UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE CIENCIAS

ESCUELA PROFESIONAL DE MATEMATICA

La teoría de los p-grupos y los teoremas de Sylow

Informe de Suficiencia Profesional para Optar

el Titulo Profesional de Licenciado en Matemática

Presentado Por

César Augusto Saal Riqueros

Lima – Perú

2003

A

Mary

Marita

Paquita

Índice

1 Generalidades 1

1.1 Grupos 1

1.2 Potencias de un elemento 2

1.3 Grupo conmutativo o abeliano 2

1.4 Propiedades básicas de un grupo 2

1.5 Orden de un grupo 3

1.6 Homomorfismos de grupos 7

1.6.1 Propiedades básicas de un homomorfismo 8

1.7 Subgrupos 9

1.7.1 Criterios para determinar si un conjunto es un subgrupo 11

1.7.2 Propiedades básicas 11

1.7.3 Generación de grupos 12

1.7.4 Propiedades básicas 13

1.8 Orden de un elemento 15

1.8.1 Propiedades básicas 15

1.9 Grupos cíclicos 16

1.9.1 Propiedades básicas 17

1.10 Multiplicación de subconjuntos no vacíos 20

1.10.1 Propiedades básicas 20

1.11 Clases laterales de un subgrupo 21

1.11.1Propiedades básicas 21

1.12 Teorema de Lagrange 23

1.12.1 Propiedades básicas 23

1.13 Conjunto cociente 24

1.13.1 Subgrupos normales 26

1.13.2 Propiedades básicas 26

1.13.3 Grupo cociente 29

1.14 Centro de un grupo 29

1.14.1 Propiedades básicas 29

1.15 Centralizador de un elemento 30

1.15.1 Propiedades básicas 30

1.16 Conjugado de un elemento 30

1.16.1 Propiedades básicas 30

1.17 Ecuación de clase 31

1.18 Los teoremas de isomorfismo 31

1.18.1 El primer teorema de isomorfismo 32

1.18.1.1 Propiedades básicas 32

1.18.2 El segundo teorema de isomorfismo 33

1.18.3 El tercer teorema de isomorfismo 34

1.18.4 El teorema de correspondencia 34

1.18.4.1 Propiedades básicas 36

1.19 El grupo simétrico 36

1.19.1 Propiedades básicas 41

1.20 Teorema de representación de Cayley 42

1.21 Grupo de permutaciones 43

1.22 Estabilizador de un elemento 44

1.22.1 Propiedades básicas 44

2 La teoría de los p-grupos y los teoremas de Sylow 47

2.1 La teoría de los p-grupos 47

2.1.1 Definición de p-grupo 47

2.1.2 Teoremas fundamentales 47

2.2 Los teoremas de Sylow 52

2.2.1 Definición de p-subgrupo de Sylow 52

2.2.2 Teoremas fundamentales 55

3 Algunas aplicaciones de los teoremas de Sylow 65

3.1 Los grupos diedrales 65

3.1.1 Definición de grupo diedral 65

3.2 El grupo Q de los cuaterniones 72

3.3 Clasificación de los grupos de orden bajo 77

3.3.1 Grupos de ordenes 2,3,5,7,11 y 13 77

3.3.2 Grupos de ordenes 4 y 9 77

3.3.3 Grupos de ordenes 6, 10 y 14 78

3.3.4 Grupos de orden 8 78

3.3.5 Grupos de orden 12 78

3.3.6 Grupos de orden 15 79

3.3.7 Tablas de grupos de ordenes desde 2 hasta 15 79

Bibliografía consultada 80

Introducción

En este trabajo se estudia los teoremas de Sylow y sus aplicaciones a la teoría de grupos finitos.

En primer lugar, se expone las generalidades de la Teoría de Grupos y a continuación se desarrolla la teoría de p-grupos. Un p-grupo es un grupo en el cual el orden de cualquier elemento es una potencia de p, donde p es un primo. Una propiedad muy importante de los p-grupos es que tienen centros no triviales. Para la demostración de este hecho se utiliza la ecuación de clase: el orden de un grupo finito es igual al orden de su centro más la suma de los índices de los centralizadores de todos los elementos no centrales y no conjugados. Se llama p-subgrupo de Sylow de un grupo G a un p-subgrupo maximal de G. Una razón por la cual la teoría de los p-grupos es fundamental es que la estructura de los p-subgrupos de Sylow de un grupo finito G determina parcialmente la estructura de G. Como un ejemplo, citamos el siguiente teorema: Si G es un grupo finito cuyos p-subgrupos de Sylow son todos cíclicos, entonces G tiene un subgrupo normal N tal que G/N y N son cíclicos. En tercer lugar, se exponen los teoremas de Sylow. Estos teoremas son básicos para determinar la estructura de algunos grupos finitos. Según estos teoremas, para un primo dado p, todos los p-subgrupos de Sylow de G son conjugados (y por lo tanto isomorfos); el número de estos subgrupos es congruente a 1 módulo p, y es un divisor de G. Un concepto clave que se utiliza en las demostraciones de estos teoremas, es el de normalizador de un

subgrupo, el cual tiene la siguiente propiedad: El índice del normalizador N(H) en G es igual al número de conjugados del subgrupo H. Otro concepto clave es el de órbita de un grupo G: Si G es un grupo de permutaciones que actúa sobre un conjunto X, es decir, G es un subgrupo del grupo simétrico S_X, entonces

x, y $\in$X son G-equivalentes si existe s$\in$G tal que s(x) = y. Las G-clases de equivalencia son llamadas las órbitas de G. El conjunto I (G) de todas las conjugaciones (o automorfismos internos) de G es un grupo de permutaciones sobre G. Las órbitas de I (G) son las clases de conjugación de G. Si G es un grupo de permutaciones que actúa sobre un conjunto X, entonces el estabilizador de x$\in$ X es un subgrupo de H_X de G formado por todos los t$\in$ G tales que t (x) = x. Un hecho muy útil es el siguiente: Si X es un conjunto finito y G es un grupo de permutaciones sobre X, entonces la cardinalidad de cada órbita de G divide a $|G|$. Precisamente; la cardinalidad de la órbita de x es igual al índice del estabilizador de x en G.

Finalmente, se consideran algunas aplicaciones de los teoremas de Sylow:

-Para cualquier primo p, los únicos grupos de orden 2p, salvo isomorfismo, son Z_{2p} y el grupo diedral D_p.

-Si G es un grupo finito de orden pq, donde p y q son primos, p > q y q no divide a p-1, entonces G es cíclico. En particular, el único grupo de orden 15, salvo isomorfismo, es Z_{15}.

-Los únicos grupos no abelianos del orden 8, salvo isomorfismo, son el grupo diedral D_4 y el grupo de los cuaterniones Q.

-Todo grupo G de orden 12 que no es isomorfo a A_4 contiene por lo menos un elemento de orden 6, y consecuentemente existen exactamente 3 grupos no abelianos de orden 12, salvo isomorfismo.

Capitulo I

Generalidades

En este capítulo presentamos los aspectos fundamentales de la teoría de grupos. Las ideas preliminares de esta teoría pueden ser construidas a partir de conceptos elementales de la Aritmética, para derivar posteriormente propiedades de sistemas algebraicos (objeto central del Álgebra Moderna). El Álgebra Moderna en general y la Teoría de Grupos en particular, estudian operaciones sobre objetos que no necesariamente son números pero que satisfacen ciertas propiedades análogas a las operaciones elementales de la Aritmética. Estas ideas previas son necesarias para desarrollar posteriormente la teoría de los p-grupos, así como el estudio de los teoremas de Sylow y sus consecuencias.

1.1. Grupos.

Definición.- Un conjunto no vacío G, provisto de una operación binaria $\bullet : G\times G \to G$, tal que a cada par (a, b) le hace corresponder el elemento $a\bullet b$, se llama grupo, si se cumplen las siguientes condiciones:

i) La operación binaria $\bullet$ es asociativa, esto es,

$$(a\bullet b)\bullet c = a\bullet (b\bullet c).$$

ii) $\exists\, e \in G$,elemento neutro, tal que $a\bullet e = a = e\bullet a$, $\forall\, a \in G$

iii) $\forall\, a\in G$, existe $a^{l}\in G$ tal que: $a\bullet a^{l} = e = a^{l}\bullet a$

Notación. El elemento a^I se llama la inversa de a y se denota por $a^I = a^{-1}$.

En lo que sigue, el elemento $a \bullet b$ se denotara por ab, y G simbolizara un grupo.

1.2. Potencias de un elemento

Definición. Se define las potencias de un elemento (en notación multiplicativa) de un grupo G de la siguiente manera: Dado $a \in G$, definimos $a^0 = e$ y, para cualquier **n** entero positivo, $a^n = aa.....a$ (n factores) y $a^{-n} = (a^{-1})^n$. De lo anterior se deduce las siguientes formulas:

i) $\forall m, n \in Z$, se tiene: $a^m a^n = a^{m+n}$

ii) $\forall m, n \in Z$, se tiene: $(a^m)^n = a^{mn}$

iii) $\forall m, n, k \in Z$, se tiene: $(a^{m+n})^k = a^{mk+nk}$

Comentario. En notación aditiva:

a^n significa: $na = a+a+a.....+a$ (n veces) y,

a^{-n} significa: $(-n)a = (-a)+(-a)+.....+(-a)$ (n veces).

1.3. Grupo conmutativo o abeliano

Definición. Se dice que G es un grupo conmutativo o abeliano, si dos elementos cualesquiera de G conmutan, esto es: $ab = ba \quad \forall a, b \in G$

1.4. Propiedades básicas de un grupo

i) Leyes de cancelación a derecha e izquierda:

$ac = bc \rightarrow a = b$ y $ca = cb \rightarrow a = b$

ii) El elemento neutro de un grupo es único.

iii) Cada elemento de un grupo tiene un único inverso

iv) Para todo $a \in G$, $(a^{-1})^{-1} = a$

v) Para todo $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$

vi) El único elemento idempotente de un grupo es **e**.

Es decir $a^2 = a \leftrightarrow a = e$

Comentario. Nótese que si en un conjunto tenemos una ley asociativa, conmutativa y posee elemento neutro; entonces dicha ley no es suficiente para garantizar que el conjunto sea grupo. Por ejemplo en Z_{12}, la multiplicación cumple las propiedades anteriores, pero $\bar{1}.\bar{1} = \bar{1}$ y $\bar{4}.\bar{4} = \bar{4}$, esto es, la ecuación a.a = a tiene mas de una solución Si consideramos una ecuación del tipo ax = b, por ejemplo 8x = 4, son soluciones de esta ecuación en Z_{12}, x = 2 , x = 5 y x =8. Es decir observamos que la solución tampoco es única. Esto no se observa en un grupo, tal como lo garantiza la siguiente propiedad..

vii) Dados $a, b \in G$, las ecuaciones ax =b e ya = b tienen soluciones únicas $x = a^{-1} b$ e $y = ba^{-1}$ respectivamente.

viii) Si todo elemento de G es su propio inverso, entonces G es abeliano, es decir: Si $a^2 = e$ para todo $a \in G$, entonces G es abeliano.

ix) Si G es abeliano, entonces $(ab)^n = a^n b^n$, para todo $n \in Z$

1.5. Orden de un grupo

Definición. Si un grupo G posee un número finito de elementos, se define el orden de G, denotamos $|G|$, como el número de elementos de G, en

cuyo caso se dice que G es un grupo finito. En caso contrario, G es un grupo infinito.

Podemos notar que los grupos más familiares son los de orden infinito. En el análisis de los grupos finitos el orden será fundamental para caracterizarlos.

Ejemplos

(1) El estudio de las tablas de los grupos cuyo orden son menores o iguales a cuatro, nos permite afirmar directamente que tales grupos resultan siempre abelianos. En particular veamos las presentaciones de las tablas de tales grupos.

a) Todos los grupos de dos elementos, G = {e, a }, poseen una tabla de operación similar a la siguiente:

•	e	a
e	e	a
a	a	e

Observamos que el grupo es conmutativo (la tabla es simétrica con respecto a la diagonal principal) y por lo tanto es abeliano.

b) Si G posee tres elementos, G = { e, a, b }, la tabla de operación es:

•	e	a	b
e	e	a	b
a	a		
b	b		

El resultado de operar **a** con **a** puede ser **b** o **e**; pero el de **a** con **b** debe ser **e** (en caso contrario, si fuera **b**, tendríamos que **a** = **e**). Luego tenemos que a•a = b , con lo cual se puede completar la tabla de la siguiente manera:

•	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

c) Para un conjunto G de la forma G = {e, a, b, c }, con cuatro elementos distintos, es posible definir dos leyes de composición interna diferentes que proveen a G la estructura de grupo abeliano, tal como se observa en las siguientes tablas:

Tabla 1

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

Tabla 2

•	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 de la tabla 1, es (Z_4 , +); mientras que la tabla 2 corresponde al conocido 4- grupo de Klein y ejemplos de este último

son , un grupo de funciones, un grupo de permutaciones de cuatro objetos, etc.

En cuanto al grupo de funciones, tenemos por ejemplo el siguiente:

$G = \{ i, g_1, g_2, g_3\}$, donde, $i(x) = x$, $g_1(x) = -x$, $g_2(x) = 1/x$, $g_3(x) = -1/x$ .La tabla correspondiente es:

o	i	g_1	g_2	g_3
i	i	g_1	g_2	g_3
g_1	g_1	i	g_3	g_2
g_2	g_2	g_3	i	g_1
g_3	g_3	g_2	g_1	I

(2) **Estudio del grupo de las congruencias.** Dado un entero positivo **n,** mostraremos que siempre existe al menos un grupo con **n** elementos.

Solución.

Para esto usaremos el concepto de congruencia : para todo a, $b \in Z$, se tiene que: **a** es congruente con **b** modulo **n**, en símbolos, $a \equiv b \pmod n$), si su diferencia a-b, es un múltiplo de **n**.

Por otro lado sabemos que la relación de congruencia definida en el conjunto Z es una relación de equivalencia, podemos por tanto considerar el conjunto cociente de Z mediante esta relación de equivalencia, $Z / \equiv_n$, el cual se simboliza por Z_n, y se denomina conjunto de las clases de congruencias modulo n .Así decimos $\bar{a} \in Z_n$, donde $\bar{a} = \{ b \in Z / b \equiv a \pmod n \}$.

