CONJUNTOS SUMA PEQUEÑOS EN GRUPOS FINITOS NO ABELIANOS

EDUAR ALIRIO ERAZO ORTIZ

SERGIO ALDEMAR MORA PORTILLA

UNIVERSIDAD DE NARIÑO

FACULTAD DE CIENCIAS EXACTAS Y NATURALES

DEPARTAMENTO DE MATEMÁTICAS Y ESTADÍSTICA

LICENCIATURA EN MATEMÁTICAS

SAN JUAN DE PASTO

2011

CONJUNTOS SUMA PEQUEÑOS EN GRUPOS FINITOS NO ABELIANOS

EDUAR ALIRIO ERAZO ORTIZ

SERGIO ALDEMAR MORA PORTILLA

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

Asesor: Wilson Fernando Mutis Cantero
Magister en Matemáticas

UNIVERSIDAD DE NARIÑO
FACULTAD DE CIENCIAS EXACTAS Y NATURALES
DEPARTAMENTO DE MATEMÁTICAS Y ESTADÍSTICA
LICENCIATURA EN MATEMÁTICAS
SAN JUAN DE PASTO
2011

Nota de Aceptación

Jurado

Jurado

Asesor

San Juan de Pasto, Noviembre de 2011

NOTA DE RESPONSABILIDAD

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 1966 emanado del Honorable Consejo Directivo de la Universidad de Nariño.

AGRADECIMIENTOS

Con este trabajo queremos expresar nuestros mas sinceros agradecimientos a todas aquellas personas que de alguna manera han contribuido a la culminación del mismo. A nuestro asesor y amigo Mg. Wilson Fernando Mutis, quien con su conocimiento y trayectoria en el campo de la investigación sirvió de guía en cada una de las etapas del presente trabajo. Al Mg. Fernando Andrés Benavides por su interés y apoyo incondicional en el desarrollo de este trabajo. A los profesores del Departamento de Matemáticas y Estadística de la Universidad de Nariño por sus valiosas enseñanzas. Finalmente agradecemos a todos nuestros familiares, en especial a nuestros padres y hermanos quienes con su apoyo, compañía y comprensión impulsaron constantemente nuestro deseo por alcanzar esta importante meta.

INTRODUCCIÓN

Sea $(G, \cdot)$ un grupo. El conjunto suma de dos subconjuntos no vacíos A y B de G, denotado con $A \cdot B$, esta dado por

$$A \cdot B = \{a \cdot b \,/\, a \in A \text{ y } b \in B\}.$$

Un problema de interés en Teoría Aditiva de Números, denominado el problema de los conjuntos suma pequeños es el siguiente: dados un grupo G y dos enteros r, s tales que $1 \leq r, s \leq |G|$, determinar una fórmula explícita que permita calcular el mínimo de los cardinales $|A \cdot B|$, donde A y B son subconjuntos de G de cardinales r y s respectivamente. Es decir, se desea hallar una fórmula que permita calcular el valor de la función

$$\mu_G \,:\, [1, |G|] \times [1, |G|] \longmapsto \mathbb{N}$$

definida por

$$\mu_G(r, s) = \min \{|A \cdot B| \,/\, A, B \subseteq G,\ |A| = r \text{ y } |B| = s\}.$$

La función μ_G ha sido determinada completamente para el caso en que G es un grupo abeliano arbitrario, y para algunas clases específicas de grupos finitos no abelianos, en particular, se ha demostrado que la fórmula para μ_G obtenida en el caso en que G es un grupo abeliano se cumple para todo grupo diédrico finito, para algunos grupos hamiltonianos y para todo p-grupo finito. Durante la investigación se hizo un estudio monográfico de la función μ_G en grupos finitos no abelianos, se implementaron algoritmos en el sistema de computación algebraico GAP que permitieron observar algunos resultados de tipo recursivo, además, se logró obtener nuevos resultados sobre la teoría de la función μ_G en algunos grupos que se pueden expresar como producto directo de otros.

El presente trabajo es el fruto de la investigación que los autores realizaron bajo la asesoría del Mg. Wilson Fernando Mutis Cantero, como requisito parcial para optar al título de licenciado en matemáticas de la Universidad de Nariño. Para su ejecución, se realizó un estudio sobre la teoría de grupos no abelianos, en particular la que refiere a grupos solubles, se hizo un análisis minucioso de los artículos de Eliahou y Kervaire (ver [Eliahou & Kervaire, 2007], [Eliahou & Kervaire, 2006], [Eliahou & Kervaire, 2006],

[Eliahou & Kervaire, 2010], [Eliahou & Kervaire, 2007]), como también los artículos de Benavides, Castillo y Mutis (ver [Benavides, Castillo & Mutis, 2009], [Benavides, Castillo & Mutis, 2010]), sobre la teoría de la función μ_G en grupos no abelianos.

El trabajo está dividido en cuatro capítulos. En el primero se establecen la notación y definiciones generales, además se hace la presentación del problema de los conjuntos suma pequeños, y se enuncian algunos resultados clásicos en Teoría de Números, los cuales se emplearan en el desarrollo del trabajo, por último se enuncian los principales resultados sobre la función μ_G en grupos abelianos. El segundo capítulo se dedica al estudio de los resultados obtenidos por Eliahou y Kervaire para la función μ_G en grupos solubles finitos, y su aplicación a grupos diédricos. En el capítulo siguiente se presenta el estudio realizado por Benavides, Castillo y Mutis sobre el problema de los conjuntos suma pequeños, en p-grupos finitos y grupos hamiltonianos finitos. El cuarto capítulo es el mas importante para los autores, porque se muestran los resultados obtenidos durante la investigación. En la primera sección de este capítulo se hace la presentación de los avances alcanzados en ciertos grupos solubles finitos, y en la segunda sección se muestran los resultados obtenidos en determinados grupos infinitos que se pueden escribir como producto directo de otros.

Finalmente, se presentan como apéndice algunos algoritmos implementados en el sistema computacional algebraico GAP, que permitieron visualizar algunos de los resultados obtenidos.

TABLA DE CONTENIDO

Capítulo 1

CONJUNTOS SUMA PEQUEÑOS

En este capítulo se establecen los conceptos generales y la notación que se utilizará en el presente trabajo. Además, se presenta el problema de los conjuntos suma pequeños junto con algunos resultados clásicos en la Teoría de Números, como son los teoremas de Cauchy-Davenport, Kneser y Olson. Por otro lado se enuncian algunas propiedades básicas de la función μ_G. Finalmente, se dan a conocer los resultados más relevantes que permitieron obtener una fórmula explícita para la función μ_G en grupos abelianos arbitrarios.

1.1. NOTACIÓN Y CONCEPTOS GENERALES

Si G es un conjunto, su cardinal se denotará por $|G|$. Dado un entero n mayor que uno, el grupo cíclico $\mathbb{Z}/n\mathbb{Z}$, de congruencias módulo n, se denotará con el conjunto $\mathbb{Z}_n$. Si p es un número primo y n es un entero positivo, el campo finito con p^n elementos se identificará mediante $\mathbb{F}_{p^n}$, en particular para $n = 1$, $\mathbb{F}_p = \mathbb{Z}_p$.

En un grupo G, mediante $\mathscr{H}(G)$ se denotará el conjunto de todos los ordenes de subgrupos finitos de G, es decir,

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

Definición 1.1. Conjunto suma
Sea $(G, \cdot)$ un grupo y sean A y B dos subconjuntos de G, no vacíos. El conjunto suma de A y B denotado por $A \cdot B$, o simplemente AB, es el conjunto de todos los elementos en G de la forma $a \cdot b$, donde $a \in A$ y $b \in B$. Es decir,

$$A \cdot B = \{a \cdot b \,/\, a \in A,\ b \in B\}.$$

Si $A = \emptyset$ o $B = \emptyset$, se define $A \cdot B = \emptyset$. Además, si $\{a\}$ es el singular de A, el conjunto suma $A \cdot B$ se escribirá como $a \cdot B$.

Definición 1.2. Subgrupo normal
Un subgrupo N de un grupo G es normal, si para todo $x \in G$ se tiene que $xNx^{-1} \subseteq N$. Esto se denota con $N \trianglelefteq G$.

Definición 1.3. Serie Subnormal y Serie Normal
Una serie subnormal de un grupo G es una sucesión finita

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

de subgrupos de G, tal que para toda $i = 1, 2, \ldots, n$ se tiene que H_i es un subgrupo normal de H_{i-1}. Una serie normal de un grupo G es una serie subnormal donde todos los subgrupos de la serie son subgrupos normales de G. En una serie subnormal (o normal) los grupos cocientes H_{i-1}/H_i, $i = 1, 2, \ldots, n$, reciben el nombre de grupos factores de la serie.

Definición 1.4. Serie de Composición y Serie Principal
Una serie subnormal de un grupo G es una serie de composición de G si todos los grupos factores son simples; es decir, si todos los grupos factores no tienen subgrupos normales no triviales. Una serie normal de un grupo G es una serie principal de G si todos los grupos factores son simples.

Definición 1.5. Grupo soluble
Un grupo G, se denomina soluble si G tiene una serie normal

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

en la que cada grupo factor H_{i-1}/H_i, $i = 1, 2, \ldots, n$, es abeliano.

Teorema 1.1. Un grupo de orden finito es soluble si y solo si los grupos factores en una serie de composición de G son cíclicos de orden primo.

Definición 1.6. Grupo nilpotente

Un grupo G es nilpotente si posee una serie normal finita

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

en la que H_{i-1}/H_i está en el centro de G/H_i para $i = 1, 2, \ldots, n$.

Definición 1.7. 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.

Definición 1.8. Función techo

Sea $\xi \in \mathbb{R}$, el techo de ξ denotado con $\lceil \xi \rceil$, es el menor entero x que no es menor que ξ, es decir $\lceil \xi \rceil = x$ si y sólo si $x \in \mathbb{Z}$ y $x - 1 < \xi \leq x$.

En el presente trabajo se utilizará con frecuencia la siguiente función aritmética:

Definición 1.9. La función κ_G

Sean G un grupo y r, s enteros no negativos tales que $r, s \leq |G|$. Con $\kappa_G(r, s)$ se denota el siguiente número entero

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

Definición 1.10. Segmento inicial

Sea $(G, <)$ un conjunto totalmente ordenado con elemento mínimo a_0. Un subconjunto ordenado $A = \{a_0 < a_1 < \ldots < a_{t-1}\}$ de G, se llama segmento inicial de longitud t si para toda $i \in \{0, 1, \ldots, t-2\}$ se tiene que no existe $x \in G$ tal que $a_i < x < a_{i+1}$. El conjunto $A = \emptyset$ es el segmento inicial de longitud cero.

Un segmento inicial en $L = \mathbb{F}_{p^v}$ es un subconjunto de la forma

$$I[a] = \{x \in L / x \leq a\}$$

para algún $a \in L$. Para cualquier entero $0 \leq r \leq p^v$, se denota por IS(r) el único segmento inicial en L de cardinalidad r.

A continuación se presenta la prueba de la fórmula utilizada para la suma de dos segmentos iniciales en L, la cual es necesaria para la prueba de la proposición 2.2.

Lema 1.1. En $L = \mathbb{F}_{p^v}$ ordenado lexicográficamente, se tiene que

$$\mathsf{IS}(t) + \mathsf{IS}(u) = \mathsf{IS}(\kappa_L(t, u))$$

para todos los enteros $0 \leq t, u \leq p^v$.

Demostración. En la prueba, $[0, k]$ denota el conjunto $\{0,\ 1, \ldots,\ k\}$ si k es un entero no negativo y $\emptyset$ si $k < 0$. Se puede asumir que $t, u \geq 1$.

La prueba procede por inducción sobre v. La afirmación es trivial para $v = 1$, ya que en $\mathbb{F}_p$ identificado con $[0, p-1]$ se sigue que

$$\{0,\ 1, \ldots,\ t-1\} + \{0,\ 1, \ldots,\ u-1\} = \{0,\ 1, \ldots,\ \mathrm{mín}(p, t+u-1)-1\},$$

y $\kappa_{\mathbb{F}_p}(t, u) = \mathrm{mín}(p, t+u-1)$ por definición de la función numérica $\kappa_{\mathbb{F}_p}$. Ahora, se asume que $v \geq 2$ y se divide el argumento en varios pasos.

Paso 1. Sea $a = (a_1, \ldots, a_v) \in L$. Entonces
$I[a] = \{(x_1, x_2, \ldots,\ x_n)/x_1 < a_1\} \cup \{(x_1, x_2, \ldots,\ x_n)/x_1 = a_1, x_2 < a_2\} \cup \ldots \cup \{(x_1, x_2, \ldots,\ x_n)/x_i = a_i, x_n < a_n, \forall i = 1. \ldots . n-1\} \cup \{(a_1, \ldots,\ a_n)\}$, luego

$$|I[a]| = 1 + \sum_{i=1}^{n} |\{(x_1, \ldots,\ x_n)/x_i < a_i, x_k = a_k, \textit{para } k \leq i-1\}|,$$

y dado que $|\{(x_1, \ldots,\ x_n)/x_i < a_i, x_k = a_k, \textit{para } k \leq i-1\}| = a_i pp \ldots\ p = a_i p^{n-i}$, entonces $I[a]$ tiene cardinalidad

$$|I[a]| = a_1 p^{v-1} + a_2 p^{v-2} + \cdots + a_v + 1.$$

Equivalentemente, se tiene la fórmula

$$I[a] = \mathsf{IS}(a_1 p^{v-1} + a_2 p^{v-2} + \cdots + a_v + 1).$$

De hecho, usando la definición de $I[a] = \{x \in L/x \leq a\}$ y el orden lexicográfico de L, se obtiene la partición

$$I[(a_1, \ldots, a_v)] = [0, a_1 - 1] \times \mathbb{F}_{p^{v-1}} \bigsqcup \{a_1\} \times I[(a_2, \ldots, a_v)],$$

donde $\sqcup$ denota la unión de conjuntos disjuntos por pares. Esto da las fórmulas de recurrencia, para $v \geq 2$

$$|I[(a_1, \ldots, a_v)]| = a_1 p^{v-1} + |I[(a_2, \ldots, a_v)]|\,,$$

y $|I[(a_v)]| = a_v + 1$ con $a_v \in \mathbb{F}_p$.

Paso 2. Sean $\mathsf{IS}(t) = I[(a_1, \ldots, a_v)],\ \mathsf{IS}(u) = I[(b_1, \ldots, b_v)]$ dos segmentos iniciales en L de longitudes t y u, respectivamente. Entonces

$$|\mathsf{IS}(t) + \mathsf{IS}(u)| = \kappa_L(t, u).$$

Paso 2.1. Sea $a_1 + b_1 \geq p$ (como enteros). Luego

$$|\mathsf{IS}(t) + \mathsf{IS}(u)| = p^v = \kappa_L(t, u).$$

De hecho, por el Paso 1 se tiene que

$$\begin{aligned} |I[(a_1, \ldots, a_v)]| + |I[(b_1, \ldots, b_v)]| &= (a_1 p^{v-1} + \ldots + a_v + 1) + (b_1 p^{v-1} + \ldots + b_v + 1) \\ &= (a_1 + b_1)p^{v-1} + (a_2 + b_2)p^{v-2} + \ldots + (a_v + b_v) + 2 \\ &\geq (a_1 + b_1)p^{v-1} + 2 > p^v = |L|. \end{aligned}$$

De ello se deduce que

$$|I[(a_1, \ldots, a_v)]| + |I[(b_1, \ldots, b_v)]| = L.$$

Para establecer la fórmula $\kappa_L(t, u) = p^v$, es suficiente mostrar que para cualquier entero $0 \leq k \leq v - 1$ se tiene que

$$\left(\left\lceil \frac{t}{p^k} \right\rceil + \left\lceil \frac{u}{p^k} \right\rceil - 1 \right) p^k > p^v.$$

Se sabe que

$$\kappa_L(r, s) = \min_{h \in \mathscr{H}(L)} \left\{ \left(\left\lceil \frac{r}{h} \right\rceil + \left\lceil \frac{s}{h} \right\rceil - 1 \right) h \right\},$$

donde $\mathscr{H}(L)$ es el conjunto de ordenes de subgrupos finitos de L, y dado que $|L| = p^v$ y $0 \leq k \leq v-1$ existe $H \leq L$ con $|H| = p^k$, de manera que

$$\left(\left\lceil \frac{t}{p^k} \right\rceil + \left\lceil \frac{u}{p^k} \right\rceil - 1 \right) p^k > p^v.$$

(Observe que para $k = v$ se tiene que $\left(\left\lceil \frac{t}{p^v} \right\rceil + \left\lceil \frac{u}{p^v} \right\rceil - 1 \right) p^v = p^v$).

