UNIVERSIDAD MICHOACANA DE
SAN NICOLÁS DE HIDALGO

FACULTAD DE CIENCIAS FÍSICO-MATEMÁTICAS
"Mat. Luis M. Rivera Gutiérrez"

"ISOMORFISMOS ENTRE TABLAS DE MARCAS DE GRUPOS DE ORDEN MENOR O IGUAL A 95"

TESIS

PARA OBTENER EL TÍTULO DE:

LICENCIADO EN CIENCIAS FÍSICO-MATEMÁTICAS

PRESENTA:

EDER VIEYRA SÁNCHEZ

ASESOR:

Dr. LUIS VALERO ELIZONDO

MORELIA MICHOACAN, JULIO DE 2009

Dedicatoria

A mi mamá y a mi papá por darme la vida, su cariño, su ejemplo y una carrera para mi futuro.

A mis hermanas Africa y Monica por presionarme a ser mejor cada dia.

A Yuri.

A todos mis amigos Sanzon, Oscar, Cesar, Raul, Memo por todos los buenos y malos momentos que pasamos juntos.

A todos mis profesores y profesoras de fismat, aprendi mucho de todos ustedes.

A mi asesor Luis Valero, muchas gracias por ayudarme con esta tesis con su entusiasmo y sus ideas.

Índice

Resumen

Es un hecho algebraicamente conocido que dados dos grupos tales que sus Tablas de Marcas sean isomorfas, sus Anillos de Burnside son también isomorfos. Tambien es cierto que dados dos grupos no isomorfos, con tablas de marcas no isomorfas sus anillos de Burnside son isomorfos. Esto había sido trabajado por Thevenaz donde propuso como el par de grupos no isomorfos con orden más chico y tal que tienen tablas de marcas isomorfas es $5x11^2$, recientemente se encontró un ejemplo de grupos cuyo orden es 96, esto fue encontrado computacionalmente usando GAP (Groups, Algorithms, Programming), en esta tesis se busca justificar de una manera matemática formal que en grupos cuyo orden sea menor a 96 no hay grupos con esta propiedad.

1. Grupos

1.1. Operaciones binarias

Definición 1.1.1. Sea C un conjunto no vacío. Una **operación binaria** en C es una función $* : C \times C \to C$. Usualmente uno escribe $a * b$ en lugar de $*(a, b)$.

1.1.2. Ejemplos de operaciones binarias

- Los enteros $\mathbb{Z}$ con la operación suma $+$.
- Los naturales $\mathbb{N}$ con el producto *.

Definición 1.3. Sea C un conjunto. Una operación binaria $*$ en C es asociativa si $a * (b * c) = (a * b) * c$ para todos $a, b, c \in C$.

1.2. Semigrupos

Un semigrupo es un par ordenado $(E, *)$, donde E es un conjunto no vacío y $*$ es una operación binaria asociativa en E. Usualmente denotamos un semigrupo $(E, *)$ simplemente por E.

1.2.1. Ejemplos de Semigrupos

- Los enteros $\mathbb{R}$ con la operación suma $+$.
- Los naturales $\mathbb{N}$ con el producto *.

1.3. Grupos

Un grupo G es un semigrupo finito o infinito de elementos con una operación binaria, que contiene un elemento 1 tal que satisface:

1. $1 * g = g = 1 * g$ para todo $g \in G$.
2. para todo $g \in G$, existe un elemento $h \in G$ tal que $h * g = 1 = g * h$, a h se le conoce como el inverso de g y se denota como g^{-1}.

OBSERVACIÓN. Cuando no se preste a mala interpretación en lugar de escribir $h * g$ se escribe hg.

1.3.1. Ejemplos de Grupos

- Sea G un grupo con un solo elemento que es el elemento neutro del grupo, a este grupo se le conoce como grupo trivial.

- Grupos cíclicos. Son aquellos que pueden ser generados por un solo elemento es decir existe un elemento x en G tal que todo elemento de G se puede expresar como una potencia de x.

- Grupos Simétricos. Se llama grupo simétrico de grado n y se denota por S_n al conjunto de todas las permutaciones del conjunto con n elementos $\{1, 2, ..., n\}$ por lo tanto tiene $n!$ elementos.

1.4. Grupos Abelianos

Definición 1.4.1. Dos elementos g y h en un grupo conmutan si $gh = hg$. Decimos que un grupo es abeliano si para todos $g, h \in G$, se tiene que g y h conmutan.

1.4.2. Ejemplos de Grupos abelianos

- Los números reales forman un grupo abeliano con la adición, al igual que los reales no nulos con la multiplicación.

Definición 1.4.3. El centro de un grupo G es el conjunto $Z(G)$ de elementos en G que conmutan con todos los elementos de G, esto es,

$$Z(G) = \{z \in G | gz = zg \, \forall \, g \in G\}$$

Definición 1.4.4. Orden. El orden de un grupo G es el número de elementos de G.

1.5. Teorema de la descomposición de Kronecker

El numero $a(n)$ de Grupos Abelianos finitos no isomorfos de un grupo dado de orden n está dado escribiendo a n como:

$$n = \prod_i p_i^{\alpha_i},$$

donde los p_i son factores primos distintos, y los α_i los exponentes correspondientes entonces:

$$a(n) = \prod_i P(\alpha_i)$$

Donde $P(n)$ es la función partición. La cual consiste en escribir el numero de formas en que se puede escribir un entero n como suma de enteros positivos donde el orden de los sumandos no importa.

Ejemplo de función partición: sea $n = 4$

1. $4 = 4$;
2. $4 = 3 + 1$;
3. $4 = 2 + 2$;
4. $4 = 2 + 1 + 1$;
5. $4 = 1 + 1 + 1 + 1$;

Por lo tanto se sigue que $P(4) = 5$;

Ejemplo de numero de grupos no abelianos de orden n: calcule numero de grupos abelianos no isomorfos del grupo de orden 12.

Utilizando el teorema de la descomposición de Kronecker tenemos que $12 = 2^2 \times 3^1$ de donde, los exponentes son $\alpha_1 = 2$ y $\alpha_2 = 1$.

Y donde $P(2) = 2$ y $P(1) = 1$

Por lo tanto $a(12) = 2 \times 1 = 2$

1.6. Subgrupos

Definición 1.6.1. Un subconjunto no vacío S de un grupo G es un subgrupo de G si para todos $g, h \in S$ se tiene que g^{-1} y gh están en S. Si S es un subgrupo de G, lo denotamos $S \leq G$. Decimos que S es un subgrupo propio de G si $S \leq G$ y $S \neq G$, y lo denotamos $S < G$. Para algunos autores $S < G$ significa que S es un subgrupo de G (que puede o no ser propio).

Definición 1.6.2. Sean G un grupo y N un subgrupo de G. Decimos que N es un subgrupo normal de G, denotado $N \trianglelefteq G$, si $gNg^{-1} = N$ para toda $g \in G$. La notación $N \triangleleft G$ significa que N es un subgrupo normal de G distinto de G.

1.7. P-Grupos

Definición 1.7.1. Decimos que G es un p-grupo si el orden de cada elemento de G es una potencia de p siendo p un numero primo.

Teorema 1.7.2 Todo p-grupo tiene centro no trivial

Demostración: Por Lagrange el orden de cualquier subgrupo H de un grupo G debe dividir el orden de G, se sigue que cada subgrupo de G que denotamos H_i tiene como orden una potencia de $p^{k_i}, 0 < k_i < n$, pero la ecuación de clase requiere que $|G| = p^n = |Z(G)| + \sum_i (p^{k_i})$. Vemos que p debe dividir a $Z(G)$ por lo cual $|Z(G)| > 1$.

1.8. Anillos

Definición 1.8.1 Sea A un conjunto, y sean $+$ y $\cdot$ dos operación matemática operaciones binarias. Se dirá que la terna $(A, +, \cdot)$ es un "'anillo"' si se cumplen las siguientes propiedades:

$(A, +)$ es un grupo abeliano, esto es, se cumple que:

1. $\forall a, b \in A, a + b \in A$ (clausura).
2. $\forall a, b \in A, a + b = b + a$ (conmutatividad).
3. $\forall a, b, c \in A, a + (b + c) = (a + b) + c$ (asociatividad).
4. $\exists 0 \in A$, tal que $\forall a \in A, 0 + a = a + 0 = a$ (elemento neutro).
5. $\forall a \in A, \exists b \in A$ tal que $a + b = b + a = 0$. Al elemento b se le llama opuesto de a, y se le denota usualmente por $-a$, de modo que la propiedad anterior se anota también como $a + (-a) = (-a) + a = 0$ (elemento inverso).

$(A, .)$ cumple que:

1. $\forall a, b, c \in A, a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (asociatividad).

2. $\forall a, b, c \in A, a \cdot (b + c) = a \cdot b + a \cdot c \quad$ y $\quad (b + c) \cdot a = b \cdot a + c \cdot a$ (propiedad distributiva de $\cdot$ respecto de $+$).

$(A, +)$ y $(A, \cdot)$ se les denomina la suma y el producto, respectivamente, del anillo A. Asimismo, al neutro de la suma suele denominársele ”’cero”’ del anillo.

Leyes de simplificación: Si $a \neq 0$, se dice que se verifican las leyes de simplificación: si $a \cdot b = a \cdot c$ implica que $b = c$; de la misma forma, $b \cdot a = c \cdot a$ implica que $b = c$.

2. Homomorfismos y Automorfismos de Grupos

2.1. Homomorfismo de Grupos

Dados dos grupos $(G, *)$ y $(H, \cdot)$ un homomorfismo de grupos de $(G, *)$ a $(H, \cdot)$ es una función $\varphi : G \rightarrow H$ tal que para todo u y v en G se tiene que:

$$\varphi(u * v) = \varphi(u) \cdot \varphi(v)$$

Donde la operación del lado derecho de la ecuación $(*)$ es la de G y la del lado izquierdo $(\cdot)$ es la de H.

Deducimos que h mapea el elemento identidad e_G de G al elemento identidad e_H de H, y además mapea inversos en inversos esto es $\varphi(u^{-1}) = \varphi(u)^{-1}$.

Se dice que φ es un monomorfismo si es inyectivo, un epimorfismo si es suprayectivo, y un isomorfismo si es biyectivo.

2.2. Automorfismo de Grupos

Un automorfismo de un grupo es un isomorfismo del grupo en sí mismo.

2.3. Automorfismos de un Espacio Vectorial

Definamos primero un espacio vectorial. Sea F un campo. Un espacio vectorial V sobre F es un conjunto con dos operaciones, $+ : V \times V \longrightarrow V$ y $\cdot : F \times V \longrightarrow V$, tales que:

1. $(u+v)+w = u+(v+w)$ para toda u, v, $w \in V$
2. $u+v = v+u$ para todo $u, v \in V$
3. Existe un elemento $0 \in V$ tal que $u+0 = u$ para todo $u \in V$
4. Para todo $u \in V$, existe un elemento $v \in V$ tal que $u+v = 0$
5. $a \cdot (b \cdot u) = (a \cdot b) \cdot u$ para todo $a, b \in F$ y $u \in V$
6. $1 \cdot u = u$ para todo $u \in V$
7. $a \cdot (u+v) = (a \cdot u) + (a \cdot v)$ para todo $a \in F$ y $u, v \in V$
8. $(a+b) \cdot u = (a \cdot u) + (b \cdot u)$ para todo $a, b \in F$ y $u \in V$

Observación: Todo espacio vectorial es un grupo con $\cdot$, ya que cumple todas las propiedades de este.

Dado un espacio vectorial V, el grupo $GL(V)$ se define como el grupo de transformaciones lineales invertibles de V a V. Cuya operación del grupo se define por la composición: dados $T : V \longrightarrow V$ y $T' : V \longrightarrow V$ en $GL(V)$, el producto TT' es la composición de los mapeos de T y T'

Si $V = \mathbb{F}^n$ para algún campo $\mathbb{F}$, entonces el grupo $GL(V)$ es denotado comúnmente por $GL(n, \mathbb{F})$. En este caso si se identifica cada transformación lineal $T : V \longrightarrow V$ con su matriz, respecto a su base estándar, este grupo se convierte en el grupo de matrices invertibles de tamaño $n \times n$, bajo la operación de grupo de producto de matrices.

