UNIVERSIDAD CENTROCCIDENTAL
"LISANDRO ALVARADO"

Decanato de Ciencias y Tecnología
Licenciatura en Ciencias Matemáticas

"Grupos finitos con un numero pequeño de subgrupos cíclicos"

Trabajo Especial de Grado presentado por

Br. Juan Carlos Mongez Duran

como requisito final
para obtener el título de Licenciado
en Ciencias Matemáticas
Área de Conocimiento: Algebra y combinatoria.
Tutor: Prof. Luz Elimar Marchan

Barquisimeto, Venezuela. Abril de 2017

Universidad Centroccidental
"Lisandro Alvarado"
Decanato de Ciencias y Tecnología
Licenciatura en Ciencias Matemáticas

ACTA
TRABAJO ESPECIAL DE GRADO

Los suscritos miembros del Jurado designado por el Jefe del Departamento de Matemáticas del Decanato de Ciencias y Tecnología de la Universidad Centroccidental "Lisandro Alvarado", para examinar y dictar el veredicto sobre el Trabajo Especial de Grado titulado:

"Grupos finitos con un numero pequeño de subgrupos cíclicos"

presentado por el ciudadano Br. Juan Carlos Mongez Duran titular de la Cédula de Identidad No. 25340348, con el propósito de cumplir con el requisito académico final para el otorgamiento del título de Licenciado en Ciencias Matemáticas.

Luego de realizada la Defensa y en los términos que imponen los Lineamientos para el Trabajo Especial de Grado de la Licenciatura en Ciencias Matemáticas, se procedió a discutirlo con el interesado habiéndose emitido el veredicto que a continuación se expresa:

[1] _____

Con una calificación de _____ puntos.

En fe de lo expuesto firmamos la presente Acta en la Ciudad de Barquisimeto a los _____ días del mes de _____ de _____.

_____	_____
TUTOR	FIRMA
_____	_____
PRINCIPAL	FIRMA
_____	_____
PRINCIPAL	FIRMA

OBSERVACIONES:

_____

_____

_____

[1] Aprobado ó Reprobado

ÍNDICE

Introducción **1**

1. Preliminares **2**

1.1. Definiciones Básicas sobre grupos 2

1.1.1. Grupos cíclicos 4

1.2. El grupo simétrico y el grupo de los cuaterniones 6

1.3. Clases laterales 7

1.4. Subgrupos normales 8

2. Grupos de Sylow **11**

2.1. Suma directa de grupos 11

2.2. Acción de un grupo sobre un conjunto 13

2.3. Teoremas de Sylow 14

3. Caracterización de los grupos con a lo más cinco subgrupos cíclicos **20**

3.1. Cálculo y observaciones sobre $C(G)$ 20

3.2. Resultados Principales 25

Conclusiones **34**

Referencias Bibliográficas **35**

INTRODUCCIÓN

Uno de los problemas que estudia la teoría de reticulados consiste en determinar propiedades y características inherentes a la estructura de un grupo finito a partir de la información que aportan los reticulados formados por algunos de sus subgrupos, tales como modularidad, distributividad, dualidad, entre otros. Además, se interpretan algunos resultados de la teoría de grupo usando lenguaje de reticulados. Por esta razón, la teoría de reticulados se considera una herramienta conveniente a usar en la teoría de grupos. Una técnica habitual consiste en asociar a un grupo finito G un conjunto parcialmente ordenado de subgrupos de G, por ejemplo, el conjunto parcialmente ordenado de subgrupos cíclicos de G, denotado generalmente por $C(G)$.

Algunas veces $C(G)$ puede decidir la estructura de G, por ejemplo, un resultado básico de teoría de grupos garantiza que un grupo finito G es un 2-grupo abeliano elemental si y solo si el cardinal de $C(G)$ coincide con el orden de G. Inspirado en este resultado, Tărnăuceanu [2] caracterizó los grupos finitos G para los cuales el cardinal de $C(G)$ coincide con el orden de G menos uno. Además planteó como un problema abierto lo siguiente:

> Describir los grupos finitos G tales que el cardinal de $C(G)$ es igual al orden de G menos r, donde r esta entre 2 y el orden de G menos 1.

Posteriormente Tărnăuceanu [3] caracterizó los grupos finitos para los cuales el cardinal de $|C(G)|$ coincide con el orden de G menos dos. Recientemente, Zhou [4] demostró que si G es un grupo finito, el cardinal de $C(G)$ es igual al orden de G menos tres si y solo si G es isomorfo al grupo diédrico D_{10} o al grupo de los cuaterniones Q_8.

Sin embargo, existen pocos trabajos sobre la relación entre el cardianal de $C(G)$, el orden de G y la estructura de G. Particularmente, si el grupo posee un número pequeño de subgrupos cíclicos. En este trabajo estudiaremos un artículo reciente de Zhou [5], en el cual se clasifican los grupos que poseen a lo más cinco subgrupos cíclicos.

El trabajo consta de tres capítulos. En el primer capítulo recordamos algunas definiciones, notaciones y resultados básicos relativos a grupos, en el segundo capítulo desarrollamos parte de la teoría de grupos de Sylow la cual es una parte fundamental para alcanzar nuestros objetivos principales, los cuales ofrecemos en el tercer capítulo.

CAPÍTULO 1

PRELIMINARES

En este capítulo definimos la terminología y presentamos algunas definiciones, notaciones y resultados elementales, necesarios como base teórica de este trabajo. Las demostraciones que omitimos pueden ser encontrados en cualquier texto de álgebra, entre ellos [1].

1.1. Definiciones Básicas sobre grupos

En esta sección vamos a fijar nuestra notación y a revisar brevemente algunas propiedades de los grupos finitos.

Recordemos que dado un conjunto no vacío G, una operacion binaria en G es una función de $G \times G$ en G. Dados $a, b \in G$, denotaremos por ab a la imagen de la operación binaria aplicada a el par ordenado (a, b).

Definición 1.1. Un semigrupo es un conjunto no vacío dotado de una operacion binaria la cual es asociativa, es decir,

$$a(bc) = (ab)c, \text{ para todo } a, b \in G.$$

Un Monoide es un semigrupo que contiene un elemento $e \in G$ (elemento neutro) tal que,

$$eb = be = b, \text{ para todo } b \in G.$$

Un grupo es un Monoide para el cual dado $a \in G$, existe a^{-1} tal que

$$aa^{-1} = a^{-1}a = e,$$

donde e es un elemento neutro del monoide.

Si la operación binaria del grupo es conmutativa, diremos que el grupo es abeliano.

Si G es un grupo, el *orden* de G es el número cardinal de G, el cual denotamos por $|G|$. Si $|G|$ es finito, decimos que G es finito. Sin riesgo de confusión, tambien denotaremos el cardinal de un conjunto A por $|A|$.

Definición 1.2. Sea H un subconjunto no vacío de G, donde G es un grupo y H es cerrado bajo la operación del grupo G. Si H es en sí mismo un grupo, con la operación de G, entonces diremos que H es un subgrupo de G y lo denotaremos por $H < G$.

El siguiente teorema da condiciones suficientes sobre un subconjunto de un grupo para que éste sea un subgrupo.

Teorema 1.1. *Sea H un subconjunto no vacío de un grupo G, H es un subgrupo de G si y solo si, para todo $h_1, h_2 \in H$, $h_1 {h_2}^{-1} \in H$.*

Ejemplo 1.1. Sea H un subgrupo de un grupo G y sea $a \in G$, el conjunto

$$aHa^{-1} := \{g \in G : g = aha^{-1}, h \in H\}$$

es un subgrupo de G. En efecto,

Sean $g_1, g_2 \in aHa^{-1}$, por definición, existen $h_1, h_2 \in H$ tales que $g_1 = ah_1a^{-1}$ y $g_2 = ah_2a^{-1}$, notemos que $g_2^{-1} = ah_2^{-1}a^{-1}$. Por otro lado,

$$g_1g_2^{-1} = (ah_1a^{-1})(ah_2^{-1}a^{-1}) = a(h_1h_2^{-1})a^{-1} \in aHa^{-1} \text{ (ya que } H < G)$$

Así, por el Teorema 1.1, aHa^{-1} es un subgrupo de G.

Definición 1.3. Sean G y K dos grupos, una función $f : G \to K$, tal que para $a, b \in G$,

$$f(ab) = f(a)f(b),$$

es llamada homomorfismo de G en K.

Si f es biyectiva decimos que f es un isomorfismo, en cuyo caso decimos también que G es isomorfo a K y lo denotamos por $G \cong K$.

Es fácil ver que si $f : G \to K$ es un isomorfismo de grupos, $f^{-1} : K \to G$ es también un isomorfismo. De modo que decimos simplemente: G y K son isomorfos, sin importar el orden de G y K.

Ejemplo 1.2. Sea H un subgrupo de un grupo G, para todo $a \in G$, el subgrupo aHa^{-1} de G, es isomorfo a H. En efecto,

Sea $f : H \to aHa^{-1}$, dada por $f(h) = aha^{-1}$. Veamos que f es un isomorfismo.

Sean $h_1, h_2 \in H$,

$$f(h_1h_2) = a(h_1h_2)a^{-1} = ah_1(a^{-1}a)h_2a^{-1} = (ah_1a^{-1})(ah_2a^{-1}) = f(h_1)f(h_2).$$

Así f es un homomorfismo. Además,

$$f(h_1) = f(h_2) \Rightarrow ah_1a^{-1} = ah_2a^{-1} \Rightarrow h_1 = h_2.$$

Por lo que f es inyectiva. Por otro lado, para $g \in aHa^{-1}$, existe $h \in H$ tal que

$$g = aha^{-1} = f(h),$$

por lo que f es sobreyectiva.

Luego, podemos concluir que f es un isomorfismo y por tanto $H \cong aHa^{-1}$.

1.1.1. Grupos cíclicos

Sea A un subconjunto no vacío de un grupo G, el *subgrupo* generado por A, denotado por $\langle A \rangle$, es la intersección de todos los subgrupos de G que continen a A, se sabe que

$$\langle A \rangle = \{a_1^{n_1}a_2^{n_2} \cdots a_t^{n_t} : a_1, \ldots, a_t \in A, n_i \in \mathbb{Z}, 1 \leq i \leq t, t \in \mathbb{N}\}.$$

En particular, si $A = \{a\}$ es unitario, escribimos $\langle a \rangle$ en lugar de $\langle \{a\} \rangle$ y

$$\langle a \rangle = \{a^n : n \in \mathbb{Z}\}.$$

Si $G = \langle a \rangle$, decimos que G es *cíclico*.

El siguiente teorema garantiza que, salvo isomorfismo, existe únicamente dos grupos cíclicos.

