EL CONJUNTO SUMA EN GRUPOS DIEDRICOS

Xavier Antonio Terán Batista

Trabajo de grado
Requisito parcial para optar al título de Matemático

Asesor
María Ofelia Vásquez Ávila

Universidad de Cartagena
Facultad de Ciencias Exactas y Naturales
Programa de Matemáticas

Cartagena de Indias D. T. y C.

Marzo de 2011

Dedico este trabajo con todo cariño y amor a mi madre Isabel Batista, por todo el esfuerzo y tolerancia que me brindo durante mi carrera, a mi hija Isabel Terán Vega y en especial a mi padre José M. Batista Martínez Q.E.P.D y a todos mis familiares que me apoyaron de un modo u otro, que me son imposible mencionar.

Doy gracias en primera instancia a Dios y a la Virgen, a mi esposa Ana Vega, a la Doctora María Ofelia Vásquez por su gran apoyo incondicional y a todos mis compañeros por su amistad y ayuda.

Índice general

Introducción IV

1. Preliminares 1
- 1.1. Notación y Conceptos Generales 1
- 1.2. Propiedades básicas de la función μ_G 3
- 1.3. El Problema de los Conjuntos Suma Pequeños 4

2. La Función μ_G en grupos abelianos 7
- 2.1. Fórmula para μ_G en grupos abelianos 7
- 2.2. Teoremas Principales 13

3. La Función μ_G en grupos no abelianos 14
- 3.1. Desigualdad principal: $\mu_{D_n}(r,s) \leq \kappa_{D_n}(r,s)$ 14
- 3.2. Desigualdad recíproca: $\mu_{D_n}(r,s) \geq \kappa_{D_n}(r,s)$ 19
- 3.3. Comentarios sobre la función descomposición 23

Conclusiones 27

Bibliografía 28

Introducción

Sea $(G, *)$ un grupo finito y sean A, B subconjuntos de G; entonces el conjunto suma (o conjunto producto) de A y B bajo G esta dado como sigue:

$$A * B = \{a * b : a \in A \quad y \quad b \in B\},$$

además si $A = \emptyset$ o $B = \emptyset$, se define $A * B = \emptyset$. Un problema de interés en teoría aditiva de números, es que dado un grupo G y r, s enteros positivos tales que $0 \leq r, s \leq \mid G \mid$, hay que determinar una fórmula explícita que permita calcular el mínimo del cardinal del conjunto $A * B$, tal que $\mid A \mid = r$ y $\mid B \mid = s$, es decir, se desea hallar una fórmula que calcule el valor de la función $\mu_G(r, s)$ dada por:

$$\mu_G(r, s) = \text{mín}\{\mid A * B \mid : A, B \subseteq G, \mid A \mid = r \quad y \quad \mid B \mid = s\}$$

La función μ_G ha sido determinada completamente para el caso en que G es un grupo abeliano arbitrario, pero se desconoce si existe una fórmula explícita que permita calcular el valor $\mu_G(r, s)$ para el caso en que G es un grupo finito no abeliano. En [9] Eliahou y Kervaire, obtienen una cota superior para $\mu_G(r, s)$ en el caso que G es un grupo soluble finito, y acotan inferiormente esta función para grupos arbitrarios. El objetivo principal en este trabajo es aclarar como ellos prueban que la fórmula para μ_G obtenida en el caso en que G es un grupo abeliano también se cumple para ciertos grupos diédricos.

Para la ejecución de este trabajo se llevo a cabo un estudio detallado sobre la teoría de grupos diédricos, además se hizo un profundo analisis de los artículos de Eliahou y Kervaire (ver [8], [7], [9]) sobre la función μ_G en grupos no abelianos.

El trabajo está dividido en tres capítulos. En el primero se establecen las definiciones generales y la notación a emplear en el desarrollo del trabajo. En el segundo capítulo se presentan los lemas y teoremas claves para desarrollar el problema principal, además se comenta la demostración de la fórmula μ_G para grupos abelianos, obtenida por Eliahou, Kervaire y Plagne y en el capítulo final se expone de manera clara el problema principal haciendo enfasis en grupos finitos no abelianos, especialmente en los grupos diédricos.

Capítulo 1

Preliminares

En este capítulo se establecen algunas definiciones y notaciones básicas, necesarias para la comprensión de este trabajo.

1.1. Notación y Conceptos Generales

Definición 1. ***(Cardinalidad de un conjunto)***
El Orden o Cardinalidad de un conjunto A se denota por $\mid A \mid$. Si A es un conjunto finito, el orden de A es simplemente el número de elementos de A.

Recordemos algunas propiedades:

a. Si $A = B$, entonces $\mid A \mid = \mid B \mid$.
b. Si $\mid A \mid \leq \mid B \mid$ y $\mid A \mid \geq \mid B \mid$, entonces $\mid A \mid = \mid B \mid$.
c. $\mid \emptyset \mid = 0$

Definición 2. ***(Grupo Simple)*** *Se llama grupo simple al grupo que solo tiene como subgrupos normales al grupo trivial y a sí mismo.*

Definición 3. ***(Serie de Composición)***
Sea G un grupo finito. Se llama serie de composición a una cadena de subgrupos

$$\{e\} = H_0 \leq H_1 \leq H_2 \leq ... \leq H_{k-1} \leq H_k = G$$

tal que $H_i \lhd H_{i+1}$, y H_{i+1}/H_i es un grupo simple para todo $i = 0, 1, 2, ..., k-1$.
Los grupos cocientes reciben el nombre de factores de composición.

Definición 4. ***(Grupo Soluble)***
Un grupo G es soluble; si existe en él una serie de composición

$$\{e\} = H_0 \leq H_1 \leq H_2 \leq ... \leq H_{k-1} \leq H_k = G$$

en la cual los factores de composición H_{i+1}/H_i, $i = 0, 1, 2, ..., k-1$, son abelianos.

Definición 5. ***(Grupo Simétrico)***
Se llama grupo simétrico, S_n, al grupo de permutaciones del conjunto $\{1, 2, 3, ..., n\}$.

Definición 6. ***(k - Ciclo)***
Una permutación $\sigma \in S_n$ se llama k - Ciclo, si existen elementos $i_1, ..., i_k \in \{1, 2, 3, ..., n\}$ con

$$i_1 \mapsto i_2 \mapsto ... \mapsto i_k \mapsto i_1 \quad y \quad \sigma(i) = i \quad para\ cualquier \quad i.$$

Definición 7. ***(Transposición)***
Un 2 - Ciclo se llama transposición; Este mapeo intercambia dos elementos y deja los otros fijos.

Teorema 1. *Ninguna permutación en S_n puede ser expresada como un producto de un número par de transposiciones, ni como un producto de un número impar de transposiciones.*

Definición 8. ***(Permutación Par e Impar)*** *Una permutación es par si es expresada como el producto de un número par de transposiciones y es impar si se expresa como el producto de un número impar de transposiciones.*

Definición 9. ***(Grupo Alternado)***
Se llama grupo alternado, A_n, al subgrupo de todas las permutaciones pares de S_n.

Definición 10. ***(Grupo Diédrico)***
Se llama grupo Diédrico de grado n, $(n \geq 3)$, al subgrupo D_n de S_n, que son las simetrías de un polígono regular de n lados.

Observación: Se puede probar que:
1. $| S_n | = n!$.
2. $| A_n | = \frac{n!}{2}$.
3. $| D_n | = 2n$ y debido a esto también se simboliza como D_{2n}.

El grupo D_n contiene dos elementos significativos que lo generan: El giro $\frac{2\pi}{n}$ radianes respecto al centro del polígono regular, que es un elemento de orden n y lo representamos por r, y la simetría respecto al eje que une al centro con uno de sus vértices, que es de orden 2 y la representamos por s. En términos de estos generadores, los $2n$ elementos de D_n se expresan de manera única en la forma

$$D_{2n} = \{1, r, r^2, ..., r^{n-1}, s, sr, sr^2, ..., sr^{n-1}\}.$$

Manejando esta representación de sus elementos, la multiplicación del grupo se deduce de las siguientes relaciones fundamentales,

$$r^n = 1, \quad s^2 = 1, \quad rs = sr^{n-1}.$$

Definición 11. ***(Segmento inicial)***
Sea G un conjunto ordenado con elemento mínimo a_0. Un subconjunto ordenado $A = \{a_0, a_1, ..., a_{t-1}\}$ con $a_0 < a_1 < ... < a_{t-1}$ de G se llama segmento inicial de longitud t si para toda $i \in \{0, 1, 2, ..., t-2\}$ se tiene que el conjunto $B = \{x \in G : a_i < x < a_{i+1}\} = \emptyset$. El conjunto $A = \emptyset$ es el segmento inicial de longitud cero (0).

