2-y
19

Universidad Nacional Autónoma de México

FACULTAD DE CIENCIAS

EL PRODUCTO DE ENTRELAZAMIENTO DE DOS GRUPOS CICLICOS DE ORDEN 3

Tesis Profesional

Que para obtener el Título de:

MATEMATICO

p r e s e n t a:

BERTHA ALICIA MADRID NUÑEZ

México, D. F. **1986**

I N D I C E

1. INTRODUCCION.

Uno de los problemas que permanece abierto en la teoría de grupos, es el de clasificarlos. No se ha resuelto ni para grupos de orden finito, y sólo en algunos casos, (abelianos por ejemplo) se ha podido dar la descripción completa de todos ellos para cada orden dado. Aparece de manera natural la cuestión de determinar en cada grupo, cuales son todos sus subgrupos y en particular aquellos que son normales, y en este contexto,un teorema notable (y sencillo) que se debe a Lagrange es el que asegura que todo grupo finito G y para todo subgrupo H de G, el orden de H divide al orden de G.(de lo que resulta, por ejemplo que todo grupo de orden primo es necesariamente simple* y cíclico).

Se sabe que una especie de inverso del teorema de Lagrange, a saber: "Si m divide al orden de G, entonces G debe de tener al menos un subgrupo de orden m", es

*Definición: Un grupo se llama simple, si sus únicos subgrupos normales son los triviales. BURNSIDE estableció la conjetura de que, en vista de que todos los grupos simples no triviales que se habían encontrado, eran de orden par, ello debía ser así, y por lo tanto, la imparidad en el orden de un grupo (no de orden primo), debía implicar solubilidad. Este resultado fué demostrado en 1950 por THOMPSON y FEIT.

falso, lo que se comprueba examinando al grupo de las permutaciones pares de cuatro objetos, cuyo orden es 12 y que no tiene ningún subgrupo de orden 6. Sin embargo si se especializa de alguna manera al conjunto de divisores del orden de G que deban considerarse, pueden obtenerse resultados afirmativos interesantes. En este sentido, quizá los mas notables son los que obtuvo Sylow, y que estan contenidos esencialmente en los teoremas que llevan su nombre, y que se pueden presentar de la manera siguiente:

TEOREMAS DE SYLOW:

Definición 1:

Sea G un grupo finito, cuyo orden es p m con p primo, y $(p,m) = 1$. Entonces todo subgrupo de G de orden p^{α} se llama p-subgrupo de Sylow de G, (y se denotará p-SS de G)

Definición 2:

Un subgrupo de un grupo finito G es un p-subgrupo de G (p-s de G) si su orden es una potencia de p. En particular los p-SS de G, son p-s de G.

TEOREMA 1:

Para cada número primo p, todo grupo finito G tiene al menos un p-SS.

TEOREMA 2:

Para cada p primo y para todo grupo finito G, los p-SS de G son conjugados entre sí. (Es decir si P_1 y P_2 son p-SS de G que corresponden al mismo primo p, existe $x \in G$ tal que $P_1 = xP_2x^{-1}$).

COROLARIO 1:

UN p-SS de G , P es único, si y sólo si P es normal de G

COROLARIO 2:

Todo grupo abeliano finito es producto directo de sus p-SS no triviales.

TEOREMA 3:

Para cada p primo y para todo grupo finito G, el número de los p-SS de G es congruente con 1 módulo p.

TEOREMA 4:

Todo p-S de un grupo finito G, está contenido en un p-SS de G.

Los teoremas anteriores constituyen una herramienta poderosa para el estudio y clasificación de los grupos finitos, (especialmente útil si para algún primo p el correspondiente p-SS resulta único y por lo tanto normal), y como ejemplos sencillos de su aplicación, se mencionan los resultados siguientes:

1) Sea G un grupo de orden pq, en donde p y q son primos, p es menor que q y q no es congruente con 1 módulo p. Entonces G es necesariamente cíclico.

2) Si el orden de G es pq^2 ,p,q primos, p menor que q y p no divide a $q^2 - 1$, entonces G es necesariamente abeliano.

3) Si elorden de G es $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ con $p_1, \ldots, p_r$ primos y $p_1, p_2, \ldots, p_r$ un conjunto de representantes de los p-SS de G, entonces G es nilpotente si y sólo si

i) cada p_i es normal en G $\qquad i = 1, \ldots, r$

ii) $G = P_1 \times P_2 \times \ldots \times P_r$

4) No existen grupos simples de ordenes 30,56 ó 200.

Cuando se presentan los teoremas de Sylow por primera vez en el estudio tradicional del álgebra moderna, los p-SS aparecen en general en forma abstracta. Los ejemplos que suelen darse a este nivel, casi siempre son tan triviales o tan complicados que pierden toda su utilidad didáctica y su valor como modelo del concepto que se quiere ilustrar. Por esto se pensó que valía la pena mostrar un caso que no cayera en los extremos antes mencionados y así surgió este trabajo que describe un p-SS de un grupo particular, junto con la red completa de sus subgrupos.