Teorema 1.2. *Todo grupo cíclico finito de orden n es isomorfo a $\mathbb{Z}_n$ y todo grupo cíclico infinito es isomorfo a $\mathbb{Z}$.*

Como todos los grupos cíclicos de orden n son isomorfos, denotaremos por C_n al grupo cíclico de orden n.

Definición 1.4. Sea G un grupo y $a \in G$, definimos el orden de a, y lo denotamos por $|a|$, como el orden del subgrupo $\langle a \rangle$.

Teorema 1.3. *Sea G un grupo y $a \in G$, si a tiene orden finito n entonces:*

1. *n es el menor entero positivo tal que $a^n = e$.*
2. *$a^k = e$ si y solo si $n|k$.*
3. *$\langle a \rangle$ esta formado por los elementos $a, a^2, a^3, \ldots, a^n$, los cuales son distintos entre sí.*
4. *Para cada $k \in \mathbb{Z}$ tal que k divide a n, $|a^k| = \frac{n}{k}$.*

Recordemos que la función phi de Euler es la función $\phi : \mathbb{N} \longrightarrow \mathbb{N}$ la cual asigna a cada número n el número $\phi(n)$ de enteros positivos menores o iguales a n que son coprimos con n

Ejemplos 1.1. 1. $\phi(1) = 1$.

2. Si p es primo, $\phi(p) = p - 1$, ya que todo los números menores a p son coprimos con p.
3. Si p es primo y $k \geq 1$ $\phi(p^k) = (p-1)p^{k-1}$.

El siguiente resultado garantiza que un grupo cíclcico de orden n tiene $\phi(n)$ generadores.

Teorema 1.4. *Sea G un grupo cíclico con orden finito n y a un generador de G, $\langle a^k \rangle = \langle a \rangle$ si y solo si n y k son coprimos. En particular, el número de generadores de G es $\phi(n)$.*

Observación 1.1. Sean C_p y C_q dos subgrupos cíclicos de un grupo G, de orden p y q, respectivamente, con p y q primos distintos, entonces $C_p \cap C_q = \{e\}$. Para ver esto notemos que por el Teorema 1.4, al ser p y q primos, para todo $a^k \in C_p \setminus \{e\}$, $C_p = \langle a^k \rangle$

y para todo $b^r \in C_q \setminus \{e\}$, $C_q = \langle b^r \rangle$ luego, si C_p y C_q compartieran algún elemento no trivial $a^k = b^r$ entonces, $\langle a^k \rangle \subseteq C_p \cap C_q$, implicando $C_p = \langle a^k \rangle = \langle b^r \rangle = C_q$, lo cual es imposible porque se han supuesto p y q distintos.

Definición 1.5. Dado un grupo G se define el exponente de G, denotado por $\exp(G)$, al menor entero positivo tal que $a^n = e$ para todo $a \in G$, es decir $exp(G) = min(\{s \in \mathrm{N} \setminus x^s = e, \forall x \in G\})$

Observación 1.2. Note que para grupos finitos $exp(G)$ siempre existe solo basta tomar el mínimo común múltiplo de todo los ordenes y este coincide con $exp(G)$. Ademas si G es un p-subgrupo de orden p^n, $exp(G) = p^s \leq p^n$ ya que todo los elementos tendrán potencia de p y ademas existirá un elemento de G con orden $exp(G)$

1.2. El grupo simétrico y el grupo de los cuaterniones

El grupo de los cuaterniones, denotados por Q_8, es grupo generado por las siguientes matrices complejas, con la multiplicación usual.

$$A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \; B = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

Se puede probar sin mucha dificultad que Q_8 es un grupo no abeliano de orden 8, además $|A| = |B| = 4$ y $BA = A^3B$, por lo que cada elemento de Q_8 es de la forma A^iB^j. Más aún

$$Q_8 = \{I, A, A^2, A^3, B, B^3, A^3B = BA, AB\}.$$

Y de esto tenemos que Q_8 tiene 5 subgrupos cíclicos, ellos son: $\langle I \rangle = \{I\}$, $\langle A \rangle = \langle A^3 \rangle = \{I, A, A^2, A^3\}$, $\langle A^2 \rangle = \{I, A^2\}$, $\langle B \rangle = \langle B^3 \rangle = \{I, B, A^2, B^3\}$, y $\langle A^3B = BA \rangle \langle AB \rangle = \{A^3B = BA, A^2, AB, I\}$

El siguiente resultado da condiciones para que un grupo finito de orden 8 sea isomorfo al grupo de los cuaterniones.

Teorema 1.5. *Sea G un grupo tal que existan $a, b \in G$ que satisfagan $a^4 = b^4 = e$, $a^2 = b^2$ y $ba = a^3b = a^{-1}b$, $a \neq b$ y $G = \langle a, b \rangle$, entonces $G \cong Q_8$.*

Otro grupo que juega un rol importante en la teoría de representación de grupos finitos el grupo simétrico. Dado $n \in \mathbb{N}$, tomamos $I_n = \{1, 2, \ldots, n\}$. El conjunto de

todas las biyecciones de I_n en I_n, dotado de la composición de funciones, es un grupo, el cual es llamado el grupo simétrico y denotado por S_n. Los elementos de S_n son llamados permutaciones y la permutación identidad es denotada por (1). Es conocido que $|S_n| = n!$. Dada $\sigma \in S_n$, σ lo escribimos de la siguiente forma:

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

Si $\{i_1, i_2, \dots, i_n\} \subseteq I_n$, la notación $\sigma = (i_1\, i_2\, \dots\, i_n)$ denota la permutación tal que $\sigma(i_j) = i_{j+1}$ para cada $j \in \{1, \dots, n-1\}$, $\sigma(i_n) = i_1$ y $\sigma(x) = x$ si $x \notin \{i_1, i_2, \dots, i_n\}$. Tales permutaciones son llamadas ciclos.

En particular,

$$S_3 = \{(1), (1,2), (1,3), (2,3), (1,2,3), (3,2,1)\}.$$

Notemos que $S_3 = \langle (1,2), (1,2,3) \rangle$, $|(1,2,3)| = 3$ y $|(1,2)| = 2$, además, $(1,2)(1,2,3) = (2,3)$ y $(1,2,3)^{-1}(1,2) = (3,2,1)(1,2) = (2,3)$.

Otro aspecto resaltante es que S_3 tiene 5 subgrupos cíclicos ya que $\langle (1) \rangle = \{(1)\}$, $\langle (1,2) \rangle = \{(1,2), (1)\}$, $\langle (1,3) \rangle = \{(1,3), (1)\}$, $\langle (2,3) \rangle = \{(2,3), (1)\}$ y $\langle (1,2,3) \rangle = \langle (3,2,1) \rangle = \{(1,2,3), (3,2,1), (1)\}$

Teorema 1.6. *Sea G un grupo finito y $a, b \in G$ tales que $G = \langle a, b \rangle$, $|a| = 3$, $|b| = 2$ y $ba = a^{-1}b$. Entonces, $G \cong S_3$.*

1.3. Clases laterales

Sea H un subgrupo de un grupo G y $a, b \in G$, decimos que a es congruente por la derecha con b módulo H, y escribimos $a \equiv_d b \,(\text{mód } H)$, si $ab^{-1} \in H$; análogamente, decimos que a es congruente por la izquierda con b módulo H, y escribimos $a \equiv_i b \,(\text{mód } H)$, si $a^{-1}b \in H$.

Teorema 1.7. *Si H es un subgrupo de un grupo G, se cumple:*

1. *La congruencia módulo H por la derecha (por la izquierda) es una relación de equivalencia.*

2. *La clase de equivalecia de $a \in G$ bajo la relación de equivalencia módulo H por la derecha (por la izquierda) es el conjuntos $Ha = \{ha : h \in H\}$ (y $aH = \{ah : h \in H\}$, respectivamente).*
3. $|Ha| = |H| = |aH|$.
4. *Si R es el conjunto de las clases de equivalencias inducidas por la relación de congruencia módulo H por la derecha y L es el conjunto de clases de equivalencia inducida por la relación de equivalencia módulo H por la izquierda, entonces $|R| = |L|$. Al entero $|R|$ se le llama índice de H en G y se denota por $[G : H]$.*

Las clases de equivalecia bajo la relación de equivalencia módulo H son llamadas *clases laterales módulo H*.

Teorema 1.8. *Sean K, H, G grupos tal que $H < K < G$ entonces,*

$$[G : K] = [G : H][H : K].$$

Una piedra angular en la teoría de grupos finitos es el teorema de Lagrange, el cual usamos ampliamente en este trabajo.

Teorema 1.9 (Teorema de Lagrange)**.** *Si H es un subgrupo de un grupo G entonces,*

$$|G| = [G : H]|H|.$$

Ejemplo 1.3. Todo grupo G de orden p, con p primo, es cíclico.
En efecto, cualquier $a \in G \setminus \{e\}$ debe tener orden p, ya que por el Teorema de Lagrange $|a|$ debe dividir a p, y como $a \neq e$, $|a| \neq 1$, así $|\langle a \rangle| = |a| = p = |G|$, implicando $G = \langle a \rangle$.

1.4. Subgrupos normales

Teorema 1.10. *Sea N un subgrupo de un grupo G, entonces son equivalentes las siguientes proposiciones:*

1. *Para todo $a \in G$, $aN = Na$.*
2. *Para todo $a \in G$, $aNa^{-1} \subset N$.*

3. *Para todo* $a \in G$, $aNa^{-1} = N$.

Un subgrupo N de un grupo G que satisface alguna de las condiciones del Teorema 1.10 es llamado *subgrupo normal de* G, para denotar este hecho escribimos $N \triangleleft G$.

Ejemplo 1.4. Si N es un subgrupo de un grupo G con índice 2 entonces, N es normal en G.

En efecto, como $[G : N] = 2$, podemos suponer que existe $a \in G \setminus \{e\}$ tal que $G = N \cup aN$ y $G = N \cup Na$, luego $aN = G \setminus N = Na$, así N es normal en G.

Ejemplo 1.5. Si H es el único subgrupo de orden n de un grupo G entonces, H es normal en G.

En efecto, para todo $a \in G$, aHa^{-1} es un subgrupo de G (ver Ejemplo 1.1), más aún $aNa^{-1} \cong N$ (ver Ejemplo 1.2), por lo que $|aNa^{-1}| = |N| = n$ pero, como solo existe un grupo de orden n, $aNa^{-1} = N$, por lo tanto N es normal en G.

Observemos que si N es un subgrupo normal de un grupo G, el conjunto de clases laterales por la izquierda coinicide con el conjunto de clases laterales por la derecha, denotamos a este conjunto por G/N. Es bien sabido que en este caso G/N tiene estructura de grupo con la siguiente operación binaria, para $aN, bN \in G/N$, $aNbN = abN$.