2.4. Automorfismos de un Grupo Cíclico

Teorema 2.4.1. Si G es un grupo cíclico de orden p con p primo, entonces $Aut(C_p) \cong C_{p-1}$

Demostración: Sea x el generador de G con orden p, cualquier automorfismo de este grupo tiene que ser de la forma $f_n(x) = x^n$ para algún entero $0 \leq n < p$. Nótese que esta función es un automorfismo para todo $0 < n < p$

dado p primo. Así que el el grupo de automorfismos es $\{f_1, f_2, ..., f_{p-1}\}$ por lo que tiene $p-1$ elementos que es su orden. Para ver que es cíclico, úsese el hecho de que p tiene al menos una raíz primitiva por ser primo, sea k esta raíz y nótese que f_k genera el grupo de automorfismos. Por lo tanto, $Aut(C_p) \cong C_{p-1}$.

2.5. Automorfismos de C_{2^n}

Definición 2.5.1. Llamemos grupo de unidades $U(R)$ de un anillo R al siguiente conjunto,

$$U(R) = \{r \in R | \exists s \in \mathbb{R}, \text{con}\, sr = 1 = rs\}.$$

Lema 2.5.2. Si G es un grupo cíclico de orden n, entonces $Aut(G) \cong U(C_n)$

Demostración: Sea $G = \langle a \rangle$, si $\varphi \in Aut(G)$, entonces $\varphi(a) = a^k$ para algún k; más aún a^k es un generador de G; por lo tanto, k y n son primos relativos $(k, n) = 1$ y $[k] \in U(C_n)$ denotando por $[k]$ a la clase de k. No es difícil ver que $\Theta : Aut(G) \to U(C_n)$, definido por $\Theta(\varphi) = [k]$ es un isomorfismo.

Teorema 2.5.3. $Aut(C_2) \cong 1$; $Aut(C_4) \cong C_2$; si $m \geq 3$, entonces $Aut(C_{2^n}) \cong C_2 \times C_{2^{n-2}}$.

Entonces $U(C_2) = 1$ y $U(C_4) = \{[1], [3]\} \cong C_2$

Si $m \geq 3$, entonces

$$U(C_{2^n}) = \langle [-1], [5] \rangle \cong C_2 \times C_{2^{m-2}}$$

Demostración: Aplicando un resultado conocido de la función de Euler a nuestro caso tenemos $|U(C_{2^n})| = \varphi(2^m) = 2^{m-1}$, por inducción y aplicando el teorema del binomio tenemos que

$$5^{2^{m-3}} = (1+4)^{2^{m-3}} \equiv 1 + 2^{m-1}\,(mod\,2^m)$$

Dado que $U(C^{2^m})$ es un 2-grupo, [5] tiene orden 2^s, para algún $s \geq m-2$ (pues si no, tendríamos que $1 + 2^{m-1} \not\equiv 1(mod\,2^m)$. Claramente $[-1]$ tiene orden 2. Aseguramos también que $< [5] > \cap < [-1] >= 1$. Si no lo fuese, entonces $[5^t] = [-1]$ para algún t; esto es $5^t \equiv -1(mod\,2^m)$. Dado $m \geq 3$, esta congruencia implica $5^t \equiv\; -1(mod\,4)$; pero sabemos que $5 = 1(mod\,4)$ lo cual implica $5^t \equiv 1(mod\,4)$, lo cual es una contradicción pues es congruente con 1 y -1. Se sigue que este par de subgrupos cíclicos generan su producto directo, el cual es un subgrupo de orden al menos $2 \times 2^s \geq 2 \times 2^{m-2} = 2^{m-1} = \varphi(2^m)$. por lo tanto este subgrupo son todas las unidades de C_{2^m}

2.6. Automorfismos de C_{p^n} con p primo diferente a 2

Teorema 2.6.1 Si p es un primo diferente de 2, entonces $Aut(C_{p^n}) \cong C_l$ donde $l = (p-1)p^{n-1}$.

Demostración Sea p un primo distinto de 2 (que es el caso que ya calculamos) entonces tenemos que el grupo multiplicativo,

$G = U(C_{p^n}) = \{[a] \in C_{p^n} |\, (a,p) = 1\}$, es cíclico de orden $(p-1)p^{n-1}$.

El caso de $n = 1$ ya está demostrado, así que supongamos $n \geq 2$. De nuevo por la función de Euler sabemos que $|U(C_{p^n})| = \varphi(p^n) = (p-1)p^{n-1}$.

Es fácil ver que $B = \{[b] \in G | b \cong 1 mod\, p\}$ es un subgrupo de G. Y cada elemento entero b tiene una expresión única en base de p: Si $1 \leq b < p^n$, entonces

$b = a_0 + a_1 p + ... + a_{n-1}p^{n-1}$ donde $0 \leq a < p$

Dado que $[b] \in B$ si y sólo si $a_0 = 1$ (para que se de la congruencia módulo 1), se sigue que $|B| = p^{n-1}$, y por lo tanto B es p-primario (p-grupo abeliano). Por la descomposición primaria (lo podemos descomponer en producto de grupos cíclicos), existe un subgrupo A de G con $|A| = p-1$ y con $G = A \times B$. Ahora si mostramos que si A y B son cíclicos, podemos concluir que G es cíclico ya que el orden de A es primo relativo con el orden de B.

Considérese $\theta : G \to U(C_p)$ definida por $\Theta([a]) = class(a)$ (haciendo notar la diferencia, $[a]$ denota la clase de congruencias de a modulo p^n, y $class(a)$ denota las clase de congruencia de a modulo p). Claramente, Θ es suprayectiva y $ker\Theta = B$, por lo que $G/B \cong U(C_p) \cong C_{p-1}$. Por otro lado, $G/B = (A \times B)/B \cong A$, y por lo tanto $A \cong C_{p-1}$.

Ahora demostremos que B es cíclico, para esto demostremos que $[1+p]$ es un generador. Probemos por inducción sobre $m \geq 0$ que

$(1+p)^{p^m} \equiv 1(\, mod\, p^{m+1})$ y que $(1+p)^{p^m} \not\equiv 1(\, mod\, p^{m+2})$.

Si $m = 0$, entonces $1 + p \equiv 1(mod\, p)$ y $1 + p \not\equiv 1\,(mod\, p^2)$. Dando el paso inductivo para $m+1$, la congruencia queda $(1+p)^{p^{m+1}} = ((1+p)^{p^m}))^p = (1+kp^{m+1})^p$, para algún entero k; la incongruencia asumida nos da que $p \nmid k$. El teorema del binomio implica que $(1+kp^{m+1})^p = 1 + kp^{m+2} + lp^{m+3}$ para algún l. Por lo tanto $(1+p)^{p^{m+1}} \equiv 1\,(mod\, p^{m+2})$ y $(1+p)^{p^{m+1}} \not\equiv 1\,(mod\, p^{m+3})$. Concluimos que $(1+p)^{p^{n-2}} \not\equiv 1\,(mod\, p^n)$, y por lo tanto $[1+p]$ tiene orden p^{n-1}.

2.7. Producto de automorfismos $Aut(H \times K)$ con $(H, K) = 1$

El siguiente resultado es importante pues es fundamental para la ultima parte de esta tesis.

Teorema 2.7.1. Sea $G = H \times K$ el producto de grupos H y K, tales que sus órdenes son primos relativos, entonces se cumple que:

$$Aut(H) \times Aut(K) \cong Aut(H \times K)$$

.

Demostración: Para ella exhibiremos un homomorfismo $\phi : Aut(H) \times Aut(K) \to Aut(H \times K)$ de la manera siguiente. Sea $\alpha \in Aut(H)$ y $\beta \in Aut(K)$. Entonces, un automorfismo $\phi(\alpha, \beta)$ de $H \times K$ está dado por

$$\phi(\alpha, \beta)(h, k) = (\alpha(h), \beta(k))$$

Sea $id_H \in Aut(H)$ y $id_k \in Aut(K)$ automorfismo identidad de H y K, respectivamente. Para probar que ϕ es un homomorfismo, notemos que $\phi(id_H, id_k) = id_{H\times K}$ y también que

$$\phi(\alpha_1\alpha_2, \beta_1\beta_2)(h,k) = (\alpha_1\alpha_2(h), \beta_1\beta_2(k)) = \phi(\alpha_1,\beta_1)\phi(\alpha_2,\beta_2)(h,k),$$

para toda $\alpha_1, \alpha_2 \in Aut(H)$, $\beta_1, \beta_2 \in Aut(K)$, y $h \in H$, $k \in K$.

Ahora verifiquemos que ϕ es un isomorfismo. Claramente ϕ es inyectiva; así que veamos si es suprayectiva. Sea $n = |H|$, $m = |K|$, y tomemos π_H y π_K el homomorfismo estándar de proyección $\pi_H : H \times K \to H$ y $\pi_K : H \times K \to K$. Fijemos $\omega \in Aut(H \times K$ y consideremos el homomorfismo $\gamma : K \to H$ dado por $\gamma(k) = \pi_H(\omega(1_H, k))$, en donde 1_H es el elemento identidad de H. Nótese que $\{k^n | k \in K\} \subseteq ker\,\gamma$ pues

$$1_H = \pi_H(\omega(1_H,k))^n = \pi_H(\omega(1_H,k)^n) = \pi_H(\omega(1_H,k^n)) = \gamma(k^n).$$

Además, como m y n son primos relativos, el conjunto $\{k^n | k \in K\}$ consiste de m elementos. Consecuentemente, se sigue que $ker\,\gamma = K$ y γ es el homomorfismo trivial. Similarmente, $\delta : H \to K$ dada por $\delta(h) = \pi_K(\omega(h, 1_K))$ es trivial.

Finalmente, definimos endomorfismos de H y K como sigue:

$$\omega_H(h) = \pi_H(\omega(h,1_k)), \omega_K(k) = \pi_K(\omega(1_H,k)).$$

De está construcción y los argumentos ya mencionados, tenemos

$$\omega(h,k) = \omega(h,1_K)\cdot\omega(1_H,k) = (\omega_H(h), \omega_K(k)) = \phi(\omega_H,\omega_K)(h,k)$$

para toda $h \in H$ y $k \in K$. Sólo falta hacer ver que $\omega_H \in Aut(H)$ y $\omega_K \in Aut(K)$, y para esto basta que ω_H y ω_K son inyectivas, supongamos que $\omega_H(h) = 1_H$ para algún $h \in H$. Entonces $\omega(h, 1_K) = (\omega_H(h), \omega_K(1_K)) = (1_H, 1_K)$, y así $h = 1_H$ por inyectividad de ω. Con un argumento similar se demuestra que $\omega_K \in Aut(K)$, y esto completa nuestra prueba.

3. Producto Semidirecto

Definición 3.0.1 Producto Semidirecto. Sea G un grupo tal que

1. $N \trianglelefteq G$, N subgrupo normal de G.
2. $H \leq G$, H subgrupo de G.

Decimos que G es un producto semidirecto de N y H si

a). $N \bigcap H = \{1\}$

b). $G = NH = \{nh | n \in N, h \in H\}$

Y lo denotamos como $N \rtimes H$.

Los productos semidirectos son una forma de construir grupos no abelianos.

3.0.2. Ejemplo de Producto semidirecto

Sean $N = X \times 1$, $H = 1 \times Y$; tenemos que:

- $N \bigcap H = \{1\}$, y
- $(x, 1)(1, y) = (x, y) = NH = G$

3.1. Productos Semidirectos y Homomorfismos de Grupos

Sea G un producto semidirecto de N y H. Con $Aut(N)$ denotando el grupo de todos los automorfismos de N. El mapeo $\varphi : H \to Aut(N)$ definido por $\varphi(h) = \varphi_h$ donde $\varphi_h(n) = hnh^{-1}$ para toda h en H y n en N es un homomorfismo de grupos. Juntos N, H y φ determinan G salvo isomorfismo como se muestra a continuación.

Dados cualesquiera dos grupos N y H (no necesariamente subgrupos de un grupo dado) y un homomorfismo de grupos $\varphi : H \to Aut(N)$, el nuevo grupo $N \rtimes_\varphi H$ se llama producto semidirecto de N y H con respecto a φ. Como conjunto, $N \rtimes_\varphi H$ se define como el producto cartesiano $N \times H$. La multiplicación de elemento en el producto cartesiano está determinada por el homomorfismo φ, con el operador $*$ definido por

$$(n_1, h_1) * (n_2, h_2) = (n_1\varphi_{h1}(n_2), h_1h_2)$$

Para toda n_1, n_2 en N y h_1, h_2 en H. Este es un grupo en el cual el elemento identidad es (e_N, e_H) y el inverso del elemento (n, h) es $(\varphi_{h^{-1}}(n^{-1}), h^{-1})$: Los pares (n, e_H) forman un subgrupo normal isomorfo a N, mientras que los pares (e_N, n) forman un subgrupo isomorfo a H. El grupo completo es un producto semidirecto de estos dos subgrupos en el sentido que se acaba de dar.