Definición 12. ***(Conjunto Suma)*** *Sea G un grupo y sean $A_1, A_2, ..., A_k$ subconjuntos no vacíos de G. El conjunto suma de $A_1, A_2, ..., A_k$, esta dado como sigue,*

$$A_1 * A_2 * \cdots * A_k = \{a_1 * a_2 * \cdots * a_k : a_i \in A_i \quad \text{para todo} \quad i = 1, 2, ..., k\}.$$

Note que, si para algún $i \in \{1, 2, ..., k\}$ se tiene $A_i = \emptyset$, se define $A_1 * A_2 * \cdots * A_k = \emptyset$. También hay que resaltar que en los resultados encontrados con respecto al conjunto suma lo importante es el cardinal y no la estructura del grupo.

El problema directo: Dado un grupo G y dos subconjuntos no vacíos A y B de G, la problemática general, de los problemas directos, es encontrar una cota inferior para $| A * B |$ en términos de $| A |$ y $| B |$.

Notación
Función μ_G: Sean G un grupo y r, s enteros no negativos tales que $r, s \leq | G |$. Entonces

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

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

Función κ_G: En un grupo G, se define $\mathcal{H}(G)$ como sigue

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

Con base a esto definimos

$$\kappa_G(r, s) = \min_{h \in \mathcal{H}(G)} \left\{ \left(\left[\frac{r}{h} \right] + \left[\frac{s}{h} \right] - 1 \right) h \right\}.$$

1.2. Propiedades básicas de la función μ_G

Lema 1. *Si G es un grupo y r, s son enteros tal que $0 \leq r, s \leq | G |$, entonces $\mu_G(r, s) = \mu_G(s, r)$.*

Prueba: Para un subconjunto A de G, sea $A^{-1} = \{a^{-1} : a \in A\}$. Sean A y B subconjuntos de G que realizan $\mu_G(r, s)$. Entonces

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

Por tanto $\mu_G(s, r) \leq \mu_G(r, s)$; análogamente se obtiene $\mu_G(r, s) \leq \mu_G(s, r)$. □

Lema 2. *Si G es un grupo y r, s son enteros tal que $1 \leq r, s \leq |\ G\ |$, entonces $\mu_G(r,s) \geq$ máx$\{r,s\}$.*

Prueba: Si A y B son subconjuntos de G que realizan $\mu_G(r,s)$, entonces para cada $a \in A$ y cada $b \in B$ se tiene $a * B \subseteq A * B$ y $A * b \subseteq A * B$. Por tanto

$$\mu_G(r,s) = |\ A * B\ | \geq \text{máx}\{|\ A * b\ |, |\ a * B\ |\} = \text{máx}\{r,s\}. \quad \square$$

Lema 3. *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.*

Prueba: Supóngase que $\mu_G(r,r) = r$ y sean A y B subconjuntos de G que realizan $\mu_G(r,r)$. Fijando un elemento $a \in A$ y un elemento $b \in B$ se tiene

$$|\ (a^{-1} * A) * (B * b^{-1})\ | = |\ a^{-1} * (A * B)\ * b^{-1}\ | = |\ (A * B) * b^{-1}\ | = |\ A * B\ | = \mu_G(r,r).$$

Luego G contiene los subconjuntos $A' = a^{-1} * A$ y $B' = B * b^{-1}$ que realizan $\mu_G(r,r)$ y tales que $1 \in A' \cap B'$, asi que $A', B' \subseteq A' * B'$ y dado que

$$|\ A'\ | = |\ B'\ | = r = \mu_G(r,r) = |\ A' * B'\ |$$

se sigue $A' = B' = A' * B'$, es decir $1 \in A' * A'$; por tanto A' es un subgrupo de G de orden r. Recíprocamente si G contiene un subgrupo H de orden r, entonces $\mu_G(r,r) \leq |\ H * H\ | = r$, así $\mu_G(r,r) \leq r$ y por Lema 2, puesto que máx$\{r,r\} = r$ se tiene que $\mu_G(r,r) \geq r$. Por tanto $\mu_G(r,r) = r$. $\square$

Ejemplo: Como el grupo alternante A_4 de orden 12 no contiene subgrupos de orden seis, a la luz del Lema 3 se tiene que $\mu_{A_4}(6,6) \neq 6$.

El problema directo de encontrar una fórmula explícita para la función μ_G es un tema de estudio en el que, últimamente se han obtenido resultados significativos. Recientemente, Eliahou y Kervaire, desarrollaron estudios encaminados a comprender dicha función en un grupo finito no abeliano G. En [8], ellos logran determinar $\mu_G(r,s)$ para algunos valores particulares de r y s, y en [7] obtienen una cota superior para μ_G cuando G es un grupo soluble.

1.3. El Problema de los Conjuntos Suma Pequeños

El primer resultado que se puede enmarcar en esta problemática de la Teoría Aditiva de Números es el Teorema de Cauchy-Davenport, probado por Cauchy en 1813 y redescubierto en forma independiente por Davenport en 1935.

Teorema 2. ***(Cauchy-Davenport)***
Sea p un número primo. Si A y B son dos subconjuntos no vacíos del grupo cíclico $\mathbb{Z}_p$, entonces

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

Entre las numerosas generalizaciones del Teorema de Cauchy-Davenport una de las más fuertes, es el Teorema de Kneser, que permite extender el Teorema de Cauchy-Davenport a grupos abelianos arbitrarios. Para lograr esta extensión, Kneser utilizó la siguiente definición:

Definición 13. ***(Estabilizador de un conjunto)***
Sea A un subconjunto no vacío de un grupo abeliano G. El Estabilizador de A es el conjunto

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

y se dice que A es un conjunto periódico si $\mathbb{S}(A) \neq \{0\}$.

Teorema 3. ***(Kneser)***
Sea G un grupo abeliano y sean A y B dos subconjuntos finitos no vacíos de G. Si $S = \mathbb{S}(A + B)$ y $| A + B | \leq | A | + | B |$, entonces

$$| A + B | = | A + S | + | B + S | - | S | .$$

El Teorema de Kneser (Ver demostración en [2], pag. 6), implica el Teorema de Cauchy-Davenport porque en el grupo cíclico $\mathbb{Z}_p$, con p primo, el único subconjunto periódico no vacío de G es el mismo G.

El problema de los conjuntos suma pequeños, es minimizar el cardinal $| A * B |$, sujeto a las condiciones $A, B \subseteq G$, $| A | = r$ y $| B | = s$; es decir, hallar el valor de $\mu_G(r, s)$.

Ejemplo: En el grupo cíclico $G = \mathbb{Z}_p$, con p primo, se tiene el siguiente teorema.

Teorema 4. *Si p es un número primo y $G = \mathbb{Z}_p$, entonces para todo par de enteros r y s tal que $1 \leq r, s \leq p$ se tiene*

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

Prueba: Para probar la desigualdad $\mu_G(r, s) \leq \text{mín}\{p, r + s - 1\}$ considérese los subconjuntos $A = \{0, 1, ..., r - 1\}$ y $B = \{0, 1, ..., s - 1\}$ de G, así que

$$\mu_G(r, s) \leq | A + B | = | \{0, 1, ..., r + s - 2\} | = r + s - 1.$$

Si $r + s - 1 \geq p$, entonces $A + B = G$, luego

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

Si $r + s - 1 < p$, entonces

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

Por lo tanto en cualquier caso, se tiene $\mu_G(r, s) \leq \text{mín}\{p, r + s - 1\}$. La otra desigualdad es consecuencia directa del Teorema de Cauchy-Davenport. □

Capítulo 2

La Función μ_G en grupos abelianos

En la primera sección se comentó que Eliahou, Kervaire y Plagne obtuvieron conclusiones y probaron teoremas que dan una fórmula exacta para $\mu_G(r,s)$ cuando G es un grupo abeliano arbitrario, y en síntesis esto lo veremos en este capitulo.

2.1. Fórmula para μ_G en grupos abelianos

En un grupo abeliano G se conoce una fórmula exacta para la función μ_G. Antes de presentar la demostración de dicha fórmula se enuncian los resultados más importantes que la anteceden.