Ahora dada una clase de equivalencia $\bar{a} \in Z_n$ siempre podemos elegir un representante **b** de a , de modo que $a = b$ y $0 \leq b < n$. Para esto basta dividir **a** entre **n** y tomar **b** como el resto de esta división, con lo cual podemos escribir $Z / \equiv_n = Z_n = \{ \bar{0}, \bar{1}, \bar{2}, ..., \overline{n-1} \}$, donde el conjunto { 0,1,2,.....,n-1 } es un sistema completo de restos modulo **n**. $\bar{a} + \bar{b} = \overline{a+b}$ es una operación bien definida, entonces (Z_n, +) es un grupo abeliano.

Hemos demostrado así , que para todo entero positivo **n** siempre existe un grupo con **n** elementos.

1.6. Homomorfismos de grupos

A continuación daremos la definición de homomorfismo, que es una aplicación que preserva las operaciones de los grupos entre los que esta definida y estudiaremos algunas de sus propiedades

Definición. Sean (G,*) y (H, o) dos grupos: Un homomorfismo de G en H es una función f: G → H tal que para todo a, b∈G se tiene

f (a*b) = f (a) o f (b).

Un monomorfismo de G en H es un homomorfismo inyectino de G en H.

Un epimorfismo de G sobre H es un homomorfismo sobreyectivo de G sobre H.

Un isomorfismo entre G y H es un homomorfismo biyectivo entre G y H.

En este ultimo caso se dice que G es isomorfo a H y se escribe G ≈H.

Además los isomorfismos de un grupo sobre si mismo reciben el nombre de automorfismos.

Ejemplos.

1. La función f definida por $f(x) = e^x$ es un isomorfismo de $(R, +)$ en $(R^+, \cdot)$, ya que es claro que f es un homomorfismo biyectivo (su inversa es ln, la función logaritmo natural)
2. Si definimos $f_a : G \to G$, mediante $f_a(x) = axa^{-1}$ para un elemento fijo **a** de G y para todo **x** de G, donde G es un grupo, entonces f_a es un automorfismo de G y es llamado la conjugación por **a**

1.6.1 Propiedades básicas de los homomorfismos.

i) Sea f un homomorfismo entre los grupos G y H, es decir $f : G \to H$, entonces se tiene:

a) $f(e) = e_1$, donde **e** y $\mathbf{e_1}$ son los elementos neutros de G y H respectivamente.

b) Para todo elemento **a** de G se tiene $f(a^{-1}) = [f(a)]^{-1}$

c) Para todo **a** de G y para todo $n \in Z$, tenemos: $f(a^n) = [f(a)]^n$

ii) Si $f : G \to H$ y $g : H \to K$ son homomorfismos de grupos, entonces $g \circ f : G \to K$ es un homomorfismo de G en K.

iii) Si $f : G \to H$ es un isomorfismo de grupos, entonces $f^{-1} : H \to G$ también es un isomorfismo de grupos.

iv) Si $\hat{G}$ es una colección no vacía de grupos , entonces la relación "es isomorfo a" es una relación de equivalencia en $\hat{G}$ esto es, para cualesquiera G, H y K $\in \hat{G}$, se tiene:

a) $G \approx G$. (La identidad $i : G \to G$ es un isomorfismo).

b) $G \approx H$ implica que $H \approx G$. (Por la propiedad (iii) anterior.).

c) $G \approx H$ y $H \approx G$ implican $G \approx K$.

v) Un grupo G es abeliano si y solamente si la función $f : G \to G$ definida por $f(x) = x^{-1}$ es un homomorfismo.

1.7. Subgrupos.

Pasamos a analizar algunas preguntas interesantes referidas a la estructura de grupos , en cuanto si esta se conserva o no en subconjuntos arbitrarios de ellos, y al hecho de cómo usar estructuras conocidas para construir nuevas estructuras. Estos conjuntos especiales de los grupos que pasaremos a estudiar se llaman subgrupos.

Definición. Dado un grupo G y un subconjunto S de G diremos que S es un subgrupo de G, y escribimos $S \leq G$, si S es un grupo bajo la operación binaria de G .

Ejemplos.

1. Sabemos que Z, Q, R, C son grupos aditivos, entonces se deduce directamente que cada uno de los tres primeros es un subgrupo del siguiente.

2. También se tiene que el grupo multiplicativo Q^+ no es isomorfo a un subgrupo del grupo aditivo R.

3. Los subconjuntos {e, a}, {e, b} y {e, c} son subgrupos del 4- grupo de Klein

4. Un subconjunto no vacío S de G es un subgrupo de G si y solamente si la inclusión $i : S \to G$ es un homomorfismo.

   En efecto, si S es un subgrupo de G, entonces S es un grupo bajo la operación binaria $*$ de G y para cualesquiera a, b $\in$ S se tiene $i(a*b) = a*b$, esto es, $i: S \to G$ es un homomorfismo. Recíprocamente, si **i** es un homomorfismo, entonces la operación binaria $\bullet$ de S debe coincidir con la operación binaria $*$, puesto que $a \bullet b = i(a \bullet b) = a*b$ para cualesquiera a, b $\in$ S, y por lo tanto S es un grupo bajo la operación binaria de G, es decir S es un subgrupo de G.

   De esto se sigue que si $S \leq G$, entonces los neutros de S y G son el mismo elemento, y el inverso de a $\in$ S es el inverso de **a** en G.

5. Si $\{ A_i \}$, donde i = 1,2,.....,n; es una colección de subgrupos de G, su intersección $A = \cap_{i=1,n} A_i$ es también un subgrupo de G

Definición. Todo grupo G posee al menos dos subgrupos: el subgrupo cuyo único elemento es el neutro de G y el subgrupo formado por todos los elementos de G. Estos subgrupos reciben el nombre de **subgrupos**

impropios (o **triviales**) de G. Al resto de los subgrupos se les denomina subgrupos propios de G.

Comentario. Debemos tener en cuenta que en grupos infinitos, los subconjuntos infinitos cerrados para una operación, no necesariamente son subgrupos. Basta analizar el conjunto de los números naturales con la suma usual, el cual no es un subgrupo del grupo aditivo Z. Esto nos obliga a tener ciertas pautas para determinar si un subconjunto es o no grupo.

1.7.1. Criterios para determinar si un subconjunto es un subgrupo.

Existen caracterizaciones que nos facilitan el estudio de los subgrupos y que están expresadas en las siguientes propiedades:

1.7.2. Propiedades básicas.

i) S es un subgrupo de G si y solo si.

(a) $e \in S$

(b) Para todo $a \in S$, se tiene $a^{-1} \in S$.

(c) Para todo a, b $\in$ S, se tiene $ab \in S$.

ii) Sea $S \subset G$ y $S \neq \phi$, tenemos . $S \leq G$ si y solo si para todo $a,b \in S$, $ab^{-1} \in S$.

iii) Sea (Z, +) el grupo aditivo de los números enteros. Entonces S es un subgrupo de Z si y solo si existe $n \in N \cup \{0\}$ tal que $S = nZ$, donde $nZ = \{ nz / z \in Z \}$

Ejemplo.

Si consideramos (Z ,+) el grupo de los números enteros,

¿ cualquier subconjunto será subgrupo?.

Solución

La respuesta es no, ¿ de que forma serán sus subgrupos?.

Después de analizar concluimos que los únicos subgrupos de

(Z , +) son de la forma S = nZ, donde nZ = {nz / z∈Z}, siendo

n ∈N ∪ {0}. Esto viene garantizado por la propiedad anterior.

A continuación presentaremos otra forma de obtener subgrupos de un grupo, para lo cual daremos previamente la siguiente definición.

Definición. Dado un subconjunto S de un grupo G, se define el **subgrupo generado** por S, y se simboliza por [S], como el menor de los subgrupos de G que contienen a S

1.7.3. Generación de grupos. La definición anterior trae consigo dos dificultades, no sabemos si el subgrupo generado por el subconjunto existirá siempre, ni si hay alguna manera sencilla de obtenerlo.

Ejemplo.

Dados subgrupos de un grupo, ¿ es posible usarlos para construir otros subgrupos?, ¿ cómo hacerlo?

Si por ejemplo, en (Z, +) tomamos los subgrupos H = 2Z y

K = 5Z, una forma natural de operar seria a través de la unión y de la intersección, es decir:

$H \cup K = \{x \in Z / x \in 2Z \text{ o } x \in 5Z\}$

$H \cap K = \{ x \in Z / x \in 2Z \text{ y } x \in 5Z\}$.

Luego $H \cup K = \{ x \in Z / x = 2m \text{ o } x = 5n ; m, n \in Z \}$,

$H \cap K = \{x \in Z / x = 2m \text{ y } x = 5n ; m, n \in Z\}$

Analizando tenemos que $H \cup K$ no es subgrupo de (Z, +), mientras que $H \cap K$ si es subgrupo de (Z, +), basta tener presente que $H \cap K = 10Z$.

Lo anterior motiva las siguientes propiedades:

1.7.4. Propiedades básicas

i) La intersección de cualquier familia de subgrupos de G es un subgrupo de G

ii) Dado un grupo G y un subconjunto arbitrario S de G, entonces el subgrupo de G generado por S, denotado por [S] ,esta dado por la intersección de todos los subgrupos de G que contienen a S

Este grupo esta caracterizado por ser el menor de los subgrupos de G que contienen a S

Demostración.

Debemos demostrar que $[S] = \cap A$, donde $A \leq G$ y $S \subseteq A$

Por la propiedad (i) anterior, tenemos que $\cap A = B$ es un subgrupo de G ; motivo por el cual debemos probar que $[S] = B$.

Como B es un subgrupo que contiene a S, se tiene que $[S] \subset B$. Por otro lado, si A es un subgrupo que contiene a S, de la definición de B se deduce que $B \subset A$, por tanto, $B \subset [S]$, y B es el menor de los subgrupos de G que contienen a S.

Luego $[S] = B$

Ejemplo.

Como $\{e\}$ es un subgrupo de G y es el menor que contiene al conjunto vacío, entonces $[\phi] = \{e\}$.

iii) Si G es un grupo y S es un subconjunto no vacío de G , $S \neq \phi$, se tiene que $\{ x_1^{n_1} x_2^{n_2} \ldots\ldots x_r^{n_r} / r \in N, x_i \in S, n_i \in Z\}$, $(x^o = e)$ donde $i = 1.2\ldots\ldots,r\ \}$ es un subgrupo de G y es el menor subgrupo de G que contiene a S , entonces:

$[S] = \{ x_1^{n_1} x_2^{n_2} \ldots\ldots x_r^{n_r} / r \in N, x_i \in S, n_i \in Z\}$,

donde $i = 1.2\ldots\ldots,r\ \}$ En particular, si S es finito, digamos que $S = \{ x_1 ,x_2 ,\ldots\ldots,x_r\}$, entonces [S] es denotado por $[x_1 ,x_2 ,\ldots\ldots,x_r]$. Por ejemplo , si S es unitario y $S = \{x\}$, entonces $[S] = [\{x\}] = \{ x^n / n \in Z \}$, representa el subgrupo generado por el elemento x del grupo G.

Ejemplo.

Tratemos de encontrar todos los generadores de (Z_8 , +).

Solución

El subgrupo generado por $\bar{1}$, es $[\bar{1}] = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7} \}$.

El subgrupo generado por $\bar{3}$, es $[\bar{3}] = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7} \}$

El subgrupo generado por $\bar{5}$, es $[\bar{5}] = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\}$.

El subgrupo generado por $\bar{7}$, es $[\bar{7}] = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\}$

Podemos concluir que $[\bar{1}] = [\bar{3}] = [\bar{5}] = [\bar{7}] = Z_8$,siendo los únicos subgrupos que generan el grupo aditivo Z_8.

iv) Si H y K son subgrupos de G, entonces el subgrupo $[H \cup K]$ es simbolizado por H v K

1.8. Orden de un elemento.

Recordemos que el orden de un grupo finito G , denotado, por IGI , se ha definido como el cardinal de G. A continuación definiremos el orden de un elemento de un grupo.

Definición. Dado un grupo G y un elemento **a** de G, definimos el orden del elemento **a** como el número de elementos que posee el subgrupo generado por **a**; si este es finito. En caso contrario, se dice que el orden de **a** es infinito.

El orden de **a** se simboliza por o(a).

1.8.1 Propiedades básicas.

i) Si el orden de **a** es finito, entonces: $o(a) = \min\{k \in Z \ / \ a^k = e\}$.

Ejemplo.

Para el grupo $(Z_8, +)$ desarrollado anteriormente, tenemos que.

Orden (0) =1, orden (1) = 8, o(2) = 4, o(3)= 8 , o(4) = 2, o(5) = 8, o(6) = 4, o(7) = 8.

ii) Se cumple que $o(a) = o(a^{-1})$, para todo elemento **a** de G.

iii) Si $m \in Z$ y $a^m = e$, entonces el orden de **a** es finito y es un divisor del número **m.**

iv) Si **a** y **b** conmutan y tienen ordenes **m** y **n** respectivamente, con **m** y **n** coprimos, entonces se tiene que o(ab) = mn.

v) Sea f un homomorfismo de G en H. Si el elemento **a** de G tiene orden finito, entonces se tiene que el elemento f(a) de H también es de orden finito, siendo este un divisor del orden de **a** .

1.9. Grupos cíclicos.

Definición. Un grupo G se dice cíclico si existe al menos un elemento **a** de G tal que el subgrupo generado por **a** es G , es decir, [a] = G.

(**a** es un generador de G.).

Ejemplos.

1. El conjunto Z con la adición es un grupo cíclico. Los únicos generadores de Z son 1 y –1.

2. Sabemos que (Z_n, +) es un grupo , aún mas es un grupo cíclico . El conjunto de todos los generadores del grupo Z_n, esta dado por: { $\bar{k} \in Z_n$, / k y n son coprimos }. Así para el ejemplo anterior, tenemos que $Z_8 = [1] = [3] = [5] = [7]$

3. El conjunto $U^{(n)} = \{ z \in C - \{0\} / z^n = 1 \}$, donde **n** es un entero positivo fijo, junto con la multiplicación forma un grupo cíclico, un generador de este grupo es $\cos(2\pi/n) + i \operatorname{sen}(2\pi/n)$.

1.9.1. Propiedades básicas .

i) El único grupo cíclico infinito, salvo isomorfismo, es Z

ii) El único grupo cíclico finito de orden **n**, salvo isomorfismo, es Z_n

iii) Todo grupo cíclico es abeliano.

iv) Un grupo finito de orden **n** es cíclico si y solamente si tiene algún elemento de orden **n**.