Inversamente supóngase que tenemos un grupo G con un subgrupo normal N, y un subgrupo H y tal que todo elemento g en G se escribe únicamente de la forma $g = nh$ donde $n \in N$ y $h \in H$. Sea $\varphi : H \to Aut(N)$ un homomorfismo dado por $\varphi(h) = \varphi_h$ donde:

$$\varphi_h(n) = hnh^{-1}$$

para toda $n \in N$ y $h \in H$. Entonces G es isomorfo al producto semidirecto $N \rtimes_\varphi H$; este isomorfismo manda al producto nh a la tupla (n, h). En G tenemos la siguiente regla para la multiplicación

$$(n_1h_1)(n_2h_2) = (n_1(h_1n_2h_1^{-1}))(h_1h_2)$$

que como ya bien vimos es isomorfa a operar las tuplas.

$$((n_1h_1),(n_2h_2)) = (n_1(h_1n_2h_1^{-1}),h_1h_2)$$

4. Otros tipo de representación de grupos

Utilizando el *teorema fundamental de los grupos abelianos* [4] afirma que todo grupo abeliano finitamente generado es isomorfo al producto directo de un número finito de grupos cíclicos. También vimos los productos semidirectos, donde estos últimos generan grupos no abelianos, más aún existen otros grupos que son no abelianos y que no son productos semidirectos.

4.1. Grupo simétrico

Dado un conjunto finito con todos sus elementos diferentes, llamamos permutación a cada una de las posibles ordenaciones de los elementos de dicho conjunto.

Por ejemplo, en el conjunto $\{1,2,3\}$, cada ordenación posible de sus elementos, sin repetirlos, es una permutación. Existe un total de 6 permutaciones para estos elementos: "$1,2,3$", "$1,3,2$", "$2,1,3$", "$2,3,1$", "$3,1,2$"y"$3,2,1$". Claramente una permutación es una función biyectiva.

Se llama grupo simétrico de orden n al conjunto de todas las permutaciones de orden n y se denota por S_n, y este conjunto forma un grupo con la ley de composición de las funciones, dado que la operación composición es siempre asociativa. La biyección trivial que asigna al elemento X en sí mismo funciona como identidad del grupo. Y toda biyección tiene una función inversa que deshace la acción, y por lo tanto cada elemento del grupo simétrico tiene un inverso.

El orden de un grupo simétrico S_n es $n!$, y por lo tanto sólo nos interesan los grupos cuyo $n \leq 4$, que están perfectamente clasificados y cumplen lo siguiente.

- $S_1 = \{id\} \cong C_1$ es abeliano.
- $S_2 = \{id, s\} \cong C_2$ es abeliano.
- $S_3 = \{id, r, r^2, s, sr, sr^2\} \cong C_2 \rtimes C_3$ grupo no abeliano.
- S_4 grupo no abeliano sin ninguna caracterización especial.

Una transposición es una permutación que intercambia dos elementos y mantiene a los demás fijos: por ejemplo el intercambiar solo dos elementos de un conjunto $(1\,3)$. Toda permutación puede ser escrita como producto de transposiciones; por ejemplo, la permutación $(1\,2\,3)(3\,4)$ puede ser escrita como $(1\,5)(1\,2)(3\,4)$. Y dado que puede ser escrita como un producto impar de transposiciones, la llamaremos permutación impar, y si se puede escribir como producto de un numero par de transposiciones, la llamares transposición par, por ejemplo $(1\,3)(4\,5)$.

4.2. Grupo alternante

El grupo alternante A_n es el grupo de permutaciones pares de un conjunto finito. El grupo alternante del conjunto $\{1, ..., n\}$ es llamado el grupo alternante de grado n.

El grupo alternante, es un subgrupo normal del grupo de permutaciones y tiene orden $n!/2$, por lo tanto sólo estudiaremos en está tesis hasta A_5.

Para $n \leq 3$ A_n es abeliano, los otros grupos A_4 y A_5 tienen las siguientes propiedades.

$$A_4 \cong (C_2 \times C_2) \rtimes C_3$$

Y A_5 tiene la propiedad de ser el grupo simple no abeliano, más pequeño, y el grupo de orden más chico no soluble. El ser soluble significa que un grupo que tenga una serie normal (es decir una secuencia de subgrupos normales A_n que cumplen $1 = A_0 \leq A_1 \leq \cdots \leq A_n = G$) tal que cada factor normal es abeliano.

4.3. Cuaternios y Cuaternios Generalizados

Los cuaternios son un anillo con división no conmutativo, son una extensión natural de los números complejos. Como estos, tienen una parte real, sin embargo, los cuaternios tienen tres partes imaginarias, con la propiedad de que $i^2 = j^2 = k^2 = ijk = -1$,

Un grupo es llamado cuaternio generalizado si tiene como representación

$\langle x, y | x^{2^{n-1}} = 1, x^{2^{n-2}} = y^2, yxy^{-1} = x^{-1} \rangle$ con $n \geq 3$

Los cuaternios generalizados tienen la propiedad de que todo subgrupo abeliano es cíclico. Y también tienen la propiedad de que todo p-grupo finito en donde hay un único subgrupo de orden p es cíclico o cuaternio generalizado.

5. Anillos de Burnside

5.1. Semianillos y anillo de Burnside

Lema 5.0.1 Sean X, Y G-conjuntos. La unión disjunta $X \sqcup Y$ es un G-conjunto con la acción ya existente de G a X y Y. También el producto cartesiano $X \times Y$ es un G-conjunto con la acción de G dada por $g \cdot (x, y) = (g \cdot x, g \cdot y)$.

Demostración. Sea $a \in X \sqcup Y$, si $a \in X$ entonces

1. $(gh) \cdot a = g \cdot (h \cdot a)$
2. $1 \cdot a = a$

Por la razón de que X es un G-Conjunto, tenemos también, que si $a \in Y$

- $(gh) \cdot (x, y) = ((gh) \cdot x, (gh) \cdot y)$=$(g \cdot (h \cdot x), g \cdot (h \cdot y))$=

  $= g \cdot (h \cdot x, h \cdot y)$=$g \cdot (h \cdot (x, y))$

  y tenemos que,
- $1 \cdot (x, y)$=$(1 \cdot x, 1 \cdot y) = (x, y)$

Definición 5.0.2. Sea C un conjunto y dos operaciones binarias $+, \cdot$, decimos que $S = (C, +, *)$ es un semianillo si S es tal que satisface las siguientes condiciones:

1. Asociatividad de la suma: $\forall a, b, c \in S$,

$$(a + b) + c = a + (b + c).$$

2. Conmutatividad de la suma: $\forall a, b, c \in S$

$$a + b = b + a.$$

3. Asociatividad del producto: $\forall a, b, c \in S$

$$(a * b) * c = a * (b * c).$$

4. Distributividad: $\forall a, b, c \in S$

$$a * (b + c) = (a * b) + (a * c),$$

$$(b + c) * a = (b * a) + (c * a).$$

Definición 5.0.3. Si S es un semianillo y además le exigimos las siguientes condiciones,

5. Existencia del neutro aditivo: $\exists 0 \in S \ \forall \ a \in S$

$$a + 0 = 0 + a = a$$

6. Existencia del neutro multiplicativo: $\exists 1 \in S \ \forall \ a \in S$,

$$a * 1 = 1 * a = a$$

7. Cancelación: $\forall \, a, b \in S, \ a + b = a + c \Rightarrow b = c$

8. Conmutatividad del producto: $\forall \, a, b \in S$,

$$a * b = b * a.$$

9. $\exists 0 \in S$ tal que si $a \in S$, $a * 0 = 0 * a = 0$.

entonces S es un **Semianillo conmutativo** con 1 y cancelación.

Ejemplos.

1. El ejemplo más simple y no trivial de un semianillo es $\mathbb{N}$, lo números naturales incluyendo al 0, con la suma y producto ordinarios.

2. Todo anillo es un semianillo.

La diferencia entre un anillo y un subanillo, es que un subanillo es un anillo sin substracción.

Lema 5.0.4. Sea S un semianillo conmutativo con 1. Sea $A_1 = S \times S$, intuitivamente $(a, b) = a - b$. Tomemos $\sim$ como la relación de equivalencia dada por

- $(a, b) \sim (c, d) \Rightarrow a + d = b + c$

  donde naturalmente $a - b = c - d$.

  Sea $A = A_1/\sim$. Procedamos a definir $+$ y $\cdot$ en A como

- $(a, b) + (c, d) = (a + c, b + d)$
- $(a, b) \cdot (c, d) = (ac + bd, bc + ad)$

Entonces $+$ y $\cdot$ están bien definidas $(A, +, \cdot)$ es un anillo conmutativo con 1. Además S está metido en A por

$a \mapsto (a + x, x)$ para un x fijo.

$\triangleright$ Demostremos que $\sim$ es de equivalencia

- Reflexiva. $(a, b) \sim (a, b)$ claramente pues $a + b = a + b$.
- Simetría. Si $(a, b) \sim (c, d)$ entonces $(c, d) \sim (a, b)$.

  $(a, b) \sim (c, d) \Rightarrow a + d = b + c =$ y dado que a, b están en un semianillo y conmutan $= c + b = d + a \Rightarrow (c, d) \sim (a, b)$.
- Transitividad. Si $(a, b) \sim (c, d)$ y $(c, d) \sim (x, y)$ entonces $(a, b) \sim (x, y)$

$$(a, b) \sim (c, d) \Rightarrow a + d = b + c,$$

$$(c,d) \sim (x,y) \Rightarrow c + y = d + x.$$

Sumando ambas ecuaciones tenemos:

$a + d + c + y = b + c + d + x$ y cancelando tenemos

$a + y = b + x$ que es equivalente a $(a,b) \sim (x,y)$.

▷ Demostremos que la suma $+$ está bien definida.

Si $(a,b) \sim (a',b')$ y $(c,d) \sim (c',d') \Rightarrow (a,b) + (c,d) = (a+c, b+d) \sim (a'+c', b'+d') = (a',b') + (c',d')$.

Tenemos que

$$(a,b) \sim (a',b') \Rightarrow a + b' = b + a',$$

$$(c,d) \sim (c',d') \Rightarrow c + d' = d + c'.$$

sumando ambas ecuaciones tenemos,

$$(a+b') + (c+d') = (b+a') + (d+c')$$

$$a + b' + c + d' = b + a' + d + c'$$

$$(a+c) + (b'+d') = (b+d) + (a+c') = (a+c') + (b+d)$$

$$\Rightarrow (a+c, b+d) \sim (a',b') + (c',d')$$

▷ Demostremos que el producto $\cdot$ está bien definido esto es $(a,b) \cdot (c,d) = (ac+bd, bc+ad) \sim (a',b') \cdot (c',d') = (a'c' + b'd', b'c' + a'd')$, con $(a,b) \sim (a',b')$ y $(c,d) \sim (c',d')$.