En el grupo cíclico $\mathbb{Z}_p$, con p primo, el Teorema 2 permite escribir la fórmula

$$\mu_{\mathbb{Z}_p}(r,s) = \min\{p, r+s-1\}.$$

En 1996 B. Bollobás y L. Leader (ver [1]) estudiaron la función μ_G donde G es un p-grupo abeliano finito arbitrario, ellos probaron que $\mu_G(r,s)$ depende únicamente del orden de G y no de la estructura particular del p-grupo.
En 1998, Eliahou y Kervaire (ver [4]) mostraron que en el grupo cíclico $G = (\mathbb{Z}_p)^n$, con p primo se tiene

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

Plagne (Ver [3]) demostró que si n es un entero positivo y $G = \mathbb{Z}_n$, entonces se cumple la fórmula

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

donde $[\xi]$ denota el menor entero x tal que $\xi \leq x$.

Posteriormente Eliahou, Kervaire y Plagne (ver [5]) extendieron el resultado anterior

para todo grupo abeliano finito. Para una mejor comprensión de la demostración de este resultado es conveniente tener en cuenta que si G es un grupo abeliano finito, entonces existen enteros $n_1, n_2, ..., n_k > 1$ tales que $G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times ... \times \mathbb{Z}_{n_k}$. Por otro lado, el grupo cíclico $\mathbb{Z}_{n_i} = \{0, 1, ..., n_i - 1\}$ 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 $x = (x_1, x_2, ..., x_k)$ y $w = (w_1, w_2, ..., w_k)$ se dice que $x < w$, si y sólo si, existe $i \in \{1, 2, ..., k\}$ tal que se cumplen las dos condiciones siguientes:

1. $x_j = w_j$ siempre que $j < i$.
2. $x_i < w_i$.

Lema 4. ***(Desigualdad de Eliahou y Kervaire)***
Sea G un grupo abeliano finito y sea $G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times ... \times \mathbb{Z}_{n_k}$ 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 (ver definición 11) no vacíos de G, entonces $| A + B | \leq | A | + | B | - 1$.

Prueba: El lema se probará por inducción sobre el número k de factores en la descomposición de G como producto directo de grupos cíclicos.
Si $k = 1$, entonces $G \cong \mathbb{Z}_{n_1} = \{0, 1, ..., n_1 - 1\}$. Sean A y B dos segmentos iniciales no vacíos de G, de longitudes r y s respectivamente, es decir

$$A = \{0, 1, ..., r - 1\} \quad y \quad B = \{0, 1, ..., s - 1\}.$$

Si $r + s - 2 < n_1 - 1$ se tiene

$$| A + B | = | \{0, 1, ..., r + s - 2\} | = r + s - 1.$$

Si $r + s - 2 \geq n_1 - 1$ se tiene

$$| A + B | = | \{0, 1, ..., n_1 - 1\} | = n_1 \leq r + s - 1.$$

Por lo tanto

$$| A + B | \leq r + s - 1 = | A | + | B | - 1.$$

Ahora supóngase que $k \geq 2$ y que el resultado del Lema 4 se cumple para grupos abelianos que se pueden descomponer como el producto directo de $k-1$ factores cíclicos. Considérese un grupo abeliano G que se pueda descomponer como el producto directo de k factores cíclicos, esto es $G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times ... \times \mathbb{Z}_{n_k}$, y sean $A, B \subseteq G$ dos segmentos iniciales en G de longitudes r y s respectivamente. Se puede asumir que $G \cong \mathbb{Z}_{n_1} \times H$, donde $H = \mathbb{Z}_{n_2} \times ... \times \mathbb{Z}_{n_k}$ con $k - 1$ factores cíclicos. Por la hipótesis inductiva H satisface el resultado del Lema 4. Sea $h = | H |$, por el algoritmo de la división se puede garantizar que existen enteros r_1, r_2, s_1 y s_2 tales que

$$r = r_1 h + r_2, \quad s = s_1 h + s_2 \quad y \quad 0 \leq r_2, s_2 < h.$$

Ahora sea A_1 el segmento inicial de longitud r_1 en $\mathbb{Z}_{n_1}$, A_2 el segmento inicial de longitud r_2 en H, B_1 el segmento inicial de longitud s_1 en $\mathbb{Z}_{n_1}$ y B_2 el segmento inicial de longitud s_2 en H, entonces

$$A = (A_1 \times H) \cup (\{r_1\} \times A_2) \quad \text{y} \quad B = (B_1 \times H) \cup (\{s_1\} \times B_2).$$

Dado que $r, s \geq 1$, no es posible tener $r_1 = r_2 = 0$ o $s_1 = s_2 = 0$. A continuación se consideran los casos restantes.

Caso 1: Supóngase $r_1 = s_1 = 0$. En este caso $A_1 \times H = \emptyset$ y así $A = \{r_1\} \times A_2$, análogamente $B = \{s_1\} \times B_2$, luego $\mid A \mid = \mid A_2 \mid$ y $\mid B \mid = \mid B_2 \mid$, además

$$\mid A + B \mid = \mid (\{r_1\} \times A_2) + (\{s_1\} \times B_2) \mid = \mid (\{r_1 + s_1\} \times (A_2 + B_2) \mid = \mid A_2 + B_2 \mid .$$

Aplicando la hipótesis inductiva al grupo abeliano H se tiene

$$\mid A + B \mid \leq \mid A_2 \mid + \mid B_2 \mid -1 = \mid A \mid + \mid B \mid -1.$$

Caso 2: Si $r_1 = s_2 = 0$, entonces $A = \{r_1\} \times A_2$ y $B = B_1 \times H$. Dado que $A_2 \subseteq H$ se sigue $A + B \subseteq (\{r_1\} + B_1) \times H$ y así

$$\mid A + B \mid \leq \mid \{r_1\} + B_1 \mid h = \mid B_1 \mid h = \mid B \mid,$$

pero $A \neq \emptyset$, esto es, $\mid A \mid -1 \geq 0$ y junto a la desigualdad anterior se obtiene

$$\mid A + B \mid \leq \mid A \mid + \mid B \mid -1.$$

Caso 3: Para el caso $r_1 = 0$ y $s_1, s_2 \neq 0$ se tiene $A = \{r_1\} \times A_2$ y dado que $A_2 \subseteq H$ se sigue

$$A + B \subseteq [(\{r_1\} + B_1) \times H] \cup [\{r_1 + s_1\} \times (A_2 + B_2)].$$

Pero $s_1$no pertenence a B_1, lo que implica $(r_1 + s_1)$ no esta en $\{r_1\} + B_1$, así que los conjuntos $(\{r_1\} + B_1) \times H$ y $\{r_1 + s_1\} \times (A_2 + B_2)$ son disjuntos, entonces

$$\mid A + B \mid \leq \mid (\{r_1\} + B_1) \times H \mid + \mid \{r_1 + s_1\} \times (A_2 + B_2) \mid = \mid B_1 \times H \mid + \mid A_2 + B_2 \mid .$$

Aplicando la hipótesis inductiva al grupo H se tiene $\mid A_2 + B_2 \mid \leq \mid A_2 \mid + \mid B_2 \mid -1$. Por lo tanto

$$\mid A + B \mid \leq \mid B_1 \mid h + \mid A_2 \mid + \mid B_2 \mid -1. \quad (*)$$

Por otro lado

$$\mid B \mid = \mid B_1 \times H \mid + \mid \{s_1\} \times B_2 \mid = \mid B_1 \mid h + \mid B_2 \mid .$$

Al sustituir la igualdad anterior en la ecuación (*) se obtiene

$$\mid A + B \mid \leq \mid A_2 \mid + \mid B \mid -1 = \mid A \mid + \mid B \mid -1.$$

Caso 4: Si $r_2 = s_2 = 0$, entonces $A = A_1 \times H$ y $B = B_1 \times H$ y se tiene

$$A + B = (A_1 + B_1) \times H,$$

es decir

$$| A + B | = | A_1 + B_1 | h.$$

Dado que A_1 y B_1 son segmentos iniciales de $\mathbb{Z}_{n_1}$ entonces $| A_1 + B_1 | \leq | A_1 | + | B_1 | - 1$; esta desigualdad junto a la ecuación anterior implican

$$| A + B | = | A_1 + B_1 | h \leq | A_1 | h + | B_1 | h - h.$$

Pero $| A | = | A_1 | h$ y $| B | = | B_1 | h$, por lo tanto

$$| A + B | \leq | A | + | B | - h \leq | A | + | B | - 1.$$

Caso 5: Si $r_2 = 0$ y $s_1, s_2 \neq 0$ entonces $A = A_1 \times H$ y $B = (B_1 \times H) \cup (\{s_1\} \times B_2)$. Luego

$$A + B \subseteq [(A_1 + B_1) \times H_2] \cup [(A_1 + \{s_1\}) \times H_2]. \quad (**)$$