Se escogió al conjunto $S = \mathbb{Z}_3 \times \mathbb{Z}_3$ (de 9 elementos) y se tomó un grupo básico al grupo S_9 de las permutaciones de S junto con la composición de permutaciones, entre las que se seleccionaron cuatro de ellas, a, b_0, b_1, y b_2 cuya acción sobre S se describió utilizando una notación matricial. Se consideraron también los subgrupos A, B_0, B_1 y B_2 de S_9 que estas permutaciones generan, y se definió como G al subgrupo de S_9 generado por las cuatro. Finalmente se hizo ver que:

1) Todo elemento de G se puede escribir en forma única como

$$a^r b_0^{s_0} b_1^{s_1} b_2^{s_2} \quad , \quad 0 \leq r, s_0, s_1, s_2 \leq 2$$

y por lo tanto:

2) El orden de G es 3^4, que también es la mayor potencia de 3 que divide al orden de S_9, (que como sabemos es 9!) y por lo tanto G resulta ser un 3-SS de S_9

Es este grupo G, 3-SS de S_9, y que, de otra manera puede definirse como el producto de entrelazamiento de dos grupos de orden 3, $\mathbb{Z}_3 \wr \mathbb{Z}_3$, sobre el que se trabajó y cuya red completa de subgrupos se exhibe en esta tesis.

El presente trabajo está basado en la monografía de H. Cárdenas y E. Lluis [2] en donde determinan la red de subgrupos del producto de entrelazamiento $\mathbb{Z}_p \wr \mathbb{Z}_p$ así como en varias conferencias de E. Lluis y C. Rincón.

A todos ellos mis sinceros agradecimientos.

2. EL GRUPO

Sea S_9 el grupo de permutaciones del conjunto de 9 elementos $Z_3 \times Z_3$. La multiplicación en S_9 es la composición de permutaciones.

Representaremos $Z_3 \times Z_3$ en forma de matriz:

$$\begin{pmatrix} (0,0) & (0,1) & (0,2) \\ (1,0) & (1,1) & (1,2) \\ (2,0) & (2,1) & (2,2) \end{pmatrix}$$

o simplemente:

$$\begin{pmatrix} \circ & \circ & \circ \\ \circ & \circ & \circ \\ \circ & \circ & \circ \end{pmatrix}$$

Entre los elementos de S_9 distinguiremos a las siguientes permutaciones.

$a \in S_9$	Permutación cíclica de los renglones
$b_0 \in S_9$	Permutación cíclica de los elementos del renglón 0
$b_1 \in S_9$	Permutación cíclica de los elementos del renglón 1
$b_2 \in S_9$	Permutación cíclica de los elementos del renglón 2.

o sea

$$a(i,j) = (i+1,j)$$

$$b_k(i,j) = \begin{cases} (i,j) & \text{si} \quad i \neq k \\ (i,j+1) & \text{si} \quad i = k \end{cases}$$

explícitamente

$a(0,0) = (1,0)$ $\quad$ $a(0,1) = (1,1)$ $\quad$ $a(0,2) = (1,2)$

$a(1,0) = (2,0)$ $\quad$ $a(1,1) = (2,1)$ $\quad$ $a(1,2) = (2,2)$

$a(2,0) = (0,0)$ $\quad$ $a(2,1) = (0,1)$ $\quad$ $a(2,2) = (0,2)$

$b_0(0,0) = (0,1)$ $\quad$ $b_0(0,1) = (0,2)$ $\quad$ $b_0(0,2) = (0,0)$

$b_0(1,0) = (1,0)$ $\quad$ $b_0(1,1) = (1,1)$ $\quad$ $b_0(1,2) = (1,2)$

$b_0(2,0) = (2,0)$ $\quad$ $b_0(2,1) = (2,1)$ $\quad$ $b_0(2,2) = (2,2)$

etc.

Gráficamente

$a =$ 

$b_0 =$ 

$b_1 =$ 

$b_2 =$ 

Se observa que:

$a^2 \neq 1$ $\quad$ $b_0^2 \neq 1$ $\quad$ $b_1^2 \neq 1$ $\quad$ $b_2^2 \neq 1$

$a^3 = 1$ $\quad$ $b_0^3 = 1$ $\quad$ $b_1^3 = 1$ $\quad$ $b_2^3 = 1$

Es decir, el orden de cada uno de estos elementos es 3 y en vista de esto, en lo sucesivo utilizaremos como exponentes de a, b_0, b_1, y b_2 a los elementos de Z_3

Denotaremos

$$A = \langle a \rangle \qquad B_0 = \langle b_0 \rangle \qquad B_1 = \langle b_1 \rangle \qquad B_2 = \langle b_2 \rangle$$

Observemos que los conjuntos en los que opera cada una de las b_i son ajenos. Por lo tanto, para toda i y toda j,

$$b_i b_j = b_j b_i$$

LEMA 1: Para cada i, i = 0,1,2

$$B_i \cap (B_j \cup B_k) = 1 \qquad (j,k \neq i)$$

DEMOSTRACION:

Cada elemento de B_i deja fijo a todos los elementos de los renglones diferentes de i y el único elemento de $B_j \cup B_k$ que hace esto es 1.

COROLARIO 3:

B es el producto directo de B_0 por B_1 por B_2

$$B = B_0 \times B_1 \times B_2$$

COROLARIO 4:

Si $b_0^{s_0} b_1^{s_1} b_2^{s_2} = b_0^{s_0'} b_1^{s_1'} b_2^{s_2'}$ entonces $s_0 = s_0'$, $s_1 = s_1'$, $s_2 = s_2'$

COROLARIO 5:

B es un grupo tal que $\exp(B) = 3$

(Recuérdese que los exponentes los estamos situando en Z_3)

LEMA 2:

$$ab_0a^{-1} = b_1$$

$$ab_1a^{-1} = b_2$$

$$ab_2a^{-1} = b_0$$

DEMOSTRACION:

$$(ab_ka^{-1})(i,j) = ab_k(i-1,j) =$$

$$\left\{\begin{array}{lll} a(i-1,j+1) = (i,j+1) & \text{si} & k = i-1 \\ a(i-1,j) = (i,j) & \text{si} & k \neq i-1 \end{array}\right\} = b_{k+1}(i,j)$$