Comentario. De la definición de orden de un elemento y de esta propiedad se deduce que el orden del elemento **a** es igual al orden de [a] . Además se deduce que $a^{o(a)} = e$

v) Si G es un grupo finito de orden un número primo, entonces G = [a] para todo elemento **a** de G , donde $a \neq e$ y por lo tanto G es un grupo cíclico.

vi) Si G es un grupo cíclico, entonces todo subgrupo de G es cíclico.

Ejemplos.

1. Todos los subgrupos de (Z_8, +) son cíclicos, para esto hagamos la lista de los subgrupos que generan cada uno de los elementos de este grupo:

   $[1] = Z_8$, $[\bar{2}] = \{ 0, \bar{2}, 4, 6 \}$, $[3] = Z_8$

   $[4] = \{ 0, 4 \}$, $[5] = Z_8$, , $[6] = \{0, 2, 4, 6 \}$, $[7] = Z_8$,

2. Estudiaremos el grupo de los cuaterniones

   Q = { 1,- 1, i , -i , j , -j , k , -k } donde se tiene que

   $i^2 = j^2 = k^2 = -1$, ij = k, jk = i, ki = j, ji =-k, kj =-i, ik =-j.

   La tabla correspondiente es:

·	1	i	j	k	-1	-i	-j	-k
1	1	i	j	k	-1	-i	-j	-k
i	i	-1	k	-j	-i	1	-k	j
j	j	-k	-1	i	-j	k	1	-i
k	k	j	-i	-1	-k	-j	i	1
-1	-1	-i	-j	-k	1	i	j	k
-i	-i	1	-k	j	i	-1	k	-j
-j	-j	k	1	-i	j	-k	-1	j
-k	-k	-j	i	1	k	j	-i	1

Observamos que Q es un grupo no abeliano de orden ocho, cuyos subgrupos propios son:

$S_1 = [-1] = \{1, -1\}$, $S_2 = [i] = \{1, -1, i, -i\} = [-i]$,

$S_3 = [j] = \{1, -1, j, -j\} = [-j]$ y

$S_4 = [k] = \{1, -1, k, -k\} = [-k]$.

Observamos que S_1, S_2, S_3 y S_4 son cíclicos, sin embargo Q no es cíclico , por que no tiene elementos de orden 8

Comentario. El hecho de que estos son los únicos subgrupos propios de Q se justificara mas adelante.

Cuando el orden del grupo cíclico es finito se puede hallar el orden de cada uno de sus elementos a partir del orden del grupo y, el número de subgrupos del grupo coincide con el número de divisores positivos del orden del grupo. Esto lo enunciaremos a continuación :

vii) Sea G un grupo de orden **n** y sea **a** un elemento de G, entonces el orden de a^k esta dado por $n / (n, k)$. En particular, si **k** es un divisor de **n**, a^k tiene orden n / k .

viii) Si G es un grupo cíclico de orden **n** y **k** es un entero positivo que divide a **n**, entonces existe un único subgrupo de G de orden **k**. Además podemos decir que el conjunto de todos los subgrupos de G esta en correspondencia biyectiva con todos los divisores positivos de **n.**

ix) Sea f un homomorfismo que va de G a H , y G un grupo cíclico generado por **a**, esto es, G = [a] , entonces f(G) = [f(a)]; es decir, toda imagen homomorfa de un grupo cíclico es un grupo cíclico.

1.10. Multiplicación de subconjuntos no vacíos.

A continuación definimos la multiplicación de subconjuntos lo cual será usado en la construcción de clases laterales, asimismo daremos algunas de sus propiedades básicas.

Definición. Sea G un grupo arbitrario dado. Para subconjuntos arbitrarios no vacíos S y T de G definimos la multiplicación de S y T de la siguiente manera $ST = \{st / s \in S, t \in T\}$.

Para cualquier $r \in G$, denotaremos $\{r\}S$ como rS, así también

$S\{r\} = Sr$

1.10.1. Propiedades básicas.

i) La multiplicación de subconjuntos no vacíos de un grupo G es asociativa. El elemento neutro es {e}, así tenemos
Se = S = eS para todo subconjunto no vacío S de G.

ii) Si S es un subgrupo de G, entonces SS = S.

iii) Si S es un subconjunto no vacío finito de G y SS = S (S es cerrado bajo la operación binaria de G), entonces S es un subgrupo de G.

iv) Dados los subgrupos S y T de un grupo G , se tiene: Si ST = TS, entonces ST es un subgrupo de G.

v) Si G es un grupo abeliano y S, T son subgrupos de G, entonces ST es subgrupo de G.

vi) La función $f : S \to St$ definida por f (s) = st es una biyección.

1.11. **Clases laterales de un subgrupo**.

Definición. Sea S un subgrupo de G. Una clase lateral derecha de S en G es un subconjunto de la forma St, donde $t \in G$. Una clase lateral izquierda de S en G es un subconjunto de G de la forma tS, donde $t \in G$.

El elemento **t** es llamado el representante de St (o de tS).

Ejemplo

Si en (Z ; +) tomamos S = 5Z, con la notación aditiva, tenemos:

Si t = 0, S +0 = 5Z+0 = 5Z = $\bar{0}$

Si t = 1, S+1 = 5Z+1 = {5z+1} = $\bar{1}$

Si t = 2, S+2 = 5Z+2 = {5z+2} = $\bar{2}$

Si t = 3, S+3 = 5Z+3 = {5z+3} = $\bar{3}$

Si t = 4, S+4 = 5Z+4 = {5z+4} = $\bar{4}$

1.11.1. Propiedades básicas.

i) Para cualquier subgrupo S de G, tenemos: Sa = Sb si y solo si $ab^{-1} \in S$.

Lo anterior nos indica que los elementos **a, b** de G están relacionados mediante S, y lo simbolizaremos por

$a \equiv b \pmod{S}$

Comentario. La relación anterior es una relación de

equivalencia y la clase de equivalencia de un elemento **a** de G en esta relación coincide con Sa .

ii) Si S es un subgrupo de G, entonces cualesquiera dos clases laterales derechas de S en G son idénticas o disjuntas.

iii) Para cualquier subgrupo S de G, denotamos R(S) ={St/ t∈G} y L(S) ={ tS / t∈G }. La función f : R(S)→ L(S), definida por f (Sa) = a^{-1}S es una biyección.

iv) Para cualquier subgrupo S del grupo finito G, tenemos que el número de elementos de St es igual al número de elementos de S, donde t ∈ G.

Ejemplo. Sea G = S_3 = { i , p_1, p_2, p_3, p_4, p_5 }, el grupo de las permutaciones de tres elementos, donde se tiene:

$$i = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\ p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},\ p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},\ p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix};$$

Considerando el subgrupo S = {i ,p_4 , p_5 } construiremos todas las clases laterales de G según S.

Observamos que las dos clases son Si = {i ,p_4 , p_5}= S y Sp_1 = {p_1, p_2, p_3} que tienen el mismo número de elementos e igual al número de elementos de S . Además el conjunto

formado por todas las clases de equivalencia según S es una partición de G. Esto viene garantizado por la siguiente propiedad.

v) Si S es un subgrupo de G y a, b∈ G, entonces Sa y Sb tienen el mismo número de elementos. (es decir, existe una correspondencia biunívoca entre los elementos de Sa y de Sb).

Comentario. Como Se = {se / s∈S}, entonces se tiene que toda clase de equivalencia en G según S tiene el mismo número de elementos de S.

1.12. Teorema de Lagrange.

Antes de proceder a enunciar el teorema de Lagrange, daremos la siguiente definición previa.

Definición. Sea S un subgrupo de G. El **índice del subgrupo** S en G, denotado por [G : S], es $|R(S)|$, el cardinal del conjunto de todas las clases laterales derechas de S en G.

1.12.1. Propiedades básicas..

i) Teorema de Lagrange. Sea G un grupo finito y S un subgrupo de G, entonces [G: S] = | G| / | S|

Demostración.

Como la relación ≡ determina una partición del grupo G , entonces cada elemento de G pertenece a una y solo una clase de equivalencia según S. Además como el grupo G es

finito, el número de clases será finito, sea este número **m**. Como cada clase posee la misma cardinalidad, y, la clase Se, coincide con el subgrupo S , entonces cada clase tendrá o(S) elementos. Luego tenemos que el orden del grupo puede expresarse como o(G) =m.o(S) de donde

m = | G| / | S| = [G: S].

Comentarios.

1) Una consecuencia inmediata del teorema es que si G es un grupo finito de orden primo, entonces sus únicos subgrupos son G mismo y {e}. Esto será analizado mas adelante.
2) Tenemos que [G: S] y | S| dividen al orden de G. Además el orden del elemento **a** divide al orden del grupo G, para todo elemento **a** de G.

ii) Si G es un grupo finito y S y T son subgrupos de G tales que T⊂S, entonces se tiene: [G:T] = [G : S][S : T].

iii) Si S y T son subgrupos de un grupo finito G, entonces se tiene | S|| T| ≤ | S∩T|| SvT|

1.13.Conjunto cociente

La importancia del estudio de una relación de equivalencia, definida en un conjunto G, radica en el hecho de que constituye una abstracción de los procesos de clasificación, ya que las clases de equivalencia que determina

forman una partición del conjunto G. Según esto tenemos la siguiente definición.

Definición. Las clases de equivalencia en que el conjunto G queda clasificado mediante la relación R se denomina conjunto cociente, y se simboliza por G / R.

Ejemplo.

En Z definimos la relación de equivalencia R mediante: a, b$\in$ R si y solo si a-b es un número par.

Solución.

De modo directo se tiene que R es una relación de equivalencia, siendo sus clases $\overline{0}$ y $\overline{1}$

Así podemos decir que Z / R = $\{\overline{0},\overline{1}\}$, $\overline{0}\cap\overline{1}=\phi$ Es decir la relación R clasifica el conjunto Z en números pares e impares.

Comentario. Si S es un subgrupo del grupo G, podemos considerar el conjunto cociente G /$\equiv_S$, donde en G se ha definido la relación de equivalencia modulo S, es decir, a $\equiv$ b (mod.S) si y solo si a $b^{-1} \in$ S.

Es natural preguntarnos si al conjunto G /$\equiv_S$ se le puede dotar de una estructura de grupo. Esto no siempre es posible, pero ocurre para algunos subgrupos distinguidos de G, los cuales recibirán el nombre de normales.

1.13.1. Subgrupos normales.

Definición. Un subgrupo S de un grupo G es llamado un subgrupo normal de G si para todo $a \in G$ se tiene que $aSa^{-1} \subset S$. Se simboliza por $S \lhd G$.

1.13.2. Propiedades básicas.

i) Si S es un subgrupo del grupo G, las siguientes propiedades son equivalentes:

   a) S es un subgrupo normal de G

   b) Para todo $a \in G$ se tiene $aSa^{-1} = S$.

   c) Para todo $a \in G$ se tiene $aS = Sa$.

   d) Toda clase lateral derecha de S en G, es también una clase lateral izquierda de S en G.

ii) Todo subgrupo de un grupo abeliano es un subgrupo normal.

iii) Si S es un subgrupo normal de G , **a** un elemento de G y **s** un elemento de S, entonces existe un elemento $\mathbf{s_1}$ de S tal que $as = s_1a$.

iv) Cualquier subgrupo S de G de índice 2, es normal.

Ejemplos.

1 Si S es el único subgrupo de G de orden $|S|$, entonces S es un subgrupo normal de G

Demostración

En efecto, $aSa^{-1} = f_a (S)$, donde f_a es la conjugación por **a**,

para todo elemento **a** de G, y por lo tanto $|aSa^{-1}| = |S|$

Luego $aSa^{-1} = S$ para todo elemento **a** de G, puesto que S es el único subgrupo de G de orden $|S|$. Así decimos que S es un subgrupo normal de G.

2 Si S es un subgrupo del grupo G entonces : S es un subgrupo normal de G si y solo si SaSb = Sab para cualesquiera $a, b \in G$.

Demostración.

Si S es un subgrupo normal de G, para todo a G se tiene Sa = aS. Considerando otra clase a la derecha Sb, tenemos: SaSb = S(aS)b = S(Sa)b = SSab = Sab. (ya que SS=S).

Concluimos que SaSb = Sab

Ahora partimos de la igualdad SaSb = Sab para cualesquiera $a, b \in G$, entonces para cualquier elemento **a** de G se tiene: $SaSa^{-1} = Saa^{-1} = Se = S$, de donde $aSa^{-1} = e(aSa^{-1}) \subset SaSa^{-1} = S$, es decir $aSa^{-1} \subset S$, por lo tanto S es normal en G.

3. El grupo multiplicativo Q = { 1, -1, i, -i , j, -j, k, -k } de los cuaterniones, no es abeliano, sin embargo todos sus subgrupos son normales.

Solución.

En efecto, todos los subgrupos propios de Q son cíclicos (como el único elemento de orden 2 es –1, mientras que los

elementos i, -i, j, -j k, -k son de orden 4; entonces existe un único subgrupo de orden dos y cualquier subgrupo de orden cuatro , necesariamente contiene por lo menos un elemento de orden cuatro). Estos subgrupos son:

[1] = {1}, [-1] = {1, -1 }, [i] = [-i] = {1, -1, i, -i },

[j] = [-j] ={1, -1, j, -j } y [k] = [-k] que se obtiene similarmente

Es claro que {1} y Q son subgrupos normales de Q. Además como a{1, -1}a = {1, -1} para cualquier elemento a de Q, entonces se tiene que el grupo {1, -1} es normal.

Por ultimo, [i] =[-i], [j] = [-j] y [k]= [-k] son subgrupos normales de Q, ya que son de índice 2. Con esto queda probada la afirmación.

Comentarios.

1 La propiedad del índice 2 nos sirve de criterio para identificar grupos normales, tal como se ha aplicado en el ejemplo 3.

2 El ejemplo 2 muestra que la condición de normalidad dada es equivalente a la siguiente:

Un subgrupo S de un grupo G se dice normal si y solo si SaSb = Sab para todo a, b$\in$ G.

1.13.3. Grupo cociente

Definición. Si S es un subgrupo normal de G , entonces G / S se llama el grupo cociente de G por S. La operación binaria en G / S es la multiplicación de subconjuntos de G definida anteriormente. En este caso debido a la normalidad de S, resulta .