Por el Paso 1, se sigue que

$$t = \sum_{i=1}^{v} a_i p^{v-i} + 1,$$

donde claramente

$$t = \sum_{i=1}^{v} a_i p^{v-i} + 1 \geq a_1 p^{v-1} + 1$$

y por tanto,

$$\left\lceil \frac{t}{p^k} \right\rceil \geq \left\lceil \frac{a_1 p^{v-1} + 1}{p^k} \right\rceil = \left\lceil a_1 p^{v-1-k} + \frac{1}{p^k} \right\rceil = a_1 p^{v-1-k} + 1,$$

del mismo modo

$$\left\lceil \frac{u}{p^k} \right\rceil \geq \left\lceil \frac{b_1 p^{v-1} + 1}{p^k} \right\rceil = \left\lceil b_1 p^{v-1-k} + \frac{1}{p^k} \right\rceil = b_1 p^{v-1-k} + 1.$$

De ahí que

$$\begin{aligned}
\left(\left\lceil \frac{t}{p^k} \right\rceil + \left\lceil \frac{u}{p^k} \right\rceil - 1 \right) p^k &\geq \left(a_1 p^{v-1-k} + 1 + b_1 p^{v-1-k} + 1 - 1 \right) p^k \\
&\geq a_1 p^{v-1} + b_1 p^{v-1} + p^k \\
&\geq (a_1 + b_1) p^{v-1} + p^k \\
&\geq p^v + p^k \\
&\geq p^v + 1 > p^v
\end{aligned}$$

como se quería. Por tanto

$$\kappa_L(t,u) = \left(\left\lceil \frac{t}{p^v} \right\rceil + \left\lceil \frac{u}{p^v} \right\rceil - 1 \right) p^v = p^v.$$

Paso 2.2. Ahora, si $a_1 + b_1 \leq p - 1$ (como enteros). Se procede a mostrar la igualdad $|\mathsf{IS}(t) + \mathsf{IS}(u)| = \kappa_L(t, u)$ por inducción sobre v.

Usando las descomposiciones en el Paso 1 para $I[(a_1, \ldots, a_v)]$ y $I[(b_1, \ldots, b_v)]$, es fácil llegar a la unión disjunta
$I[(a_1, \ldots, a_v)] + I[(b_1, \ldots, b_v)] = [0, a_1 + b_1 - 1] \times \mathbb{F}_{p^{v-1}} \bigsqcup \{a_1 + b_1\} \times (I[(a_2, \ldots, a_v)] + I[(b_2, \ldots, b_v)])$.

En consecuencia, se obtiene la fórmula

$$|I[(a_1, \ldots, a_v)] + I[(b_1, \ldots, b_v)]| = (a_1 + b_1)p^{v-1} + |I[(a_2, \ldots, a_v)] + I[(b_2, \ldots, b_v)]|.$$

Del paso 1, se desprende que

$$|I[(a_2, \ldots, a_v)]| = t - a_1 p^{v-1} \text{ y } |I[(b_2, \ldots, b_v)]| = u - b_1 p^{v-1}.$$

Por lo tanto, de la hipótesis de inducción se tiene que

$$\begin{aligned} |I[(a_2, \ldots, a_v)] + I[(b_2, \ldots, b_v)]| &= \min_{k \leq v-1} (\lceil (t - a_1 p^{v-1})/p^k \rceil + \lceil (u - b_1 p^{v-1})/p^k \rceil - 1)p^k \\ &= \min_{k \leq v-1} (\lceil (t/p^k \rceil + \lceil (u/p^k \rceil - 1)p^k - (a_1 p^{v-1-k} + b_1 p^{v-1-k})p^k \\ &= \min_{k \leq v-1} (\lceil (t/p^k \rceil + \lceil (u/p^k \rceil - 1)p^k - (a_1 p^{v-1} + b_1 p^{v-1}). \end{aligned}$$

Puesto que $\lceil m + x \rceil = \lceil m \rceil + \lceil x \rceil$, dado que $\lceil x \rceil = x' \in \mathbb{Z}$ si y solo si $x' - 1 < x \leq x'$, así, $x' + m - 1 < x + m \leq x' + m \in \mathbb{Z}$, lo cual implica que

$$\lceil x + m \rceil = x' + m = \lceil x \rceil + \lceil m \rceil.$$

Recogiendo las fórmulas anteriores, se obtiene que

$$\begin{aligned} |I[(a_1, \ldots, a_v)] + I[(b_1, \ldots, b_v)]| &= (a_1 + b_1)p^{v-1} + |I[(a_2, \ldots a_v)] + I[(b_2, \ldots, b_v)]| \\ &= (a_1 + b_1)p^{v-1} + \min_{k \leq v-1} (\lceil t/p^k \rceil + \lceil u/p^k \rceil - 1)p^k \\ &\quad - (a_1 p^{v-1} + b_1 p^{v-1}) \\ &= \min_{k \leq v-1} (\lceil t/p^k \rceil + \lceil u/p^k \rceil - 1)p^k. \end{aligned}$$

Para mostrar que el resultado anterior puede extenderse a $k = v$, basta con comparar los casos $k = v - 1$ y $k = v$, y probar la desigualdad

$$(\lceil t/p^{v-1} \rceil + \lceil u/p^{v-1} \rceil - 1)p^{v-1} \leq p^v = (\lceil t/p^v \rceil + \lceil u/p^v \rceil - 1)p^v.$$

(La segunda igualdad ya se ha observado.) Para $k = v - 1$, se deduce de las fórmulas

$$t = \sum_{i=1}^{v} a_i p^{v-i} + 1 \text{ y } u = \sum_{i=1}^{v} b_i p^{v-i} + 1$$

donde

$$\begin{aligned} \lceil t/p^{v-1} \rceil &= \lceil a_1 + a_2/p + \ldots + a_v/p^{v-1} + 1/p^{v-1} \rceil \\ &= a_1 + \lceil a_2/p^{v-1} + \ldots + a_v/p^{v-1} + 1/p^{v-1} \rceil, \end{aligned}$$

luego, si $a_i = p - 1$ para toda $i = 2, \ldots, v$ se tiene la serie

$$(1 - 1/p) + (1/p - 1/p^2) + (1/p^2 - 1/p^3) + \ldots + (1/p^{v-2} - 1/p^{v-1}) + 1/p^{v-1},$$

de modo que $0 < \lceil a_2/p + \ldots + a_v/p^{v-1} + 1/p^{v-1} \rceil \leq 1$, así que $\lceil t/p^{v-1} \rceil = a_1 + 1$ y $\lceil u/p^{v-1} \rceil = b_1 + 1$. Por lo tanto,

$$(\lceil t/p^{v-1} \rceil + \lceil u/p^{v-1} \rceil - 1)p^{v-1} = (a_1 + b_1 + 1)p^{v-1} \leq p^v,$$

como se deseaba.

Resumiendo lo anterior, se obtienen las igualdades

$$\begin{aligned} |I[(a_1, \ldots, a_v)] + I[(b_1, \ldots, b_v)]| &= \min_{k \leq v-1} (\lceil t/p^k \rceil + \lceil u/p^k \rceil - 1)p^k \\ &= \min_{k \leq v} (\lceil t/p^k \rceil + \lceil u/p^k \rceil - 1)p^k \\ &= \kappa_L(t, u). \end{aligned}$$

Paso 3. Para cualquier par de segmentos iniciales $\mathsf{IS}(t), \mathsf{IS}(u) \in L$, se tiene que

$$\mathsf{IS}(t) + \mathsf{IS}(u) = \mathsf{IS}(\kappa_L(t, u)).$$

Se ha mostrado en el Paso 2 que estos dos conjuntos tienen la misma cardinalidad. Ahora, el conjunto suma IS(t) + IS(u) es un segmento inicial en L, esto se deduce de las pruebas en el Paso 2. Si

$$\text{IS}(t) = I[(a_1, \ldots, a_v)] \text{ y } \text{IS}(u) = I[(b_1, \ldots, b_v)],$$

entonces

$$I[(a_1, \ldots, a_v)] + I[(b_1, \ldots, b_v)] = L$$

como en el Paso 2.1, o por una descomposición

$$I[(a_1, \ldots, a_v)] + I[(b_1, \ldots, b_v)] = [0, a_1 + b_1 - 1] \times \mathbb{F}_{p^{v-1}} \bigsqcup \{a_1 + b_1\} \times (I[(a_2, \ldots, a_v)] + I[(b_2, \ldots, b_v)]),$$

como en el Paso 2.2. Por inducción sobre v, se tiene que IS(t) + IS(u) es un segmento inicial en L. Por lo tanto

$$\text{IS}(t) + \text{IS}(u) = \text{IS}(\kappa_L(t, u)).$$

□

1.2. EL PROBLEMA DE LOS CONJUNTOS SUMA PEQUEÑOS

Sean G un grupo y r, s enteros no negativos tales que $r, s \leq |G|$, un problema de interés en Teoría Aditiva de Números, denominado *El Problema de los Conjuntos Suma Pequeños*, es minimizar el cardinal $|A \cdot B|$, sujeto a las condiciones $A, B \subseteq G$, $|A| = r$ y $|B| = s$.

Definición 1.11. Función μ_G

Sean G un grupo y r, s enteros no negativos tales que $r, s \leq |G|$. Por $\mu_G(r, s)$ se denota el mínimo de los cardinales $|A \cdot B|$, donde A y B son subconjuntos del grupo G tales que $|A| = r$ y $|B| = s$, es decir,

$$\mu_G(r, s) = \min \{|A \cdot B| \ / \ A, B \subseteq G, \ |A| = r \text{ y } |B| = s\}.$$

Además, se dice que los subconjuntos A y B de G realizan a $\mu_G(r,s)$ si $|A| = r$, $|B| = s$ y $|A \cdot B| = \mu_G(r,s)$.

Así, el problema de los conjuntos suma pequeños, consiste en hallar el valor de $\mu_G(r,s)$. Determinar directamente el valor de $\mu_G(r,s)$ 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 $\mu_G(r,s)$.

Uno de los primeros resultados que se puede enmarcar dentro de esta problemática, es el teorema de Cauchy-Davenport, probado por Cauchy en 1813 y redescubierto en forma independientemente por Davenport en 1935.

Teorema 1.2. Cauchy-Davenport
Sea p un número primo. Si A y B son dos subconjuntos no vacíos del grupo cíclico $\mathbb{Z}_p$, entonces

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

Una consecuencia inmediata del teorema anterior es le siguiente teorema:

Teorema 1.3. Si p es un número primo y $G = \mathbb{Z}_p$, entonces para todo par de enteros r y s tales que $1 \leq r, s \leq p$ se tiene que

$$\mu_G(r,s) = \text{mín}\left\{p, r+s-1\right\}.$$

Entre las diversas generalizaciones del teorema de Cauchy-Davenport quizá la más importante es el teorema de Kneser que enunciamos a continuación.

Teorema 1.4. Kneser
Sea G un grupo abeliano. Si A y B son dos subconjuntos finitos no vacíos de G y $|A+B| \leq |A|+|B|$, entonces existe un subgrupo finito S de G tal que

$$|A+B| \geq |A+S| + |B+S| - |S|.$$

El teorema de Kneser implica el teorema de Cauchy-Davenport porque el grupo cíclico $\mathbb{Z}_p$, con p primo, no tiene subgrupos propios no triviales.

Teorema 1.5. Olson

Sean A y B dos subconjuntos finitos no vacíos de un grupo G. Entonces existe un subgrupo finito H de G y un subconjunto no vacío S de AB tales que

$$|AB| \geq |S| \geq |A| + |B| - |H|,$$

y $HS = S$ o $SH = S$.

Teorema 1.6. Feit-Thompson

Todo grupo finito de orden impar es soluble.

1.2.1. PROPIEDADES BÁSICAS DE LA FUNCIÓN μ_G

A continuación se presentan como lemas, una serie de resultados probados en [Eliahou, Kervaire & Plagne, 2003] y [Eliahou & Kervaire, 2007], ilustrando otra forma de buscar la solución al problema de los conjuntos suma pequeños.

Lema 1.2. Si G es un grupo y r, s son enteros tales que $0 \leq r, s \leq |G|$, entonces $\mu_G(r, s) = \mu_G(s, r)$.

Lema 1.3. Si G es un grupo y r, s son enteros tales que $1 \leq r, s \leq |G|$, entonces $\mu_G(r, s) \geq \max\{r, s\}$.

Lema 1.4. Sean G un grupo y r un entero tal que $1 \leq r \leq |G|$. Entonces $\mu_G(r, r) = r$ si y sólo si G contiene un subgrupo de orden r.

Como el grupo alternante A_4 de orden 12 no contiene subgrupos de orden seis, a la luz del lema 1.4 se tiene que $\mu_{A_4}(6, 6) \neq 6$.

Lema 1.5. Sea G un grupo finito y r, s enteros tales que $1 \leq r, s \leq |G|$.

1. Si $r + s > |G|$, entonces $\mu_G(r, s) = \kappa_G(r, s) = |G|$.
2. Si $r + s = |G|$, entonces $\mu_G(r, s) = \kappa_G(r, s)$.
3. Si $r + s = |G| - 1$, entonces $\mu_G(r, s) \leq \kappa_G(r, s)$.

4. 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,se tiene la siguiente equivalencia:

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

para todos los enteros i tales que $0 \leq i < \frac{r}{2}$.

5. Si $\kappa_G(r,s) = s + \left\lceil \frac{r}{2} \right\rceil$, entonces $\mu_G(r,s) \geq \kappa_G(r,s)$.

6. Si $1 \leq r \leq 3$ entonces $\mu_G(r,s) = \kappa_G(r,s)$.

1.3. LA 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 1998, Eliahou y Kervaire (ver [Eliahou & Kervaire, 1998]) mostraron que en el grupo cíclico $G = (\mathbb{Z}_p)^n$, con p primo, se tiene que

$$\mu_G(r,s) = \min\left\{k \,/\, (x+y)^k \in (x^r, y^s) \text{ en } \mathbb{F}_p[x,y]\right\}.$$

donde (x^r, y^s) denota el ideal generado en el anillo de polinomios $\mathbb{F}_p[x,y]$.

Plagne (ver [Plagne, 2007]) demostró que si n es un entero positivo y $G = \mathbb{Z}_n$, entonces se cumple la fórmula

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

Posteriormente, Eliahou, Kervaire y Plagne (ver [Eliahou, Kervaire & Plagne, 2003]) extendieron el resultado anterior para todo grupo abeliano finito. Es conveniente tener en cuenta que si G es un grupo abeliano finito, entonces existen enteros $n_1, n_2, \ldots, n_k > 1$ tales que $G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$. Por otro lado, el grupo cíclico $\mathbb{Z}_{n_i} = \{0, 1, \ldots, n_i - 1\}$ se puede ver como un conjunto ordenado según el orden natural en el conjunto $\mathbb{Z}$ de los

números enteros y de esta manera es posible dotar al grupo G del orden lexicográfico, es decir, dados dos elementos $x = (x_1, x_2, \ldots, x_k)$ y $w = (w_1, w_2, \ldots, w_k)$ se dice que $x < w$, si y sólo si, existe $i \in \{1, 2, \ldots, k\}$ tal que se cumplen las dos condiciones siguientes:

1. $x_j = w_j$ siempre que $j < i$.

2. $x_i < w_i$.

En 2003, Plagne prueba la siguiente desigualdad:

Lema 1.6. Desigualdad de Plagne

Sea G un grupo abeliano finito de orden n. Si r y s son dos enteros positivos tales que $r, s \leq n$, entonces

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

Demostración. Ver [Plagne, 2003].

Lema 1.7. Desigualdad de Eliahou y Kervaire

Sea G un grupo abeliano finito y sea $G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$ una descomposición de G como producto directo de grupos cíclicos. Si se ordena G según el orden lexicográfico y $A, B \subseteq G$ son dos segmentos iniciales no vacíos de G, entonces $|A+B| \leq |A|+|B|-1$.

Demostración. Ver [Eliahou, Kervaire & Plagne, 2003].

Teorema 1.7. Eliahou, Kervaire y Plagne

Sea G un grupo abeliano finito de orden n. Si r y s son dos enteros positivos tales que $r, s \leq n$, entonces

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

Demostración. Ver [Eliahou, Kervaire & Plagne, 2003].

En 2005 Eliahou y Kervaire (ver [Eliahou & Kervaire, 2005]) y posteriormente Plagne en 2007 (ver [Plagne, 2007]), trabajando independientemente lograron determinar una fórmula explícita para la función μ_G cuando G es un grupo abeliano arbitrario. Ellos demostraron el siguiente teorema:

Teorema 1.8. Si G es un grupo abeliano, entonces

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

El problema de encontrar una fórmula explícita para la función μ_G es un tema de estudio en el que últimamente se han obtenido resultados significativos, en el siguiente capítulo se presentan los teoremas que han obtenido Eliahou y Kervaire en el estudio de la función μ_G. En particular, se muestran algunos resultados obtenidos en grupos solubles y su aplicación en grupos diédricos.