Observemos primero que $(a,b)\cdot(c,d) = (ac+bd, bc+ad) \sim (a',b')\cdot(c,d) = (a'c+b'd, b'c+a'd)$ pues

$$ac+bd+a'd+b'c =$$

$$= (b+a')d + (a+b')c =$$

$$= (a'+b)c + (a+b')d =$$

$$= ad+bc+a'c+b'd$$

Luego

$$(a',b')\cdot(c,d) =$$

$$= (a'c+b'd, b'c+a'd) \sim (a',b')\cdot(c',d') =$$

$$= (a'c'+b'd', b'c'+a'd')$$

Y dado que

$$a'c+b'd+b'c'+a'd' =$$

$$= a'(c+d') + b'(c'+d) =$$

$$= a'(c'+d) + b'(c+d') =$$

$$= a'd+b'c+a'c'+b'd'$$

▷ Demostremos que la suma $+$ es asociativa $((a,b)+(c,d))+(x,y) = (a,b)+((c,d)+(x,y))$.

$$((a,b)+(c,d))+(x,y) =$$

$$= (a+c, b+d) + (x,y) =$$

$$= ((a+c)+x, (b+d)+y) =$$

$$(a+(c+x), b+(d+y))$$

$$(a,b) + (c+x, d+y)$$

$$(a+b) + ((c,d)+(x,y))$$

▷ Demostremos que la suma $+$ es conmutativa.

$$(a,b)+(c,d) = (a+c, b+d) = (c+a, d+b) = (c,d)+(a,b)$$

▷ La suma $+$ tiene neutro dado por $(a,a) = a - a = 0$ para cualquier $a \in S$

$$(a,a)+(c,d) = (a+c, a+d) = a+c-(a+d) = c-d = (c,d)$$

▷ La suma $+$ tiene inversos, $-(a,b) = (b,a)$ es el inverso de (a,b) para todo $a, b \in S$

$$(a,b)+(b,a) = (a+b, b+a) = a+b-(b+a) = 0$$

▷ El producto $\cdot$ es asociativo, $((a,b)\cdot(c,d))\cdot(x,y) = (a,b)\cdot((c,d)\cdot(x,y))$

$$((a,b)\cdot(c,d)\cdot(x,y)) =$$

$$= (ac+bd, bc+ad)\cdot(x,y) =$$

$$= ((ac+bd)x + (ad+bc)y, (ac+bd)y + (ad+bd)x) =$$

$$= (acx + bdx + ady + bcy, acy + bdy + adx + bcx) =$$

$$= (a(cx + dy) + b(cy + dx), b(cx + dy) + a(cy + dx)) =$$

$$= (a, b) \cdot (cx + dy, cy + dx) =$$

$$(a, b) \cdot ((c, d) \cdot (x, y))$$

▷ El producto $\cdot$ es conmutativo.

$$(a, b) \cdot (c, d) =$$

$$= (ac + bd, bc + ad) =$$

$$= (ca + db, da + cb) =$$

$$= (c, d) \cdot (a, b)$$

▷ El producto $\cdot$ tiene neutro dado por $(1 + x, x)$ para cualquier $x \in S$

$$(a, b) \cdot (1 + x, x) =$$

$$= (a(1 + x) + bx, ax + b(1 + x)) =$$

$$= (a + (ax + bx), b + (ax + bx)) = (a, b) + (ax + bx, ax + bx) \sim (a, b)$$

▷ El producto $\cdot$ distribuye a la suma $+$. $(a, b) \cdot ((c, d) + (x, y)) = (a, b) \cdot (c, d) + (a, b) \cdot (x, y)$

$$(a, b) \cdot ((c, d) + (x, y)) =$$

$$= (a, b) \cdot (c + x, d + y) =$$

$$= (a(c + x) + b(d + y), a(d + y) + b(c + x)) =$$

$$= ((ac + bd) + (ax + by), (ad + bc) + (ay + bx)) =$$

$$= (ac + bd, bc + ad) + (ax + by, bx + ay) =$$

$$(a, b) \cdot (c, d) + (a, b) \cdot (x, y)$$

Además, $f : S \to A$, $f(a) = (a + x, x)$ es homomorfismo inyectivo. $f(a+b) = (a+b+x, x) \sim (a+x+b+x, x+x) = (a+x, x) + (b+x, x) = f(a)+f(b)$ y $f(ab) = (ab+x, x) \sim (ab+ax+bx+2x^2+x, ax+bx+2x^2+x) \sim ((a+x)(b+x)+x^2, (a+x)x+(b+x)x) = (a+x, x)\cdot(b+x, x) = f(a)\cdot f(b)$

Observación. Sean X, Y conjuntos finitos, entonces $\#(X \sqcup Y) = \#X \sqcup \#Y$ y $\#(X \times Y) = \#(X)\#(Y)$. Lo mismo se cumple para el número de órbitas de $X \sqcup Y$ y $X \times Y$

Lema 5.0.5. Sean X, Y G-conjuntos. X es isomorfo a Y como G-conjuntos si y sólo si tienen el mismo número de orbitas y existe una asignación biyectiva de estas tal que a cada órbita de X le corresponde una órbita de Y y son isomorfas como G-conjuntos.

Demostración. Si X y Y son isomorfos como G-conjuntos con isomorfismo f, entonces tienen el mismo número de órbitas ya asignación de órbitas está dada por f. Al contrario, si tenemos la segunda condición, tenemos $G \cdot x_1, G \cdot x_2, ..., G \cdot x_n$ y $G \cdot y_1, G \cdot y_2, ..., G \cdot y_n$ las correspondientes orbitas de X y de Y, entonces definimos $\forall 1 \leq i \leq n f(x_i) = y_i$ y extendiéndolo en todo X como $f(g \cdot x) = g \cdot f(x)$, el cual es claramente un isomorfismo de G-conjuntos.

Lema 5.0.6. Las clases de isomorfismo de G-conjuntos finitos junto con la ó disjunta y el producto cartesiano forman un semianillo conmutativo con 1 denotado por $B^+(G)$, donde el neutro de la unión disjunta es $\emptyset$ y el neutro del producto cartesiano es G/G

1. $(X \sqcup Y) \sqcup Z \cong X \sqcup (Y \sqcup Z)$
2. $X \sqcup Y \cong Y \sqcup X$

3. $X \sqcup \emptyset \cong \emptyset \sqcup X \cong X$

4. $X \sqcup Z \cong Y \sqcup Z \Rightarrow X \cong Y$

5. $(X \times Y) \times Z \cong X \times (Y \times Z)$

6. $X \times Y \cong Y \times Z$

7. $X \times G/G \cong G/G \times X \cong X$

8. $X \times (Y \sqcup Z) \cong (X \times Y) \sqcup (X \times Z)$

Demostración. Todas las proposiciones son claramente consecuencia del lema, excepto 4, Tenemos una asignación de órbitas de $X \sqcup Z$ y $Y \sqcup Z$, vamos a dar una para X y Y. Para cada órbita $\theta \subseteq X$ tenemos $f(\theta)$ donde f es el isomorfismo de $X \sqcup Z$ a $Y \sqcup Z$, si $f(\theta) \subseteq Y$ entonces le asignamos esa órbita, si $f(\theta) \subseteq Z$ podemos aplicar f otra vez y repetir el procedimiento hasta obtener la orbita de Y; el proceso es finito dado que el número de orbitas de Z es finito. Aplicando el lema anterior $X \cong Y$.

Definición 5.0.7. El anillo conmutativo con 1 que resulta de completar $B^+(G)$ denotado por $B(G)$ se llama **el anillo de Burnside** del grupo G.

Ejemplo: Sea $G = C_2 = \{1, x | x^2 = 1\}$. Entonces $B(G) = \mathbb{Z}G/1 \times \mathbb{Z}G/G$.

Si X es un G-conjunto, $a \in X$, si a es punto fijo bajo G, $\{a\}$ es órbita y $\{a\} \cong G/G$.

Si $b \in X$ no es punto fijo, $\{b, x \cdot b\}$ es orbita y $\{b, x \cdot b\} \cong G/1$. Entonces:

$$X \cong \alpha G/1 + \beta G/G$$

donde α, β son los números de órbitas isomorfas a cada cociente. Además: $(X, Y) \cong X - Y = (\alpha G/1 + \beta G/G) - (\alpha' G/1 + \beta' G/G) = (\alpha - \alpha')G/1 + (\beta - \beta')G/G$ donde $\alpha - \alpha', \beta - \beta' \in \mathbb{Z}$

6. Tablas de Marcas

6.1. Homomorfismo de marcas

Denotemos por $\mathscr{C}_G$ al conjunto de las clases de conjugación de los subgrupos de G.

Definición 6.1.1. El **anillo fantasma** con la operación coordenada a coordena es $\tilde{B}(G) = \Pi_{\mathscr{C}_G}\mathbb{Z}$.

Proposición. El conjunto $\{G/H\}_{H\in\mathscr{C}_G}$ es una base de $B(G)$ como grupo abeliano.

Notemos que como grupos $B(G) \cong \tilde{B}(G)$.

Demostración. Queremos demostrar que los $\{G/H\}_{H\in\mathscr{C}_G}$ generan a $B(G)$.

Sea $X - Y \in B(G)$ con X, Y G-conjuntos. Basta generar a X, siendo

$$X = \bigsqcup_{orbitas} G \cdot x_i$$

$$G \cdot x_i \cong G/H_i$$

$$X = \sum G/H_i$$

Demostremos que los $G/H_{H\in\mathscr{C}_G}$ son linealmente independientes sobre $\mathbb{Z}$.

Sea $\displaystyle\sum_{H\in\mathscr{C}_G} a_H(G/H) = 0$

Necesitamos hacer ver que $a_H = 0 \forall H$. Lo haremos por contradicción. Supongamos que hay algunos $a_K < 0$ y algunos $a_H > 0$. Tomams todos los $a_K < 0$ y los pasamos del otro lado de la igualdad, obteniendo:

$$\sum_{a_H}(G/H) = \sum_{-a_k}(G/K)$$

con $a_H \geq 0$ y $-a_K > 0$.

Sean x, y los G-conjuntos

$$X = \bigsqcup_{\forall H_i} \underbrace{((G/H_i \sqcup) \cdots \sqcup (G/H_i))}_{a_{H_i}\, veces (orbitas\, de\, X)}$$

$$Y = \bigsqcup_{\forall K_j} \underbrace{((G/K_j \sqcup) \cdots \sqcup (G/K_j))}_{a_{K_j}\, veces (orbitas\, de\, X)}$$

Tenemos que $X \cong Y$ como G-conjuntos, entonces $\sum_i a_{H_i} = \sum_j a_{K_j}$ y $\forall H_i \, \exists \, K_j$ tal que $G/H_i \cong G/K_j$ lo que implica que H_i, K_j son conjugados. Lo cual es una contradicción. Nuestro error fue pensar que los a_H son distintos de cero $\therefore a_H = 0 \, \forall \, H \in \mathscr{C}_G$.

Lema 6.1.2. $(G/1)(G/1) = |G|(G/1)$

Demostración.

$$G \times G \cong \bigsqcup_{g \in G} \{(xg, x) | x \in G\}$$

Proposición 6.1.3. Para $G \neq 1$, el Anillo de Burnside y el Anillo Fantasma no son isomorfos como anillos, $B(G) \ncong \tilde{B}(G)$.

Demostración. Supongamos que $\exists \, f : B(G) \longrightarrow \tilde{B}(G)$ un isomorfismo de anillos con 1. veamos en particular,

$$f((G/1)(G/1)) = f((G/1)^2) = ((a_1)^2, \cdots, (a_n)^2)$$

pero además usando el lema anterior tenemos que

$$f((G/1)(G/1)) = f(|G|(G/1)) = |G|(a_1, \cdots, a_n) = |G|f(G/1)$$

y entonces

$$((a_1)^2, \cdots, (a_n)^2) = |G|(a_1, \cdots, a_n)$$

$$((a_1)^2, \cdots, (a_n)^2) = (|G|a_1, \cdots, |G|a_n)$$

$$\Rightarrow = \left\{ \begin{array}{ll} a_i = 0 & \text{ó} \\ a_i = |G| & \end{array} \right.$$

en cualquier caso $|G|$ divide a a_i, peo no todas las $a_{i,s}$ pueden ser cero porque entonces las dimensiones serían distintas.

$$\tilde{B}(G) = \langle f(G/H_1), f(G/H_2), \cdots, f(G/H_n) \rangle$$

Tenemos entonces que como $(G/H_i)_i$ genera al $B(G)$ como grupo abeliano y como f es un isomorfismo de anillos entre $B(G)$ y $\tilde{B}(G) \Rightarrow f(G/H_i)$ genera a $\tilde{B}(G)$ como grupo abeliano.

Sea M la representación matricial del anillo fantasma $\tilde{B}(G) = \langle f(G/1), \cdots, f(G/G) \rangle$

$$M = \begin{pmatrix} |G|b_1 & |G|b_2 & \cdots & |G|b_n \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \end{pmatrix}$$

$$\Rightarrow |G| det(M)$$

llevemos M a su forma Normal de Schmidt (M_S), pero M_S no puede ser la matriz identidad porque no concordarían los determinantes.

$$M_S = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

$$\frac{\tilde{B}(G)}{\langle f(G/1), \cdots, f(G/G) \rangle} \neq 0$$

$$\Rightarrow Im(f) \neq \tilde{B}(G)$$

$\therefore f$ no es un isomorfismo y

$$B(G) \neq \tilde{B}(G)$$

Proposición 6.1.4. Sea $H \leq G$ y sea

$$\varphi_H : B(G) \longrightarrow \mathbb{Z}$$

$$G/K \longmapsto \#(G/K)^H$$

Y luego extendemos linealmente

$$X \longmapsto \#(X^H) = \#(\sqcup a_i G/K_i)^H = \sum a_i (G/K_i)^H$$

$$X - Y \longmapsto \#(X^H) - \#(Y^H)$$

Siendo $X^H = \{x \in X | hx = x \,\forall\, h \in H\}$. Entonces φ_H esta bien definida y es un homomorfismo suprayectivo de anillos con 1, llamado **la marca de H**.