Pero $A_1 + B_1 = \{0, 1, 2, ..., r_1 + s_1 - 2\}$ y $A_1 + \{s_1\} = \{s_1, s_1 + 1, ..., r_1 + s_1 - 1\}$, así que

$$(A_1 + B_1) \cap (A_1 + \{s_1\}) = \begin{cases} \emptyset, & si \quad r_1 = 1 \\ \{s_1, s_1 + 1, ..., r_1 + s_1 - 2\}, & si \quad r_1 \geq 2 \end{cases}$$

Supóngase $r_1 = 1$, entonces el único elemento de A_1 es la identidad de G, de tal manera que $A_1 + B_1 = B_1$ y $A_1 + \{s_1\} = \{s_1\}$, esto junto a la expresión (**) implican

$$| A + B | \leq | B_1 \times H | + | \{s_1\} \times H | = | B_1 | h + h.$$

Dado que $| B_2 | - 1 \geq 0$, $| A | = h$ y $| B | = | B_1 | h + | B_2 |$ se tiene

$$\begin{aligned} | A + B | &\leq | B_1 | h + h + | B_2 | - 1 \\ &= (| B_1 | h + | B_2 |) + h - 1 \\ &= | A | + | B | - 1. \end{aligned}$$

Ahora supóngase $r_1 \geq 2$. Por la expresión (**) se tiene

$$\begin{aligned} | A + B | &\leq | A_1 + B_1 | h + | A_1 + \{s_1\} | h - | \{s_1, s_1 + 1, ..., r_1 + s_1 - 2\} | h \\ &= | A_1 + B_1 | h + | A_1 | h - (r_1 - 1)h \\ &= | A_1 + B_1 | h + r_1 h - r_1 h + h \\ &= | A_1 + B_1 | h + h. \end{aligned}$$

Pero A_1 y B_1 son segmentos iniciales de $\mathbb{Z}_{n_1}$, entonces

$$\begin{aligned} \mid A+B \mid &\leq (\mid A_1 \mid + \mid B_1 \mid -1)h + h \\ &= \mid A_1 \mid h + \mid B_1 \mid)h \\ &\leq \mid A_1 \mid h + \mid B_1 \mid)h + \mid B_2 \mid -1 \\ &= \mid A \mid + \mid B \mid -1. \end{aligned}$$

Caso 6: Si $r_1, r_2, s_1, s_2 \neq 0$, se tiene

$$A+B = [(A_1 \times H) \cup (\{r_1\} \times A_2)] + [(B_1 \times H) \cup (\{s_1\} \times B_2)].$$

Entonces

$$A+B \subseteq \{[(A_1+B_1) \cup (A_1+\{s_1\}) \cup (\{r_1\}+B_1)] \times H\} \cup [\{r_1+s_1\} \times (A_2+B_2)].$$

Pero $A_1 + B_1 = \{0, 1, 2, ..., r_1+s_1-2\}$, $A_1 + \{s_1\} = \{s_1, s_1+1, ..., r_1+s_1-1\}$ y $\{r_1\} + B_1 = \{r_1, r_1+1, ..., r_1+s_1-1\}$, luego

$$(A_1+B_1) \cup (A_1+\{s_1\}) \cup (\{r_1\}+B_1) = \{0, 1, 2, ..., r_1+s_1-1\}$$

Llamando $P_1 = \{0, 1, 2, ..., r_1+s_1-1\} \times H$ y $P_2 = (r_1+s_1) \times (A_2+B_2)$ se tiene $A+B \subseteq P_1 \cup P_2$, además $P_1 \cap P_2 = \emptyset$, entonces

$$\mid A+B \mid \leq \mid P_1 \mid + \mid P_2 \mid = (r_1+s_1)h + \mid A_2+B_2 \mid .$$

Dado que A_2 y B_2 son segmentos iniciales de H, se tiene $\mid A_2+B_2 \mid \leq \mid A_2 \mid + \mid B_2 \mid -1$ y por lo tanto

$$\begin{aligned} \mid A+B \mid &\leq \mid A_1 \mid h + \mid B_1 \mid h + \mid A_2 \mid + \mid B_2 \mid -1 \\ &= (\mid A_1 \mid h + \mid A_2 \mid) + (\mid B_1 \mid h + \mid B_2 \mid) - 1 \\ &= \mid A \mid + \mid B \mid -1. \quad \square \end{aligned}$$

Los casos restantes son similares a algunos de los seis casos expuestos, lo que finaliza la prueba.

Lema 5. ***(Desigualdad de Plagne)***
Sea G un grupo abeliano finito de orden n. Si r y s son enteros positivos tal que $r, s \leq n$, entonces $\mu_G(r,s) \geq \min_{d \mid n} \left\{ \left(\left[\frac{r}{d} \right] + \left[\frac{s}{d} \right] - 1 \right) d \right\}$.

Prueba: Sean A y B dos subconjuntos de G que realizan $\mu_G(r,s)$. El teorema de Kneser (teorema 2) garantiza que existe un subgrupo H de G tal que

$$\mid A+B \mid = \mid A+H \mid + \mid B+H \mid - \mid H \mid .$$

Con $h = \mid H \mid$ se tiene

$$\mid A+B \mid = \left(\frac{\mid A+H \mid}{h} + \frac{\mid B+H \mid}{h} - 1 \right) h.$$

Pero $\frac{|A+H|}{h} \geq \frac{|A|}{h} = \frac{r}{h}$ y $\frac{|B+H|}{h} \geq \frac{|B|}{h} = \frac{s}{h}$. Además, $A+H = \bigcup_{a \in A} (a+H)$, es decir $A+H$ es la unión de H-clases laterales dijuntas y como todas las H-clases laterales dijuntas tienen el mismo número de elementos que el subgrupo H se sigue que $\frac{|A+H|}{h}$ y $\frac{|B+H|}{h}$ son números enteros, luego $\frac{|A+H|}{h} \geq \left[\frac{r}{h}\right]$ y $\frac{|B+H|}{h} \geq \left[\frac{s}{h}\right]$. Por lo tanto

$$\mid A+B \mid \geq \left(\left[\frac{r}{h}\right] + \left[\frac{s}{h}\right] - 1 \right) h.$$

Ahora, h divide a n ya que h es el orden de un subgrupo de G y $n = \mid G \mid$, además A y B realizan $\mu_G(r,s)$ entonces

$$\mu_G(r,s) = \mid A+B \mid \geq \left(\left[\frac{r}{h}\right] + \left[\frac{s}{h}\right] - 1 \right) h \geq \min_{d|n} \left\{ \left(\left[\frac{r}{d}\right] + \left[\frac{s}{d}\right] - 1 \right) d \right\}. \quad \square$$

Teorema 5. ***(Eliahou, Kervaire y Plagne)***
Sea G un grupo abeliano finito de orden n. Si r, s son enteros positivos tal que $r, s \leq n$, entonces

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

Prueba: Para probar la desigualdad $\mu_G(r,s) \leq \min_{d|n} \left\{ \left(\left[\frac{r}{d}\right] + \left[\frac{s}{d}\right] - 1 \right) d \right\}$, sea h un entero positivo que divida a $n = \mid G \mid$ y tal que $\mu_G(r,s) = \left(\left[\frac{r}{h}\right] + \left[\frac{s}{h}\right] - 1 \right) h$. Como G es un grupo abeliano existe un subgrupo H de G tal que $\mid H \mid = h$. Sea $G_0 = G/H$ y póngase $n_0 = \frac{n}{h} = \mid G_0 \mid$, entonces $1 \leq \left[\frac{r}{h}\right], \left[\frac{s}{h}\right] \leq n_0$. Sean A_0 y B_0 subconjuntos de G_0 que realizan $\mu_{G_0}\left(\left[\frac{r}{h}\right], \left[\frac{s}{h}\right]\right)$ por el lema 4 se tiene

$$\mu_{G_0}\left(\left[\frac{r}{h}\right], \left[\frac{s}{h}\right]\right) = \mid A_0 + B_0 \mid \leq \mid A_0 \mid + \mid B_0 \mid - 1 = \left[\frac{r}{h}\right] + \left[\frac{s}{h}\right] - 1.$$