Capítulo 2

LA FUNCIÓN μ_G EN GRUPOS SOLUBLES

En este capítulo se presentan los resultados que Eliahou y Kervaire han obtenido en el estudio de la función μ_G para el caso en que G es un grupo soluble. Inicialmente se expone el estudio de cotas superiores para la función μ_G en grupos solubles, en seguida se describen las cotas inferiores obtenidas para estos grupos. Además, una aplicación interesante de este capitulo es la completa determinación de la función μ_G para el grupo diédrico $G = D_n$ de orden $2n$ para toda $n \geq 1$.

2.1. COTAS SUPERIORES PARA LA FUNCIÓN μ_G

Según el teorema 1.8, si G es un grupo abeliano y r, s son dos enteros positivos tales que $r, s \leq |G|$, entonces $\mu_G(r, s) = \kappa_G(r, s)$, sin embargo, en grupos no abelianos esta igualdad, en general, no se tiene.

En un grupo soluble finito G, Eliahou y Kervaire en [Eliahou & Kervaire, 2006], probaron que para todo par de enteros positivos $r, s \leq |G|$ se tiene la desigualdad $\mu_G(r, s) \leq r + s - 1$.

Definición 2.1. Propiedad del conjunto suma pequeño
Se dice que un grupo finito G tiene la propiedad del conjunto suma pequeño si para cada par de enteros positivos $r, s \leq |G|$ existen subconjuntos $A, B \subseteq G$ tales que $|A| = r$, $|B| = s$ y $|AB| \leq r + s - 1$.

A continuación se muestra que todo grupo soluble finito tiene *La propiedad del conjunto suma pequeño, para ello se hace uso del siguiente resultado:*

Teorema 2.1. Sea $\{1\} \longrightarrow F \xrightarrow{\lambda} G \xrightarrow{\pi} \mathscr{C} \longrightarrow \{1\}$ una secuencia exacta de grupos finitos, esto es λ y π son homomorfismos de grupos tales que λ es inyectivo, π es suprayectivo e $Im(\lambda) = ker(\pi)$. Si el grupo F tiene la propiedad del

conjunto suma pequeño y $\mathscr{C}$ es un grupo cíclico, entonces G tiene la propiedad del conjunto suma pequeño.

Demostración. Ver [Eliahou & Kervaire, 2006].

Por construcción se tiene el siguiente teorema:

Teorema 2.2. Si G es un grupo finito soluble, entonces G tiene la propiedad del conjunto suma pequeño.

Demostración. Por el teorema 1.1, el grupo G tiene una serie de composición

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

donde para toda $i = 1, 2, \ldots, n$ los grupos factores H_{i-1}/H_i son cíclicos, entonces H_{n-1} es cíclico, y por el lema 1.7 se sigue que H_{n-1} tiene la propiedad del conjunto suma pequeño. Considérese la siguiente secuencia exacta de grupos finitos:

$$\{1\} \longrightarrow H_{n-1} \xrightarrow{\iota} H_{n-2} \xrightarrow{\pi} H_{n-2}/H_{n-1} \longrightarrow \{1\}$$

donde ι es la inclusión de H_{n-1} en H_{n-2} y π es el epimorfismo natural. Por el teorema 2.1 se sigue que H_{n-2} tiene la propiedad del conjunto suma pequeño. Ahora considérese la secuencia exacta

$$\{1\} \longrightarrow H_{n-2} \xrightarrow{\iota} H_{n-3} \xrightarrow{\pi} H_{n-3}/H_{n-2} \longrightarrow \{1\}$$

donde ι es la inclusión de H_{n-2} en H_{n-3} y π es el epimorfismo natural. Dado que H_{n-2} tiene la propiedad del conjunto suma pequeño y H_{n-3}/H_{n-2} es cíclico, el teorema 2.1 implica que H_{n-3} tiene la propiedad del conjunto suma pequeño. Continuando de esta forma, en un número finito de pasos, se obtiene el resultado del teorema. □

Como consecuencia inmediata del teorema anterior se tiene el siguiente corolario:

Corolario 2.1. Si G es un grupo finito soluble, entonces para todo par de enteros r y s, tales que $1 \leq r, s \leq |G|$ se tiene que $\mu_G(r, s) \leq r + s - 1$.

En 2006, Eliahou y kervaire extienden el resultado a grupos finitos no necesariamente solubles.

Teorema 2.3. Sea G un grupo finito y sean r, s dos enteros tales que $1 \leq r, s \leq |G|$. Si G tiene un subgrupo H de orden $d \geq r$ que satisface la propiedad del conjunto suma pequeño, entonces $\mu_G(r, s) \leq r + s - 1$.

Demostración. Ver [Eliahou & Kervaire, 2006].

Lema 2.1. Sea G un grupo soluble finito y sean r y s enteros tales que $1 \leq r, s \leq |G|$. Si k es el orden de un subgrupo normal K de G, entonces

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

Demostración. Sean $G_0 = G/K$, $r_0 = \left\lceil \frac{r}{k} \right\rceil$ y $s_0 = \left\lceil \frac{s}{k} \right\rceil$. Así $1 \leq r_0, s_0 \leq |G_0|$, y dado que G es soluble se tiene que G_0 es soluble. El corolario 2.1 implica

$$\mu_{G_0}(r_0, s_0) \leq r_0 + s_0 - 1.$$

Sean A_0 y B_0 dos subconjuntos de G_0 que realizan $\mu_{G_0}(r_0, s_0)$. Sea $\pi : G \to G_0$ el homomorfismo natural y considérense los siguientes subconjuntos de G:

$$A' = \pi^{-1}(A_0) \quad \text{y} \quad B' = \pi^{-1}(B_0),$$

luego $|A'| = |A_0|\,|K| = r_0 k$ y $|B'| = |B_0|\,|K| = s_0 k$. Dado que $r_0 \geq \frac{r}{k}$ y $s_0 \geq \frac{s}{k}$, se sigue que $|A'| \geq r$ y $|B'| \geq s$. Del hecho que π es un homomorfismo sobreyectivo se obtiene

$$|A'B'| = (r_0 + s_0 - 1)k = \left(\left\lceil \frac{r}{k} \right\rceil + \left\lceil \frac{s}{k} \right\rceil - 1 \right) k.$$

Sean $A \subset A'$ y $B \subset B'$ tales que $|A'| = r$ y $|B'| = s$, se sigue que

$$\mu_G(r, s) \leq |AB| \leq |A'B'| = \left(\left\lceil \frac{r}{k} \right\rceil + \left\lceil \frac{s}{k} \right\rceil - 1 \right) k.$$

□

Definición 2.2. Función kappa normal

Sea G un grupo y r, s dos enteros no negativos tales que $r, s \leq |G|$, entonces se define la función kappa normal como

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

donde

$$\mathscr{N}(G) = \{h \in \mathbb{N}/h \text{ es el orden de un subgrupo normal finito de } G\}.$$

Por el lema 2.1 y por la definición 2.2 se tiene el siguiente corolario:

Corolario 2.2. Sea G un grupo soluble finito y sean r, s dos enteros positivos tales que $r, s \leq |G|$. Entonces

$$\mu_G(r,s) \leq \mathscr{N}\kappa_G(r,s).$$

2.2. COTAS INFERIORES PARA LA FUNCIÓN μ_G

A continuación se presentan los argumentos que permitieron establecer una cota inferior para μ_G cuando G es un grupo soluble finito, para ello es importante tener en cuenta las siguientes definiciones introducidas por Eliahou y Kervaire:

Definición 2.3. Función kappa débil

Sea G un grupo y t un entero positivo. Por $\mathscr{H}_t(G)$ se denota el conjunto de órdenes h de un subgrupo finito de G que satisface $h \leq t$. Dados dos enteros no negativos $r, s \leq |G|$, entonces se define la función kappa débil como

$$\mathscr{W}\kappa_G(r,s) = \min_{h\in\mathscr{H}'} \left(\left\lceil \frac{r+s}{h} \right\rceil - 1 \right) h$$

donde

$$\mathscr{H}' = \mathscr{H}_{r+s-1}(G) = \{h \in \mathscr{H}(G)/h \leq r+s-1\}.$$

Teorema 2.4. Sea G un grupo, y sean r, s dos enteros positivos tales que $1 \leq r, s \leq |G|$. Entonces

$$\mu_G(r,s) \geq \mathscr{W}\kappa_G(r,s).$$

Demostración. Dados los enteros positivos $r, s \leq |G|$, sean $A, B \subset G$, de cardinales r, s respectivamente. Sean $S \subset AB$ y H un subgrupo finito de G, como en el teorema de Olson. Entonces

$$|AB| \geq |S| \geq r + s - |H|$$

donde $HS = S$ o $SH = S$. Así que S debe ser la unión disjunta de clases laterales izquierdas o derechas de H. Sea $|H| = h$, entonces $|S|$ es un múltiplo de h, es decir $|S| = qh$ para algún entero positivo q. En consecuencia, se tiene que

$$|AB| \geq |S| = qh \geq r + s - h.$$

Ahora, considérese los siguientes casos:

Caso 1. Sea $h \geq r + s$. Como $\mathscr{H}'$ contiene $h = 1$, se sigue que

$$\mathscr{W}\kappa_G(r, s) \leq r + s - 1.$$

De ahí que

$$|AB| \geq qh \geq r + s > \mathscr{W}\kappa_G(r, s).$$

Caso 2. Sea $h \leq r + s - 1$. Entonces $h \in \mathscr{H}'$ y $|S| = qh \geq r + s - h$, de donde $q \geq \dfrac{(r+s)}{h} - 1$. Puesto que q es entero, se tiene que $q \geq \left\lceil \dfrac{r+s}{h} \right\rceil - 1$.

Por lo tanto,

$$|AB| \geq qh \geq \left(\left\lceil \frac{r+s}{h} \right\rceil - 1 \right) h.$$

Como $h \in \mathscr{H}'$, se concluye que $|AB| \geq \mathscr{W}\kappa_G(r, s)$. □

Definición 2.4. Función $\mathscr{D}\kappa_G$

Dado un grupo G y dos enteros $r, s \leq |G|$, entonces se define la función $\mathscr{D}\kappa_G$ como

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

donde $\mathscr{D}(G) = \{d \in \mathbb{N} / d$ es un divisor del orden h de un subgrupo finito de $G\}$.

Note que si G es abeliano entonces $\mathscr{D}(G) = \mathscr{H}(G)$, por lo tanto $\mathscr{D}\kappa_G(r,s) = \kappa_G(r,s)$ para todos los enteros $1 \leq r, s \leq |G|$.

Teorema 2.5. Sea G un grupo soluble finito. Entonces se tiene que

$$\mu_G(r,s) \geq \mathscr{D}\kappa_G(r,s)$$

para todos los enteros positivos $r, s \leq |G|$.

Demostración. Para la prueba de este resultado Eliahou y Kervaire consideran grupos G que satisfacen la condición $\mu_{X\times G}(r,s) \geq \mathscr{D}\kappa_{X\times G}(r,s)$ para todo grupo abeliano X y enteros $1 \leq r, s \leq |X \times G|$. Si esta condición es válida para G, se dice que μ_G es *establemente acotada inferiormente* por $\mathscr{D}\kappa_G$, o más bien, que G es *conveniente*.

Sean G, Γ grupos, tales que existe un homomorfismo sobreyectivo $\pi : G \to \Gamma$ y sea H el kernel de π. Dados los subconjuntos finitos $A, B \subset G$, se obtendrá una cota inferior para $|AB|$, mediante la estimación de los cardinales de la intersección AB con diversas imágenes inversas $\pi^{-1}(\alpha)$ del homomorfismo π.

Se define la *descomposición* de A asociada con π, como la colección $\{A_\alpha,\ \alpha \in \Gamma\}$ de A, donde $A_\alpha = A \cap \pi^{-1}(\alpha)$ para todo $\alpha \in \Gamma$. Observe que $\{A_\alpha,\ \alpha \in \Gamma\}$ es una partición del conjunto A. Sea $r = |A|$. Los cardinales $r_\alpha = |A_\alpha|$ definen una función $\mathfrak{r} : \Gamma \to \mathbb{N}$, la *función descomposición* de A, dada por $\mathfrak{r}(\alpha) = r_\alpha$ para todo $\alpha \in \Gamma$. Luego,

$$A = \bigcup_{\alpha\in\Gamma} A_\alpha \quad \text{y} \quad |A| = \left|\bigcup_{\alpha\in\Gamma} A_\alpha\right|$$

y dado que la colección $\{A_\alpha,\ \alpha \in \Gamma\}$ es una partición, se tiene que

$$r = \sum_{\alpha\in\Gamma} |A_\alpha| = \sum_{\alpha\in\Gamma} r_\alpha = \sum_{\alpha\in\Gamma} \mathfrak{r}(\alpha).$$

A continuación se ilustra la relación entre la función descomposición de A y B con la función μ_H ($H = \ker\pi$), para buscar estimar el mínimo cardinal del conjunto suma AB. Por conveniencia, $\mu_H(r_\alpha, s_\beta) = 0$ si $r_\alpha = 0$ o $s_\beta = 0$.

Proposición 2.1. Sea $\pi : G \to \Gamma$ un homomorfismo sobreyectivo de grupos y sea H el kernel de π. Sean $A,\ B$ dos subconjuntos finitos de G con cardinales $r,\ s$ respectivamente y con descomposiciones $r = \sum_{\alpha\in\Gamma} r_\alpha,\ s = \sum_{\beta\in\Gamma} s_\beta$. Sean $\mathfrak{r}, \mathfrak{s} : \Gamma \to \mathbb{N}$ las funciones descomposición asociadas a estos conjuntos y sea

$$M(\mathfrak{r}, \mathfrak{s}) = \sum_{\gamma\in\Gamma} \max_{\alpha\in\Gamma} \{\mu_H(r_\alpha, s_{\alpha^{-1}\gamma})\}.$$

Entonces se tiene que $|AB| \geq M(\mathfrak{r}, \mathfrak{s})$.

Demostración. Para cada $\gamma \in \Gamma$ sea $C_\gamma = \bigcup_{\alpha\in\Gamma} A_\alpha B_{\alpha^{-1}\gamma}$, observe que si $x \in C_\gamma$ entonces existen $\alpha \in \Gamma$, $a \in A_\alpha$ y $b \in B_{\alpha^{-1}\gamma}$ tales que $x = ab$, así que $\pi(x) = \pi(ab) = \pi(a)\pi(b) = \alpha\alpha^{-1}\gamma = \gamma$, luego $C_\gamma \subset \pi^{-1}(\gamma)$, es decir $C_\gamma \cap C_{\gamma'} = \emptyset$ siempre que $\gamma \neq \gamma'$. Además, $C_\gamma = \bigcup_{\alpha\in\Gamma} A_\alpha B_{\alpha^{-1}\gamma} \subset AB$ porque $A_\alpha \subset A$ y $B_{\alpha^{-1}\gamma} \subset B$.

Por otro lado, si $x \in AB$ entonces existen $a \in A$ y $b \in B$ tales que $x = ab$, dado que la colección $\{A_\alpha,\ \alpha \in \Gamma\}$ es una partición de A y la colección $\{B_\alpha,\ \alpha \in \Gamma\}$ es una partición de B, entonces existen $\delta, \theta \in \Gamma$ tales que $\pi(a) = \delta$ y $\pi(b) = \theta$, de modo que $\pi(ab) = \delta\theta$, esto es, $ab \in \pi^{-1}(\delta\theta)$. Tomando $\gamma = \delta\theta$ y $\alpha = \pi(a) \in \Gamma$ se tiene que $a \in A_\alpha$ y $b \in B\alpha^{-1}\gamma$. Así que $ab \in A_\alpha B_{\alpha^{-1}\gamma} \subset \bigcup_{\alpha\in\Gamma} A_\alpha B_{\alpha^{-1}\gamma} = C_\gamma$.

Por lo tanto $AB = \bigsqcup_{\gamma\in\Gamma} C_\gamma$, donde $\sqcup$ denota la unión de conjuntos disjuntos por pares. De lo anterior $|AB| = \sum_{\gamma\in\Gamma} |C_\gamma|$.

Ahora, si $X \subset \pi^{-1}(\xi)$ para algún $\xi \in \Gamma$ y g es un elemento de G tal que $\pi(g) = \xi^{-1}$, entonces gX y Xg son subconjuntos de $H = \ker\pi$ que satisfacen la ecuación $|gX| = |Xg| = |X|$. De esto se deduce que si $X \subset \pi^{-1}(\alpha)$ con cardinalidad r_X y $Y \subset \pi^{-1}(\beta)$ con cardinalidad s_Y, entonces $|XY| \geq \mu_H(r_X, s_Y)$.

Dado que $C_\gamma = \bigcup_{\alpha\in\Gamma} A_\alpha B_{\alpha^{-1}\gamma}$ se tiene que $|C_\gamma| \geq \max_{\alpha\in\Gamma} \{|A_\alpha B_{\alpha^{-1}\gamma}|\}$, y por lo anterior se sigue que $|C_\gamma| \geq \max_{\alpha\in\Gamma} \{\mu_H(r_\alpha, s_{\alpha^{-1}\gamma})\}$.