Teorema 1.11. *Sean* K *y* N *subgrupos de un grupo* G*, con* N *normal en* G *entonces,*

1. $N \cap K$ *es un subgrupo normal de* K.
2. $NK = KN$*, donde* $NK := \{nk : n \in N, k \in K\}$ *y* $KN := \{kn : k \in K, n \in N\}$.
3. *Si* K *es normal en* G *y* $N \cap K = \langle e \rangle$ *, entonces* $nk = kn$ *para todo* $n \in N$ *y* $k \in K$.

Ejemplo 1.6. Sean H y K subgrupos normales de G entonces, HK es un subgrupo normal de G. Más aún, sea $N_1, N_2, \ldots, N_k$ una colección finita de subgrupos normales de G, tal que para todo $1 \leq i \leq n$, $N_i \cap (\bigcup_{j \neq i} N_j) = \{e\}$, entonces

$$N_1 N_2 \cdots N_k := \{n_1 n_2 \cdots n_k : n_i \in N_i, 1 \leq i \leq k\}$$

es un subgrupo normal en G.

En efecto, el Teorema 1.11 parte 2) implica que HK es subgrupo de G. Ahora, dado $a \in G$, $aHKa^{-1} = aH(a^{-1}a)Ka^{-1} = (aHa^{-1})(aKa^{-1}) = HK$, así HK es subgrupo normal de G. Un proceso inductivo nos lleva a la segunda conlusión.

Finalizamos esta sección con un teorema que establece una correspondencia biunívoca entre ciertos subgrupos de un grupo y los subgrupos de un conjunto cociente.

Teorema 1.12. *Si N es un subgrupo normal de G, entonces cada subgrupo de G/N es de la forma K/N donde K es un subgrupo de G que contiene a N. Además, $K//N$ es normal en G/N si y solo si K es normal en G.*

CAPÍTULO 2

GRUPOS DE SYLOW

Estudiar los grupos finitos no abelianos es una tarea más complicada que estudiar los grupos abelianos finitos. Los teoremas de Sylow son el primer paso básico para entender la estructura de un grupo finito arbitario. La motivación principal de este estudio es la respuesta a la siguiente pregunta, ¿si un entero positivo m divide el orden de un grupo G, G tiene un subgrupo de orden m?, éste es el recíproco del Teorema de Lagrange y sabemos que se cumple para los grupos cíclicos, incluso para los grupos abelianos finitos. Los teoremas de Sylow dan respuesta a esta pregunta en el caso que m potencia de un primo. Comenzamos recordando algunos resultados concernientes a suma directas de grupos y acción de un grupo sobre un conjunto.

2.1. Suma directa de grupos

Teorema 2.1. *Sea* $(G_1, *_1)$, $(G_2, *_2)$,. . . ,$(G_n, *_n)$ *una colección finita de grupos, el conjunto* $G_1 \times G_2 \times \ldots \times G_n$ *dotado de la operación binaria dada por*

$$(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n) = (a_1 *_1 b_1, a_2 *_2 b_2, \ldots, a_n *_n b_n),$$

es un grupo, el cual llamamos suma directa de $G_1, G_2, \ldots, G_n$*, y denotamos por*

$$G_1 \bigoplus G_2 \bigoplus \ldots \bigoplus G_n.$$

Observemos que si $G_1, G_2, \ldots, G_n$ son subgrupos de un grupo G, la suma directa $G_1 \bigoplus G_2 \bigoplus \cdots \bigoplus G_n$ coincide con $G_1 \times G_2 \times \ldots \times G_n$, ya que la operación binaria en cada subgrupo G_i es la misma para todos los subgrupos.

Sea $A_1, A_2, \ldots, A_k$ una colección finita de subconjuntos de un grupo G, denotamos por $A_1A_2 \ldots A_n$ al siguiente conjunto:

$$A_1A_2 \ldots A_k := \{a_1a_2 \ldots a_k : a_i \in A_i, \text{ para } 1 \leq i \leq k\}.$$

Teorema 2.2. *Si m es un entero positivo, tal que m se descompone en factores primos como $m = {p_1}^{n_1}{p_2}^{n_2} \ldots {p_t}^{n_t}$, con $p_1, p_2, \ldots p_{n_t}$ primos distintos y cada n_i un entero positivo, entonces*

$$\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{n_1}} \mathbb{Z}_{p_2^{n_2}} \ldots \mathbb{Z}_{p_t^{n_t}}.$$

Proposición 2.1. *Sean C_m y C_n subgrupos cíclicos normales, de orden m y n, respectivamente de un grupo G , tales que $C_m \cap C_n = \{e\}$, entonces*

$$C_mC_n \cong C_m \times C_n.$$

Demostración. Notemos que como C_m y C_n son normales en G, el Teorema 1.11 parte 2) garantiza que C_mC_n es un subgrupo de G, ya que los elementos de C_m conmutan con los elementos de C_n. Supongamos que $C_m = \langle a \rangle$ y $C_n = \langle b \rangle$, entonces todo elemento de C_mC_n se escribe como a^rb^s con $r, s \in \mathbb{Z}$, más aún, $a^rb^s = b^sa^r$, notemos también que los elementos de $C_m \times C_n$ se escriben de la forma (a^r, b^s) con $r, s \in \mathbb{Z}$.

La función $f : C_m \times C_n \to C_mC_n$, dada por $f((a^r, b^s)) = a^rb^s$ es un isomorfismo. En efecto, dados $(a^r, b^s), (a^t, b^l) \in C_m \times C_n$

$$f((a^r, b^s)(a^t, b^l)) = f((a^ra^t, b^sb^l)) = (a^ra^t)(b^sb^l) = (a^rb^s)(a^tb^l) = f((a^r, b^s))f((a^t, b^l)).$$

Por lo que f es homorfismo. Ahora,

$$\begin{aligned} f((a^r, b^s)) = f((a^t, b^l)) \Rightarrow a^rb^s = a^tb^l \quad &\Rightarrow \quad a^{r-t} = b^{s-l} \\ &\Rightarrow \quad a^{r-t}, b^{s-l} \in C_m \cap C_n = \{e\} \\ &\Rightarrow \quad a^{r-t} = e \wedge b^{s-l} = e \\ &\Rightarrow \quad a^r = a^t \wedge b^s = b^l \\ &\Rightarrow \quad (a^r, b^s) = (a^t, b^l) \end{aligned}$$

De modo que f es inyectiva. La sobreyectidad es evidente. Podemos concluir entonces que $C_m C_n \cong C_m \times C_n$.

■

Observación 2.1. Sea $C_1, C_2, \ldots, C_k$ una colección finita de subgrupos cíclicos normales de G, tal que $C_i \cap (\bigcup_{j \neq i} C_j) = \{e\}$, entonces

$$C_1 C_2 \ldots C_k \cong C_{n_1} \times C_{n_2} \times \ldots \times C_{n_k}.$$

Para ver esto, basta proceder por inducción sobre el número de subgrupos de la colección y usar la Proposición 2.1.

En particular, si $C_{p_1}, C_{p_2}, \ldots, C_{p_k}$ es una colección finita de subgrupos cíclicos normales de G con $p_1, p_2, \ldots, p_k$ primos distintos,

$$\begin{aligned} C_{p_1} C_{p_2} \ldots C_{p_k} &\cong C_{p_1} \times C_{p_2} \times \ldots \times C_{p_k} \\ &\cong \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \ldots \times \mathbb{Z}_{p_k} \\ &\cong \mathbb{Z}_{p_1 p_2 \ldots p_k} \text{ (por Teorema 2.2)} \\ &\cong C_{p_1 p_2 \ldots p_k} \end{aligned}$$

2.2. Acción de un grupo sobre un conjunto

Definición 2.1. Una acción de un grupo G sobre un conjunto S es una aplicación $* : G \times S \to S$, tal que para todo $g_1, g_2 \in G$ y $x \in S$ se cumple que $e * x = x$ y $(g_1 g_2) * x = g_1 * (g_2 * x)$.

Ejemplo 2.1. Sea H un subgrupo de un grupo G. La aplicación $* : H \times G \to G$ dada por $h * x = hxh^{-1}$, es una acción de H sobre G llamada *acción conjugación*, al elemento hxh^{-1} se le dice conjugado de x. En este caso decimos que H actúa sobre G por conjugación.

Consideremos el conjunto S de todos los subgrupos de un grupo G, sabemos que para todo $h \in H$ y $K \in S$, hKh^{-1} es un subgrupo de G isomorfo a K (ver Ejemplos 1.1 y 1.2). La aplicación $* : H \times S \to S$ dada por $h * K = hKh^{-1}$ es una acción de H sobre S llamada *acción conjugación*, al elemento hKh^{-1} se le dice subgrupo conjugado a K. En este caso decimos que H actúa sobre S por conjugación.

Teorema 2.3. *Dado un grupo G que actúa sobre un conjunto S, se cumple:*

1. *La relación sobre S definida por $x \sim y$ si y solo si $g * x = y$ para algún $g \in G$, es una relación de equivalencia.*
2. *Para cada $x \in S$, $G_x = \{g \in G : g * x = x\}$ es un subgrupo de G.*

Observación 2.2. Las cases de equivalencias mencionadas en el Teorema 2.3 son llamadas *órbitas*. La órbita de $x \in S$ es denotada por $\bar{x}$. El subgrupo G_x es llamado el *estabilizador de x*.

Ejemplo 2.2. Si un subgrupo H de un grupo G actúa sobre el conjunto de todos los subgrupos de G por conjugación, el estabilizador de un subgrupo K de G, el cual es $G_K = \{h \in H : hKh^{-1} = K\}$, es llamado *normalizador* de K en H y denotado por $N_H(K)$. Claramente cada subgrupo K es normal en $N_H(K)$ y K es normal en G si y solo si $N_H(K) = G$.

Teorema 2.4. *Si un grupo G actúa sobre un conjunto S, entonces el numero de elementos de la órbita de $x \in S$ es el índice $[G : G_x]$, es decir,*

$$|\overline{x}| = [G : G_x]$$

Corolario 2.1. *El número de conjugados que tiene un subgrupo H de un grupo G es $[G : N_G(H)]$.*

En adelante, cuando un grupo G actúe sobre un conjunto S, para $g \in G$ y $x \in S$ usaremos la notación gx en lugar de $g * x$. El contexto evitará abigüedades con la operación interna del grupo G.