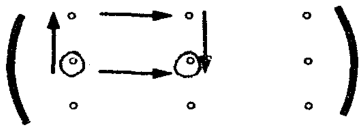
Obsérvese que también los subíndices se están utilizando módulo 3

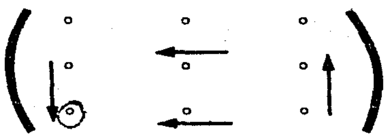
Ejemplos:

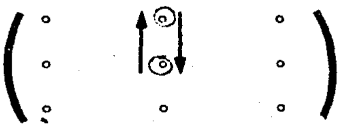
1) $ab_0a^{-1}(1,0) = b_1(1,0) = (1,1)$

2) $ab_1a^{-1}(2,2) = b_2(2,2) = (2,0)$

3) $ab_1a^{-1}(1,1) = b_2(1,1) = (1,1)$

1)


2)


3)


Del lema anterior se siguen directamente las siguientes reglas de conmutación que serán útiles en calculos posteriores:

$$ab_0 = b_1a$$

$$ab_1 = b_2a$$

$$ab_2 = b_0a$$

$$b_ib_j = b_jb_i$$

Es decir, en todo producto en el que aparezca la "a" a la derecha de cualquier "b", se puede pasar la "a" a la izquierda de la "b" restándole uno (mod 3) al subíndice de la "b".

Utilizando repetidamente las fórmulas anteriores obtenemos:

$$b_i^{r_i} a^r = a^r b_{i-r}^{r_i} \qquad \ldots\ldots\ldots\ldots(1)$$

Denotaremos con G al subgrupo de S generado por los elementos antes considerados:

$$G = \langle a, b_0, b_1, b_2 \rangle \ .$$

Cada elemento de G es producto de potencias de a, b_0, b_1, b_2 en cualquier orden (lo que incluye a los inversos). Ahora bien, las reglas de conmutación anteriores permiten "llevar" todas las "a" hacia la izquierda y escribir el elemento en la forma

$$a^r b_0^{s_0} b_1^{s_1} b_2^{s_2}$$

o simplemente

$$a^r b, \qquad b \in B$$

se insiste en que los exponentes se toman en Z_3

Hemos demostrado así:

LEMA 3:

Todo elemento de G se puede escribir en la forma:

$$a^r b_0^{s_0} b_1^{s_1} b_2^{s_2} \qquad 0 \le r, \quad s_0, s_1, s_2 \le 2$$

Ejemplos:

1) $ab_0ab_2aab_1a = ab_0ab_2aaab_0 = a^2b_2b_2b_0 = a^2b_0b_2^2$

2) $b_2b_1b_0a = ab_1b_0b_2$

3) $b_0^2b_2aaaab_1^2b_0 = ab_2^2b_1b_1^2b_0 = ab_0b_2^2$

4) $b_0a^2 = b_0aa = ab_2a = a^2b_1$

5) $b_0^{r_0}b_1^{r_1}b_2^{r_2}a^r = a^rb_{0-r}^{r_0}b_{1-r}^{r_1}b_{2-r}^{r_2}$

6) $a^sb_0^{s_0}b_1^{s_1}b_2^{s_2}a^rb_0^{r_0}b_1^{r_1}b_2^{r_2}b_2^{-s_0}b_1^{-s_1}b_0^{-s_2}a^{-s} =$

$= a^rb_{0+s-r}^{s_0}b_{1+s-r}^{s_1}b_{2+s-r}^{s_2}b_{0+s}^{r_0-s_0}b_{1+s}^{r_1-s_1}b_{2+s}^{r_2-s_2}$

Obsérvese que la conjugación de un elemento $g\varepsilon G$ con cualquier otro elemento $h\varepsilon G$, deja invariante la suma de los exponentes de las b_i de g, así como al exponente de la a.

Dado que cada elemento de A "manda" cada columna en sí misma, y que el único elemento de $B = B_0 \times B_1 \times B_2$ con tal propiedad es el idéntico, se cumple el lema siguiente:

LEMA 4:

$$A \cap (B_0 \cup B_1 \cup B_2) = \{1\}$$

COROLARIO 6:

Si $a^rb = a^{r'}b'$, entonces $r = r'$.

DEMOSTRACION:

$a^rb = a^{r'}b' \rightarrow a^{r-r'} = b'b^{-1}\varepsilon\ A \cap B = \{1\} \quad \therefore \quad r = r'$

De los lemas anteriores se sigue directamente el siguiente teorema.

TEOREMA 5:

Los elementos del grupo G se pueden escribir en forma única, de la manera siguiente:

si $g \in G$, $g = a^r b_0^{s_0} b_1^{s_1} b_2^{s_2}$

COROLARIO 7:

$[G:1] = 3^4 = 81$ elementos.

Obsérvese que $[S_9:1] = 9! = 3^4 \cdot 2^7 \cdot 5 \cdot 7 = 362880$ y que por lo tanto, la máxima potencia de 3 que divide a $[S_9:1]$ es 3^4, de donde G es, por definición, un 3-subgrupo de Sylow de S_9.

El grupo G es el subgrupo de S_9 con el que trabajaremos.