Sean $\Pi : G \to G_0$ la proyección natural, $A' = \Pi^{-1}(A_0)$ y $B' = \Pi^{-1}(B_0)$. Como todas las H-clases laterales tienen h elementos, entonces

$$\mid A' \mid = \mid A_0 \mid h = \left[\frac{r}{h}\right] h \geq r$$

$$\mid B' \mid = \mid B_0 \mid h = \left[\frac{s}{h}\right] h \geq s$$

Ahora, sean $A \subseteq A'$ y $B \subseteq B'$ tales que $\mid A \mid = r$ y $\mid B \mid = s$, se tiene, $\mid A+B \mid \leq \mid A'+B' \mid$. Por otro lado $x \in (A'+B')$, si y sólo si $\Pi(x) \in (A_0+B_0)$, luego

$$\mu_G(r,s) \leq \mid A'+B' \mid = \mid A_0+B_0 \mid h \leq \left(\left[\frac{r}{h}\right] + \left[\frac{s}{h}\right] - 1 \right) h.$$

Dado que h es un divisor positivo de n se concluye

$$\mu_G(r,s) \leq \min_{d|n} \left\{ \left(\left[\frac{r}{d} \right] + \left[\frac{s}{d} \right] - 1 \right) d \right\}. \quad \square$$

La otra desigualdad es una consecuencia del lema 5 (Desigualdad de Plagne) y al combinar ambas desigualdades se obtiene el siguiente resultado.

Teorema 6. *Si G es un grupo abeliano finito, entonces*

$$\mu_G(r,s) = \min_{h \in \mathcal{H}(G)} \left\{ \left(\left[\frac{r}{h} \right] + \left[\frac{s}{h} \right] - 1 \right) h \right\}.$$

2.2. Teoremas Principales

El estudio del artículo *"Sumsets in dihedral groups"* escrito por Eliahou y Kervaire se sintetiza en los siguientes resultados que serán más detallados en el siguiente capitulo.

Teorema 7. *Para cada entero positivo n se tiene la desigualdad*

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

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

Junto a este teorema en el siguiente capitulo probamos tambien la desigualdad recíproca para n una potencia prima.

Teorema 8. *Sea D_q el grupo diédrico de índice $q = p^v$, una potencia prima. Sea r, s enteros tal que $1 \leq r, s \leq 2q$. Entonces*

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

Luego, combinando los dos resultados obtenemos el siguiente Corolario.

Corolario 1. *Cuando n es una potencia prima, entonces*

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

A continuación en el capitulo final, encontramos una explicación un poco más clara de estos resultados y se hallaran conclusiones del problema principal.

Capítulo 3

La Función μ_G en grupos no abelianos

En este capitulo se presenta en síntesis los resultados que Eliahou y Kervaire han obtenido en el estudio de la funciíon μ_G para el caso en que G es un grupo finito no abeliano.

Según el Teorema 5, si G es un grupo abeliano y r, s son dos enteros positivos tales que $r, s \leq \mid G \mid$, entonces $\mu_G(r,s) = \kappa_G(r,s)$, pero en grupos no abelianos esta igualdad, en general, no se tiene. Los trabajos de Eliahou y Kervaire en grupos no abelianos han permitido establecer que bajo ciertas condiciones es posible tener esta igualdad.

3.1. Desigualdad principal: $\mu_{D_n}(r,s) \leq \kappa_{D_n}(r,s)$

Definición 14. ***(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 $r, s \leq \mid G \mid$ existen subconjuntos $A, B \subseteq G$ tales que $\mid A \mid = r$, $\mid B \mid = s$ y $\mid A * B \mid \leq r + s - 1$.

A la luz del Lema 4 (Desigualdad de Eliahou y Kervaire), los grupos abelianos gozan de esta propiedad.

A continuación mostramos unos resultados que serán muy útiles, las demostraciones de tales resultados se encuentran en el artículo [7] de Eliahou y Kervaire como Teorema 2.2 y Corolario 2.3.

Teorema 9. *Si G es un grupo finito soluble, entonces G tiene la propiedad del conjunto suma pequeño.*

Corolario 2. *Si G es un grupo finito soluble, entonces para todo par de enteros r y s, tal que $1 \leq r, s \leq \mid G \mid$ se tiene $\mu_G(r,s) \leq r + s - 1$.*

El teorema siguiente es más fuerte que el Corolario 2, y fue probado por Eliahou y Kervaire en [7] como Proposición 3.1.

Teorema 10. *Sea G un grupo finito y sean r, s enteros tal que $1 \leq r, s \leq \mid G \mid$. Si G tiene un subgrupo H de orden $d \geq r$ que satisface la propiedad del conjunto suma pequeño, entonces $\mu_G(r, s) \leq r + s - 1$.*

Lema 6. *Sea G un grupo finito soluble y sean r, s enteros tal que $1 \leq r, s \leq \mid G \mid$. Sea k el orden de un subgrupo normal K de G. Entonces*

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

Prueba: Sean $G_0 = G/K$, $r_0 = \left[\frac{r}{k}\right]$ y $s_0 = \left[\frac{s}{k}\right]$. Así $1 \leq r_0, s_0 \leq \mid G_0 \mid$, y dado que G es soluble se tiene que G_0 es soluble. El Corolario 2 implica que

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

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 considérese los siguientes subconjuntos de G:

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

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

$$\mid A' * B' \mid = (r_0 + s_0 - 1)k = \left(\left[\frac{r}{k}\right] + \left[\frac{s}{k}\right] - 1\right) k.$$

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

$$\mu_G(r, s) \leq \mid A * B \mid \leq \mid A' * B' \mid = \left(\left[\frac{r}{k}\right] + \left[\frac{s}{k}\right] - 1\right) k. \quad \square$$

Una consecuencia inmediata del lema 6 es el siguiente corolario:

Corolario 3. *Sea G un grupo finito soluble y sean r, s enteros positivos tal que $r, s \leq \mid G \mid$. Entonces*

$$\mu_G(r, s) \leq \kappa_G(r, s).$$

Ahora observemos el siguiente resultado para los grupos diédricos; entonces enunciemos las siguientes propiedades que caracterizan este grupo.

Proposición 1. *Sea $n > 2$ un número entero y sea*

$$D_n =< \alpha, \beta : \alpha^n = \beta^2 = 1, \beta\alpha\beta^{-1} = \alpha^{-1} >,$$

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

1. Un subgrupo propio H de D_n es normal en D_n si y sólo si cumple uno de los siguientes enunciados:

a) *H es un subgrupo del grupo $< \alpha >$ generado por la rotación α.*
b) *H es el subgrupo $< \alpha^2, \beta >$ generado por α^2 y β o H es el subgrupo $< \alpha^2, \alpha\beta >$ generado por α^2 y $\alpha\beta$. En este caso H es de índice 2 y n es par.*

2. Los grupos cocientes de D_n son diédricos y los subgrupos de D_n son diédricos o cíclicos.

3. D_n es soluble.

Teorema 11. *Sea $n > 2$ un número entero y sean r, s enteros tal que $1 \leq r, s \leq 2n$. Sea h el orden de un subgrupo H de D_n. Entonces, existen subconjuntos $A, B \subset D_n$ con cardinales $\mid A \mid = r$, $\mid B \mid = s$ tal que*

$$\mid A * B \mid \leq \left(\left[\frac{r}{h} \right] + \left[\frac{s}{h} \right] - 1 \right) h.$$

Prueba: Supóngase que H es un subgrupo normal de D_n. Por el punto 3 de la propiedad, D_n es soluble y por el Lema 6 se obtiene el resultado deseado. Ahora supóngase que H no es un subgrupo normal de D_n, entonces a la luz de la parte 2 de la propiedad H debe ser un subgrupo diédrico de D_n y en tal caso existen $i \in \{0, 1, 2, ..., n-1\}$ y un divisor propio m de n tales que

$$H =< \alpha^m, \alpha^i\beta >= D_{\frac{n}{m}}.$$

Sea $E =< \alpha^m >$ el subgrupo cíclico de H generado por α^m y sea $e =\mid E \mid$, de tal manera que $h =\mid H \mid = 2e$. Con el fin de facilitar la demostración se denota el entero $f_d(r, s)$ como sigue,

$$f_d(r, s) = \left(\left[\frac{r}{d} \right] + \left[\frac{s}{d} \right] - 1 \right) d.$$

