ESTUDIO DE LOS CONJUNTOS PRODUCTO PEQUEÑOS EN GRUPOS FINITOS NO ABELIANOS

DORIS YOLIMA MADROÑERO TORO

UNIVERSIDAD DE NARIÑO
FACULTAD DE CIENCIAS EXACTAS Y NATURALES
DEPARTAMENTO DE MATEMÁTICAS Y ESTADÍSTICA
SAN JUAN DE PASTO
2019

ESTUDIO DE LOS CONJUNTOS PRODUCTO PEQUEÑOS EN GRUPOS FINITOS NO ABELIANOS

DORIS YOLIMA MADROÑERO TORO

Trabajo presentado como requisito parcial para optar al título de Licenciada en Matemáticas

Asesor
Wilson Fernando Mutis Cantero
Ph. D. en Matemáticas

UNIVERSIDAD DE NARIÑO
FACULTAD DE CIENCIAS EXACTAS Y NATURALES
DEPARTAMENTO DE MATEMÁTICAS Y ESTADÍSTICA
SAN JUAN DE PASTO
2019

Nota de Responsabilidad

Todas las ideas y conclusiones aportadas en el siguiente trabajo son responsabilidad exclusiva de los autores.

Artículo 1^{ro} del Acuerdo No. 324 de octubre 11 de 1996 emanado por el Honorable Consejo Directivo de la Universidad de Nariño.

Nota de Aceptación

Wilson Fernando Mutis Cantero

Asesor del trabajo de grado

Viviana Carolina Guerrero Pantoja

Jurado 1

Oscar Fernando Soto Ágreda

Jurado 2

San Juan de Pasto, 20 de noviembre de 2019

Este trabajo está dedicado a:
Manuel Madroñero †*, Teresa Toro y a mis hermanos,*
por su apoyo incondicional en este proceso.

Agradecimientos

Con este trabajo quiero dar mis mas sinceros agradecimientos a todas aquellas personas que de una u otra forma han contribuido para que la culminación del mismo sea posible. A Dios por darme todo. A mis familiares, especialmente a mis padres Manuel † y Teresa por darme la oportunidad de vivir, quienes con su amor, apoyo, confianza y consejos impulsaron constantemente mi deseo por estudiar. A mi asesor Dr. Wilson Fernando Mutis Cantero, quien con su dedicación y conocimiento guió este trabajo. A los docentes del Departamento de Matemáticas y Estadística de la Universidad de Nariño por sus valiosas enseñanzas. A la Vicerrectoría de Investigaciones, Posgrados y Relaciones Internacionales por la aprobación y financiación del proyecto de investigación "problema de los conjuntos producto pequeños en grupos no abelianos finitos", por facilitar económicamente la asistencia a eventos académicos. Al Grupo de Investigación ALTENUA por brindarme los espacios de divulgación de conocimiento. Finalmente quiero agradecer a mis amigos Dario, Jeniffer, Leidy y Ronald, por su maravillosa amistad.

Resumen

En el presente trabajo se realiza el estudio detallado de los resultados mas relevantes sobre el problema de los Conjuntos Producto Pequeños en grupos no abelianos finitos, en particular para los grupos no abelianos de orden pq, donde p y q son primos impares distintos. También se muestra las propiedades básicas de la función $\mu_G(r, s)$ y los resultados obtenidos para las clases de grupos diédricos, hamiltonianos, $p - grupos$ y solubles, que en la actualidad solo aparecen en la literatura especializada. Además, se presentan los algoritmos implementados por los autores en el software matemático libre SageMath, que permiten calcular el valor de la función $\mu_G(r, s)$ en el grupo no abeliano de orden 55.

Palabras claves: Producto pequeño, grupo no abeliano, algoritmo, función $\mu_G(r, s)$, orden pq.

Abstract

In this work the detailed study of the results most relevant on the problem of Small Product Sets in finite nonabelian groups, in particular for nonabelian groups of order pq, where p and q are different odd primes. It also shows the basic properties of the function in $\mu_G(r, s)$ and the obtained results for the classes of groups dihedral, hamiltonian, $p - groups$ and solvable, which currently only appear in specialized literature. In addition, it presents algorithms implemented by the authors in the free mathematical software SageMath, which can calculate the value of the function in $\mu_G(r, s)$ in the nonabelian goup or order 55.

Keywords: Small product, nonabelian group, algorithm, function $\mu_G(r, s)$, order pq.

Índice general

Índice de figuras

Índice de tablas

Introducción

Dados un grupo G y subconjuntos no vacíos A y B de G, un problema de interés es el estudio del cardinal del conjunto producto AB. En este contexto, el denominado **Problema de los Conjuntos Producto Pequeños** consiste en determinar una fórmula explícita para calcular el valor de la función

$$\mu_G(r,s) = \text{mín}\{|AB| : A, B \subseteq G, |A| = r, |B| = s\},$$

donde r y s son enteros positivos tales que $r, s \leq |G|$. Para este problema se han obtenido grandes avances pues poco tiempo atrás sólo se conocían resultados de la función $\mu_G(r,s)$ para algunas clases de grupos abelianos. Debido a los trabajos de Eliahou, Kervaire y Plagne (2003), (2005) y (2007) [1], [2] y [3] el problema está completamente resuelto para el caso que G es un grupo abeliano arbitrario, de hecho se tiene

$$\mu_G(r,s) = \min_{n \in H(G)} \left\{ \left(\left\lceil \frac{r}{n} \right\rceil + \left\lceil \frac{s}{n} \right\rceil - 1 \right) n \right\} = \kappa_G(r,s). \tag{1}$$

Sin embargo, se desconoce si existe una fórmula unificada para esta función en el caso que G es no abeliano. Se sabe que la fórmula de la función $\mu_G(r,s)$ obtenida para grupos abelianos no se puede extender para el caso en que G es no abeliano Eliahou y Kervaire (2007) [4]. No obstante, diferentes autores han logrado extender esta fórmula para algunas clases de grupos no abelinos finitos: Deckelbaum (2009) [5] probó este resultado en grupos no abelianos de orden $3p$, para primos impares $p > 3$ y $p \equiv 1(\text{mód } 3)$, por Eliahou y Kervaire (2010) [6] la fórmula (1) se satisface en grupos diédricos y Mutis, Benavides y Castillo (2010) y (2012) [7], [8] prueban que esta fórmula también se cumple para $p - grupos$ finitos y grupos hamiltonianos finitos de orden 2^{n+3}, donde n es un entero no negativo.

Este trabajo es una monografía que recopila los resultados mas relevantes sobre el problema de los conjuntos producto pequeños en grupos no abelianos finitos. En la actualidad los resultados conocidos sobre este problema aparecen en artículos de revistas especializadas y en general no se presentan todos los detalles de las pruebas. Sin embargo, como resultado del

estudio y análisis de los artículos donde aparecen los avances del problema de los conjuntos producto pequeños en grupos no abelianos, se escribió esta monografía en la cual se explican detalladamente los procedimientos con los cuales se prueban los teoremas mas importantes y en el caso del teorema (3.20) del artículo Deckelbaum (2009) [5], se reescribe la prueba para un mejor entendimiento de las personas interesadas en estudiar este problema.

El trabajo está dividido en cuatro capítulos. En el primero se establece la notación, se presentan las definiciones generales y se enuncian algunos resultados clásicos de la Teoría de Números y la Teoría de Grupos, los cuales se emplearán en el desarrollo del trabajo, además se hace la presentación del problema de los conjuntos producto pequeños. En el segundo capítulo se presentan los resultados de la función $\mu_G(r, s)$ para un grupo G no abeliano finito. En el tercer capítulo se dedica exclusivamente al estudio de este problema para grupos no abelianos de orden pq. Finalmente, en el cuarto capítulo se muestran los algoritmos que los autores implementaron en el software matemático SageMath, con los cuales se realizaron algunos cálculos de la función $\mu_G(r, s)$.

Capítulo 1

Preliminares

En este capítulo se establece la notación que será utilizada a lo largo del trabajo, se exponen los conceptos básicos de teoría de números y teoría de grupos, además se presenta el **problema de los conjuntos producto pequeños**, el resultado más importante de éste problema en los grupos abelianos obtenidos por Eliahou Kervaire y Plagne (2003),(2005) y (2007) [1], [2] y [3], la función $\mu_G(r,s)$ y algunas variaciones de esta.
Se utilizará letras mayúsculas para representar subconjuntos, conjuntos y grupos. Para un subconjunto X de un grupo G, se denota $X^{-1} = \{x^{-1} : x \in X\}$. Si G es un conjunto finito, el cardinal de G se denota por $|G|$. Si $n > 1$, el grupo cíclico $\mathbb{Z}/n\mathbb{Z}$, de congruencias módulo n, se identificará con el grupo cíclico $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. Para $a \in \mathbb{Z}$, el subconjunto de los enteros mayores e iguales que a se denota $\mathbb{Z}_{\geq a}$, es decir, $\mathbb{Z}_{\geq a} = \{n \in \mathbb{Z} : n \geq a\}$.

1.1. Aspectos generales de teoría de números

A continuación, se presentan las definiciones de Teoría de Números tomadas de Burton (2007) [9], que se utilizan en el desarrollo de este trabajo.

Teorema 1.1. ***(Algoritmo de la división)***
Dados $a, b \in \mathbb{Z}$ con $b \neq 0$, existen $q, r \in \mathbb{Z}$, únicos, tales que $a = qb + r$ y $0 \leq r < |b|$. Al entero q se le denomina cociente y al entero r se le denomina resto.

Definición 1.2. Divisor
Dados a y b enteros, con $a \neq 0$, se dice que a divide b, o que b es múltiplo de a o que a es un divisor de b, si existe $c \in \mathbb{Z}$ tal que $b = ac$. Esto se denota con $a \mid b$, en caso contrario se dice que b no es divisible por a y se escribe $a \nmid b$.

Definición 1.3. Máximo Común Divisor
Dados dos enteros a y b, con al menos uno de los dos diferente de cero, el mayor entero que divide simultáneamente a a y b se denomina el máximo común divisor de a y b, esto se denota

por $mcd(a, b)$, es decir, $mcd(a, b) = d$ si y solo si, se satisfacen las dos condiciones siguientes:

1. $d \mid a$ y $d \mid b$;
2. Si $c \mid a$ y $c \mid b$, entonces $c \leq d$. Se dice que los enteros a y b son primos relativos (o coprimos) si $mcd(a, b) = 1$.

Lema 1.4. ***(Lema de Euclides)***
Dados $a, b, c \in \mathbb{Z}$. Si $a \mid bc$ y $mcd(a, b) = 1$, entonces $a \mid c$.

Definición 1.5. Número primo
Un entero $p > 1$ se denomina primo, si sus únicos divisores positivos son 1 y p. Un entero mayor que 1 que no es un primo se denomina compuesto.

Definición 1.6. Congruencia módulo n
Dados un entero $n > 1$ y dos números $a, b \in \mathbb{Z}$, se dice que a es congruente con b módulo n, y se denota por $a \equiv b(\text{mód } n)$, si $n \mid (a - b)$.

Teorema 1.7. *Si $a, b, c, d, n \in \mathbb{Z}$, con $n > 1$, entonces*

1. *$a \equiv a(mód\ n)$.*
2. *$a \equiv b(mód\ n)$ si y solo si, $b \equiv a(mód\ n)$.*
3. *Si $a \equiv b(mód\ n)$ y $b \equiv c(mód\ n)$, entonces $a \equiv c(mód\ n)$.*
4. *Si $a \equiv b(mód\ n)$ y $c \equiv d(mód\ n)$, entonces $a \pm c \equiv b \pm d(mód\ n)$, y $ac \equiv bd(mód\ n)$.*
5. *Si $a \equiv b(mód\ n)$, entonces $a \pm c \equiv b \pm c(mód\ n)$ y $ac \equiv bc(mód\ n)$.*
6. *Si $a \equiv b(mód\ n)$, entonces $a^k \equiv b^k(mód\ n)$ para todo $k \in \mathbb{N}$.*
7. *Si $ac \equiv bc(mód\ n)$ y $mcd(n, c) = 1$, entonces $a \equiv b(mód\ n)$.*

1.2. Aspectos generales de teoría grupos

Las siguientes definiciones sobre teoría de grupos son tomadas de Gallian (2010) [10].

Definición 1.8. Grupo
Un grupo es un par $(G, *)$, donde G es un conjunto no vacío y $*$ es una operación binaria definida en G que satisface las siguientes condiciones:

1. Para todo $x, y, z \in G$ se tiene $(x * y) * z = x * (y * z)$.
2. Existe $1 \in G$ tal que $x * 1 = 1 * x = x$, para todo $x \in G$. El elemento 1 se denomina identidad del grupo.

3. Para cada $x \in G$ existe $y \in G$ tal que $x * y = 1 = y * x$. Se puede probar que y es único, este elemento se denomina inverso de x y se denota con $y = x^{-1}$.

Además, si para todo $x, y \in G$ se cumple $x * y = y * x$ se dice que $(G, *)$ es grupo abeliano en caso contrario se dice que es un grupo no abeliano. Si G es un conjunto finito, se dice que $(G, *)$ es un grupo de orden finito y el $|G|$ es el orden de G. En general, el grupo $(G, *)$ se denota con G y la operación binaria $*$ se omite. Si G es abeliano, la operación binaria se denota con $+$, y el elemento identidad con 0.

Ejemplo. Los conjuntos numéricos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, con la adición usual, son grupos abelianos. Además, para $n \in \mathbb{Z}_{\geq 3}$, el conjunto S_n de permutaciones del conjunto $\{1, 2, \ldots, n\}$, con la composición de funciones, es un grupo finito no abeliano de orden $n!$.

Definición 1.9. Progresión aritmética
Sea G un grupo abeliano. Una sucesión $\{a_n\}$ de elementos en G es una progresión aritmética si existe $d \in G$ tal que $a_{n+1} = a_n + d$. El número d se denomina diferencia de la progresión.

Definición 1.10. Subgrupo
Sean G un grupo y H un subconjunto no vacío de G. Se dice que H es un subgrupo de G si H es grupo con la misma operación binaria que da la estructura de grupo en G. Se denota $H \leq G$.

Ejemplo. Sea $\mathbb{R}^*$ el conjunto de los números reales no nulos, con la multiplicación en $\mathbb{R}$ es un grupo abeliano con identidad 1 y el inverso de cualquier elemento $a \in \mathbb{R}^*$ es $\frac{1}{a}$. Además $\mathbb{Q}^*$

$$\mathbb{Q}^* = \left\{ \frac{p}{q} : p \text{ y } q \text{ son enteros no nulos} \right\},$$

es un subgrupo de $\mathbb{R}^*$.

Observación 1.11. Todo grupo G tiene por lo menos dos subgrupos, $\{1\}$ y G, denominados subgrupos triviales.

Teorema 1.12. ***(Subgrupo generado)***
Sean G un grupo y $S \subseteq G$. Si $\mathcal{F} = \{H \leq G : S \subseteq G\}$, entonces el conjunto $\langle S \rangle = \bigcap_{H \in \mathcal{F}} H$ es un subgrupo de G denominado el subgrupo generado por S. Además, si $S = \{x_1, x_2, \ldots, x_m\}$, entonces $\langle S \rangle = \{x_{i_1}^{n_1} \cdots x_{i_r}^{n_r} : x_{i_j} \in S, n_i = \pm 1\}$.

Ejemplo. Para todo grupo G, $\langle \emptyset \rangle = \{1\}$.

Observación 1.13. Si G es abeliano y $S = \{x_1, x_2, \ldots, x_m\}$, entonces

$$\langle S \rangle = \langle x_1, x_2, \ldots, x_m \rangle = \{x_1^{n_1} \cdots x_m^{n_m} : n_j \in \mathbb{Z}\}.$$

Teorema 1.14. ***(Teorema de Lagrange)***
Si G es un grupo finito y $H \leq G$, entonces $|H|$ divide a $|G|$.

Definición 1.15. Grupo cíclico
Sea G un grupo. Se dice que G es cíclico si existe $a \in G$ tal que $G = \langle a \rangle = \{a^k : k \in \mathbb{Z}\}$.

Observación 1.16. Todo grupo cíclico es abeliano. El grupo $\mathbb{Z}$ de los números enteros es cíclico infinito y para todo entero $n > 1$, el grupo $\mathbb{Z}_n$ es cíclico finito. Además, se puede probar que todo grupo cíclico infinito es isoformo a $\mathbb{Z}$ y todo grupo cíclico finito de orden n es isoformo a $\mathbb{Z}_n$.

Teorema 1.17. *Todo subgrupo de un grupo cíclico es cíclico.*

Teorema 1.18. *Si A es un conjunto no vacío, entonces el conjunto de funciones de A en A tiene estructura de grupo definiendo la multipicación como la composición de funciones.*

El grupo del teorema anterior (1.18) se denota S_A. Además, si A es finito, con $|A| = n > 0$, se puede identificar a A con el conjunto $\{1, \ldots, n\}$, en este caso S_A se denota S_n y $|S_n| = n!$.

Ejemplo. El grupo simétrico S_3 de orden 6 esta dado por $S_3 = \{(1), (12), (13), (23), (123), (132)\}$.

Teorema 1.19. ***(Teorema de Cayley)***
Si G es un grupo finito, entonces existe $n > 1$ tal que G es isomorfo a un subgrupo de S_G.

Definición 1.20. Clase lateral derecha e izquierda
Sean G un grupo y $H \leq G$. La clase lateral derecha (izquierda) módulo H es el conjunto denotado con $(G/H)_{der}$ ($(G/H)_{izq}$) y definida por:

$$(G/H)_{der} = \{Ha : a \in G\}$$

$$(G/H)_{izq} = \{aH : a \in G\},$$

donde $Ha = \{ha : h \in H\}$ y análogamente, $aH = \{ah : h \in H\}$.

Ejemplo. Sean $G = S_3$ y $H = \{(1), (13)\}$. Las clases laterales izquierdas módulo H en G son:

$$\begin{aligned}
(1)H &= H, \\
(12)H &= \{(12), (12)(13)\} = \{(12), (132)\} = (132)H, \\
(13)H &= \{(13), (1)\} = H, \\
(23)H &= \{(23), (23)(13)\} = \{(23), (123)\} = (123)H.
\end{aligned}$$

Y las clases laterales derechas módulo H en G son:

$$\begin{aligned} H(1) &= H, \\ H(12) &= \{(12), (13)(12)\} = \{(12), (123)\} = (123)H, \\ H(13) &= \{(13), (13)(13)\} = H, \\ H(23) &= \{(23), (13)(23)\} = \{(23), (213)\} = (213)H. \end{aligned}$$

En general, la clase lateral izquierda aH es diferente de la clase lateral derecha Ha.

Teorema 1.21. *Si G un grupo y $H \leq G$, entonces las clases laterales izquierdas (derechas) módulo H en G particionan G, es decir, el grupo G es la unión órbitas de las clases laterales (derechas) módulo H en G.*

Definición 1.22. Subgrupo normal
Sean G un grupo y $H \leq G$. Se dice que H es subgrupo normal de G si para todo $a \in G$ se cumple $aH = Ha$. Esto se denota con $H \trianglelefteq G$.

Observación 1.23. En un grupo abeliano todo subgrupo es normal.

Ejemplo. Sea G un grupo. El centro de G, denotado con $Z(G)$, se define por

$$Z(G) = \{x \in G : xa = ax, \text{ para todo } a \in G\}.$$

No es difícil probar que $Z(G)$ es un subgrupo normal de G.

Observación 1.24. Para todo grupo G, los subgrupos triviales de G son subgrupos normales.

Un resultado clásico de la teoría de grupos es el siguiente teorema.

Teorema 1.25. ***(Grupo cociente)***
Sean G un grupo y $H \leq G$. Si $H \trianglelefteq G$, entonces el conjunto de la clase lateral derechas(izquierdas) con la operación binaria definida por:

$$(Ha)(Hb) = H(ab)$$

es un grupo denominado grupo cociente módulo H. Este grupo se denota G/H.

Definición 1.26. Grupo diédrico
Sea $n > 2$ un número entero. El n-ésimo grupo diédrico, denotado D_n, es el grupo de simetrías de un polígono regular de n lados. Si α es la rotación de ángulo $\frac{2\pi}{n}$ alrededor del centro del polígono y β es la reflexión con respecto a una recta que contiene al centro del mismo y uno cualquiera de sus vértices, entonces

$$D_n = \{\alpha^i : i \in \mathbb{Z}_n\} \cup \{\alpha^i\beta : i \in \mathbb{Z}_n\} = \langle \alpha, \beta : \alpha^n = \beta^2 = 1, \beta\alpha\beta^{-1} = \alpha^{-1} \rangle.$$

Ejemplo. El grupo de simetrías del cuadrado $D_4 = \{H, V, D_1, D_2, R_0, R_{\frac{\pi}{2}}, R_\pi, R_{\frac{3\pi}{2}}\}$ donde

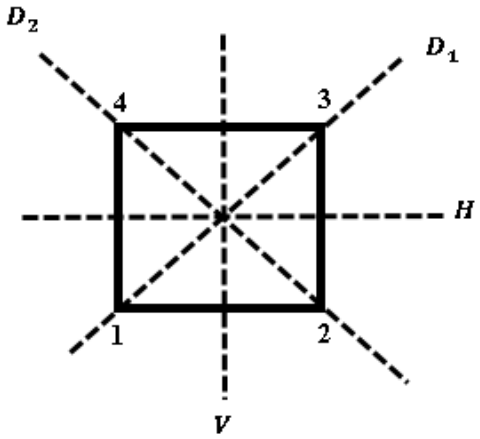

Figura 1.1: Elementos de D_4. Fuente: esta investigación.