SaSb = S(aS)b = S(Sa)b = (SS)ab = Sab

Comentario. Si G es un grupo finito y S es un subgrupo normal de G, de la definición de índice tenemos que

o(G / S) = [G : S] = o(G)/o(S).

1.14. Centro de un grupo.

Definición. El centro de un grupo G, denotado por Z(G), es el conjunto de los elementos de G que conmutan con todos los elementos de G, es decir:

Z(G) = {a∈G / ax = xa para todo elemento x de G}.

1.14.1. Propiedades básicas.

i) El centro de cualquier grupo abeliano G es el mismo grupo abeliano G.

ii) El centro del grupo G es un subgrupo abeliano de G.

iii) El centro del grupo G es un subgrupo normal del grupo G

iv) Si G / Z(G) es cíclico, entonces G es abeliano.

1.15. Centralizador de un elemento.

Definición. Sea G un grupo y **a** un elemento fijo de G. El centralizador de **a** en G, denotado por C_G (a), es el conjunto

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

Si no hay lugar a confusión, entonces $C_G(a)$ es simbolizado por C(a).

1.15.1 Propiedades básicas

i) El centralizador de **a** es un subgrupo de G, para todo $a \in G$

ii) Para cualquier $a \in G$ se cumple: C(a) = G si y solo si $a \in Z(G)$.

iii) $Z(G) = \cap [C(a) / a \in G\}$

1.16. Conjugado de un elemento.

Definición. Sea G un grupo y sean **a** y **b** elementos de G. Se dice que **b** es un **conjugado** de **a** en G si existe un elemento **x** de G tal que

$b = xax^{-1}$

Definición. Las clases de equivalencia determinadas en un grupo por la relación " es un conjugado" son llamadas clases de conjugación. La clase de conjugación del elemento a de G se denotara por Cnjg(a).

1.16.1. Propiedades básicas

i) Si **b** es un conjugado de **a**, entonces o(a) = o(b)

ii) o(ab) = o(ba) para elementos cualesquiera a, b de G.

iii) $|Cnjg(a)| = [G: C(a)]$ para todo elemento **a** de G, donde $|Cnjg(a)|$ es el cardinal de la clase de conjugación de **a**.

iv) Si G es un grupo finito, entonces el número de conjugados de cualquier elemento **a** de G es un divisor de IGI.

v) Para cualquier elemento **a** de G se verifica:

Cnjg(a) = {a} si y solo si **a** es un elemento del centro de G.

Comentario. En un grupo abeliano G las clases de conjugación no son de interés (en este caso Z(G) = G).

1.17. Ecuación de clases.

Comentarios.

1 Si G es un grupo finito no abeliano, entonces $Z(G) \neq G$ y por lo tanto G contiene elementos no centrales

2 También sabemos que la clase de conjugación de un elemento **a** de G es unitaria si y solo si **a** es un elemento central, es decir $a \in Z(G)$.

3 Sean $k_1, k_2, \ldots\ldots, k_m$ todas las clases de conjugación no unitarias ($k_1, k_2, \ldots, k_m$ distintas entre si) y sea R un conjunto completo de representantes de estas clases de conjugación. Entonces R tiene elementos no centrales y no conjugados.

Definición. Según lo anterior como las distintas clases de conjugación forman una partición de G, entonces contando elementos se obtiene la formula: $|G| = |Z(G)| + [G : C(x)]$, la cual es llamada la **ecuación de clases de G**.

1.18. Los teoremas de isomorfismo.

Existen tres teoremas que describen la relación entre grupos cocientes, subgrupos normales y homomorfismos. Para esto daremos una definición previa

Definición. Dado un homomorfismo entre los grupos G y H, f : G→ H, definimos el **núcleo** de f mediante, N (f) = {x ∈ G / f (x) = e }, donde **e** es el elemento neutro de H.

Otras notaciones para representar el núcleo de f, son

N(f) = Nu (f)= Ker (f)

1.18.1. El primer teorema de isomorfismo. Dado un homomorfismo entre los grupos G y H, f : G→ H ,con núcleo K. Entonces se tiene que K es un subgrupo normal en G y que G /K es isomorfo a f (G).

1.18.1.1. Propiedades básicas.

i) Si f: G→ H es un homomorfismo con núcleo K, entonces existe un homomorfismo g : G /K→ H tal que f = gπ, donde π : G→ G / K esta definida por π(x) = Kx.

ii) Sea N un subgrupo normal de G y sea f : G→ H un homomorfismo cuyo núcleo contiene a N. Entonces $\bar{f}$ induce un homomorfismo $\bar{f}$: G / N → H , nominalmente, $\bar{f}$ (Na) = f (a) .

iii) Sea f : G→ H un homomorfismo. Entonces f es inyectivo si y solamente si N(f) = {e}

iv) Sea $f: G \rightarrow H$ un homomorfismo. Si T es un subgrupo de H, entonces $f^{-1}(T)$ es un subgrupo de G que contiene al núcleo de f.

v) Si K es un subgrupo normal de G, entonces existe un grupo H (nominalmente, G / K) y un homomorfismo sobreyectivo π de G sobre H cuyo núcleo es exactamente K, definido por $\pi : G \rightarrow G / K$, donde a **a** le corresponde Ka.

vi) Si S y T son subgrupos de G y uno de ellos es normal, entonces $ST = S \vee T = TS$.

Definición. La función $\pi : G \rightarrow G / K$ es llamado el **homomorfismo natural o canónico**.

Comentario. Con el primer teorema de isomorfismo y con la propiedad (v) hemos exhibido la relación entre subgrupos normales y homomorfismos: Dado cualquier homomorfismo, existe un subgrupo normal (su núcleo); dado cualquier subgrupo normal K, existe un homomorfismo (el homomorfismo natural) cuyo núcleo es K.

1.18.2. El segundo teorema de isomorfismo. Sean S y T subgrupos de G. Si T es un subgrupo normal en G, entonces $S \cap T$ es un subgrupo normal de S, y $S / (S \cap T)$ es isomorfo a ST/ T

Demostración.

Para la demostración de este teorema, se considera el

homomorfismo natural π:G$\rightarrow$G/T. La restricción de π a S es un homomorfismo π_o cuyo núcleo es ST y cuya imagen es ST / T. La conclusión se obtiene aplicando el primer teorema de isomorfismo.

1.18.2.1. Propiedad básica. Si uno de los subgrupos S y T es normal, entonces se tiene:

$$|S||T| = |S \cap T||S \vee T| = |S \cap T||ST|$$

1.18.3. El tercer teorema de isomorfismo. Si H y K son subgrupos normales de G tales que $K \subset H \subset G$, entonces H / K es un subgrupo normal de G / K, y (G / K) / (H / K) es isomorfo a (G / H).

Demostración.

Definimos f : G / K$\rightarrow$ G / H por medio de f (Ka) = Ha. Se verifica que f esta bien definida, f es un homomorfismo cuyo núcleo es H / K y cuya imagen es G / H.

De acuerdo con el primer teorema de isomorfismo, se obtiene el resultado deseado.

1.18.4. El teorema de correspondencia. Este teorema podría ser llamado, justificadamente, el cuarto teorema de isomorfismo. Antes de proponerlo efectuamos un comentario.

Comentario. Sean G y H conjuntos no vacíos y f : G$\rightarrow$H una función. Esta función induce un “movimiento hacia adelante” y un “ movimiento hacia atrás” entre los subconjuntos de G y los subconjuntos de H. El “ movimiento hacia adelante”asigna a todo

subconjunto S de G su imagen f(S) en H. Mientras que el "movimiento hacia atrás"asigna a todo subconjunto L de H su imagen inversa $f^{-1}(L)$ en G

Si f es sobreyectiva, entonces estos "movimientos" definen una correspondencia biunívoca entre los subconjuntos de H y algunos de los subconjuntos de G. El siguiente teorema es una traslación grupo-teórica de este comentario.

Teorema de correspondencia. Si K es un subgrupo normal de G, entonces el homomorfismo natural $\pi : G \rightarrow G / K$ define una correspondencia biunívoca entre el conjunto de todos los subgrupos de G que contienen a K y el conjunto de todos los subgrupos de G / K

Si el subgrupo de G / K correspondiente a $S \subseteq G$ es denotado por S^* entonces se tiene:

a) $S^* = S / K = \pi(S)$; en particular, $K^* = K / K$ es la identidad de G / K

b) $T \subseteq S$ si y solo si $T^* \subseteq S^*$, y por lo tanto $[S : T] = [S^* : T^*]$

b) T es un subgrupo normal de S si y solo si T^* es un subgrupo normal de S^*, por lo tanto S /T es isomorfo a S^* / T^* .

1.18.4.1. Propiedades básicas.

i) Sea G un grupo finito. Si H es un subgrupo normal de G tal que H y [G : H] son coprimos, entonces H es el único subgrupo de G de orden IHI

ii) H es un subgrupo normal maximal si y solo si G / H no tiene subgrupos normales propios.

1.19 El grupo simétrico.

Definición. Dado un conjunto no vacío X, denotamos por S_X al **conjunto de todas las biyecciones** del conjunto X en si mismo.

Si f y g son dos funciones biyectivas del conjunto X en si mismo, se comprueba fácilmente que fog es también una función biyectiva de X en si mismo y que f es también una función biyectiva, demostrándose que (S_X :o) es un grupo.

Definición. Cuando el conjunto X es el conjunto de los **n** primeros números naturales, los elementos de S_X se denominan **permutaciones** de **n** elementos.

Definición. El conjunto de las permutaciones de **n** elementos se simboliza por S_n y el grupo (S_n ;o) se llama **grupo simétrico** de **n** elementos. (es el grupo de todas las permutaciones de **n** elementos y tiene orden n!).

Comentario. Si tenemos dos conjuntos X y Y con el mismo número de elementos, entonces el grupo de todas las permutaciones de X tiene la misma estructura que el grupo de todas las permutaciones de Y

Ejemplos.

1 Un elemento **p** (permutación) de S se denota de la siguiente manera:

$$p = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ p(1) & p(2) & \dots & p(n-1) & p(n) \end{pmatrix}$$

Donde observamos que 1 es enviado en p(1), 2 en p(2), y así sucesivamente.

Comentario . Si **p** y **q** son dos elementos de S, su compuesta se escribirá como pq.

2 Sea A = {1, 2, 3}, entonces el grupo de permutaciones S tiene 3! = 6 elementos, los cuales son

$$i = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\ p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix};\ p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix};\ p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix};\ p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

La tabla respectiva es :

	i	p_1	p_2	p_3	p_4	p_5
i	i	p_1	p_2	p_3	p_4	p_5
p_1	p_1	p_2	i	p_4	p_5	p_3
p_2	p_2	i	p_1	p_5	p_3	p_4
p_3	p_3	p_5	p_4	i	p_2	p_1
p_4	p_4	p_3	p_5	p_1	i	p_2
p_5	p_5	p_4	p_3	p_2	p_1	i

Comentarios

1 Se observa que este grupo no es abeliano, siendo el grupo de menor orden entre todos los no abelianos.

2 En lo que sigue nos dedicaremos a analizar permutaciones sobre conjuntos finitos. Siendo nuestro primer objetivo simplificar la notación de las pemutaciones.

Ejemplo :Consideremos la siguiente permutación:

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 1 & 5 & 6 \end{pmatrix}$$

Observamos que p(1) = 2, p(2) = 3, p(3) = 4 y p(4) = 1. Habiendo empezado y finalizado con 1 decimos que se ha completado un ciclo. Este primer ciclo tiene la forma (1 2 3 4) y tiene 4 elementos Como 5 y 6 son dejados fijos, escribimos los ciclos (5) y (6) con un elemento cada uno Esto motiva la siguiente definición:

Definición. Un **m-ciclo**, m>1, (a_1 a_2 a_3 .....a_m) es una permutación de **m** elementos distintos de un conjunto A, que envía a_i en a_{i+1} , para i = 1, 2, ..., m-1; y a_m lo envía en a_1. Si m = 1, definimos el 1-ciclo como la **identidad.**

Comentarios.

1 Como los ciclos son en realidad permutaciones, ellos pueden multiplicarse. Sin embargo el producto de ciclos no necesariamente es un ciclo.

2 Representaremos el producto de dos ciclos escribiéndolos en posiciones adyacentes, con la aplicación derecha actuando primeramente.

3 Un 2-ciclo es llamado una **transposición.**

4 Cualquier permutación de al menos dos elementos puede ser escrita de diversas maneras como un producto de transposiciones.

5 Llamaremos **ciclos ajenos** a aquellos ciclos que no tienen elementos comunes.

6 Cualquier permutación de un conjunto finito es producto de ciclos ajenos

7 La multiplicación de ciclos ajenos es conmutativa.

Ejemplos

1 La permutación del ejemplo anterior puede escribirse como:

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 1 & 5 & 6 \end{pmatrix}$$

obtenemos p = (1 2 3 4)(5)(6) = (1 2 3 4).

Los ciclos de longitud 1 pueden omitirse.

2 El producto de los ciclos (2 1 5)(1 4 5 6) = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 3 & 2 & 6 & 5 \end{pmatrix}$ no es un ciclo, sin embargo puede ser escrita de diversas maneras, tales como:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 1 & 5 & 6 \end{pmatrix} = (2\ 1)(2\ 5)(1\ 4)(1\ 5)(1\ 6) = (1\ 4)(1\ 2)(5\ 6).$$

Nótese además que cada una de estas factorizaciones tiene un número impar de elementos.

3 En la permutación $s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix} = (1\ 2)(4\ 5)$,

Nótese que $s^2 = i$, es decir s^2 es la permutación identidad

Por otra parte si q = (1 2 3 4), fácilmente se encuentra que el orden de q es 4

Definición. Una permutación **p** puede ser escrita como un producto de **m** transposicionès, entonces cualquier otra factorizacion de **p** tendrá (m + número par) de transposiciones. Una permutación **p** de un conjunto finito es **par o impar** de acuerdo con el hecho de que pueda expresarse como un producto de un número par de transposiciones o como el producto de un número impar de transposiciones respectivamente.

Comentario. El hecho de que un producto arbitrario de permutaciones pares de cómo resultado una permutación par, nos indica que este conjunto es cerrado bajo tal operación.