2.3. Teoremas de Sylow

Lema 2.1. *Sea H un grupo de orden p^n actuando sobre un conjunto finito S y sea $S_0 = \{x \in S \mid gx = x \text{ para todo } g \in G\}$, entonces*

$$|S_0| \equiv |S| \,(mód\ p).$$

Demostración. Nótese que para $x \in S$, la órbita $\bar{x}$ contiene exactamente un elemento si y solo si $x \in S_0$, además, sabemos que S es unión disjunta de órbitas, así $S =$

$S_0 \cup \bar{x_1} \cup \bar{x_2} \cup \ldots \cup \bar{x_l}$, donde cada $\bar{x_i}$ tiene más de un elemento, esto implica que $|S| = |S_0| + |\bar{x_1}| + |\bar{x_2}| + \ldots + |\bar{x_l}|$, ahora p divide a $|\bar{x_i}|$ para cada i, ya que $|\bar{x_i}| > 1$ y por el Teorema 2.4 y el Teorema de Lagrange, $|\overline{x}_i| = [H : H_{x_i}]$ divide a $|H| = p^n$. Por tanto,

$$|S| = |S_0| + pl$$

Con $l \in \mathbb{N}$. ■

El siguiente teorema responde parcialmente la pregunta planteada al inicio de este capítulo.

Teorema 2.5 (Teorema de Cauchy)**.** *Si G es un grupo finito cuyo orden es divisible por un número primo p, entonces G contiene un elemento de orden p.*

Demostración. sea $S = \{(a_1, a_2, \ldots, a_p) \in G^p : a_i \in G,\ a_1 a_2 \ldots a_p = e\}$, $(e, e, \ldots, e) \in S$ por lo que $S \neq \emptyset$. Ya que a_p está determinado de forma única por $(a_1 a_2 \ldots a_{p-1})^{-1}$, tenemos que $|S| = n^{p-1}$, donde $n = |G|$. Como p divide a n, $|S| \equiv 0 \,(\text{mód}\, p)$.

La aplicación $\mathbb{Z}_p \times S \longrightarrow S$, dada por $\bar{k}(a_1, a_2, \ldots, a_p) = (a_{k+1}, a_{k+2}, \ldots, a_p, a_1 \ldots, a_k)$ es una acción de $\mathbb{Z}_p$ sobre S.

Ahora, $(a_1, a_2, \ldots, a_p) \in S_0$ si y solo si $a_1 = a_2 = \ldots = a_p$, como $(e, e, \ldots, e) \in S_0$, $|S_0| > 0$ y por el Lema 2.1, existen al menos p elementos en S_0 luego, existe $a \neq e$ tal que $(a, a, \ldots, a) \in S_0$, por lo que $a^p = e$ y, como p es primo, el Teorema 1.3 implica que a debe tener orden p, así existe un subgrupo cíclico de orden p en H. ■

Un grupo G es un *p-grupo* si cada uno de sus elementos tiene como orden una potencia de un primo p fijo. Si H es un subgrupo de G y H es un p-grupo, decimos que H es un *p-subgrupo de G*. En particular, $G = \langle e \rangle$ es un p-subgrupo de G, para todo primo p, ya que $|e| = p^0$.

Corolario 2.2. *Un grupo finito G es un p-grupo si y solo si $|G|$ es una potencia de p.*

Demostración. Supongamos que G es un p-grupo, si $G = e\rangle$, evidentemente |G| es una potencia de p. Supongamos $G \neq \langle e \rangle$ y sea q un divisor primo de $|G|$, por el Teorema de Cauchy, existe un elemento en G de orden q, pero todos los elementos de G tienen orden potencia de p, así q debe ser igual a p, por lo tanto $|G|$ es un potencia de p. El recíproco es consecuencia inmediata del Teorema de Lagrange. ■

Lema 2.2. *Si H es un p-subgrupo de un grupo finito G, entonces*

$$[N_G(H) : H] \equiv [G : H] \, (mód p).$$

Demostración. Sea S el conjunto de las clases laterales izquierda módulo H en G, entonces $|S| = [G : H]$. Consideremos la acción de S sobre H dada por $h(xH) = (hx)H$. Entonces,

$$\begin{aligned} xH \in S_0 &\Leftrightarrow hxH = xH, \text{ para todo } h \in H \\ &\Leftrightarrow x^{-1}hxH = H, \text{ para todo } h \in H \\ &\Leftrightarrow x^{-1}hx \in H, \text{ para todo } h \in H \\ &\Leftrightarrow x^{-1}Hx = H \\ &\Leftrightarrow xHx^{-1} = H \\ &\Leftrightarrow x \in N_G(H). \end{aligned}$$

Así, $|S_0|$ es el número de clases laterales izquierda módulo H con $x \in N_G(H)$; esto es, $|S_0| = [N_G(H) : H]$ y por el Lema 2.1, $[N_G(H) : H] = |S_0| \equiv |S| \, (\text{mód } p)$ pero $[G : H]$. ■

Corolario 2.3. *Sea H un p-subgrupo de un grupo finito G. Si p divide a $[G : H]$, entonces $N_G(H) \neq H$.*

Demostración. Dado que p divide a $[G : H]$, $[G : H] \equiv 0 \, (\text{mód } p)$, luego el Lema 2.2 implica $[N_G(H) : H] \equiv [G : H] \, (\text{mód } p) \equiv 0 \, (\text{mód } p)$, pero $[N_G(H) : H] \geq 1$, así $[N_G(H) : H] > 1$ y por tanto $N_G(H) \neq H$. ■

Teorema 2.6 (Primer Teorema de Sylow)**.** *Sea G un grupo de orden $p^n m$ con $n \geq 1$, p primo y coprimo con m. Entonces G contiene un subgrupo de orden p^i para cada $1 \leq i \leq n$ y cada subgrupo de G de orden p^i, $(i < n)$ es normal en algún subgrupo de orden p^{i+1}.*

Demostración. Como p divide a $|G|$, por el Teorema de Cauchy existe $a \in G$ tal que $|a| = p$.

Supongamos, por inducción, que H es un subgrupo de G de orden p^i con $1 \leq i < n$. Por el Teorema 1.9 p divide a $[G : H]$ y por el Lema 2.2 y el Corolario 2.3 H es normal

en $N_G(H)$, $H \neq N_G(H)$ y $1 < |N_G(H)/H| = [N_G(H) : H] \equiv [G : H] \equiv 0 \,(\text{mód } p)$. Así p divide a $|N_G(H)/H|$ y por el Teorema de Cauchy, $N_G(H)/H$ contiene un subgrupo de orden p, notemos que el Corolario 1.12, implica que tal subgrupo es de la forma H_1/H, donde H_1 es un subgrupo de $N_G(H)$ conteniendo a H. Como H es normal en $N_G(H)$, H es normal en H_1. Finalmente $|H_1| = |H||H_1/H| = p^i p = p^{i+1}$ ■

Sea p un número primo. Un subgrupo P de un grupo G es llamado un *p-subgrupo de Sylow*, si P es un p-subgrupo maximal de G, esto es, si H es un p-subgrupo de G con $P < H < G$ entonces, $H = P$.

Observación 2.3. los p-grupos de Sylow siempre existen y cada p-subgrupo esta contenido en un p-subgrupo de Sylow.

Corolario 2.4. *Sea G un grupo de orden $p^n m$ con $n \geq 1$, p primo y coprimo con m y sea H un p-subgrupo de G, entonces se cumple:*

1. *H es p-subgrupo de Sylow de G si y solo si $|H| = p^n$.*
2. *Cada conjugado de un p-subgrupo de Sylow es un p-subgrupo de Sylow.*
3. *Si existe un único p-subgrupo de Sylow P, entonces P es normal en G.*

Demostración.

1. Supongamos que H es un p-subgrupo de Sylow de G, el Corolario 2.2 y el Teorema de Lagrange implican que $|H| = p^k$ para algún $0 \leq k \leq n$. Supongamos $k < n$. Por el primer Teorema de Sylow, existe un p-subgrupo K de G tal que $|K| = p^n$ y $H < K < G$, como H es maximal, $H = K$ lo cual contradice nuestra suposición, en consecuencia, $|H| = |K| = p^n$. Recíprocamente, si H es un p-subgrupo de G con $|H| = p^n$ y K es un p-subgrupo de G tal que $H < K < G$, entonces $|K| \geq |H| = p^n$, pero por el Teorema de Lagrange,$|K|$ divide al orden de $G = p^n m$, como p y m son primos relativos, tenemos que $|K| \leq p^n$, luego $|K| = |H|$ implicando $H = K$, así H es maximal, es decir, H es un p-subgrupo de Sylow.
2. Si K es un conjugado de un p-subgrupo de Sylow H, entonces $K = aHa^{-1}$ para algún $a \in G$. El Ejemplo 1.2 implica que K y H deben tener el mismo orden y la parte 1) implica que K es un p-subgrupo de Sylow.

3. Por la parte 1) existe un único subgrupo de orden p^n y por el Ejemplo 1.5, éste seria normal en G.

■

Teorema 2.7 (Segundo Teorema de Sylow)**.** *Si H es un p-subgrupo de un grupo finito G y P es un p-subgrupo de Sylow de G, entonces existe $x \in G$ tal que H es un subgrupo de xPx^{-1}. En particular, cualquier par de p-subgrupos de Sylow de G son conjugados.*

Demostración. Sea S el conjunto de las clases laterales a izquierda módulo P en G y sea H actuando sobre S como en la demostración del Lema 2.2. Por el Lema 2.1 $|S_0| \equiv |S| = [G : P] \,(\text{mód } p)$, pero por el Teoerma de Lagrange, $[G : P] = \frac{|G|}{|P|}$ y por Corolario 2.4, p no divide a $[G : P]$ de ahí que $|S_0| \neq 0$ y, por tanto, existe $x \in P$ tal que $xP \in S_0$, sin embargo,

$$\begin{aligned} xP \in S_0 &\Leftrightarrow hxP = P, \text{ para todo } h \in H \\ &\Leftrightarrow x^{-1}HxP = P \text{ para todo } h \in H \\ &\Leftrightarrow x^{-1}Hx < P \\ &\Leftrightarrow H < xPx^{-1}. \end{aligned}$$

Si H es un p-subgrupo de Sylow de G, $|H| = |P| = |xPx^{-1}|$ y así, $H = x^{-1}Px$.