Por lo tanto, $|AB| \geq \sum_{\gamma\in\Gamma} \max_{\alpha\in\Gamma} \{\mu_H(r_\alpha, s_{\alpha^{-1}\gamma})\} = M(\mathfrak{r}, \mathfrak{s})$. □

Proposición 2.2. Sea $\pi : G \to \Gamma$ un homomorfismo sobreyectivo de grupos finitos, con kernel un $p-$grupo abeliano P. Si para cada grupo abeliano X y enteros positivos $r, s \leq |X \times \Gamma|$ se tiene que $\mu_{X\times\Gamma}(r, s) \geq \mathscr{D}\kappa_{X\times\Gamma}(r, s)$, entonces para todo par de enteros positivos $r, s \leq |G|$,

$$\mu_G(r, s) \geq \mathscr{D}\kappa_G(r, s).$$

Demostración. Sean $A, B \subset G$ subconjuntos de G que realizan $\mu_G(r, s)$. Los subconjuntos A y B determinan las funciones de descomposición $\mathfrak{r}, \mathfrak{s} : \Gamma \to \mathbb{N}$ asociadas con π, dadas por $\mathfrak{r}(\alpha) = r_\alpha,\ \mathfrak{s}(\beta) = s_\beta$ para todo $\alpha, \beta \in \Gamma$, y con $r = \sum_{\alpha\in\Gamma} r_\alpha,\ s = \sum_{\beta\in\Gamma} s_\beta$. Por la proposición 2.1, se sigue que

$$|AB| \geq M(\mathfrak{r}, \mathfrak{s}) = \sum_{\gamma\in\Gamma} \max_{\alpha\in\Gamma} \{\mu_P(r_\alpha, s_{\alpha^{-1}\gamma})\}.$$

En particular, se tiene que $\mu_G(r, s) \geq M(\mathfrak{r}, \mathfrak{s})$.

Sea L un grupo abeliano de cardinalidad $|L| = |P| = p^v$. Entonces
$|L \times \Gamma| = |P \times \Gamma| = |G|$, y por lo tanto

$$\mathscr{D}\kappa_{L\times\Gamma}(r, s) = \mathscr{D}\kappa_{P\times\Gamma}(r, s) = \mathscr{D}\kappa_G(r, s).$$

Dados cualquier subconjuntos $U_\alpha,\ V_\beta \subset L$ con $|U_\alpha| = r_\alpha$ y $|V_\beta| = s_\beta$ para todos los $\alpha, \beta \in \Gamma$, se construyen los subconjuntos $U, V \subset L \times \Gamma$ como sigue:

$$U = \bigsqcup_{\alpha\in\Gamma} U_\alpha \times \{\alpha\}, \qquad V = \bigsqcup_{\beta\in\Gamma} V_\beta \times \{\beta\}.$$

En consecuencia $|U| = |A| = r$ y $|V| = |B| = s$, ya que $|U| = \sum_{\alpha\in\Gamma} r_\alpha = r$ y $|V| = \sum_{\beta\in\Gamma} s_\beta = s$.

Escribiendo $L \times \Gamma$ en forma aditiva, y usando la hipótesis $\mu_{X\times\Gamma}(r, s) \geq \mathscr{D}\kappa_{X\times\Gamma}(r, s)$ para todo grupo abeliano X, se sigue que

$$|U + V| \geq \mu_{L\times\Gamma}(r, s) \geq \mathscr{D}\kappa_{L\times\Gamma}(r, s) = \mathscr{D}\kappa_G(r, s).$$

A continuación se prueba que para una elección adecuada del grupo L y de los subconjuntos $U_\alpha, V_\beta \subset L$ para todo $\alpha, \beta \in \Gamma$, se puede obtener que

$$M(\mathfrak{r}, \mathfrak{s}) = |U + V|.$$

Esto es suficiente para concluir la prueba de la proposición 2.2, así

$$\mu_G(r, s) \geq M(\mathfrak{r}, \mathfrak{s}) = |U + V| \geq \mathscr{D}\kappa_G(r, s).$$

Como grupo específico se elige el elemental $p-$grupo abeliano $L = \mathbb{F}_{p^v}$, donde $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Luego, $|L| = |P| = p^v$. Se ordena a $\mathbb{F}_p$ mediante el orden natural, identificado con el conjunto $\{0, 1, \ldots, p-1\}$, como también se ordena al conjunto L, lexicográficamente.

Como L es totalmente ordenado, un segmento inicial, está completamente determinado por su cardinalidad. Así, la elección de los subconjuntos $U_\alpha,\ V_\beta$ en L será segmentos iniciales de las cardinalidades requeridas. Tomando $U_\alpha = \mathsf{IS}(r_\alpha)$ y $V_\beta = \mathsf{IS}(s_\beta)$ para todo $\alpha, \beta \in \Gamma$, y usando el lema 1.1 se tiene que $\mathsf{IS}(t) + \mathsf{IS}(u) = \mathsf{IS}(\kappa_L(r_\alpha, s_\beta))$ para todo $0 \leq t, u \leq p^v$, de ahí que,

$$U_\alpha + V_\beta = \mathsf{IS}(r_\alpha) + \mathsf{IS}(s_\beta) = \mathsf{IS}(\kappa_L(r_\alpha, s_\beta)),$$

por lo tanto

$$|U_\alpha + V_\beta| = \kappa_L(r_\alpha, s_\beta) = \kappa_P(r_\alpha, s_\beta)$$

para todo $\alpha, \beta \in \Gamma$. Dado que $U = \bigsqcup_{\alpha\in\Gamma} U_\alpha \times \{\alpha\},\ V = \bigsqcup_{\beta\in\Gamma} V_\beta \times \{\beta\}$, se tiene que

$$|U + V| = \sum_{\gamma\in\Gamma} |\bigcup_{\alpha\in\Gamma} (U_\alpha + V_{\alpha^{-1}\gamma}) \times \{\gamma\}| = \sum_{\gamma\in\Gamma} \max_{\alpha\in\Gamma}\{\kappa_P(r_\alpha, s_{\alpha^{-1}\gamma})\}.$$

(La segunda igualdad utiliza el hecho de que la unión de los segmentos iniciales es de nuevo un segmento inicial). Como P es un grupo abeliano, se tiene la igualdad $\mu_P(t, u) = \kappa_P(t, u)$ para todo $0 \leq t, u \leq p^v$, como se presenta en el Capítulo 1. Por lo tanto, se sigue que

$$\sum_{\gamma\in\Gamma} \max_{\alpha\in\Gamma}\{\kappa_P(r_\alpha, s_{\alpha^{-1}\gamma})\} = \sum_{\gamma\in\Gamma} \max_{\alpha\in\Gamma}\{\mu_P(r_\alpha, s_{\alpha^{-1}\gamma})\},$$

y se concluye que $|U + V| = M(\mathfrak{r}, \mathfrak{s})$. □

Por comodidad, se dirá que un grupo Γ es conveniente si Γ satisface la condición $\mu_{X\times\Gamma}(r,s) \geq \mathscr{D}\kappa_{X\times\Gamma}(r,s)$ para todos los grupos abelianos X y enteros positivos r, s tales que $r, s \leq |X \times \Gamma|$. La proposición 2.2 establece que si G es un grupo finito con $P \trianglelefteq G$, un $p-$subgrupo normal abeliano, tal que $\Gamma = G/P$ es conveniente, entonces $\mu_G(r,s) \geq \mathscr{D}\kappa_G(r,s)$.

Proposición 2.3. Sea $\pi : G \to \Gamma$ un homomorfismo sobreyectivo de grupos finitos, con kernel un p-grupo abeliano P. Si Γ es conveniente, entonces G también es conveniente.

Demostración. Sea Y un grupo abeliano arbitrario. Se debe mostrar que $\mu_{Y\times G}(r,s) \geq \mathscr{D}\kappa_{Y\times G}(r,s)$ para todos los enteros positivos $r, s \leq |Y \times G|$. De acuerdo con la proposición 2.2, esta desigualdad se mantiene para el grupo trivial $Y_0 = \{1\}$.

Sea $G' = Y \times G$, $\Gamma' = Y \times \Gamma$ y $\pi' : G' \to \Gamma'$ el mapeo $\pi' = \mathrm{id}_Y \times \pi$. De Γ conveniente, se desprende de la definición que Γ' también es conveniente. Por otra parte, $\ker \pi'$ es un $p-$grupo abeliano, ya que $\ker \pi' = \ker \pi = P$. De este modo, se puede aplicar la proposición 2.2 a $\pi' : G' \to \Gamma'$, por lo tanto se concluye que

$$\mu_{G'}(r,s) \geq \mathscr{D}\kappa_{G'}(r,s)$$

para todos los enteros positivos $r, s \leq |G'|$. □

Proposición 2.4. Sea $\pi : G \to \Gamma$ un homomorfismo sobreyectivo de grupos finitos, con kernel abeliano H. Si Γ es conveniente, entonces G también es conveniente.

Demostración. Por ser abeliano finito, el grupo H es el producto directo de sus $p-$subgrupos de Sylow $P_1, \ldots, P_m$, el orden de P_i es una potencia q_i del primo p_i. H es normal en G puesto que es el kernel de π.

Sea $g \in G$, se define el automorfismo ϕ_g como sigue

$$\begin{aligned} \phi_g : H &\longrightarrow H \\ h &\longrightarrow \phi_g(h) = g^{-1}hg \end{aligned}$$

Observe que ϕ_g así definido es un isomorfismo.

Como P_i es un subgrupo del grupo abeliano H entonces $P_i \trianglelefteq H$. Ahora, sea $f : H \longrightarrow H$ un automorfismo, entonces $f(P_i)$ es un subgrupo de H y $|f(P_i)| = |P_i|$, de donde $f(P_i)$ es un $P-$subgrupo de Sylow, de H, pero por ser abeliano H tiene un único $P-$subgrupo de Sylow de orden $|P_i|$, así $f(P_i) = P_i$, es decir P_i es invariante bajo cualquier automorfismo en H, en particular bajo ϕ_g. De ahí que $P_i \trianglelefteq G$.

Por lo tanto definamos los grupos

$$G_j = G/(P_j \times \cdots \times P_m)$$

para todo $1 \leq j \leq m+1$.

Se probará por inducción en j, que G_j es conveniente para todo j. Esto será suficiente para concluir la prueba, tomando $G_{m+1} = G$. Para $j = 1$, el grupo $G_1 = G/H$ es isomorfo a Γ y por lo tanto por hipótesis es conveniente. Ahora, se supone G_j es conveniente para $1 \leq j \leq m$. Y se tiene la secuencia exacta dada por el monomorfismo inclusión i y el epimorfismo natural π, con $i(P_j) = \ker(\pi) = P_j$

$$1 \ \rightarrow \ P_j \ \rightarrow \ G_{j+1} \ \rightarrow \ G_j \ \rightarrow \ 1,$$

donde G_j es isomorfo a G_{j+1}/P_j por construcción. Por otra parte, P_j es un P_j-grupo abeliano, por ser subgrupo de H, y aplicando la proposición 2.3, se concluye que G_{j+1} también es conveniente. □

Ahora se prueba la afirmación más fuerte, que G es conveniente, es decir,

$$\mu_{Y\times G}(r,s) \geq \mathscr{D}\kappa_{Y\times G}(r,s)$$

para todo grupo abeliano Y y enteros $1 \leq r, s \leq |Y \times G|$. El teorema se sigue, tomando para Y el grupo trivial $\{1\}$.

Como G es soluble, sea

$$G = G_0 \supsetneq G_1 \supsetneq \cdots \supsetneq G_\ell = \{1\}$$

la serie finita de iteraciones derivadas (idénticamente conmutador) de los subgrupos de G, donde $G_{i+1} = [G_i,\ G_i]$ para todo i. El índice ℓ se conoce como la longitud derivada de G. Para probar que G es conveniente se procederá por inducción sobre ℓ. El caso $\ell \leq 1$ corresponde a los grupos abelianos, que son convenientes.

Ahora para $\ell \geq 2$, se supone el subgrupo $G_{\ell-1}$ abeliano, y normal en G. El grupo cociente $G/G_{\ell-1}$ es soluble de longitud derivada $\ell - 1$, ya que su serie derivada viene dada por

$$G/G_{\ell-1} = G_0/G_{\ell-1} \supsetneq G_1/G_{\ell-1} \supsetneq \cdots G_{\ell-1}/G_{\ell-1} = \{1\}.$$

Por lo tanto, por la hipótesis de inducción, el grupo $G/G_{\ell-1}$ es conveniente. Con la secuencia exacta

$$\{1\} \to G_{\ell-1} \to G \to G/G_{\ell-1} \to \{1\}$$

y el hecho de que el kernel $G_{\ell-1}$ es abeliano, por la proposición 2.4 se tiene que G es conveniente. □

2.3. LA FUNCIÓN μ_G EN GRUPOS DIÉDRICOS

En esta sección se estudia la función μ_G para $G = \mathscr{D}_n$, el grupo diédrico de orden $2n$. Aquí se presenta la solución obtenida por Eliahou y Kervaire en [Eliahou & Kervaire, 2010], para $\mu_{\mathscr{D}_n}(r, s)$ que es valida para todo n y para todo par de enteros r y s tales que $1 \leq r, s \leq 2n$, partiendo de la solución alcanzada para cuando n es potencia de un número primo.

Definición 2.5. Grupo diédrico

Sea $n > 2$ un número entero. El n-ésimo grupo diédrico, denotado $\mathscr{D}_n$, es el grupo de simetrías de un polígono regular de n lados. Si α es la rotación del ángulo $\dfrac{2\pi}{n}$ 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

$$\mathscr{D}_n = \{\alpha^i \ / \ i \in \mathbb{Z}_n\} \cup \{\alpha^i\beta \ / \ i \in \mathbb{Z}_n\} = \left\langle \alpha, \beta \ / \ \alpha^n = \beta^2 = 1, \ \beta\alpha\beta^{-1} = \alpha^{-1} \right\rangle.$$

En todo grupo diédrico se cumplen las siguientes propiedades:

Teorema 2.6. Sea $n > 2$ un número entero y sea

$$\mathscr{D}_n = \left\langle \alpha, \beta \ / \ \alpha^n = \beta^2 = 1, \ \beta\alpha\beta^{-1} = \alpha^{-1} \right\rangle,$$

el grupo diédrico de orden $2n$. Entonces:

1. Un subgrupo propio H de $\mathscr{D}_n$ es normal en $\mathscr{D}_n$ si, y sólo si, cumple uno de los siguientes enunciados.

   a) H es un subgrupo del grupo $\langle\alpha\rangle$ generado por la rotación α.

   b) H es el subgrupo $\langle\alpha^2, \beta\rangle$ generado por α^2 y β o H es el subgrupo $\langle\alpha^2, \alpha\beta\rangle$ generado por α^2 y $\alpha\beta$. En este caso H es de índice 2 y n es par.

2. Los grupos cocientes de $\mathscr{D}_n$ son diédricos y los subgrupos de $\mathscr{D}_n$ son diédricos o cíclicos.

3. $\mathscr{D}_n$ es soluble.

Teorema 2.7. Sea $n > 2$ un número entero y sean r, s dos enteros positivos tales que $r, s \leq 2n$. Si h es el orden de un subgrupo H del grupo diédrico

$$\mathscr{D}_n = \left\langle \alpha, \beta \ / \ \alpha^n = \beta^2 = 1, \ \beta\alpha\beta^{-1} = \alpha^{-1} \right\rangle,$$

entonces existen subconjuntos A y B de $\mathscr{D}_n$ tales que $|A| = r$, $|B| = s$ y

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

Demostración. Ver [Eliahou & Kervaire, 2006].

En particular, el teorema 2.7, muestra que para todo entero $n > 2$ y para todo par de enteros positivos $r, s \leq 2n$ se tiene la desigualdad $\mu_{\mathscr{D}_n}(r,s) \leq \kappa_{\mathscr{D}_n}(r,s)$. En [Eliahou & Kervaire, 2006], Eliahou y Kervaire muestran que si n es potencia de un número primo y r, s son dos enteros tales que $1 \leq r, s \leq 2n$, entonces $\mu_{\mathscr{D}_n}(r,s) \geq \kappa_{\mathscr{D}_n}(r,s)$, en realidad, ellos prueban el siguiente teorema:

Teorema 2.8. Eliahou y Kervaire
Sean p un número primo, m un entero positivo y $\mathscr{D}_n$ el grupo diédrico de orden $2p^m$. Si r y s son dos enteros tales que $1 \leq r, s \leq 2p^m$, entonces

$$\mu_{\mathscr{D}_n}(r,s) = \kappa_{\mathscr{D}_n}(r,s).$$

Recientemente, Eliahou y Kervaire en [Eliahou & Kervaire, 2010] prueban el siguiente teorema:

Teorema 2.9. Para el grupo diédrico D_n de orden $2n$, se tiene

$$\mu_{D_n}(r,s) = \kappa_{D_n}(r,s)$$

para todo $n \geq 1$ y enteros positivos $r, s \leq 2n$.