Esto a su vez nos da la idea de que el conjunto de las permutaciones pares es un grupo. Para n>1 tenemos, además, que el número de permutaciones pares en S es igual al número de permutaciones impares ; lo cual viene garantizado por las siguientes propiedades.

1.19.1 Propiedades básicas.

i) El ciclo (1 2 ..n-1 n) puede escribirse como

(1 n)(1 n-1)...(1 2)

ii) Sea s = (a_1 a_2 ... . a_m) un m-ciclo de S, entonces el orden de **s** es **m**.

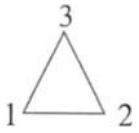
iii) Si p = p_1 p_2 ..... p_{n-1} $p_n \in S_n$, donde los ciclos $\mathbf{p_i}$ son ajenos de longitudes k_1 , k_2, ..., k_n respectivamente. Entonces el orden de p esta dado por el mcm de k_1 , k_2, .., k_n

iv) Ninguna permutación de un conjunto finito puede expresarse como un producto de un número par de transposiciones y como un producto de un número impar de transposiciones.

Definición. La colección A_n de todas las permutaciones pares de S_n es un subgrupo de S_n, con orden n! /2, donde n>1. A_n se llama **grupo alternante.**

Ejemplo

A continuación estableceremos una correspondencia natural entre los elementos de S_3 y la manera en que pueden colocarse dos copias de un triangulo equilátero, una encima de otra, de vértices 1, 2 y 3. Por esta razón S_3 es además el grupo D_3 de simetrías de un triangulo equilátero (D_3 representa también el tercer grupo diedrico). Si llamamos $\mathbf{a_i}$ las rotaciones y $\mathbf{b_i}$ a las imágenes reflejadas en las bisectrices de los triángulos, tenemos:

$a_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ 

permanece igual

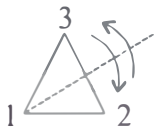
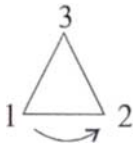
$b_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ 

imagen reflejada en bisectriz del ángulo 1

$a_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ 

rotación de 120°

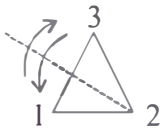
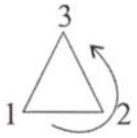
$b_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ 

imagen reflejada en bisectriz del ángulo 2

$a_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ 

rotación de 240°

$b_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ 

imagen reflejada en bisectriz del ángulo 3

Comentario. Este ejemplo trae consigo la idea de que los elementos de cualquier grupo pueden representarse por permutaciones, como veremos enseguida.

1.20 **Teorema de representación de Cayley**. Todo grupo G es isomorfo a un subgrupo del grupo simétrico S_G . En particular, todo grupo finito de orden **n** es isomorfo a un subgrupo de S_n

Demostración.

Para cada elemento **a** de G definimos $T_a : G \rightarrow G$, mediante $T_a(x) = ax$. T_a es una biyeccion llamada traslación a izquierda por **a**. Entonces $T_a \in S_G$ (el grupo simétrico sobre G) para todo elemento **a** de G. Por lo tanto la

función ϕ que asigna a cada elemento **a** de G la permutación T_a es una función de G en S_G .Mostraremos que $\phi : G \rightarrow S$ es un monomorfismo.

En efecto para elementos cualesquiera **a, b** y **x** de G se tiene:

$T_{ab}(x) = (ab)x = a(bx) = T_a(bx) = T_a(T_b(x)) = (T_a T_b)(x)$.

Luego $\phi(ab) = T_{ab} = T_a T_b = \phi(a)\,\phi(b)$ para cualesquiera **a, b** de G.

Además, si **a** es un elemento del núcleo de ϕ , entonces $T_a = \phi(a) = i$;

Luego $a = ae = T_a(e) = I(e) = e$. Por lo tanto Ker $(\phi) = \{e\}$ y, en consecuencia, es un monomorfismo.

Concluimos que $G \approx \phi(G)$, donde $\phi(G)$ es un subgrupo de S_G

1.21 **Grupo de permutaciones**

Definición. Sea X un subconjunto no vacío. Si G es un subgrupo del grupo simétrico S_X , entonces decimos que G es un **grupo de permutaciones que actúa sobre X**.

Definición. Sea G un grupo de permutaciones que actúa sobre un conjunto X y sean **x, y** elementos de X. Se dice que **x** es **G-equivalente** a **y** si existe $t \in G$ tal que $y = t(x)$.

Comentario. Se verifica inmediatamente que la relación "es G-equivalente a" es una relación de equivalencia sobre X.

Definición. Las G-clases de equivalencia de X son llamadas las **orbitas de G**. La G-orbita de x será denotada por $Orb_G(x)$ o simplemente Orb(x).

Ejemplos.

1. Por el teorema de Cayley, cualquier subgrupo H de un grupo G puede ser considerado como un grupo de permutaciones que actúa sobre G: esto se consigue identificando cada $h \in H$ con la traslación a izquierda por **h**. La orbita de $a \in G$ es $Ha = \{ ha / h \in H \}$.

   Así, pues, las orbitas de H son exactamente las clases laterales de H en G.

2 Denotemos por I(G) el conjunto de todas las conjugaciones de G. Como $(f_a) = f_a^{-1}$ (f_a es la conjugación por **a**, es decir, $f_a(x) = axa^{-1}$, $x \in G$) y $f_a f_b = f_{ab}$ para cualesquiera $a, b \in G$, entonces I(G) es un subgrupo de S, es decir, I(G) es un grupo de permutaciones que actúa sobre G. La orbita del elemento **x** de G es la conjugación de **x**, esto es, $\{axa^{-1} / a \in G\}$.

1.22 Estabilizador de un elemento.

Definición. Sea G un grupo de permutaciones que actúa sobre un sobre un conjunto X y sea **x** un elemento de X. El estabilizador de **x**, denotado por st(x), es el conjunto $st(x) = \{ t \in G / t(x) = x \}$.

1.22.1 Propiedades básicas.

i) Sea G un grupo de permutaciones que actúa sobre un conjunto X. entonces para cada elemento **x** de X, se tiene que st(x) es un subgrupo de G..

Demostración.

Es claro que id_X (la aplicación identidad sobre X) pertenece a

st(x), entonces st(x) $\neq \phi$. Si **t** y **s** son elementos arbitrarios de st(x), entonces t(x) = x y s(x) = x; luego

$ts^{-1}(x) = ts^{-1}(s(x)) = t(s^{-1}s(x)) = t(x) = x$,y por lo tanto,

$ts^{-1} \in st(x)$.

Por consiguiente st(x) es un subgrupo de G.

ii) Si G es un grupo de permutaciones que actúa sobre un conjunto finito X, entonces para cada elemento **x** de X, la cardinalidad de la orbita de **x** es igual a [G : st(x)] y por lo tanto divide a $|G|$

Demostración.

Supongamos que $t_1st(x), t_2st(x), \ldots, t_rst(x)$ son las distintas clases laterales izquierdas de st(x) en G, donde r = [G : st(x)]

Mostraremos que la orbita de **x** es $\{ t_1(x), t_2(x), \ldots\ldots, t_r(x)\}$.

En efecto, para cualquier elemento **t** de G, existe $i \in \{1, 2, \ldots, r\}$ tal que $t \in t_i st(x)$, porque $\{ t_1st(x), t_2st(x), \ldots\ldots, t_rst(x)\}$ es una partición de G. Luego $t^{-1}t_i \in st(x)$, es decir, $t^{-1}t_i(x) = x$ y por lo tanto $t(x) = t_i(x)$. Se sigue que

$\{ t(x) / t \in G\} = \{ t_1(x), t_2(x), \ldots\ldots, t_r(x)\}$.

Ahora veamos que $t_1(x), t_2(x), \ldots\ldots, t_r(x)$ son distintos.

En efecto, si $i \neq j$, entonces $t_i^{-1}t_j \notin st(x)$; luego $t_i^{-1}t_j(x) \neq x$ y por lo tanto $t_i(x) \neq t_j(x)$.

Por consiguiente la cardinalidad de {t(x) / t∈ G } (la orbita de x)

es r = [G : st(x)]

Capitulo II

La teoría de los p-grupos y los teoremas de Sylow

2.1 La teoría de los p-grupos.

2.1.1. Definición de p-grupo. Sea G un grupo y **p** un número primo.

Decimos que G es un p-grupo si para cada $x \in G$, existe

$k \in Z^+ \cup \{0\}$ tal que $o(x) = p^k$.

Comentario. Es claro, de la definición, que si G es un grupo finito y

$|G| = p^n$, para algún primo **p** y algún $n \in Z^+ \cup \{0\}$, entonces G es un

p-grupo.

2.1.2 **Teoremas fundamentales**

Teorema 2.1.1. Sea G un grupo y sea H un subgrupo normal de G. Si H y G/H son p-grupos, entonces G es un p-grupo.

Demostración.

Supongamos que H y G / H son p-grupos. Sea **x** un elemento cualquiera de G . Como G / H es un p-grupo, entonces $o(Hx) = p^k$ para algún entero no negativo k. Si denotamos $r = p^k$, se tiene:

$Hx^r = (Hx)^r = He$, con lo cual $x^r \in H$. Como H es un p-grupo, sea $o(x^r) = t = p^m$ para algún entero no negativo **m.** Entonces se tiene: $x^{rt} = (x^r)^t = e$, donde $rt = p^k p^m = p^{k+m}$. Por lo tanto, el orden de **x** es una potencia de **p**.

Se concluye que el orden de todo elemento de G es una potencia de **p**, es decir, G es un p-grupo.

Lema 2.1.1, Si G es un grupo abeliano finito cuyo orden es divisible por un primo **p**, entonces algún elemento de G es de orden **p**.

Demostración .

Sea $x \in G-\{e\}$.Tenemos dos casos:

a) Supongamos que $o(x) = pm$, para algún $m \in Z$. Entonces $(x^m)^p = e$ y por lo tanto $o(x^m)$ divide a **p**. Luego $o(x^m) = p$, es decir, x^m es un elemento de orden **p**.

b) Ahora supongamos que $o(x) = r$, donde **r** es coprimo con **p**, es decir, **r** no es divisible por **p**. Como G es abeliano, entonces [x] es un subgrupo normal de G y G / [x] es un grupo abeliano de orden $|G|/ r$. Puesto que **r** no es divisible por **p**, se tiene que $|G|/ r$ es divisible por **p** y $(|G| / r) < |G|$ Por inducción sobre $|G|$, se obtiene un elemento $y \in G / [x]$ de orden **p**. Siendo y la imagen de $\mathbf{y} \in G$ bajo el homomorfismo canónico, resulta que o(y) es divisible por **p**. Con esto, hemos vuelto al primer caso.

Teorema 2.1.2 (Cauchy) Si G es un grupo finito cuyo orden es divisible por un primo **p**, entonces algún elemento de G es de orden **p**.

Demostración.

Como G es un grupo finito y **p** divide al orden de G, tenemos los casos siguientes:

a) Si G es abeliano, entonces por el lema 2.1.1 algún elemento de G es de orden **p**, con lo cual queda probado.

b) Si G no es abeliano, entonces $G \neq Z(G)$, es decir existen en G elementos no centrales.

∗Si existe $x \notin Z(G)$ tal que **p** divide a $|C(x)|$, entonces el resultado se obtiene por inducción sobre G . Veamos:

Para $|G| = 6$ se cumple lo que afirma el teorema.

Ahora supongamos que el teorema vale para grupos de orden menor que **n**, donde $n = |G|$ y $n > 6$.

Luego por la hipótesis inductiva, en C(x), existe $a \in C(x)$ talque $o(a) = p$, y en consecuencia siendo **a** un elemento de G, se tendrá que en G existe por lo menos un elemento de orden **p**.

∗Si para todo $x \notin Z(G)$, **p** no divide a $|C(x)|$, entonces **p** divide a $[G : C(x)]$ para todo $x \notin Z(G)$, ya que **p** es primo y además $|G| = [G : C(x)]\,|C(x)|$

De la ecuación de clases $|G| = |Z(G)| + \sum [G : C(x)]$, se deduce que **p** divide a $|Z(G)|$

Por el lema 2.1.1, se concluye que algún elemento de Z(G) es de orden **p**.

Comentario. Los teoremas de Cauchy y de Lagrange nos permiten caracterizar los p-grupos de la siguiente manera:

Corolario. Un grupo finito G es un p-grupo si y solamente si $|G|$ es una potencia de **p**.

Demostración.

* Si $|G|$ es una potencia de **p**, entonces por el teorema de Lagrange, el orden de cualquier elemento de G es una potencia de **p**, es decir, G es un p-grupo.

* Si G es un p-grupo, entonces $|G|$ es una potencia de **p**, porque, en caso contrario, existirá un primo $q \neq p$ que divide a $|G|$. El teorema de Cauchy implicaría que algún elemento de G tendría orden **q**, lo cual estaría en contradicción con el hecho de que G es un p-grupo.

Comentario. Una consecuencia inmediata de este corolario y del teorema de Lagrange, es que todo subgrupo de un p-grupo finito tiene como orden una potencia de **p**.

Teorema 2.1.3. Si G es un p-grupo finito y $|G| > 1$, entonces $|Z(G)| > 1$

Demostración.

*Si G es abeliano, entonces G = Z(G) y en este caso no hay nada que demostrar.

∗Ahora supongamos que G no es abeliano. Consideremos la ecuación de clases $|G| = |Z(G)| + h_1 + h_2 + ... + h_m$, donde $h_1, h_2 ....., h_m$ son los cardinales de las distintas clases de conjugación de elementos no centrales de G. Para cada $a \in G - Z(G)$, C(a) es un subgrupo propio de G. Por un corolario anterior, |C(a)| es una potencia de **p** y por lo tanto [G : C(a)] es una potencia de **p** diferente de 1. Luego **p** divide a cada h_i. Por consiguiente **p** divide a |Z(G)|.

Corolario 1. Cualquier grupo G de orden p^2 (donde **p** es un número primo) es abeliano.

Demostración .

Supongamos que G no es abeliano, es decir, $G \neq Z(G)$. Por el teorema 2.1.3, |Z(G)| = p. Luego G / Z(G) es de orden **p** y por lo tanto cíclico, lo cual es falso. Por consiguiente G es abeliano.

Comentario. Este corolario es valido a partir de p=3, ya que para p=2, los grupos de orden 4, son abelianos por si solos

Corolario 2 . Sea G un p-grupo tal que $|G| = p^k$.

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

Demostración.

Procedemos por inducción sobre **k**.

Para k = 1, la afirmación es verdadera.

