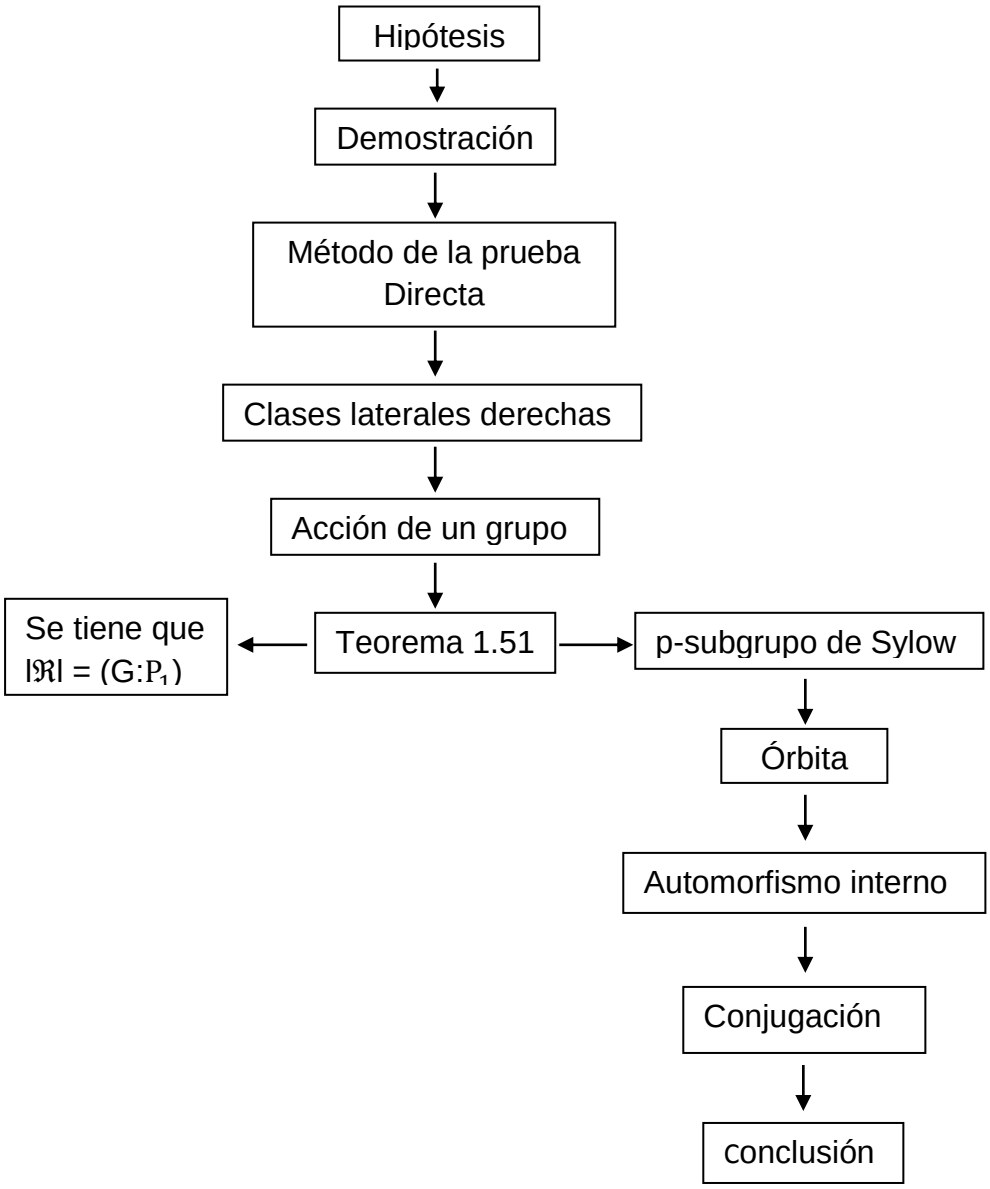
2.5 ESQUEMAS DE DEMOSTRACIONES DE LOS TEOREMAS DE SYLOW

En esta sección presentamos los esquemas para cada una de las demostraciones anteriores de los teoremas de Sylow. Al esquematizar dichas demostraciones se refleja de una forma más sencilla la secuencia que se sigue para su elaboración.