Rotaciones

$$R_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

$$R_{\frac{\pi}{2}} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

$$R_\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

$$R_{\frac{3\pi}{2}} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

Reflexiones

$$H = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

$$V = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$D_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

$$D_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

Definición 1.27. Producto directo externo
Sean $G_1, G_2, \cdots, G_k$ grupos. El producto directo externo de los grupos G_i, con $i = 1, \ldots, k$, denotado con $G_1 \times G_2 \times \cdots \times G_k$, es el conjunto de todas las k-uplas ordenadas $(g_1, g_2, \ldots, g_k)$ tal que $g_i \in G_i$, es decir,

$$G = G_1 \times G_2 \times \cdots \times G_k = \{(g_1, g_2, \ldots, g_k) : g_i \in G \text{ para } i = 1, \ldots, k\}.$$

Se puede probar que el producto directo externo es un grupo definiendo la multiplicación en G componente a componente, es decir,

$$(g_1, \ldots, g_n)(g'_1, \ldots, g'_n) = (g_1 g'_1, \ldots, g_n g'_n).$$

En caso que todos los G_i son abelianos, se dice suma directa externa y se escribe

$$G = G_1 \oplus G_2 \oplus \cdots \oplus G_k.$$

Definición 1.28. Producto directo interno
Sea G un grupo y sean $H_1, H_2, \ldots, H_k$ subgrupos normales de G. Se dice que G es el producto directo interno de los H_i si se satisface las dos condiciones siguientes

1. $G = H_1H_2 \cdots H_k = \{h_1h_2 \cdots h_k : h_i \in H_i, i = 1, \ldots, k\}$
2. $H_i \cap \left(\prod_{\substack{j=1 \\ j \neq i}}^{k} H_j \right) = \{1\}$, para todo $i = 1, \ldots, k$.

Teorema 1.29. *Todo grupo abeliano finito G es isomorfo a un producto directo externo de grupos cíclicos, es decir,*

$$G = \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_s},$$

además, $m_j \mid m_{j+1}$, para todo $j = 1, \ldots, s-1$

Definición 1.30. Serie subnormal
Sea G un grupo. Una serie subnormal de G es una sucesión finita

$$G = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_n = \{1\},$$

de subgrupos de G tal que $H_i \trianglelefteq H_{i-1}$, para todo $i = 1, 2, \ldots, n$.

Definición 1.31. Serie normal
Sea G un grupo. Una serie normal de G es una serie subnormal donde todos los subgrupos de la serie son subgrupos normales de G.

Ejemplo. Una serie subnormal no necesariamente es una serie normal, considere la siguiente serie subnormal del grupo D_4

$$D_4 \supset \{R_0, H, R_\pi, V\} \supset \{R_0, H\} \supset \{R_0\}.$$

El subgrupo $\{R_0, H\}$ no es normal en D_4, dado que $HR_{\frac{\pi}{2}} \neq R_{\frac{\pi}{2}}H$, pues $D_1 \neq D_2$, por lo tanto esta no es una serie normal.

Observación 1.32. En un grupo abeliano toda serie subnormal es normal. En particular, las siguientes series son series normales en el grupo $\mathbb{Z}$.

$$\mathbb{Z} \supset 9\mathbb{Z} \supset 45\mathbb{Z} \supset 180\mathbb{Z} \supset \{0\},$$

$$\mathbb{Z}_{24} \supset \langle 2 \rangle \supset \langle 6 \rangle \supset \langle 12 \rangle \supset \{0\}.$$

Definición 1.33. Grupo soluble
Sea G un grupo. Se dice que G es un grupo soluble si tiene una serie normal

$$G = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_n = \{1\},$$

tal que cada grupo cociente H_{i-1}/H_i es abeliano.

Ejemplo. Los grupos S_3, S_4, A_3 y A_4 son solubles, basta exhibir las series de composición

$$\begin{aligned}
&\{1\} \leq A_3 \leq S_3\\
&\{1\} \leq \{(12)(34), (13)(24)\} \leq A_4 \leq S_4\\
&\{1\} \leq A_3\\
&\{1\} \leq \{(12)(34), (13)(24)\} \leq A_4.
\end{aligned}$$

Teorema 1.34. *Para $n \geq 5$ los grupos S_n y A_n no son solubles.*

Observación 1.35. Todo grupo abeliano es soluble y un subgrupo H de un grupo soluble G es también soluble .

Definición 1.36. Grupo Hamiltoniano
Un grupo H es hamiltoniano si H es no abeliano y todo subgrupo de H es normal.

Definición 1.37. Grupo de los Cuaterniones
El conjunto de los cuaterniones puede expresarse como:

$$\mathcal{Q} = \langle a, b : a^4 = 1, b^2 = a^2, bab^{-1} = a^{-1}\rangle = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}.$$

Teorema 1.38. *H es un grupo hamiltoniano finito si y solo si, $H = \mathcal{Q} \times (\mathbb{Z}_2)^n \times G$, donde $\mathcal{Q}$, es el grupo de los cuaterniones y G un grupo abeliano finito de orden impar.*

Teorema 1.39. *Sea G un grupo no abeliano de orden 8, entonces $G \cong D_4$ ó $G \cong \mathcal{Q}$*

Ejemplo. El grupo de los Cuaterniones es Hamiltoniano porque es no abeliano y los subgrupos $\mathcal{Q}$, $\{1\}, \{1, a^2\}$, $\{1, a, a^2, a^3\}$, $\{1, b, a^2, a^2b\}$ y $\{1, ab, a^2, a^3b\}$ son normales.

A continuación, se presentan las definiciones y los teoremas que sustentan los temas de la teoría de Sylow que se utilizarán en este trabajo. Las demostraciones de estos resultados se pueden consultar Lezama (2014) [11].

Definición 1.40. Acción de grupo
Sea G un grupo y X un conjunto no vacío. Se dice que G actúa sobre X (o X es un $G-$*conjunto*) si está definida una aplicación $\alpha : G \times X \to X$, que asigna a cada pareja ordenada $(g, x) \in G \times X$ el elemento $\alpha(g, x) = g \cdot x \in X$ y que satisface las siguientes condiciones.

1. Para cualesquiera $x \in X$ se cumple $1 \cdot x = x$.

2. Para cualesquiera $h, g \in G$ y $x \in X$ se cumple $(hg) \cdot x = h \cdot (g \cdot x)$. Se dice que X es un $G - conjunto$ (izquierdo).

Definición 1.41. $G -$ **órbita**
Sean G un grupo y X un $G - conjunto$. Para cada $x \in X$, la $G -$ órbita determinada por x, denotada Gx, es el subconjunto de X definido de la siguiente forma

$$Gx = \{g \cdot x : g \in G\}.$$

Teorema 1.42. *Sea X un $G - conjunto$ y sea x un elemento de X. El subgrupo estacionario del punto x en G, denotado G_x, es el subgrupo de G definido por*

$$G_x = \{g \in G : g \cdot x = x\}.$$

Además, $|Gx| = |G : G_x|$.

Teorema 1.43. *Sea X un $G - conjunto$. La relación $\sim$ definida en x por*

$$x \sim y \Longleftrightarrow g \cdot x = y, \text{ para algún } g \in G,$$

es una relación de equivalencia en X. Las clase de equivalencia del elemento $x \in X$ es la $G -$ órbita determinada por x. En particular, X se descompone en la unión disjunta de sus $G -$ órbitas:

$$X = \dot{\bigcup_{Gx \subset G/X}} Gx,$$

donde G/X denota el conjunto de las órbitas.

Ejemplo. Sea G un grupo. Si $H \leq G$, entonces G es un $H - conjunto$ definiendo la acción de forma natural , es decir, $h \cdot x = hx$, para todo $h \in H$ y todo $x \in G$.

Definición 1.44. Conjugado
Sean G un grupo, $A \subset G$ y $x \in G$. El conjunto $xAx^{-1} = \{xax^{-1} : a \in A\}$, se denomina el conjugado de A por x.

Ejemplo. Para el grupo G y el subgrupo H del anterior ejemplo, el conjugado de H por $(12) \in G$ esta dado por

$$(12)H(12) = \{(12)(1)(12), (12)(13)(12)\} = \{(1), (23)\}.$$

Teorema 1.45. *Sea G un grupo que actúa sobre el conjunto X.*

1. *Si x, y están en la misma órbita, entonces sus grupos estacionarios son conjugados:*

$$y = g \cdot x \Rightarrow G_y = gG_xg^{-1}.$$

2. *Si G es un grupo finito y $X = X_1 \cup \cdots \cup X_r$ es la partición de X en un número finito de r órbitas con representantes $x_1, \cdots, x_r$, entonces*

$$|X| = \sum_{i=1} r[G : G_{x_i}].$$

Definición 1.46. Transportador
Sea G un grupo y sean U, V dos subconjuntos no vacíos de G. El conjunto transportador de V en U, denotado con $U : V$, se define por

$$U : V = \{x \in G : xV \subseteq U\}.$$

Lema 1.47. *Sea G un grupo. Si $A, B, U, V \subseteq G$, entonces*

$$G \setminus (AB) = (G \setminus A) : B^{-1} \quad y \quad G \setminus (U : V) = (G \setminus U)V^{-1}.$$

Demostración. Se va probar la igualdad $G \setminus (AB) = (G \setminus A) : B^{-1}$. Sea $A = G \setminus U$ y $B = V^{-1}$. Reemplazando, el objetivo es mostrar $G \setminus AB = U : V$. Para probar $U : V \subseteq G \setminus AB$ suponga que $x \notin G \setminus AB$, así $x \in AB$, luego existen $a \in A$ y $b \in B$ tales que $x = ab$, entonces $xb^{-1} = a$, además $a \notin U$, $b \in V^{-1}$, así $x \notin U : V$. Para demostrar $G \setminus AB \subseteq U : V$ suponga que $x \notin U : V$, entonces existe $v \in V$ tal que $xv \notin U$, luego $xv \in A$, es decir, $xv = a$, para algún $a \in A$, entonces $x = av^{-1} \in AB$. Por tanto $G \setminus AB = U : V$. De manera similar, se prueba $G \setminus (U : V) = (G \setminus U)V^{-1}$, o equivalente $G \setminus (U : V) = AB$. □

Definición 1.48. Estabilizador
Sea G un grupo y A subconjunto no vacío de G. El conjunto estabilizador de A en G, denotado con $\mathbb{S}(A)$ es el conjunto definido por

$$\mathbb{S}(A) = \{g \in G : gA = A\}.$$

Teorema 1.49. *Si A es un subconjunto no vacío de un grupo G, entonces $\mathbb{S}(A) \leq G$. Además, Si A es finito, $|\mathbb{S}(A)|$ divide a $|A|$.*

Demostración. Sean G un grupo y $A \subseteq G$. Dado que $1A = A$ se tiene $1 \in \mathbb{S}(A)$. Sea $h, g \in \mathbb{S}(A)$, se tiene $(gh)A = g(hA) = gA = A$ luego $gh \in \mathbb{S}(A)$. Además,
$g^{-1}A = g^{-1}(gA) = 1A = A$. Por lo tanto, $\mathbb{S}(A) \leq G$. Ahora, se va probar que en el caso que A es finito, se tiene $|\mathbb{S}(A)|$ divide a $|A|$. Sea $S = \mathbb{S}(A)$ y defina la acción de grupo $\alpha : S \times A \to A$ que asigna a cada pareja ordenada $(s, a) \in S \times A$ el elemento $\alpha(s, a) = s \cdot a$. Dado que A es

finito y la relación $\sim$ definida en (1.43) es de equivalencia en A, entonces existen elementos $a_1, \ldots, a_r \in A$, tal que A se particiona en $A = Sa_1 \cup \cdots \cup Sa_r$, donde Sa_j es la $S-$órbita de a_j. Por teoremas (1.45) y (1.42) se tiene $|A| = \sum_{i=1}^{r} |Sa_i|$, además, la función $f : S \to Sa_i$, definida por $f(x) = xa_i$ es biyectiva, es decir, $|S| = |Sa_i|$, para todo $i = 1, \ldots, r$, por lo tanto $|A| = \sum_{i=1}^{r} |S| = r|S|$.

Teorema 1.50. ***(Cauchy)***
Si G es un grupo finito cuyo orden es divisible por un primo p, entonces G contiene un elemento de orden p.

Definición 1.51. ***$p-$ grupo***
Sea G un grupo y sea p un número primo. Se dice que G es un $p-$*grupo*, si el orden de todo elemento de G es una potencia de p.

Teorema 1.52. *Un grupo finito G es un $p-$ grupo si y solo si, $|G| = p^n$, para algún entero no negativo n.*

Ejemplo. El grupo de Klein de 4 elementos $V = \{1, a, b, ab\}$, donde $a = a^{-1}$, $b = b^{-1}$, $ab = (ab)^{-1}$ es un $2-$*grupo*.

Definición 1.53. ***$P-$ subgrupo***
Sea G un grupo y sea p un número primo. Se dice que $H \leq G$ es un $p-$*subgrupo* de G , si H es un $p-$*grupo*.

Definición 1.54. ***$P-$ subgrupo* de Sylow**
Sea G un grupo. Un $p-$*subgrupo* H se denomina $p-$*subgrupo* de Sylow de G si H es maximal entre los $p-$*subgrupos* de G. El conjunto de todos los $p-$*subgrupos* de Sylow de un grupo G se denota con $N_G(p)$ y $|N_G(p)|$ se denota con N_p.

Teorema 1.55. ***(Primer teorema de Sylow)***
Si G es un grupo finito y p un número primo, entonces para cada potencia p^α que divide $|G|$, existe en G un subgrupo de orden p^α. Además, si $p^{\alpha+1}$ también divide $|G|$, entonces cada subgrupo de orden p^α está incluido en un subgrupo de orden $p^{\alpha+1}$. En particular, los $p-$ subgrupos de Sylow de G existen y son los subgrupos de G de orden p^r, donde p^r es la máxima potencia de p que divide $|G|$.

Teorema 1.56. ***(Segundo teorema de Sylow)***
Si G un grupo finito y p un número primo que divide $|G|$, entonces todos los $p-$ subgrupos de Sylow de G son conjugados.

Teorema 1.57. ***(Tercer teorema de Sylow)***
Si G un grupo finito y p un número primo que divide $|G|$, entonces $N_p \equiv 1 (\text{mód } p)$, y $N_p \mid |G|$.

Teorema 1.58. *Un $p-$ subgrupo de Sylow de un grupo G es normal en G si y solo si, H es el único $p-$ subgrupo de Sylow de G.*

1.3. Problema de los conjuntos producto pequeños

En un grupo G, mediante $H(G)$, se denotará el conjunto de todos los órdenes de subgrupos finitos de G y con $N(G)$ el subconjunto de $H(G)$ formado por los órdenes de subgrupos normales de G, es decir,

$$H(G) = \{n \in \mathbb{N} : n \text{ es el orden de un subgrupo finito de } G\}.$$
$$N(G) = \{n \in \mathbb{N} : n \text{ es el orden de un subgrupo normal finito de } G\}.$$

Además, cuando G es un grupo finito se denotará con $D(G)$ el conjunto de divisores de $|G|$, es decir, $D(G) = \{d \in \mathbb{N} : d \text{ es divisor de } |G|\}$. Observe que para un grupo abeliano finito G se tiene $H(G) = D(G) = N(G)$.

Definición 1.59. Conjunto producto
Sea G un grupo y sean A, B subconjuntos no vacíos de G. El conjunto producto de A y B, denotado por AB, es el conjunto de todos los elementos en G de la forma ab, donde $a \in A$ y $b \in B$, es decir, $AB = \{ab : a \in A \text{ y } b \in B\}$. Si $A = \emptyset$ o $B = \emptyset$, se define $AB = \emptyset$.

Uno de los problemas de la Teoría Aditiva de Números consiste en determinar el mínimo de los cardinales $|AB|$, donde A y B son subconjuntos no vacíos de un grupo G tales que $|A| = r$ y $|B| = s$. En grupos abelianos, por la notación aditiva, este problema se denomina problema de los conjuntos suma pequeños y en grupos no abelianos, por la notación multiplicativa, se denomina **problema de los conjuntos producto pequeños**. Los avances obtenidos dentro de este problema utilizan las siguientes definiciones.

Definición 1.60. Función $\mu_G(r, s)$
Sean G un grupo y r, s enteros positivos tales que $r, s \leq |G|$, se define $\mu_G(r, s)$ de la siguiente forma:

$$\mu_G(r, s) = \text{mín}\{|AB| : A, B \subseteq G, |A| = r, |B| = s\}$$

y se dice que $A, B \subseteq G$ realizan a $\mu_G(r, s)$ si $|A| = r, |B| = s$ y $|AB| = \mu_G(r, s)$.

Es decir, para un grupo G y enteros positivos r y s, el problema de los conjuntos producto pequeños trata de calcular el valor de $\mu_G(r, s)$. Determinar directamente este valor es un proceso complicado debido al gran número de operaciones que se deben realizar, de hecho, no existe un algoritmo en tiempo polinomial que de solución al problema, por tal motivo adquiere importancia la búsqueda de una fórmula explícita que facilite el cálculo de $\mu_G(r, s)$ que dependa únicamente de r y s. En 2005 Eliahou y Kervaire [1] introducen la función aritmética $\kappa_G(r, s)$ que depende solo de r, s, y los órdenes de los subgrupos de G, y con ella describen varios casos donde las funciones $\kappa_G(r, s)$ y $\mu_G(r, s)$ coinciden, además introducen variantes de esta función, con las cuales consiguen acotar la función $\mu_G(r, s)$.

Definición 1.61. Función techo
Sea $\epsilon \in \mathbb{R}$, el techo de ϵ denotado con $\lceil \epsilon \rceil$, es el menor entero x mayor o igual que ϵ, es decir, $\lceil \epsilon \rceil = x$ si y solo si, $x \in \mathbb{Z}$ y $x - 1 < \epsilon \leq x$.

Definición 1.62. Función $\kappa_G(r, s)$
Sean G un grupo y r, s enteros positivos tales que $r, s \leq |G|$, se define $\kappa_G(r, s)$ de la siguiente forma:

$$\kappa_G(r, s) = \min_{n \in H(G)} \left\{ \left(\left\lceil \frac{r}{n} \right\rceil + \left\lceil \frac{s}{n} \right\rceil - 1 \right) n \right\}.$$

Definición 1.63. Función $N_{\kappa_G}(r, s)$
Sean G un grupo y r, s enteros tales que $1 \leq r, s \leq |G|$, se define $N_{\kappa_G}(r, s)$ de la siguiente forma:

$$N_{\kappa_G}(r, s) = \min_{n \in N(G)} \left\{ \left(\left\lceil \frac{r}{n} \right\rceil + \left\lceil \frac{s}{n} \right\rceil - 1 \right) n \right\}.$$

Definición 1.64. Función $D_{\kappa_G}(r, s)$
Sean G un grupo y r, s enteros tales que $1 \leq r, s \leq |G|$, se define $D_{\kappa_G}(r, s)$ de la siguiente forma:

$$D_{\kappa_G}(r, s) = \min_{n \in D(G)} \left\{ \left(\left\lceil \frac{r}{n} \right\rceil + \left\lceil \frac{s}{n} \right\rceil - 1 \right) n \right\}.$$

Las funciones $\kappa_G(r, s)$, $N_{k_G}(r, s)$ y $D_{k_G}(r, s)$ se definen como el valor mínimo de

$$f_d(r, s) = \left(\left\lceil \frac{r}{d} \right\rceil + \left\lceil \frac{s}{d} \right\rceil - 1 \right) d,$$

donde d está en $H(G), N(G)$ y $D(G)$, respectivamente. Para un breve resumen de estas funciones Eliahou y Kervaire (2007) [12]. Note que en todo grupo finito G y todo par de enteros r, s tales que $1 \leq r, s \leq |G|$, se tiene $D_{k_G}(r, s) \leq \kappa_G(r, s) \leq N_{k_G}(r, s)$, porque $N(G) \subseteq H(G) \subseteq D(G)$.

1.4. Función μ_G en grupos abelianos

En un grupo abeliano G se conoce una fórmula exacta para la función μ_G. Antes de presentar dicha fórmula se enuncian los resultados más importantes que la antecedieron.
En 1813 el famoso matemático francés Augustin Louis Cauchy probó que tal aseveración permanece verdadera cuando G es un grupo cíclico de orden primo. Dicho resultado fue redescubierto por Davenport en 1935 y actualmente se conoce como el teorema de Cauchy-Davenport, Wheeler (2012) [13], este es uno de los primeros resultados dentro del problema de los conjuntos suma pequeños.

Teorema 1.65. ***(Cauchy-Davenport)***
Si p es un número primo, A y B son dos subconjuntos no vacíos del grupo cíclico $\mathbb{Z}_p$, entonces

$$|A + B| \geq \min\{|A| + |B| - 1, p\}.$$

Una consecuencia inmediata del teorema anterior es el siguiente corolario:

Corolario 1.66. *Sean p un número primo A y B subconjuntos no vacíos del grupo cíclico $\mathbb{Z}_p$. Si $|A| = r$ y $|B| = s$, con $1 \leq r, s \leq p$, entonces $\mu_G(r, s) = \min\{r + s - 1, p\}$.*

Para un grupo libre de torsión G, es decir, todos los elementos de G tienen orden infinito, Kemperman (1956) [14] demuestra que $\mu_G(r, s) = \kappa_G(r, s)$. En 2003, Plagne [2] probó que en un grupo abeliano finito G, se cumple que

$$\mu_G(r, s) \geq \min_{n \in D(G)} \left\{ \left(\left\lceil \frac{r}{d} \right\rceil + \left\lceil \frac{s}{d} \right\rceil - 1 \right) d \right\}.$$

Posteriormente en 2005 Eliahou, Kervaire [1] extendieron el resultado anterior para todo grupo abeliano arbitrario, y este resultado también fue obtenido por Plagne (2007) [3], realmente ellos probaron el siguiente teorema.

Teorema 1.67. *Sea G es un grupo abeliano arbitario. Si r y s son enteros tales que $1 \leq r, s|G|$, entonces*

$$\mu_G(r, s) = \min_{n \in H(G)} \left\{ \left(\left\lceil \frac{r}{n} \right\rceil + \left\lceil \frac{s}{n} \right\rceil - 1 \right) n \right\} = \kappa_G(r, s).$$

Ejemplo. Sean el grupo $\mathbb{Z}_5$, los enteros $r = 4$ y $s = 5$, entonces $\mu_{\mathbb{Z}_5}(4, 5) = 5$.