Demostración. $\mathscr{D}\kappa_{D_n} = \kappa_{D_n}$, ya que todo divisor positivo de $2n$ es el orden de un subgrupo de D_n. Por lo tanto

$$\mu_{D_n}(r,s) \geq \kappa_{D_n}(r,s)$$

para todos los enteros positivos $r, s \leq 2n$. Combinando esto con la cota superior de [Eliahou & Kervaire, 2006] recordada anteriormente, se concluye que se tiene la igualdad. □

Ahora, sea G un grupo soluble finito. Combinando el teorema 2.5, el corolario 2.2 y utilizando el hecho de que $\mathscr{H}(G) \supset \mathscr{N}(G)$, se obtienen las siguientes cotas para la función μ_G.

Corolario 2.3. Si G es un grupo soluble finito entonces para todo par de enteros $r,\ s$ tal que $0 \leq r, s \leq |G|$, se tiene que

$$\mathscr{D}\kappa_G(r,s) \leq \mu_G(r,s) \leq \mathscr{N}\kappa_G(r,s). \tag{2.1}$$

Por comparación, se observa que para cualquier grupo G y enteros r, s, se tiene que

$$\mathscr{N}\kappa_G(r,s) \geq \kappa_G(r,s) \geq \mathscr{D}\kappa_G(r,s). \tag{2.2}$$

Esto se deduce de la propia definición de estas funciones aritméticas y de las inclusiones $\mathscr{D}(G) \supset \mathscr{H}(G) \supset \mathscr{N}(G)$. En particular, si G es soluble finito, y si las funciones $\mathscr{D}\kappa_G$ y $\mathscr{N}\kappa_G$ coinciden en algún par $1 \leq r, s \leq |G|$, entonces $\mu_G(r,s)$ es determinada e igual a $\kappa_G(r,s)$.

Capítulo 3

LA FUNCIÓN μ_G EN P-GRUPOS Y GRUPOS HAMILTONIANOS

En este capítulo se exponen los resultados obtenidos por Benavides, Castillo y Mutis para la función μ_G, tanto en p-grupos como en grupos hamiltonianos (ver [Benavides, Castillo & Mutis, 2009],[Benavides, Castillo & Mutis, 2010]). Inicialmente, se describen los resultados logrados en p-grupos finitos. En seguida se presenta el estudio de la función μ_G en grupos hamiltonianos de orden 2^{n+3}, con n entero no negativo. Finalmente, se da a conocer la demostración de la fórmula obtenida para la función μ_G en grupos hamiltonianos que se pueden escribir como $\mathscr{Q} \times (\mathbb{Z}_2)^n \times \mathbb{Z}_m$, donde m es un entero positivo.

3.1. LA FUNCIÓN μ_G EN P-GRUPOS FINITOS

Como ya se mencionó, no se conoce una fórmula explícita para la función μ_G, cuando G es un grupo finito no abeliano, sin embargo, Benavides, Castillo y Mutis en 2009 (Ver [Benavides, Castillo & Mutis, 2010]), lograron establecer una fórmula para la función μ_G cuando G es un p-grupo finito. En esta sección se presenta la demostración de la fórmula obtenida para la función μ_G cuando G es un p-grupo finito, la cual coincide con la obtenida para cuando G es un grupo abeliano.

Definición 3.1. Expansión p-adica
Sea p un entero positivo mayor que uno. La expansión p-adica de un entero positivo m es la única sucesión $\{m_i\}_{i\geq 0}$, con $m_i \in \{0, 1, \ldots, p-1\}$, tal que $m = \sum_{i\geq 0} m_i p^i$.

Definición 3.2. Suma p-adica
Sea p un entero positivo mayor que uno y sean l y m dos enteros no negativos cuyas expansiones p-adicas son $\{l_i\}_{i\geq 0}$ y $\{m_i\}_{i\geq 0}$, respectivamente. La suma p-adica de l y m, denotada por $l \oplus_p m$, es el entero positivo cuya expansión p-adica es la sucesión $\{t_i\}_{i\geq 0}$ donde para cada $i \geq 0$ se tiene que $t_i \in \{0, 1, \ldots, p-1\}$ y $t_i \cong (l_i + m_i)$ mód p.

Si p es un número primo, entonces el conjunto $\mathbb{N}_0$, de los enteros no negativos, tiene estructura de espacio vectorial sobre el campo finito $\mathbb{F}_p$, con la suma p-adica como la adición de vectores. Una $\mathbb{F}_p$-base para $\mathbb{N}_0$ es $\{1, p, \ldots, p^\nu, \ldots\}$. Para subconjuntos A y B de $\mathbb{N}_0$, se denotará con $A \oplus_p B$, al conjunto suma de A y B bajo la suma p-adica.

Teorema 3.1. Teorema de Cauchy

Si G es un grupo finito y p un número primo tal que $p \big| |G|$, entonces G contiene al menos un elemento de orden p. Más precisamente, el número de elementos de orden p es congruente con -1 mód p.

Teorema 3.2. Sea p un número primo. Un grupo finito G es un p-grupo si, y sólo si, para algún entero positivo n se tiene que $|G| = p^n$.

La prueba del teorema anterior se obtiene aplicando los teoremas de Cauchy y Lagrange. Por ejemplo, el grupo cuaternión $\mathscr{Q} = \{1,\ -1,\ i,\ -i,\ j,\ -j,\ k,\ -k\}$, de orden 2^3, es un p-grupo con $p = 2$.

Definición 3.3. Grupo Supersoluble

Un grupo G es supersoluble si posee una serie normal $G = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_n = \{1\}$, donde para cada $i = 1, 2, \ldots, n$ el grupo factor H_{i-1}/H_i es cíclico.

Dado que todo grupo cíclico es abeliano, entonces todo grupo supersoluble es soluble. En [Marshall, 1979] se demuestra la siguiente caracterización de los grupos supersolubles finitos:

Teorema 3.3. Un grupo finito G es supersoluble si, y sólo si, todos sus subgrupos maximales son de índice primo.

Teorema 3.4. Todo subgrupo propio de un p-grupo P de orden p^n está contenido en un subgrupo maximal de orden p^{n-1}, y todos los subgrupos maximales de P son normales.

Los teoremas 3.3 y 3.4 implican que todo p-grupo finito es supersoluble y por lo tanto soluble.

Teorema 3.5. Sean $p_1 \leq p_2 \leq \cdots \leq p_r$ números primos. Si G es un grupo finito supersoluble de orden $p_1 p_2 \cdots p_r$, entonces G tiene una serie principal

$$G = H_0 \supset H_1 \supset \cdots \supset H_r = \{1\},$$

donde para cada $i = 1, 2, \ldots, r$ el grupo factor H_{i-1}/H_i es de orden p_i.

Teorema 3.6. Sea p un número primo. Si G es un p-grupo finito, entonces para cada divisor positivo t de $|G|$ existe un subgrupo normal H de G tal que $|H| = t$.

Teorema 3.7. Sean p un número primo y G un p-grupo finito no trivial. Entonces, el centro $\mathscr{Z}(G)$ es no trivial.

Corolario 3.1. Sean p un número primo y G un p-grupo finito no trivial. Entonces el centro $\mathscr{Z}(G)$ de G contiene al menos un elemento de orden p.

Teorema 3.8. 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 $\mu_G(r, s) = \kappa_G(r, s)$.

Demostración. Por teorema 3.2 se puede suponer $|G| = p^n$, para algún entero positivo n, así el conjunto $\mathscr{H}(G)$ de órdenes de subgrupos de G está dado por $\mathscr{H}(G) = \{1, p, p^2, \ldots, p^n\}$. Sea $p^x \in \mathscr{H}(G)$ tal que

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

Por teorema 3.6 G contiene un subgrupo normal de orden p^x, esto junto al hecho que todo p-grupo finito es soluble y el lema 2.1 implican

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

La desigualdad $\mu_G(r, s) \geq \kappa_G(r, s)$ se probará por inducción sobre el orden del p-grupo G. Para $n = 1$ se tiene que $|G| = p$, luego $G \cong \mathbb{Z}_p$, donde $\mathbb{Z}_p$ denota el grupo de congruencias módulo p, así G es cíclico y por lo tanto $\mu_G(r, s) = \kappa_G(r, s)$, en particular $\mu_G(r, s) \geq \kappa_G(r, s)$. Supóngase que el teorema es válido para p-grupos de orden p^n, con $n > 1$, y sea G un p-grupo de orden p^{n+1}. Por el corolario 3.1 existe un elemento $c \in \mathscr{Z}(G)$ de orden p. Sea T un subgrupo maximal de G, por el teorema 3.4, $|T| = p^n$ y T es un subgrupo normal de G, de manera que se puede escribir a G como la union de p clases laterales derechas disjuntas, así

$$G = T \cup Tc \cup Tc^2 \cup \cdots \cup Tc^{p-1}. \tag{3.1}$$

Sean r, s enteros positivos con $r, s \leq p^{n+1}$ y sean A, B dos subconjuntos de G tales que A y B realizan $\mu_G(r,s)$. Por la igualdad 3.1 T contiene subconjuntos $A_0, A_1, \ldots, A_{p-1}$ de cardinales $r_0, r_1, \ldots, r_{p-1}$, respectivamente, y subconjuntos, $B_0, B_1, \ldots, B_{p-1}$ de cardinales $s_0, s_1, \ldots, s_{p-1}$, respectivamente, tales que

$$A = A_0 \ \cup A_1 c \ \cup A_2 c^2 \ \cup \cdots \cup A_{p-1} c^{p-1} = \bigcup_{i=0}^{p-1} A_i c^i. \tag{3.2}$$

$$B = B_0 \ \cup B_1 c \ \cup B_2 c^2 \ \cup \cdots \cup B_{p-1} c^{p-1} = \bigcup_{j=0}^{p-1} B_j c^j. \tag{3.3}$$

Luego,

$$r = |A| = |A_0| + |A_1| + |A_2| + \cdots + |A_{p-1}| = r_0 + r_1 + r_2 + \cdots + r_{p-1}$$

$$s = |B| = |B_0| + |B_1| + |B_2| + \cdots + |B_{p-1}| = s_0 + s_1 + s_2 + \cdots + s_{p-1}.$$

Llamando $F_l = \{(i,j) \ / \ 0 \leq i, j \leq p-1 \ \text{ e } \ i + j \cong l \ \text{mód} \ p\}$, de las igualdades 3.2 y 3.3, se sigue que

$$AB = \left(\bigcup_{i=0}^{p-1} A_i c^i \right) \left(\bigcup_{j=0}^{p-1} B_j c^j \right) = \bigcup_{l=0}^{p-1} \left[\left(\bigcup_{(i,j) \in F_l} A_i B_j \right) c^l \right]$$

entonces

$$|AB| = \sum_{l=0}^{p-1} \left| \bigcup_{(i,j) \in F_l} A_i B_j \right|,$$

y dado que $\mu_G(r,s) = |AB|$ se tiene que

$$\begin{aligned} \mu_G(r,s) &\geq \sum_{l=0}^{p-1} \big(\text{máx} \{ |A_i B_j| \ / \ (i,j) \in F_l \} \big) \\ &\geq \sum_{l=0}^{p-1} \big(\text{máx} \{ \mu_T(r_i, s_j) \ / \ (i,j) \in F_l \} \big). \end{aligned}$$

La hipótesis inductiva aplicada al p-grupo T implica

$$\mu_G(r,s) \geq \sum_{l=0}^{p-1} \big(\text{máx} \{ \kappa_T(r_i, s_j) \ / \ (i,j) \in F_l \} \big). \tag{3.4}$$

Ahora bien, el conjunto $\mathbb{N}_0$ de los enteros no negativos tiene estructura de espacio vectorial sobre el campo finito $\mathbb{F}_p$, donde la suma de vectores es la suma p-adica (ver definición 3.2). Sea $\mathscr{V}$ el subespacio de $\mathbb{N}_0$ generado por el conjunto $\{1, p, p^2, \ldots, p^{n-1}\}$, es decir, $\mathscr{V} = \{0, 1, 2, \ldots, p^n - 1\}$. Utilizando la notación I_t para representar el segmento inicial de longitud t de $\mathscr{V}$ (ver definición 1.10), se sigue que

$$\mu_{\mathscr{V}}(u, v) = |I_u \oplus_p I_v| \quad \text{siempre que} \quad 1 \leq u, v \leq |\mathscr{V}|.$$

La igualdad anterior junto al hecho que la suma de dos segmentos iniciales de $\mathscr{V}$ es de nuevo un segmento inicial de $\mathscr{V}$, implican

$$\begin{cases} I_u \oplus_p I_v = I_{\mu_{\mathscr{V}}(u,v)} & \text{siempre que } 1 \leq u, v \leq |\mathscr{V}| \\ I_u \cup I_v = I_{\max\{u,v\}} & \text{para todo par de enteros no negativos } u \text{ y } v. \end{cases} \tag{3.5}$$

Sea M el grupo abeliano de orden p^{n+1} definido por $M = \mathscr{V} \times \mathbb{Z}_p$. Por el teorema 1.8 y dado que el conjunto $\mathscr{H}(M)$ de todos los órdenes de subgrupos de M coincide con el conjunto de todos los órdenes de subgrupos de $\mathscr{V}$, se tiene que

$$\mu_M(r, s) = \kappa_M(r, s) = \kappa_G(r, s). \tag{3.6}$$

Ahora, viendo al grupo $\mathscr{V}$ como un subgrupo de M y tomando $b = (0, 1) \in M$, se sigue que

$$M = \mathscr{V} \cup (\mathscr{V} + b) \cup \cdots \cup (\mathscr{V} + (p-1)b).$$

Para $i, j = 0, 1, \ldots, p-1$ sean I_{r_i} e I_{s_j} los segmentos iniciales de $\mathscr{V}$ de longitudes r_i y s_j, respectivamente, y considérense los conjuntos

$$E = I_{r_0} \cup (I_{r_1} + b) \cup (I_{r_2} + 2b) \cup \cdots \cup (I_{i_{p-1}} + (p-1)b) = \bigcup_{i=0}^{p-1} (I_{r_i} + ib)$$

$$D = I_{s_0} \cup (I_{s_1} + b) \cup (I_{s_2} + 2b) \cup \cdots \cup (I_{s_{p-1}} + (p-1)b) = \bigcup_{j=0}^{p-1} (I_{s_j} + jb)$$

entonces $|E| = r$ y $|D| = s$. Para $l \in \{0, 1, 2, \ldots, p-1\}$ sea $W_l = \bigcup_{(i,j) \in F_l} (I_{r_i} \oplus_p I_{s_j})$.

Realizando algunos cálculos se puede observar que

$$E + D = W_0 \ \cup (W_1 + b) \ \cup (W_2 + 2b) \ \cup \cdots \cup (W_{p-1} + (p-1)b).$$

Aplicando la ecuación 3.6, se sigue que

$$\sum_{l=0}^{p-1} |W_l| = |E + D| \geq \mu_M(r, s) = \kappa_M(r, s) = \kappa_G(r, s). \tag{3.7}$$

Utilizando las igualdades 3.5 se tiene que

$$\sum_{l=0}^{p-1} |W_l| = \sum_{l=0}^{p-1} \left| \bigcup_{(i,j)\in F_l} I_{\mu_{\mathscr{V}}(r_i,s_j)} \right| = \sum_{l=0}^{p-1} \big(\text{máx} \left\{ \mu_{\mathscr{V}}(r_i, s_j) \ / \ (i,j) \in F_l \right\} \big),$$

pero $\mathscr{V}$ es un grupo abeliano; entonces

$$\sum_{l=0}^{p-1} |W_l| = \sum_{l=0}^{p-1} \big(\text{máx} \left\{ \kappa_{\mathscr{V}}(r_i, s_j) \ / \ (i,j) \in F_l \right\} \big),$$

además $\mathscr{V}$ y T son p-grupos del mismo orden, así que $\kappa_{\mathscr{V}}(r_i, s_j) = \kappa_T(r_i, s_j)$ para toda $(i,j) \in F_l$ y toda $l \in \{0, 1, 2, \ldots, p-1\}$, entonces

$$\sum_{l=0}^{p-1} |W_l| = \sum_{l=0}^{p-1} \big(\text{máx} \left\{ \kappa_T(r_i, s_j) \ / \ (i,j) \in F_l \right\} \big). \tag{3.8}$$

De la ecuación 3.8 y las desigualdades 3.4 y 3.7 se concluye que

$$\mu_G(r, s) \geq \sum_{l=0}^{p-1} |W_l| \geq \kappa_G(r, s).$$

□

3.2. LA FUNCIÓN μ_G EN GRUPOS HAMILTONIANOS

Uno de los resultados más importantes para el desarrollo de la presente investigación fue el obtenido por Benavides, Castillo y Mutis en [Benavides, Castillo & Mutis, 2009], debido a que llevó a conjeturar una solución al problema de los conjuntos suma pequeños en grupos hamiltonianos finitos arbitrarios.