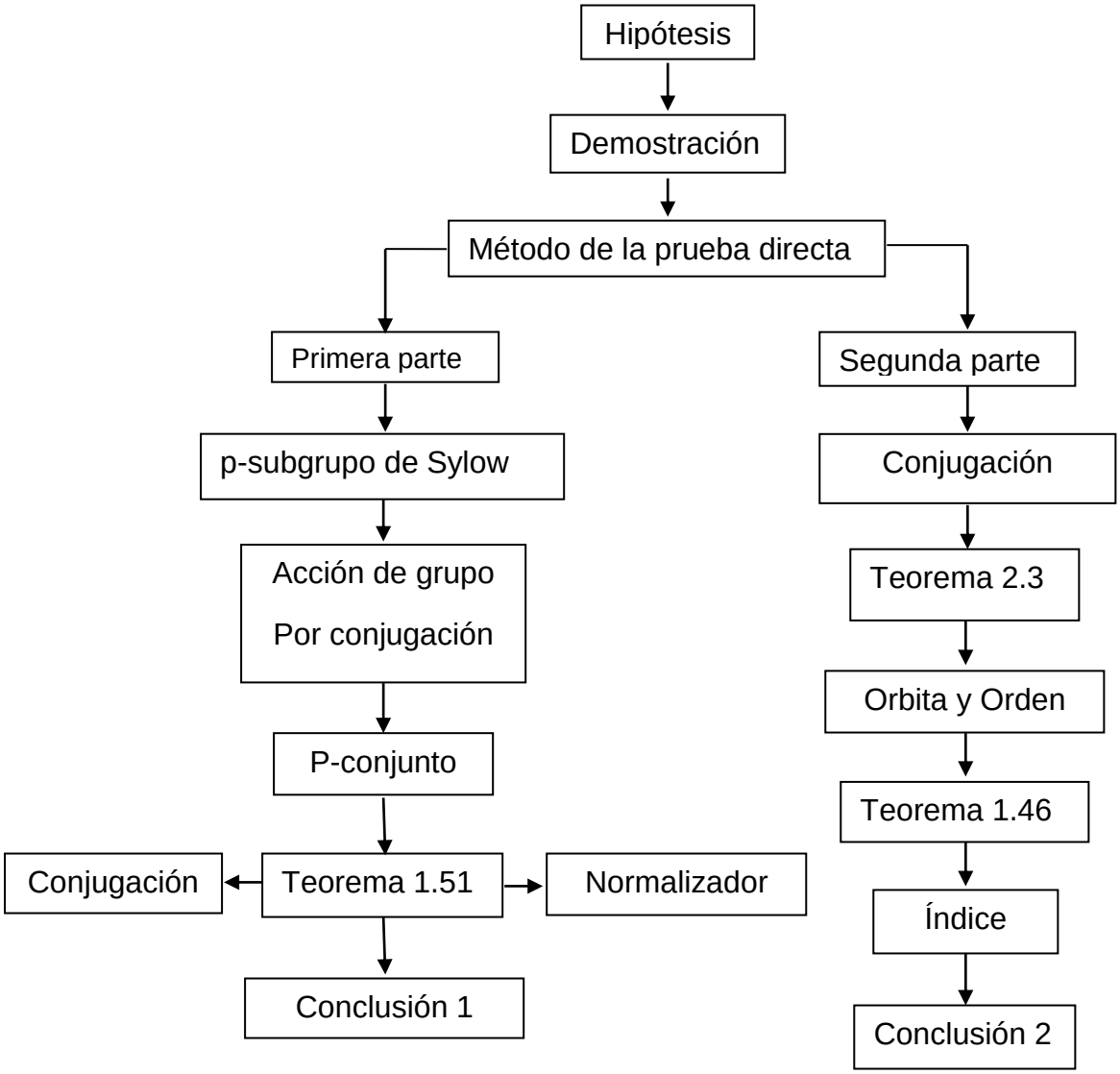
2.5.1 ESQUEMA DE DEMOSTRACIÓN DEL PRIMER TEOREMA DE SYLOW



2.5.2 ESQUEMA DE DEMOSTRACIÓN DEL SEGUNDO TEOREMA DE SYLOW



2.5.3 ESQUEMA DE DEMOSTRACIÓN DEL TERCER TEOREMA DE SYLOW



Concluimos este segundo capítulo esperando que las ilustraciones presentadas y el lenguaje usado sean de mucha utilidad para la mayor comprensión de este interesante trabajo.

Cabe señalar que los teoremas de Sylow tienen la misma característica implicativa, con una hipótesis y una conclusión definida. No obstante se observó que para probar éstos; el método da la prueba directa fue utilizado en dos casos y la inducción en un caso.

CAPITULO III

Algunas Aplicaciones de Los Teoremas de Sylow

3.1 INTRODUCCIÓN

Un problema de mucha importancia ha sido determinar si el grupo bajo estudio contiene subgrupos normales propios, esto lleva al problema de clasificar los grupos no simples de los simples, lo que constituyó uno de los avances más significativos de las matemáticas en el siglo XX.

Hoy en día estos resultados han dado lugar a muchas aplicaciones en diversos temas, puesto que son una herramienta muy poderosa a la hora de clasificar grupos no simple de los simples.

El principal logro de los últimos años ha sido completar la clasificación de todos los grupos simples y no simples. Este resultado sorprendente está basado en el arduo trabajo de una cantidad de equipos de teóricos.