El teorema anterior da solución completa al problema de determinar una fórmula explícita para la función $\mu_G(r, s)$ en grupos abelianos. El problema de los conjuntos producto pequeños en grupos no abelianos no esta completamente resuelto, y se conoce por Eliahou y Kervaire (2007) [4], que la formula obtenida en el teorema anterior no se se puede extender para grupos no abelianos, ellos encontraron que en el grupo $G = \langle x, y : x^3 = 1, y^7 = 1, x*y*x^{-1}*y^{-2} = 1 \rangle$, para los siguientes valores de r y s la igualdad $\mu_G(r, s) = \kappa_G(r, s)$ no se cumple, como se muestra en la tabla.

(r, s)	μ_G	κ_G
(6, 8)	13	12
(6, 9)	14	12
(8, 9)	16	15
(9, 9)	17	15
(5, 9)	1 3	12

Tabla 1.1: Comparación de μ_G y κ_G. Fuente: esta investigación.

Sin embargo, se conoce que la igualdad $\mu_G(r, s) = \kappa_G(r, s)$ se satisface en algunas clases de grupos no abelianos finitos, esto se presentará en el siguiente capítulo.

Capítulo 2

Función μ_G en grupos no abelianos

En el capítulo anterior se expusieron los teoremas que resuelven el problema de los conjuntos suma pequeños en grupos abelianos. Aunque en el caso no abeliano este problema aún está abierto, se conoce algunos resultados, que se presentaran en este capítulo. Eliahou y Kervaire (2007) [4] estudiaron las propiedades básicas de la función μ_G en un grupo finito no abeliano y (2006), (2006) y (2007) [15], [16] y [12] probaron teoremas para esta función en grupos solubles y diédricos, por su parte Mutis, Benavides y Castillo (2010) y (2012) [7] y [8] estudiaron la función μ_G en grupos hamiltonianos y $p-$ *grupos* finitos.

2.1. Propiedades básicas de μ_G

En 2007 Eliahou y Kervaire [4] demuestran que para algunos valores r y s se tiene la igualdad $\mu_G(r,s) = \kappa_G(s,r)$ y estudiaron las propiedades que satisface la función $\mu_G(r,s)$, esto se puede ver en los siguientes teoremas.

Teorema 2.1. *Si G es un grupo finito, entonces existen A, B subconjuntos de G que realizan $\mu_G(r,s)$ y tal que $1 \in A \cap B$.*

Demostración. Sean A y B dos subconjuntos de G que realizan $\mu_G(r,s)$, fije $a \in A$, $b \in B$ y denote $A' = a^{-1}A$ y $B' = Bb^{-1}$. Se tiene $r = |A| = |A'|$ y $s = |B| = |B'|$, luego

$$|Bb^{-1}a^{-1}A| = |A'B'| = |AB| = \mu_G(r,s).$$

Dado que $a^{-1}a = 1 = bb^{-1}$ se tiene $1 \in A' \cap B'$. □

Teorema 2.2. *Sea G un grupo finito. Si r,s son enteros tales que $1 \leq r, s \leq |G|$, entonces $\mu_G(r,s) = \mu_G(s,r)$.*

Demostración. Sean A y B dos subconjuntos de G que realizan $\mu_G(r,s)$. Se tiene $r = |A| = |A^{-1}|$ y $s = |B| = |B^{-1}|$. Además

$$|B^{-1}A^{-1}| = |(AB)^{-1}| = |AB| = \mu_G(r,s).$$

Luego, $\mu_G(s,r) \leq |B^{-1}A^{-1}| \leq \mu_G(r,s)$. De manera de similar, se prueba $\mu_G(r,s) \leq \mu_G(s,r)$ y de las dos desigualdades se concluye $\mu_G(s,r) = \mu_G(r,s)$. □

Teorema 2.3. *Sea G un grupo finito. Si r,s son enteros tales que $1 \leq r,s \leq |G|$, entonces $\mu_G(r,s) \geq \text{máx}\{r,s\}$.*

Demostración. Sean A y B dos subconjuntos de G que realizan $\mu_G(r,s)$. Fijando un elemento $a \in A$ y un elemento $b \in B$ se tiene $aB \subseteq AB$ y $Ab \subseteq AB$, luego

$$|AB| \geq \text{máx}\,\{|aB|, |Ab|\} \geq \text{máx}\,\{r,s\}.$$

Por lo tanto $\mu_G(r,s) \geq \text{máx}\{r,s\}$. □

Teorema 2.4. *Sea G un grupo finito, se tiene que $\mu_G(r,r) = r$ si y solo si, G contiene un subgrupo H de orden r.*

Demostración. Por el teorema (2.1) G se pueden escoger A y B subconjuntos de G que realizan $\mu_G(r,r)$ tales que $1 \in A \cap B$. Luego $A, B \subseteq AB$ y dado que

$$|A| = |B| = r = \mu_G(r,r) = |AB|,$$

entonces $A = B = AB$, es decir, $A = AA$ y así A es un subgrupo de G de orden r. Para el recíproco sea H un subgrupo de G de orden r se tiene

$$\mu_G(r,r) \leq |HH| = |H| = r.$$

Por el teorema (2.3), $\mu_G(r,r) \geq \text{máx}\{r,r\} = r$. Por lo que se concluye $\mu_G(r,r) = r$. □

Teorema 2.5. *Si s,t son enteros positivos tales que $s \leq t$, entonces $\mu_G(r,s) \leq \mu_G(r,t)$*

Demostración. Sean A y B dos subconjuntos de G que realizan $\mu_G(r,t)$ y sea D un subconjunto de B de cardinal s, se tiene

$$\mu_G(r,s) \leq |AD| \leq |AB| = \mu_G(r,t).$$

□

Teorema 2.6. *Si r, s son enteros tales que $r + s > |G|$, entonces $\mu_G(r,s) = \kappa_G(r,s) = |G|$.*

Demostración. Sean A y B dos subconjuntos de G que realizan $\mu_G(r,s)$. Denote $g=|G|$ y h el orden de un subgrupo de G tal que

$$\kappa_G(r,s)=\left(\left\lceil\frac{r}{h}\right\rceil+\left\lceil\frac{s}{h}\right\rceil-1\right)h.$$

Se conoce que $\left\lceil\frac{r}{h}\right\rceil+\left\lceil\frac{s}{h}\right\rceil\geq\frac{r}{h}+\frac{s}{h}$ y por hipótesis $[\left\lceil\frac{r}{h}\right\rceil+\left\lceil\frac{s}{h}\right\rceil>\frac{g}{h}$. Por el teorema de Lagrange (1.14), $\frac{g}{h}$ es entero, entonces $\left\lceil\frac{r}{h}\right\rceil+\left\lceil\frac{s}{h}\right\rceil-1\geq\frac{g}{h}$, es decir, $\left(\left\lceil\frac{r}{h}\right\rceil+\left\lceil\frac{s}{h}\right\rceil-1\right)h\geq g$, por tanto $\kappa_G(r,s)\geq g$. Por otro lado,

$$\kappa_G(r,s)\leq\left(\left\lceil\frac{r}{g}\right\rceil+\left\lceil\frac{s}{g}\right\rceil-1\right)g=(1+1-1)g=g.$$

De las anteriores desigualdades se concluye $\kappa_G(r,s)=g$. Para verificar que $\mu_G(r,s)=g$, sea x un elemento arbitrario de G y observe que los conjuntos A y xB^{-1} no pueden ser disjuntos porque tienen cardinales r y s respectivamente y $r+s>g$, luego

$$G=\{x\in G:A\cap xB^{-1}\neq\emptyset\}\subseteq AB,$$

así $G=AB$. Por tanto $g=|AB|=\mu_G(r,s)$. □

Teorema 2.7. *Si $\kappa_G(r,s)<s+\frac{r}{2}$ o $\mu_G(r,s)<s+\frac{r}{2}$, entonces $\mu_G(r,s)=\kappa_G(r,s)$, es decir, para todo i tal que $0\leq i<\frac{r}{2}$ se tiene la equivalencia*

$$\mu_G(r,s)=s+i \text{ si y solo si, } \kappa_G(r,s)=s+i.$$

Demostración. La prueba se hará por inducción. Para $i=0$, suponga $\mu_G(r,s)=s$ y sea d el orden de un subgrupo de G tal que

$$\kappa_G(r,s)=\left(\left\lceil\frac{r}{d}\right\rceil+\left\lceil\frac{s}{d}\right\rceil-1\right)d.$$

Se conoce que $\left\lceil\frac{r}{d}\right\rceil-1\geq 0$ y $\left\lceil\frac{s}{d}\right\rceil\geq\frac{s}{d}$, entonces $\left\lceil\frac{r}{d}\right\rceil+\left\lceil\frac{s}{d}\right\rceil-1\geq\frac{s}{d}$, por lo tanto $\kappa_G(r,s)\geq s$. Por el teorema (2.1) existen A y B subconjuntos de G que realizan $\mu_G(r,s)$ tal que $1\in A\cap B$, entonces $B\subseteq AB$, así $|B|\leq|AB|$. Además, por hipótesis se tiene $|AB|=\mu_G(r,s)=s$, es decir, $B=AB$ pues los dos subconjuntos tienen la misma cardinalidad. Ahora sea H el estabilizador de B definido en (1.48), luego $A\subseteq H$. Observe que la función $*:H\times B\to B$ que asigna a cada pareja $(x,b)\in H\times B$ el elemento $xb\in B$ define una acción de H en B porque H es el estabilizador de B. La $H-$órbita determinada por un elemento $b\in B$ definida en (1.41) está dada por $Hb=\{hb:h\in H\}$, y por teorema (1.45) el conjunto B se descompone en unión disjunta de $H-$órbitas. Suponga que l es la cantidad de estas $H-$órbitas y denote $h=|H|$, entonces $B=Hb_1\dot\cup\cdots\dot\cup Hb_l$, así que $s=|B|=l|H|=lh$. De lo anterior se tiene que $h|s$, además, $r\leq h$ porque $A\subseteq H$ entonces

$$\kappa_G(r,s)\leq\left(\left\lceil\frac{r}{h}\right\rceil+\left\lceil\frac{s}{h}\right\rceil-1\right)h=\frac{s}{h}h=s.$$

De las dos desigualdades se concluye $\kappa_G(r,s) = s$. Ahora suponga que $\kappa_G(r,s) = s$ y sea h el cardinal de un subgrupo H de G tal que $\kappa_G(r,s) = \left(\left\lceil \frac{r}{h} \right\rceil + \left\lceil \frac{s}{h} \right\rceil - 1\right) h$, esto significa que $\frac{s}{h}$ es un entero, entonces

$$\left\lceil \frac{r}{h} \right\rceil + \left\lceil \frac{s}{h} \right\rceil - 1 = \frac{s}{h} = \left\lceil \frac{s}{h} \right\rceil,$$

luego $\left\lceil \frac{r}{h} \right\rceil = 1$, así $r \leq h$. Por el teorema (2.3) se tiene $\mu_G(r,s) \geq \text{máx}\{r,s\} = s$ porque $r \leq h \leq s$. Sea $q = \frac{s}{h}$, entonces $|B| = s = qh$, luego existen elementos $b_1, \ldots, b_q \in B$ tales que $B = Hb_1 \dot{\cup} Hb_2 \dot{\cup} \cdots \dot{\cup} Hb_q$. Ahora, sea $A \subseteq H$ de cardinal r, entonces $AB \subseteq HB \subseteq B$ luego

$$\mu_G(r,s) \leq |AB| \leq |B| = hq = s.$$

De las dos desigualdades se concluye $\mu_G(r,s) = s$. Para continuar el proceso de inducción, acepte que se cumple que para todo j tal que $0 \leq j < i < \frac{r}{2}$ se tiene

$$\mu_G(r,s) = s + j \text{ si y solo si, } \kappa_G(r,s) = s + j.$$

Finalmente, suponga $\mu_G(r,s) = s + j + 1$ y sea d el orden de un subgrupo de G tal que

$$\kappa_G(r,s) = \left(\left\lceil \frac{r}{d} \right\rceil + \left\lceil \frac{s}{d} \right\rceil - 1\right) d.$$

Dado que $\kappa_G(r,s) \geq s$, existe un entero no negativo k tal que $\kappa_G(r,s) = s + k$. Note que si $k \in \{0, \ldots, j\}$, por hipótesis inductiva, se tendría $\mu_G(r,s) = s+k \leq s+j < s+j+1 = \mu_G(r,s)$, esto es una contradicción, luego $k \geq j+1$, es decir,

$$\mu_G(r,s) = s + j + 1 \leq s + k = \kappa_G(r,s).$$

Por el teorema (2.1) existen subconjuntos A y B de G que realizan $\mu_G(r,s)$ tal que $1 \in A \cap B$ y dado que $j + 1 < \frac{r}{2}$ se tiene

$$|AB| = \mu_G(r,s) = s + j + 1 =< s + \frac{r}{2} = \frac{1}{2}|A| + |B|.$$

Además , $|A^{-1}| = r$ y $|B^{-1}| = s$ y por el teorema principal de Olson, Olson (1984) [17] se debe tener $(B^{-1}A^{-1})A^{-1} = B^{-1}A^{-1}$, luego

$$[(B^{-1}A^{-1})A^{-1}]^{-1} = [B^{-1}A^{-1}]^{-1}$$
$$A(AB) = AB.$$

Por tanto, A está contenido en el estabilizador $H = \mathbb{S}(AB)$ definido en 1.48, luego $AB \subseteq HB$. Por otro lado $B \subseteq AB$ porque $1 \in A$, luego $HB \subseteq H(AB) = AB$. Por lo tanto $AB = HB$, entonces existen $b_1, b_2, \ldots, b_l \in B$ tales que $AB = Hb_1 \dot{\cup} Hb_2 \dot{\cup} \cdots \dot{\cup} Hb_l$ y denotando $h = |H|$ se tiene $s + j + 1 = |AB| = l|H| = lh$, es decir, $h \mid (s + j + 1)$ y así

$$\kappa_G(r,s) \leq \left(\left\lceil \frac{r}{h} \right\rceil + \left\lceil \frac{s}{h} \right\rceil - 1\right) h = \left\lceil \frac{s}{h} \right\rceil h \leq \left\lceil \frac{s+j+1}{h} \right\rceil h = \frac{s+j+1}{h} h = s + j + 1.$$

Por tanto $\kappa_G(r,s) = s+j+1$. Para probar el recíproco suponga $\kappa_G(r,s) = s+j+1$. Dado que $\mu_G(r,s)$ existe un entero no negativo k tal que $\mu_G(r,s) = s+k$, y por hipótesis inductiva se debe tener $k \geq j+1$ y así $\mu_G(r,s) \geq s+j+1$. Ahora resta probar que $\mu_G(r,s) \leq s+j+1$. Sea h el orden de un subgrupo de G tal que

$$\kappa_G(r,s) = s+j+1 = \left(\left\lceil \frac{r}{h} \right\rceil + \left\lceil \frac{s}{h} \right\rceil - 1\right) h.$$

Esto significa que $h \mid (s+j+1)$. Sea $s' = \text{mín}\{ht \in \mathbb{Z} : s \leq ht \leq s+j+1\}$. Luego,

$$\left\lceil \frac{s}{h} \right\rceil \leq \left\lceil \frac{s'}{h} \right\rceil \leq \left\lceil \frac{s+j+1}{h} \right\rceil$$

$$\left\lceil \frac{s}{h} \right\rceil \leq \frac{s'}{h} \leq \frac{s+j+1}{h}.$$

Además, $\left\lceil \frac{s}{h} \right\rceil - 1 < \frac{s}{h} \leq \left\lceil \frac{s}{h} \right\rceil$, entonces $s \leq h\left\lceil \frac{s}{h} \right\rceil \leq s' \leq s+j+1$. Por minimilidad de s' se tiene $s' = h\left\lceil \frac{s}{h} \right\rceil$ ó $s' = s$. Para el caso $s = s'$ se tiene $\left\lceil \frac{s}{h} \right\rceil = \frac{s}{h}$, es decir, $h \mid s$. Pero $h \mid (s+j+1)$, entonces $h \mid j+1$, de aquí, $h \leq j+1$ y se tiene $h+j+1 \leq 2(j+1)$. Dado que

$$\left(\left\lceil \frac{r}{h} \right\rceil + \left\lceil \frac{s}{h} \right\rceil - 1\right) h = s+j+1,$$

se tiene $\left\lceil \frac{r}{h} \right\rceil - 1 = \frac{j+1}{h}$, esto es, $\left\lceil \frac{r}{h} \right\rceil h = h+j+1 \leq 2(j+1)$, además $r \leq \left\lceil \frac{r}{h} \right\rceil h$, así que, $r \leq 2(j+1)$, lo que contradice $j+1 < \frac{r}{2}$. Por tanto $s' = h\left\lceil \frac{s}{h} \right\rceil$, entonces

$$\kappa_G(r,s') \leq \left(\left\lceil \frac{r}{h} \right\rceil + \frac{s'}{h} - 1\right) h = \left(\left\lceil \frac{r}{h} \right\rceil + \left\lceil \frac{s}{h} \right\rceil - 1\right) h = s+j+1.$$

Dado que $s' > s$ existe $k \in \mathbb{Z}^+$ tal que $s'-k = s$, luego $s+j+1 = s'+(j+1-k)$, además $j+1-k < j+1$. Así aplicando al par (r,s') la hipótesis inductiva se tiene $\mu_G(r,s') = \kappa_G(r,s')$ y la propiedad (2.5) garantiza $\mu_G(r,s) \leq \mu_G(r,s')$ entonces $\mu_G(r,s) \leq s+j+1$. Por lo tanto, $\mu_G(r,s) = s+j+1$. □

Corolario 2.8. *Si $\kappa_G(r,s) = s + \frac{r}{2}$, entonces $\mu_G(r,s) \geq \kappa_G(r,s)$.*

Teorema 2.9. *Si $r \leq 3$, entonces $\mu_G(r,s) = \kappa_G(r,s)$.*

Demostración. Esta prueba se va realizar por casos. Para $r = 1$ se tiene $\mu_G(1,s) = s$ y el teorema (2.7) garantiza $\kappa_G(1,s) = s$. Para $r = 2$ se tiene

$$s \leq \kappa_G(2,s) \leq \left(\left\lceil \frac{2}{1} \right\rceil + \left\lceil \frac{s}{1} \right\rceil - 1\right) 1 = s+1.$$

Además, $\mu_G(2,s) \geq s$. A continuación se probará que $\mu_G(2,s) \leq s+1$. Sea $x \in G \setminus \{1\}$, con $d = |x| > 1$, es decir, $\langle x \rangle = \{1, x, \ldots, x^{d-1}\}$. Por algoritmo de la división existen $q, i \in \mathbb{Z}^+$

tales que $s = qd + i$, con $0 \leq i \leq d$. Sean $y_1, y_2, \ldots, y_q \in G$ tales que $\langle x\rangle y_1, \cdots, \langle x\rangle y_q$ son disjuntas por pares y considere los siguientes subconjuntos de G:

$$A = \{1, x\} \quad \text{y} \quad B = \{1, x, \ldots, x^{i-1}\} \cup \langle x\rangle y_1 \cup \cdots \cup \langle x\rangle y_q,$$

luego $\mu_G(2, s) \leq |AB|$, observe que

$$AB = B \cup xB = B \cup \{x, x^2, \ldots, x^i\} \cup \langle x\rangle y_1 \cup \cdots \cup \langle x\rangle y_q \subseteq B \cup \{x^i\},$$

entonces, $\mu_G(2, s) \leq |B \cup \{x^i\}| \leq s + 1$. Por lo anterior $s \leq \mu_G(2, s), \kappa_G(2, s) \leq s + 1$. Si $\mu_G(2, s) = s$ ó $\mu_G(2, s) = s + 1$ el teorema (2.7) garantiza $\kappa_G(2, s) = s$ ó $\kappa_G(2, s) = s + 1$, respectivamente. Para $r = 3$ se tiene

$$s \leq \kappa_G(3, s) \leq \left(\left\lceil \frac{3}{1} \right\rceil + \left\lceil \frac{s}{1} \right\rceil - 1\right) 1 = s + 2.$$

Además, $\mu_G(3, s) \geq s$. A continuación se probará que $\mu_G(3, s) \leq s + 2$. Sea $x \in G \setminus \{1\}$, con $d = |x| > 2$, es decir, $\langle x\rangle = \{1, x, \cdots, x^{d-1}\}$. Por algoritmo de la división existen $q, i \in \mathbb{Z}^+$ tales que $s = qd + i$, con $0 \leq i \leq d$. Sean $y_1, y_2, \ldots, y_q \in G$ tales que $\langle x\rangle y_1, \cdots, \langle x\rangle y_q$ son disjuntas por pares y considere los siguientes subconjuntos de G:

$$A = \{1, x, x^2\} \quad \text{y} \quad B = \{1, x, \ldots, x^{i-1}\} \cup \langle x\rangle y_1 \cup \cdots \cup \langle x\rangle y_q.$$

luego $\mu_G(3, s) \leq |AB|$, observe que

$$AB = B \cup x^2B = B \cup \{x^2, x^3, \ldots, x^i, x^{i+1}\} \cup \langle x\rangle y_1 \cup \cdots \cup \langle x\rangle y_q \subseteq B \cup \{x^i\},$$

entonces, $\mu_G(3, s) \leq |B \cup \{x^i, x^{i+1}\}| \leq s + 2$. Por lo anterior $s \leq \mu_G(3, s), \kappa_G(3, s) \leq s + 2$. Si $\mu_G(3, s) = s$ ó $\mu_G(3, s) = s + 1$ ó $\mu_G(3, s) = s + 2$ el teorema (2.7) garantiza $\kappa_G(3, s) = s$ ó $\kappa_G(3, s) = s + 1$ ó $\kappa_G(3, s) = s + 2$, respectivamente. Ahora, si cada elemento de G es de orden menor e igual que 2, se tiene $|x| = 2$ para todo $x \in G \setminus \{1\}$, entonces G es abeliano, y por el teorema (1.67) para grupos abelianos se tiene $\mu_G(r, s) = \kappa_G(r, s)$. □

Definición 2.10. Sean G un grupo, t un entero tal que $1 \leq t \leq |G|$ y $D(t)$ el conjunto de los divisores de t, se define $\mathfrak{h}(t)$ como el máximo entero del conjunto $H(G) \cap D(t)$, es decir, $\mathfrak{h}(t) = \text{máx}\{H(G) \cap D(t)\}$.