SUBGRUPOS MAXIMOS DE G

$$B = \{ b_0^{r_0}b_1^{r_1}b_2^{r_2}\} = B_0 \times B_1 \times B_2$$

$$F_0 = \{a^r b_0^{r_0}b_1^{r_1}b_2^{r_2} \mid r_0 + r_1 + r_2 = 0 \}$$

$$F_1 = \{a^r b_0^{r_0}b_1^{r_1}b_2^{r_2} \mid r_0 + r_1 + r_2 = r \}$$

$$F_2 = \{a^r b_0^{r_0}b_1^{r_1}b_2^{r_2} \mid r_0 + r_1 + r_2 = 2r\}$$

PROPOSICION 1:

B, F_0, F_1, F_2, son subgrupos normales de G y de orden 27. Obviamente ninguno de ellos es vacío.

DEMOSTRACION: (de que B es un subgrupo)

$$b_0^{r_0}b_1^{r_1}b_2^{r_2}b_0^{s_0}b_1^{s_1}b_2^{s_2} = b_2^{r_0}b_0^{r_1}b_1^{r_2}b_0^{s_0}b_1^{s_1}b_2^{s_2} = b_0^{r_1+s_0}b_1^{r_2+s_1}b_2^{r_0+s_2}$$

DEMOSTRACION: (de que las F's son subgrupos)

sean $g,h \in F_i$ $\quad (0 \leq i \leq 2)$

$g = a^r b_0^{r_0}b_1^{r_1}b_2^{r_2}$, $h = a^s b_0^{s_0}b_1^{s_1}b_2^{s_2}$, con $r_0 + r_1 + r_2 = ir$

y $s_0 + s_1 + s_2 = is$ entonces $gh = a^r b_0^{r_0}b_1^{r_1}b_2^{r_2}a^s b_0^{s_0}b_1^{s_1}b_2^{s_2}$

observese que $\{ -s, 1-s, 2-s\} = \{ 0,1,2 \}$ $\therefore$ $gh = a^{r+s}b_0^{t_0}b_1^{t_1}b_2^{t_2}$

en donde $t_0 + t_1 + t_2 = r_0 + r_1 + r_2 + s_0 + s_1 + s_2 = i(r + s)$

lo que prueba $gh \in F_i$.

Por otro lado el hecho de que el orden es 27 se sigue de contarlos ya que la condición $r_0 + r_1 + r_2 = ir$ da 3 grados de libertad para seleccionar las r's .

DEMOSTRACION: (de que son normales)

la propiedad que determina si $a^r b_0^{r_0}b_1^{r_1}b_2^{r_2}$ esta en B, es $r = 0$, y la que caracteriza a los elementos de los grupos F_0, F_1 , F_2 es la relación entre r y la suma $r_0 + r_1 + r_2$. Tanto r como ---

$r_0 + r_1 + r_2$, son invariantes bajo conjugación (observación del ejemplo 6 página (6) y por lo tanto B, F_0 , F_1 , F_2 son subgrupos normales de G.

Podría también considerarse las funciones

$$G \xrightarrow{\Psi_i} Z_3$$

$$a^r b_0^{r_0} b_1^{r_1} b_2^{r_2} \longrightarrow ir \qquad (r_0 + r_1 + r_2\ )$$

Ψ_i es un homomorfismo de grupo y ker $\Psi_i = F_i$ $(0 \leq i \leq 2)$

OBSERVACIONES:

B, F_0 , F_1 , F_2 son subgrupos máximos de G, ya que su orden es 27 y el grupo G es de orden 81.

Más adelante demostraremos que son los únicos subgrupos máximos y que por lo tanto cualquier subgrupo de G esta contenido en uno de ellos .

3. EL HOMOMORFISMO Δ

Recordamos que $A = \{ 1 , a , a^2 \}$

Sea $Z_3A = \{s_0 + s_1a + s_2a^2 \mid s_i \in Z_3\}$

con las definiciones:

i) $$s_0 + s_1a + s_2a^2 = t_0 + t_1a + t_2a^2$$

si y sólo si $s_i = t_i$,

$i = 0 , 1 , 2$

ii)

$$(s_0 + s_1a + s_2a^2)(t_0 + t_1a + t_2a^2) =$$
$$(s_0t_0 + s_1t_2 + s_2t_1) + (s_0t_1 + s_1t_0 + s_2t_2)a +$$
$$(s_0t_2 + s_1t_1 + s_2t_0)a^2$$

esto es:

Z_3A es el anillo de grupo de A sobre el anillo Z_3

(Z_3A resulta ser, además, una Z_3 - álgebra)

Recordemos también que

$$B = B_0 \times B_1 \times B_2 \quad (\cong Z_3 \times Z_3 \times Z_3),$$

es un grupo abeliano,al que se le da la estruc tura de Z_3A - modulo definido para $b \in B$,

$$(s_0 + s_1a + s_2a^2 \ , b) \longrightarrow b^{s_0}(aba^{-1})^{s_1}(a^2ba^{-2})^{s_2} \doteq$$
$$\doteq b^{s_0}(b^a)^{s_1}(b^{a^2})^{s_2} = b^{s_0 + s_1a + s_2a^2}$$

Nótese que si $b_j, b_k \in B$,

$(b_jb_k)^{a^r} = a^rb_jb_ja^{-r} = a^rb_ja^{-r}a^rb_ka^{-r} = b_j^{a^r}b_k^{a^r}$ y como para $i = 0,1,2$ si es un exponente, la notación adoptada resulta "consistente" en el sentido que "valen las leyes de los exponentes".