En este capítulo, nuestro trabajo principal será presentar una variedad de aplicaciones existentes, las cuales hemos dividido en cuatro casos. Seguramente les parecerá sorprendente la facilidad con que se puede deducir ciertos hechos acerca de grupos de orden particular.

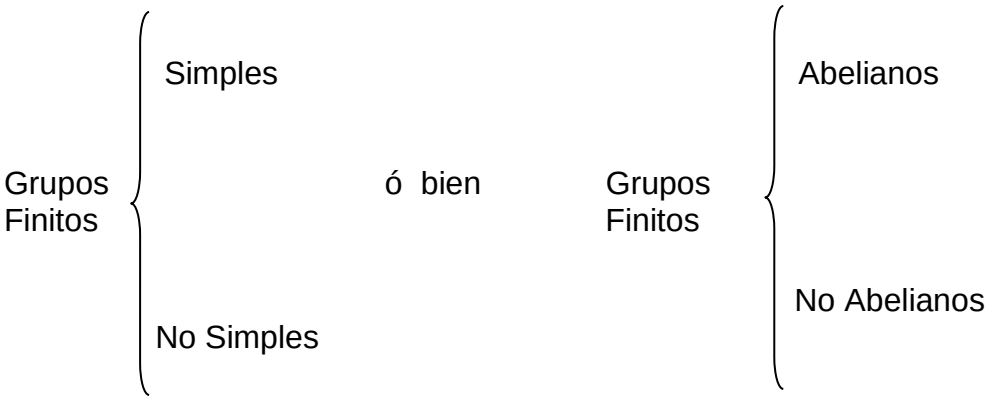
Sin embargo trataremos con grupos finitos de orden pequeño ya que si el orden de un grupo tiene solo unos cuantos factores, entonces las técnicas ilustradas en este capítulo pueden ser útiles para determinar la estructura del grupo pero si el orden de un grupo finito es altamente compuesto, esto es, si tiene un numero grande de factores, en general el problema es más difícil.

Por tal motivo listaremos primero a los grupos simples y nos interesaremos en la clasificación de los grupos no simples cuyos órdenes son menores o iguales a 100.

En todo éste capítulo denotaremos con p, q, r números primos tales que $p \leq q < r$ con las restricciones de que su orden sea a lo más el producto de tres primos.

3.2 CLASIFICACIÓN DE LOS GRUPOS FINITOS

Para clasificar todos los grupos finitos de orden $n \in N$, básicamente podemos dividirlos, tal como se muestra en los esquemas siguientes:



En esta sección se clasificarán los grupos simples de orden menor oigual a 100, lo que se reflejará en una tabla a la que nos referiremos como Tabla de Simples. El siguiente resultado indica la existencia de los grupos de orden p.

Teorema 3.1

Si G es un grupo de orden primo p, entonces G es isomorfo a Z_P.

Demostración

Por el Teorema 1.48 (Teorema de Cauchy**),** G tiene un elemento a de orden p. Sea A=<**a**>, como $|A|=|G|$, entonces A=G, de donde G es cíclico. Claramente la función $\psi: Z_p \to A$, definida como $\psi(k)=a^K, \forall k \in Z_p$, es un isomorfismo de grupos, por tanto $A= G \approx Z_p$.

Por el teorema de Lagrange (teorema 1.21) un grupo de orden primo no tiene subgrupos propios no triviales de ningún tipo. Por tanto los grupos de orden primo son simples.

Los grupos que nos interesan son aquellos cuyo orden es menor que 100 y sus órdenes son: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.

En la Tabla de Simples, marcamos los grupos simples de color rojo, de acuerdo a si su orden es primo.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

En anexo No.5 se mostrará la factorización en números primos del orden de los grupos no simples.

A continuación presentamos algunas de las aplicaciones de los teoremas de Sylow, en las cuales, los tres primeros casos serán gruposde diferentes ordenes y estos siendo no simples, seguido se concluye con un último caso para los grupos abelianos no simples.

3.3 CASO 1: GRUPOS NO SIMPLES DE ORDEN pq

Comenzaremos presentando algunos resultados que nos lleven a caracterizar a los grupos no simples.

Definición 3.2

Sean H y K subgrupos de un grupo G. El **ensamble** H∨K de H y K es la intersección de todos los subgrupos que contienen HK= {hk ⎪ h∈Hy k∈K}.

Lema 3.3

Sea G un grupo que contiene a los subgrupos normales H y K tales que H∩K= {x⎪ x∈H y x∈K}= {e} y H∨K=G entonces, G es isomorfo a HxK.

El siguiente teorema muestra que ningún grupo cuyo orden es de la forma pq con $p \neq q$, y ambos primos, no es simple.

Teorema 3.4

Si p y q son primos distintos con p<q, entonces, todo grupo G de orden pq tiene un solo subgrupo de orden q y este subgrupo es normal en G. De aquí, G no es simple. Si q no es congruente con 1 módulo p, entonces G es abeliano y cíclico.