∗Supongamos que la afirmación se verifica para todo m < k, donde k >1. Por el teorema 2.1.3, Z(G) ≠ {e}, por lo tanto **p** divide a | Z(G)|. Por el lema 2.1.1, existe x ∈ Z(G) tal que o(x) = p. Sea N = [x]. Entonces N es un subgrupo normal de G, ya que todo subgrupo de Z(G) es normal en G. Luego se tiene que $|G / N| = p^{k-1}$. Entonces por la hipótesis inductiva, G / N contiene un subgrupo normal H* de orden n-1 (la afirmación es verdadera para n = 0).

En este caso existe un subgrupo normal H en G tal que $N \subset H$ y $H / N = H^*$. Se tiene $| H | = |H^*| | N | = p^{n-1} p = p^n$, con lo cual se completa la prueba.

2.2 Los Teoremas de Sylow

2.2.1. Definición. Sea **p** un número primo. Decimos que un subgrupo P de G es un p-subgrupo de Sylow si es un p-subgrupo maximal de G

Ejemplo.

Hallar los 2-subgrupos de Sylow y los 3-subgrupos de Sylow de S_3, S_4 y S_5

Solución

∗**Los elementos de S_3** son: e = (1) , a_1 = (1 2) , a_2 = (1 3) , a_3 = (2 3) , b_1 = (1 2 3) y b_2 = (1 3 2) = $b_1^2 = b_1^{-1}$

El orden de cualquier 2-subgrupo de Sylow de S_3 es 2, y el orden de cualquier 3-subgrupo de Sylow de S_3 es 3, pues $|S_3| = 6 = 2 \times 3$.

Los tres 2-subgrupos de Sylow de S_3 son los grupos cíclicos: $[a_1]$,

$[a_2]$ y $[a_3]$.

El único 3-subgrupo de Sylow de S_3 es el grupo cíclico (subgrupo normal de S_3) : $[b_1] = [b_2]$.

***Para estudiar S_4 construimos su tabla**:

Estructura de ciclos	Número de ellos	Orden
(1)	1	1
(1 2)	6 = (4x3)/2	2
(1 2 3)	8 = (4x3x2)/3	3
(1 2 3 4)	6 = (4x3x2x1)/4	4
(1 2) (3 4)	$3 = \frac{1}{2}\left(\frac{4x3}{2} x \frac{2x1}{2}\right)$	2

Los únicos divisores de $|S_4| = 2^3 \times 3$, congruentes a 1 módulo 2, son 1 y 3. Luego existen en S_4, uno o tres 2-subgrupos de Sylow.

Sean a = (1 2 3 4) y b = (1 3). Entonces a^{-1} = (4 3 2 1) y ba = (1 2) (3 4) = $a^{-1}b$. Luego H = {e, a, a^2, a^3, b, ab, a^2b, a^3b} es 2-subgrupo de Sylow de S_4.

Los elementos de H son los siguientes:

e = (1)	a = (1 2 3 4)	a^2 = (1 3) (2 4)	a^3 = (4 3 2 1)
b = (1 3)	ab = (1 4) (2 3)	a^2b = (2 4)	a^3b = (1 2) (3 4)

Sean c = (1 2) y d = (1 4) Como:

cac^{-1} = (c(1) c(2) c(3) c(4)) = (2 1 3 4) = (1 3 4 2)

ca^3c^{-1} = (c(4) c(3) c(2) c(1)) = (4 3 1 2)

$dad^{-1} = (d(1)\ \ d(2)\ \ d(3)\ \ d(4)) = (\ 4\ \ 2\ \ 3\ \ 1)$

$da^3d^{-1} = (d(4)\ \ d(3)\ \ d(2)\ \ d(1)) = (1\ \ 3\ \ 2\ \ 4)$

Entonces H, cHc^{-1} y dHd^{-1} son distintos entre sí. Por consiguiente H, cHc^{-1} y dHd^{-1} son todos los 2-subgrupos de Sylow de S_4.

Por otro lado, los únicos divisores de $|S_4| = 2^3 \times 3$, congruentes a 1, mód 3, son 1 y 4. Luego existen uno o cuatro 3-subgrupos de Sylow en S_4.

Para cualesquiera 3-ciclos (i j k) y (m n p):

[(i j k)] = [(m n p)] si y solamente si {i, j, k} ={m, n, p}. Luego el número de 3-subgrupos de Sylow en S_4 es igual al número de subconjuntos de 3 elementos del conjunto {1, 2, 3, 4}, es decir, (4x3x2)/6 = 4. Estos cuatro 3-subgrupos de Sylow son los siguientes grupos cíclicos:

[(1 2 3)], [(1 2 4)], [(1 3 4)], [(2 3 4)]

***De igual modo para S_5** :

Estructura de Ciclos	Número de ellos	Orden
(1)	1	1
(1 2)	10 = (5x4)/2	2
(1 2 3)	20 = (5x4x3)/3	3
(1 2 3 4)	30 = (5x4x3x2)/4	4
(1 2 3 4 5)	24 = 4x3x2x1	5
(1 2) (3 4)	$15 = \frac{1}{2}\left(\frac{5\times 4}{2}\times\frac{3\times 2}{2}\right)$	2
(1 2) (3 4 5)	$20 = \frac{5\times 4}{2}\times\frac{3\times 2\times 1}{3}$	6

Como $|S_5| = 2^3 \times 3 \times 5$, entonces cualquier 2-subgrupo de Sylow de S_5 es de orden 8, y cualquier 3-subgrupo de Sylow de S_5 es de orden 3.

Los únicos divisores de $|S_5|$, congruentes a 1 (mod 2), son 1, 3, 5 y 15. Luego, existen uno, tres, cinco o quince 2-subgrupos de Sylow en S_5. Un 2-subgrupo de Sylow de S_5 es

$H = \{e, a, a^2\ a^3, b, ab, a^2b, a^3b\}$, donde $a = (1\ 2\ 3\ 4)$ y $b = (1\ 3)$.

Por último, el número de subgrupos cíclicos de orden 3 en S_5 es (5x4x3)/6 = 10. Por consiguiente, existen diez 3-subgrupos de Sylow en S_5 y son los siguientes:

[(1 2 3)], [(1 2 4)], [(1 2 5)], [(1 3 4)], [(1 3 5)], [(1 4 5)], [(2 3 4)] y [(2 3 5)], [(2 4 5)] y [(3 4 5)]

2.2.2 **Teoremas fundamentales**

Teorema 2.2.1_ Todo conjugado de un p-subgrupo de Sylow de G es un p-subgrupo de Sylow de G. Por lo tanto si, para algún primo fijo **p**, G tiene un único p-subgrupo de Sylow P, entonces P es normal en G.

Demostración

Sea H un p-subgrupo de Sylow de G. Supongamos que $|G| = p^r m$, donde $r \geq 0$ y **p** no divide a **m**. Entonces $|H| = p^r$. Para cualquier $a \in G$: aHa^{-1} es un subgrupo de G y $| aHa^{-1} | = |H| = p^r$. Luego, para

cualquier a $\in$ G, aHa^{-1} es un p-subgrupo de Sylow. Por lo tanto, todo conjugado de un p-subgrupo de Sylow de G es un p-subgrupo de Sylow de G.

Ahora, si G tiene un único p-subgrupo de Sylow P (para un primo fijo **p**), entonces la colección de p-subgrupos de Sylow de G: $\{aPa^{-1} / a \in G\}$ es unitaria. Luego para todo a $\in$ G : $aPa^{-1} = P$, es decir, P es normal en G.

Comentario. Las nociones de conjugado y centralizador de un elemento son útiles. Ahora consideremos los análogos de estas nociones para un subgrupo.

Definición . Sea H un subgrupo de G. Decimos que un subgrupo S de G es un **conjugado** de H si existe un elemento **a** de G tal que $S = a Ha^{-1}$.

Comentario. Observamos que los subgrupo conjugados son isomorfos.

Definición . Sea H un subgrupo de G. El **normalizador** de H en G, denotado por N_G (H), es el conjunto $N_G(H) = \{a \in G / aHa^{-1} = H\}$

Si no hay lugar a confusión, escribiremos N(H) en vez de $N_G(H)$.

Ejemplos

1 Denótese por I(G) al grupo de todas las conjugaciones de G y por X al conjunto de todos los subgrupos de G. [Si $f_a : x \rightarrow axa^{-1}$, entonces también denotemos por f_a a la función F_a definida por

$F_a(S) = aSa^{-1}$, $S \in X$]. Probar que I(G) es un grupo de permutaciones sobre X, y que si $H \in X$, entonces la órbita de H es el conjunto de todos los subgrupos conjugados a H.

Solución

Sea $f_a \in I(G)$ arbitrario. Veamos que f_a es una permutación de X, es decir, una biyección sobre X. En efecto: $\forall$ S, T $\in$ X :

$f_a(S) = f_a(T)$, $a\,Sa^{-1} = a\,Ta^{-1} \rightarrow S = a^{-1}\,a\,Sa^{-1}\,a = a^{-1}\,a\,Ta^{-1}\,a = T$.

$\forall S \in X : S = a\,a^{-1}\,Saa^{-1} = f_a\ (a^{-1}Sa)$.Luego f_a es inyectiva y sobreyectiva.

Ahora se tiene que para todo $H \in X$, la órbita de H, es

$orb(H) = \{f_a(H) / f_a \in I(G)\} = \{aHa^{-1} / a \in G\}$ = clase de conjugación de H.

2 Probar que el estabilizador de un subgrupo H [bajo la acción de I(G)] es$\{f_a \in I(G) / a \in N_G(H)\}$

Solución

Denotemos por Est(H) al estabilizador de H. Luego tenemos:

$f_a \in Est(H) \leftrightarrow f_a(H) = H \leftrightarrow aHa^{-1} = H \leftrightarrow a \in N_G(H)$.

$\therefore$ Est (H) = $\{f_a \in I(G) / a \in N_G(H)\}$

Teorema 2.2.2_ $N_G(H)$ es un subgrupo de G que contiene a H y es el mayor subgrupo en el cual H es normal.

Demostración

Es claro que $H \subset N_G(H)$ y que H es normal en $N_G(H)$.

Sean a, b $\in N_G(H)$ cualesquiera, tenemos:

$*a\,Ha^{-1} = H$, luego $H = a^{-1}Ha = a^{-1}\,H\,(a^{-1})^{-1}$, es decir, $a^{-1} \in N_G(H)$.

$*$ Por otro lado, $b\,Hb^{-1} = H$, entonces

$abH(ab)^{-1} = abHb^{-1}a^{-1} = aHa^{-1} = H$. Por lo tanto $ab \in N_G(H)$, con lo concluimos que $N_G(H)$ es un subgrupo de G

Sea S un subgrupo de G tal que $H \subset S$ y H es normal en S. Para cualquier $a \in S$, se tiene: $aHa^{-1} = H$, es decir $a \in N_G(H)$. En consecuencia, $S \subset N_G(H)$.

Luego $N_G(H)$ es el mayor subgrupo de G

Finalmente concluimos que $N_G(H)$ es un subgrupo de G, H es normal en $N_G(H)$ y éste es el mayor subgrupo de G en el cual H es normal.

Teorema 2.2.3. El número de los distintos conjugados de H en G es [G : N(H)] y este número divide al orden de G , si G es finito

Demostración

Para cualesquiera a, b $\in$ G, son equivalentes las siguientes afirmaciones:

1 $aHa^{-1} = bHb^{-1}$

2 $H = a^{-1}\,bHb^{-1}\,a$

3 $H = a^{-1} bH(a^{-1} b)^{-1}$

4 $a^{-1}b \in N(H)$

5 $aN(H) = bN(H)$

Por lo tanto, la función F definida por $F(aHa^{-1}) = aN(H)$, es una biyección entre el conjunto de los conjugados distintos de H y las clases laterales a izquierda de N(H). En consecuencia el número de los conjugados distintos de H es [G : N(H)].

Si G es finito, entonces $|G| = [G : N(H)] |N(H)|$ y por lo tanto [G : N(H)] divide a |G|.

Lema 2.2.1 .Si P es un p-subgrupo de Sylow de G, entonces el único elemento de N(P)/ P cuyo orden es una potencia de **p** es P (el elemento neutro).

Demostración

Supongamos que $Px \in N(P) / P$ tiene orden p^k, para algún entero no negativo **k**. Si S* es el subgrupo de N(P)/P generado por Px, entonces S* es un p-grupo, por el corolario del teorema 2.1.2. Según el teorema de correspondencia, existe un subgrupo S de G tal que $P \subset S$ y $S / P = S^*$. Por el teorema 2.1.1, S es un p-grupo que contiene a P. La maximalidad de P implica que S = P y por lo tanto $S^* = \{P\}$ y Px = P.

Lema 2.2.2 .Sean P un p-subgrupo de Sylow de G y $a \in G$ de orden p^k, para algún entero no negativo **k**. Si $aPa^{-1} = P$, entonces $a \in P$

Demostración.

Supongamos que $aPa^{-1} = P$. Entonces $a \in N(P)$. Si π es el homomorfismo canónico de N(P) sobre N(P) / P, entonces el orden de $\pi(a)$ es una potencia de **p**, puesto que $[\pi(a)]^m = \pi(a^m) = \pi(e) = P$, donde $m = p^k$. Por el lema 2.2.1,$\pi(a) = P$, es decir, $a \in \text{Ker}(\pi) = P$.

Lema 2.2.3. Si P es un p-grupo y α es un homomorfismo de P en S_n, entonces la cardinalidad de cada órbita de $\alpha(P)$ es una potencia de **p** (considerando a $\alpha(P)$ como un grupo de permutaciones sobre **n** letras).

Demostración.

Como P es un p-grupo, entonces $\alpha(P) \subset S_n$ es un p-grupo finito y, por lo tanto, su orden es una potencia de **p**. Por consiguiente, el tamaño de cada órbita divide a $|\alpha(P)|$.

Teorema 2.2.4 (Primer teorema de Sylow).

Sea G un grupo finito. Si P es un p-subgrupo de Sylow de G, entonces todos los p-subgrupos de Sylow de G son conjugados a P, y el número de estos subgrupos es congruente a 1, módulo **p**, y es un divisor de IGI.

Demostración.

La idea básica es la realización de que la conjugación por cualquier elemento de G envía un p-subgrupo de Sylow en un p-subgrupo de Sylow.