Definición 3.4. Grupo hamiltoniano

Un grupo H es hamiltoniano si H es no abeliano y todo subgrupo de H es normal.

Una caracterización de los grupos hamiltonianos es la siguiente:

Teorema 3.9. Un grupo hamiltoniano es el producto directo del grupo cuaternión con un grupo abeliano en el que todo elemento es de orden finito impar y un grupo abeliano en el que todo elemento es de orden 2. Es decir, si H es hamiltoniano y $\mathscr{Q}$ es el grupo de los cuaterniones entonces existen un grupo G en el que todo elemento es de orden finito impar y un entero no negativo n, tal que $H \cong \mathscr{Q} \times (\mathbb{Z}_2)^n \times G$

En particular, el grupo $\mathscr{Q}$, de los cuaterniones, es el grupo hamiltoniano de menor orden.

Teorema 3.10. Un grupo hamiltoniano finito es soluble.

Demostración. Sea $H \cong \mathscr{Q} \times (\mathbb{Z}_2)^n \times G$ un grupo hamiltoniano finito. Se puede considerar al grupo $N = \mathscr{Q} \times (\mathbb{Z}_2)^n$ como un subgrupo normal de H. Luego N es de orden 2^{n+3} y por el teorema 3.2 se sigue que N es un p-grupo finito y por lo tanto N es soluble. Por otro lado $|H/N| = |G|$, es decir H/N es de orden impar y por el famoso teorema de Feit-Thompson se tiene que H/N es soluble. Así, H contiene un subgrupo normal N tal que N y H/N son solubles, por lo tanto H es soluble. □

Teorema 3.11. Sea $\mathscr{Q}$ el grupo de los cuaterniones. Si r y s son dos enteros positivos menores o iguales a 8, entonces $\mu_{\mathscr{Q}}(r, s) = \kappa_{\mathscr{Q}}(r, s)$.

Demostración. La demostración es consecuencia inmediata de el lema 1.5. □

Lema 3.1. El conjunto $\mathscr{H}(H)$, de ordenes de subgrupos del grupo hamiltoniano finito H es,

$$\mathscr{H}(H) = \{\ 2^x d\ /\ 0 \leq x \leq k+3,\ d|n\ \}.$$

donde $n = |G|$.

Demostración. Es consecuencia del teorema de Lagrange y del hecho que $|H| = 2^{k+3}n$.

Lema 3.2. Sean $n \geq 1$, $\widehat{H} \cong \mathscr{Q} \times (\mathbb{Z}_2)^n$ y $T \cong \mathscr{Q} \times (\mathbb{Z}_2)^{n-1}$ entonces, para todo terna de enteros positivos r, s_0, s_1 tales que $r, s_0, s_1 \leq |T|$ se tiene que

$$\kappa_T(r, s_0) + \kappa_T(r, s_1) \geq \kappa_{\widehat{H}}(r, s_0 + s_1).$$

Demostración. Dado que todo p-grupo finito es supersoluble, entonces, del teorema 3.6 se tiene que el conjunto $\mathscr{H}(T)$ de órdenes de subgrupos de T, coincide con el conjunto Div$(T) = \{1, 2, 2^2, \cdots, 2^{n+2}\}$ de divisores de $|T|$, así para cada par de enteros positivos $r', s' \leq |T|$ se tiene que

$$\kappa_T(r', s') = \min_{d \in \mathscr{H}(T)} \left\{ \left(\left\lceil \frac{r'}{d} \right\rceil + \left\lceil \frac{s'}{d} \right\rceil - 1 \right) d \right\}.$$

Sean r, s_0, s_1 enteros positivos tales que $r, s_0, s_1 \leq |T|$ y sean x, y dos enteros tales que $0 \leq x, y \leq n+2$ y

$$\kappa_T(r, s_0) = 2^x \left(\left\lceil \frac{r}{2^x} \right\rceil + \left\lceil \frac{s_0}{2^x} \right\rceil - 1 \right) \quad \text{y} \quad \kappa_T(r, s_1) = 2^y \left(\left\lceil \frac{r}{2^y} \right\rceil + \left\lceil \frac{s_1}{2^y} \right\rceil - 1 \right).$$

No se pierde generalidad al suponer $x \leq y$, luego

$$\kappa_T(r, s_0) + \kappa_T(r, s_1) = 2^x \left(\left\lceil \frac{r}{2^x} \right\rceil + \left\lceil \frac{s_0}{2^x} \right\rceil - 1 + 2^{y-x} \left(\left\lceil \frac{r}{2^y} \right\rceil + \left\lceil \frac{s_1}{2^y} \right\rceil - 1 \right) \right)$$

pero $\left\lceil \frac{r}{2^y} \right\rceil - 1 \geq 0$, entonces

$$\kappa_T(r, s_0) + \kappa_T(r, s_1) \geq 2^x \left(\left\lceil \frac{r}{2^x} \right\rceil + \left\lceil \frac{s_0}{2^x} \right\rceil - 1 + 2^{y-x} \left\lceil \frac{s_1}{2^y} \right\rceil \right).$$

Además $\left\lceil \frac{s_1}{2^y} \right\rceil \geq \frac{s_1}{2^y}$, de ahí que $2^{y-x} \left\lceil \frac{s_1}{2^y} \right\rceil \geq \frac{s_1}{2^x}$, así

$$\kappa_T(r, s_0) + \kappa_T(r, s_1) \geq 2^x \left(\left\lceil \frac{r}{2^x} \right\rceil + \left\lceil \frac{s_0}{2^x} \right\rceil - 1 + \left\lceil \frac{s_1}{2^x} \right\rceil \right).$$

Por otro lado $\lceil \xi_1 \rceil + \lceil \xi_2 \rceil \geq \lceil \xi_1 + \xi_2 \rceil$ para todo $\xi_1, \xi_2 \in \mathbb{R}$, entonces

$$\kappa_T(r, s_0) + \kappa_T(r, s_1) \geq 2^x \left(\left\lceil \frac{r}{2^x} \right\rceil + \left\lceil \frac{s_0 + s_1}{2^x} \right\rceil - 1 \right) \geq \kappa_{\widehat{H}}(r, s_0 + s_1).$$

La última desigualdad se debe a que 2^x es un divisor de $|H|$. □

A pesar de que un grupo finito G de orden 2^{n+3}, por el teorema 3.2 es un p-grupo, se presenta la demostración obtenida por Benavides, Castillo y Mutis (ver [Benavides, Castillo & Mutis, 2009]), para la función μ_G en grupos hamiltonianos de orden 2^{n+3}, porque fue el que abrió camino a la búsqueda de nuevas soluciones.

Teorema 3.12. Sea n un entero no negativo. Si $\widehat{H}$ 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 que $\mu_{\widehat{H}}(r, s) = \kappa_{\widehat{H}}(r, s)$.

Demostración. Dado que $\widehat{H}$ es un grupo hamiltoniano de orden 2^{n+3} entonces, por el teorema 3.9, $\widehat{H} \cong \mathscr{Q} \times (\mathbb{Z}_2)^n$, donde $\mathscr{Q}$ es el grupo de los cuaterniones. Por el teorema 3.10 y el corolario 2.2 se tiene que la desigualdad $\mu_{\widehat{H}}(r,s) \leq \kappa_{\widehat{H}}(r,s)$. La prueba de la desigualdad $\mu_{\widehat{H}}(r,s) \geq \kappa_{\widehat{H}}(r,s)$ procede por inducción sobre n. Para $n = 0$ se tiene que $|\widehat{H}| = 2^3 = 8$, luego $\widehat{H} = \mathscr{Q}$ y el teorema 3.11 implica que

$$\mu_{\widehat{H}}(r,s) \geq \kappa_{\widehat{H}}(r,s) \text{ para todo par de enteros positivos } r, s \leq |\mathscr{Q}|.$$

Ahora, supóngase que el enunciado se cumple para todo entero $n > 1$, es decir, si $\mathscr{T}$ es un subgrupo hamiltoniano de orden 2^{n+3} entonces

$$\mu_{\mathscr{T}}(r,s) \geq \kappa_{\mathscr{T}}(r,s) \quad \text{para todo par de enteros positivos } r, s \leq 2^{n+3}.$$

Sea H un grupo hamiltoniano de orden 2^{n+4} y considerando al grupo hamiltoniano $\mathscr{T} = \mathscr{Q} \times (\mathbb{Z}_2)^n$ como un subgrupo de H de índice 2, entonces existe un elemento c en el centro de H tal que c es de orden 2 y $H = \mathscr{T} \cup \mathscr{T}c$. Ahora sean r y s enteros tales que $1 \leq r, s \leq 2^{n+4}$ y A, B dos subconjuntos de H que realizan $\mu_H(r,s)$. Para probar que $\mu_H(r,s) \geq \kappa_H(r,s)$ se escogen subconjuntos $A_0, A_1, B_0, B_1 \subset \mathscr{T}$ de cardinales r_0, r_1, s_0, s_1, respectivamente, tales que

$$A = A_0 \cup A_1 c \text{ y } B = B_0 \cup B_1 c.$$

Así que

$$AB = (A_0B_0 \cup A_1B_1) \cup (A_0B_1 \cup A_1B_0)c,$$

de donde

$$\mu_H(r,s) = |AB| = |A_0B_0 \cup A_1B_1| + |A_0B_1 \cup A_1B_0|. \tag{3.9}$$

Ahora se consideran los siguientes casos:

1. Si $A_1 = B_1 = \emptyset$. En este caso $r = |A| = |A_0| = r_0$, $s = |B| = |B_0| = s_0$, y de la ecuación 3.9 se tiene que

$$\mu_{\mathscr{T}}(r,s) \leq |A_0B_0| = |AB| = \mu_H(r,s) \leq \mu_{\mathscr{T}}(r,s),$$

es decir, $\mu_H(r,s) = \mu_{\mathscr{T}}(r,s)$. Aplicando la hipótesis inductiva al grupo hamiltoniano $\mathscr{T}$ de orden 2^{n+3} se tiene que $\mu_{\mathscr{T}}(r,s) = \kappa_{\mathscr{T}}(r,s) \geq \kappa_H(r,s)$, por lo tanto

$$\mu_H(r,s) \geq \kappa_H(r,s).$$

2. Los casos $A_1 = B_0 = \emptyset$, $A_0 = B_1 = \emptyset$ y $A_0 = B_0 = \emptyset$ implican $r = r_0$, $s = s_1$ y por la ecuación 3.9 se tiene la desigualdad

$$\mu_{\mathscr{T}}(r,s) \leq \mu_H(r,s) \leq \mu_{\mathscr{T}}(r,s).$$

Procediendo de forma similar al caso anterior, se sigue que

$$\mu_H(r,s) \geq \kappa_H(r,s).$$

3. Si $A_1 = \emptyset$ y $A_0, B_0, B_1 \neq \emptyset$. En este caso $r = r_0$ y por la ecuación 3.9 se tiene que

$$\mu_H(r,s) = |A_0 B_0| + |A_0 B_1|.$$

La hipótesis inductiva aplicada al grupo hamiltoniano $\mathscr{T}$ implica que

$$\mu_H(r,s) \geq \mu_{\mathscr{T}}(r_0,s_0) + \mu_{\mathscr{T}}(r_0,s_1) = \kappa_{\mathscr{T}}(r,s_0) + \kappa_{\mathscr{T}}(r,s_1), \tag{3.10}$$

y aplicando el lema 3.2 a la desigualdad 3.10, se sigue que

$$\mu_H(r,s) \geq \kappa_H(r,s_0+s_1) = \kappa_H(r,s).$$

4. Si $A_0 = \emptyset$ y $A_1, B_0, B_1 \neq \emptyset$. En este caso $r = r_1$ y de la ecuación 3.9 se tiene que

$$\mu_H(r,s) = |A_1 B_1| + |A_1 B_0|.$$

La hipótesis inductiva aplicada al grupo hamiltoniano $\mathscr{T}$ implica que

$$\mu_H(r,s) \geq \mu_{\mathscr{T}}(r_1,s_1) + \mu_{\mathscr{T}}(r_1,s_0) = \kappa_{\mathscr{T}}(r,s_1) + \kappa_{\mathscr{T}}(r,s_0), \tag{3.11}$$

y aplicando el lema 3.2 a la desigualdad 3.11, se sigue que

$$\mu_H(r,s) \geq \kappa_H(r,s_0+s_1) = \kappa_H(r,s).$$

5. El caso $B_1 = \emptyset$ y $A_0, A_1, B_0 \neq \emptyset$ es similar al caso 3 y el caso $B_0 = \emptyset$ y $A_0, A_1, B_1 \neq \emptyset$ es similar al caso 4.

6. Finalmente supóngase $A_0, A_1, B_0, B_1 \neq \emptyset$. De la ecuación 3.9 se tiene que

$$\mu_H(r,s) \geq \max\{|A_0B_0|, |A_1B_1|\} + \max\{|A_0B_1|, |A_1B_0|\},$$

luego

$$\mu_H(r,s) \geq \max\{\mu_{\mathscr{J}}(r_0,s_0), \mu_{\mathscr{J}}(r_1,s_1)\} + \max\{\mu_{\mathscr{J}}(r_0,s_1), \mu_{\mathscr{J}}(r_1,s_0)\}. \quad (3.12)$$

Aplicando la hipótesis inductiva en la desigualdad 3.12, se sigue que

$$\mu_H(r,s) \geq \max\{\kappa_{\mathscr{J}}(r_0,s_0), \kappa_{\mathscr{J}}(r_1,s_1)\} + \max\{\kappa_{\mathscr{J}}(r_0,s_1), \kappa_{\mathscr{J}}(r_1,s_0)\}. \quad (3.13)$$

Ahora, el conjunto $\mathbb{N}_0$, de los enteros no negativos, tiene estructura de espacio vectorial sobre el campo finito $\mathbb{F}_2$, donde la suma de vectores es la suma p-adica (ver definición 3.2) con $p = 2$. Sea $\mathscr{V}$ el subespacio de $\mathbb{N}_0$ generado por el conjunto $\{1, 2, 2^2, \ldots, 2^{n+2}\}$, es decir, $G = \{0, 1, 2, \ldots, 2^{n+3} - 1\}$. Utilizando la notación I_t para representar el segmento inicial de longitud t de $\mathscr{V}$ (ver definición 1.10), se sigue que

$$\mu_{\mathscr{V}}(u,v) = |I_u \oplus_2 I_v| \quad \text{siempre que} \quad 1 \leq u, v \leq |\mathscr{V}|. \quad (3.14)$$

Sea M el grupo abeliano de orden 2^{n+4} definido por $M = \mathscr{V} \times \mathbb{Z}_2$. Por el teorema 1.8 y el hecho que el conjunto $\mathscr{H}(M)$ de todos los órdenes de subgrupos finitos de M coincide con el conjunto de todos los órdenes de subgrupos finitos de H, se tiene que

$$\mu_M(r,s) = \kappa_M(r,s) = \kappa_H(r,s). \quad (3.15)$$

Ahora, viendo al grupo $\mathscr{V}$ como un subgrupo de M y tomando $b = (0,1) \in M$ se sigue que $M = \mathscr{V} \cup (\mathscr{V} + b)$. Sean $I_{r_0}, I_{r_1}, I_{s_0}, I_{s_1}$ los segmentos iniciales de $\mathscr{V}$ de longitudes r_0, r_1, s_0, s_1, respectivamente, y se consideran los conjuntos

$$E = I_{r_0} \cup (I_{r_1} + b) \quad \text{y} \quad D = I_{s_0} \cup (I_{s_1} + b).$$

Entonces,

$$|E| = |I_{r_0} \cup (I_{r_1} + b)| = |I_{r_0}| + |I_{r_1}| = r_0 + r_1 = r$$

$$|D| = |I_{s_0} \cup (I_{s_1} + b)| = |I_{s_0}| + |I_{s_1}| = s_0 + s_1 = s$$

además,

$$E + D = [(I_{r_0} \oplus_2 I_{s_0}) \cup (I_{r_1} \oplus_2 I_{s_1})] \cup \{[(I_{r_0} \oplus_2 I_{s_1}) \cup (I_{r_1} \oplus_2 I_{s_0})] + b\}.$$

Así que,

$$\mu_M(r,s) \leq |(I_{r_0} \oplus_2 I_{s_0}) \cup (I_{r_1} \oplus_2 I_{s_1})| + |(I_{r_0} \oplus_2 I_{s_1}) \cup (I_{r_1} \oplus_2 I_{s_0})|. \qquad (3.16)$$