Demostración

Por los teoremas 2.2 y 2.4 (Primer y Tercer Teorema de Sylow) los cuales señalan que G tiene un q-subgrupo de Sylow y que el número de dichos subgrupos es congruente con 1 módulo q y divide a pq y, por tanto, debe dividir a p. Como p<q, la única posibilidad es el número 1.

Así, hay un solo q-subgrupo de Sylow Q de G. este grupo Q debe ser normal en G, pues bajo un automorfismo interno, va a dar un grupo del mismo orden, es decir, asimismo. Entonces, G no es simple.

Asimismo, existe un p-subgrupo de Sylow p de G, y el número de estos divide a q y es congruente con 1 módulo p. este número debe ser 1 ó q, si q no es congruente con 1 módulo p, entonces el número debe ser 1 y p es normal en G.

Supongamos que q no es congruente con 1 módulo p, como todo elemento de Q, distinto de e, es de orden q y todo elemento de p, distinto de e, es de orden p, tenemos $Q \cap P = \{e\}$, además, $Q \vee P$ debe ser un subgrupo de G que contiene propiamente Q y de orden que divida pq.

De aquí, $Q \vee P = G$ y por el lema 3.3, G es isomorfo a QxP ó $Z_p x Z_q \cong Z_{pq}$. Así, G es abeliano y cíclico.

En la siguiente Tabla de Simples, se mostrarán con azul, los grupos no simples cuyo orden es menor que 100 y sus órdenes son: 6, 10, 14, 15, 21, 22, 26, 34, 35, 38, 39, 51, 55, 57, 58, 62, 65, 69, 74, 77, 82, 85,87, 91, 93, 94 y 95.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Se dará un ejemplo de dichos grupos para probar que éste no es simple.

Ejemplo:

Ningún grupo de orden 15 es simple.

Solución:

Sea G un grupo de orden 15. Como 15 =3*5 por el teorema 2.2 (Primer Teorema de Sylow), G tiene al menos un subgrupo de orden 5 y por el teorema 2.4 (Tercer Teorema de Sylow), el número de dichos subgrupos es congruente con 1 módulo 5 y divide a 15.

Como 1, 6 y 11 son los únicos enteros positivos menores que 15 que son congruentes con 1 módulo 5 y entre ellos solo el número 1 divide al 15, vemos entonces que G tiene solo un subgrupo de Sylow P de orden 5.

También se tiene que 5 no es congruente con 1 módulo 3, entonces podemos decir que dicho grupo es cíclico y abeliano por el teorema 3.4. Luego el subgrupo de Sylow P de orden 5 es normal y concluimos que G no es simple.

3.4 CASO 2: GRUPOS NO SIMPLES DE ORDEN p^2q

Caracterizaremos a continuación a grupos no simples de orden p^2q, con p y q primos.

Teorema 3.5

Todo grupo G de orden p^2q con p y q primos, no es simple.

Demostración

Supongamos primero que p<q y por el teorema 2.4 (Tercer Teorema de Sylow) sea n_q el número de q-subgrupos de Sylow. Entonces n_q es 1 ó p^2. En el caso que n_q=1, G tendría un subgrupo normal de orden q, y sería no simple.

Ahora supongamos que $n_q=p^2$. Entonces tendríamos que $q \mid (p^2-1)$ y, por lo tanto, $q \mid (p-1)$ o $q \mid (p+1)$. Como $p+1 \leq q$ el primer caso no puede pasar, y el segundo es posible si q=p+1. Pero, como los únicos primos consecutivos son p=2 y q=3, entonces $\mid G \mid =12$, por lo tanto la demostración se reduce a probar que un grupo de orden 12 no puede ser simple.

Luego, los subgrupos de Sylow de G serán de orden 3 y 4. Y aplicando nuevamente el Teorema 2.4 (Tercer Teorema de Sylow), el número de 3-subgrupo de Sylow definido por n_3, es 1 o 4. Si n_3=1, entonces G tendría un subgrupo normal de orden q, y sería no simple.

Luego, si n_3=4, entonces tenemos cuatro 3-subgrupos de Sylow, los cuales tienen orden 3, así que cada uno de ellos aporta 2 elementos de orden 3 (excluyendo al neutro). También, dados P_1,P_2 con $P_1 \neq P_2$, 3-subgrupo de Sylow, estos se cortan trivialmente, ya que $P_1 \cap P_2 \leq P_1$ y como $|P_1|=3$, entonces o bien $|P_1 \cap P_2| = 1$ o bien $|P_1 \cap P_2| = 3$. Si fuera el segundo caso, entonces sería $P_1 \cap P_2 = P_1$ y análogamente sería $P_1 \cap P_2 = P_2$ de donde $P_1 = P_2$, lo cual es falso. Asi la intersección es trivial, por lo que los cuatros 3-subgrupo de Sylow aportan $4 \cdot 2 = 8$ elementos de orden 3. Y asi ya no hay mas elementos de orden 3 en G.