Para demostrar el teorema se construirán subconjuntos A y B de D_n tales que $\mid A \mid = r$, $\mid B \mid = s$ y $\mid A * B \mid \leq f_{2e}(r, s)$. Primero supóngase que $f_e(r, s) \leq f_{2e}(r, s)$. Dado que E es un subgrupo normal de D_n, el Lema 6 permite escribir la siguiente desigualdad:

$$\mu_{D_n} \leq \left(\left[\frac{r}{e} \right] + \left[\frac{s}{e} \right] - 1 \right) e = f_e(r, s) \leq f_{2e}(r, s).$$

Así al escoger subconjuntos A y B de D_n que realicen μ_{D_n} se obtiene el resultado deseado. Ahora, supóngase $f_{2e}(r,s) < f_e(r,s)$. Llamando $u = \left[\frac{r}{2e}\right]$ y $v = \left[\frac{s}{2e}\right]$, se puede garantizar que existen enteros $\delta, \lambda \in \{0,1\}$ y $0 \leq r_1, s_1 < e$ tales que

$$r = 2eu - (\delta e + r_1) = e\left[\frac{r}{e}\right] - r_1 \quad \text{y} \quad s = 2ev - (\lambda e + s_1) = e\left[\frac{s}{e}\right] - s_1. \qquad (1)$$

Luego $u = \frac{1}{2}\left(\left[\frac{r}{e}\right] + \delta\right)$ y $v = \frac{1}{2}\left(\left[\frac{s}{e}\right] + \lambda\right)$, entonces

$$f_{2e}(r,s) = 2e(u+v-1) = 2e\left[\frac{1}{2}\left(\left[\frac{r}{e}\right] + \left[\frac{s}{e}\right] - 1\right) + \frac{1}{2}(\delta + \lambda - 1)\right].$$

Así que

$$f_{2e}(r,s) = f_e(r,s) + (\delta + \lambda - 1)e.$$

Dado que $f_{2e}(r,s) < f_e(r,s)$ y $\delta, \lambda \in \{0,1\}$ se tiene $\delta = \lambda = 0$. Sustituyendo en la ecuación (1) se puede escribir

$$r = (2u-1)e + (e - r_1) \quad \text{y} \quad s = (2v-1)e + (e - s_1),$$

donde $1 \leq e - r_1, e - s_1 < e$, además $1 \leq u, v \leq m$. A fin de determinar los subconjuntos A y B de cardinales r y s, respectivamente, tales que $| A * B | \leq f_{2e}(r,s)$, se definen los siguientes conjuntos:

$$\begin{aligned} X_0 &= \emptyset, \\ X_t &= \{1, \alpha, ..., \alpha^{t-1}\} \text{ para toda } t \in \{1,2,...,m\}, \\ E_j &= \{1, \alpha^m, ..., \alpha^{(j-1)m}\} \text{ para toda } j \in \{1,2,...,e\}, \\ Y^{-1} &= \{y^{-1} : y \in Y\} \text{ para todo } Y \subseteq < \alpha >. \end{aligned}$$

Ahora, sea $l = e - r_1$, $q = e - s_1$ y considérense los siguientes subconjuntos de D_n:

$$\begin{aligned} A &= (EX_u) \cup (EX_{u-1} \cup E_l \alpha^{u-1})\alpha^{v-1}\beta, \\ B &= (EX_v) \cup (EX_{v-1} \cup E_q \alpha^{v-1})\beta. \end{aligned}$$

Se puede probar que

$$EX_{u-1} \cap E_l \alpha^{u-1} = EX_{v-1} \cap E_q \alpha^{v-1} = \emptyset,$$

así que

$$\begin{aligned} | A | &= | EX_u | + | EX_{u-1} | + | E_l \alpha^{u-1} | \\ &= | E || X_u | + | E || X_{u-1} | + | E_l | \\ &= eu + e(u-1) + l \\ &= 2eu - e + e - r_1 \\ &= r. \end{aligned}$$

De forma similar se tiene que $\mid B \mid = s$. Ahora se probará la desigualdad $\mid A * B \mid \leq f_{2e}(r,s)$.
Sean

$$\begin{aligned} \mathcal{C}_1 &= (EX_u)(EX_v), \\ \mathcal{C}_2 &= (EX_u)(EX_{v-1} \cup E_q\alpha^{v-1})\beta, \\ \mathcal{C}_3 &= (EX_{u-1} \cup E_l\alpha^{u-1})\alpha^{v-1}\beta(EX_v), \\ \mathcal{C}_4 &= [(EX_{u-1} \cup E_l\alpha^{u-1})\alpha^{v-1}\beta][(EX_{v-1} \cup E_q\alpha^{v-1})\beta], \end{aligned}$$

entonces

$$A * B = \mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{C}_3 \cup \mathcal{C}_4.$$

Dado que $EE_q = E$, $\beta(EX_v) = (EX_v^{-1})\beta$ y $\alpha^{v-1}X_v^{-1} = X_v$, al desarrollar los productos, se tiene

$$\begin{aligned} \mathcal{C}_1 &= EX_uX_v, \\ \mathcal{C}_2 &= (EX_uX_{v-1} \cup EX_u\alpha^{v-1})\beta, \\ \mathcal{C}_3 &= (EX_{u-1}X_v \cup EX_v\alpha^{u-1})\alpha^{v-1}\beta, \\ \mathcal{C}_4 &= (EX_{u-1}X_{v-1}) \cup (EX_{v-1}\alpha^u) \cup (E_lE_q^{-1}\alpha^{u-1}). \end{aligned}$$

Además se tiene que $\mathcal{C}_4 \subseteq \mathcal{C}_1$ y que $\mathcal{C}_2 \cup \mathcal{C}_3 = EX_uX_v\beta$. Luego

$$A * B = (EX_uX_v) \cup (EX_uX_v\beta),$$

de donde

$$\mid A * B \mid = \mid EX_uX_v \mid + \mid EX_uX_v\beta \mid = 2 \mid EX_uX_v \mid = 2 \mid EX_{u+v-1} \mid .$$

Pero

$$EX_{u+v-1} = \begin{cases} E\{1, \alpha, ..., \alpha^{u+v-1}\}, & si \quad u+v-1 \leq m; \\ E, & si \quad u+v-1 > m. \end{cases}$$

Luego $EX_{u+v-1} = EX_{\text{mín}\{u+v-1\}}$ y por lo tanto

$$\mid A * B \mid = 2 \mid E \mid (\text{mín}\{u+v-1, m\}) \leq 2e(u+v-1) = f_{2e}(r,s). \quad \square$$

Nota: En particular, el Teorema 10, muestra que para todo entero $n > 2$ y para todo par de enteros positivos $r, s \leq 2n$ se tiene la desigualdad $\mu_{D_n}(r,s) \leq \kappa_{D_n}(r,s)$, lo que ratifica el Teorema 7 y que se deseaba probar en esta sesión.

3.2. Desigualdad recíproca: $\mu_{D_n}(r,s) \geq \kappa_{D_n}(r,s)$

A manera de conjetura, la desigualdad $\mu_{D_n}(r,s) \geq \kappa_{D_n}(r,s)$ se da para todo entero positivo n. Sin embargo, sólo se tiene una demostración completa en el caso en que n es una potencia prima, es decir; $n = p^v$ con p primo. Para comenzar probemos unas afirmaciones preliminares; Usando la representación $D_n =< \alpha, \beta : \alpha^n = \beta^2 = 1, \beta\alpha\beta^{-1} = \alpha^{-1} >$, sea C el subgrupo cíclico $C =< \alpha > \subset D_n$ de orden n.