Demostración. Que φ_H está bien definida. Queremos ver que si $X - Y \sim X' - Y'$, entonces $X \sqcup Y' \sim X' \sqcup Y'$, entonces $X \sqcup Y' \sim X' \sqcup Y'$, aplicando φ_H, $\#X^H + \#Y'^H {=} \#X'^H + \#Y^H$, $\#X^H - \#Y^H = \#X'^H + \#Y'^H$. φ_H, preserva la operación de suma(unión) y el producto claramente. Además, φ_H es suprayectiva pues $G/G \mapsto 1$.

Teorema 6.1.5. de Burnside. Sean X y Y G-conjuntos. Entonces

$$X \cong Y \Leftrightarrow \forall\, H \leq G, \varphi_H(X) = \varphi_H(Y)$$

Demostración. Si $X \cong Y \cong \sum a_i(G/K_i)$ es claro que $\varphi_H(X) = \varphi_H(Y) \,\forall\, X \leq G$. Por otra parte, si $x \in X$, $H = Stab_G$, $G \cdot x \cong G/H$, esto quiere decir que $x \in X^H$ además, existe $y \in Y^H$ y que $H = Stab_G(y)$, entonces $G \cdot x \cong G \cdot y \cong G/H$, sean $X' = X/G \cdot x$, $Y' = Y/G \cdot y$ y las descomposiciones como órbitas de los dos G-conjuntos son iguales y por lo tanto son isomorfos.

Teorema 6.1.6. Sean $H, K \leq G$

$$\varphi_H = \varphi_K \Leftrightarrow H =_G K$$

Demostración. Si $H =_G K$, sea X transitivo. $\varphi_H(X) = \#\{x \in X | h \cdot x = x \,\forall h \in H\}$ $= \#\{x \in X | (g^{-1}Kg) \cdot x = x \,\forall k \in K\} = \#\{x \in X | (kg) \cdot x = gx \,\forall\, k \in K\} =$ $\#\{y \in X | k \cdot y = y \,\forall\, k \in K\}$=$\varphi_K(X)$, esto ultimo porque X es transitivo y nos dice que las $\varphi' s$ son iguales en los G-conjuntos base y por lo tanto en todos. Si $\varphi_H = \varphi_K$, entonces, por las fórmulas que veremos en la siguiente sección, donde también se dice que significa la α, $|N_G(K)|/|K|\alpha(H,K) = \varphi_H(G/K) = \varphi_K(G/K) = |N_G(K)|/|K|$ por lo tanto hay un conjugado de K que contiene a H, análogamente, hay un conjugado de H que contiene a K, y por lo tanto $H =_G K$.

6.2. Tabla de marcas

Notación: Ordenaremos las clases de conjugación de G como $H_1, H_2, \cdots, H_n$ donde $|H_i \leq H_{i+1}|$. Esto implica que $H_1 = 1_G$ y $H_n = G$.

Proposición 6.2.1. $\varphi_H(G/K) = \frac{N_G(H)}{K}\beta(H,K) = \frac{N_G(K)}{K}\alpha(H,K)$, donde $\alpha(H,K) = \{\#E \leq G | E =_G K, H \leq E\}$, $\beta(H,K)$=$\{E \leq G | E =_G H, E \leq K\}$.

Demostración.

$$\varphi_H(G/K) = (G/K)^H = \#\left\{gK | g^{-1}hgK = K \,\forall\, h \in H\right\} =$$

$$= \frac{\{\#g \in G | hgK = gK \,\forall\, h \in H\}}{|K|} = \frac{\{\#g \in G | g^{-1}hgK = K \,\forall\, h \in H\}}{|K|} =$$

$$= \frac{\#\{g \in G | g^{-1}hg \in K \,\forall\, h \in H\}}{|K|} = \frac{\#\{g \in G | g^{-1}Hg \subseteq K\}}{|K|} =$$

$$= \frac{N_G(H)\#\{\, E\ \leq G | E \,\text{es conjugado a}\, H, E \leq K\}}{K} = \frac{N_G(H)}{K}\beta(H,K)$$

la otra igualdad la tenemos de

$$\varphi_H(G/K) = \frac{\#\{g \in G | g^{-1}Hg \subseteq K\}}{|K|} = \frac{\#\{g \in G | H \subseteq gKg^{-1}\}}{|K|} =$$

$$\frac{N_G(K)\#\{E \leq G | E \, \text{es conjugado a} \, K, H \leq E\}}{|K|} = \frac{N_G(K)}{|K|}\alpha(H,K)$$

Definición 6.2.2. **La tabla de marcas** del grupo G es la matriz $(a_{i,j}) = \varphi_{H_i}(G/H_j) = \frac{|N_G(H_i)|}{|H_j|}\beta(H_i,H_j) = \frac{|N_G(H_j)|}{|H_j|}\alpha(H_i,H_j)$

Proposición 6.2.3. La tabla de marcas $A = (a_{i,j})$ del grupo G satisface:

1. A es cuadrada de tamaño $n \times n$ donde $n = \#\mathscr{C}_G$
2. A tiene coordenadas enteras
3. A es triangular superior
4. $a_{i,n} = 1 \, \forall 1 \leq i \leq n$, es decir, la última columna es la unidad de $\prod_{\mathscr{C}_G} \mathbb{Z}$
5. La primera fila de G corresponde a los índices de los subgrupos de G, esto es: $a_{1,i} = |G/H_i| \, \forall \, 1 \leq i \leq n$, como casos particulares $a_{1,1} = |G|$, $a_{1,n} = 1$
6. $a_{i,i} = |\frac{N_G(H_i)}{H_i}| \, \forall 1 \leq i \leq n$ los órdenes de subgrupos Weyl.
7. Un elemento en la diagonal divide a cada elemento de la misma columna que él, esto es: $\varphi_{H_i}(G/H_j) | \varphi_{H_j}(G/H_i)$
8. $a_{1,1} = |G|$ es la mayor entrada de A
9. $|H_i| = \frac{a_{1,1}}{a_{1,i}/a_{i,i}}$
10. $\alpha(H_i,H_j) = \frac{a_{i,j}}{a_{j,j}}$

11. $\beta(H_i, H_j) = \frac{a_{i,j}a_{1,i}}{a_{i,i}a_{1,j}}$

Demostración

1. Por construcción A es cuadrada y $n = \#\mathscr{C}_G$
2. Basta recordar que $\varphi_{H_i}(G/H_j) = \#(G/H_j)^{H_i}$ son los puntos fijos de H_j bajo H_i lo cual es entero.
3. $a_{i,j} = 0$ si $i > j$ pues si $|H_i| > |H_j|$ entonces $\alpha(H_i, H_j) = 0$, y si $|H_i| = |H_j|$ corresponden a clases de conjugación diferentes y $\alpha(H_i, H_j) = 0$, por lo tanto $\varphi_{H_i}(G/H_j) = 0 = a_{i,j}$
4. $N_G(G) = G$, $\alpha(H_i, G) = 1$ esto último es porque G no tiene conjugados, entonces $\frac{|N_G(H_n)|}{|H_n|}\alpha(H_i, H_n) = \frac{|G|}{|G|} = 1$
5. $N_G(1_G) = G$, $\beta(1_G, H_i) = 1$ pues 1_G no tiene conjugados, entonces $\frac{|N_G(H_1)|}{|H_i|}\beta(H_1, H_i) = \frac{|G|}{|H_i|} = |\frac{G}{H_i}|$
6. $\alpha(H_i, H_i) = 1$ y $a_{i,i} = \frac{|N_G(H_i)|}{|H_i|} = |\frac{N_G(H_i)}{H_i}|$
7. $a_{j,i} = \frac{|N_G(H_i)|}{|H_i|}\alpha(H_j, H_i) = a_{i,i}\alpha(H_j, H_i)$ y $a_{i,i}|a_{j,i}$
8. $a_{i,j} = \varphi_{H_i}(G/H_j)$ son los puntos fijos de G/H_j bajo la acción de H_i, entonces $a_{i,j} \leq |G/H_j| \leq |G|$, donde la última igualdad se da únicamente cuando $j = 1, H_j = 1_G$. Así $a_{1,1} > a_{i,j}$ si $i \neq 1$ o $j \neq 1$
9. $\frac{a_{1,1}}{a_{1,i}} = \frac{|G|}{|G/H_i|} = |H_i|$
10. $\frac{a_{1,1}}{a_{1,i}/a_{i,i}} = |G|/(\frac{|G|/|H_i|}{|N_G(H_i)|/|H_i|}) = |G|/|G/N_G(H_i)| = N_G(H_i)$
11. $\frac{a_{i,j}}{a_{j,j}} = \frac{N_G(H_j)}{H_j}\alpha(H_i, H_j)/\frac{N_G(H_j)}{H_j} = \alpha(H_i, H_j)$
12. $\frac{a_{i,j}a_{1,i}}{a_{i,i}a_{1,j}} = \frac{\frac{|N_G(H_i)|}{|H_j|}\beta(H_i,H_j)\frac{|G|}{|H_i|}}{\frac{|N_G(H_i)|}{|H_i|}\frac{|G|}{|H_j|}} = \beta(H_i, H_j)$

Nota: para calcular la tabla de marcas de un grupo G usando GAP, utilícese el comando

```
Display(TableOfMarks(G));
```

Ejemplos.

1. Trivial: $\varphi(1/1) = 1$. genera la tabla de marcas trivial:

$$(1)$$

2. $G = C_p$, grupo cíclico de orden primo p. Tiene dos subgrupos $\{1, C_p\}$, por lo tanto su tabla de marcas es la siguiente:

$$\begin{pmatrix} |G/1| & 1 \\ 0 & |G/C_p| \end{pmatrix} = \begin{pmatrix} p & 1 \\ 0 & 1 \end{pmatrix}$$

3. $G = C_6$ el cual tiene como subgrupos a $1, C_2, C_3, C_6$. Y su tabla de marcas queda:

$$\begin{pmatrix} 6 & 3 & 2 & 1 \\ 0 & 3 & 0 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

4. Ahora veamos el grupo de orden 6 S_3 el cual tiene como subgrupos $\{1, \langle(1,2)\rangle, \langle(1,2,3)\rangle, S_3\}$

$$\begin{pmatrix} 6 & 3 & 2 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

7. Grupos de orden menor o igual a 95 (Aportaciones Originales)

Intentemos demostrar que si G y Q son grupos con tablas de marcas no isomorfas, entonces $|G| \geq 96$. La siguiente tabla representa los grupos de orden 1 hasta 95 con el número de grupos no abelianos según GAP.

1:0	2:0	3:0	4:0	5:0	6:1	7:0	8:2	9:0	10:1
11:0	12:3	13:0	14:1	15:0	16:9	17:0	18:3	19:0	20:3
21:1	22:1	23:0	24:12	25:0	26:1	27:2	28:2	29:0	30:3
31:0	32:44	33:0	34:1	35:0	36:10	37:0	38:1	39:1	40:11
41:0	42:5	43:0	44:2	45:0	46:1	47:0	48:47	49:0	50:3
51:0	52:3	53:0	54:12	55:1	56:10	57:1	58:1	59:0	60:11
61:0	62:1	63:2	64:256	65:0	66:3	67:0	68:3	69:0	70:3
71:0	72:44	73:0	74:1	75:1	76:2	77:0	78:5	79:0	80:47
81:10	82:1	83:0	84:13	85:0	86:1	87:0	88:9	89:0	90:8
91:0	92:2	93:1	94:1	95:0					

Por [8] sólo nos ocuparemos de grupos no abelianos. Y el menor orden encontrado donde hay dos grupos distintos no abelianos cuyas tablas de marcas sean isomorfas es en orden 96 [9].

7.1. Teorema de P. Hall

Teorema Sea G un grupo soluble de orden ab, donde $(a, b) = 1$. Entonces G contiene al menos un subgrupo de orden a, y cualquier otro es conjugado.

Demostración. Se omite y se encuentra en [4] como teorema con número [5.28].