Así estos 4 subgrupos reúnen 8 elementos de orden 3 distintos. Los 4 elementos restantes necesariamente deben formar el único y por lo tanto normal 2-subgrupo de Sylow de G, y en este caso, también resulta que G no es simple.

Por último, en el caso en que p>q, y por el teorema 2.4 (Tercer Teorema de Sylow) sea n_p el número de p-subgrupos de Sylow, entonces necesariamente n_p=1 y G contendría un subgrupo normal de orden p^2.

Marcamos de color verde los nuevos grupos no simples, en la Tabla de simples, cuyo orden es menor que 100 y son: 12, 18, 20, 28, 44, 45, 50, 52, 63, 68, 75, 76, 92, 98 y 99.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Veremos un ejemplo de dichos grupos para probar que este no es simple.

Ejemplo:

Ningún grupo de orden 63 es simple.

Solución:

Puesto que 63 = $3^2 \cdot 7$, y usando el teorema 2.2 (Primer Teorema de Sylow) implicala existencia de un subgrupo de orden 7 (7-subgrupo de Sylow en este caso, ya que 7∤9). Según el teorema 2.4 (Tercer Teorema de Sylow), el número de 7-subgruposde Sylow, denotado por n_7, cumple las condiciones $n_7 \equiv 1$(módulo 7), y $n_7 \mid 63$. Por tanto, para n_7=1 hay un subgrupo único de orden 7. Puesto que es el único de ese orden, debe ser normal. Eso demuestra que un grupo de orden 63 tiene un subgrupo normal no trivial y, por definición, no es simple.

3.5 CASO 3: GRUPOS NO SIMPLES DE ORDEN pqr

El siguiente teorema que se enuncia será de gran utilidad para el desarrollo de la aplicación.

Teorema 3.6

Si N es un subgrupo normal de G, entonces los subgrupos normales de G/N son de la forma K/N con K<G tal que N<K. Además, K/N es un subgrupo normal de G/N si K es un subgrupo normal de G.

El teorema que sigue afirma que los grupos cuyo orden es de la forma pqr con p<q<r, no es simple y se define pqr como el producto de tres primos.

Teorema 3.7

Todo grupo G de orden pqr con p<q<r donde p,q y r son primos, no es simple.

Demostración

Supongamos que G fuese simple, por el teorema 2.4 (Tercer Teorema de Sylow) tenemos que n_p, n_q y n_r son mayores a uno. Veamos los posibles valores de n_r. Como n_r tiene que ser un divisor de pqr, luego n_r será p, q, r, pq, pr o qr, y además debe ser congruente con 1 módulo r, es decir, de la forma tr+1 con t∈Z^+, lo que excluye a r, pr y qr, pero además debe ser mayor que r, esto excluye a los valores p y q. Luego se tiene que n_r=pq. En consecuencia G tendría pq(r-1) elementos de orden r, lo que implica que hay pqr-pq(r-1)=pq elementos que no sonde orden r.

Consideremos ahora las posibilidades de n_q: igual que antes, n_q debe ser un divisor de pqr, por tanto puede ser p, q, r, pq, pr o qr, y de la forma tq+1 con t∈Z^+, entonces quedan excluidos p, q, pq y qr. También podemos descartar que n_q=pr, pues sino existiría en el grupo pr(q-1) elementos de orden q. Pero pr(q-1)>pq, y como vimos antes, no existen tantos elementos de orden q, esto fuerza a que n_q=r.

Finalmente estudiemos los casos posibles de n_p: haciendo el mismo razonamiento que en los dos casos anteriores las únicas posibilidades son: q, r y qr. En cualquiera de los tres casos tenemos que n_p ≥q y el grupo está obligado a contener al menos q(p-1) elementos de orden p. Entonces el grupo contiene al menos pq(r-1)+r(q-1)+q(p-1)+1=pqr+rq-r-q+1 elementos distintos, pero esta cantidad es mayor a |G| (pues rq>r+q). Por tanto, tenemos que n_p, n_q on_r es igual a 1.

Si n_p=1, sea P∈p-subgrupo de Sylow de G. Como |G/P|=qr existe un H que es un subgrupo normal de G/P tal que |H|=r y por el Teorema 3.4, H=H/P siendo K un subgrupo normal de G y por el Teorema 3.6, |K|=pr. Entonces existe un único R que es subgrupo normal de K tal que |R|=r, y por el Teorema 3.4. Como R es normal en K y K es normal en G, tenemos que R es un subgrupo normal de G. El mismo razonamiento se aplica para n_q=1. Por tanto G no es simple■

Los nuevos grupos no simples, los marcaremos de color rosa, en la Tabla de simples, cuyo orden es menor que 100 y son: 30, 42,66, 70 y 78.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Se dará un ejemplo de éstos grupos para mostrar que dicho grupo no es simple.