$$(s_0 + s_1a + s_2a^2, b) \longrightarrow b^{s_0}(ab^{s_1}a^{-1})(a^2b^{s_2}a^{-2}) =$$
$$= b^{s_0}b^{s_1a}b^{s_2a} = b^{s_0}(b^a)^{s_1}(b^{a^2})^{s_2}$$

$$\alpha = s_0 + s_1a + s_2a^2$$

$$\beta = t_0 + t_1a + t_2a^2$$

$$\alpha + \beta = (s_0 + t_0) + (s_1 + t_1)a + (s_2 + t_2)a^2$$

$$b^\alpha b^\beta \stackrel{?}{=} b^{\alpha+\beta}$$

$$b^\alpha b^\beta = b^{s_0}(b^a)^{s_1}(b^{a^2})^{s_2}b^{t_0}(b^a)^{t_1}(b^{a^2})^{t_2} = b^{s_0+t_0}(b^a)^{s_1+t_1}(b^{a_2})^{s_2+t_2}$$

$$= (b^\alpha)^\beta \stackrel{?}{=} b^{\alpha\beta}$$

NOTESE:

i) $(b^{a^r})^s = (a^rba^{-r})(a^rba^{-r})\ldots.(a^rb^{-r}) = a^rb^sa^{-r} = (b^s)^{a^r}$

ii) $(b^{a^r})^s = a^sb^{a^r}a^{-s} = a^sa^rba^{-r}a^{-s} = a^{r+s}ba^{-(r+s)} =$
$= b^{a^{r+s}} = b^{a^ra^s}$

$$\therefore (b^\alpha)^\beta = (b^\alpha)^{t_0}[(b^\alpha)^a]^{t_1}[(b^\alpha)^{a^2}]^{t_2} =$$
$$= [b^{s_0}(b^a)^{s_1}(b^{a^2})^{s_2}]^{t_0}\cdot[(b^{s_0}(b^a)^{s_1}(b^{a^2})^{s_2})^a]^{t_1}\cdot[(b^{s_0}(b^a)^{s_1}(b^{a^2})^{s_2})^{a^2}]^{t_2}$$
$$= [(b^a)^{s_0t_1}(b^{a^2})^{s_1t_1}(b)^{s_2t_1}][(b^{a^2})^{s_0t_2}(b)^{s_1t_2}(b^a)^{s_2t_2}] \ .$$
$$\cdot [b^{s_0t_0}(b^a)^{s_1t_0}(b^{a^2})^{s_2t_0}] = b^{(s_0t_0+s_1t_2+s_2t_2)}(b^a)\ldots = b^{\alpha\beta}$$

En Z_3 destacamos el siguiente elemento

$$\Delta = a - 1$$
$$\Delta^2 = a^2 + a + 1$$
$$\Delta^3 = 0$$

Denotaremos con

$$B^{\Delta} = \{ b^{\Delta} \mid b \in B \}$$
$$B^{\Delta^2} = \{ b^{\Delta^2} \mid b \in B \}$$

Entonces se tiene

$$B \supset B^{\Delta} \supset B^{\Delta^2} \supset 1$$

se tiene $o(B) = 27$ y $o(1) = 1$

se demostrara $o(B^{\Delta}) = 9$ y $o(B^{\Delta^2}) = 3$

describiremos a continuación B^{Δ} y B^{Δ^2}

sea $b_0^{r_0}b_1^{r_1}b_2^{r_2} \in B^{\Delta}$.·. $b_0^{s_0}b_1^{s_1}b_2^{s_2} \ni$

$(b_0^{r_0}b_1^{r_1}b_2^{r_2})^{\Delta} = (b_0^{s_0}b_1^{s_1}b_2^{s_2})^{a-1} = (b_0^{s_0}b_1^{s_1}b_2^{s_2})^{a}(b_0^{s_0}b_1^{s_1}b_2^{s_2})^{-1} =$

$= a(b_0^{s_0}b_1^{s_1}b_2^{s_2})a^{-1}(b_0^{-s_0}b_1^{-s_1}b_2^{-s_2}) = b_1^{s_0}b_2^{s_1}b_0^{s_2}b_0^{-s_0}b_1^{-s_1}b_2^{-s_2} =$

$= b_0^{s_2-s_0}b_1^{s_0-s_1}b_2^{s_1-s_2}$ y aqui $(s_2-s_0)+(s_0-s_1)+(s_1-s_2) = 0$

hemos así demostrado el lema siguiente:

LEMA 5 :

Si $b_0^{r_0}b_1^{r_1}b_2^{r_2} \in B^{\Delta}$ entonces $r_0+r_1+r_2 = 0$.·. $B^{\Delta} \subset F_0$

probaremos ahora el reciproco

LEMA 6 :

Si $r_0 + r_1 + r_2 = 0$ entonces $b_0^{r_0}b_1^{r_1}b_2^{r_2} \in B^{\Delta}$

DEMOSTRACION:

Tomemos $b_0^{r_0}b_1^{r_1}b_2^{r_2}$ tal que $r_0 + r_1 + r_2 = 0$ y buscamos s_0 , s_1 , s_2 de tal manera que

$$\begin{cases} s_2 - s_0 = r_0 \\ s_0 - s_1 = r_1 \\ s_1 - s_2 = r_2 \end{cases}$$

$$\begin{pmatrix} -1 & 0 & 1 & r_0 \\ 0 & -1 & 1 & r_0 + r_1 \\ 0 & 1 & -1 & r_2 \end{pmatrix} \sim \begin{pmatrix} -1 & 0 & 1 & r_0 \\ 0 & -1 & 1 & r_0 + r_1 \\ 0 & 0 & 0 & r_0 + r_1 + r_2 \end{pmatrix}$$

y como $r_0 + r_1 + r_2 = 0$,este sistema tiene solución.