Sea $X = \{P_1, P_2, \ldots, P_r\}$, donde $P_1 = P$, el conjunto de todos los conjugados de P.

Para cada $a \in G$, definimos $\alpha_a : X \to X$ por medio de

$\alpha_a (P_i) = aP_i a^{-1}$

Como $aP_i a^{-1} = aP_j a^{-1}$ implica $P_i = P_j$, entonces cada α_a es inyectiva. Puesto que cualquier aplicación inyectiva sobre un conjunto finito, debe ser sobreyectiva, resulta que cada α_a es una permutación de X. Más aún, la función $\alpha : G \to S_X$ dada por $\alpha(a) = \alpha_a$, es un homomorfismo. En efecto:

$\alpha_a \alpha_b (P_i) = \alpha_a (bP_i b^{-1}) = abP_i b^{-1}a^{-1} = (ab)P_i(ab)^{-1} = \alpha_{ab} (P_i)$

De manera que $\alpha_a \alpha_b = \alpha_{ab}$

Consideremos la restricción de α a P. Por el lema 2.2.3, la cardinalidad de cada órbita de $\alpha(P)$ es una potencia de **p**. Decir que uno de estas cardinalidades es 1, significa que existe **i** tal que para todo α_a se tiene $\alpha_a (P_i) = P_i$, osea, para todo $a \in G$: $aP_i a^{-1} = P_i$. Por el lema 2.2.2, para todo $a \in P = P_1$: $a \in P_i$, y por lo tanto $P \subset P_i$. Como P es un p-subgrupo de Sylow, entonces $P_i = P$.

En conclusión, cada órbita tiene como cardinalidad una "honesta" potencia de **p** ($p^k \neq 1 \forall k$) , excepto $\{P_1\}$, la cual tiene cardinalidad 1. Consecuentemente **r** es congruente a 1, (mod p).

Ahora supongamos que Q es un p-subgrupo de Sylow de G y que no es un conjugado de P, es decir, $Q \neq P_i$ para todo **i**.

Consideremos la restricción de α a Q. Nuevamente el lema 2.2.3 nos garantiza que la cardinalidad de cada órbita de $\alpha(Q)$ es una potencia de **p**. Si alguna de estas órbitas fuera de cardinalidad 1, entonces esta órbita sería $\{P_i\}$ para algún **i**. El mismo argumento anterior mostraría que $Q = P_i$, contradiciendo la elección de Q. Luego, toda órbita de $\alpha(Q)$ tiene como cardinalidad una "honesta" potencia de **p**, de manera que **p** divide a **r**, o sea, **r** es congruente a 0, (mod p). Esto contradice nuestra previa congruencia, así que tal Q no existe. Por consiguiente, todo p-subgrupo de Sylow de G es un conjugado de P.

Finalmente, como r = [G: N(P)], entonces **r** es un divisor de |G| .

Teorema 2.2.5. (**Segundo teorema de Sylow**)

Si G es un grupo finito de orden $p^k m$, donde **p** es un primo que no divide a **m**, y **k** es un entero positivo, entonces todo p-subgrupo de Sylow de G tiene orden p^k. Además si s_p es el número de p-subgrupos de Sylow de G, entonces s_p divide a **m**

Demostración.

Sea P un p-subgrupo de Sylow de G. En primer lugar, demostraremos que **p** no divide a [G : P]. Como [G : P] = [G : N(P)] [N(P):P], entonces es suficiente demostrar que **p** no divide a ninguno de estos factores. De acuerdo con el teorema 2,2.1, [G: N(P)], que es el número de conjugados de P, es congruente a 1, (mod p). Por lo tanto **p** no divide a [G : N(P)]. Por otro lado, [N(P):P] = |N(P) / P|, y N(P) / P no tiene elementos de orden **p**, conforme el lema 2.2.1. Por el teorema de Cauchy (teorema 2.1.2), **p** no divide a |N(P) / P|. Se infiere que **p** no divide a [G : P].

Por el teorema de Lagrange; $|P| = p^n$, donde $n \leq k$. Luego $[G : P] = |G| / |P| = mp^{k-n}$. Pero **p** no divide a [G:P]. Por consiguiente, $k = n$ y $| P| = p^k$.

Por otro lado, s_p divide a $p^k m$ y es congruente a 1 modulo **p**, de acuerdo con el teorema 2.2.4. Luego s_p no es múltiplo de **p** y por lo tanto s_p y p^k son coprimos. En consecuencia, s_p divide a **m**

Corolario. Sea G un grupo finito y sea **p** un número primo. Si p^n divide a |G|, entonces G contiene un subgrupo de orden p^n.

Demostración.

Si P es un p-subgrupo de Sylow de G, entonces p^n divide a |P|, por el teorema precedente. Por el corolario 2 del teorema 2.1.3, P (y luego G) contiene un subgrupo de orden p^n.

Comentario. Ahora vemos cuánto del recíproco del teorema de Lagrange se puede salvar. Si **m** divide a |G| y **m** es una potencia de un primo, entonces G contiene un subgrupo de orden **m**. Sin embargo, si **m** tiene dos factores primos distintos, entonces se puede mostrar un grupo G, nominalmente A_4, tal que **m** divide a |G| y G no contiene subgrupos de orden **m**.

Capitulo III

Algunas aplicaciones de los teoremas de Sylow

Ilustraremos la potencia de los teoremas de Sylow clasificando los grupos de orden bajo.

3.1 Los grupos diedrales

3.1.1 Definición de grupo diedral. El grupo diedral D_n es un grupo de orden 2n generado por dos elementos **a** y **b** que satisfacen las relaciones $a^n = e$, $b^2 = e$ y $bab = a^{-1}$

Ejemplos

1. Sea A un polígono regular con vértices $v_1, v_2, \ldots, v_n$. Sea G el conjunto de todos los movimientos rígidos de A que llevan vértices en vértices. En particular, sea S una rotación en sentido antihorario que envía cada vértice en uno adyacente, y sea T una reflexión de A en la línea que une $\mathbf{v_1}$ con el centro de A. Como es usual, multiplicaremos en G realizando primero un movimiento y luego el otro.

   Mostraremos que $G \approx D_n$

Consideremos un sistema rectangular de coordenadas con el origen en el centro de A y tal que las coordenadas de v_1 sean (r, 0). Los movimientos rígidos S y T están dados por

$$S(x,y) = (x,y)\begin{bmatrix} \cos(2\pi/n) & -sen(2\pi/n) \\ sen(2\pi/n) & \cos(2\pi/n) \end{bmatrix}$$

$$T(x,y) = (x,-y) = (x,y)\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Por inducción matemática se obtiene:

$\forall k \in N$:

$$S^k(x,y) = (x,y)\begin{bmatrix} \cos(2k\pi/n) & -sen(2k\pi/n) \\ sen(2k\pi/n) & \cos(2k\pi/n) \end{bmatrix}$$

$\forall k \in N$:

$$S^{-k}(x,y) = (x,y)\begin{bmatrix} \cos(-2k\pi/n) & -sen(-2k\pi/n) \\ sen(-2k\pi/n) & \cos(-2k\pi/n) \end{bmatrix}$$

Luego $S^n = I$.

Por otro lado, para cualquier (x,y):

$T^2(x,y) = T(T(x,y)) = T(x,-y) = (x, -(-y)) = (x,y)$.

Entonces $T^2 = I$

Ahora, para cualquier (x,y):

TST (x,y) = TS(x, -y)

$$= T\left((x,-y)\begin{bmatrix} \cos(2\pi/n) & -sen(2\pi/n) \\ sen(2\pi/n) & \cos(2\pi/n) \end{bmatrix} \right)$$

$$= (x, -y) \begin{bmatrix} \cos(2\pi/n) & -sen(2\pi/n) \\ sen(2\pi/n) & \cos(2\pi/n) \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

$$= (x,-y) \begin{bmatrix} \cos(2\pi/n) & sen(2\pi/n) \\ sen(2\pi/n) & -\cos(2\pi/n) \end{bmatrix}$$

$$=T(x,y) \begin{bmatrix} \cos(2\pi/n) & sen(2\pi/n) \\ sen(2\pi/n) & -\cos(2\pi/n) \end{bmatrix}$$

$$=(x,y) \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \cos(2\pi/n) & sen(2\pi/n) \\ sen(2\pi/n) & -\cos(2\pi/n) \end{bmatrix}$$

$$=(x,y) \begin{bmatrix} \cos(2\pi/n) & sen(2\pi/n) \\ -sen(2\pi/n) & \cos(2\pi/n) \end{bmatrix} = S^{-1}(x,y)$$

Por lo tanto $TST = S^{-1}$. Se sigue que $G \approx D_n$.

2. ¿Cuál es el Centro de D_n?

Mostraremos que $Z(D_n)=\{e\}$ si **n** es impar, y que

$Z(D_n) = \{ e, a^{n/2} \}$ si **n** es par, donde $n \geq 3$

Veamos que $D_n = \{a^i b^j / 0 \leq i \leq n-1, 0 \leq j \leq 1\}$

Sean $H = [a] = \{e, a, a^2, ..., a^{n-1}\}$ y $K = [b] = \{e,b\}$.

Veamos que H es un subgrupo normal de D_n, es decir, $xHx^{-1} \subset H$ para todo $x \in D_n$. Es suficiente verificar que $bHb^{-1} \subset H$.

Por inducción matemática se prueba que $a^m\, ba^m = b$ para todo $m \in N$. Sea $a^i \in H$ arbitrario. Se tiene:

$b\, a^i b^{-1} = b\, a^i b = b\, a^i b\, a^i a^{-i} = b\, b\, a^{-i} = a^{-i} \in H$.

Luego $bHb^{-1} \subset H$.

Como H es un subgrupo normal de D_n, entonces HK es un subgrupo de D_n.

Ahora veamos que $H \cap K = \{e\}$.

Si esto no fuera cierto, entonces se tendría $b = a^i$ para algún i, lo cual implicará que ba = ab y por lo tanto sería

$a^{-1} = bab = abb = ae = a$, de manera que o(a) = 2 y $H = [a] = \{e, a\}$, resultando b = a, lo cual no es cierto. Por consiguiente $H \cap K = \{e\}$.

Se sigue que $|HK| = |H||H||K| / |H \cap K| = n(2)/1 = 2n$

En consecuencia $D_n = HK = \{a^i b^j / 0 \leq i \leq n-1, 0 \leq j \leq 1\}$

Todo elemento de D_n es de la forma a^i o de la forma $a^i b$, donde $0 \leq i \leq n-1$.

Es claro que a^i conmuta con cualquier a^j. Luego se tiene las siguientes afirmaciones equivalentes:

$a^i \in Z(D_n)$; $a^i(a^j b) = (a^j b)\, a^i$ para todo **j** en {0,1,2...,n-1};

$a^j a^i b = a^j b\, a^i$ para todo **j** en {0,1,2...n-1};

$a^i b = ba^i$; $a^i b = a^{-i}(a^i b\, a^i)$; $a^i b = a^{-i} b$; $a^i = a^{-i}$; $a^{2i} = e$;

$2i \equiv 0 \pmod n$.

Escribamos J = {0,1,2…,n-1}. Se $a^i b \in Z(D_n)$, entonces, en particular, $(a^i b)a^k = a^k(a^i b)$ para todo **k** en J y por lo tanto $a^{-k} = a^k$ para todo **k** en J, y se sigue que $2k \equiv 0 \pmod n$ para todo **k** en J, lo cual es falso: si **n** es impar y $2K \equiv 0 \pmod n$, entonces k = 0, puesto que $k \in$ J; si **n** es par, entonces $2(n-1) \neq 0 \pmod n$.

Se concluye que $Z(D_n) = \{a^i / 2i \equiv 0 \pmod n\}$.

Si n es impar, entonces $Z(D_n) = \{e\}$

Si n es par, entonces $Z(D_n) = \{e, a^{n/2}\}$.

3. Sea G un grupo finito y sea P un p-subgrupo de Sylow de G. Si $P \lhd G$, ¿P es un factor directo de G?

El siguiente contraejemplo muestra que la respuesta es “no”. Sea $G = S_3$ existe en G un único subgrupo P de orden 3. P es un 3-subgrupo de Sylow de G. $P \lhd G$, por ser el único 3-subgrupo de Sylow de G. Supongamos que P es un factor directo de G. Entonces existe en G un subgrupo normal N tal

que $G \approx P \times N$, de manera que el orden de N es 2. En este caso, P y N son abelianos.. Por lo tanto $G = S_3$ es abeliano. Como esto es falso, concluimos que P no es un factor directo de G.

4. Sea G un grupo finito con subgrupo normales H y K.

   Si $G/H \approx G/K$, ¿Es $H \approx K$?

   La respuesta es "no". El contraejemplo siguiente muestra esto.

   Sea $G = Z_2 \times Z_4$. Se tiene: $H = \{0\} \times Z_4$ y

   $K = \{(0,0),(1,0),(0,1),(1,1)\}$ son subgrupos normales (de índice 2) de G; $G/H \approx Z_2 \approx G/K$

   H no es isomorfo a K, puesto que $H \approx Z_4$ y K es isomorfo al grupo de Klein (todo elemento de K es de orden 2, excepto (0,0)).

Teorema 3.1.1. Sea p un primo impar. Si G es un grupo de orden 2p, entonces es cíclico o diedral.

Demostración..

De acuerdo con el teorema de Cauchy, existen en G un elemento **a** de orden **p** y un elemento **b** de orden 2.

Si $H = [a]$, entonces $H \triangleleft G$, por tener índice 2.

Luego $bab = bab^{-1} = a^m$ para algún entero **m**. Como

$a = eae = b^2ab^2 = b(bab)\,b = ba^mb = ba^mb^{-1} = (bab^{-1})^m = (bab)^m = (a^m)^m = a^k$,

donde $K = m^2$, entonces $m^2 \equiv 1 \pmod p$, esto es, $m \equiv 1 \pmod p$ o

$m \equiv -1 \pmod p$. Por lo tanto $bab = a$ o $bab = a^{-1}$. En el primer caso, **a** y **b** conmutan, G es abeliano y se sigue que $G \approx Z_p \times Z_2 \approx Z_{2p}$. En el segundo caso, se tiene $G \approx D_p$.