■

Teorema 2.8 (Tercer Teorema de Sylow)**.** *Si G es un grupo finito y p un número primo, entonces el número de p-subgrupos de Sylow de G divide al orden de G y viene dado por $kp + 1$, donde k es un entero no negativo.*

Demostración. Por el segundo Teorema de sylow, el número de p-subgrupos de Sylow de G es igual al número de conjugados de uno de ellos, digamos P. Por el Corolario 2.1 éste coincide con $[G : N_H(P)]$, el cual por el Teorema de Lagrange, divide a $|G|$. Sea S el conjunto de todo los p-subgrupos de Sylow de G y consideremos a P actuando por conjugación sobre S. Observemos que un subgrupo Q de G pertenece a S_0 si y solo si $xQx^{-1} = Q$ para todo $x \in P$, es decir, si $P < N_G(Q)$. Como P y Q son p-subgrupos de Sylow de G, también son p-subgrupos de Sylow de $N_G(Q) < G$ y por el segundo Teorema de Sylow son conjugados en $N_G(Q)$, es decir, $xQx^{-1} = P$, para algún $x \in N_G(Q)$, pero como Q es normal en $N_G(Q)$, $Q = P$. Así $S_0 = \{P\}$ y el Lema 2.1 implica que $|S| = kp + 1$ ■

Corolario 2.5. *Sea G es un p-grupo finito, siendo p un número primo. Si G contiene más de un p-subgrupo de Sylow, entonces el número de p-subgrupos de Sylow de G es mayor que p.*

Demostración. Por el tercer Teorema de Sylow, el número de subgrupos de Sylow de G es $kp + 1$, donde k es un entero no negativo, pero

$$kp + 1 > 2 \Leftrightarrow kp > 1,$$

en consecuencia, $k > 0$, en otras palabras, $k \geq 1$. Así el número de p-subgrupos de Sylow G es

$$kp + 1 \geq p + 1 > p$$

■

CAPÍTULO 3

CARACTERIZACIÓN DE LOS GRUPOS CON A LO MÁS CINCO SUBGRUPOS CÍCLICOS

En este capítulo ofrecemos los resultados principales de este trabajo, recordemos que nuestro objetivo es caracterizar los grupos finitos que poseen a lo más cinco subgrupos cíclicos. Comenzamos mostrando algunos cálculos relacionados con el número de subgrupos cíclicos de algunos grupos finitos.

3.1. Cálculo y observaciones sobre $C(G)$

Dado un grupo G denotaremos por $C(G)$ al conjunto de todo los subgrupos cíclicos de G, tal conjunto es parcialmente ordenado por la inclusión.

Para todo grupo finito G denotaremos por $\pi_e(G)$ al conjunto de todo los órdenes de elementos de G, esto es

$$\pi_e(G) := \{|g| : g \in G\}.$$

Para todo $i \in \pi_e(G)$, denotaremos por $C_i(G)$ al conjunto de todo los subgrupos

cíclicos de orden i en G, es decir,

$$C_i(G) := \{C_i < G : C_i \text{ es cíclico de orden } i\},$$

además,

$$c_i := |C_i(G)|.$$

Para todo grupo finito G denotaremos por $\pi(G)$ al conjunto de los números primos que dividen a $|G|$, es decir,

$$\pi(G) := \{p \in \mathbb{N} : p \text{ divide a } |G|,\ p \text{ es primo}\}.$$

Los siguientes resultados establecen algunas relaciones entre los términos que acabamos de definir.

Teorema 3.1. *Si G es un grupo finito entonces,*

$$|C(G)| = \sum_{k \in \pi_e(G)} c_k \tag{3.1}$$

y

$$|G| = \sum_{k \in \pi_e(G)} c_k \phi(k), \tag{3.2}$$

donde ϕ es la función de Euler.

Demostración. La ecuación 3.1 es fácil de deducir usando la propiedad asociativa y conmutativa de la adición en $\mathbb{N}$ y por la definición de $C(G)$ y de $\pi_e(G)$. Mostraremos que la ecuación 3.2 es válida. Sean $a, b \in G$, diremos que a esta relacionado con b, y escribiremos $a \sim b$, si $\langle a \rangle = \langle b \rangle$.

Nótese que dados $a, b, c \in G$, $a \sim a$. Si $a \sim b$, $b \sim a$. Si $a \sim b$ y $b \sim c$, $a \sim c$. Así, la relación definida es de equivalencia y genera una partición de G a través de las clases de equivalencia, más aún, cada clase de equivalencia $[a]$ tiene cardinalidad $\phi(|a|)$ (por Teorema 1.4).

Observemos que existen $|C(G)|$ clases de equivalencia, en efecto, sea $f : C(G) \to G/\sim$, dada por $f(\langle a \rangle) = [a]$, donde $[a]$ es la clase de equivalencia a la cual pertenece a. Notemos que si tomamos otro generador de $\langle a \rangle$, él también pertenece a $[a]$, así la función esta bien definida. Veamos que f es biyectiva.

Para $[a] \in G/\sim$, tenemos que $f(\langle a\rangle) = [a]$, así f es sobreyectiva. Por otro lado, sean $\langle a\rangle$ y $\langle b\rangle$ subgrupos cíclicos de G con $\langle a\rangle \neq \langle b\rangle$, entonces $a \nsim b$ así $f(\langle a\rangle) = [a] \neq [b] = f(\langle b\rangle)$, por lo que f es inyectiva.

Como f es biyectiva, tenemos que hay tantas clases de equivalencia como subgrupos cíclicos tiene G, esto es, $|C(G)|$. Supongamos que $[a_1], [a_2], \ldots, [a_{C(G)}]$ son las distintas clases de equivalencia de G entonces, $G = \bigcup_{i=1}^{C(G)} [a_i]$, así

$$|G| = \sum_{i=1}^{C(G)} |[a_i]| = \sum_{i=1}^{C(G)} \phi(|a_i|) = \sum_{k\in\pi_e(G)} c_k\phi(k).$$

■

Lema 3.1. *Sea G un grupo con $|G| = p^r q^s$, donde p y q son primos distintos y $r, s \in \mathbb{N}$. Si G posee más de un subgrupo cíclico de orden p^r, entonces*

$$c_{p^r} = [G : N_G(C_{p^r})] > p.$$

En efecto, sea C_{p^r} un subgrupo cíclico de G de orden p^r. El Corolario 2.4 implica que C_{p^r} es un p-subgrupo de Sylow, más aún, cualquier otro subgrupo de G de orden p^r es un p-subgrupo de Sylow de G.

Por el segundo Teorema de Sylow, cualquier p-subgrupo de Sylow de G es conjugado a C_{p^r}, es decir, es de la forma $aC_{p^r}a^{-1}$ para algún $a \in G$, como C_{p^r} es cíclico, $aC_{p^r}a^{-1}$ también lo es (ver Ejemplo 1.2), así podemos concluir que todo p-subgrupo de Sylow de G es cíclico de orden p^r.

Luego G tiene tantos p-subgrupos de Sylow como grupos cíclicos de orden p^r (este número es c_{p^r}) y tantos p-subgrupos de Sylow como conjugados tiene C_{p^r}, entonces por el Corolario 2.1 y el Corolario 2.5,

$$c_{p^r} = [G : N_G(H)] > p.$$

Ahora calcularemos el valor de $C(G)$ para algunos abelianos grupos finitos.

Proposición 3.1. *Si C_n es un grupo cíclico de orden n entonces, $|C(C_n)|$ es el número de divisores de n.*

Demostración. Sea a un generador de C_n y $n_1 = 1, n_2, \ldots, n_k$ los distintos divisores de n, por el Teorema 1.3 $|a^{n_i}| = n/n_i$, luego cada divisor de n determina un subgrupo

cíclico $\langle a^{n_i}\rangle$, de modo que existen al menos k subgrupos cíclicos de G. Probaremos que todo elemento de C_n genera alguno tales subgrupos cíclicos y así podemos concluir que C_n tiene exactamente k subgrupos cíclicos.

Sea $a^r \in C_n$ con $1 \leq r \leq n$. Si $r = n_i$ para algún $i = 1, 2, \ldots k$, no hay nada que probar. Si r y n son coprimos, el Teorema 1.4 implica que $\langle a^r\rangle = \langle a\rangle = \langle a^{n_1}\rangle$. Supongamos que r no divide a n y no es coprimo con n, y sea $d > 1$ el máximo común divisor de r y n, sin perder generalidad, podemos suponer $d = n_k$, así podemos escribir $r = n_k s$ y $n = n_k t$ con $s < t$ siendo primos relativos. Sea $b = a^{n_k}$ entonces $|b| = |a^{n_k}| = n/n_k = t$, notemos que $a^r = a^{n_k s} = (a^{n_k})^s = b^s \in \langle b\rangle$ como t y s son coprimos, el Teorema 1.4 implica que b^s es un generador de $\langle b\rangle$, así $\langle a^r\rangle = \langle b^s\rangle = \langle b\rangle = \langle a^{n_k}\rangle$. ■

Proposición 3.2. *Si C_p es un grupo cíclico de orden p primo entonces,*

$$|C(C_p \times C_p)| = p + 2.$$

Demostración. Sea $g = (a, b) \in C_p \times C_p$. Supongamos que $g \neq e$, entonces $a \neq e$ o $b \neq e$, por el Teorema de Lagrange todo elemento, a excepción del neutro, en C_p tiene orden p así g tiene orden p, luego todo elemento de $C_p \times C_p$ distinto de e tiene orden p.

Ahora por la ecuación (3.2), se tiene que:

$$\begin{aligned} p^2 = |C(C_p \times C_p)| &= \sum_{k\in\{1,p\}} c_k\phi(k) \\ &= c_1 + c_p(p-1) \text{ (ver Ejemplo 1.1 parte 2)} \\ &= c_p(p-1) + 1, \end{aligned}$$

implicando que

$$\frac{p^2-1}{p-1} = c_p,$$

luego $c_p = p + 1$, es decir, $C_p \times C_p$ tiene $p + 1$ subgrupos cíclicos de orden p, pero todo subgrupo cíclico de $C_p \times C_p$ tiene orden 1 o p, entonces $C(C_p \times C_p) = p + 2$. ■

Observación 3.1. Sea G un p-grupo, con $|G| = p^n$ para algún $n \geq 2$. Si para $k < n$ tenemos $c_1 + c_p + c_{p^2} + \ldots + c_{p^k} < |C(G)|$, entonces G debe contener al menos un subgrupo cíclico de orden $m > p^k$, por el Teorema de Lagrange, $m = p^r$ con $r \geq k + 1$ y, por el Teorema 1.3, éste contiene un subgrupo cíclico de orden p^{k+1}.

Finalizamos esta sección con un resultado que, bajo ciertas condiciones, caracteriza los p-grupos que poseen exactamente 5 subgrupos cíclicos.

Lema 3.2. *Sea G un p-grupo con p primo y $p \geq 3$ tal que $C(G) = 5$. Si G tiene un único subgrupo cíclico de orden p, entonces $G \cong C_{p^4}$.*

Demostración. Como $|C(G)| = 5$, el Ejemplo 1.3 y la Proposición 3.1 implican que $|G| = p^n$ con $n > 1$, además, como $c_1 + c_p = 1 + 1 = 2 < |C(G)|$, por la Observación 3.1, G contiene un subgrupo cíclico de orden p^2, de hecho $c_{p^2} \leq 3$.