Antes de continuar destacaremos el subgrupo de G al que - llamaremos diagonal, $D = < d >$,en donde $d = b_0b_1b_2$.

(D es de orden 3)

$B^{\Delta^2} = (B^{\Delta})^{\Delta}$ $\qquad d = b_0b_1b_2$

TEOREMA 6:

$B^{\Delta^2} = D = <d> = \{1, d, d^2\}$.

DEMOSTRACION:

Sea $b \in B^{\Delta^2}$.·. $\exists$ $b_0^{r_0}b_1^{r_1}b_2^{r_2}$ con $r_0 + r_1 + r_2 = 0$ $\nrightarrow$

$b = (b_0^{r_0}b_1^{r_1}b_2^{r_2})^{a-1} = b_0^{r_2-r_0}b_1^{r_0-r_1}b_2^{r_1-r_2}$ con $r_0 = -(r_1 + r_2)$

.·. $b = b_0^{r_1-r_2}b_1^{r_1-r_2}b_2^{r_1-r_2} = d^{r_1-r_2} \in D$

reciprocamente sea $b \in D$ $\quad b = b_0^{s_0}b_1^{s_1}b_2^{s_2}$ por demostrar - que existen r_0, r_1, r_2, $r_0 + r_1 + r_2 = 0$ tales que $(b_0^{r_0}b_1^{r_1}b_2^{r_2})^{\Delta} = b$.

se definen $r_1, r_2, \ni\ r_1 - r_2 = s_0$, y $r_0 = -(r_1 + r_2)$

entonces $b = b_0^{r_2-r_0} b_1^{r_0-r_2} b_2^{r_1-r_2} = (b_0^{r_0} b_1^{r_1} b_2^{r_2})^{a-1} \in (B^\Delta)^\Delta$

ya que por construcción $r_0 + r_1 + r_2 = 0$

PROPOSICION 2:

Si $g = a^r b_0^{r_0} b_1^{r_1} b_2^{r_2}$, entonces $g^3 = d^{r_0+r_1+r_2} \in D$.

DEMOSTRACION:

$$g^2 = a^r b_0^{r_0} b_1^{r_1} b_2^{r_2} a^r b_0^{r_0} b_1^{r_1} b_2^{r_2} = a^{2r} b_{0+r}^{r_0} b_{1+r}^{r_1} b_{2+r}^{r_2} b_0^{r_0} b_1^{r_1} b_2^{r_2}$$

$$\begin{aligned} g^3 &= a^{2r} b_{0+r}^{r_0} b_{1+r}^{r_1} b_{2+r}^{r_2} b_0^{r_0} b_1^{r_1} b_2^{r_2} a^r b_0^{r_0} b_1^{r_1} b_2^{r_2} \\ &= a^{3r} b_{0+2r}^{r_0} b_{1+2r}^{r_1} b_{2+2r}^{r_2} b_{0+r}^{r_0} b_{1+r}^{r_1} b_{2+r}^{r_2} b_0^{r_0} b_1^{r_1} b_2^{r_2} \end{aligned}$$

si $r = 0$, $b_0^{3r_1} b_1^{3r_1} b_2^{3r_2} = 1$ pero ya lo sabemos porque $g \in B$

si $r = 1$, $g^3 = b^{r_0+r_1+r_2} b^{r_0+r_1+r_2} b^{r_0+r_1+r_2} = d^{r_0+r_1+r_2} \in D$

si $r = 2$, $g^3 = b^{r_0+r_1+r_2} b^{r_0+r_1+r_2} b^{r_0+r_1+r_2} = d^{r_0+r_1+r_2} \in D$

COROLARIO 8:

$(a^r b_0^{r_0} b_1^{r_1} b_2^{r_2})^9 = 1$ siempre. Es decir $\exp(G) = 9$

COROLARIO 9:

Si $g = a^r b$ con $b \in B$ entonces $g^3 = 1$

PROPOSICION 3:

$g = a^r b$ es de orden 9 si y sólo si $r \neq 0$ y $b \notin B^\Delta$

DEMOSTRACION:

$\rightarrow$) Supongamos que $o(g) = 9$ entonces $g \notin B$ lo cual implica que $r \neq 0$; entonces

$$g = \left\{ \begin{array}{c} ab = ab_0^{r_0} b_1^{r_1} b_2^{r_2} \\ \text{ó} \\ a^2 b = a^2 b_0^{r_0} b_1^{r_1} b_2^{r_2} \end{array} \right\}$$

En ambos casos $g^3 = (b_0b_1b_2)^{r_0+r_1+r_2}$ y como es de orden 9 entonces $(b_0b_1b_2)^{r_0+r_1+r_2} \neq 1$ $\therefore$ $r_0 + r_1 + r_2 \neq 0$

$\therefore$ $b \notin B^\Delta$

$\leftarrow$) Si $r = 0$ y $b \in B^\Delta$ entonces $o(a^r b) \neq 9$

COROLARIO 10:

$\exp B = \exp F_0 = 3$, $\exp F_1 = \exp F_2 = 9$

Hemos demostrado así la siguiente proposición :

PROPOSICION 4:

$B^\Delta = \{b_0^{r_0}b_1^{r_1}b_2^{r_2} \mid r_0 + r_1 + r_2 = 0\}$

COROLARIO 11:

$[B^\Delta:1] = 9$, $B^\Delta \subset B, F_0, F_1, F_2$ y $B \cap F_i = F_j \cap F_k = B^\Delta$