Observe que para todo $t \in \{1, \ldots, |G| - 1\}$ se tiene $\mathfrak{h}(t) = \mathfrak{h}(|G| - t)$. Esta definición se utiliza en los resultados que se presentan a continuación.

Teorema 2.11. *Sea G un grupo finito de orden g. Si $t \in \{1, \ldots, g - 1\}$, entonces*

$$\mu_G(g - t, t) \leq g - \mathfrak{h}(t).$$

Demostración. Seleccione $t \in \{1, \dots, g-1\}$ y sea $h = \mathfrak{h}(t)$. Luego G contiene un subgrupo H de orden h y $q = \dfrac{t}{h} \in \mathbb{Z}$. Sea $p = \dfrac{g-t}{h}$, dado que el número de clases laterales módulo H en G es $\dfrac{g}{h}$ entonces

$$G = Hv_1 \dot{\cup} \cdots \dot{\cup} Hv_p \dot{\cup} Hw_1 \dot{\cup} \cdots \dot{\cup} Hw_q,$$

donde $v_1, \dots, v_p, w_1, \dots, w_q \in G$. Considere los subconjuntos

$$\begin{aligned} A =& Hv_1 \dot{\cup} \cdots \dot{\cup} Hv_p \\ B =& (G \setminus A)^{-1} = w_1^{-1} H \dot{\cup} \cdots \dot{\cup} w_q^{-1} H. \end{aligned}$$

Luego $|A| = ph = g - t$ y $|B| = qh = t$. Se probará que $AB \subseteq G \setminus H$, en efecto, sean $h_1 v_i \in A$ y $w_j^{-1} h_2 \in B$, con $h_1, h_2 \in H$. Si $(h_1 v_i)(w_j^{-1} h_2) = h \in H$, entonces $v_i w_j^{-1} = h_1^{-1} h h_2 \in H$, así $Hw_j = Hv_i$, esto es una contradicción, por lo tanto $(h_1 v_i)(w_j^{-1} h_2) \in G \setminus H$. En consecuencia $\mu_G(g-t, t) \leq |AB| \leq g - h$. □

Teorema 2.12. *Sea G un grupo finito de orden g. Si r, s son enteros positivos tales que $r + s \leq |G|$, entonces*

$$\mu_G(r, s) \leq |G| - \text{máx}\{\mathfrak{h}(s+i) : 0 \leq i \leq |G| - (r+s)\}.$$

Demostración. Para cada $i \in \{0, \dots, g-r-s\}$ se tiene $r \leq g-s-i$. Sea $t = s+i$ por el teorema 2.5 se tiene $\mu_G(r, s) \leq \mu_G(g-t, t)$, además $t = s+i \leq g-r \leq g-1$, es decir, $t \in \{1, \dots, g-1\}$ y el teorema 2.11 garantiza $\mu_G(g-t, t) \leq g - \mathfrak{h}(t)$, por lo tanto $\mu_G(r, s) \leq g - \mathfrak{h}(t)$.

□

El siguiente corolario es consecuencia de el teorema (2.12) y el lema (1.47).

Corolario 2.13. *Sea G un grupo finito. Si r, s enteros positivos tales que $r+s \leq |G|$, entonces $\mu_G(r, s) \leq |G| - 1$ y existen subconjuntos A y B de G que realizan $\mu_G(r, s)$ y satisfacen $A \cap B^{-1} = \emptyset$.*

Teorema 2.14. *Sea G un grupo finito de orden g. Si r, s son enteros tales que $1 \leq r, s \leq g$ y $\mathcal{A} = \{(x, y) \in \mathbb{Z}^2 : r \leq x \leq g, s \leq y \leq g\}$, entonces*

$$\kappa_G(r, s) = \min_{(x,y) \in \mathcal{A}} \{x + y - \mathfrak{h}(mcd(x, y))\}.$$

Demostración. Sea d el orden de un subgrupo de G tal que $\kappa_G(r, s) = \left(\left\lceil \frac{r}{d} \right\rceil + \left\lceil \frac{s}{d} \right\rceil - 1\right) d$. Para los enteros $a = \left\lceil \frac{r}{d} \right\rceil d$ y $b = \left\lceil \frac{s}{d} \right\rceil d$, se satisface $r \leq a \leq g$ y $s \leq b \leq g$, luego $\kappa_G(r, s) = a+b-d$. Además, d es un divisor de $mcd(a, b)$, por lo tanto, $d \leq \mathfrak{h}(mcd(a, b))$. Se sigue que

$$\kappa_G(r, s) \geq a + b - \mathfrak{h}(mcd(a, b)) \geq \min_{(x,y) \in \mathcal{A}} \{x + y - \mathfrak{h}(mcd(x, y))\}.$$

Para probar la otra desigualdad sea $(a,b) \in \mathcal{A}$ y $d = mcd(a,b)$ tales que

$$a + b - \mathfrak{h}(d) = \min_{(x,y)\in\mathcal{A}} \{x + y - \mathfrak{h}(mcd(x,y))\}.$$

Dado que $d \mid a$ y $d \mid b$ se tiene $\left\lceil \frac{r}{d} \right\rceil d \leq a$ y $\left\lceil \frac{s}{d} \right\rceil d \leq b$, entonces

$$\kappa_G(r,s) \leq \left(\left\lceil \frac{r}{d} \right\rceil + \left\lceil \frac{s}{d} \right\rceil - 1 \right) d \leq a + b - d.$$

□

El siguiente corolario es una consecuencia inmediata de el teorema (2.14).

Corolario 2.15. *Si $1 \leq r, s \leq g-1$, entonces*

$$\kappa_G(r,s) = \min\{r + s - \mathfrak{h}(mcd(r,s)), \kappa_G(r+1,s), \kappa_G(r,s+1)\}.$$

Teorema 2.16. *Si G es un grupo finito, se satisfacen los siguientes enunciados.*

1. *Si r, s son enteros tales que $r + s = |G|$, entonces $\kappa_G(r,s) = |G| - \mathfrak{h}(r) = |G| - \mathfrak{h}(s)$.*
2. *Si r, s son enteros tales que $r + s = |G| - 1$, entonces $\kappa_G(r,s) = |G| - \max\{2, \mathfrak{h}(r), \mathfrak{h}(s)\}$, o equivalente, $\kappa_G(|G| - s - 1, s) = |G| - \max\{2, \mathfrak{h}(s), \mathfrak{h}(s+1)\}$.*

Demostración.

1. Por el corolario 2.15 se tiene

   $$\kappa_G(r,s) = \min\{|G| - \mathfrak{h}(mcd(r,s)), \kappa_G(r+1,s), \kappa_G(r,s+1)\}.$$

   Dado que $r + s + 1 > |G|$ la propiedad (2.6) garantiza

   $$\kappa_G(r+1,s) = \kappa_G(r,s+1) = |G|,$$

   así que $\min\{|G| - \mathfrak{h}(mcd(r,s)), |G|\} = |G| - \mathfrak{h}(mcd(r,s))$. Además por hipótesis $r + s = |G|$ entonces $\mathfrak{h}(r) \mid s$, luego $\mathfrak{h}(r) \in \{H(G) \cup D(s)\}$, por ello $\mathfrak{h}(r) \leq \mathfrak{h}(s)$, de manera similar se tiene que $\mathfrak{h}(r) \geq \mathfrak{h}(s)$, por lo tanto $\mathfrak{h}(r) = \mathfrak{h}(s)$. Dado que $\mathfrak{h}(mcd(r,s)) = \max\{H(G) \cup D(mcd(r,s))\}$ se tiene $\mathfrak{h}(mcd(r,s)) = \mathfrak{h}(r)$. Por tanto $\kappa_G(r,s) = |G| - \mathfrak{h}(r) = |G| - \mathfrak{h}(s)$.

2. Por el corolario 2.15 se tiene

   $$\kappa_G(r,s) = \min\{|G| - \mathfrak{h}(mcd(r,s)), \kappa_G(r+1,s), \kappa_G(r,s+1)\}.$$

Dado que $r+s+1=|G|$, se aplica el item anterior y se tiene
$\kappa_G(r+1,s)=\kappa_G(r,s+1)=|G|-h(r)=|G|-h(s)$, así

$$\begin{aligned}\kappa_G(r,s)=&\min\{|G|-1-\mathfrak{h}(mcd(r,s)),|G|-h(r),|G|-h(s)\}\\ =&|G|-\max\{1+\mathfrak{h}(mcd(r,s)),h(r),h(s)\}.\end{aligned}$$

De la definición de $\mathfrak{h}$ se tiene

$$\mathfrak{h}(mcd(r,s))=\mathfrak{h}((mcd(r,s,|G|))=\mathfrak{h}(mcd(r,r+s,|G|)).$$

Por tanto, $\mathfrak{h}(mcd(r,s))=\mathfrak{h}(1)=1$, entonces $1+\mathfrak{h}(mcd(r,s))=2$, en consecuencia $\kappa_G(r,s)=|G|-\min\{2,h(r),h(s)\}$. La última parte del segundo enunciado se deriva del hecho que $\mathfrak{h}(r)=\mathfrak{h}(|G|-r)$ y dado que $r+s=|G|-1$, entonces $\mathfrak{h}(r)=\mathfrak{h}(s+1)$.

□

Teorema 2.17. *Sean r y s enteros positivos. Si $r+s=|G|-1$, entonces $\mu_G(r,s)\leq\kappa_G(r,s)$.*

Demostración. De el teorema (2.16) se tiene $\kappa_G(r,s)=|G|-\max\{2,\mathfrak{h}(r),\mathfrak{h}(s)\}$. Dado que $\mathfrak{h}(r)=\mathfrak{h}(|G|-r)$ y por hipótesis $s+1=|G|-r$ entonces

$$\kappa_G(r,s)=|G|-\max\{2,\mathfrak{h}(s),\mathfrak{h}(s+1)\}.$$

Sea $p=\max\{\mathfrak{h}(s),\mathfrak{h}(s+1)\}$, el teorema (2.12) afirma que $\mu_G(r,s)\leq|G|-p$. Si $p\geq 2$, entonces $\mu_G(r,s)\leq\kappa_G(r,s)$. De lo contrario, $p=1$, es decir, $\mathfrak{h}(s)=\mathfrak{h}(s+1)=1$. En este caso $\kappa_G(r,s)=|G|-2$. Para probar que $\mu_G(r,s)\leq|G|-2$ escoja un elemento $x\in G\setminus\{1\}$ de orden $d\geq 2$. Como $h(s)=1$ se sigue que $d\nmid s$ y por el algoritmo de la división existen enteros positivos q,i, tales que $s=dq+i$ con $i<d$. Sean $y_1,\ldots,y_q\in G$ tales que las clases $\langle x\rangle y_1,\langle x\rangle y_2,\ldots,\langle x\rangle y_q$ son disjuntas por pares y considere los siguientes subconjuntos de G:

$$V=\{1,x,\ldots,x^{i-1}\}\cup\left(\bigcup_{j=1}^{q}\langle x\rangle y_j\right)\qquad\text{y}\qquad U=V\cup\{x^i\}.$$

Luego $|V|=s$, $|U|=s+1$, además $1,x$ son elementos del conjunto transportador $U:V$ definido en (1.46). Por lo tanto, $|U:V|\geq 2$. Considere los conjuntos $A=G\setminus U$ y $B=V^{-1}$, entonces $|A|=|G|-s-1=r$, $|B|=s$ y por lema (1.47) se tiene $G\setminus(AB)=U:V$, así $|G\setminus(AB)|\geq 2$, es decir, $|AB|\leq|G|-2$. Por tanto $\mu_G(r,s)\leq|AB|\leq|G|-2=\kappa_G(r,s)$. □

Teorema 2.18. *Si r,s son enteros tales que $r+s=|G|$, entonces*

$$\mu_G(r,s)=\kappa_G(r,s)=|G|-\mathfrak{h}(r)=|G|-\mathfrak{h}(s).$$

Demostración. Sean $A, B \subseteq G$, por lema (1.47), se tiene $G \setminus (AB) = (G \setminus A) : B^{-1}$. Tomando $B = (G \setminus A)^{-1}$ se sigue que $G \setminus (AB) = B^{-1}) : B^{-1}$. Por el teorema (1.49), $|B^{-1} : B^{-1}|$ es un divisor de $|B^{-1}|$. Ahora sean $A, B \subseteq G$ que realizan $\mu_G(r, s)$ y tales que $A \cap B^{-1} = \emptyset$ ver corolario (2.13), con estas condiciones $B^{-1} : B^{-1}$ es un subgrupo de G cuyo orden divide $|B^{-1}| = s$. Luego $|B^{-1} : B^{-1}| \leq \mathfrak{h}(s)$. Además $|B^{-1} : B^{-1}| = |G \setminus (AB)| = |G| - |AB|$, entonces

$$|AB| = |G| - |B^{-1} : B^{-1}| \geq |G| - \mathfrak{h}(s)$$

Por otro lado de el teorema (2.12), se tiene $\mu_G(r, s) \leq |G| - \mathfrak{h}(s)$. Además $\mathfrak{h}(r) = \mathfrak{h}(s)$. Por tanto $\mu_G(r, s) = \kappa_G(r, s)$.

□

En la sección anterior se expusieron las propiedades que satisfacen las funciones $\mu_G(r, s)$ y $\kappa_G(r, s)$ en un grupo finito y se pudo observar que bajo ciertas condiciones se tiene la igualdad $\mu_G(r, s) = \kappa_G(r, s)$, sin embargo, en general no se tiene una expresión para la función $\mu_G(r, s)$ para grupos no abelianos. Eliahou, Kervaire, Mutis, Castillo y Benavides lograron probar que la fórmula obtenida para la función $\mu_G(r, s)$ en grupos abelianos se puede extender para algunas clases de grupos no abelianos finitos. En la siguiente sección se presentan estos resultados.

2.1.1. Función μ_G en grupos diédricos

A continuación se enuncian, sin demostración, algunos de los teoremas demostrados por Eliahou y Kervaire y otros autores. En 2006 Eliahou y Kervaire [15] estudian la función μ_G para $G = D_n$, el grupo diédrico de orden $2n$ y lograron extender el resultado que se obtuvo para grupos abelianos la clase de grupos diédricos, esto puede ver en los siguientes teoremas.
En 2006 Eliahou y Kervaire [15] demostraron.

Teorema 2.19. ***(Eliahou y Kervaire)***
Sean p un número primo, m un entero positivo y D_n el grupo diédrico de orden $2p^m$. Si r y s son dos enteros tales que $1 \leq r, s \leq 2p^m$, entonces $\mu_{D_n}(r, s) = \kappa_{D_n}(r, s)$.

Luego en 2010 Eliahou y Kervaire [6] lograron demostrar la igualdad para cualquier grupo diédrico, el resultado se puede ver en el siguiente teorema.

Teorema 2.20. *Sea G el grupo diédrico D_n de orden $2n$, se tiene $\mu_{D_n}(r, s) = \kappa_{D_n}(r, s)$, para $n > 1$ y enteros positivos $r, s \leq 2n$.*

Ejemplo. En el grupo de simetrías del cuadrado $D_4 = \{H, V, D_1, D_2, R_0, R_{90}, R_{180}, R_{270}\}$, el conjunto $H(G) = \{1, 3, 4, 12\}$ y tomando $r = 4$ y $s = 3$, se tiene que $\mu_{D_4}(4, 3) = \kappa_{D_4}(4, 3) = 4$.

2.1.2. Función μ_G en grupos $p-grupos$

En 2010 Mutis, Castillo y Benavides [7] en la clase de $p-grupos$ probaron el siguiente resultado.

Teorema 2.21. *Sea p un número primo y sea G un $p-$grupo finito. Si r, s son dos enteros tales que $1 \leq r, s \leq |G|$, entonces $\mu_G(r,s) = \kappa_G(r,s)$.*

Ejemplo. En el grupo de Klein $V = \{1, a, b, ab\}$, el conjunto $H(G) = \{1, 3, 4, 12\}$ y tomando $r = 3$ y $s = 3$, se tiene que $\mu_V(3,3) = \kappa_V(3,3) = 4$.

2.1.3. Función μ_G en grupos hamiltonianos

En 2012 para la clase de grupos hamiltonianos Mutis, Castillo y Benavides [8] también mostraron el siguiente teorema.

Teorema 2.22. *Sea n un entero no negativo. Si H es un grupo hamiltoniano de orden 2^{n+3}, entonces para todo par de enteros r, s tales que $1 \leq r, s \leq 2^{n+3}$ se tiene $\mu_H(r,s) = \kappa_H(r,s)$.*

Ejemplo. En el grupo de los Cuaterniones $\mathcal{Q} = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}$, el conjunto $H(G) = \{1, 2, 4, 8\}$ y tomando $r = 2$ y $s = 5$, se tiene que $\mu_{\mathcal{Q}}(2,5) = \kappa_{\mathcal{Q}}(2,5) = 6$.

2.1.4. Función μ_G en grupos solubles

Para grupos solubles finitos en general no se tiene una fórmula para la función μ_G. Eliahou y Kervaire en (2006), (2006) y (2007) [15], [16] y [12] lograron acotar superior e inferiormente esta función. En lo que sigue se presentan los teoremas que dan las cotas para la función μ_G en un grupo soluble finito G.

Teorema 2.23. *Si r y s son enteros tales que $r, s \leq |G|$, entonces $\mu_G(r,s) \leq r + s - 1$.*

Lema 2.24. *Si r y s son enteros tales que $r, s \leq |G|$ y k es el orden de un subgrupo normal de G, entonces*

$$\mu_G(r,s) \leq \left(\left\lceil \frac{r}{k} \right\rceil + \left\lceil \frac{s}{k} \right\rceil - 1 \right) k.$$

Corolario 2.25. *Si r y s son enteros tales que $\kappa_G(r,s) = \left(\left\lceil \frac{r}{h} \right\rceil + \left\lceil \frac{s}{h} \right\rceil - 1 \right) h$ donde h es el orden de un subgrupo normal de G, entonces $\mu_G(r,s) \leq \kappa_G(r,s)$.*

Teorema 2.26. *Si $1 \leq r, s \leq |G|$, entonces $D_{\kappa_G}(r,s) \leq \mu_G(r,s) \leq N_{k_G}(r,s)$.*

Ejemplo. En el grupo simétrico S_4 de 24 elementos, el conjunto $D(G) = H(G) = \{1, 2, 3, 4, 6, 8, 12, 24\}$, $N(G) = \{1, 4, 12, 24\}$ y tomando $r = 4$ y $s = 5$, se tiene que

$$6 = D_{\kappa_{S_4}}(4,5) \leq \mu_{S_4}(4,5) \leq N_{\kappa_{S_4}}(4,5) = 8.$$

Además $\kappa_G(4,5) = 6$.

En este capítulo se presentó los resultados que se conocen del problema de los conjuntos producto pequeños en algunos grupos no abelianos finitos. En el siguiente capítulo se muestra el estudio de este problema en grupos no abelianos de orden pq.

Capítulo 3

La función μ_G en grupos no abelianos de orden pq

En el capítulo anterior se presentaron los resultados del problema de los conjuntos producto pequeños en grupos solubles, hamiltonianos, $p-grupos$ y diédricos. En este capítulo se presenta el estudio para grupos no abelianos de orden pq, en particular el resultado que probó en 2009 Deckelbaum [5] para un grupo de orden $3p$, cuando $r, s > 3$ y $\left\lceil \frac{r}{3} \right\rceil + \left\lceil \frac{s}{3} \right\rceil < p$, entonces $\mu_G(r,s) = N_{K_G}(r,s)$, de lo contrario $\mu_G(r,s) = \kappa_G(r,s)$. En primer lugar se presenta detalladamente los grupos no abelianos de orden pq, luego algunos resultados previos necesarios para el estudio y finalmente los resultados obtenidos para la función μ_G en grupos no abelianos de orden pq.

3.1. Grupos no abelianos de orden pq

En seguida se presenta algunos teoremas relevantes de los grupos no abelianos de orden pq, donde p y q primos impares distintos. Las demostraciones utilizan resultados de la teoría de Sylow que se presentaron en los preliminares.

Teorema 3.1. *Todo grupo G de orden pq, con $p > q$ tiene un único subgrupo de orden p y es normal en G.*

Demostración. Por teorema de Sylow (1.57) se tiene que $N_p \equiv 1(\text{mód } p)$ y N_p divide $|G|$, dado que $|G| = pq$ y p, pq son nulos módulo p entonces $N_p \in \{1, q\}$. Además $q \not\equiv 1(\text{mód } p)$ porque $p > q$, necesariamente $N_p = 1$. Sea N el único p-subgrupo de Sylow en G, por teorema (1.58) N es normal en G. □

Teorema 3.2. ***(Caracterización de grupos de orden pq)***
Si G es un grupo de orden pq, donde p y q primos impares y $p > q$, entonces $G \cong \mathbb{Z}_{pq}$ ó G es no abeliano y se tiene que

$$G = \langle x, y : x^q = y^p = 1, xyx^{-1} = y^n \rangle,$$

donde n es un número entero fijo tal que $n \not\equiv 1 (mód\ p)$, $n^q \equiv 1 (mód\ p)$ y $p \equiv 1 (mód\ q)$.