Ejemplo:

Ningún grupo de orden 30 es simple.

Solución:

En efecto, supongamos que G es un grupo de orden 30= 2·3·5, cuyos divisores son: 1, 2, 3, 5, 6, 10, 15, 30.

El número n_5 de 5-subgrupos de Sylow de G debe ser un divisor de 30 y además $n_5 \equiv 1$(módulo 5), por lo que las posibilidades para n_5 son 1 o 6. Si n_5=1, entonces el 5-subgrupo de Sylow será normal y por lo tanto G no es un grupo simple. Probaremos que éste es el caso mostrando que el caso n_5=6 no puede suceder, pero antes de hacer esto consideremos el número n_3 de 3-subgrupos de Sylow de G, como $n_3 \equiv 1$(módulo 3), las posibilidades para n_3 son 1 y 10. Si n_3 =1, entonces el 3-subgrupo de Sylow sería normal y por lo tanto G no es un grupo simple. Por lo tanto, debemos mostrar que los casos n_3 =10 y n_5=6 no pueden darse. En efecto, si n_5=6, entonces los seis 5-subgrupos de Sylow de G contribuyen 6(5-1) elementos a G y si n_3 =10 los diez 3-subgrupos de Sylow de G contribuyen 10(3-1) elementos a G. Así, con las contribuciones de los 5-subgrupos de Sylow y los 3-subgrupos de Sylow, y del neutro, G tiene al menos 6(5-1)+10(3-1)+1=45 elementos, una contradicción con el orden de G que es 30.

3.6 CASO 4: GRUPOS ABELIANOS NO SIMPLES DE ORDEN p^2

El siguiente resultado, nos proporciona una propiedad importante sobre los grupos cuyo orden es de la forma p^2.

Teorema 3.8

Si G es un grupo de orden p^2, entonces G es isomorfo a uno de los grupos Z_{p^2} ó Z_p x 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 e isomorfo a Z_{p^2}. En el caso de que G no tenga elemento de orden p^2, entonces por el Teorema 1.48 (Teorema de Cauchy) se tiene que G contiene un elemento **a** de orden p.

Sea A el subgrupo cíclico generado por **a**. De aquí que A es de orden p, por lo que A no es todo G, además por el teorema 2.2 (Primer Teorema de Sylow), A es normal en G. Sea **b** un elemento de G tal que **b**$\notin$A. El orden de este elemento divide al orden de G y no es p^2, por tanto es también de orden p. Denotemos a B como el subgrupo cíclico generado por **b**, análogamente B también es normal en G.

Entonces A$\cap$B={e}**,** ya que si no fuera así un elemento **c**$\in$A$\cap$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 teorema 2.2 (PrimerTeorema de Sylow), estos subgrupos son normales en G. Por tanto, estos subgrupos cumplen con las hipótesis del lema 3.3, de donde G es el producto directo de A y B, por tanto isomorfo a Z_P x Z_P; pero por el mismo lema 3.3, entonces G es abeliano■

Una forma de representar estos grupos es: G= <**a**,**b**>, donde $\mathbf{a}^p=\mathbf{b}^p$=e, con la relación **ab**=**ba**.

Marcamos de color amarillo a los grupos abelianos no simples encontrados, en la Tabla de simples, cuyo orden es menor que 100 y son: 4, 9, 25 y 49.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Presentamos un ejemplo de uno de éstos grupos para mostrar que éste es abeliano.

Ejemplo:

Todo grupo de orden 9 debe ser abeliano.

Solución:

Sea G un grupo de orden 3^2=9 el cual es un 3-grupo, por corolario 1.49. Luego todo elemento en G tiene orden alguna potencia del primo 3. Esto es, los posibles órdenes de los elementos de G son: 1, 3 y 9. Salvo isomorfismo hay dos grupos de orden 9. De este modo, se tienen dos posibilidades $G\cong Z_9$ o $G\cong Z_3xZ_3$, ya que $Z_3xZ_3\cong Z_9$. Para el primer caso como Z_9 es cíclico, se tiene que Z_9 es abeliano y lo tendría que ser G.

Para el segundo caso, como Z_3 es cíclico entonces Z_3 es abeliano y también lo es Z_3xZ_3 y lo tendría que ser G.

Muchas de las aplicaciones de los teoremas de Sylow consisten en demostrar que un grupo de un orden dado no es simple, es decir que tiene subgrupos normales propios. Para grupos de orden pequeño, con frecuencia es suficiente la condición de congruencia del tercer teorema de Sylow para forzar la existencia de un subgrupo normal, pero a veces se requiere un análisis de la interacción de los diversos primos que dividen al orden del grupo, análisis del que se deduce la existencia de un subgrupo normal.

CONCLUSIONES

- Una primera aproximación al estudio de la existencia de subgrupos normales se hace con los Teoremas de Sylow.