LEMA 7:

ab es de orden 9 si y sólo si $b \notin B^\Delta$

DEMOSTRACION:

Sea $ab = ab_0^{r_0}b_1^{r_1}b_2^{r_2}$; entonces

$$(ab)^3 = ab_0^{r_0}b_1^{r_1}b_2^{r_2}ab_0^{r_0}b_1^{r_1}b_2^{r_2}ab_0^{r_0}b_1^{r_1}b_2^{r_2} =$$

$$= a^3 b_0^{r_0+r_1+r_2} b_1^{r_0+r_1+r_2} b_2^{r_0+r_1+r_2} =$$

$$= b_0^{r_0+r_1+r_2} b_1^{r_0+r_1+r_2} b_2^{r_0+r_1+r_2} \neq 1$$

$\therefore$ $r_0 + r_1 + r_2 \neq 0$ $\therefore$ $b \notin B^\Delta$.

Se dará una caracterización de todos los subgrupos de G que no estén contenidos en B .

LEMA 8:

$$h \in (B^{\Delta^s} - B^{\Delta^{s+1}}) \rightarrow \langle h, h^a, h^{a^2} \rangle = B^{\Delta^s}$$

DEMOSTRACION:

Si $s = 0$ entonces tenemos que demostrar:

$h \in (B - B^{\Delta}) \quad \rightarrow \quad \langle h, h^a, h^{a^2} \rangle = B^{\Delta^S}$.

Sea $h \in B - B^{\Delta}$ $\therefore$ $h = b_0^{r_0} b_1^{r_1} b_2^{r_2}$ con $r_0 + r_1 + r_2 \neq 0$.

Recordamos entonces que

$h^a = b_0^{r_1} b_1^{r_2} b_2^{r_0}$ y

$h^{a^2} = b_0^{r_2} b_1^{r_0} b_2^{r_1}$

Sea $g \in B$, $g = b_0^{s_0} b_1^{s_1} b_2^{s_2}$; $g \in \langle h, h^a, h^{a^2} \rangle$ si y sólo si existen $x,y,z \in Z_3 \ni g = h^x (h^a)^y (h^{a^2})^z$ si y sólo si tiene solución el sistema siguiente:

$$r_0 x + r_1 y + r_2 z = s_0$$

$$r_1 x + r_2 y + r_0 z = s_1$$

$$r_2 x + r_0 y + r_1 z = s_2$$

y esto pasa ya que su determinante es

$-(r_0^3 + r_1^3 + r_2^3) = -(r_0 + r_1 + r_2)^3 \neq 0$

Si $s = 1$ entonces tenemos que demostrar

$h \in B^{\Delta} - B^{\Delta^2} \quad \rightarrow \quad \langle h, h^a, h^{a^2} \rangle = B^{\Delta}$.

Demostración:

Sea $h \in B^{\Delta} - B^{\Delta^2}$ $\therefore$ $h = b_0^{r_0} b_1^{r_1} b_2^{r_2}$ con $r_0 + r_1 + r_2 = 0$ y no todas iguales ;

se recuerda que:

$h = b_0^{r_0} b_1^{r_1} b_2^{r_2}$

$h^a = b_0^{r_1} b_1^{r_2} b_2^{r_0}$

$h^{a^2} = b_0^{r_2} b_1^{r_0} b_2^{r_1}$

Sea $g = b_0^{s_0} b_1^{s_1} b_2^{s_2} \in B^{\Delta}$; $g \in \langle h, h^a, h^{a^2} \rangle$ si y sólo si existen $x,y,z \in Z_3 \ni g = h^x (h^a)^y (h^{a^2})^z$; lo que pasa, si y sólo si tiene solución el sistema siguiente

$$\begin{cases} r_0x + r_1y + r_2z = s_0 \\ r_1x + r_2y + r_0z = s_1 \\ r_2x + r_0y + r_1z = s_2 \end{cases}$$

Sumando los renglones 1 y 2 al 3 se obtiene

$$\begin{cases} r_0x + r_1y + r_2z = s_0 \\ r_1x + r_2y + r_0z = s_1 \end{cases}$$

Los determinantes de 2x2 de la matriz de los coeficientes son

$r_0r_2 - r_1^2$; $r_0^2 - r_1r_2$; $r_0r_1 - r_2^2$;

como no todas las r´s son iguales existe una diferente de cero. Entonces, la condición de que la suma sea cero obliga que alguna de las otras dos sea cero y por tanto algún determinante de coeficientes es diferente de cero y el sistema tiene solución .

Si s = 2 entonces si $h \in B^{\Delta^2} - \{e\}$; entonces obviamente $\langle h\rangle = B^{\Delta^2}$ $\therefore$ $\langle h,h^a,h^{a^2}\rangle$ genera B^{Δ^2}

LEMA 9;

Sea $F \not\subseteq B$, $H = F \cap B$; entonces existe s $(0 \leq s \leq 3)$ $\ni$ $H = B^{\Delta^s}$

DEMOSTRACION:

Si $H = \{1\}$ entonces $H = B^{\Delta^3}$. Sea ahora $H = \{1\}$; existe s con $0 \leq s \leq 3$ tal que $H \subset B^{\Delta^s} - B^{\Delta^{s+1}}$ $\therefore$ existe $h \in H$ $\ni$ $h \in B^{\Delta^s} - B^{\Delta^{s+1}}$; por demostrar que h^a y h^{a^2} estan en H.