Demostración. Dado que $|G| = pq$, por teorema de Cauchy (1.50) existen $x, y \in G$ tal que $H = \langle x \rangle$ es de orden q y $N = \langle y \rangle$ es de orden p. Por teorema (3.1) $N \trianglelefteq G$ y por teorema de Sylow (1.57) $N_q \equiv 1 (\text{mód } q)$ y N_p es divisor de $|G|$, entonces $N_q = 1$ ó $N_q = p$. Para $N_q = 1$, el único subgrupo de Sylow de orden q de G es H y $H \trianglelefteq G$, luego $yxy^{-1}x^{-1} \in H \cap N = \{1\}$, entonces $yx = xy$, por tanto $G \cong \langle x \rangle \times \langle y \rangle = H \times N \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$. Para $N_q = p$ por teorema (1.57) se tiene $p \equiv 1 (\text{mód } q)$ y G tiene p subgrupos de Sylow de orden q, observe que G debe ser no abeliano porque en caso contrario H es un $p - subgrupo$ de Sylow normal en G, esto contradice el teorema (1.58). Dado que $N \trianglelefteq G$, existe un único entero n tal que $1 < n < p$ y $xyx^{-1} = y^n$. Observe que $n \equiv 1 (\text{mód } p)$ implica $xyx^{-1} = y$, es decir $xy = yx$, así G sería abeliano, lo que es una contradicción, así que, $n \not\equiv 1 (\text{mód } p)$. Ahora se probará que $n^q \equiv 1 (\text{mód } p)$, observe que

$$y^{n^2} = (y^n)^n = (xyx^{-1})^n = xy^n x^{-1} = x(xyx^{-1})x^{-1} = x^2 y x^{-2},$$

y se puede mostrar por inducción que

$$x^j y x^{-j} = y^{n^j}, \text{ para todo } j \geq 0 \tag{3.1}$$

En particular, para $j = q$ se obtiene $y = y^{n^q}$, o equivalente $x^{n^q - 1} = 1$ en $\mathbb{Z}_p$, luego $n^q - 1$ es un múltiplo de p, esto es, $n^q \equiv 1 (\text{mód } p)$. Sea $W = \langle x, y \rangle$ el subgrupo de G generado por $\{x, y\}$ y sea $w \in W$, entonces $w^{-1} = x^{r_1} y^{l_1} \cdots x^{r_m} y^{l_m}$, con $0 \leq r_i \leq q - 1$, $0 \leq l_i \leq p - 1$, y $0 \leq i \leq m$. Considere el producto $x^r y^l$ con $0 \leq l \leq p - 1$, $0 \leq r \leq q - 1$. De la ecuación (3.1) se tiene $x^r y^l = y^{ln^r} x^r$. De esta relación se obtiene que w^{-1} se puede expresar como $w^{-1} = y^l x^r$, luego cada elemento $w \in G$ tiene la forma $w = x^k y^t$, con $0 \leq kq - 1$ y $0 \leq t \leq p - 1$. Ahora suponga que $x^r y^l = x^s y^m$, donde $0 \leq r, s \leq q - 1$ y $0 \leq l, m \leq p - 1$, entonces $y^{m-l} = x^{r-s} \in \langle x \rangle \cap \langle y \rangle$, luego $\left| y^{m-l} \right|$ es un divisor común de p y q, entonces $y^{m-l} = 1$. Por la condición de m y l se tiene $|m - l| \leq p - 1$, así $m = l$. Análogamente $r = s$, por lo tanto $|W| = pq$, es decir, $G = W$. □

Aunque es posible que haya más de una elección para n, se puede probar que todos los grupos no abelianos de orden pq se construyen de forma semejante al grupo W del teorema anterior y por lo tanto son isomorfos.

Teorema 3.3. *Si p y q son primos distintos con $p > q$, entonces todo grupo G de orden pq es soluble.*

Demostración. Sea N el único subgrupo de G de orden p y considere la cadena $\{1\} \trianglerighteq N \trianglerighteq G$, dado que G/N tiene orden q es cíclico, es decir, el grupo cociente G/N es abeliano, por tal razón G es soluble.

□

3.2. Resultados previos

Para hacer un estudio de la función μ_G en grupos no abelianos de orden pq se utilizan los siguientes teoremas que proporcionan cotas para la función $\mu_G(r, s)$.

Teorema 3.4. ***(Zemor (1994) [18])***
Sean G un grupo finito y A un subconjunto de G. Si para todo subgrupo propio H de G se cumple $|AH| \geq |A| + |H| - 1$ y $|HA| \geq |A| + |H| - 1$, entonces para todo $B \subseteq G$ para el cual el cual se satisfaga $AB \neq G$ o $BA \neq G$, entonces se tiene

$$|AB| \geq |A| + |B| - 1 \text{ y } |BA| \geq |A| + |B| - 1.$$

Teorema 3.5. ***(Kemperman (1956) [14])***
Sea $C = AB$ el producto de dos subconjuntos finitos de un grupo G. Si existe un elemento $c \in C$ tal que $c = ab$ para un único $a \in A$ y un único $b \in B$, entonces $|C| \geq |A| + |B| - 1$.

Teorema 3.6. ***(Vosper (1956) [19])***
Sea p un numero primo y sean A y B subconjuntos de $\mathbb{Z}_p$ tales que $|A| \geq 2$, $|B| \geq 2$ y $|A| + |B| < p$. Si $|A + B| = |A| + |B| - 1$, entonces A y B son progresiones aritméticas con la misma diferencia común.

Teorema 3.7. *Sea p un número primo y sea B un subconjunto de $\mathbb{Z}_p$. Si n es un entero talque $n \equiv 1 (mód\ p)$ y $nB = \{nb : b \in B\}$ es una progresión aritmética en $\mathbb{Z}$, entonces B es una progresión aritmética en $\mathbb{Z}_p$.*

Demostración. Sea $k = |B|$ y d la diferencia común de la progresión aritmética nB, luego existe $a \in \mathbb{Z}$ tal que $nB = \{a, a + d, \ldots, a + (k - 1)d\}$, además para cada $a + jd \in nB$ existe un único $b_j \in B$ tal que $a + jd \equiv nb_j (\text{mód } p)$, entonces $B = \{b_0, b_1, \ldots, b_{k-1}\}$. Dado que $n \equiv 1 (\text{mód } p)$ para todo $j = 1, \ldots, k - 1$ se tiene

$$d = (a + jd) - (a + (j - 1)d) \equiv n(b_j - b_{j-1}) (\text{mód } p) \equiv b_j - b_{j-1} (\text{mód } p).$$

Por lo tanto B es una progresión aritmética en $\mathbb{Z}_p$. □

Corolario 3.8. *Sea p un número primo y sea B un subconjunto no vacío de $\mathbb{Z}_p$. Si n es un entero tal que $n^i \equiv 1(\text{mód } p)$, para algún $i \in \mathbb{Z}^+$ y $nB = \{nb : b \in B\}$ es una es una progresión aritmética en $\mathbb{Z}$., entonces B es una progresión aritmética en $\mathbb{Z}_p$.*

Demostración. Sea d la diferencia común de la progresión aritmética nB, entonces n^iB es una progresión aritmética de diferencia común $n^{i-1}d$ y por el teorema anterior (3.7) B es una progresión aritmética en $\mathbb{Z}_p$. □

Teorema 3.9. *Sea p un primo impar y $S \subset \mathbb{Z}_p$ con $2 \leq |S| \leq p-2$. Si S es una progresión aritmética de diferencia d entonces la congruencia $s \equiv t + d(\text{mód } p)$ tiene exactamente una solución con $s \in S$ y $t \notin S$.*

Demostración. Sea d la diferencia común de la progresión aritmética S de cardinal n. Dado que $n \geq 2$ se debe tener $0 < d < p$, luego $S = \{s_0\} + \{0, d, 2d, \ldots, (n-1)d\}$ para algún $s_0 \in \mathbb{Z}_p$. Para mostrar la existencia considere los elementos $s_0 \in S$ y $t = s_0 + (p-1)d$ que satisfacen la congruencia $s \equiv t + d(\text{mód } p)$. Si $t \in S$, entonces $t = s_0 + jd$, para algún $0 < j \leq n-1$, entonces $s_0 + jd = s_0 + (p-1)d(\text{mód } p)$, pero $p \nmid d$ y p es primo, luego $j+1 \equiv 0(\text{mód } p)$. Dado que $0 < j \leq n-1$ se sigue $1 < j+1 \leq n < p-1$, esto contradice que $p \mid j+1$, por lo tanto $t \notin S$. Ahora se desea probar que la solución es única, suponga que existen $s' \in S$ y $t' \notin S$ que satisfacen $s' \equiv t' + d(\text{mód } p)$. Observe que $\mathbb{Z}_p = \{s_0, s_0+d, \cdots, s_0+(n-1)d, \cdots, s_0+(p-1)d\}$ porque $mcd(p, d) = 1$, entonces $s' = s_0 + jd$ para algún $0 \leq j \leq n-1$ y $t' = s_0 + kd$ para algún $n \leq k \leq p-1$. Sustituyendo se tiene $s_0 + jd \equiv s_0 + kd + d(\text{mód } p)$, esto significa $p \mid (k+1-j)d$, entonces p divide $k+1-j$. De las desigualdades $-n+1 \leq -j \leq 0$ y $n+1 \leq k+1 \leq p$ se sigue $2 \leq k+1-j \leq p$ y dado que p es primo impar, la única posibilidad para $p \mid k+1-j$ es que $p = k+1-j$, además $k+1 \leq p$ de esto se sigue que $p - j \leq p$, por lo tanto $j = 0$ y $k = p-1$, es decir, $s = s'$ y $t = t'$. □

Lema 3.10. *Sea p un primo impar y S una progresión aritmética de diferencia d en $\mathbb{Z}_p$. Si $2 \leq |S| \leq p-2$, entonces cualquier permutación de los elementos de S que genere una progresión aritmética debe tener diferencia común $\pm d$ módulo p.*

Demostración. Sea S una progresión aritmética de diferencia d en $\mathbb{Z}_p$ de cardinal n, y suponga que una permutación de los elementos de S genera una progresión aritmética de diferencia l. Sea $R = \mathbb{Z}_p \setminus S$ y sean $s \in S$ y $t \in R$ los únicos elementos en $\mathbb{Z}_p$ tales que $s \equiv t + d(\text{mód } p)$, entonces se satisfacen las congruencias $(s+l) \equiv (t+l) + d(\text{mód } p)$ y $(s-l) \equiv (t-l) + d(\text{mód } p)$, debido a la unicidad de la pareja $(s, t) \in S \times R$, se debe tener $(s+l, t+l) \notin S \times R$ y $(s-l, t-l) \notin S \times R$ y se tiene las siguientes posibilidades.

1. $s + l \notin S$ y $s - l \notin S$. Dado que $s \in S$, entonces $n = 1$ pero esto no es posible porque $2 \leq n$.

2. $t+l \in S$ y $t-l \in S$. Dado que $t \in R$, entonces $S = \{t+l, \ldots, t+(p-1)l\}$, así $n = p-1$, esto no es posible porque $n \leq p-2$.

3. $s+l \notin S$ y $t-l \in S$. Dado que $s \in S$ y $s+l \notin S$, entonces $s-l \in S$, así que $S = \{s-kl : 0 \leq k \leq n-1\}$, además $t-l \in S$ luego $t-l = s-kl$ para algún k, entonces $t = s-(k-1)l \notin S$, pero $-1 \leq k-1 \leq n-2$, así la única posibilidad es $k = 0$, es decir, $t = s+l$. Esto junto a la congruencia $s \equiv t+d(\text{mód } p)$ implica $l \equiv -d(\text{mód } p)$.

4. $t+l \in S$ y $s-l \notin S$, entonces $s+l \in S$, así $S = \{s+kl : 0 \leq k \leq n-1\}$, además $t+l \in S$ luego $t+l = s+kl$ para algún k, entonces $t = s+(k-1)l \notin S$, pero $-1 \leq k-1 \leq n-2$, así la única posibilidad es $k = 0$, es decir, $t = s-l$. Esto junto a la congruencia $s \equiv t+d(\text{mód } p)$ implica $l \equiv d(\text{mód } p)$.

Por tanto $l \equiv \pm d(\text{mód } p)$. □

Lema 3.11. *Sean p, q primos impares, $A_0, A_1, \ldots, A_{q-1}$ y B subconjuntos de $\mathbb{Z}_p$. Si se satisfacen las siguientes condiciones.*

1. $|A_0| + |A_1| + \cdots + |A_{q-1}| = u > q$ *y* $u \not\equiv 1(\text{mód } q)$
2. $|B| = v > 1$ *y* $\left\lceil \frac{u}{q} \right\rceil + v < p$
3. $n \not\equiv 1(\text{mód } p)$ *y* $n^q \equiv 1(\text{mód } p)$,

entonces denotando $D = (A_0 + B) \cup (A_1 + nB) \cup (A_2 + n^2B) \cup \cdots \cup (A_{q-1} + n^{q-1}B)$, se tiene $|D| \geq \left\lceil \frac{u}{q} \right\rceil + v$.

Demostración. El resultado es inmediato cuando $D = \mathbb{Z}_p$. Así que se puede suponer $D \neq \mathbb{Z}_p$, en este caso el lema se obtendrá como consecuencia de las siguientes afirmaciones.

Afirmación 3.12. Si A_i es un subconjunto de cardinalidad maximal, entonces $|A_i| \geq \left\lceil \frac{u}{q} \right\rceil$.

En efecto, se tiene $|A_i + n^iB| \leq |D| < p$. Suponga que $|A_i| < \left\lceil \frac{u}{q} \right\rceil$, entonces $|A_j| \leq \left\lceil \frac{u}{q} \right\rceil - 1$ para todo $j = 0, \ldots, q-1$, luego $u = \sum_{j=0}^{q-1} |A_j| \leq q\left(\left\lceil \frac{u}{q} \right\rceil - 1\right)$. Observe que no es posible tener $q \mid u$ porque $u \leq q\left\lceil \frac{u}{q} \right\rceil - q = u - q$, lo que es una contradicción, así que existen enteros positivos t, r tales que $u = tq + r$ con $r \leq q-1$, entonces $\left\lceil \frac{u}{q} \right\rceil = \left\lceil t + \frac{r}{q} \right\rceil = t+1$, luego

$$u \leq q\left\lceil \frac{u}{q} \right\rceil - q = q(t+1) - q = qt < u,$$

esto es una contradicción, por lo tanto $|A_i| \geq \left\lceil \frac{u}{q} \right\rceil$.

Afirmación 3.13. Si A_i es de cardinalidad maximal, $|A_i| = \left\lceil \frac{u}{q} \right\rceil$ y $|A_i + n^i B| = \left\lceil \frac{u}{q} \right\rceil + v - 1$, entonces A_i, $n^i B$ y $A_i + n^i B$ son progresiones aritméticas de la misma diferencia común.

Por hipótesis del lema $\sum_{j=}^{q-1} |A_j| = u > q$, entonces $|A_i| \geq 2$, también $|n^i B| = v \geq 2$, luego se satisfacen las hipótesis del teorema de Vosper (3.6), por lo tanto A_i y $n^i B$ son progresiones aritméticas con la misma diferencia común. Por el corolario (3.8) B es una progresión aritmética. Sean d la diferencia común de B y $b_0 \in \mathbb{Z}_p$ tales que $B = \{b_0 + kd : 0 \leq k \leq v\}$, luego $S = \{n^i b_0 + k(n^i d) : 0 \leq k \leq v\}$ es una progresión aritmética de diferencia común $n^i d$ y $n^i B$ debe ser una permutación de los elementos de S. Dado que $2 \leq v \leq p-2$, el lema (3.10) garantiza que $n^i B$, e igualmente A_i, deben ser progresiones aritméticas de diferencia común $t \equiv \pm n^i d (\text{mód } p)$. Entonces, existen $a, b \in \mathbb{Z}_p$ tales que

$$A_i = \left\{ a + jt : 0 \leq j \leq \left\lceil \frac{u}{q} \right\rceil - 1 \right\}, n^i B = \{b + jt : 0 \leq j \leq v - 1\}.$$

Observe que $A_i + n^i B = \left\{ a + b + jt : 0 \leq j \leq \left\lceil \frac{u}{q} \right\rceil + v - 1 \right\}$, también es una progresión aritmética de $\mathbb{Z}_p$. Por tanto, A_i, $n^i B$ y $A_i + n^i B$ son progresiones aritméticas de la misma diferencia común $\pm n^i d (\text{mód } p)$.

Afirmación 3.14. Si A_i es de cardinalidad maximal y $|A_i| = \left\lceil \frac{u}{q} \right\rceil$, entonces existe $j \neq i$ tal que $|A_j| = |A_i|$. Además, $n^i d \not\equiv n^j d (\text{mód } p)$.

Suponga lo contrario, entonces $|A_j| \leq \left\lceil \frac{u}{q} \right\rceil - 1$ para todo $j \neq i$, y se tiene

$$\sum_{\substack{j=0 \\ j \neq i}}^{q-1} |A_j| \leq (q-1) \left(\left\lceil \frac{u}{q} \right\rceil - 1 \right),$$

pero $\sum_{\substack{j=0 \\ j \neq i}}^{q-1} |A_j| = u - \left\lceil \frac{u}{q} \right\rceil$, entonces $u \leq q \left\lceil \frac{u}{q} \right\rceil - (q-1)$, y esta desigualdad solo es posible cuando q no divide a u, entonces existen enteros positivos t, r tales que $\left\lceil \frac{u}{q} \right\rceil = \left\lceil t + \frac{r}{q} \right\rceil = t+1$ y se sigue

$$u \leq q \left\lceil \frac{u}{q} \right\rceil - (q-1) = q(t+1) - q + 1 = qt + 1 \leq u - r + 1.$$

Así $r = 1$, esto implica $u = tq + 1 \equiv 1 (\text{mód } q)$, pero esto contradice el hecho que $u \not\equiv 1 (\text{mód } q)$, por lo tanto se puede encontrar A_j con $j \neq i$ y $|A_j| = |A_i| = \left\lceil \frac{u}{q} \right\rceil$. Resta probar que

$n^i d \not\equiv n^j d(\text{mód } p)$, para esto suponga $n^i d \equiv n^j d(\text{mód } p)$, es decir, $p|d(n^i - n^j)$. Si $p|d$, entonces para todo $a \in \mathbb{Z}_p$ se tiene $a + d = a$, y dado que A_i es progresión aritmética en $\mathbb{Z}_p$ se sigue

$$|A_i| = |\{a_0 + n^i d, \ldots, a_0 + kn^i d\}| = |\{a_0\}| = 1,$$

esto contradice que $|A_i| = \left\lceil \frac{u}{q} \right\rceil \geq 2$, en consecuencia $p \mid (n^i - n^j)$. Sin pérdida de generalidad suponga $i > j$, entonces $p \mid n^j(n^{i-j} - 1)$. Dado que $n^q \equiv 1(\text{mód } p)$, se debe tener $p \mid (n^{i-j} - 1)$, es decir, $n^{i-j} \equiv 1(\text{mód } p)$, con $0 < i - j < q$. Luego, en el grupo multiplicativo $\mathbb{Z}_p^*$, se tiene que el orden de n divide a q y es menor que q, entonces $n = 1$ en $\mathbb{Z}_p$, esto contradice el hecho que $n \not\equiv 1(\text{mód } p)$, por tanto $n^i d \not\equiv n^j d(\text{mód } p)$.
Reanudando la prueba del lema (3.11). Sea A_i un subconjunto de cardinalidad maximal, por la afirmación (3.12) se tiene $|A_i| \geq \left\lceil \frac{u}{q} \right\rceil$. Si $|A_i| > \left\lceil \frac{u}{q} \right\rceil$, entonces $|A_i| \geq \left\lceil \frac{u}{q} \right\rceil + 1$, y por teorema de Cauchy-Davenport (1.65) se sigue

$$|A_i + n^i B| \geq |A_i| + |n^i B| - 1 \geq \left\lceil \frac{u}{q} \right\rceil + v,$$

entonces $|D| \geq \left\lceil \frac{u}{q} \right\rceil + v$, y se satisface el resultado del lema. Luego se puede suponer que $|A_i| = \left\lceil \frac{u}{q} \right\rceil$, por el teorema de Cauchy-Davenport se sigue

$$|A_i + n^i B| \geq \left\lceil \frac{u}{q} \right\rceil + v - 1,$$

para el caso que $|A_i + n^i B| > \left\lceil \frac{u}{q} \right\rceil + v - 1$ el enunciado del lema se cumple y se puede considerar $|A_i + n^i B| = \left\lceil \frac{u}{q} \right\rceil + v - 1$. Por la afirmación (3.14) existe $j \neq i$ tal que $|A_j| = |A_i|$ y $n^i d \not\equiv n^j d(\text{mód } p)$ y por la afirmación (3.13) se tiene que $A_i + n^i B$ es progresión aritmética de diferencia común $n^i d$ y $A_j + n^j B$ es progresión aritmética de diferencia común $n^j d$, donde d es la diferencia común de la progresión aritmética B. Además, por hipótesis $\left\lceil \frac{u}{q} \right\rceil + v < p$, entonces $2 \leq \left\lceil \frac{u}{q} \right\rceil + v - 1 \leq p - 2$, aplicando el lema (3.10) se concluye que $A_i + n^i B \neq A_j + n^j B$. Dado que $|A_i + n^i B| = |A_j + n^j B| = \left\lceil \frac{u}{q} \right\rceil + v - 1$, se tiene

$$|(A_i + n^i B) \cup (A_j + n^j B)| \geq \left\lceil \frac{u}{q} \right\rceil + v.$$

Por lo tanto $|D| \geq \left\lceil \frac{u}{q} \right\rceil + v$.

□

En lo que sigue G es un grupo no abeliano de orden pq, donde p, q son primos impares con $p > q$, $H = \langle x \rangle$ denotará un subgrupo de G de orden q, $N = \langle y \rangle$ será el único p-subgrupo de Sylow de G de orden p y se usará n para el entero en la definición de G tal que $n \not\equiv 1(\text{mód } p)$, $n^q \equiv 1(\text{mód } p)$, y $xyx^{-1} = y^n$.

Lema 3.15. *Sean A y B subconjuntos no vacíos de G de cardinales r y s, respectivamente. Si $|AN| \leq |A| + |N| - 2$ y $|BN| \leq |B| + |N| - 2$, entonces*

$$|AB| \geq \text{mín}\{f_1(r,s), f_p(r,s), pq\} = N_{\kappa_G}(r,s).$$

Demostración. El lema se obtendrá como consecuencia de las siguientes afirmaciones.

Afirmación 3.16. Existen subconjuntos no vacíos $M_1, \ldots, M_u \subseteq N$ tales que $A = \bigcup_{k=1}^{u} x^{j_k} M_k$ y $\sum_{i=1}^{u} |N \setminus M_i| \leq p - 2$. Además, $u = \left\lceil \frac{r}{p} \right\rceil$.