Teorema 3.1.2. Si G es un grupo de orden pq, donde **p** y **q** son primos y $p > q$, entonces G es cíclico o G es generado por dos elementos **a** y **b** que satisfacen las siguientes relaciones: $b^p = e$, $a^q = e$, $a^{-1}ba = b^r$

Donde no se cumple que $r \equiv 1 \pmod p$, pero si $r^q \equiv 1 \pmod p$

La segunda posibilidad puede ocurrir solamente si **q** divide a p-1.

Demostración.

De acuerdo con el teorema de Cauchy, en G existen un elemento **b** de orden **p** y un elemento **a** de orden **q**. Sea H = [b]. Como H es un p-subgrupo de Sylow de G, entonces el número de sus conjugados es $1 + kp$ para algún entero no negativo **k**. Pero $1 + kp = [G: N(H)]$, de manera que $1 + kp$ divide a $|G| = pq$. Luego $1 + kp$ divide a q, ya que $1 + kp$ y **p** son coprimos. Se sigue que $k = 0$, puesto que $q < p$.

En consecuencia $H \triangleleft G$.

Por otro lado, si K = [a], entonces K es un q-subgrupo de Sylow de G y por lo tanto el número de sus conjugados es [G: N(K)] = 1 + mq, para algún entero no negativo **m**. Como en el caso del subgrupo H, se deduce que 1 + mq divide a **p**, y por lo tanto m = 0 o **q** divide a p-1. Si m = 0, entonces $K \lhd G$ y se sigue que $G \approx H \times K$. En este caso se tiene: $G \approx Z_p \times Z_q \approx Z_{pq}$.

Ahora supongamos que K no es normal (en este caso q divide a p-1). Como H es normal, entonces $a^{-1}ba = b^r$ para algún entero **r**; además, podemos asumir que no se cumple que $r \equiv 1 \pmod p$, para no retornar al caso abeliano. Por inducción sobre **i**, se infiere que $a^{-i}ba^i = b^t$, donde $t = r^i$. En particular si i = q, entonces $b = ebe = a^{-q}ba^q = b^s$, donde $s = r^q$, de manera que $r^q \equiv 1 \pmod p$.

Corolario. Si |G| = pq, donde **p** y **q** son primos, p > q y **q** no divide a p-1, entonces G es cíclico.

Ejemplo.

Mostraremos que A_5 no tiene subgrupos de orden 15.

Solución.

Para A_5 tenemos la siguiente tabla:

Estructura de ciclos	Orden	Número de ellos
(1)	1	1
(1 2) (3 4)	2	15
(1 2 3)	3	20
(1 2 3 4 5)	5	24

De acuerdo con el corolario del teorema 3.1.2, cualquier grupo de orden 15 es cíclico. Como en A_5 no existen elementos de orden 15, entonces A_5 no tiene sub-grupos de orden 15.

3.2. El grupo Q de los cuaterniones

Definición. El grupo Q de los cuaterniones es un grupo de orden 8 generado por dos elementos a y b que satisfacen las relaciones

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

Ejemplos.

1 Sea G el grupo multiplicativo de todas las matrices complejas no singulares 2 x 2, y sea H el subgrupo de G generado por:

$A=\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ y $B=\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

Mostraremos que H ≈ Q.

Se tiene: $B^2 = A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ $A^{-1}= A^3 =\begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$

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

Esto implica que H ≈ Q, el grupo de los cuaterniones.

2 Consideremos el subconjunto: G = {1, -1, i, -i, j, -j, k, -k }

del anillo de división H (R) de los cuaterniones de Hamilton.

Mostraremos que G es isomorfo al grupo Q de los cuaterniones.

.Se tiene $[i, j] = \{ 1, i, i^2, i^3, j, ij, i^2 j, i^3 j \} = \{1, i, -1, -i, j, k, -j, -k \} = G$

De manera que G es el subgrupo de H (R) generado por **i** y **j**. Como:

$i^4 = 1$, $i^2 = -1 = j^2$ y $j^{-1} i j = -i = i^{-1}$, entonces $G \approx Q$.

3. ¿Cuál es el centro de Q?

Para dar respuesta a esta cuestión hallemos el centro del grupo G del ejemplo anterior:

Es claro $\{1, -1\} \subset Z(G)$. Se observa que **i, j** y **k** no son elementos centrales, puesto que ij = k, ji = -k, jk = i, kj = -i, y por lo tanto **-i, -j** y **-k** no son centrales. Se concluye que Z (G) = {1, -1}.

Como G y Q son isomorfos, entonces existe un isomorfismo f de G sobre Q tal que f(i) = a y f(j) = b, donde a y b son los generadores de Q.

Luego $Z (Q) = \{f(1), f(-1)\} = \{e, f(i^2)\} = \{e, a^2 \}$.

4 Mostraremos que Q / Z (Q) es abeliano.

Como: $| Q / Z(Q) | = | Q | / | Z(Q) | = 8/2 = 4$, entonces Q / Z(Q) es abeliano ($Q/ Z(Q) \approx Z_4$ o $Q / Z(Q) \approx K$, el grupo de Klein)

5 Mostraremos que todo subgrupo de Q es normal.

Consideremos el grupo G = {1, -1, i, -i, j, -j, k, -k} del ejemplo 2. El único elemento de orden 2 es –1 y [-1] = {1, -1} = Z (G) es un subgrupo normal de G. Si H es un subgrupo de G y | H|= 4, entonces H es normal en G, porque su índice en G es 2. Se sigue que todos los subgrupos de G son normales. Como Q es isomorfo a G, entonces todo subgrupo de Q es normal.

6 Mostraremos que Q no es isomorfo a D_4.

Consideremos el grupo G = {1, -1, i, -i, j, -j, k, -k} del ejemplo 2.

El grupo D_4 es generado por dos elementos **a** y **b** que satisfacen las relaciones: $a^4 = e$, $b^2 = e$, y $bab = a^{-1}$

D_4 tiene por lo menos dos elementos de orden 2: $\mathbf{a^2}$ y **b**

($D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$), mientras que G tiene un único elemento de orden 2: el elemento –1. Entonces Q tiene un único elemento de orden 2. Se concluye que Q no es isomorfo a D_4 .

Teorema 3.1.3. Q y D_4 son los únicos grupos no abelianos de orden 8.

Demostración.

Sea G un grupo no abeliano de orden 8. Entonces G no tiene elementos de orden 8. Se sabe que si $x^2 = e$ para todo elemento de un grupo, entonces este grupo es abeliano. Luego G tiene por lo menos un elemento **a** de orden 4. Como [a] tiene índice 2 en G, entonces [a] es un subgrupo normal de G. Sea **b** un elemento de G que no pertenece al subgrupo [a].

Como G / [a] es un grupo de orden 2 y [a]b no es el elemento neutro de G / [a], entonces $[a]b^2 = ([a]b)^2 = [a]e$ y por lo tanto $b^2 \in [a]$. Ahora $b^2 \neq a$ y $b^2 \neq a^3$, porque a y a^3 son de orden 4 y **b** no es de orden 8. Se sigue que:

$b^2 = a^2$ o $b^2 = e$

Además, como [a] es normal, entonces $b^{-1}ab \in [a]$

En consecuencia, $b^{-1}ab = a$ o $b^{-1}ab = a^3$,puesto que $o(b^{-1}ab) = o(a) = 4$ y $o(a^2) = 2$. El primer caso implica que **a** y **b** conmutan. Como los únicos elementos de G / [a] son [a] y [a]b, entonces [a] y [a]b son clases disjuntas y $G = [a] \cup [a]b = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, de manera que G es generado por **a** y **b**. El hecho de que **a** y **b** conmuten contradice el que G sea no abeliano. Entonces la única posibilidad es que $b^{-1}ab = a^{-1}$ (pues $a^3 = a^{-1}$). En resumen, se tienen las siguientes posibilidades:

(i) $a^4 = e$, $b^2 = a^2$ y $b^{-1}ab = a^{-1}$

(ii) $a^4 = e$, $b^2 = e$ y $b^{-1}ab = a^{-1}$

Como (i) describe al grupo Q de los cuaterniones, y (ii) describe al grupo diedral D_4 , entonces se concluye que los únicos grupos no abelianos de orden 8 son Q y D_4.

El siguiente teorema muestra que el único grupo de orden 12 que no tiene elementos de orden 6 es A_4.

Teorema 3.1.4. Todo grupo G de orden 12 no isormorfo a A_4 tiene por lo menos un elemento de orden 6.

Demostración

Por el teorema de Cauchy, existe $b \in G$ tal que $o(b) = 3$. Sea $H = [b]$. Como H es un 3-subgrupo de Sylow de G y como H tiene índice 4 en G, entonces existe un homomorfismo $f: G \to S_4$ cuyo núcleo K es un subgrupo de H. Se sigue que $K = \{e\}$ o $K = H$, puesto que $|H| = 3$ (primo). Si $K = \{e\}$, entonces f es inyectivo y G es isomorfo a un subgrupo de S_4 de orden 12. Como el único subgrupo de S_4 de orden 12 es A_4 y G no es isomorfo a A_4, por hipótesis, entonces $K \neq \{e\}$ y por lo tanto $K = H$, es decir, H es el núcleo de f. Luego $H \triangleleft G$ y, en consecuencia, H es el único 3-subgrupo de Sylow de G. Entonces todos los elementos de G cuyo orden es una potencia de 3, están en H.

En particular, los únicos elementos en G de orden 3 son b y b^2.

Sea C(b) el centralizador de **b** en G. Como $[G: C(b)]$ es el número de conjugados de **b** y los conjugados de **b** son de orden 3, entonces $[G: C(b)] = 1$ o $[G:C(b)] = 2$, de manera que $|C(b)| = 12$ o $|C(b)| = 6$. En cualquier caso, existe $a \in C(b)$ tal que $o(a)=2$, por el teorema de Cauchy. Como $a \in C(b)$, entonces **a** y **b** conmutan. Siendo, además, los órdenes de **a** y **b** coprimos, se infiere que ab tiene orden 6.

De la demostración del teorema anterior se tiene el siguiente resultado.

Corolario. Si G es de orden 12 y G no es isomorfo a A_4, entonces G tiene un 3-subgrupo de Sylow normal.

3.3 Clasificación de los grupos de orden bajo

3.3.1. Grupos de órdenes 2,3,5,7,11 y 13

Se sabe que si G es un grupo de orden primo **p**, entonces G es cíclico y por lo tanto $G = Z_p$, salvo isomorfismo. Luego los únicos grupos de órdenes 2,3,5,7,11 y 13 son Z_2, Z_3, Z_5, Z_{11} y Z_{13}, respectivamente, salvo isomorfismo.

3.3.2 Grupos de órdenes 4 y 9

Mostraremos que para todo primo **p** ($p \geq 2$), existen exactamente dos grupos no isomorfos de orden p^2: Z_{p^2} y $Z_p \times Z_p$.

Supongamos que $|G| = p^2$. Entonces G tiene un subgrupo normal H de orden **p**, por el corolario 2 del teorema 2.1.3 H es cíclico porque IHI es primo.

Sea $a \notin H$. El orden de **a** divide a p^2. Luego o(a) es **p** o p^2, puesto que $a \neq e$

. Si $o(a) = p^2$, entonces $G = [a]$, es decir, G es cíclico de orden p^2. En este caso $G \approx Z_{p^2}$.

Si $o(a) = p$, entonces $[a] \cap H = \{e\}$, porque si existiera $b \in [a] \cap H$, $b \neq e$, entonces sería $o(b) = p$ y se tendría $[b] = [a]$ y $[b] = H$, y esto implicaría que $a \in H$. Por otro lado, $I[a]IIHI = p^2$ y como G es abeliano (por el corolario 1 del teorema 2.1.3), entonces $[a] \triangleleft G$.

Por consiguiente $G \approx [a] \times H \approx Z_p \times Z_p$.

En particular, los únicos grupos de orden 4 son Z_4, y $Z_2 \times Z_2$, salvo isomorfismo, y los únicos grupos de orden 9 son Z_9 y $Z_3 \times Z_3$, salvo isomorfismo.

3.3.3 Grupos de órdenes 6, 10 y 14

De acuerdo con el teorema 3.1.1, tenemos:

Los únicos grupos de orden 6 son Z_6 y D_3, salvo isomorfismo; los únicos grupos de orden 10 son Z_{10} y D_5, salvo isomorfismo; y los únicos grupos de orden 14 son Z_{14} y D_7, salvo isomorfismo.

3.3.4. Grupos de orden 8

De acuerdo con el teorema 3.1.3, los únicos grupos de orden 8 son Z_8, $Z_4 \times Z_2$, $Z_2 \times Z_2 \times Z_2$, Q (el grupo de los cuaternianos) y D_4, salvo isomorfismos.

3.3.5. Grupos de orden 12. De acuerdo con el teorema 3.1.4, los únicos grupos de orden 12 (salvo isomorfismo) son Z_{12}, $Z_2 \times Z_6$, $Z_2 \times S_3$, A_4 y el grupo T generado por dos elementos **a** y **b** que satisfacen las relaciones

$a^6 = e$, $b^2 = a^3 = (ab)^2$.

3.3.6. Grupos de orden 15

De acuerdo con el corolario del teorema 3.1.2, el único grupo de orden 15 es Z_{15}, salvo isomorfismos.

3.3.7 Tabla de grupos de órdenes desde 2 hasta 15

Orden	Número de grupos no isomorfos	Grupos
2	1	Z_2
3	1	Z_3
4	2	Z_4 y Z_2xZ_2
5	1	Z_5
6	2	Z_6 y $D_3 \approx S_3$
7	1	Z_7
8	5	Z_8 , Z_4xZ_2 , $Z_2xZ_2xZ_2$, Q y D_4
9	2	Z_9 y Z_3xZ_3
10	2	Z_{10} y D_5
11	1	Z_{11}
12	5	Z_{12} , Z_2xZ_6 , Z_2xS_3 , A_4 y T
13	1	Z_{13}
14	2	Z_{14} y D_7
15	1	Z_{15}

Bibliografía Consultada

1 Rotman, J.J.

The Theory of Groups: An introduction. Allyn and Bacon. 1965

2 Fraleigh, John B.

Álgebra Abstracta (Primer curso) Addison–Wesley Iberoamericana.1987

3 Burnside, W

Theory of Groups of finite order. Dover. 1955

4 O'Brien, H

Estructuras Algebraicas III (Grupos finitos). Monografía de la OEA

5 Herstein, I. N

Topics in Álgebra. John Wiley 1975

6 Baumslag, B-Chandler, B

Teoría de grupos. McGraw-Hill. 1972