- Para la demostración de los teoremas de Sylow fue necesaria la utilización de la teoría básica de grupos.

- Las aplicaciones de los teoremas de Sylow son muy importantes en lo que se refiere a la clasificación de los grupos finitos no simples de acuerdo al orden dado.

- El primer paso en cualquier aplicación numérica de los teoremas de Sylow es hallar la descomposición en factores primos del orden del grupo.

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

- 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.

ANEXOS

ANEXO No.1

BIOGRAFIA DE PETER LUDWIG MEJDELL SYLOW

El matemático Peter Ludwig Mejdell Sylow nació el 12 de diciembre de 1832 en Cristianía (actual Oslo) y murió el 7 de septiembre de 1918 en la misma ciudad.

Estudió en la universidad de Cristianía donde ganó un concurso matemático en 1853. En 1856, al no haber puesto docente en la universidad se fue a la ciudad de Frederikshald, donde se dedicó a la enseñanza secundaria desde 1858 a 1898.

Sin embargo, Sylow continuó estudiando, primero funciones elípticas en la tradición de Abel y Jacobi, y después resolubilidad de ecuaciones algebráicas por radicales, siguiendo a Abel y a Galois.

En 1861, Sylow obtuvo una beca para viajar a Berlín y Paris. En Paris asistió a las clases de Chasles sobre cónicas, a las de Liouville sobre mecánica racional y a las de Duhamel sobre teoría de límites. En Berlín, intercambió opiniones con Kronecker pero no pudo asistir a las clases de Weierstrass, que estaba enfermo.

En 1862, Sylow sustituyó por un tiempo a Broch en la universidad de Cristianía (Oslo). En sus clases Sylow explicaba la teoría de Abel y Galois sobre ecuaciones algebráicas. Merece la pena resaltar, que aunque no había probado todavía sus célebres teoremas (los publicó 10 años después) en estas clases ya dejó planteado parte del enunciado de dichos teoremas.

Después de probar el conocido teorema de Cauchy: "un grupo de orden divisible por un primo p siempre posee un subgrupo de orden p", Sylow se preguntaba si ese resultado se podía generalizar a potencias de p.

Entre 1873 y 1881, Sylow y Lie prepararon una edición de todos los trabajos de Abel. Lie dijo que la mayor parte del trabajo fue realizado por Sylow.

Sin embargo, toda la fama de Sylow recae en un artículo de 10 páginas publicado en 1872. Se titulaba Théorèmes sur les groupes de substitutions y se publicó en los Mathematische Annalen, donde aparecen los tres teoremas famosos de

Sylow. Sylow probó el resultado, quizás, más profundo de toda la teoría de grupos finitos.

Si p^r es la máxima potencia de un primo p, que divide al orden n de un grupo finito G, entonces existe al menos un subgrupo de este orden dentro de G, hay 1 + kp de tales subgrupos, y cualesquiera dos de tales subgrupos son conjugados.

Desde entonces, casi todos los demás resultados y trabajos sobre grupos finitos usan estos teoremas.

A raíz de esa publicación, Sylow se convirtió en editor de la revista Acta Matemática y, en 1894, fue nombrado doctor honoris causa por la universidad de Copenhage.

Lie creó una cátedra con su nombre en la universidad de Christianía y Sylow ocupó dicha cátedra desde 1898.

.

ANEXO No. 2

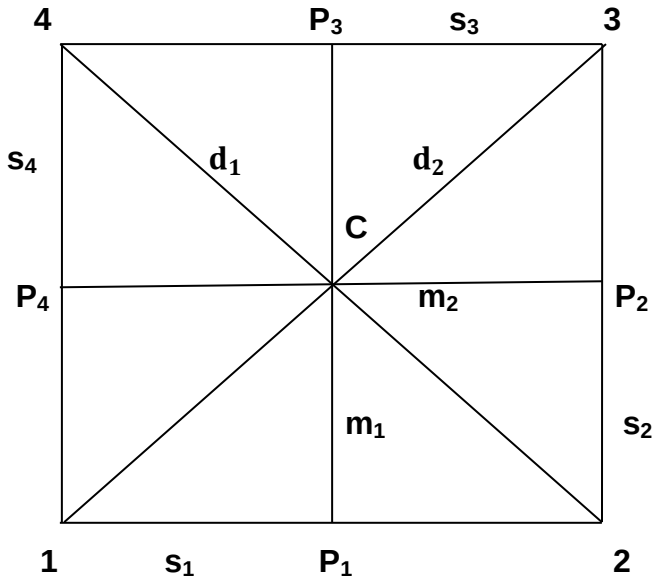
GRUPO DE PERMUTACIONES DE S_3

Tabla

	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_2	μ_3	μ_1
ρ_2	ρ_2	ρ_0	ρ_1	μ_3	μ_1	μ_2
μ_1	μ_1	μ_3	μ_2	ρ_0	ρ_2	ρ_1
μ_2	μ_2	μ_1	μ_3	ρ_1	ρ_0	ρ_2
μ_3	μ_3	μ_2	μ_1	ρ_2	ρ_1	ρ_0