Notación
Sean r_0, r_1, s_0, s_1 enteros positivos tales que $r_0, r_1, s_0, s_1 \leq n$; entonces $M_C(r_0, r_1, s_0, s_1)$ se llama función descomposición, y esta dada por:

$$M_C(r_0, r_1, s_0, s_1) = \text{máx}\{\kappa_C(r_0, s_0), \kappa_C(r_1, s_1)\} + \text{máx}\{\kappa_C(r_0, s_1), \kappa_C(r_1, s_0)\}.$$

Lema 7. *Dados los enteros positivos r, s, n. Si para cada elección de enteros positivos $r_0, r_1, s_0, s_1 \leq n$ se satisface $r_0 + r_1 = r$ y $s_0 + s_1 = s$ se tiene la desigualdad*

$$M_C(r_0, r_1, s_0, s_1) \geq \kappa_{D_n}(r, s),$$

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

Prueba: Sean $A, B \subset D_n$ tales que $\mid A \mid = r$ y $\mid B \mid = s$. Se quiere probar que $\mid A * B \mid \geq \kappa_{D_n}(r,s)$.
En efecto; Sea $A = A_0 \cup A_1 b$ y $B = B_0 \cup B_1 b$, donde A_0, A_1, B_0, B_1 son subconjuntos del grupo cíclico C; tales que $\mid A_0 \mid = r_0$, $\mid A_1 \mid = r_1$, $\mid B_0 \mid = s_0$ y $\mid B_1 \mid = s_1$.
Se tiene que

$$A * B = (A_0 \cup A_1 b) * (B_0 \cup B_1 b) = (A_0 * B_0 \cup A_1 * B_1^{-1}) \cup (A_0 * B_1 \cup A_1 * B_0^{-1})b.$$

Además,

$$\mid A * B \mid = \mid A_0 * B_0 \cup A_1 * B_1^{-1} \mid + \mid A_0 * B_1 \cup A_1 * B_0^{-1} \mid .$$

De donde se sigue que

$$\mid A * B \mid \geq \text{máx}\{\mid A_0 * B_0 \mid, \mid A_1 * B_1^{-1} \mid\} + \text{máx}\{\mid A_0 * B_1 \mid, \mid A_1 * B_0^{-1} \mid\}.$$

Por el Teorema 5 del capitulo 2 (Ver [5]), se tiene que $\mu_C = \kappa_C$ en el grupo abeliano C. De donde, si ninguno de los subconjuntos A_0, A_1, B_0, B_1 es vacío, se tiene que

$$\mid A * B \mid \geq \text{máx}\{\kappa_C(r_0, s_0), \kappa_C(r_1, s_1)\} + \text{máx}\{\kappa_C(r_0, s_1), \kappa_C(r_1, s_0)\} = M_C(r_0, r_1, s_0, s_1).$$

Luego, la desigualdad $M_C(r_0, r_1, s_0, s_1) \geq \kappa_{D_n}(r,s)$, implica que $\mid A * B \mid \geq \kappa_{D_n}(r,s)$. Ahora resta probar, que si uno de los subconjuntos $A_0, A_1, B_0, B_1 \subset C$ es vacío, también se tiene $\mid A * B \mid \geq \kappa_{D_n}(r,s)$, como se desea.
Considere el grupo abeliano $G = C \times < c >$, el producto directo de C, de orden n, con

un grupo cíclico de orden 2, cuyo generador es denotado por c. Sea $X, Y \subset G$ tales que $\mid X \mid = r$ y $\mid Y \mid = s$, con $r, s \geq 1$. Por la fórmula $\mu_G = \kappa_G$ en el grupo abeliano G, se tiene $\mid X * Y \mid \geq \kappa_G(r, s)$.
Además como G tiene orden $2n$ y los ordenes de los subgrupos de G son todos los divisores positivos de $2n$, como es el caso para el grupo no abeliano D_n, se tiene que $\kappa_G(r, s) = \kappa_{D_n}(r, s)$.

La idea es demostrar que si cualquiera de los r_0, r_1 o s_0, s_1 se hace cero, entonces se puede construir subconjuntos $X, Y \subset G$ de cardinales $r = r_0 + r_1$ y $s = s_0 + s_1$ respectivamente tal que $\mid X * Y \mid = \mid A * B \mid$.

Ahora para subconjuntos $X, Y \subset G$, $X = A_0 \cup A_1 c$ y $Y = B_0 \cup B_1 c$, donde A_0, A_1, B_0, B_1 son subconjuntos del grupo cíclico C; se tiene

$$X * Y = (A_0 \cup A_1 c) * (B_0 \cup B_1 c) = (A_0 * B_0 \cup A_1 * B_1) \cup (A_0 * B_1 \cup A_1 * B_0)c,$$

y

$$\mid X * Y \mid = \mid A_0 * B_0 \cup A_1 * B_1 \mid + \mid A_0 * B_1 \cup A_1 * B_0 \mid.$$

Caso 1: Si $A_0 = \emptyset$, se debe tener $X = A_1 c$ y $Y = B_0^{-1} \cup B_1^{-1} c$. Note que $\mid X \mid = \mid A_1 \mid = r$, $\mid Y \mid = s$. Tomando el producto de X y Y en G, se tiene

$$X * Y = A_1 * B_1^{-1} \cup A_1 * B_0^{-1} c,$$

y

$$\mid X * Y \mid = \mid A_1 * B_1^{-1} \mid + \mid A_1 * B_0^{-1} \mid = \mid A * B \mid.$$

Caso 2: Si $A_1 = \emptyset$, se debe tener $X = A_0$ y $Y = B_0 \cup B_1 c$. Note que $\mid X \mid = \mid A_0 \mid = r$, $\mid Y \mid = s$. Tomando el producto de X y Y en G, se tiene

$$X * Y = A_0 * B_0 \cup A_0 * B_1 c,$$

y

$$\mid X * Y \mid = \mid A_0 * B_0 \mid + \mid A_0 * B_1 \mid = \mid A * B \mid.$$

Caso 3: Si $B_0 = \emptyset$, se debe tener $X = A_0^{-1} \cup A_1 c$ y $Y = B_1^{-1} c$. Note que $\mid X \mid = \mid A_0^{-1} \cup A_1 \mid = r$, $\mid Y \mid = \mid B_1^{-1} \mid = s$. Tomando el producto de X y Y en G, se tiene

$$X * Y = A_1 * B_1^{-1} \cup A_0^{-1} * B_1^{-1} c,$$

y

$$| X * Y | = | A_1 * B_1^{-1} | + | A_0^{-1} * B_1^{-1} | = |A * B|.$$

Caso 4: Si $B_1 = \emptyset$, se debe tener $X = A_0^{-1} \cup A_1 c$ y $Y = B_0^{-1}$. Note que $| X | = | A_0^{-1} \cup A_1 | = r$, $| Y | = | B_0^{-1} | = s$. Tomando el producto de X y Y en G, se tiene

$$X * Y = A_0^{-1} * B_0^{-1} \cup A_1 * B_0^{-1} c,$$

y

$$| X * Y | = | A_0^{-1} * B_0^{-1} | + | A_1 * B_0^{-1} | = |A * B|.$$

Por tanto, en todo los casos

$$| A * B | = | X * Y | \geq \kappa_G(r, s) = \kappa_{D_n}(r, s). \quad \square$$

Ahora veremos que la desigualdad $M_C(r_0, r_1, s_0, s_1) \geq \kappa_{D_n}(r, s)$, es verdadera cuando n es una potencia prima.

Teorema 12. *Sea p un número primo y $v \in \mathbb{N}$ un entero positivo. Para cada $1 \leq r_0, r_1, s_0, s_1 \leq p^v$. Se tiene*

$$M_C(r_0, r_1, s_0, s_1) \geq \kappa_D(r_0 + r_1, s_0 + s_1),$$

donde C es el grupo cíclico de orden p^v y D el grupo diédrico de orden $2p^v$.

Prueba: Sea H cualquier grupo abeliano de orden p^v. Entonces se sigue que $\mu_H(x, y) = \kappa_C(x, y)$ para todo $1 \leq x, y \leq | H |$. Similarmente si G es cualquier grupo abeliano de orden $2p^v$, se tiene $\mu_G(x, y) = \kappa_{D_{2p^v}}(x, y)$, para todo $1 \leq x, y \leq | G |$ pues los ordenes de los subgrupos de G y D_{p^v} coinciden. Ambos consisten exactamente de los divisores positivos de $2p^v$.

Ahora se fijará especificamente cada grupo H y G. Es decir; H será el grupo aditivo del campo finito $\mathbb{F}_q$ de orden $q = p^v$, y G será el producto directo $G = H \times \mathbb{Z}/2\mathbb{Z}$.

Sea $c = (0, 1) \in G$, el cual es de orden 2; Por un leve abuso de notación, se considera a H como un subgrupo de G, y por tanto G como la unión disjunta de dos clases, H y $H + c$.
Dados los subconjuntos $A_0, A_1, B_0, B_1 \subset H$ de cardinales r_0, r_1, s_0, s_1 respectivamente y ahora sea $A, B \subset G$ definimos $A = A_0 \cup (A_1 + c)$ y $B = B_0 \cup (B_1 + c)$. Como esas uniones son disjuntas, $| A | = r_0 + r_1$ y $| B | = s_0 + s_1$. Considere el conjunto suma $A + B \subset G$.