En efecto, dado que $|G/N| = q$, el grupo cociente G/N es cíclico, luego $G/N = \langle xN \rangle$ para x en la definición de G en el teorema (3.2) y se tiene $G = \bigcup_{j=0}^{q-1} x^j N$, entonces

$$A = G \cap A = \bigcup_{j=0}^{q-1} (x^j N \cap A) = (x^{j_1} N \cap A) \cup (x^{j_2} N \cap A) \cup \cdots \cup (x^{j_u} N \cap A),$$

donde $j_1, \ldots, j_u$ son todos los enteros que satisfacen $x^{j_k} N \cap A \neq \emptyset$. Observe que tomando $M_k = \{t \in N : x^{j_k} t \in A\} \subseteq N$, se tiene $x^{j_i} N \cap A = x^{j_i} N_i$, para todo $1 \leq i \leq u$, se sigue que

$$r = |A| = \sum_{k=1}^{u} |x^{j_k} M_k| = |x^{j_1} M_1| + |x^{j_2} M_2| + \cdots + |x^{j_u} M_u| = |M_1| + |M_2| + \cdots + |M_u|,$$

Además, $\sum_{i=1}^{u} |N \setminus M_i| = \sum_{i=1}^{u} (|N| - |M_i|) = u|N| - \sum_{i=1}^{u} |M_i| = up - r$, y despejando r se sigue $r = up - \sum_{i=1}^{u} |N \setminus M_i|$. Por otro lado $AN = \left(\bigcup_{k=1}^{u} x^{j_k} M_k \right) N$, luego

$$\begin{aligned} |AN| &= |x^{j_1} N \cup x^{j_2} N \cup \cdots \cup x^{j_u} N| \\ &= |x^{j_1} N| + |x^{j_2} N| + \cdots + |x^{j_u} N| \\ &= \sum_{i=1}^{u} |x^{j_i} N| \\ &= \sum_{i=1}^{u} |N| \\ &= up, \end{aligned}$$

Por lo anterior y utilizando la hipótesis $|AN| \leq |A| + |N| - 2$, se tiene

$$up \leq up - \sum_{i=1}^{u} |N \setminus M_i| + p - 2,$$

por lo tanto $\sum_{i=1}^{u} |N \setminus M_i| \leq p - 2$. Ahora se va verificar $\left\lceil \frac{r}{p} \right\rceil = u$, observe que

$$\frac{r}{p} = \frac{|M_1| + |M_2| + \cdots + |M_u|}{p} = \frac{|M_1|}{p} + \frac{|M_2|}{p} + \cdots + \frac{|M_u|}{p} \leq \sum_{j=1}^{u} 1 = u.$$

Por tanto $\left\lceil \frac{r}{p} \right\rceil \leq u$. Además, $up \leq r + p - 2$ entonces $p(u-1) + 2 \leq r$, se sigue

$$u = \left\lceil u - \frac{p-2}{p} \right\rceil \leq \left\lceil \frac{r}{p} \right\rceil.$$

Así que $\left\lceil \frac{r}{p} \right\rceil = u$.

Afirmación 3.17. Si $r \leq p$, entonces $|AB| \geq \text{mín}\{f_p(r,s), f_1(r,s)\}$.

Sean $u = \left\lceil \frac{r}{p} \right\rceil$ y $v = \left\lceil \frac{s}{p} \right\rceil$, luego $u = 1$ y por la afirmación anterior existen subconjuntos no vacíos $M, N_1, \ldots, N_v \subseteq N$ tales que $A = x^j M$ para algún $0 \leq j \leq p-1$ y $B = \bigcup_{k=1}^{v} N_k x^{t_k}$, donde $0 \leq t_k \leq p-1$. Si $MN_j = N$, para todo $1 \leq j \leq v$ entonces

$$AB = \bigcup_{k=1}^{v} (x^j M)(N_k x^{t_k}) = \bigcup_{k=1}^{v} \left(x^j M N_k x^{t_k}\right) = \bigcup_{k=1}^{v} \left(x^{j+t_k} N\right)$$

De ahí, $|AB| = |N|v = p\left\lceil \frac{s}{p} \right\rceil$. Pero $u = \left\lceil \frac{r}{p} \right\rceil = 1$, entonces

$$p\left\lceil \frac{s}{p} \right\rceil = p\left(\left\lceil \frac{s}{p} \right\rceil + \left\lceil \frac{r}{p} \right\rceil - 1 \right) = f_p(r,s),$$

por lo tanto $|AB| = f_p(r,s)$. Ahora suponga que para algún $1 \leq w \leq v$ se cumple $MN_w \neq N$. Sin pérdida de generalidad suponga $MN_v \neq N$, sin embargo, M, N_v son subconjuntos de $\mathbb{Z}_p$ y aplicando el teorema de Cauchy-Davenport se tiene $|MN_v| \geq |M| + |N_v| - 1$ y por la afirmación anterior $s = |B| = |N_1| + |N_2| + \cdots + |N_v|$ y además, $AB = \bigcup_{k=1}^{v} \left(x^j M N_k x^{t_k}\right)$, entonces

$$|AB| = \sum_{k=1}^{v} |MN_k| \geq \sum_{k=1}^{v-1} |N_k| + |MN_v| \geq \sum_{k=1}^{v} |N_k| + |M| - 1 = s + r - 1 = f_1(r,s).$$

Por lo tanto $|AB| \geq \text{mín}\{f_p(r,s), f_1(r,s)\}$.

Afirmación 3.18. Suponga $u, v \geq 2$, entonces $|AB| \geq \min\{f_p(r,s), f_1(r,s), pq\}$.

Sin pérdida de generalidad, se asume que M_u tiene mínima cardinalidad entre todos los M_i y todos los N_j y considere el conjunto $\overline{A} = x^{j_1}M_1 \cup x^{j_2}M_2 \cup \cdots \cup x^{j_{u-1}}M_{u-1}$. Primero se probará que para todo $1 \leq i \leq u-1$ y para todo $1 \leq j \leq v$ se cumple que $M_iN_j = N$. Fijando i tal que $1 \leq i \leq u-1$, se tiene

$$|N| - |M_u| + |N| - |M_i| \leq \sum_{k=1}^{u} |N \setminus M_k|,$$

Dado que $\sum_{k=1}^{u} |N \setminus M_k| \leq p-2$ y $|M_u| \geq 2$ se sigue $2p - |M_u| - |M_i| \leq p-2$, así $|M_i| + |M_u| \geq p+2$. Luego para cada $1 \leq j \leq v$ se tiene

$$|M_i| + |N_j| - 1 \geq |M_i| + |M_u| - 1 \geq p + 1$$

Aplicando el teorema de Cauchy-Davenport a los subconjuntos $M_i, N_j \subseteq N \subseteq \mathbb{Z}_p$ se sigue

$$p \geq |M_iN_j| \geq \min\{|M_i| + |N_j| - 1, p\} = p,$$

esto implica $N = M_iN_j$, en consecuencia

$$\bar{A}B = \bigcup_{i=1}^{u-1} \left(\bigcup_{k=1}^{v} (x^{j_i}M_i)(N_kx^{t_k}) \right) = \bigcup_{i=1}^{u-1} \left(\bigcup_{k=1}^{v} \left(x^{j_i}Nx^{t_k}\right) \right) = \bigcup_{i=1}^{u-1} \left(\bigcup_{k=1}^{v} \left(x^{j_i+t_k}N\right) \right)$$

Por lo tanto, $\bar{A}B$ es unión de clases laterales izquierdas módulo N y se puede aplicar el teorema de Cauchy-Davenport a los subconjuntos $\bar{A}/N, B/N \subseteq G/N \cong \mathbb{Z}_q$, luego

$$|(\bar{A}B)/N| = |(\bar{A}/N)(B/N)| \geq \min\{|(\bar{A}/N)| + |(B/N)| - 1, q\} = \min\{(u-1) + v - 1, q\}.$$

Si $|(\bar{A}B)/N| = q$, entonces $|AB| \geq |\bar{A}B| = pq$, y se satisface la afirmación. Así que, se puede asumir $|(\bar{A}B)/N| \geq u + v - 2$. Para el caso $|(\bar{A}B)/N| \geq u + v - 1$, se sigue

$$|AB| \geq |\bar{A}B| \geq p(u+v-1) = p\left(\left\lceil \frac{r}{p} \right\rceil + \left\lceil \frac{s}{p} \right\rceil - 1 \right) = f_p(r,s).$$

De manera que la única posibilidad restante es que $|(\bar{A}B)/N| = u + v - 2$. Aplicando el teorema de Cauchy-Davenport a AB/N

$$|AB/N| \geq \min\{u + v - 1, q\} = u + v - 1 > |(\bar{A}B)/N|.$$

De modo que existe algún $N_kx^{j_k} \subseteq B$ para el cual $\left(x^{j_u}M_u\right)\left(N_kx^{t_k}\right) \not\subset \bar{A}B$, pero $\bar{A}B$ es unión de clases laterales izquierdas módulo N y $x^{j_u}M_uN_kx^{t_k} \subseteq x^{j_u+t_k}N$, por ello

$$\left(x^{j_u}M_u\right)\left(N_kx^{t_k}\right) \cap \bar{A}B = \emptyset.$$

Por lo anterior,

$$|AB| \geq |\bar{A}B| + |M_u N_j| \geq p(u+v-2) + \text{mín}\{|M_u| + |N_j| - 1, p\}. \tag{3.2}$$

A continuación, sin pérdida de generalidad suponga que N_v tiene cardinalidad mínima entre los N_j y sean $m(r)$ y $m(s)$ los enteros positivos más pequeños congruentes con r y s módulo p, respectivamente. Ahora se probará que $|M_u| \geq m(r)$ y $|N_v| \geq m(s)$. Para el caso que $r \equiv 0(\text{mód } p)$, se tiene $m(r) = p$ y $r = up$, luego

$$|A| = \sum_{k=1}^{u} |M_k| = |M_u| + \sum_{k=1}^{u-1} |M_k| \leq |M_u| + p(u-1),$$

así $p \leq |M_u|$, en consecuencia $|M_u| = p = m(r)$. Para el caso que $r \not\equiv 0(\text{mód } p)$ se tiene $r = tp + m(r)$, donde $1 < m(r) < p$, entonces $u = \left\lceil \frac{r}{p} \right\rceil = \left\lceil \frac{tp + m(r)}{p} \right\rceil = t + 1$ y así

$$tp + m(r) = |A| = |M_u| + \sum_{k=1}^{u-1} |M_k| \leq |M_u| + p(u-1),$$

luego $tp + m(r) \leq |M_u| + tp$, por tanto $m(r) \leq |M_u|$ y la desigualdad $m(s) \leq |N_v|$ se prueba de manera similar. Luego existen $x, y \in \mathbb{Z}$, tales que $r = yp + m(r)$ y $s = xp + m(s)$, además $1 \leq m(r), m(s) < p$, observe que

$$\left(\left\lceil \frac{r}{p} \right\rceil + \left\lceil \frac{s}{p} \right\rceil \right) p = p(x + 1 + y + 1) = px + py + 2p = r + s + 2p - m(s) - m(r).$$

Por la desigualdad (3.2) se obtiene

$$\begin{aligned} |AB| &\geq p(u+v-2) + \text{mín}\{|M_u| + |N_j| - 1, p\} \\ &\geq p\left(\left\lceil \frac{r}{p} \right\rceil + \left\lceil \frac{s}{p} \right\rceil - 2 \right) + \text{mín}\{m(r) + m(s) - 1, p\} \\ &= r + s - m(s) - m(r) + \text{mín}\{m(r) + m(s) - 1, p\}. \end{aligned}$$

Observe que $f_p = \left(\left\lceil \frac{r}{p} \right\rceil + \left\lceil \frac{s}{p} \right\rceil - 1 \right) p = r+s-m(s)-m(r)+p$. Si $\text{mín}\{m(r)+m(s)-1, p\} = p$, se tiene $|AB| \geq f_p(r,s)$. Resta probar para el caso $\text{mín}\{m(r)+m(s)-1, p\} = m(r)+m(s)-1$, se obtiene la desigualdad $|AB| \geq r+s-m(s)-m(r)+m(r)+m(s)-1 = f_1(r,s)$. Reuniendo todo lo anterior se concluye que $|AB| \geq \text{mín}\{f_1(r,s), f_p(r,s), pq\}$.

Retomando la demostración del lema (3.15), si $u = \left\lceil \frac{r}{p} \right\rceil = 1$ o $v = \left\lceil \frac{s}{p} \right\rceil = 1$, entonces por la afirmación (3.17) se concluye $|AB| \geq \text{mín}\{f_1(r,s), f_p(r,s)\}$. Para el caso $u, v \geq 2$ por el teorema (3.18) se tiene satisface el resultado del lema. □

3.3. La función μ_G en grupos no abelianos de orden pq

En esta sección se presentaran los avances que hasta el momento se tienen en el estudio de la función μ_G cuando G es un grupo no abeliano de orden pq, donde p, q son primos impares con $p > q$. Primero se obtiene una cota inferior para $\mu_G(r, s)$.

Lema 3.19. *Si r, s son enteros positivos tales que $1 \leq r, s \leq pq$, entonces $\mu_G(r, s) \geq \kappa_G(r, s)$.*

Demostración. Dado que $|G| = pq$ los divisores de pq son $\{1, q, p, pq\}$. Se conoce que G contiene un subgrupo de cada de una de estas cardinalidades, y así $D_{k_G}(r, s) = \kappa_G(r, s)$ y dado que G es soluble el teorema (2.26) garantiza $D_{k_G}(r, s) \leq \mu_G(r, s)$, entonces $\mu_G(r, s) \geq \kappa_G(r, s)$. □

Ahora se prueba que $\mu_G(r, s) = N_{k_G}(r, s)$ para r y s que satisfacen criterios específicos. La prueba se centra en mejorar la cota inferior para $\mu_G(r, s)$ que se obtuvo en el lema (3.19).

Teorema 3.20. *Sea G un grupo no abeliano de orden pq, donde p y q son primos impares tales que $p \equiv 1(\text{mód } q)$. Se tiene $\mu_G(r, s) = N_{k_G}(r, s)$ siempre que se cumplan las siguientes condiciones.*

1. $q + 1 \leq r, s \leq pq$
2. $\left\lceil \frac{r}{q} \right\rceil + \left\lceil \frac{s}{q} \right\rceil < p$
3. *r y s son congruentes con 0 o $q - 1$ módulo q y $rs \equiv 0(\text{mód } q)$.*

Demostración. La desigualdad $\mu_G(r, s) \leq N_{k_G}(r, s)$ es consecuencia del teorema (2.26) porque G es un grupo soluble. Falta demostrar que $\mu_G(r, s) \geq N_{k_G}(r, s)$. Primero considere el caso $\mu_G(r, s) \geq f_1(r, s)$, entonces

$$N_{k_G}(r, s) = \text{mín}\{f_1(r, s), f_p(r, s), pq\} \leq f_1(r, s).$$

Así pues, $N_{k_G}(r, s) \leq \mu_G(r, s) \leq N_{k_G}(r, s)$, por lo tanto se satisface el resultado del teorema. Para el caso $\mu_G(r, s) < f_1(r, s) = r + s - 1$, sean A y B subconjuntos de G que realizan $\mu_G(r, s)$, luego $|AB| < r + s - 1$ y por hipótesis $\left\lceil \frac{r}{q} \right\rceil + \left\lceil \frac{s}{q} \right\rceil < p$ se tiene

$$|G| = pq \geq q\left(\left\lceil \frac{r}{q} \right\rceil + \left\lceil \frac{s}{q} \right\rceil + 1\right) > |AB|,$$

luego $AB \neq G$ y se tienen las condiciones del contrarrecíproco del teorema de Zemor (3.4), entonces existe un subgrupo propio K de G tal que $|KA| < |K| + r - 1$ o $|AK| < |K| + r - 1$. De la misma manera, existe un subgrupo propio K' de G tal que $|K'B| < |K'| + s - 1$ o $|BK'| < |K'| + s - 1$, así los subgrupos K y K' deben tener orden p o q. Para el caso $|K| = |K'| = |N|$, se tiene $K = K' = N$, donde N es el único subgrupo normal de G de orden

p, entonces $|AN| = |NA|$ y $|BN| = |NB|$, se sigue que $|AN| < p + r - 1$ y $|BN| < p + s - 1$. Aplicando el lema (3.15) se concluye que $\mu_G(r, s) \geq N_\kappa(r, s)$ y se satisface el teorema. Ahora se probará que no es posible tener $|K| = q$ o $|K'| = q$, sin pérdida de generalidad suponga que $|K'| = q$, entonces K' es un q-subgrupo de Sylow de G y por teorema (1.56) todos los subgrupos de Sylow son conjugados, luego se puede suponer que $H' = H$, es decir, $|BH| < q + s - 1$ o $|HB| < q + s - 1$. Para continuar se estudia cada posibilidad por separado.

Caso 1: $|BH| < q + s - 1$

En este caso el resultado se obtendrá como consecuencia de las cuatro afirmaciones siguientes.

Afirmación 3.21. Existen subconjuntos no vacíos $H_1, \ldots, H_u \subseteq H$ y enteros $0 \leq k_i \leq p-1$, con $i \in \{1, \ldots, u\}$ tales que $B = \bigcup_{i=1}^{u} y^{k_i} H_i$. Además, $\left\lceil \frac{s}{q} \right\rceil = u$.

En efecto, por teorema (3.2) se tiene $G = \langle x, y : x^q = y^p = 1, xyx^{-1} = y^n \rangle$, luego $G = \bigcup_{j=0}^{p-1} y^j H$, entonces

$$B = B \cap G = B \cap \left(\bigcup_{j=0}^{p-1} y^j H \right) = y^{k_1} H_1 \cup y^{k_2} H_2 \cup \cdots \cup y^{k_u} H_u,$$

donde $k_1, \ldots, k_u$ son todos los enteros que satisfacen $B \cap y^{k_i} H_i \neq \emptyset$, luego $s = |B| = \sum_{i=1}^{u} |H_i|$ y se tiene

$$\frac{s}{q} = \frac{\sum_{i=1}^{u} |H_i|}{q} \leq \sum_{i=1}^{u} 1 = u,$$

así $\left\lceil \frac{s}{q} \right\rceil \leq u$. Además,

$$|BH| = |y^{k_1} H \cup y^{k_2} H \cup \cdots \cup y^{k_u} H| = u|H| = uq,$$

entonces $uq < q + s - 1$, luego $q(u-1) + 2 \leq s$, así $\left\lceil \frac{q(u-1)+2}{q} \right\rceil \leq \left\lceil \frac{s}{q} \right\rceil$, se tiene $u \leq \left\lceil \frac{s}{q} \right\rceil$. Por lo tanto $\left\lceil \frac{s}{q} \right\rceil = u$.

Afirmación 3.22. Existe $\overline{H} \subseteq H$ con $|\overline{H}| \geq q - 1$, tal que $B = y^{k_1} \overline{H} \cup y^{k_2} H \cup \cdots \cup y^{k_u} H$.

En efecto, por la afirmación anterior $B = \bigcup_{i=1}^{u} y^{k_i} H_i$, donde $u = \left\lceil \frac{s}{q} \right\rceil$ y los H_i son subconjuntos no vacíos de H. Primero suponga que $s \equiv 0 (\text{mód } q)$, entonces $s = uq$. Si existe $H_j \neq H$, se tiene

$$|B| = \sum_{i=1}^{u} |H_i| \leq \sum_{\substack{i=1 \\ i \neq j}}^{u} |H_i| + |H_j| \leq (u-1)q + |H_j| < uq - q + q = uq,$$

esto contradice $|B| = s = uq$, por lo tanto $H_i = H$ para todo $i = 1, \ldots, u$ y en este caso $B = y^{k_1}H \cup y^{k_2}H \cup \cdots \cup y^{k_u}H$. Para el caso que $s \equiv q - 1(\text{mód } q)$, dado que $s \geq q + 1$ se sigue que existe un entero m tal que $s = mq - 1$ y $2 \leq m \leq p$, entonces

$$m = \left\lceil \frac{s}{q} + \frac{1}{q} \right\rceil \geq \left\lceil \frac{s}{q} \right\rceil = u.$$

Suponga que dos de los H_i son subconjuntos propios de H, no se pierde generalidad en asumir que estos dos subconjuntos son H_1 y H_2, entonces

$$|B| = |H_1| + |H_2| + \sum_{i=3}^{u} |H_i| \leq 2(q-1) + \sum_{i=3}^{u} |H_i| \leq 2q + (u-2)q - 2 < uq - 1,$$

esto contradice $|B| = s = mq - 1$, por lo tanto no es posible encontrar dos de los H_i que sean subconjuntos propios de H, luego existe a lo más uno de los H_i que es subconjunto propio de H, así que $s = |B| = |\overline{H}| + (u-1)q$ para algún subconjunto propio $\overline{H} \subset H$. Pero $s \equiv q - 1(\text{mód } q)$, luego $|\overline{H}| \equiv q - 1(\text{mód } q)$ y $\overline{H} \subseteq H$, por lo tanto $|\overline{H}| = q - 1$, por lo tanto

$$B = y^{k_1}\overline{H} \cup y^{k_2}H \cup \cdots \cup y^{k_u}H.$$

Afirmación 3.23. *AB es unión de clases laterales izquierdas módulo H.*

Efectivamente, sean $a \in A, b \in B$, luego $a = y^j x^t$ y $b = y^i x^l$, para $j, i \leq p$ y $t, l \leq q$. De la definición del grupo G se tiene $xyx^{-1} = y^n$, entonces $(xyx^{-1})^k = xy^k x^{-1} = y^{n^k}$, así

$$(y^j x^t)(y^i x^l) = y^j x^{t-1}(xy^i x^{-1})x^{l+1} = y^j x^{t-1} y^{n^i} x^{l+1}.$$

y continuando de esta forma se tiene

$$ab = (y^j x^t)(y^i x^l) = y^w x^z, \tag{3.3}$$

para algunos enteros w y z, por tanto $ab \in y^w H$, esto significa que AB está contenida en alguna unión de clases laterales izquierdas módulo H. De la afirmación (3.22) se sabe que $B = y^{k_1}\overline{H} \cup y^{k_2}H \cup \cdots \cup y^{k_u}H$, entonces que para completar la prueba es suficiente mostrar que para todo elemento $a \in A$ y todo $i = \{1, \ldots, u\}$ se tiene $ay^{k_i}H \subseteq AB$. Observe que tomando $i \geq 2$, se tiene $ay^{k_i}H \subseteq \left(\bigcup_{i=2}^{u} ay^{k_i}H \right) \subseteq AB$. Resta probar que $ay^{k_1}H \subseteq AB$, fije