ANEXO No. 3

GRUPO DE SIMETRIAS DEL CUADRADO



ANEXO No. 4

ACCION DE D_4 EN X

Tabla de las Simetrías del Cuadrado

	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_1	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_1	C	P_4	P_3	P_2	P_1

ANEXO No. 5

FACTORIZACION DE LOS NÚMEROS PRIMOS

$2=2$

$3=3$

$5=5$

$7=7$

$11=11$

$12=2^2 \cdot 3$

$13=13$

$17=17$

$18=2 \cdot 3^2$

$19=19$

$23=23$

$24=2^3 \cdot 3$

$29=29$

$30=2 \cdot 3 \cdot 5$

$31=31$

$36=2^2 \cdot 3^2$

$37=37$

$41=41$

$42=2 \cdot 3 \cdot 5$

$43=43$

$47=47$

$49=7^2$

$53=53$

$55=5 \cdot 11$

$59=59$

$60=2^2 \cdot 3 \cdot 5$

$61=61$

$66=2 \cdot 3 \cdot 11$

$67=67$

$71=71$

$72=2^3 \cdot 3^2$

$73=73$

$78=2 \cdot 3 \cdot 13$

$79=79$

$83=83$

$84=2^2 \cdot 3 \cdot 7$

$85=5 \cdot 17$

$89=89$

$90=2 \cdot 3^2 \cdot 5$

$91=7 \cdot 13$

$96=2^5 \cdot 3$

$97=97$

NOTACIONES

$a*b$:	Operación binaria
<G,$*$>:	Grupo
|G|:	Orden de G
H≤G:	Inclusión de subgrupos
S_n:	Grupo simétrico de n letras
A_n:	Grupo alternante de n letras
$\prod_{i=1}^{n} G_i$:	Producto directo de grupos
HK:	Conjuntos de productos
H∨K:	Ensamble de grupos
<**a**>:	Subgrupo cíclico generado por a
G≅G':	Grupos isomorfos
aH, a+H:	Clases laterales izquierdas
Ha, H+a:	Clases laterales derechas
(G:H):	Índice de H en G
i_g:	Conjugación por g
G/N:	Grupo factor
γ:	Transformación natural de clases residuales
xG:	Órbita de x en G
Gx:	Conjunto de isotropía
a≡b(mod n):	Congruencia
N[H]:	Normalizador de H
$\mathcal{P}$:	La colección de todos los p-subgruposde Sylowde
n_p:	El número de p- subgrupos de Sylow.

BIBLIOGRAFIA

- Fraleigh John B. Algebra Abstracta. Tercera Edición. Editorial Addison-Wesley Iberoamericana. Wilmington Delaware, 1987.

- HersteinI.N. Algebra Abstracta. Editorial Macmillan Publishing Company, Iberoamerica, S.A de C.v 1988.

- HersteinI.N. Algebra Moderna. Primera Edición. Editorial Trillas-México 1970.

- Frank Ayres JR. Ph.D. Teoría y Problemas del Algebra Moderna. Editorial McGraw-Hill de México, S.A de C.V 1969.

- Ferrario Julieta. Aplicaciones de los Teoremas de Sylow. Instituto Argentino de Matemática "Alberto P.Calderon" Saavedra 15-Piso 3 Buenos Aires-Argentina. Encontrado en:

  http://www.iam.conicet.gov.ar/cms/?q=es/system/files/u3/...pdf (28/08/2011)

- Jesús Mendivil León. Teoremas de Sylow, Productos semidirectos y Clasificación de los grupos de orden pqr<100. Universidad de Sonora-México. Encontrado en:

  http://www.lic.mat.uson.mx/tesis/110TesisMendivil.pdf (03/09/2011)

- Rubén A. Hidalgo. Estructuras Algebraicas, Gruposy Anillos. Universidad Técnica Federico Santa María. Santiago- Chile. Encontrado en:

  http://www.docencia.mat.utfsm.cl/~rhidalgo/files/estructuras.pdf(12/10/2011)

- Académicos. 3º Profesorado en Matemática-Álgebra. Instituto 127 Unidad: Teoría de Grupos. Ciudad del Acuerdo, Buenos Aires-Argentina. Encontrado en:

  http://www.instituto127.com.ar/Academicos/Catedras/ProfMatealgebra/1Teoria_de_grupos.pdf(10/11/2011)

- Fernando Barrera Mora. Introducción a la Teoría de Grupos. Centro de Investigación en Matemáticas. Universidad Autónoma del Estado de Hidalgo (UAEH)- México. Encontrado en:

  http://www.mimosa.pntic.mec.es/jgomez53/matema/docums/barrera-grupos.pdf(25/11/2011)