7.2. Grupos de orden p

Teorema. Todo grupo cíclico G es abeliano.

Demostración:

Usando que los enteros modulo n son isomorfos al grupo cíclico C_n. Sean $x, y \in G$ como el grupo es cíclico, sus elementos están generados por el elemento a entonces sea $x = a^m, y = a^n$, por lo cual $x * y = a^m * a^n = a^{m+n} = a^{n+m} = a^n * a^m = y * x$.

Por lo tanto los grupos de orden primo son abelianos, y los eliminamos de nuestra lista.

~~1~~	~~2~~	~~3~~	4	~~5~~	6	~~7~~	8	9	10
~~11~~	12	~~13~~	14	15	16	~~17~~	18	~~19~~	20
21	22	~~23~~	24	25	26	27	28	~~29~~	30
~~31~~	32	33	34	35	36	~~37~~	38	39	40
~~41~~	42	~~43~~	44	45	46	~~47~~	48	49	50
51	52	~~53~~	54	55	56	57	58	~~59~~	60
~~61~~	62	63	64	65	66	~~67~~	68	69	70
~~71~~	72	~~73~~	74	75	76	77	78	~~79~~	80
81	82	~~83~~	84	85	86	87	88	~~89~~	90
91	92	93	94	95					

7.3. Grupos de orden p^2

Teorema 7.2.1. Si p es número primo, entonces todo grupo G de orden p^2 es abeliano.

Demostración: Procedamos por contradicción. Supongamos que G es no abeliano. entonces $Z(G) < G$ pues si fuera G implica que todo los elementos conmutan; dado que $Z(G) \neq 1$ puesto que el centro de un p-grupo es no trivial, nos resta que $|Z(G)| = p$. El grupo cociente $G/Z(G)$ está bien definido pues $Z(G) \triangleleft G$, y es cíclico, pues si $|G| = p^2$ y $|Z(G)| = p$ tenemos que $|G|/|Z(G)| = p$ Esto contradice el hecho de que si un grupo G es no abeliano, entonces $G/Z(G)$ es no cíclico. Y aquí tuvimos un grupo cíclico.

Por lo que nos queda ahora la tabla como sigue:

~~1~~	~~2~~	~~3~~	~~4~~	~~5~~	6	~~7~~	8	~~9~~	10
~~11~~	12	~~13~~	14	15	16	~~17~~	18	~~19~~	20
21	22	~~23~~	24	~~25~~	26	27	28	~~29~~	30
~~31~~	32	33	34	35	36	~~37~~	38	39	40
~~41~~	42	~~43~~	44	45	46	~~47~~	48	~~49~~	50
51	52	~~53~~	54	55	56	57	58	~~59~~	60
~~61~~	62	63	64	65	66	~~67~~	68	69	70
~~71~~	72	~~73~~	74	75	76	77	78	~~79~~	80
81	82	~~83~~	84	85	86	87	88	~~89~~	90
91	92	93	94	95					

7.4. Grupos de orden p^3

Estos grupos están resueltos hasta isomorfismos en la literatura, en particular citamos el articulo [10] en donde se demuestra que hay 5 grupos hasta isomorfismos de orden p^3. veamos cuales son los grupos que existen de estos órdenes para el par de grupos que nos interesan 8 y 27:

para $|G| = 8$ tenemos:

1. C_8
2. $C_4 \times C_2$
3. $C_2 \times C_2 \times C_2$
4. $D_8 \cong C_4 \rtimes C_2$
5. Q_8

Ahora bien de los grupos no abelianos que son Q_8 y D_8 sus tablas de marcas no pueden ser isomorfas pues para Q_8 todo subgrupo es normal y para D_8 esto no es así.

para $|G| = 27$ tenemos:

1. C_{27}
2. $C_9 \times C_3$
3. $C_3 \times C_3 \times C_3$
4. $C_9 \rtimes C_3$
5. $(C_3 \times C_3) \rtimes C_3$

Los primeros 3 son abelianos y de los 2 no abelianos el caso 4 tiene un subgrupo cíclico de orden 9, (C_9), y el caso 5 no tiene subgrupos cíclicos de orden 9, por lo tanto sus tablas de marcas no pueden ser isomorfas.

7.5. Grupos de orden pq

Teorema. Sea $|G| = pq$, donde $p > q$ primos, Entonces o G es un grupo cíclico o G es generado por dos elementos a y b que satisfacen las siguientes relaciones.

$a^p = 1$; $b^q = 1$; $aba^{-1} = b^r$;

donde $r \equiv 1(mod\, p)$ pero $r^q \equiv 1(mod\, p)$. Esta segunda posibilidad sólo ocurre si q divide $p-1$.

Demostración: G contiene un elemento b de orden p; sea $S =< b >$. Dado que S es un p-subgrupo de Sylow de G, el número de sus conjugados por el tercer teorema de Sylow es $1+up$ para algún $u \geq 0$. y divide a pq. Puesto que $(1+up, p) = 1$, ya que $1+up$, tiene que dividir q. Y ya que $q < p$, $u = 0$ y $S \lhd G$ puesto que solo tiene un único subgrupo de Sylow.

Similarmente G contiene un elemento a de orden q; sea $T =< a >$. T es un q-subgrupo de Sylow de G, por lo que el número de sus conjugados es $1+kq$ para algún $k \geq 0$. Similarmente al caso anterior, $1+kq$ divide p, de donde tenemos los siguientes dos casos, que $k = 0$ o que $q|(p-1)$. Si $k = 0$, $T \lhd G$ por lo tanto $G \cong S \times T$. Y como sabemos que si todo subgrupo de G es normal, G es el producto directo de sus subgrupos de Sylow. Por lo que $G \cong C_p \times C_q \cong C_{pq}$.

Si $q|p-1$, entonces $Aut(T) = C_{q-1}$ tiene un único subgrupo S' de orden p, donde $S' = \{x \to x^i | i \in \mathbb{Z}/q\mathbb{Z}, i^p = 1\}$. Sean a y b generadores para S y T respectivamente, supóngase que la acción de a en T por conjugación es $x \to x^{i_0}$, donde $i_0 \neq 1$ en $\mathbb{Z}/q\mathbb{Z}$. Entonces $G = \langle a, b | a^p = b^q = 1, aba^{-1} = b^{i_o} \rangle$. Escogiendo diferente i_0 nos lleva a escoger un generador diferente a para S, y por lo tanto, no resulta en una nueva clase de isomorfismos. Por lo tanto concluimos que hay exactamente dos clases de isomorfismos de grupos de orden pq.

Por lo que nos queda ahora la tabla como sigue:

Corolario: Si $|G| = pq$, donde $p > q$ primos, entonces G tiene un subgrupo normal de orden p. Más aún, si q no divide a $p-1$, entonces G es cíclico.

~~1~~	~~2~~	~~3~~	~~4~~	~~5~~	~~6~~	~~7~~	8	~~9~~	~~10~~
~~11~~	12	~~13~~	~~14~~	~~15~~	16	~~17~~	18	~~19~~	20
~~21~~	~~22~~	~~23~~	24	~~25~~	~~26~~	27	28	~~29~~	30
~~31~~	32	~~33~~	~~34~~	~~35~~	36	~~37~~	~~38~~	~~39~~	40
~~41~~	42	~~43~~	44	45	~~46~~	~~47~~	48	~~49~~	50
~~51~~	52	~~53~~	54	~~55~~	56	~~57~~	~~58~~	~~59~~	60
~~61~~	~~62~~	63	64	~~65~~	66	~~67~~	68	~~69~~	70
~~71~~	72	~~73~~	~~74~~	~~75~~	76	~~77~~	78	~~79~~	80
81	~~82~~	~~83~~	84	~~85~~	~~86~~	~~87~~	88	~~89~~	90
~~91~~	92	~~93~~	~~94~~	~~95~~					

7.6. Grupos de orden 45

Este es el último grupo que nos falta en donde todos los grupos de ese orden son abelianos y no queda dentro de los casos anteriores puesto que $45 = 3^2 \times 5$.

Utilizando el teorema de la descomposición de Kronecker sabemos que el número de grupos abelianos no isomorfos de este grupo es 2 a saber C_{45} y $C_5 \times C_9 \cong C_5 \times C_3 \times C_3$. Veamos no existen grupos no abelianos de este orden:

Sea n_p el número de p-subgrupos de sylow de G, tomemos en nuestro caso n_5 por lo tanto el número de p-subgrupos de Sylow puede ser 1 , 3 ó 9 pero $n_5 \nmid 3$,$n_5 \nmid 9$, y $n_5 \cong 1(mod\, 5)$ similarmente con n_3 el número de p-subgrupos de Sylow puede ser 1 ó 5 tenemos $n_3 \nmid 5$ y $n_3 \cong 1(mod\, 3)$,entonces su intersección es trivial, ambos son normales y por lo tanto G debe ser el producto directo de grupos de orden 9 y 5 que son los ya dados.

7.7. Grupos de orden 75

Trataremos aparte los grupos cuyo orden sea $75 = 5^2 \times 3$ que son los últimos que tienen un solo grupo no abeliano, y los otros que solo tenían un Grupo no abeliano fueron trataron en la sección de grupos de orden pq

Utilizando el teorema de la descomposición de Kronecker sabemos que el número de grupos abelianos no isomorfos de este grupo es 2 a saber C_{75} y $C_{25} \times C_3$, veamos qué sabemos sobre sus grupos no abelianos.

El número 3-subgrupos de Sylow de G puede ser $1, 5, 25$ de donde $n_3 \nmid 5$, $n_3 \mid 25$, $n_3 \cong 1(mod\, 3)$, por lo tanto $n_3 = 25$ o $n_3 = 1$ y el número de 5-subgrupos de sylow de G puede ser $1, 3$ pero $n_5 \nmid 3$,$n_5 \cong 1(mod\, 5)$, por lo tanto este es normal.

Ahora si $n_3 = 1$ estamos en el caso en que ambos son normales y sería el grupo abeliano descrito anteriormente, entonces nos falta analizar el caso $n_3 = 25$ que no es normal y el otro sí, por lo tanto podemos formar el producto semidirecto $G \cong P_5 \rtimes P_3$ donde $P_3 = C_3$ y $P_5 = C_5 \times C_5$ ó $P_5 = C_{25}$, y de aquí $Aut(C_5 \times C_5) = GL(2, 5)$ y $Aut(C_{25}) = C_{20}$ y donde el segundo caso no se puede dar, puesto que no es posible formar un morfismo no trivial de C_3

a $Aut(C_{25})$ pues no hay un elemento de orden 3 en C_{25}, Y en $GL(2,5)$ existe un subgrupo de orden 3 por lo cual es posible formar el producto semidirecto con este grupo.

7.8. Grupos de orden 2^2p con $4 \nmid p-1$

Por el teorema de la descomposición de Kronecker estos grupos tienen 2 grupos abelianos no isomorfos.

Teorema 7.9.1. El número de grupos no abelianos de orden 2^2p es 2 si $4 \nmid p-1$.

Muy claramente $n_P \equiv 1 (mod\, p)$ bajo la condición de que $4 \nmid p-1$ pues si no el 2-subgrupo de Sylow ya no sería normal.

Nuestros 2-subgrupos de Sylow tienen orden 4 y pueden ser C_4 o $C_2 \times C_2$.

Utilizando el resultado de que $Aut(C_p) \cong C_{p-1}$ analicemos los posibles casos:

Caso 1.

$C_4 \longrightarrow Aut(C_p) \cong C_{p-1}$,

$C_4 = \{0,1,2,3\}$ de aquí mandamos al 2 a un elemento de orden 2 en C_{p-1} que es $\frac{p-1}{2}$

Caso 2.

$C_2 \times C_2 \longrightarrow Aut(C_p) \cong C_{p-1}$,

Salvo isomorfismos tenemos un morfismo no trivial analizando los generadores de $C_2 \times C_2$

$(1,0) \longrightarrow 0$

$(0,1) \longrightarrow \dfrac{p-1}{2}$

$\therefore$ Sólo existen 2 grupos no abelianos de orden 2^2p, que tienen 2-subgrupos de Syllow que no pueden corresponder, pues para el primero tenemos a C_4 y para el otro $C_2 \times C_2$ y por ende sus tablas de marcas no son isomorfas.

Con este teorema, añadimos a nuestra lista, los siguientes órdenes $28, 44, 76, 92$

7.9. Grupo de orden 63

Este caso es similar al anterior ya que $63 = 3^2 7$ tiene dos grupos abelianos y dos no abelianos.