Si $c_{p^2} = 3$, entonces $c_{p^r} = 0$ para $3 \leq r \leq n$, así la ecuación (3.2) queda como sigue,

$$p^n = |G| = 1\phi(1) + 1\phi(p) + 3\phi(p^2) = 1(1) + 1(p-1) + 3(p-1)p = 3p^2 - 2p = p(3p-2),$$

implicando que $p^{n-1} = 3p - 2$ o, equivalentemente, $2 = 3p - p^{n-1} = p(3 - p^{n-2})$, como $n \geq 2$, p divide a 2, pero p es primo, entonces $p = 2$ lo cual contradice la hipótesis.

Si $c_{p^2} = 2$, entonces $c_1 + c_p + c_{p^2} = 1 + 1 + 2 < |C(G)|$, así G debe contener un subgrupo cíclico de orden p^3 (por la Observación 3.1) y $c_{p^r} = 0$ para $4 \leq r \leq n$, entonces la ecuación (3.2) queda como sigue,

$$\begin{aligned} p^n = |G| &= 1\phi(1) + 1\phi(p) + 2\phi(p^2) + 1\phi(p^3) \\ &= 1(1) + 1(p-1) + 2(p-1)p + 1(p-1)p^2 \\ &= p^3 + p^2 - p, \end{aligned}$$

implicando que $p^{n-1} = p^2 + p - 1$ o, equivalentemente, $1 = p^2 + p - p^{n-1} = p(p + 1 - p^{n-2})$, como $n \geq 2$, p divide a 1, lo cual es una contradicción.

Supongamos que $c_{p^2} = 1$, entonces $c_1 + c_p + c_{p^2} = 3 < |C(G)|$, por la Observación 3.1, debe existir al menos un subgrupo cíclico de G de orden p^3, más aún, $1 \leq c_{p^3} \leq 2$.

Si $c_{p^3} = 2$, entonces $c_{p^r} = 0$ para $4 \leq r \leq n$ y la ecuación (3.2) queda,

$$p^n = |G| = 1\phi(1) + 1\phi(p) + 1\phi(p^2) + 2\phi(p^3) = 1 + (p-1) + (p-1)p + 2(p-1)p^2 = 2p^3 - p^2,$$

implicando que $p^{n-2} = 2p - 1$ o, equivalentemente, $1 = 2p - p^{n-2} = p(2 - p^{n-3})$, notemos que como G tiene un subgrupo de orden p^3, entonces $n \geq 3$, luego p divide a 1, lo cual es una contradicción.

Por tanto, $c_{p^3} = 1$ y tenemos $c_1 + c_p + c_{p^2} + c_{p^3} = 1 + 1 + 1 + 1 < |C(G)|$, usando la Observación 3.1, G posee un subgrupo cíclico de orden p^4, más aún, G no debe poseer subgrupos cíclicos de orden p^r con $4 \leq r \leq n$. La ecuación (3.2) queda como sigue,

$$\begin{aligned} |G| = p^n &= 1\phi(1) + 1\phi(p) + 1\phi(p^2) + 1\phi(p^3) + 1\phi(p^4) \\ &= 1 + (p-1) + (p-1)p + (p-1)p^2 + (p-1)p^3 \\ &= p^4. \end{aligned}$$

Como G contiene un subgrupo cíclico, digamos H, de orden p^4, tenemos que $G = H \cong C_{p^4}$. ■

3.2. Resultados Principales

En esta sección ofrecemos nuestros resultados principales, específicamente, caracterizamos los subgrupos finitos que poseen a lo más cinco subgrupos cíclicos.

Teorema 3.2. *$|C(G)| = 1$ si y solo si $G = \langle e \rangle$.*

Demostración. Es claro que si $G = \{e\}$, $|C(G)| = 1$. Ahora, supongamos que $|C(G)| = 1$ y supongamos que $G \neq \{e\}$. Sea $a \in G$, con $a \neq e$, luego $\langle a \rangle \neq \langle e \rangle$, por tanto $|C(G)| \geq 2$ contradiciendo la hipótesis, de ahí que $G = \{e\}$.

■

Teorema 3.3. *$|C(G)| = 2$ si y solo si $G \cong C_p$ para algún p primo.*

Demostración. Por la Proposición 3.1 si $G \cong C_p$, $|C(G)| = 2$.

Recíprocamente, si $|C(G)| = 2$, G debe ser un grupo cíclico, de lo contrario, existirían dos elementos $a, b \in G \setminus \{e\}$ tales que $\langle a \rangle \neq \langle b \rangle$ y si se cuenta al subgrupo trivial, habrían mas de dos subgrupos cíclicos en él. Sea $G = \langle a \rangle$ con $a \in G$.

Ahora veamos que $|G|$ es primo, supongamos que r divide a $|G|$, esto es, $|G| = rs$ con $s \in \mathbb{Z}$ y $1 < r, s < |G|$. Como G es cíclico, el Teorema 1.3 implica que $|a^s| = r$, esto implica que existen al menos tres subgrupos cíclicos distintos en G, a saber, $\langle e \rangle$, $\langle a^s \rangle$ y $\langle a \rangle$ los cuáles tienen órdenes 1, s y $|G| > s$, respectivamente, contradiciendo la hipótesis. Así $r = 1$ o $r = |G|$, de modo que $|G|$ es primo. Por tanto, $G \cong C_p$ para algún p primo.

■

Teorema 3.4. $|C(G)| = 3$ *si y solo si* $G \cong C_{p^2}$*, para algún primo* p*.*

Demostración. Supongamos que $|C(G)| = 3$. Si $|\pi(G)| \geqslant 3$, existen al menos tres primos distintos que dividen a $|G|$, digamos p, q y r, por el Teorema de Cauchy, G posee 3 subgrupos distintos de orden p, q y r, respectivamente, los cuales son cíclicos, así $|C(G)| \geq 4$, contradiciendo la hipótesis.

Si $|\pi(G)| = 2$, entonces $|G| = p^a q^b$, con $a, b \geqslant 1$. Por el Teorema de Cauchy existen al menos dos subgrupos cíclicos de G, digamos A y B, isomorfos a C_p y a C_q, respectivamente. Como $|C(G)| = 3$, $c_p = c_q = 1$, es decir, A es el único subgrupo de G de orden p y B es el único subgrupo de G de orden q (recordar que cualquier subgrupo de G de orden p (o q) es cíclico) luego, el Ejemplo 1.5 implica que A y B son normales en G. Ahora por la Proposición 2.1, $AB \cong C_p \times C_q$, y por la Observación 2.1 $AB \cong C_{pq}$, pero por Proposición 3.1, $|C(C_{pq})| = 4$, contradiciendo la hipótesis. Por tanto, $\pi(G) \neq 2$.

Podemos concluir entonces que $|\pi(G)| = 1$, es decir, G es un p-grupo con $|G| = p^n$, con $n > 1$ (ya que si $n = 1$, por el Ejemplo 1.3, G seria cíclico de orden p y por el Teorema 3.3 tendríamos $|C(G)| = 2$). Por otro lado, como $|C(G)| = 3$, entonces $c_p \leq 2$.

Si $c_p = 2$, la ecuación (3.2) sería

$$|G| = p^n = 1\phi(1) + 2\phi(p) = 2p - 1,$$

siendo esto imposible, ya que implicaría $0 = p^n - 2p + 1 \geq 2p - 2p + 1 = 1$.

Si $c_p = 1$, $c_1 + c_p < |C(G)|$ y la Observación 3.1 implica que G contiene un subgrupo cíclico de orden p^2, más aún, $c_{p^2} = 1$ y $c_{p^r} = 0$ para $3 \leq r \leq n$. Así la ecuación (3.2) queda como sigue,

$$|G| = p^n = 1\phi(1) + 1\phi(p) + 1\phi(p^2) = 1(1) + 1(p-1) + (p-1)p = p^2$$

Como G contiene un subgrupo de orden p^2, tenemos que $G \cong C_{p^2}$.

Recíprocamente, si $G \cong C_{p^2}$, la Proposición 3.1 implica $|C(G)| = 3$. ■

Teorema 3.5. $|C(G)| = 4$ *si solo si* G *es isomorfo a alguno de los siguientes grupos:* $C_2 \times C_2$*,* C_{p^3}*,* C_{pq}*, donde* p *y* q *son números primos distintos.*

Demostración. Supongamos que $|C(G)| = 4$. Si $|\pi(G)| \geq 4$, el Teorema de Cauchy implica que G posee al menos cuatro subgrupos cíclicos distintos, no triviales, de modo que $|C(G)| > 4$. Así $|\pi(G)| \leq 3$.

Si $\pi(G) = \{p, q, r\}$ con p, q y r primos distintos, entonces por el Teorema de Cauchy y dado que $|C(G)| = 4$, debemos tener $c_p = c_q = c_r = 1$, sean $A \cong C_p$, $B \cong C_q$ y $C \cong C_r$ los únicos subgrupos cíclicos (y por Ejemplo 1.5 los únicos subgrupos) de G de orden p, q y r, respectivamente. Por Ejemplo 1.5 A, B y C son subgrupos normales de G, además, por Teorema 2.2 y Observación 2.1, $ABC \cong C_{pqr}$ pero, por la Proposición 3.1, $|C(C_{pqr})| = 8 > 4$, contradiciendo la hipótesis.

Supongamos $\pi(G) = \{p, q\}$, esto es, $|G| = p^a q^b$ con $a, b \geq 1$ y $p \neq q$, por la ecuación (3.1), $c_p = 2$ y $c_q = 1$, o $c_p = c_q = 1$.

Si $c_p = 2$ y $c_q = 1$, la ecuación (3.2) queda como sigue

$$|G| = p^a q^b = 1\phi(1) + 2\phi(p) + \phi(q) = 1 + 2(p-1) + (q-1) = 2p + q - 2,$$

luego

$$0 = p^a q^b - 2p - q + 2 \geq pq - 2p - q + 2 = (p-1)(q-2). \tag{3.3}$$

Notemos que al ser p y q primos, la desigualdad (3.3) implica $q = 2$, sustituyendo el valor de q en (3.3) obtenemos $0 = p^a 2^b - 2p$, pero

$$\begin{aligned} 0 = p^a 2^b - 2p &\Rightarrow p^a 2^b = 2p \\ &\Rightarrow p^{a-1} 2^{b-1} = 1 \\ &\Rightarrow a = b = 1 \end{aligned}$$

Así $c_2 = 1$ y $c_p = 2$ y $|G| = 2p$, por el Teorema de Cauchy sabemos que existen A y B subgrupos de G isomorfos a C_2 y C_p, respectivamente. Por el Teorema de Lagrange, $[G : B] = 2$ y por el Ejemplo 1.4, B es normal en G, además como A es el único subgrupo de G de orden 2, por el Ejemplo 1.5, A también es normal en G. Luego, $AB \cong C_{2p}$ (Veáse Teorema 2.2 y Observación 2.1), como $AB \subseteq G$ y $|G| = 2p$, $G \cong C_{2p}$, pero esto contradice nuestra suposición ya que C_{2p} es cíclico por que tiene un único subgrupo de orden p.