$a_0 \in A$ y observe que

$$\begin{aligned} a_0B \cap a_0y^{k_1}H &= \left[\left(\bigcup_{j=2}^{u} a_0y^jH\right) \cup (a_0y^{k_1}\overline{H})\right] \cap a_0y^{k_1}H \\ &= \left(a_0y^{k_1}\overline{H} \cap a_0y^{k_1}H\right) \cup \left[\left(\bigcup_{j=2}^{u} a_0y^jH\right) \cap a_0y^{k_1}H\right] \\ &= a_0y^{k_1}\overline{H} \neq \emptyset. \end{aligned}$$

Sea $T = \{a \in A : aB \cap a_0y^{k_1}H \neq \emptyset\}$, por lo anterior se sigue que $a_0 \in T$. Suponga que a_0 es el único elemento en T, entonces

$$aB \cap a_0y^{k_1}H = \emptyset, \text{ para todo } a \in A, \text{ con } a \neq a_0.$$

Así, todo elemento en $a_0y^{k_1}\overline{H}$ se puede expresar de forma única en AB, y aplicando el teorema de Kemperman (3.5) se sigue que $|AB| \geq r + s - 1$, pero esto contradice el hecho que A y B realizan $\mu_G(r, s) < r + s - 1$, por lo tanto, $|T| \geq 2$. Escoja $a \in T \setminus \{a_0\}$, por la definición del conjunto T se sigue que $(aB) \cap (a_0y^{k_1}H) \neq \emptyset$, luego existe $b \in B$ tal que $ab \in (a_0y^{k_1})H$, pero $B \subseteq \bigcup_{i=1}^{u} y^{k_i}H$ entonces $b \in y^{k_c}H$ para algún $c \in \{1, \ldots, u\}$ y se tiene $ab \in ay^{k_c}H$, es decir,

$$(ay^{k_c}H) \cap (a_0y^{k_1}H) \neq \emptyset.$$

así que $ay^{k_c}H = a_0y^{k_1}H$, pero $ay^{k_c}H \subseteq AB$ para todo $c \in \{2, \ldots, u\}$, entonces $c = 1$, equivalente, $ay^{k_1}H = a_0y^{k_1}H$. Además, $\overline{H} \subseteq H$, con $|\overline{H}| \geq q - 1$, si $|\overline{H}| = q$, se satisface el enunciado porque $\overline{H} = H$, en el otro caso existe un único $h \in H$ tal que $h \notin \overline{H}$ y se tiene

$$ay^{k_1}\overline{H} = ay^{k_1}H \setminus \{ay^{k_1}h\} = a_0y^{k_1}H \setminus \{ay^{k_1}h\},$$

entonces

$$(ay^{k_1}\overline{H}) \cup (a_0y^{k_1}\overline{H}) = \left(a_0y^{k_1}H \setminus \{ay^{k_1}h\}\right) \cup \left(a_0y^{k_1}H \setminus \{a_0y^{k_1}h\}\right),$$

No obstante, $ay^{k_1}h \neq a_0y^{k_1}h$, porque $a \neq a_0$, por consiguiente $\{ay^{k_1}h\} \cap \{a_0y^{k_1}h\} = \emptyset$, y así que

$$(ay^{k_1}\overline{H}) \cup (a_0y^{k_1}\overline{H}) = a_0y^{k_1}H \setminus \left(\{ay^{k_1}h\} \cap \{a_0y^{k_1}h\}\right) = a_0y^{k_1}H.$$

Por lo tanto $a_0y^{k_1}H \subseteq AB$ y así AB es unión de clases laterales izquierdas módulo H.

Afirmación 3.24. Definiendo $C_j = \{i : y^ix^j \in A\}$ y $D = \{w : y^wH \cap B \neq \emptyset\}$, con $j \in \{0, \ldots, q-1\}$, subconjuntos de $\mathbb{Z}_p$, se cumple

1. $|AB| \geq q|(C_0 + D) \cup (C_1 + nD) \cup (C_2 + n^2D) \cup \cdots \cup (C_{q-1} + n^{q-1}D)|$.

2. $|C_0| + |C_1| + \cdots + |C_{q-1}| = r$.

Dado que $xyx^{-1} = y^n$, se tiene $y^{-1} = xy^nx$, y así $y^w = x^{-1}y^{nw}x$, luego

$$\begin{aligned} x^j y^w &= x^{j-1}(x^{-1}y^w x)x = x^{j-1}yy^{nw}x \\ &= x^{j-1}(x^{-1}y^w x)x = x^{j-2}y^{n^2w}x^2, \end{aligned}$$

y continuando de esta forma se tiene

$$x^j y^w = y^{n^j w}x^j, \tag{3.4}$$

entonces para todo $i \in C_j$ y todo $w \in D$ se tiene $y^{i+n^j w}H = y^i y^{n^j w}x^j H = y^i x^j y^w H \subseteq AB$, de modo que el número de las clases laterales izquierdas módulo H que están contenidas en AB es el número de valores distintos de $i + n^j w (\text{mód } p)$, donde $i \in C_j$ y $w \in D$, y así

$$|AB| \geq q|(C_0 + D) \cup (C_1 + nD) \cup C_2 + n^2D \cup \cdots \cup (C_{q-1} + n^{q-1}D)|.$$

Ahora para demostrar el segundo enunciado de esta afirmación considere la función biyectiva $f : A \to \bigcup_{j=0}^{q-1} C_j \times \{j\}$ definida por $f(y^i x^j) = (i, j)$, para todo $y^i x^j \in A$ se tiene

$$r = |A| = \left|\bigcup_{j=0}^{q-1} C_j \times \{j\}\right| = \sum_{j=0}^{q-1} |C_j \times \{j\}| = \sum_{j=0}^{q-1} |C_j|.$$

Para concluir el caso $|BH| < q + s - 1$, por la afirmación (3.24) se tiene

$$|AB| \geq q|(C_0 + D) \cup (C_1 + nD) \cup C_2 + n^2D \cup \cdots \cup (C_{q-1} + n^{q-1}D)|.$$

y $\sum_{j=0}^{q-1} |C_j| = r$. Observe que $|D| = u = \left\lceil \frac{s}{q} \right\rceil$, esto junto con las hipótesis del teorema permiten usar el lema (3.11) y concluir que

$$|(C_0 + D) \cup (C_1 + nD) \cup (C_2 + n^2D) \cup \cdots \cup (C_{q-1} + n^{q-1}D)| \geq \left\lceil \frac{r}{q} \right\rceil + \left\lceil \frac{s}{q} \right\rceil$$

Por lo tanto,

$$|AB| \geq q\left(\left\lceil \frac{r}{q} \right\rceil + \left\lceil \frac{s}{q} \right\rceil\right) \geq r + s.$$

Pero esto contradice $|AB| = \mu_G(r, s) < r + s - 1$.

Caso $|HB| < q + s - 1$

En este caso se cumplen las afirmaciones que se enuncian a continuación.

Afirmación 3.25. Con las hipótesis del teorema se satisfacen los siguientes enunciados.

1. Existe $\overline{H} \subset H$, con $|\overline{H}| \geq q-1$ tal que $B = \overline{H}y^{b_1} \cup \left(\bigcup_{j=2}^{v} Hy^{b_j} \right)$, para algunos enteros $b_1, \ldots, b_v \in \{0, \ldots, p-1\}$. Además $v = \lceil \frac{s}{q} \rceil \geq 2$.

2. Para todo $a, b \in \{0, \ldots, p-1\}$ y todo $m \in \{0, \ldots, q-1\}$, se tiene

$$(y^a x^m)(Hy^b) = \{y^{a+n^j b} x^j : 0 \leq j \leq q-1\}.$$

3. Existen subconjuntos no vacíos $H_1, \ldots, H_u \subset H$ tales que $A = \bigcup_{t=1}^{u} y^{a_t} H_t$, para algunos enteros $a_{t_1}, \ldots, a_{t_u} \in \{0, \ldots, p-1\}$. Además $u \geq \lceil \frac{r}{q} \rceil \geq 2$.

En efecto, el primer enunciado se prueba con un procedimiento similar al realizado en la afirmación (3.22). Para el segundo, todo elemento de A se puede escribir de la forma $y^a x^m$, donde $0 \leq a \leq p-1$ y $0 \leq m \leq q-1$, observe que

$$(y^a x^m)(Hy^b) = y^a (x^m H) y^b = y^a H y^b = \{y^a x^j y^b : 0 \leq j \leq q-1\}.$$

Luego, por la ecuación (3.4) se tiene $x^j y^b = y^{n^j b} x^j$, entonces

$$(y^a x^m)(Hy^b) = \{y^{a+n^j b} x^j : 0 \leq j \leq q-1\}. \tag{3.5}$$

Finalmente, el tercer enunciado es concecuencia de la afirmación (3.21).

Afirmación 3.26. Definiendo los subconjuntos $C, D \subseteq \mathbb{Z}_p$, por

$$C = \{a \in \mathbb{Z}_p : y^a x^m \in A, \text{ para algún } m \in \mathbb{Z}_q\}, \quad D = \{b \in \mathbb{Z}_p : Hy^b \subseteq B\}.$$

Se tiene $|AB| \geq \sum_{j=0}^{q-1} |C + n^j D|$, y la igualdad se cumple cuando $s \equiv 0 (\text{mód } q)$.

En efecto, observe que el item (2) de la afirmación (3.25), garantiza que para cada $a \in C$ y cada $b \in D$, el conjunto $\left\{ y^{a+n^j b} x^j : 0 \leq j \leq q-1 \right\} \subseteq AB$. Ahora, para $j \in \{0, \ldots, q-1\}$ considere el conjunto

$$\mathcal{M}_j = \left\{ y^{a+n^j b} x^j \in AB : a \in C, b \in D \right\},$$

es decir, para cada $a \in C$ y cada $b \in D$, el conjunto $\mathcal{M}_0$ esta formado por todos los elementos de la forma $y^{a+b} \in AB$, $\mathcal{M}_1$ es el conjunto de todos los elementos de la forma $y^{a+nb} x \in AB$, y

así sucesivamente. Luego, $\mathcal{M}_j \cap \mathcal{M}_i = \emptyset$, cuando $j \neq i$, además se cumple $|\mathcal{M}_j| = |C + n^j D|$, para toda $j \in \{0, \ldots, q-1\}$, entonces

$$|AB| \geq \left| \bigcup_{j=0}^{q-1} \mathcal{M}_j \right| = \sum_{j=0}^{q-1} |\mathcal{M}_j| = \sum_{j=0}^{q-1} |C + n^j D|$$

En el caso $s \equiv 0(\text{mód } q)$, por la afirmación 3.11, existen $b_1, \ldots, b_v \in \{0, \ldots, p-1\}$ tales que $B = \bigcup_{j=1}^{v} Hy^{b_j}$, con $v = \lceil \frac{s}{q} \rceil \geq 2$. Luego, $D = \{b_1, \ldots, b_v\}$ y todo elemento en AB tiene la forma $y^{a+n^j b} x^j$, con $a \in C$, $b \in D$ y $j \in \{0, \ldots, q-1\}$. Por lo tanto, $AB = \bigcup_{j=0}^{q-1} \mathcal{M}_j$, de aquí se sigue $|AB| = \sum_{j=0}^{q-1} |C + n^j D|$.

Retomando el caso $|HB| < q + s - 1$, suponga $s \equiv 0(\text{mód } q)$, entonces se satisface afirmación (3.26) y por la afirmación (3.25), existen subconjuntos no vacíos $H_1, \ldots, H_u \subset H$ tales que $A = \bigcup_{t=1}^{u} y^{a_t} H_t$, para algunos enteros $a_{t_1}, \ldots, a_{t_u} \in \{0, \ldots, p-1\}$, con $u \geq \lceil \frac{r}{q} \rceil \geq 2$. Luego, $C = \{a_{t_1}, \ldots, a_{t_u}\}$, $D = \{b_1, \ldots, b_v\}$ e igualmente

$$|AB| = \sum_{j=0}^{q-1} |C + n^j D|.$$

Escoja $j_0 \in \{0, \ldots, q-1\}$ de tal manera que $|C + n^{j_0} D| \leq |C + n^j D|$ para toda j, entonces $|AB| \geq q|C + n^{j_0} D|$ y dado que $|AB| = \mu_G(r, s) < r + s - 1$ se tiene

$$|C + n^{j_0} D| < \frac{r}{q} + \frac{s}{q} - \frac{1}{q} \leq \left\lceil \frac{r}{q} \right\rceil + \left\lceil \frac{s}{q} \right\rceil \leq u + v.$$

Por otro lado, $|C + n^{j_0} D| \leq \frac{|AB|}{q} < \frac{pq}{q} = p$, esto junto con el teorema de Cauchy-Davenport implican $|C + n^{j_0} D| \geq \text{mín}\{|C| + |n^{j_0} D| - 1, p\} = u + v - 1$, entonces

$$|C + n^{j_0} D| = u + v - 1,$$

y se tienen las hipótesis del teorema de Vosper, luego C y $n^{j_0} D$ son progresiones aritméticas en $\mathbb{Z}_p$ de la misma diferencia común, además D es una progresión arimética en $\mathbb{Z}_p$. Tomando $d \in \mathbb{Z}_p \setminus \{0\}$ como la diferencia común de D, se sigue que C y $n^{j_0} D$ tienen diferencia común $t \equiv \pm n^{j_0} d(\ \text{mód } p)$. Si para algún $j \neq j_0$ se satisface $|C + n^j D| = u + v - 1$, entonces por lo anterior $n^j D$ es una progresión arimética en $\mathbb{Z}_p$ de diferencia común t, es decir, $n^{j_0} d \equiv n^j d(\ \text{mód } p)$, o equivalente, $n^{j-j_0} \equiv 1(\ \text{mód } p)$ y por hipótesis del teorema, se sigue $j = j_0$, así que, $|C + n^j D| \geq u + v - 1$, para toda $j \neq j_0$. Entonces,

$$|AB| = \sum_{j=0}^{q-1} |C + n^j D| \geq u + v - 1 + (q-1)(u+v) = q(u+v) - 1 \geq r + s - 1,$$

pero esto contradice el hecho que $|AB| < r + s - 1$.

Para el caso $s \equiv q - 1(\text{mód } q)$, por hipótesis del teorema se debe tener $r \equiv 0(\text{mód } q)$ y por la afirmación 3.11, existe $\overline{H} \subset H$, con $|\overline{H}| = q - 1$ tal que $B = \overline{H}y^{b_1} \cup \left(\bigcup_{j=2}^{v} Hy^{b_j} \right)$, para algunos enteros $b_1, \ldots, b_v \in \{0, \ldots, p-1\}$, con $v = \lceil \frac{s}{q} \rceil \geq 2$, y existen subconjuntos no vacíos $H_1, \ldots, H_u \subset H$ tales que $A = \bigcup_{t=1}^{u} y^{a_t} H_t$, para enteros $a_{t_1}, \ldots, a_{t_u} \in \{0, \ldots, p-1\}$, con $u \geq \lceil \frac{r}{q} \rceil \geq 2$. Luego, $|D| = \lceil \frac{s}{q} \rceil - 1$ y $|C| \geq \frac{r}{q}$. En el caso $|C| = \frac{r}{q}$, con los mismos argumentos empleados en la afirmación 3.8, se tiene $A = \bigcup_{t=1}^{u} y^{a_t} H$, es decir, A es union de clases laterales izquierdas módulo H y tomando $W = \{b \in \mathbb{Z}_p : Hy^b \cap B \neq \emptyset\}$, se satisface

$$|AB| = \sum_{j=0}^{q-1} |C + n^j W|.$$

De nuevo escogiendo $j_0 \in \{0, \ldots, q-1\}$ de tal manera que $|C + n^{j_0} W| \leq |C + n^j W|$ para toda j, entonces $|AB| \geq q|C + n^{j_0} W|$ y dado que $|AB| = \mu_G(r, s) < r + s - 1$ se tiene

$$|C + n^{j_0} W| < \frac{r}{q} + \frac{s}{q} - \frac{1}{q} \leq \left\lceil \frac{r}{q} \right\rceil + \left\lceil \frac{s}{q} \right\rceil = u + |n^{j_0} W|.$$

Por el teorema de Cauchy-Davenport

$$|C + n^{j_0} W| \geq \text{mín}\{|C| + |n^{j_0} W| - 1, p\} = u + |n^{j_0} W| - 1,$$

luego, $|C + n^{j_0} W| = u + |n^{j_0} W| - 1$, y se tienen las condiciones del teorema de Vosper y con un razonamiento similar al hecho en el caso $s \equiv 0(\ \text{mód } p)$ se obtiene la contradicción $|AB| \geq r+s-1$. Para el caso $|C| > \frac{r}{q}$, primero considere que $|C| \geq \frac{r}{q}+2$, por la afirmación 3.12 se sabe que $|AB| \geq \sum_{j=0}^{q-1} |C+n^j D|$ y escogiendo $j_0 \in \{1, \ldots, q-1\}$ tal que $|C+n^{j_0} D| \leq |C+n^j D|$ para toda j, se tiene $|AB| \geq q|C + n^{j_0} G|$ y aplicando el teorema de Cauchy- Davenport se sigue

$$\begin{aligned} |C + n^{j_0} D| &\geq \text{mín}\{|C| + |D| - 1, p\} \\ &\geq \text{mín}\left\{ \left\lceil \frac{r}{q} \right\rceil + 2 + \left\lceil \frac{s}{q} \right\rceil - 1 - 1, p \right\} \\ &= \text{mín}\left\{ \left\lceil \frac{r}{q} \right\rceil + \left\lceil \frac{s}{q} \right\rceil, p \right\} \\ &= \left\lceil \frac{r}{q} \right\rceil + \left\lceil \frac{s}{q} \right\rceil. \end{aligned}$$

Por tanto

$$|AB| \geq q \left(\left\lceil \frac{r}{q} \right\rceil + \left\lceil \frac{s}{q} \right\rceil \right) \geq r + s$$

Pero esto contradice $\mu_G(r,s) < r+s-1$. La única posibilidad es que $|C| = \left\lceil \frac{r}{q} \right\rceil + 1$ y observe que a lo más un H_i tiene cardinalidad 1, en efecto, suponga $|H_1| = |H_2| = 1$, entonces

$$r = |A| = 2 + \sum_{i=3}^{u} |H_i| \leq 2 + q(u-2),$$

así $\frac{r}{q} + 1 \leq \frac{2}{q} + u - 1$, luego $u \leq \frac{2}{q} + u - 1$, es decir, $q \leq 2$, esto es una contradicción. Ahora, sin pérdida de generalidad, suponga que $|H_i| \geq 2$ para todo $i \geq 2$, entonces $H_i\overline{H} = H$ para todo $i \geq 2$ porque $|\overline{H}| = q-1$, además, $|H_1\overline{H}| \geq q-1$. Sea $D' = \{b : \overline{H}y^b \subset B\}$ y note que

$$|AB| \geq |C + D'| + |C + nD'| + |C + n^2D'| + \cdots + |C + n^{q-1}D'| - 1,$$

Dado que $|D'| = \left\lceil \frac{s}{q} \right\rceil$, se tiene

$$\begin{aligned} |AB| &\geq \text{mín}\{q\left(|C| + |D'| - 1\right) - 1, pq - 1\} \\ &\geq \text{mín}\left\{q\left(\left\lceil \frac{r}{q} \right\rceil + 1 + \left\lceil \frac{s}{q} \right\rceil - 1\right), pq - 1\right\} \\ &\geq \text{mín}\{r + s - 1, pq - 1\} \\ &= r + s - 1 \end{aligned}$$

Pero esto contradice $\mu_G(r,s) < r+s-1$. Por lo tanto $|K| = |K'| = p$, esto concluye la prueba del teorema. □

El teorema (3.20) proporciona el valor de $\mu_G(r,s)$ para muchos r y s. En particular, estos valores son suficientes para demostrar que en todos los grupos no abelianos de orden pq existe $1 \leq r, s \leq pq$ con $\mu_G(r,s) > \kappa_G(r,s)$. Esto mejora los cálculos de Eliahou y Kervaire (2007) [4], donde ellos usan una búsqueda por computadora para proporcionar un solo ejemplo de un grupo G donde $\mu_G(r,s)$ no siempre es igual a $\kappa_G(r,s)$.

Teorema 3.27. *Si G un grupo no abeliano de orden pq, donde $p > q$ son primos impares y $p \equiv 1 (\text{mód } q)$, entonces existen $1 \leq r, s \leq pq$ tales que $\mu_G(r,s) > \kappa_G(r,s)$.*

Demostración. Del teorema anterior (3.20), es suficiente encontrar enteros r, s tales que son congruentes con 0 o $q-1$ módulo q, con al menos uno de ellos 0 módulo q, y $q+1 \leq r, s \leq pq$, $\left\lceil \frac{r}{q} \right\rceil + \left\lceil \frac{s}{q} \right\rceil < p$ y $N_{k_G}(r,s) > \kappa_G(r,s)$. Sea $r = 2q$ y $s = 3q$, entonces $\left\lceil \frac{2q}{q} \right\rceil + \left\lceil \frac{3q}{q} \right\rceil = 5$, además p, q son primos impares con $p > q$ y $p \equiv 1 (\text{mód } q)$, es decir, 7 es el valor más pequeño que puede tomar p, así que $5 < p$. Observe que

$$f_q(2q, 3q) = \left(\left\lceil \frac{2q}{q} \right\rceil + \left\lceil \frac{3q}{q} \right\rceil - 1\right) q = (5-1)q = 4q,$$

es estrictamente menor que

$$f_1(2q,3q) = \left(\left\lceil \frac{2q}{1} \right\rceil + \left\lceil \frac{3q}{1} \right\rceil - 1\right) = 5q-1$$

y

$$f_{pq}(2q,3q) = \left(\left\lceil \frac{2q}{pq} \right\rceil + \left\lceil \frac{3q}{pq} \right\rceil - 1\right) pq = \left(\left\lceil \frac{2}{p} \right\rceil + \left\lceil \frac{3}{p} \right\rceil - 1\right) pq = (2-1)pq = pq.$$

Lo que resta por probar es $f_q(2q,3q) < f_p(2q,3q)$. Como $p \equiv 1 (\text{mód } q)$, entonces $p = mq+1$, donde m es un entero. Si m es impar, entonces $m = 2t+1$ para algún entero t, luego $p = (2t+1)q+1 = 2tq+(q+1)$ y dado que q es impar se sigue que p es par, esto es una contradicción. Así que m es par. Para el caso $m = 2$ se tiene

$$f_p(2q,3q) = p + 2p - p = 4q+2 > f_q(2q,3q).$$

Para $m > 2$ se sigue $p \geq 4q+1$, así

$$f_p(2q,3q) = p \geq 4q+1 > f_q(2q,3q).$$

Por lo tanto $N_{k_G}(2q,3q) > \kappa_G(2q,3q)$, y por teorema 3.20 $\mu_G(2q,3q) = N_{k_G}(2q,3q)$, se concluye $\mu_G(2q,3q) > \kappa_G(2q,3q)$. □

El teorema (3.20) es una herramienta principal para determinar completamente $\mu_G(r,s)$ cuando G es un grupo no abeliano de orden $3p$. Sin embargo, queda calcular $\mu_G(r,s)$ en los casos donde el teorema (3.20) no se aplica. En particular, es sencillo obtenerlo cuando $\left\lceil \frac{r}{q} \right\rceil + \left\lceil \frac{s}{q} \right\rceil \geq p$ o cuando mín$\{r,s\} \leq q$, esto se puede ver en los dos siguientes resultados.