Demostración:

$n_7 \cong 1 (mod\, 7)$ y $n_7 \nmid 3$, $n_7 \nmid 9$

$|P_3| = 9$, entonces $P_3 = C_9$ y $P_3 = C_3 \times C_3$

usando que $Aut(C_7) = C_6$ analizaremos los dos casos:

Caso 1.

$C_9 \longrightarrow C_6$, donde un elemento de orden 3 en C_9 es 3 y uno de este orden en C_6 es 2 lo cual define un morfismo no trivial.

Caso 2.

$C_3 \times C_3 \longrightarrow C_6$ donde salvo isomorfismos tenemos el siguiente morfismo no trivial.

$(0, 1) \longrightarrow 0$

$(0, 1) \longrightarrow 2$

$\therefore$ Sólo existen 2 grupos no abelianos de orden 63 que tienen 3-subgrupos de Syllow que no pueden corresponder, pues para el primero tenemos a C_9 y para el otro $C_3 \times C_3$ y por ende sus tablas de marcas no son isomorfas.

Con los casos anteriores podemos eliminar de nuestra tabla todos los grupos en cuyo orden tienen hasta isomorfismo 2 grupos no abelianos.

~~1~~	~~2~~	~~3~~	~~4~~	~~5~~	~~6~~	~~7~~	~~8~~	~~9~~	~~10~~
~~11~~	12	~~13~~	~~14~~	~~15~~	16	~~17~~	18	~~19~~	20
~~21~~	~~22~~	~~23~~	24	~~25~~	~~26~~	~~27~~	~~28~~	~~29~~	30
~~31~~	32	~~33~~	~~34~~	~~35~~	36	~~37~~	~~38~~	~~39~~	40
~~41~~	42	~~43~~	~~44~~	~~45~~	~~46~~	~~47~~	48	~~49~~	50
~~51~~	52	~~53~~	54	~~55~~	56	~~57~~	~~58~~	~~59~~	60
~~61~~	~~62~~	~~63~~	64	~~65~~	66	~~67~~	68	~~69~~	70
~~71~~	72	~~73~~	~~74~~	~~75~~	~~76~~	~~77~~	78	~~79~~	80
81	~~82~~	~~83~~	84	~~85~~	~~86~~	~~87~~	88	~~89~~	90
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~					

7.10. Grupos de orden 2^2p con $4 \mid p-1$

Teorema: El número de grupos no isomorfos de un grupo de orden 2^2p con $4 \nmid p-1$ es 5 ,donde 2 son grupos abelianos y los otros 3 son grupos no abelianos.

Demostración:

Para estos grupos vemos que tienen dos grupos abelianos por el teorema de la descomposición de Kronecker. Y sus grupos no abelianos se determinan de la siguiente forma.

$n_p \cong 1(mod\, p)$ y $n_p \nmid 2$, $n_p \nmid 4$ pues p es mayor que 2 y 4, por lo tanto n_p es normal. Y $Aut(C_p) = C_{p-1}$

Utilizando el tercer teorema de Sylow, $n_4 \cong 1(mod\, 4)$ y $n_4 \mid p$ por lo tanto no es normal y se puede formar alguno de los siguientes productos semidirectos.

$C_p \rtimes C_4$ o el caso $C_p \rtimes (C_2 \times C_2)$

Caso 1: $C_4 \longrightarrow C_{p-1}$

a) $1 \longrightarrow \dfrac{p-1}{2}$

b) $1 \longrightarrow \dfrac{p-1}{4}$ este caso se puede por la hipótesis de que $4 \mid p-1$.

Y de aquí tenemos dos morfismos nos triviales a) y b).

Caso 2: $C_2 \times C_2 \to C_{p-1}$

Salvo ismorfismos dentro del mismo grupo tenemos los siguientes morfismos no triviales

$(0,1) \longrightarrow 0$

$(1,0) \longrightarrow 1$

Para el caso 2, sólo tenemos un morfismo no trivial.

Por lo tanto existen 3 grupos no abelianos hasta isomorfismos de orden 2^2p cuyas tablas de marcas son no isomorfas puesto que, en el caso a) el morfimos actúa como la involución $x \longmapsto x^{-1}$, por lo tanto C_2 centraliza a C_p y por lo tanto el grupo tiene un subgrupo normal de orden 4 mientras que para el caso b), C_4 actúa por un automorfismo de C_p con orden 4 y por lo tanto C_2 no centraliza a C_p, y este grupo no tiene subgrupo normal de orden 4, por lo tanto los grupos a) y b) del caso 1, no tienen tablas de marcas isomorfas, y la tabla de marcas del caso 2, no puede ser igual a las del caso 1 pues los 2-subgrupos de Sylow no corresponden pues en el primer caso tenemos a C_4 como 2-subgrupo de Sylow, mientras que en el otro caso tenemos a $C_2 \times C_2$.

Y por lo tanto ahora podemos eliminar de nuestra tabla los órdenes $20, 52, 68$.

7.11. Grupos orden $2p^2$

Claramente el p subgrupo de Sylow es normal puesto que $n_p \nmid 2$ y $n_p \cong 1 (mod\, p)$. Y el 2 subgrupo de Sylow no es es normal pues $n_2 \mid p$ y $n_2 \cong 1(mod 2)$.

Entonces tenemos las 2 siguientes posibilidades:

Caso 1. $C_2 \longrightarrow Aut(C_{p^2}) \cong C_{p(p-1)}$

En este caso tenemos el morfismo no trivial $1 \longrightarrow \dfrac{p(p-1)}{2}$
Caso 2. $C_2 \longrightarrow Aut(C_p \times C_p) \cong GL(2,p)$

Y en este caso tenemos dos morfismos no triviales.

Para las tablas de marcas entre el caso 1 y caso 2 las podemos distinguir debido a que en el primer caso tenemos un p-subgrupo cíclico de Sylow y en el caso 2 no, y para distinguir los dos morfismos del caso 2 dado que $C_p \times C_p$ es un espacio vectorial sobre el campo con p elementos, uno de sus automorfismos tiene un subespacio invariante unidimensional mientras que el otro no. Uno tiene a C_p como un sumando directo mientras que el otro no. Por lo tanto, sus tablas de marcas no son isomorfas.

Ahora podemos eliminar de nuestra tabla $18, 50$

7.12. Grupos orden $2pq$ $p \nmid q-1$

Sean p y q tales que $2 < p < q$ y $p \nmid q-1$ p y q son normales, mientras que 2 no lo es. por el teorema de P. Hall nuestro grupo de orden $2pq$ tiene un subgrupo normal H de orden pq por lo tanto $G = H \rtimes C_2$

Entonces existen 3 morfismos no triviales de C_2 a $Aut(pq) \cong Aut(p)Aut(q) \cong (C_{p-1})(C_{q-1})$

Caso 1.

$1 \longrightarrow (\frac{p-1}{2}, 0)$

Caso 2.

$1 \longrightarrow (0, \frac{q-1}{2})$

Caso 3.

$1 \longrightarrow (\frac{p-1}{2}, \frac{q-1}{2})$

Como podemos observar de los casos 1 y 2, uno tiene a C_p como factor directo mientras que que el otro a C_q y el caso 3 tiene a ambos. por lo tanto sus tablas de marcas no pueden ser isomorfas.

Por lo tanto podemos eliminar de nuestra lista los grupos de orden $30, 66, 70$

Actualicemos ahora si nuestra tabla.

~~1~~	~~2~~	~~3~~	~~4~~	~~5~~	~~6~~	~~7~~	~~8~~	~~9~~	~~10~~
~~11~~	12	~~13~~	~~14~~	~~15~~	16	~~17~~	~~18~~	~~19~~	~~20~~
~~21~~	~~22~~	~~23~~	24	~~25~~	~~26~~	~~27~~	~~28~~	~~29~~	~~30~~
~~31~~	32	~~33~~	~~34~~	~~35~~	36	~~37~~	~~38~~	~~39~~	40
~~41~~	42	~~43~~	~~44~~	~~45~~	~~46~~	~~47~~	48	~~49~~	~~50~~
~~51~~	~~52~~	~~53~~	54	~~55~~	56	~~57~~	~~58~~	~~59~~	60
~~61~~	~~62~~	~~63~~	64	~~65~~	~~66~~	~~67~~	~~68~~	~~69~~	~~70~~
~~71~~	72	~~73~~	~~74~~	~~75~~	~~76~~	~~77~~	78	~~79~~	80
81	~~82~~	~~83~~	84	~~85~~	~~86~~	~~87~~	88	~~89~~	90
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~					

7.13. Grupos de orden 12

Por [7] tenemos que los grupos de orden 12 son:

- ▷ C_{12}
- ▷ $C_2 \times C_2 \times C_3$
- ▷ A_4
- ▷ D_{12}
- ▷ $C_3 \rtimes C_4$

Los 3 grupos no abelianos claramente son $\{A_4, D_{12}, C_3 \times C_4\}$ de donde vemos que $C_3 \times C_4$ tiene un 2-sbugrupo de Sylow isomorfo a C_4 y el segundo un subgrupo normal de orden 6 puesto que $D_{12} \cong S_3 \times C_2$ mientras que A_4 no, por lo tanto estos grupos no tienen tablas de marcas isomorfas.

7.14. Grupos de orden 42 y 78

.

Veamos que existen hasta isomorfismos 5 grupos no abelianos de estos órdenes. Observemos primero que $42 = 2 \times 3 \times 7$ y que $78 = 2 \times 3 \times 13$, por lo que observamos que ambos números son de la forma $2pq$ más exactamente $2 \times 3 \times q$, $p > q$. Vemos que $3|q-1$. Dado que 42 y 78 son solubles, podemos utilizar el teorema de P. Hall el cual nos dice que existe un subgrupo normal H de orden pq (21 o 39). Por lo tanto tenemos dos posibilidades. H puede ser el único grupo no abeliano de orden pq (el producto semidirecto $p \rtimes q$) o H puede ser el único grupo abeliano de este orden C_{pq}. Veamos el caso en que $H \cong C_{pq}$.

Veamos si existe un mofismo no trivial de $C_2 \longrightarrow Aut(C_{pq})$

Observamos que $Aut(C_{pq}) \cong Aut(C_p) \times Aut(C_q)$ por lo tanto

$Aut(C_p) \times Aut(C_q) \cong C_{p-1} \times C_{q-1}$

donde en C_{p-1} existe un único elemento de orden 2 a saber $\frac{p-1}{2}$ y similarmente en C_{q-1} existe un único elemento de orden 2 a saber $\frac{q-1}{2}$

Por lo tanto se pueden formar 3 productos semidirectos no triviales que son:

- $\triangleright$ $1 \longrightarrow (\frac{p-1}{2}, 0)$
- $\triangleright$ $1 \longrightarrow (0, \frac{q-1}{2})$
- $\triangleright$ $1 \longrightarrow (\frac{p-1}{2}, \frac{q-1}{2})$

Como el primero tiene a C_p como factor directo, el segundo tiene a C_q como factor directo, y el tercero no tiene tales factores directos, concluimos que no pueden tener tablas de marcas isomorfas entre si, y también no isomorfas a las tablas de los casos pues el subgrupo $|H| = pq$ es cíclico y en los otros casos no.

Ahora veamos el caso cuando H es no abealiano, claramente tenemos el caso en que $G = H \times C_2$ pues H existía y multiplicarlo por C_2 nos genera de nuevo un grupo no abeliano, resta ver si existe otro caso cuando H es no abeliano. Veamos que se puede construir un producto semidirecto de H con C_2 esto es buscar elementos de orden 2 en H, para esto observemos que H tiene un subgrupo normal C_p y p subgrupos C_q, entonces un automorfismo φ de H de orden dos fija a C_p, y permuta los p diferentes C_q. Así que fija uno de los C_q, y actúa en este y en C_p como la involución $x \rightarrow x^{-1}$ o la identidad. Por lo que H puede ser generado por un generador de C_p y un generador de C_q por ende solo hay un único automorfismo de orden 2, y el otro es el caso trivial. Concluimos que tenemos otros dos grupos no abelianos $H \times C_2$ y $H \rtimes C_2$. Y estos grupos no tienen tablas de marcas isomorfas por que uno es producto directo y el otro un semidirecto.