Ahora supongamos $c_p = 1$ y $c_q = 1$, por el Teorema de Cauchy existen A y B subgrupos de G tal que $C_p \cong A$ y $C_q \cong B$, y por Ejemplo 1.5 A y B son subgrupos

normales de G. Entonces, por Teorema 2.2 y Observación 2.1, $AB \cong C_{pq}$ y por Proposición 3.1, $|C(AB)| = |C_{pq}| = 4$. Si $G \neq AB$, existe un elemento en G que no esta en AB y éste generaría un subgrupo cíclico distinto a los subgrupos cíclicos de AB, de modo que $|C(G)| > |C(AB)| = 4$, lo cual contradice la hipótesis, por tanto podemos concluir $G = AB \cong C_{pq}$.

Finalmente, nos queda estudiar el caso $\pi(G) = \{p\}$, con p primo, entonces $|G| = p^n$, claramente $c_p \leq 3$ ya que $c_1 = 1$ y $|C(G)| = 4$. Observemos que $|C(G)| = 4$ y la Proposición 3.1 implican $n > 1$.

Si $c_p = 3$ la ecuación (3.2) queda como sigue,

$$p^n = |G| = 1\phi(1) + 3\phi(p) = 1 + 3(p-1) \tag{3.4}$$

o, equivalentemente,

$$0 = p^n - 3p + 2 \geq p^2 - 3p + 2 = (p-2)(p-1).$$

Como p es primo debemos tener $p = 2$, al sustituir en (3.4) obtenemos $2^n = 1+3(2-1) = 4$, implicando $n = 2$, luego $|G| = 2^2 = 4$. Recordemos que, salvo isomorfismo, solo existen dos tipos de grupos de orden 4, C_4 y $C_2 \times C_2$, pero por la Proposición 3.1, $|C(C_4)| = 3$, de modo que $G \cong C_2 \times C_2$.

Si $c_p = 2$, como $c_1 + c_p = 3 < |C(G)|$, la Observación 3.1 implica que G posee al menos un subgrupo de orden p^3, más aún, $c_{p^3} = 1$. Entonces, la ecuación (3.2) queda de la siguiente manera,

$$p^n = |G| = 1\phi(1) + 2\phi(p) + \phi(p^2) = 1 + 2(p-1) + (p-1)p = p^2 + p - 1,$$

luego

$$0 = p^n - p^2 - p + 1 \geq p^3 - p^2 - p + 1 = (p-1)(p^2-1) > 0 \text{ ya que } p \text{ es primo,}$$

como lo anterior no tiene sentido, este caso se descarta.

Supongamos $c_p = 1$. Si $c_{p^2} = 2$, $n \geq 3$ ya que contiene dos subgrupos distintos de orden p^2, además, existen subgrupos distintos de G, digamos A,B y C, tales que A y B son isomorfos a C_{p^2} y $C \cong C_p$. Nótese que $C \subseteq A \cap B$ ya por el Teorema de Cauchy, A tiene un subgrupo de orden p y B tiene un subgrupo de orden p, pero G tiene un único

subgrupo de orden p. Más aún, $A \cap B = C$ ya que la intersección de dos subgrupos de G es un subgrupo de G y, por el Teorema de Lagrange, su orden debe ser divisor de p^n, pero además debe ser menor o igual que p^2, ya que ese es el orden de A y de B. Si el orden de $A \cap B$ es igual a p^2, entonces $A = B$, pero a ellos los hemos supuesto distintos. Así que $|A \cap B| = p$, por lo tanto $A \cap B = C$, ya que $C_p \cong C \subseteq A \cap B$.

Afirmamos también que $G = A \cup B$, de lo contrario, tomando $a \in G \setminus A \cup B$, $\langle a \rangle$ sería un subgrupo cíclico de G distinto a los subgrupos cíclicos incluidos en $A \cup B$, pero $A \cup B$ posee $C(G) = 4$ subgrupos cíclicos. Ahora, la ecuación (3.2) es equivalente a

$$p^n = |G| = |A| + |B| - |A \cap B| = p^2 + p^2 - p = 2p^2 - p$$

o, equivalentemente, $0 = p(p^{n-1} - 2p + 1)$ implicando $p^{n-1} = 2p - 1$. Como $n \geq 3$ y $p \geq 2$, se cumple lo siguiente

$$0 = p^{n-1} - 2p + 1 \geq 2p - 2p + 1 = 1$$

Siendo esto una contradicción.

Podemos concluir que $c_p = 1$ y $c_{p^2} = 1$, como $c_1 + c_p + c_{p^2} = 3 < |C(G)| = 4$, la Proposición 3.1 implica $c_{p^3} = 1$ y la ecuación (3.2) es la siguiente,

$$|G| = 1\phi(1) + 1\phi(p) + 1\phi(p^2) + 1\phi(p^3) = 1 + 1(p-1) + 1(p-1)p + 1(p-1)p^2 = p^3.$$

Como G contiene un subgrupo cíclico de orden p^3, tenemos $G \cong C_{p^3}$.

El recíproco lo conseguimos usando las Proposición 3.1 y la Proposición 3.2. ■

Teorema 3.6. $|C(G)| = 5$ *si y solo si* G *es isomorfo a uno de los siguiente subgrupos:* S_3, $C_{p^4}, C_3 \times C_3$, Q_8.

Demostración. Supongamos que $|C(G)| = 5$. Sea $\pi(G) = \{p_1, \ldots, p_t\}$ debemos tener $t \leq 4$, de lo contrario, el Teorema de Cauchy implicaría la existencia de más 5 subgrupos cíclicos.

Si $t = 4$ entonces, nuevamente por el Teorema de Cauchy y por Ejemplo 1.3, existen A, B, C y D subgrupos cíclicos de G de orden p_1, p_2, p_3 y p_4, respectivamente. Dado que $|C(G)| = 5$, $c_{p_i} = 1$ para $i = 1, 2, 3, 4$ y por el Ejemplo 1.5, A, B, C y D son subgrupos normales de G. Luego, por Teorema 2.2 y Observación 2.1, $ABCD \cong C_{p_1p_2p_3p_4}$, pero por la Proposición 3.1, $C_{p_1p_2p_3p_4}$ tiene 6 subgrupos cíclicos, contradiciendo nuestra hipótesis.

Si $t = 3$, el Teorema de Cauchy garantiza $c_{p_i} \geq 1$ para $i = 1, 2, 3$ y por la ecuación (3.2) podemos suponer que c_{p_1} es igual a 1 o 2 y $c_{p_2} = c_{p_3} = 1$. Por el Ejemplo 1.3, todo grupo de orden primo debe ser cíclico, así solo existe un subgrupo de orden p_2 y un subgrupo de orden p_3, digamos $B \cong C_{p_2}$ y $C \cong C_{p_3}$, de orden p_2 y p_3, respectivamente. Luego por el 1.5, B y C son normales en G, además, por el Teorema 1.11, AB es un subgrupo de G y, por Teorema 2.2 y Observación 2.1, $AB \cong C_{p_2p_3}$. Luego la Proposición 3.1 implica $C(AB) = 4$, de modo que $c_{p_1} = 1$, esto implica nuevamente que solo existe un subgrupo de orden p_1, digamos $A \simeq C_{p_1}$, usando el argumento anterior podemos concluir que $A(BC)$ es un subgrupo de G tal que $A(BC) \cong C_{p_1}C_{p_2p_3} \cong C_{p_1p_2p_3}$, luego la Proposición 3.1 implica $|C(G)| \geq |C(ABC)| = 8 > 5$, contradiciendo la hipótesis.

Si $t = 2$, $|G| = p^a q^b$ con p y q primos y $a, b \geq 1$. Sea $P \in Syl_p(G)$ y $Q \in Syl_q(G)$, por Corolario 2.4, $|P| = p^a$ y $|Q| = p^b$. Supóngase que $a > 1$ y $b > 1$, por el Teorema de Cauchy, tanto P como Q contienen subgrupos propios de orden p y q, respectivamente, los cuales son cíclicos y distintos, así $|C(P)| \geq 3$ y $C(Q) \geq 3$. Nótese que por el Teorema de Lagrange, los subgrupos no triviales de P son disjuntos a los subgrupos no triviales de Q (ya que los no triviales de P deben tener orden potencia de p con exponente entero positivo y los no triviales de Q deben tener como orden potencia de q con exponente entero positivo), luego $P \bigcup Q$ contiene los 5 subgrupos cíclicos de G y, por tanto $G = P \cup Q$, lo cual es imposible ya que $|G| = p^a q^b > p^a + q^b = |P| + |Q| = |P \cup Q|$. De ésta manera, $a = 1$ o $b = 1$ así $|G| = pq^b$. Sin pérdida de generalidad supongamos que $P \cong C_p$.

Supongamos que $b = 1$. En primer lugar, por el Corolario 2.4 $|Q| = q$. Nótese que P y Q no pueden ser normales en G simultáneamente ya que por el Teorema 2.2 y Observación 2.1, se tendría $AB \cong C_{pq}$, implicando $G \cong C_{pq}$, pero $|C(C_{pq}| = 4$ (por Teorema 3.1). Sin pérdida de generalidad supongamos que Q no es normal en G, luego $|N_G(Q)| < pq = |G|$ y como $Q \subseteq N_G(Q)$ tenemos que $|N_G(Q)| = q$ implicando que $[G : N_G(Q)] = q$. Además, por Ejemplo 1.5 debe existir más de un subgrupo de G orden q, luego por el Lema 3.1 $c_q = [G : N_G(Q)] = p > q$. Como $|C(G)| = 5$ y existen al menos dos subgrupos cíclicos de orden q, entonces $2 \leq q < p < 5$, así $p = 3$ y $q = 2$, esto implica que $c_p = 1$, luego por el Ejemplo 1.5, P es normal en G, sea a y b, generadores de P y Q, respectivamente. Tenemos las siguientes observaciones:

1. $|b| = 2$ y $|a| = 3$

2. Como P es normal en G, $bP = Pb$, luego $ba = a^n b$ con $1 \leq n \leq 3$. $n \neq 3$, de lo contrario $a = b^{-1}$ pero P y Q solo tienen en común el elemento neutro. Si $n = 1$, a y b conmutan implicando $a \in N_G(Q)$ pero $|a| = p$ y $|N_G(Q)| = q$ Por tanto, $ba = a^2 b = a^{-1} b$

3. $a^{n_1} b^{n_2} = a^{n_3} b^{n_4} \Leftrightarrow a^{n_1} a^{-n_3} = b^{n_4} b^{-n_2}$.