Dado que la suma de dos segmentos iniciales de $\mathscr{V}$ es de nuevo un segmento inicial de $\mathscr{V}$, entonces de la ecuación 3.14 y la desigualdad 3.16 se tiene que

$$\mu_M(r,s) \leq \left|I_{\mu_{\mathscr{V}}(r_0,s_0)} \cup I_{\mu_{\mathscr{V}}(r_1,s_1)}\right| + \left|I_{\mu_{\mathscr{V}}(r_0,s_1)} \cup I_{\mu_{\mathscr{V}}(r_1,s_0)}\right|.$$

Pero

$$I_{\mu_{\mathscr{V}}(r_0,s_0)} \cup I_{\mu_{\mathscr{V}}(r_1,s_1)} = I_{\max\{\mu_{\mathscr{V}}(r_0,s_0),\mu_{\mathscr{V}}(r_1,s_1)\}}$$

$$I_{\mu_{\mathscr{V}}(r_0,s_1)} \cup I_{\mu_{\mathscr{V}}(r_1,s_0)} = I_{\max\{\mu_{\mathscr{V}}(r_0,s_1),\mu_{\mathscr{V}}(r_1,s_0)\}}.$$

Luego

$$\mu_M(r,s) \leq \max\{\mu_{\mathscr{V}}(r_0,s_0), \mu_{\mathscr{V}}(r_1,s_1)\} + \max\{\mu_{\mathscr{V}}(r_0,s_1), \mu_{\mathscr{V}}(r_1,s_0)\}.$$

Como $\mathscr{V}$ es abeliano, el teorema 1.8 implica

$$\mu_M(r,s) \leq \max\{\kappa_{\mathscr{V}}(r_0,s_0), \kappa_{\mathscr{V}}(r_1,s_1)\} + \max\{\kappa_{\mathscr{V}}(r_0,s_1), \kappa_{\mathscr{V}}(r_1,s_0)\}.$$

Además, los conjuntos de ordenes de subgrupos $\mathscr{H}(\mathscr{T})$ y $\mathscr{H}(\mathscr{V})$, son iguales, así que

$$\mu_M(r,s) \leq \max\{\kappa_{\mathscr{T}}(r_0,s_0), \kappa_{\mathscr{T}}(r_1,s_1)\} + \max\{\kappa_{\mathscr{T}}(r_0,s_1), \kappa_{\mathscr{T}}(r_1,s_0)\}. \qquad (3.17)$$

La desigualdad 3.13, la ecuación 3.15 y la desigualdad 3.17 implican

$$\mu_H(r,s) \geq \kappa_H(r,s).$$

□

Teorema 3.13. En el grupo $H = \mathscr{Q} \times (\mathbb{Z}/2\mathbb{Z})^k \times G$, con G un grupo cíclico de orden impar, se tiene que $\mu_H(r,s) = \kappa_H(r,s)$, para todo par de enteros positivos $r, s \leq |H|$.

Demostración. Por el teorema 3.10 y el lema 2.2 de [Eliahou & Kervaire, 2006] se obtiene que $\mu_H(r,s) \leq \kappa_H(r,s)$. Sea $b = (1,0,g) \in H$ entonces b es un elemento de orden n en el centro de H, luego

$$H = \widehat{H} \cup \widehat{H}b \cup \cdots \cup \widehat{H}b^{n-1}$$

con $\widehat{H} = \mathscr{Q} \times (\mathbb{Z}/2\mathbb{Z})^k$.

Sean $A, B \subseteq H$ que realizan $\mu_H(r,s)$, existen subconjuntos $A_{r_0}, A_{r_1}, \ldots, A_{r_{n-1}}$ de $\widehat{H}$ y de cardinales $r_0, r_1, \ldots, r_{n-1}$, respectivamente, con $\sum r_i = r$ y existen subconjuntos $B_{s_0}, B_{s_1}, \ldots, B_{s_{n-1}}$ de $\widehat{H}$ y de cardinales $s_0, s_1, \ldots, s_{n-1}$, respectivamente, con $\sum s_i = s$ tales que

$$A = \bigcup_{i=0}^{n-1} A_{r_i} b^i \qquad \text{y} \qquad B = \bigcup_{i=0}^{n-1} B_{s_i} b^i.$$

Sea $F_l = \{\ (i,j) \mid 0 \leq i,j \leq n-1,\ i+j \cong l(\ \ \text{mód}\ n)\ \}$ entonces

$$AB = \left(\bigcup_{i=0}^{n-1} A_{r_i} b^i \right) \left(\bigcup_{j=0}^{n-1} B_{s_j} b^j \right) = \bigcup_{l=0}^{n-1} \left[\left(\bigcup_{(i,j)\in F_l} A_{r_i} B_{s_j} \right) b^l \right].$$

De ahí que,

$$\begin{aligned} \mu_H(r,s) &= |AB| = \sum_{l=0}^{n-1} \left| \bigcup_{(i,j)\in F_l} A_{r_i} B_{s_j} \right| \\ \mu_H(r,s) &\geq \sum_{l=0}^{n-1} (\text{máx}\{\ |A_{r_i} B_{r_j}| \mid (i,j) \in F_l\}) \\ &\geq \sum_{l=0}^{n-1} (\text{máx}\{\ \mu_{\widehat{H}}(r_i, s_j) \mid (i,j) \in F_l\}). \end{aligned}$$

Por el teorema 3.12,

$$\mu_H(r,s) \geq \sum_{l=0}^{n-1} (\text{máx}\{\ \kappa_{\widehat{H}}(r_i, s_j) \mid (i,j) \in F_l\}). \tag{3.18}$$

Sea $\mathscr{V}$ el subespacio de $\mathbb{N}_0$ mencionado anteriormente, se sigue que

$$\mu_{\mathscr{V}}(u,v) = |I_u \oplus_2 I_v| \quad \text{siempre que } \ 1 \leq u, v \leq |\mathscr{V}|. \tag{3.19}$$

Sea $M = \mathscr{V} \times (\mathbb{Z}/n\mathbb{Z})$. Dado que M es abeliano y $\mathscr{H}(M) = \mathscr{H}(H)$ se tiene que

$$\mu_M(r,s) = \kappa_M(r,s) = \kappa_H(r,s). \tag{3.20}$$

Ahora, viendo al grupo $\mathscr{V}$ como un subgrupo de M y tomando $b = (0,1) \in M$, se sigue que $M = \bigcup_{k=0}^{n-1} (\mathscr{V} + kb)$. Sean $I_{r_0}, I_{r_1}, \ldots, I_{r_{n-1}}$ los segmentos iniciales de $\mathscr{V}$ de longitudes $r_0, r_1, \ldots, r_{n-1}$ respectivamente y $I_{s_0}, I_{s_1}, \ldots, I_{s_{n-1}}$ los segmentos iniciales de $\mathscr{V}$ de longitudes $s_0, s_1, \ldots, s_{n-1}$, respectivamente. Considerando los conjuntos

$$E = \bigcup_{k=0}^{n-1} (I_{r_k} + kb) \quad \text{y} \quad D = \bigcup_{k=0}^{n-1} (I_{s_k} + kb).$$

Entonces,

$$|E| = \sum_{k=0}^{n-1} r_k = r$$

$$|D| = \sum_{k=0}^{n-1} s_k = s$$

además, si $F_l = \{\ (i,j) \mid 0 \leq i,j \leq n-1,\ i + j \cong l(\mod n)\}$,

$$E + D = \bigcup_{l=0}^{n-1} \left[\left(\bigcup_{(i,j) \in F_l} (I_{r_i} \oplus_2 I_{s_j}) \right) + lb \right].$$

Así que

$$\mu_M(r,s) \leq \sum_{l=0}^{n-1} \left| \left(\bigcup_{(i,j) \in F_l} I_{\mu_{\mathscr{V}}(r_i, s_j)} \right) \right|.$$

Por otro lado,

$$I_{\mu_{\mathscr{V}}(r_i,s_j)} \cup I_{\mu_{\mathscr{V}}(r_k,s_t)} = I_{\max\{\mu_{\mathscr{V}}(r_i,s_j), \mu_{\mathscr{V}}(r_k,s_t)\}},$$

entonces

$$\mu_M(r,s) \leq \sum_{l=0}^{n-1} \max\{\ \mu_{\mathscr{V}}(r_i,s_j) \mid (i,j) \in F_l\ \}.$$

Como $\mathscr{V}$ es abeliano, se tiene que

$$\mu_M(r,s) \leq \sum_{l=0}^{n-1} \text{máx}\{\ \kappa_{\mathscr{V}}(r_i, s_j) \mid (i,j) \in F_l\ \}.$$

Además $\mathscr{H}(\widehat{H}) = \mathscr{H}(\mathscr{V})$, luego

$$\mu_M(r,s) \leq \sum_{l=0}^{n-1} \text{máx}\{\ \kappa_{\widehat{H}}(r_i, s_j) \mid (i,j) \in F_l\ \}.$$

La desigualdad 3.18, la ecuación 3.20 y la desigualdad anterior implican que

$$\mu_H(r,s) \geq \kappa_H(r,s).$$

□

Capítulo 4

LA FUNCIÓN μ_G EN PRODUCTOS DIRECTOS

En este capítulo se describen los principales resultados obtenidos en el presente trabajo de investigación, entre los cuales está una solución al problema de los conjuntos suma pequeños en grupos hamiltonianos finitos. Además, se presenta una fórmula para la función μ_G, cuando G es un grupo soluble finito que se puede escribir como producto directo de sus p-subgrupos de Sylow. Finalmente, se dan a conocer los resultados obtenidos en ciertos grupos infinitos, que se pueden ver como producto directo finito de otros grupos.

4.1. LA FUNCIÓN μ_G EN GRUPOS FINITOS

Los resultados que se muestran a continuación, son el fruto del estudio detallado de los artículos [Benavides, Castillo & Mutis, 2009], [Benavides, Castillo & Mutis, 2010] y [Eliahou & Kervaire, 2010].

Teorema 4.1. *Sea H un grupo hamiltoniano finito, entonces $\mathscr{N}\kappa_H(r,s) = \mathscr{D}\kappa_H(r,s)$.*

Demostración. Por teorema 3.9, $H = \mathscr{Q} \times (\mathbb{Z}/2\mathbb{Z})^n \times G$ donde G es un grupo abeliano en el que todo elemento es orden finito impar.

Sea $d \in \text{Div}(|H|) = \{2^t k / \ 0 \leq t \leq n+3$ y $k \Big| |G|\}$.

Luego $d = 2^t k$ para algún $t \in \{0, 1, \ldots, n+3\}$ y algún k divisor de $|G|$. Dado que G es abeliano finito, existe $K \trianglelefteq G$ tal que $|K| = k$, consideremos los siguientes casos:

Caso 1. Si $t \leq n$, entonces

$$\{1\} \times (\mathbb{Z}/2\mathbb{Z})^t \times K \trianglelefteq H \ \text{ y } \ \Big|\{1\} \times (\mathbb{Z}/2\mathbb{Z})^t \times K\Big| = d.$$

Caso 2. Si $n+1 \leq t \leq n+3$*, entonces existe un subgrupo normal* M *de* $\mathscr{Q}$ *con* $|M| = 2^{t-n}$ *y se tiene que*

$$M \times (\mathbb{Z}/2\mathbb{Z})^n \times K \trianglelefteq H \text{ y } |M \times (\mathbb{Z}/2\mathbb{Z})^n \times K| = d.$$

De ahí que

$$\textit{Div}(|H|) = \mathscr{D}(G) = \mathscr{N}(G).$$

□

Lo anterior, junto con las desigualdades (2.1) *y* (2.2)*, implican que en un grupo hamiltoniano finito* H *se satisface la igualdad* $\mu_H(r,s) = \kappa_H(r,s)$*, para todo par de enteros no negativos* $r, s \leq |H|$*. De esta manera, se reafirma el resultado obtenido por Benavides, Castillo y Mutis en [Benavides, Castillo & Mutis, 2010].*

Corolario 4.1. Sea P un p-grupo finito, entonces $\mu_P(r,s) = \kappa_P(r,s)$.

Demostración. Por teorema 3.6, para cada divisor positivo t de $|P|$ existe un subgrupo normal T de P tal que $|T| = t$, entonces $\mathscr{N}(P) = \mathscr{D}(P)$ y por lo tanto $\mathscr{N}\kappa_P(r,s) = \mathscr{D}\kappa_P(r,s)$. □

Teorema 4.2. Sea G un grupo finito, tal que $G = P_1 \times P_2 \times \cdots \times P_n$, donde P_i es un P-grupo, $|P_i| = {p_i}^{\alpha_i}$ y $p_i \neq p_j$ siempre que $i \neq j$ para todo $i, j = 1, 2, \ldots, n$, entonces $\mathscr{D}\kappa_G(r,s) = \mathscr{N}\kappa_G(r,s)$ para todo par de enteros no negativo $r, s \leq |G|$.

Demostración. Se tiene que $|G| = {p_1}^{\alpha_1}{p_2}^{\alpha_2}\cdots{p_n}^{\alpha_n}$.

Sea $d \in \text{Div}(|G|)$, entonces $d = {p_1}^{\beta_1}{p_2}^{\beta_2}\cdots{p_n}^{\beta_n}$ con $0 \leq \beta_i \leq \alpha_i$ para todo $i = 1, 2, \ldots, n$. Como $\mathscr{D}(P_i) = \mathscr{N}(P_i)$ para todo $i = 1, 2, \ldots, n$, entonces existen $Q_i \trianglelefteq P_i$ tales que $|Q_i| = {p_i}^{\beta_i}$ para todo $i = 1, 2, \ldots, n$.

Así que $Q_1 \times Q_2 \times \cdots \times Q_n \trianglelefteq G$ y $|Q_1 \times Q_2 \times \cdots \times Q_n| = d$.

Por lo tanto $\mathscr{D}(G) = \mathscr{N}(G)$, y en consecuencia $\mathscr{D}\kappa_G(r,s) = \mathscr{N}\kappa_G(r,s)$ para todo par de enteros no negativos $r, s \leq |G|$. □

De este teorema se deduce que si G es un grupo soluble finito y se puede escribir como producto directo de p-grupos, entonces $\mu_G(r,s) = \kappa_G(r,s)$ para todo par de enteros $r, s \leq |G|$. En particular, si un grupo soluble G es el producto directo de sus p-subgrupos de Sylow, entonces $\mu_G(r,s) = \kappa_G(r,s)$.

Corolario 4.2. Sea G un grupo nilpotente finito, entonces $\mu_G(r,s) = \kappa_G(r,s)$ para todo par de enteros no negativos $r, s \leq |G|$.

4.2. LA FUNCIÓN μ_G EN GRUPOS INFINITOS

A continuación se presenta uno de los principales resultados, que abre paso a la solución del Problema de los Conjuntos Suma Pequeños en algunas clases específicas de grupos no abelianos infinitos.

Lema 4.1. Sea $G = G_1 \times G_2$, el producto directo de los grupos G_1 y G_2, y sean $A, B \subseteq G$ tales que $A = A_1 \times A_2$ y $B = B_1 \times B_2$ donde $A_1, B_1 \subseteq G_1$ y $A_2, B_2 \subseteq G_2$, entonces

$$A \cdot B = (A_1 \cdot B_1) \times (A_2 \cdot B_2)$$

Demostración. Sea $x \in A \cdot B$, entonces $x = a \cdot b$, tal que $a \in A$ y $b \in B$. Puesto que $A = A_1 \times A_2$ y $B = B_1 \times B_2$ se tiene que $a = (a_1, a_2)$ y $b = (b_1, b_2)$, con $a_i \in A_i$ y $b_i \in B_i$ para $i = 1, 2$.

Así,

$$\begin{aligned} x &= (a_1, a_2) \cdot (b_1, b_2) \\ &= (a_1 \cdot b_1, a_2 \cdot b_2). \end{aligned}$$

Como $a_1 \cdot b_1 \in A_1 \cdot B_1$ y $a_2 \cdot b_2 \in A_2 \cdot B_2$, entonces $x \in (A_1 \cdot B_1) \times (A_2 \cdot B_2)$.

Por otro lado, sea $x \in (A_1 \cdot B_1) \times (A_2 \cdot B_2)$, entonces $x = (a_1 \cdot b_1, a_2 \cdot b_2)$ con $a_1 \cdot b_1 \in A_1 \cdot B_1$ y $a_2 \cdot b_2 \in A_2 \cdot B_2$, luego $a_i \in A_i$ y $b_i \in B_i$ para $i = 1, 2$. De donde se obtiene que

$$x = (a_1, a_2) \cdot (b_1, b_2) \in (A_1 \times A_2) \cdot (B_1 \times B_2) = A \cdot B.$$

Por lo tanto $x \in A \cdot B$. □

Este resultado implica que

$$|(A_1 \times A_2) \cdot (B_1 \times B_2)| = |A_1 \cdot B_1||A_2 \cdot B_2|, \tag{4.1}$$

cuando $A = A_1 \times A_2$ *y* $B = B_1 \times B_2$ *son finitos.*

Teorema 4.3. Sea G un grupo tal que $G = G_1 \times G_2$, el producto directo de los grupos G_1 y G_2. Para todos los enteros no negativos $r_1, s_1 \leq |G_1|$, $r_2, s_2 \leq |G_2|$, se tiene que

$$\mu_G(r_1 r_2, s_1 s_2) \leq \mu_{G_1}(r_1, s_1)\mu_{G_2}(r_2, s_2).$$

Demostración. Sean $r_1, s_1 \leq |G_1|$ y $r_2, s_2 \leq |G_2|$, entonces existen $A_1, B_1 \subseteq G_1$ y $A_2, B_2 \subseteq G_2$ de cardinales r_1, s_1, r_2, s_2 respectivamente, tales que $|A_1 \cdot B_1| = \mu_{G_1}(r_1, s_1)$ y $|A_2 \cdot B_2| = \mu_{G_2}(r_2, s_2)$.