7.15. Grupos de orden 90

Demostremos que hasta isomorfismos sólo existen 8 grupos no abelianos de orden 90. Observemos primero que $90 = 2 \times 5 \times 3^2$. Aplicando el teorema de P. Hall. tenemos que existe un subgrupo normal H de G, y entonces G es igual a

Sea $G = H \rtimes C_2$ con H subgrupo normal

Sea $|H| = 45$, y sabemos que de orden 45 sólo hay 2 grupos abelianos y no hay abelianos, tales grupos abelianos son:

1. $C_9 \times C_5$
2. $C_3 \times C_3 \times C_5$

Caso 1. $G = (C_9 \times C_5) \rtimes C_2$ veamos si existe un morfismo no trivial $\alpha : C_2 \longrightarrow Aut(C_9 \times C_5)$

Veamos a que es equivalente el grupo de automorfismos:

$$Aut(C_9 \times C_5) \cong Aut(C_9) \times Aut(C_5) \cong C_6 \times C_4$$

los posibles elementos de orden 2 en $C_6 \times C_4$ son:

- ▷ $(C_3, 0)$
- ▷ $(0, C_2)$
- ▷ (C_3, C_2)

Por lo tanto tenemos de este caso 3 elementos no abelianos, los cuales tienen tablas de marcas no isomorfas puesto que el primero tiene a C_3 como factor directo, el segundo tiene a C_2 como factor directo y el tercero no tiene a ninguno de estos 2. Los del caso 1 y los del caso 2 se diferencian porque en el primero hay un p-subgrupo cíclico de Sylow, mientras que en el caso 2 tenemos un espacio vectorial sobre el campo con 3 elementos.

Caso 2. $G = (C_3 \times C_3 \times C_5) \rtimes C_2$ veamos si existe un morfismo no trivial $\beta : C_2 \longrightarrow Aut(C_3 \times C_3 \times C_5)$

Analicemos a qu´e es equivalente este grupo de automorfismos

$Aut(C_3 \times C_3 \times C_5) = Aut(C_3 \times C_3) \times C_5) \cong Aut(C_3 \times C_3) \times Aut(C_5)$ $\cong GL(2,3) \times C_4$

¿Cuáles son los elementos de orden 2 en $GL(2,3) \times C_4$?

▷ (I, C_2)

▷ $([A], 0)$

▷ $([B], 0)$

▷ $([A], C_2)$

▷ $([B], C_2)$

Donde $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

A y B son matrices de tamaño 2×2 con entradas en C_3 que no son conjugadas, cualesquiera dos matrices en $GL(2,3)$ que cumplan que elevadas al cuadrado son iguales a la matriz I son conjugadas a estas. $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ y $B = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$.

Del caso 2 sus tablas de marcas difieren entre s´i puesto que los grupos difieren al tener un subespacio invariante unidimensional o no, y en tener o no a un 2-subgrupo de Sylow.

7.16. Grupos de orden 88

Demostremos que hasta isomorfismo, sólo existen 9 grupos no abelianos. Podemos ver que $88 = 2^3 \times 11$ y que nuestro 11 subgrupo de Sylow es normal en G. Entonces construyamos grupos tales que $|H| = 8 \longrightarrow Aut(C_{11})$.

Las posibilidades para H son las siguientes.

▷ C_8

▷ $C_4 \times C_2$

▷ $C_2 \times C_2 \times C_2$

$\triangleright$ $D_8 \cong C_4 \rtimes C_2$

$\triangleright$ Q_8

Y también tenemos que $Aut(C_{11}) \cong C_{10}$. Analicemos por casos el número de morfismos no triviales de H en C_{10}

Si $H = C_8$ el 4 es el único elemento de orden 2 en C_8 por lo tanto tenemos un único morfismo:

1. $4 \longrightarrow 5$

Si $H = C_4 \times C_2$ tenemos tres elementos de orden 2, hasta isomorfismos.

1. $(0,1) \longrightarrow 5$
2. $(2,0) \longrightarrow 5$
3. $(2,1) \longrightarrow 5$

Si $H = C_2 \times C_2 \times C_2$ tenemos de nuevo tres elementos de orden 2 hasta isomorfismos.

1. $(1,0,0) \longrightarrow 5$
2. $(1,1,0) \longrightarrow 5$
3. $(1,1,1) \longrightarrow 5$

Si $H = D_8 \cong C_4 \rtimes C_2$ en donde solo hay un elemento de orden 2 hasta isomorfismo.

Si $H = Q_8$ hay un elemento de orden 2

Por lo tanto existen hasta isomorfismo, tenemos 9 grupos no abelianos de orden 88

7.17. Grupos de orden 16

Para estos grupos encontramos su clasificación en [5], donde son 14 grupos cuyo orden es 16 hasta isomorfismo y son los siguientes.

- ▷ $G_0 = C_2 \times C_2 \times C_2 \times C_2$
- ▷ $G_1 = C_8 \times C_2$
- ▷ $G_2 = SD_{16}$
- ▷ $G_3 = C_8 \rtimes C_2$
- ▷ $G_4 = D_{16}$
- ▷ $G_5 = Q_{16}$
- ▷ $G_6 = C_{16}$
- ▷ $G_7 = K_4 \times C_4$
- ▷ $G_8 = D_8 \times C_2$
- ▷ $G_9 = K_4 \rtimes C_4$
- ▷ $Q_{10} \rtimes C_2$
- ▷ $Q_{11} \times C_2$
- ▷ $C_{12} \rtimes C_4$
- ▷ $C_{13} \times C_4$

De los cuales 5 grupos son abelianos, a saber: $G_0, G_1, G_6, G_7, G_{13}$

Dentro del grupo de orden 2^x con $x \geq 4$ tenemos 4 grupos no abelianos el Quasidihedrico, Dihedrico, Semidihedrico y "el otro", veremos como se pueden distinguir estos cuatro grupos en sus Tablas de Marcas.

Comenzamos distinguiendo el Grupo de los cuaternios Q_{2n}, el cual tiene entre sus propiedades que tiene un solo elemento de orden 2 y todos sus subgrupos son normales, lo cual lo diferencia de los otros grupos y es distinguible dentro de las tablas de marcas.

Para el grupo Dihedrico D_{2n} tenemos que si $|G| = 2n$ existe un subgrupo cíclico $N \leq G$, $[G : N] = 2, \forall g \in G, g \notin N$ entonces el orden de $g = 2$ mientras que para nuestro grupo de cuaternios era para un único g.

El grupo semidihedrico S_{2n} con representación $\langle r, s | r^{2^{m-1}} = s^2 = 1, srs = r^{2^{m-2}-1} \rangle$ contiene dos subgrupos maximales no cíclicos a saber (D_n, Q_n) que difieren de los grupos anteriores pues el grupo de los cuaternios tiene a (Q_n, Q_n) y el Dihedrico a D_n, D_n, [11] por lo tanto estos grupos no tienen tablas de marcas isomorfas entre sí.

Para el otro grupo con presentación $M = \langle r, s | r^{2^{m-1}} = s^2 = 1, srs = r^{2^{m-2}+1} \rangle$ todos sus subgrupos maximales son abelianos a saber son $C_4 \times C_2$, C_8, C_8 lo cual también se distingue en la tabla de marcas y se diferencia de los otros 3 grupos.

$H \leq M$, $[M : H] = 2$ demostremos que H es abeliano.

$H = \{r^a s^b\}$

Si b es par, tenemos

$r^a s r^b s = r^a (r^b)^{2^{m-2}+1} = r^a r^{2^{m-2}b+b} = r^a r^b$

Si b impar tendríamos

$r^a r^{b-1} 2^{m-2} + 2^{m-2} + b$ pero observemos que $2^{m-2}(b-1)$ es de la forma 2^{m-1} y por la forma de nuestro grupo $r^{2^{m-1}} = 1$. por lo tanto $r^a r^{b-1} 2^{m-2} + 2^{m-2} + b = r^a r^{2^{m-2}+b}$

Veamos para que a's, b's, c's y d's se cumple que $r^a s^b = r^c s^d$.

Sin perdida de generalidad $a, b, c, d \in \{0, 1\}$.

Si $a = 0 \to c = 0$ por lo tanto se cumple la igualdad, caso con b y d es similar.

Si $a = 1 = c$, $r^a s^b = rs$ implicando $r^c s^d = rs$.

H está propiamente contenido en M por lo tanto es un subgrupo maximal abeliano, y concluimos que estos 4 cuatros son diferenciables entre sí dentro de sus tablas de marcas.

Para los otros grupos restantes nótese que uno tine a un grupo cíclico de orden 4 mientras que los otros no G_9, G_{12}, sus 2-subgrupos de Sylow no coinciden. Además los subgrupos normales de G_8, G_{11} no coinciden pues ambos tienen como factor directo a C_2 sabiendo que todos los subgrupos de los cuaternios son normales, G_{10} no satisface las propiedades anteriores. Por lo tanto en orden 16, todos los grupos tienen tablas de marcas distintas.

Finalmente mostremos la última tabla de todos los órdenes de los grupos con los que se trabajó en esta tesis

~~1~~	~~2~~	~~3~~	~~4~~	~~5~~	~~6~~	~~7~~	~~8~~	~~9~~	~~10~~
~~11~~	~~12~~	~~13~~	~~14~~	~~15~~	~~16~~	~~17~~	~~18~~	~~19~~	~~20~~
~~21~~	~~22~~	~~23~~	24	~~25~~	~~26~~	~~27~~	~~28~~	~~29~~	~~30~~
~~31~~	32	~~33~~	~~34~~	~~35~~	36	~~37~~	~~38~~	~~39~~	40
~~41~~	~~42~~	~~43~~	~~44~~	~~45~~	~~46~~	~~47~~	48	~~49~~	~~50~~
~~51~~	~~52~~	~~53~~	54	~~55~~	56	~~57~~	~~58~~	~~59~~	60
~~61~~	~~62~~	~~63~~	64	~~65~~	~~66~~	~~67~~	~~68~~	~~69~~	~~70~~
~~71~~	72	~~73~~	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	~~79~~	80
81	~~82~~	~~83~~	84	~~85~~	~~86~~	~~87~~	~~88~~	~~89~~	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~					

Faltando los grupos de orden $24, 32, 36, 40, 48, 54, 56, 60, 64, 72, 80, 81, 84$ en total 13 para futuros trabajos.

Conclusiones

- ▷ Este trabajo consistió en buscar y demostrar para cada orden el numero de grupos que existen hasta isomorfismo, una vez hecho esto se procedió a dar las razones por las cuales sus tablas de marcas no eran isomorfas.

- ▷ El uso de Gap es meramente ilustrativo pero muy útil, ayuda muy bien a comprender la estructura del grupo, pero aun tiene muchos errores y no podemos confiar en el.

- ▷ El grupo mas complicado fue de orden 16, de encontrarse un ejemplo mas chico que cumpla que los grupos sean no isomorfos y sus tablas de marcas si lo sean, seria en uno de sus múltiplos, recordemos que 96 es múltiplo de 16.

- ▷ Se encontro una manera para distinguir en sus tablas de marcas los 4 grupos no abelianos de orden 2^n que tienen un subgrupo ciclico de orden 2, siendo estos los cuaternios, dihedricos, semidihedricos y el otro grupo.

Referencias

[1] Some invariants preserved by isomorphism of table of marks- Luis M. Huerta-Aparicio, Ariel Molina-Rueda, Alberto G.Raggi-Cardenas, Luis Valero-Elizondo-UMSNH.

[2] Un anillo para controlarlos a todos (los grupos finitos)- Alberto G. Raggi, Luis Valero-Elizondo -UMSNH.

[3] Contemporary Abstract Algebra 2^{nd} edition- Joseph A. Gallian

[4] An introduction to the Theory of Groups 4ed- Joseph J. Rotman. Spinger Verlag. 1994

[5] The groups of order sixteen made easy - Marcel Wild. University of Stellenbosh. American Mathematical Monthly.

[6] Automorphism Groups of Finite p-Groups: Structure and Applications- Geir T. Helleloid. 2007.

[7] Groups of Order 12. Keith Conrad- Paper, University of Connecticut.

[8] Normalizing Isomorphisms Between Burnside Rings- Alberto G. Raggi-Cárdenas and Luis Valero Elizondo- UNAM- Journal of Algebra 277.

[9] Comprobación Computacional de una Conjetura de Tablas de Marcas y Anillos de Burnside- Ariel Molina Rueda, Luis Valero Elizondo, tesis, Facultad de Cs. Físico Matemáticas, UMSNH 2006.

[10] Groups of Order P^3. Keith Conrad- Paper, University of Connecticut.

[11] Group Theory. Vol 1.- Michio Suzuki