Ya que $F \not\subset B$ entonces existe $a^r b' \in F$ con $r \neq 0$ tal que $g = ab \in F$; entonces $h^a = aha^{-1} = ghg^{-1}$.
Ya que $g \in F$, $h \in B \cap F$ y $g^{-1} \in F$, $ghg^{-1} \in F$ y como B es normal en G y $h \in B \cap F$, $ghg^{-1} \in B$.
Entonces $h^a = ghg^{-1} \in H$. Analogamente para h^{a^2}; por lo tanto, $B^{\Delta^s} = \langle h, h^a, h^{a^2} \rangle \subset H$ y como además $H \subset B^{\Delta^s}$, $H = B^{\Delta^s}$

TEOREMA 7:

F subgrupo de G, $F \not\subset B$ $\rightarrow$ existe $f \in F$ y $s \in \{0,1,2,3\}$ $\ni$ $F = \langle f \rangle B^{\Delta^s}$

DEMOSTRACION:

Sea $\Psi : F \rightarrow A$ $(A = \{1, a, a^2\})$, definida por $\Psi(a^r b) = a^r$; como $a^r b a^s b' = a^{r+s} b''$, Ψ es homomorfismo.
En vista de que $F \not\subset B$, existen elementos de la forma $a^r b \in F$, $r = 0$ $\therefore$ Ψ es epimorfismo ;además $Ker\Psi = B \cap F = B^{\Delta^s}$ y por el primer teorema de isomorfismo $F/B^{\Delta^s} \cong A$
Tomamos cualquier $f \in F$ que sea de la forma $a^r b$, $r \neq 0$; como $f \notin B^{\Delta^s}$ y F/B^{Δ^s} es un grupo de orden 3, F queda partida en las tres clases laterales izquierdas
$F = 1 \cdot B^{\Delta^s} \cup f \cdot B^{\Delta^s} \cup f^2 B^{\Delta^s} = \langle f \rangle B^{\Delta^s}$

OBSERVACIONES:

1. $F_i \not\subset B$ y $F_i \cap B = B^{\Delta}$, $i = 0,1,2$
   $\therefore$ $F_i = \langle f \rangle B^{\Delta}$ en donde f es cualquier elemento de $F_i - B^{\Delta}$ (en particular puede ser $f = ab_n^i$)

2. En el teorema anterior:

$s = 0 \rightarrow \Delta^s = 1$, $B^{\Delta^s} = B$ y $F = G$ ya que B es máximo y $B \subsetneq F$

$s = 1 \rightarrow F = \langle f \rangle B^{\Delta}$, es decir F es un F_i , $i = 0,1,2$ en donde i queda determinada por el grupo máximo al cual pertenezca la f

$s = 2 \rightarrow B^{\Delta^2} = D$ (T.6) y por tanto $F = \langle f \rangle D$, y en éste caso puede suceder que el orden de f sea igual a 9 entonces $f^3 \in D - \{1\}$ $\therefore$ $\langle f \rangle \supset D$ y $\therefore$ $F = \langle f \rangle$, cíclico de orden 9, o bien si $o(f) = 3$ y en ese caso $\langle f \rangle \cap D = \{1\}$ $(F \not\subset B)$ y $\therefore$ $F = \langle f \rangle D$. Finalmente

$s = 3 \rightarrow B^{\Delta^s} = \{1\}$ $\therefore$ $F = \langle f \rangle$, cíclico de órden 3 .

TEOREMA 8:

Sea F cualquier subgrupo de G , $F \not\subset B$. Entonces $f \in F$ y $f \notin B \rightarrow F = \langle f \rangle B^{\Delta^s}$ y se tiene que

si $s = 0$, $F = G$ que no es máximo y si

$s \neq 0$, $\langle f \rangle B^{\Delta^s} \subset \langle f \rangle B^{\Delta} = F_i$ $(i = 0,1,2)$

$\therefore$ $F \subset F_i$ $\therefore$ son los únicos subgrupos máximos y así

$B^{\Delta^0} = B^1 = B \supset B^{\Delta} \supset B^{\Delta^2} = D \supset B^{\Delta^3} = \{1\}$

OBSERVACIONES:

1. $\Psi : G \rightarrow Z_3 \times Z_3$

$$a^r b_0^{r_0} b_1^{r_1} b_2^{r_2} \rightarrow (r, r_0 + r_1 + r_2)$$

es epimorfismo de grupos y

$$Ker \Psi = B^{\Delta}$$

2. Los subgrupos máximos de $Z_3 \times Z_3$ son:

$L = \{(0,s)\}$

$L_0 = \{(r,s) | \quad s = 0 \}$

$L_1 = \{(r,s) | \quad s = r \}$

$L_2 = \{(r,s) | \quad s = 2r \}$

3. $\psi^{-1}(L) = B$

$\psi^{-1}(L_0) = F_0$

$\psi^{-1}(L_1) = F_1$

$\psi^{-1}(L_2) = F_2$

4. REFERENCIAS

[1] H.Cárdenas y E.Lluis. El normalizador del p-subgrupo de Sylow de $\mathcal{S}_{p^2}$. Bol.Soc.Mat.Mex. 1965,p.1-6.

[2] H.Cárdenas y E.Lluis. La red de subgrupos del producto de entrelazamiento $\mathbb{Z}_p \wr \mathbb{Z}_p$. (Por aparecer)

[3] M.L.Kaloujnine. La structure des p-grupes de Sylow des groupes symétriques. Ann.Ec. Normale 3(65),1948,p.239-276.

[4] I.N.Herstein.Topics in Algebra.John Wiley. 1964.