Lema 3.28. *Si $q+1 \leq r,s \leq pq$ tal que $\left\lceil \frac{r}{q} \right\rceil + \left\lceil \frac{s}{q} \right\rceil \geq p$, entonces $\mu_G(r,s) = \kappa_G(r,s)$.*

Demostración. Primero se va considerar el caso que $\left\lceil \frac{r}{q} \right\rceil + \left\lceil \frac{s}{q} \right\rceil = p$, entonces

$$f_q(r,s) = \left(\left\lceil \frac{r}{q} \right\rceil + \left\lceil \frac{s}{q} \right\rceil - 1\right) q = (p-1)q = pq - q.$$

Sean $r' = q\left\lceil \frac{r}{q} \right\rceil$ y $s' = q\left\lceil \frac{s}{q} \right\rceil$, observe que $r' \geq r$ y $s' \geq s$, entonces

$$f_q(r',s') = \left(\left\lceil \frac{q\left\lceil \frac{r}{q} \right\rceil}{q} \right\rceil + \left\lceil \frac{q\left\lceil \frac{s}{q} \right\rceil}{q} \right\rceil - 1\right) q = \left(\left\lceil \frac{r}{q} \right\rceil + \left\lceil \frac{s}{q} \right\rceil - 1\right) q = f_q(r,s).$$

También

$$r' + s' = q\left\lceil \frac{r}{q} \right\rceil + q\left\lceil \frac{s}{q} \right\rceil = q\left(\left\lceil \frac{r}{q} \right\rceil + \left\lceil \frac{s}{q} \right\rceil\right) = pq.$$

Se aplica el teorema (2.18) y se tiene $\mu_G(r',s') = \kappa_G(r',s')$, además $\kappa_G(r',s') \leq f_q(r',s')$, es decir, sean subconjuntos A' y B' de G que realizan $\mu_G(r',s')$, entonces $|A'B'| \leq f_q(r',s')$. Ahora elija $A \subseteq A'$ y $B \subseteq B'$ con cardinales r y s, respectivamente y por el teorema (2.5) se sigue $|AB| \leq |A'B'|$, entonces $|AB| \leq f_q(r',s') = f_q(r,s)$, por lo tanto, $\mu_G(r,s) \leq f_q(r,s)$ y según el teorema (2.26) $\mu_G(r,s) \leq N_{k_G}(r,s)$, luego

$$\mu_G(r,s) \leq \text{mín}\{f_q(r,s), N_{k_G}(r,s)\} = \kappa_G(r,s).$$

Si $\left\lceil \frac{r}{q} \right\rceil + \left\lceil \frac{s}{q} \right\rceil > p$, entonces

$$f_q(r,s) = \left(\left\lceil \frac{r}{q} \right\rceil + \left\lceil \frac{s}{q} \right\rceil - 1 \right) q \geq pq = f_{pq}(r,s).$$

En consecuencia $\kappa_G(r,s) = N_{k_G}(r,s)$, luego por el teorema (2.26) se sigue $\mu_G(r,s) \leq N_{k_G}(r,s)$ y por lema (3.19) se tiene $\mu_G(r,s) \geq \kappa_G(r,s)$, por lo tanto $\mu_G(r,s) = \kappa_G(r,s)$. □

Lema 3.29. *Si $1 \leq r,s \leq pq$ tal que al menos uno de r o s es a lo sumo q, entonces $\mu_G(r,s) = \kappa_G(r,s)$.*

Demostración. Por teorema (2.26) $\mu_G(r,s) \leq N_{k_G}(r,s)$ y por lema (3.19) $\mu_G(r,s \geq \kappa_G(r,s)$, entonces basta con encontrar los conjuntos A y B con $|A| = r, |B| = s$, y $|AB| \leq f_q(r,s)$. Sin pérdida de generalidad, suponga $r \leq q$, entonces $\left\lceil \frac{r}{q} \right\rceil = 1$. Tome A un subconjunto de H con $|A| = r$ y sea B un conjunto de s elementos contenido en la unión de no más de $v = \left\lceil \frac{s}{q} \right\rceil$ clases laterales derechas módulo H, es decir, $B \subseteq Hy^{k_1} \cup Hy^{k_2} \cup \cdots \cup Hy^{k_v}$. Por la ecuación (3.5) se puede concluir $AB \subseteq Hy^{k_1} \cup Hy^{k_2} \cup \cdots \cup Hy^{k_v}$, así

$$|AB| \leq q \left\lceil \frac{s}{q} \right\rceil = q \left(\left\lceil \frac{r}{q} \right\rceil + \left\lceil \frac{s}{q} \right\rceil - 1 \right) = f_q(r,s).$$

Por tanto $\mu_G(r,s) = \kappa_G(r,s)$. □

La combinación del teorema (3.20) y los lemas (3.28) y (3.29) permite calcular $\mu_G(r,s)$ para muchos valores de r y s. En particular, estos tres resultados permiten determinar completamente $\mu_G(r,s)$ en el caso en que G es un grupo no abeliano de orden $3p$, como se presenta en el siguiente teorema.

Teorema 3.30. *Sea G un grupo no abeliano de orden $3p$, donde $p > 3$ es primo. Si $1 \leq r,s \leq 3p$, entonces*

$$\mu_G(r,s) = \begin{cases} N_{k_G}(r,s) & \text{si } r,s > 3 \text{ y } \left\lceil \frac{r}{3} \right\rceil + \left\lceil \frac{s}{3} \right\rceil < p. \\ \\ \kappa_G(r,s) & \text{otro caso.} \end{cases}$$

Demostración. El segundo caso se sigue del lema (3.28) y del lema (3.29). Cuando $r, s > 3$ y $\left\lceil \frac{r}{3} \right\rceil + \left\lceil \frac{s}{3} \right\rceil < p$. Cuando $r \equiv 0(\text{mód } 3)$ o $r \equiv 2(\text{mód } 3)$ y cuando $s \equiv 0(\text{mód } 3)$ o $s \equiv 2(\text{mód } 3)$, en este caso la igualdad $\kappa_G(r, s) = N_{\kappa_G}(r, s)$ se tiene por el teorema (3.20). De lo contrario, en caso que $r \equiv 2(\text{mód } 3)$ o $s \equiv 2(\text{mód } 3)$, es decir, $r = 3t + 2$ y $s = 3l + 2$, donde $t, l \in \mathbb{Z}$. Observe que $t < p$, cuando $t \geq p$, se sigue

$$\left\lceil \frac{r}{3} \right\rceil = \left\lceil t + \frac{2}{3} \right\rceil = t + 1 > t \geq p,$$

esto es una contradicción con el hecho que $\left\lceil \frac{r}{3} \right\rceil + \left\lceil \frac{s}{3} \right\rceil < p$. Por ello, $t \leq p - 1$, pero $3t = r - 2$, reemplazando el valor de t se tiene $3t \leq 3p - 3$, luego $r - 2 \leq 3p - 3$, así $r \leq 3p - 1$, entonces

$$\left\lceil \frac{r}{3p} \right\rceil = \left\lceil \frac{3t + 2}{3p} \right\rceil = \left\lceil \frac{t}{p} + \frac{2}{3p} \right\rceil = 1,$$

de manera similar $\left\lceil \frac{s}{3p} \right\rceil = 1$, por tanto

$$f_{3p}(r, s) = 3p \left(\left\lceil \frac{r}{3p} \right\rceil + \left\lceil \frac{s}{3p} \right\rceil - 1 \right) = 3p(2 - 1) = 3p.$$

Observe que $r \leq 3 \left\lceil \frac{r}{3} \right\rceil$ y $s \leq 3 \left\lceil \frac{s}{3} \right\rceil$, entonces $r + s - 1 \leq 3 \left\lceil \frac{r}{3} \right\rceil + 3 \left\lceil \frac{s}{3} \right\rceil - 1$, además $3 \left\lceil \frac{r}{3} \right\rceil = 3t + 3 = r + 1$, de manera similar $3 \left\lceil \frac{s}{3} \right\rceil = s + 1$, entonces

$$f_3(r, s) = 3 \left(\left\lceil \frac{r}{3} \right\rceil + \left\lceil \frac{s}{3} \right\rceil - 1 \right) = r + 1 + s + 1 - 3 = r + s - 1 = f_1(r, s).$$

Además en caso $f_p(r, s)$, recuerde que G tiene el subgrupo normal de orden p, entonces $\kappa_G(r, s) = N_{K_G}(r, s)$. Por teorema (2.26) $\mu_G(r, s) \leq N_{k_G}(r, s) = \kappa_G(r, s)$ y por lema (3.19) $\mu_G(r, s \geq \kappa_G(r, s)$, por lo tanto $\mu_G(r, s) = N_{K_G}(r, s)$.

□

Se presentaron las pruebas de los resultados obtenidos dentro del problema conjuntos producto pequeños en grupos no abelianos de orden $3p$, donde $p > 3$ es primo. Deckelbaum conjetura que este resultado se puede extender para grupos no abelianos de orden pq.

Capítulo 4

Algoritmos

En este capítulo se presentan los algoritmos implementados por los autores en el software matemático SageMath, los cuales permiten apreciar lo complicado que resulta encontrar el valor de la función $\mu_G(r, s)$ en algunos grupos finitos no abelianos. SageMath es un entorno de cálculo algebraico discreto de libre distribución que hace énfasis en la Teoría de Grupos Computacional, pero que no se restringe sólo a ella. Se puede encontrar información acerca de este software en la página oficial http://www.sagemath.org/es/.

4.1. Algoritmo para la función μ_G

La función *cardinalAB* toma como argumentos dos listas A y B del grupo G, y posteriormente multiplica los elementos de A por cada uno de los elementos de B, para obtener el conjunto AB y como resultado devuelve la concatenación de listas $AB + A + B$.

Algoritmo 4.1: Algoritmo para producto AB

```
def cardinalAB(A,B):
    AB= [];
    for i ∈A do
        for j ∈B do
            AB.append(i*j);
        end
    end
    return AB+A+B
```

4.2. Algoritmo para generar el grupo no abeliano de orden pq

La función *generado* recibe dos primos impares distintos p, q tales que $p > q$ y $p \equiv 1(\text{mód})$, calcula n un entero fijo tal que $n \not\equiv 1(\text{mód } p)$ y $n^q \equiv 1(\text{mód } p)$ y retorna el grupo no abeliano

de orden pq, que tiene la siguiente representación algebraica:

$$G = \langle x, y : x^q = y^p = 1, xyx^{-1} = y^n \rangle.$$

Algoritmo 4.2: Algoritmo para generar el grupo de orden pq

```
def generado(q,p):
    if ((p − 1) %q == 0)&(p > q)&(p %2 ≠ 0)&(q %2 ≠ 0) then
        i = 2
        while (i^q − 1) %p ≠ 0 do
            i = i + 1
        end
        n=i
        G.⟨x, y⟩= FreeGroup()
        H = G/[x^q, y^p, x ∗ y/(y^n ∗ x)]
    end
    return H
```

Los dos algoritmos anteriores son necesarios para obtener el valor de $\mu_G(r, s)$, estos son llamados dentro del algoritmo para la función μ_G.

4.3. Algoritmo para la función μ_G

La función *mu* es un algoritmo de búsqueda exhaustiva, porque se debe probar uno a uno todos los productos de todos los subconjuntos A y B de cardinal r y s respectivamente, luego devuelve el cardinal más pequeño encontrado del conjunto producto AB. Este algoritmo recibe un subgrupo de permutaciones isoformo al grupo G, que en SageMath se obtiene mediante el comando *G.as_permutation_group()*, enteros positivos r, s tales que $r, s \leq |G|$ y primos impares p, q que cumplen con la definición del grupo no abeliano de orden pq, realiza el conjunto producto para $r-1$ y $s-1$, porque se remueve la identidad al grupo G, pues siempre se puede encontrar subconjuntos A y B que realizan $\mu_G(r, s)$ tales que $1 \in A \cap B$, y así cuando se llama la función *CardinalAB* que da la concatenación de listas $AB + A + B$ y al agregar la identidad de nuevo se consigue tener r y s y finalmente retorna el valor de la función $\mu_G(r, s)$.

Algoritmo 4.3: Algoritmo para μ_G

```
def mu(G, r, s,q,p):
    g=p*q
    e=G.one()
    G=list(G)
    G.remove(e)
    g1= Combinations(G,r-1)
    g2= Combinations(G,s-1)
    for i ∈ g1 do
        for j ∈ g2 do
            D=cardinalAB(i,j);
            D.append(e);
            m=len(Set(D))
            if m<g then
                g=m
            end
        end
    end
    return g
```

4.4. Algoritmo para la función κ_G

La función *kappa* recibe un subgrupo de permutaciones isoformo al grupo G, enteros positivos r, s tales que $r, s \leq |G|$ y p, q primos impares que cumplen con la definición del grupo no abeliano de orden pq y retorna el valor de la función $\kappa_G(r, s)$.

Algoritmo 4.4: Algoritmo para κ_G

```
def kappa(G,r,s,q,p):
    g= p*q
    O=[1,p,q,pq]
    for i ∈ O do
        t=((r/i).ceil()+(s/i).ceil()-1)*i
        if t<g then
            g=t
        end
    end
    return g
```

A continuación se presenta algunos valores de la función μ_G y κ_G obtenidos mediante los anteriores algoritmos implementados en SageMath.

Ejemplo. Mediante el algoritmo *generado(p,q)* se genera el grupo: Finitely presented group $\langle x, y : x^3 = 1, y^7 = 1, x * y * x^{-1} * y^{-2} = 1\rangle$ de orden 3×7, donde $p = 3$, $q = 7$ y $n = 2$ tales que cumplen con las condiciones de la definición de grupos no abelianos de orden pq, con el comando $.list()$ se obtiene la lista de los elementos que lo conforman, así $(1, x^{-1}, y, x, x^{-1} * y, y^2, x * y, y * x^{-1}, x^{-1} * y^{-1} * x, x * y^2, x * y^{-1} * x, x^{-1} * y * x, y^{-1} * x, x * y * x, y^{-2}, y * x, y^{-1} * x^{-1}, y^{-1}, x * y^{-2}, x^{-1} * y^{-1}, x * y^{-1})$ y se realiza el cálculo para todos los valores de r y s posibles, algunos se muestran en la tabla siguiente.

(r, s)	μ_G	κ_G	$N_{\kappa G}$
(4, 4)	7	7	7
(6, 2)	6	6	7
(6, 8)	13	12	13
(6, 9)	14	12	14
(8, 9)	16	15	16
(9, 9)	17	15	17
(5, 9)	13	12	13

Tabla 4.1: Cálculos en el grupo no abeliano de orden 3×7. Fuente: esta investigación.

Se reafirma el resultado que probó Deckelbaum en [5] para grupos no abelianos de orden $3p$.

Ejemplo. Mediante el algoritmo *generado(p,q)* se genera el grupo no abeliano de orden 5×11: Finitely presented group $\langle x, y : x^5, y^{11}, x * y * x^{-1} * y^{-3}\rangle$, donde $p = 11$, $q = 5$ y $n = 3$, se realiza el cálculo para todos los valores de $r, s \leq 55$, y al realizar los cálculos se encuentra que para los valores de (r, s) siguientes no se satisface el teorema que se tiene para $3p$.

r	9	9	9	9	13	13	13	13	14	14	14	14	14	14	19
s	13	14	23	34	14	19	29	34	14	18	13	23	29	34	23

Algunos de estos cálculos se muestran en la tabla siguiente.

(r, s)	μ_G	κ_G	$N_{\kappa G}$
(2, 5)	5	5	6
(4, 4)	5	5	7
(3, 4)	5	5	6
(4, 23)	25	25	26
(4, 23)	25	25	26
(9, 35)	43	40	43

Tabla 4.2: Cálculos en el grupo no abeliano de orden 5×11. Fuente: esta investigación.

Pero dado que el grupo es no abeliano G de orden 55 por el teorema (3.3) es soluble, además para esta clase de grupos coinciden los conjuntos $H(G) = D(G)$ y se tiene $\kappa_G(r, s) = D_{\kappa G}(r, s)$ y la teoría estudiada permite establecer que

$$\kappa_G(r, s) \leq \mu_G(r, s) \leq N_{\kappa G}(r, s).$$

En particular, para los enteros 9 y 13 se tiene $20 \leq \mu_G(9, 13) \leq 21$, y mediante el algoritmo *mu(G,r,s)* e imprimiendo el valor de g con el comando *print*, se obtiene 44 veces subconjuntos A y B tales que el valor $|AB| = 21$, sin embargo no se obtuvo una respuesta satisfactoria, debido a que la gran cantidad de operaciones que se realizan ha desbordado la memoria de los procesadores con los que se cuenta para el desarrollo del proyecto de investigación.

Conclusiones

Se presenta una monografía en la cual se exponen ordenada y detalladamente todos los resultados del problema los conjuntos producto pequeños en grupos no abelianos finitos.

Las pruebas de los resultados presentadas en este trabajo son de otros autores, pero se reescribieron con todos los detalles de manera que facilite la lectura para personas interesadas en incursionar dentro de este problema y que no cuenten con los conocimientos necesarios para entender los artículos en los que se encuentran estos resultados.

El teorema (3.9) es un resultado de la teoría de números que no se encontró en la revisión bibliográfica que se tenia disponible y la demostración presentada fue realizada por los autores.

En el artículo de Deckelbaum (2009) [5], la demostración del teorema (3.20) se realiza mediante el método directo y en este estudio se reescribe por contradicción.

Los métodos computacionales han sido de gran utilidad para el cálculo de $\mu_G(r, s)$ debido a que ofrecen una forma de agilizar las operaciones en un tiempo relativamente pequeño, mas por el momento los algoritmos implementados en esta investigación resultan no ser el camino más eficiente, para buscar la solución a este problema, pues no se estudia la eficiencia algorítmica.

Referencias

[1] Eliahou, S and Kervaire, M. Minimal sumsets in infinite abelian groups. *Journal of Algebra*, 287(2), pag 449-457, (2005).

[2] Plagne, A. Additive number theory sheds new light on the Hopf-Stiefel o function. *Enseignement Mathematique*, 49(1/2), pag 109-116, (2003).

[3] Plagne, A. Optimally small sumsets in general Abelian groups. *Advances in Applied Mathematics* , 38, pag 324-326, (2007).

[4] Eliahou, S and Kervaire, M. Some results on minimal sumset sizes in finite non-abelian groups. *Journal of Number Theory*, 124(1), pag 234-247, (2007).

[5] Deckelbaum, A. Minimum product set sizes in nonabelian groups of order pq. *Journal of Number Theory*, 129(6), pag 1234-1245, (2009).

[6] Eliahou, S and Kervaire, M. Minimal sumsets in finite solvable groups. *Discrete Mathematics*, 310(3), pag 471-479,(2010).

[7] Mutis, W, Benavides, F and Castillo, J. Conjuntos suma pequeños en $p-grupos$ finitos. *Revista Integración*, 28(1), pag 79-83,(2010).

[8] Mutis, W, Benavides, F and Castillo, J. Conjuntos suma pequeños en grupos hamiltonianos. *Revista de la unión matemática argentina*, 53(1), pag 1,(2012).

[9] Burton D. Elementary number theory, Mc. Graw Hill, New York. Ed. 6, pag 13-26, ISBN$-13 : 97-0-07-305188-8$, pag 61-63. (2007).

[10] Gallian, J. Contemporary Abstract Algebra, Brooks/Cole, Cengage Learning, EEUU. Ed. 7, ISBN$-13 : 978-0-547-16509-7$, pag 40-235. (2010).

[11] Lezama, O. Cuadernos de Álgebra, (1), (2014).

[12] Eliahou, S and Kervaire, M. Some extensions of the Cauchy-Davenport theorem. *Electronic Notes in Discrete Mathematics*, 28, pag 557-564,(2007).

[13] Wheeler,J. P. The cauchy-davenport theorem for finite groups, *arXiv preprint arXiv:* 1202.1816, (2012).

[14] Kemperman, J. On complexes in a semigroup. *In Indagationes Mathematicae*, 59, pag 247-254, (1956).

[15] Eliahou, S and Kervaire, M. The small sumsets property for solvable finite groups. *European Journal of Combinatorics*, 27(7), pag 1102-1110,(2006).

[16] Eliahou, S and Kervaire, M. Sumsets in dihedral groups. *European Journal of Combinatorics*, 27(4), pag 617-628, (2006).

[17] Olson, J. On the sum of two sets in a group. *Journal of Number Theory*, 18(1), pag 110-120, (1984).

[18] Zémor, G. A generalisation to noncommutative groups of a theorem of Mann. *Discrete Mathematics*, 126(1-3), pag 365-372, (1994).

[19] Vosper, A. G. The critical pairs of subsets of a group of prime order. *Journal of the London Mathematical Society*, 1(2), pag 200-205, (1956).