   Pero como P y Q solo tienen el elemento neutro en común, $a^{n_1} = a^{n_3}$ y $b^{n_4} = b^{n_2}$ y de aquí que todos los elementos de la forma $a^n b^n$ son distintos, así $|\langle a \rangle \langle b \rangle| = 6$ y como $\langle a \rangle \langle b \rangle \subseteq \langle a, b \rangle$ y $|G| = 6$, $G = \langle a, b \rangle$.

Luego, por Teorema 1.6, $G \cong S_3$.

Ahora supongamos $b > 1$. Si $c_p > 1$, por el Lema 3.1 $c_p = [G : N_G(P)] \geq p + 1$, pero p es primo, así $c_p \geq 3$, por otro lado, por el Teorema de Cauchy, Q contiene al menos un subgrupo de orden q, digamos B, el cual es cíclico, entonces como $|C(G)| = 5$ debemos tener $p = 2$ y $c_p = 3$. Ahora, $|Q| = q^b$, como $b > 1$, podemos tomar $a \in Q \setminus B$, $|a|$ es una potencia de q, pero esto implica que existen mas de 5 subgrupos cíclicos de G. Así $c_p = 1$ y P debe ser normal en G (por Ejemplo 1.5). Esto implica que $|C(Q)| \leq 3$, luego por los Teoremas 3.2, 3.3 y 3.4, $Q \cong \{e\}$ o $G \cong C_q$ o $G \cong C_{q^2}$, pero $|Q| = q^b$ con $b > 1$, $Q \cong C_{q^2}$. Si Q es el único grupo de orden p^2, el es normal en G y Teorema 2.2 y Observación 2.1, $PQ \cong C_p \times C_{q^2} \cong C_{pq^2}$ y por la Proposición 3.1, $|C(C_{pq^2})| = 6$, contradiciendo nuestra hipótesis. Así Q no es normal en G, de modo que debe existir al menos un par de subgrupos de orden q, los cuale son cíclicos, luego por Lema 3.1, $c_{q^2} = [G : N_G(H)] > q \geq 3$, además, por el Teorema de Cauchy, $c_q \geq 1$ y como $c_p = 1$, $|C(G)| \geq 6$, contradiciendo la hipótesis.

Consideremos el caso $t = 1$, entonces $|G| = p^a$, la Proposición 3.1 implica que $a \geq 2$.

Si $p \geq 5$, todo subgrupo cíclico de G es normal en G, en efecto, sea H subgrupo cíclico de G y supongamos que H no es normal en G, por el Teorema de Lagrange, $[G : N_G(H)] \geq p$ y, por el Corolario 2.1 el número de grupos conjugados a H coincide con $[G : N_G(H)] \geq p$, además todos los conjugados a H resultan isomorfos a H (ver Ejemplo 1.2). Luego, $|C(G)| \geq p + 1 > 5$ contradiciendo la hipótesis. Por tanto todo subgrupo cíclico de G debe ser normal en G. Supongamos que existen dos subgrupos distintos de orden p, digamos H y K, entonces $H \cap K = \langle e \rangle$ y, por Proposición2.1, $HK \cong C_p \times C_p$ pero, por Proposición 3.2, $|C(C_p \times C_p)| = p + 2 \geq 5$, así debe existir

un único subgrupo de G de orden p, entonces por el Lema 3.2, $G \cong C_{p^3}$.

Supongamos $p = 3$. Si $G \cong C_3 \times C_3$, no hay nada que probar. Supongamos $G \ncong C_3 \times C_3$. La Proposición 3.2 garantiza que $|C(C_3 \times C_3)| = 5 = |C(G)|$ por lo que no debe existir un subgrupo de G isomorfo a $C_3 \times C_3$. Como los grupos de orden 9 o son cíclicos o son congruentes a $C_3 \times C_3$, todo subgrupo de orden 9 de G debe ser cíclico, más aún, $|G| \geq 3^3$, pues si $|G| = 3$ o $|G| = 9$, G sería cíclico con $|C(G)| \leq 3$. Supongamos que existen dos subgrupos distintos de G de orden 3, por el primer Teorema de Sylow, cada uno de ellos son subgrupos normales en un subgrupo de G, digamos A y B de orden 9, pero A y B deben ser cíclicos y como ellos contienen grupos de orden 3 distintos, se concluye que $A \cap B = \{e\}$. Notemos que por la Proposición 3.1, un grupo cíclico de orden 9 tiene 3 subgrupos cíclicos y como A y B solo tiene en común el elemento neutro, $A \cup B$ contiene 5 subgrupos cíclicos, luego $G = A \cup B$ entonces

$$|A \cup B| = |G| = p^a \geq p^3 > 2p^2 > 2p^2 - 1 = |A \cup B|,$$

lo cual es una contradicción. De aquí que solo existe un subgrupo de G de orden p, luego por el Lema 3.2, $G \cong C_{p^3}$.

Finalmente, supongamos $p = 2$, esto es, $|G| = 2^n$. Dado que $|C(G)| = 5$ y usando la Observación 1.2, existe un elemento $x \in G$ tal que $|x| = \exp(G)$, luego $\exp(G) = 2^s \leq 2^4$, ya que $|C(\langle x \rangle)| = s + 1 \leq 5$.

Si $s = 1$, todo los elementos de G distintos del trivial tienen orden 2 y, en consecuencia, cada elemento de G genera un subgrupo cíclico de G distinto, luego $5 = |C(G)| = |G| = 2^a$, esto es imposible.

Si $s = 3$, entonces $|C(\langle x \rangle)| = 4$, así todos los elementos de $G \setminus \langle x \rangle$ estan contenidos en un mismo subgrupo cíclico el cual, digamos, tiene orden 2^r con $1 \leq r \leq \exp(G) = 2^3$, más aún, cada elemento de $G \setminus \langle x \rangle$ debe generar a $G \setminus \langle x \rangle \cup \{e\}$, luego $G \setminus \langle x \rangle = \phi(2^r)$ y esto implica que $|G - \langle x \rangle| = 2^n - 8 = 2^3(2^{n-3} - 1) > 2^3 \geq 2^r > 2^{r-1} = \phi(2^r)$ esto es una contradicción.

Si $s = 4$, $C(\langle x \rangle) = 5$ y por tanto $G \cong C_{p^4}$.

Solo falta considerar $s = 2$, en este caso $|\langle x \rangle| = 4$ y $C(\langle x \rangle) = 3$, luego $a > 2$ y los elementos de $G \setminus \langle x \rangle$ están incluidos en dos subgrupos cíclicos distintos, digamos de orden 2^r y 2^t con $1 \leq r, s \leq 2$, respectivamente, más aún, cada elemetos de $G \setminus \langle x \rangle$ deben ser generador de uno de tales subgrupos. Por el Teorema 1.4 la cantidad de

elementos que generan al grupo de orden 2^r es $\phi(2^r) = 2^{r-1}$ y la cantidad de elementos que generan al grupo de orden 2^t es $\phi(2^t) = 2^{t-1}$, así $2^n - 4|G \setminus \langle x\rangle| = 2^{r-1} + 2^{t-1}$. Si $r = t = 1$, $2^n - 4 = 2$ lo cual es imposible. Si $\{r, t\} = \{1, 2\}$, $2^n - 4 = 3$, lo cual es imposible. Así $r = t = 2$ y, en consecuencia, $n = 3$, $c_2 = 1$ y $c_4 = 3$.

Ahora sean $x_1, x_2, x_3 \in G$, tal que $|x_i| = 4$ y $\langle x_i\rangle \neq \langle x_j\rangle$ para $i, j = 1, 2, 3$ e $i \neq j$, como $c_2 = 1$, $x_1^2 = x_2^2 = x_3^2$.

Observemos que $x_1x_2 \notin \langle x_1\rangle$, de lo contrario, $x_2 \in \langle x_1\rangle$, pero $\langle x_1\rangle \neq \langle x_2\rangle$, análogamente $x_1x_2 \notin \langle x_1\rangle$. Como $c_2 = 1$, entonces x_1x_2 no pude tener orden 2, pues el único subgrupo de G de orden 2 está incluido en $\langle x_1\rangle$. Entonces podemos concluir que x_1x_2 tiene orden 4 y $\langle x_1x_2\rangle = \langle x_3\rangle$, así $e, x, x_1, x_2, x_3 \in \langle x_1, x_2\rangle$, luego $C(G) \geq C(\langle x_1, x_2\rangle) \geq 5 = C(G)$, en consecuencia,

$$G = \langle x_1, x_2\rangle.$$

Además, $(x_1x_2)^2$ tiene orden 2, luego $(x_1x_2)^2 = x_2^2$ pero

$$\begin{aligned}(x_1x_2)^2 = x_2^2 &\Leftrightarrow (x_1x_2)(x_1x_2) = x_2^2\\ &\Leftrightarrow x_1x_2x_1 = x_2\\ &\Leftrightarrow x_2x_1 = x_1^{-1}x_2.\end{aligned}$$

Hemos probado que $x_1^4 = x_2^4 = e$, $x_1^2 = x_2^2$, $x_2x_1 = x_1^{-1}x_2$ y $G = \langle x_1, x_2\rangle$, entonces por el Teorema 1.5 $G \cong Q_8$.

■

CONCLUSIONES

Clasificar el número de subgrupos cíclicos distintos de un grupo finito dado G es un problema interesante que es sorprendentemente subexplorado en la literatura. El Teorema de Cauchy proporciona una cota inferior para $|C(G)|$, mientras que en [2] y [3] se clasifican los grupos para los cuales $|C(G)|$ es grande respecto a $|G|$. En este trabajo estudiamos los Teoremas de Sylow, los cuales jugaron un rol preponderante para clasificar los grupos finitos G para los cuales $|C(G)| = 5$.

En general, el siguiente problema aún permanece abierto: Describir los grupos finitos G tales que $|C(G)| = |G| - r$, donde $2 \leq r \leq |G| - 3$.

Aunque los resultados presentados en este trabajo no son inéditos, se espera que las técnicas usadas para las demostraciones contribuyan a la formación de estudiantes que se inician en la investigación y motiven el estudio del problema que permanece abierto.

REFERENCIAS BIBLIOGRÁFICAS

[1] T. Hungerford (1974), Algebra. Springer-Verlag, New York.

[2] M. Tărnăuceanu, Finite groups with a certain number of cyclic subgroups, *Amer. Math. Monthly* **Vol. 122** (2015), 275-276.

[3] M. Tărnăuceanu Finite groups with a certain number of cyclic subgroups II, (2016) preprint.

[4] W. Zhou, On the number of cyclic subgroups in finite groups (2016) preprint.

[5] W. Zhou, Finite groups with small number of cyclic subgroups (2016) preprint.