Sean $A = A_1 \times A_2$ y $B = B_1 \times B_2$, entonces $|A| = r_1 r_2$ y $|B| = s_1 s_2$.

Puesto que $\mu_G(r_1 r_2, s_1 s_2) \leq |A \cdot B|$, se sigue que

$$\begin{aligned} \mu_G(r_1 r_2, s_1 s_2) &\leq |A_1 \cdot B_1||A_2 \cdot B_2| \qquad \text{por (4.1).} \\ &= \mu_{G_1}(r_1, s_1)\mu_{G_2}(r_2, s_2) \qquad \text{por hipótesis.} \end{aligned}$$

Por lo tanto $\mu_G(r_1 r_2, s_1 s_2) \leq \mu_{G_1}(r_1, s_1)\mu_{G_2}(r_2, s_2)$. □

El teorema 4.3 se puede generalizar como sigue:

Teorema 4.4. Sea $G = G_1 \times G_2 \times \cdots \times G_n$, el producto directo finito de los grupos $G_1, G_2, \ldots, G_n$. Si $r_i, s_i \leq |G_i|$ para toda $i = 1, 2, \ldots n$, entonces

$$\mu_G(r_1 r_2 \ldots r_n, s_1 s_2 \ldots s_n) \leq \mu_{G_1}(r_1, s_1)\mu_{G_2}(r_2, s_2) \cdots \mu_{G_n}(r_n, s_n)$$

Demostración. Se procederá por inducción matemática. Para $n = 2$, se tiene que $G = G_1 \times G_2$. Luego por el teorema 4.3, para todos los pares de enteros tales que $0 \leq r_1, s_1 \leq |G_1|$ y $0 \leq r_2, s_2 \leq |G|$, se verifica que

$\mu_G(r_1r_2, s_1s_2) \leq \mu_{G_1}(r_1, s_1)\mu_{G_2}(r_2, s_2)$.

Supóngase que para $n = k$ se satisface el teorema, es decir, que para $G' = G_1 \times G_2 \times \cdots \times G_k$, si $0 \leq r_i, s_i \leq |G_i|$ para todo $i = 1, 2, \ldots, k$, entonces

$$\mu_{G'}(r_1r_2 \ldots r_k, s_1s_2 \ldots s_k) \leq \mu_{G_1}(r_1, s_1)\mu_{G_2}(r_2, s_2) \cdots \mu_{G_k}(r_k, s_k).$$

Ahora para $n = k + 1$, sea $G = G_1 \times G_2 \times \cdots \times G_{k+1}$. Puesto que el producto directo finito de grupos es un grupo, entonces $G^{'} = G_1 \times G_2 \times \cdots \times G_k$ es un grupo, luego $G = G^{'} \times G_{k+1}$ y por teorema 4.3, se sigue que para todos los pares de enteros no negativos $r^{'}, s^{'} \leq |G^{'}|$ y $r_{k+1}, s_{k+1} \leq |G_{k+1}|$ se tiene que

$$\mu_G(r^{'}r_{k+1}, s^{'}s_{k+1}) \leq \mu_{G'}(r^{'}, s^{'})\mu_{G_{k+1}}(r_{k+1}, s_{k+1}).$$

Por lo tanto, aplicando la hipótesis de inducción se sigue que $r^{'}r_{k+1} = r_1r_2 \ldots r_kr_{k+1}$, $s^{'}s_{k+1} = s_1s_2 \ldots s_ks_{k+1}$, y

$$\begin{aligned}\mu_G(r_1r_2 \ldots r_kr_{k+1}, s_1s_2 \ldots s_ks_{k+1}) &= \mu_G(r^{'}r_{k+1}, s^{'}s_{k+1}) \\ &\leq \mu_{G'}(r^{'}, s^{'})\mu_{G_{k+1}}(r_{k+1}, s_{k+1}) \\ &\leq \mu_{G_1}(r_1, s_1)\mu_{G_2}(r_2, s_2) \cdots \mu_{G_k}(r_k, s_k)\mu_{G_{k+1}}(r_{k+1}, s_{k+1}).\end{aligned}$$

□

Proposición 4.1. Sea G un grupo tal que $G = G_1 \times G_2$, el producto directo de los grupos G_1 y G_2. Sean $r, s \leq |G|$ enteros no negativos, entonces existen enteros $r_1, s_1 \leq |G_1|$, $r_2, s_2 \leq |G_2|$ tales que $r = r_1r_2$, $s = s_1s_2$ y

$$\mu_G(r, s) \geq \mu_{G_1}(r_1, s_1)\mu_{G_2}(r_2, s_2).$$

Demostración. Sean $A, B \subseteq G$ tales que $|A \cdot B| = \mu_G(r, s)$, entonces existen $A_1, B_1 \subseteq G_1$ y $A_2, B_2 \subseteq G_2$ tales que $A = A_1 \times A_2$ y $B = B_1 \times B_2$.

Dado que $|A| = |A_1||A_2|$ y $|B| = |B_1||B_2|$, entonces $r = r_1r_2$ y $s = s_1s_2$, donde $r_1 = |A_1|$, $r_2 = |A_2|$, $s_1 = B_1$ y $s_2 = B_2$. Luego se tiene que

$$\begin{aligned}\mu_G(r,s) &= |A \cdot B| \qquad \text{por hipótesis.}\\ &= |A_1 \cdot B_1||A_2 \cdot B_2| \qquad \text{por (4.1).}\\ &\geq \mu_{G_1}(r_1,s_1)\mu_{G_2}(r_2,s_2).\end{aligned}$$

□

Corolario 4.3. Sea G un grupo tal que $G = G_1 \times G_2 \times \cdots \times G_n$, el producto directo finito de los grupos $G_1, G_2, \ldots, G_n$. Sean $r, s \leq |G|$ enteros no negativos, entonces existen enteros $r_i, s_i \leq |G_i|$ para toda $i = 1, 2, \ldots, n$ tales que $r = r_1r_2 \cdots r_n$, $s = s_1s_2 \cdots s_n$ y

$$\mu_G(r,s) \geq \mu_{G_1}(r_1,s_1)\mu_{G_2}(r_2,s_2) \cdots \mu_{G_n}(r_n,s_n)$$

Una consecuencia inmediata del teorema 4.4 y del corolario 4.3 es el siguiente resultado:

Corolario 4.4. Sea G un grupo tal que $G = G_1 \times G_2 \times \cdots \times G_n$, el producto directo finito de los grupos $G_1, G_2, \ldots, G_n$. Sean $r, s \leq |G|$, entonces existen enteros $r_i, s_i \leq |G_i|$ para toda $i = 1, 2, \ldots, n$ tales que $r = r_1r_2 \cdots r_n$, $s = s_1s_2 \cdots s_n$ y $\mu_G(r,s) = \mu_{G_1}(r_1,s_2)\mu_{G_2}(r_2,s_2) \cdots \mu_{G_n}(r_n,s_n)$.

Apéndice A

ALGORITMOS

Los algoritmos que se presentan a continuación fueron elaborados por los autores y utilizados en el desarrollo de este trabajo. Estos algoritmos están implementados en el sistema de álgebra computacional GAP.

A.1. ALGORITMO FUNCIÓN μ_G

A.1.1. ALGORITMO SubConj

El algoritmo recibe un grupo G y dos enteros positivos u, i. El parámetro u es el cardinal de un subconjunto A de G, por ende, no puede ser mayor que el orden de G. i es una posición en el conjunto de todos los subconjuntos de G de cardinal u, el cual tiene tamaño n. Este algoritmo, como salida imprime, o bien, un conjunto de cardinal u ubicado en la posición i ó un mensaje donde se pide cambiar un parámetro.

```
>SubConj:=function(G,u,i)
 local n, m;
 m:=Order(G);
 GrCn:=Set(G);
 if u<=m then
   gr:=Combinations(GrCn,u);
   n:=Number(gr);
   if i<>0 then
      if n>=i then
         subconjunto:=gr[i];
         return subconjunto;
      else
```

```
        return ["argumentos SubConj(Set,u,i) i<=",n];
      fi;
   else
   return [n,gr];
   fi;
 else
 return ["argumentos SubConj(Set,u,i) u<=",m];
 fi;
 end;
```

A.1.2. ALGORITMO CardProd

Este algoritmo CardProd recibe dos conjuntos Conj1 y Conj2, y devuelve a p, quien es el cardinal de su conjunto producto.

```
>CardProd:=function(Conj1,Conj2)
 local n,m,p;
 n:=Number(Conj1);
 m:=Number(Conj2);
 Prod:=Set([]);
 for i in [1..n] do
   for j in [1..m] do
      H:=Conj1[i]*Conj2[j];
      Prod:=Union(Prod,[H]);
   od;
 od;
 p:=Number(Prod);
 return p;
 end;
```

A.1.3. ALGORITMO Mu_G

El algoritmo recibe un grupo `G` *y dos enteros no negativos* `r, s`*. Como salida retorna una lista en orden descendente, la cual culmina con el valor de* $\mu_G(r, s)$*.*

```
>Mu_G:=function(G,r,s)
 local m, cd1, cd2, l;
 GrCn:=Set(G);
 gr1:=Combinations(GrCn,r);
 gr2:=Combinations(GrCn,s);
 cd1:=Number(gr1);
 cd2:=Number(gr2);
 l:=Number(GrCn);
 for i in [1..cd1] do
   conj1:=gr1[i];
   for j in [1..cd2] do
      conj2:=gr2[j];
      m:=CardProd(conj1, conj2);
      if m<l then l:=m;
      fi;
   od;
   Print (l,"\n");
 od;
 return [l];
end;
```

A.2. ALGORITMO FUNCIÓN κ_G

A.2.1. ALGORITMO Techo

Este algoritmo recibe dos enteros `m, n` *y como salida imprime el techo de su cociente,* $\left\lceil \frac{m}{n} \right\rceil$.

```
>Techo:=function(m,n)
    if IsInt(m/n) then
        return m/n;
    else
        return Int(m/n)+1;
    fi;
 end;
```

A.2.2. ALGORITMO CardSubgSol

El algoritmo recibe un grupo soluble `G` *y retorna una lista* `L` *con los cardinales de todos sus subgrupos, sin repetir elementos.*

```
>CardSubgSol:=function(G)
 l:=SubgroupsSolvableGroup(G);
 l1:=List(l,Size);
 L:=[1];
 for i in l1 do
    L:=Union(L,[i]);
 od;
 return L;
 end;
```

A.2.3. ALGORITMO kappa_G

Este algoritmo recibe un grupo soluble `G` *y dos enteros no negativos* `r, s`*, y devuelve* `K`*, tal que* `K` *es el valor de* $\kappa_G(r, s)$*.*

```
>kappa_G:=function(G,r,s)
 g:=Order(G);
 if r+s>g then
    return g;
 else
    K:=g;
    L:=CardSubgSol(G);
    for i in L do
        K1:=(Techo(r,i)+Techo(s,i)-1)*i;
        if K1<K then
            K:=K1;
        fi;
    od;
  return K;
 fi;
 end;
```

CONCLUSIONES

1. *Se presenta un panorama general del problema de los conjuntos suma pequeños en grupos finitos no abelianos, con el propósito de motivar al lector a iniciar investigaciones tendientes a comprender la función μ_G en ciertas clases de grupos finitos no abelianos.*

2. *En un grupo hamiltoniano finito H, arbitrario, se satisface la fórmula obtenida por Eliahou, Kervaire y Plagne, en grupos abelianos.*

3. *Según el corolario 4.1, se reafirma el resultado obtenido por Benavides, Castillo y Mutis, para la función μ_G en la clase de p-grupos finitos.*

4. *Se determina una fórmula explícita para la función μ_G, cuando G es el producto directo finito de otros grupos. En particular, cuando G es un grupo soluble finito que se puede escribir como producto directo de sus p-subgrupos de Sylow.*

5. *Se presentan los algoritmos desarrollados en el sistema de álgebra computacional GAP, los cuales nos condujeron a la conjetura de los teoremas demostrados en la primera sección del cuarto capitulo.*

6. *Se considera que éste trabajo de investigación contribuye a sentar las bases necesarias para continuar el estudio del problema de los conjuntos suma pequeños en grupos no abelianos, particularmente se sugiere adelantar investigaciones que den respuesta a los siguientes problemas abiertos:*

   a) *Estudiar el comportamiento de la función μ_G alrededor de las funciones aritméticas $\mathscr{D}\kappa_G(r,s)$ y $\mathscr{N}\kappa_G(r,s)$ en grupos solubles infinitos.*

   b) *El corolario 4.4 afirma que si G es un grupo tal que $G = G_1 \times G_2 \times \cdots \times G_n$, el producto directo de los grupos $G_1, G_2, \ldots, G_n$, entonces existen enteros $r_i, s_i \leq |G_i|$ para toda $i = 1, 2, \ldots, n$, tales que $r = r_1 r_2 \cdots r_n$, $s = s_1 s_2 \cdots s_n$ y $\mu_G(r,s) = \mu_{G_1}(r_1, s_2)\mu_{G_2}(r_2, s_2) \cdots \mu_{G_n}(r_n, s_n)$. Este podría ser un camino adecuado para hacer avances en el estudio de la función μ_G en grupos infinitos no abelianos.*

REFERENCIAS BIBLIOGRÁFICAS

[Benavides, Castillo & Mutis, 2009] Benavides, F., Castillo, J. & Mutis, W. (2009). Conjuntos suma pequeños en grupos hamiltonianos. preprint.

[Benavides, Castillo & Mutis, 2010] Benavides, F., Castillo, J. & Mutis, W. (2010). Conjuntos suma pequeños en p-grupos finitos. Revista Integración, 79–83.

[Bollobás & Leader, 1996] Bollobás, B & Leader, I. (1996). Sums in the grid. Discrete Math, 31–48.

[Eliahou & Kervaire, 2007] Eliahou, S. & Kervaire, M. (2007). Bounds on the minimal sumset size function in groups. J. Number Theory, 503–511.

[Eliahou & Kervaire, 2010] Eliahou, S. & Kervaire, M. (2010). Minimal sumsets in finite solvable groups. Discrete Math., 471–479.

[Eliahou & Kervaire, 2005] Eliahou, S. & Kervaire, M. (2005). Minimal sumsets in infinite abelian groups. J. Algebra, 449–457.

[Eliahou & Kervaire, 2005] Eliahou, S. & Kervaire, M. (2005). Old and new formulas for the Hopf-Stiefel and related functions. Expo. Math., 127–145.

[Eliahou, Kervaire & Plagne, 2003] Eliahou, S., Kervaire, M. & Plagne, A. (2003). Optimally small sumsets in finite abelian groups. J. Number Theory, 338–348.

[Eliahou & Kervaire, 2007] Eliahou, S. & Kervaire, M. (2007). Some results on minimal sumset sizes in finite non-abelian groups. J. Number Theory, 234–247.

[Eliahou & Kervaire, 2006] Eliahou, S. & Kervaire, M. (2006). Sumsets in dihedral groups. European J. Combin., 617–628.

[Eliahou & Kervaire, 1998] Eliahou, S. & Kervaire, M. (1998). Sumsets in vector spaces over finite fields. J. Number Theory, 12–39.

[Eliahou & Kervaire, 2006] Eliahou, S. & Kervaire, M. (2006). The small sumsets property for solvable finite groups. European J. Combin., 1102–1110.

[Kemperman, 1956] Kemperman, J. H. B. (1956). On complexes in a semigroup. Indag. Math, 247–254.

[Kemperman, 1960] Kemperman, J. H. B. (1960). On small sumsets in an abelian group. Acta Math, 63–88.

[Lev,2005] Lev, V. F. (2005). Restricted set addition in abelian groups: results and conjectures. J. Théor. Nombres Bordeaux, 181–193.

[Marshall, 1979] Marshall Hall, Jr. (1979). Teoría de los Grupos. México: Trillas. 440.p.

[Plagne, 2003] Plagne, A. (2003). Additive number theory sheds extra light on the Hopf-Stiefel $\circ$ function. Enseign. Math. (2), 109–116.

[Plagne, 2007] Plagne, A. (2007). Optimally small sumsets in general Abelian groups. Adv. in Appl. Math., 324–326.

ÍNDICE ALFABÉTICO