Como $2c = 0$, sea $U = (A_0 + B_0) \cup (A_1 + B_1)$ y $V = \{(A_0 + B_1) \cup (A_1 + B_0)\} + c$; entonces $A + B = U \cup V$, luego

$$\begin{aligned} |\, U \,| + |\, V \,| &= |\, A + B \,| \geq \mu_G(r_0 + r_1, s_0 + s_1) \\ &= \kappa_G(r_0 + r_1, s_0 + s_1) \\ &= \kappa_D(r_0 + r_1, s_0 + s_1), \end{aligned}$$

Donde la última igualdad se da porque los grupos $G = H \times \mathbb{Z}/2\mathbb{Z}$ y $D = D_{p^v}$ tienen en mismo conjunto de ordenes de subgrupos.

Ahora elijamos los subconjuntos $A_0, A_1, B_0, B_1 \subset H$ tal que $|\, U \,| + |\, V \,|$ es el mínimo de $M_C(r_0, r_1, s_0, s_1)$.
Aquí apelamos a la descripción de H como el grupo aditivo de $\mathbb{F}_{p^v}$ y para el (recíproco) orden lexicográfico en H, es visto como un espacio vectorial sobre $\mathbb{F}_p$. En [4] este orden es descrito como el orden natural en el intervalo de enteros $[0, p^v - 1]$, donde la adición del espacio vectorial $\mathbb{F}_p$ esta dada por la suma p-ádica de Nim (Ver pagina 17 de [4]).

Así, dado $1 \leq t \leq p^v$, denotemos por IS_t el segmento inicial de H de cardinalidad t, entonces dado cualesquiera dos segmentos iniciales IS_t, IS_u $(1 \leq t, u \leq p^v)$, se sigue de la proposición (3.1) de [4], que su conjunto suma $IS_t + IS_u$ es optimamente pequeño; esto es $|\, IS_t + IS_u \,| = \mu_H(t, u)$. Más precisamente,

$$IS_t + IS_u = IS_{\mu_H(r,s)},$$

como el conjunto suma de dos segmentos iniciales de H, que se probó en [4] ser otra vez un segmento inicial.
Una simple pero crucial observación para lo que sigue es que IS_t contiene a IS_u, o IS_u contiene a IS_t; en efecto, se tiene que $IS_t \cup IS_u = IS_{\text{máx}\{t,u\}}$.

Ahora, nuestra elección específica de los subconjuntos A_0, A_1, B_0, B_1 será tomar segmentos iniciales de los cardinales requeridos. Esto es, $A_0 = IS_{r_0}$, $A_1 = IS_{r_1}$, $B_0 = IS_{s_0}$ y $B_1 = IS_{s_1}$.
Sea $\mu_{i,j} = \mu_H(r_i, s_j) = \kappa_C(r_i, s_j)$ para $i, j \in \{0, 1\}$. Pero como $IS_{r_i} + IS_{s_j} = IS_{\mu_{i,j}}$, se tiene $U = (A_0 + B_0) \cup (A_1 + B_1) = IS_{\text{máx}\{\mu_{0,0}, \mu_{1,1}\}}$ y similarmente, $V = (A_0 + B_1) \cup (A_1 + B_0) = IS_{\text{máx}\{\mu_{0,1}, \mu_{1,0}\}}$.
Luego, $|\, U \,| + |\, V \,| = \text{máx}\{\mu_{0,0}, \mu_{1,1}\} + \text{máx}\{\mu_{0,1}, \mu_{1,0}\}$; por la desigualdad

$$|\, U \,| + |\, V \,| \geq \kappa_D(r_0 + r_1, s_0 + s_1),$$

se tiene

$$\text{máx}\{\mu_{0,0}, \mu_{1,1}\} + \text{máx}\{\mu_{0,1}, \mu_{1,0}\} \geq \kappa_D(r_0 + r_1, s_0 + s_1);$$

Lo que concluye que

$$M_C(r_0, r_1, s_0, s_1) \geq \kappa_D(r_0 + r_1, s_0 + s_1). \quad \square$$

Nota: El Lema 7 y el Teorema 11 sintetizan que cuando n es una potencia prima $\mu_{D_n}(r,s) \geq \kappa_{D_n}(r,s)$, que era lo que se deseaba probar en esta sesión.

A manera de concluir, la sesión 3.1 y 3.2 dan prueba al corolario 1.

3.3. Comentarios sobre la función descomposición

En esta sección se discute la validez de la desigualdad

$$M_C(r_0, r_1, s_0, s_1) \geq \kappa_D(r_0 + r_1, s_0 + s_1);$$

en el Lema 7, de la sección anterior.
Nos dan un entero positivo n y un cuadruple de enteros (r_0, r_1, s_0, s_1) tal que $1 \leq r_i, r_j \leq n$ para $i, j \in \{0, 1\}$.
La función descomposición $M_C(r_0, r_1, s_0, s_1)$ es la expreción

$$M(r_0, r_1, s_0, s_1) = \text{máx}\{\kappa_n(r_0, s_0), \kappa_n(r_1, s_1)\} + \text{máx}\{\kappa_n(r_0, s_1), \kappa_n(r_1, s_0)\},$$

donde $\kappa_g(r,s) = \min_{d|g} \left\{ \left(\left[\frac{r}{d}\right] + \left[\frac{s}{d}\right] - 1 \right) d \right\}$.
La hipótesis en el lema 7, fue la desigualdad

$$M(r_0, r_1, s_0, s_1) \geq \kappa_{2n}(r_0 + r_1, s_0 + s_1).$$

En el Teorema 11, Se probó que la desigualdad anterior se da para todo (r_0, r_1, s_0, s_1) con $1 \leq r_0, r_1, s_0, s_1 \leq n$, si n es una potencia prima.
Ahora se muestra que la desigualdad anterior es falsa para al menos un cuadruple (r_0, r_1, s_0, s_1) con $1 \leq r_0, r_1, s_0, s_1 \leq n$, si n es divisible por dos primos distintos.

Proposición 2. *Sea $n = uv$, donde u, v son enteros primos relativos con $u, v \geq 2$, entonces*

$$\text{máx}\{\kappa_n(r_0, s_0), \kappa_n(r_1, s_1)\} + \text{máx}\{\kappa_n(r_0, s_1), \kappa_n(r_1, s_0)\} < \kappa_{2n}(r, s), \quad (3)$$

para $r_0 = u$, $r_1 = v$, $s_0 = n - u$ y $s_1 = n - v$.

Para la demostración de la proposición, se usará de [8], el siguiente resultado,

Corolario 4. *Si $1 \leq r, s \leq g - 1$, entonces*

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

Donde g es el orden del grupo G y h es el orden más grande de un subgrupo de G.

En el contexto presente, la fórmula anterior queda como sigue,

$$\kappa_g(x,y) = \min\{x+y-\gcd(x,y,g), \kappa_g(x+1,y), \kappa_g(x,y+1)\}, \quad (2)$$

para $1 \leq x, y \leq g-1$.
Y la prueba de la Proposición 2 se puede observar en [6].

El Lema 7 , implica que es suficiente verificar $\mid A*B \mid \geq \kappa_{D_n}(r,s)$ para los subconjuntos $A = A_0 \cup A_1 b$, $B = B_0 \cup B_1 b$ tal que $\mid A \mid = r$, $\mid B \mid = s$ con $r_i = \mid A_i \mid \geq 1, s_j = \mid B_j \mid \geq 1$ y tal que

$$M_C(r_0, r_1, s_0, s_1) \geq \kappa_D(r_0+r_1, s_0+s_1).$$

Además, para el siguiente lema podemos tambien restringir la búsqueda del cuadruple (r_0, r_1, s_0, s_1) que satisface $r_i + s_j \leq n$ para todo i, j.

Lema 8. *Si $A = A_0 \cup A_1 b$, $B = B_0 \cup B_1 b$ es un par de subconjuntos $A, B \subset D_n = C \cup Cb$, tal que $\mid A_i \mid + \mid B_j \mid > n$ para algún índice $i, j \in \{0,1\}$, entonces*

$$\mid A*B \mid \geq \kappa_{D_n}(r,s),$$

donde $r = \mid A \mid$, $s = \mid B \mid$.

La prueba de este lema es consecuente a la del lema 7 en el siguiente sentido;

Prueba: El conjunto producto $A*B$ de $A = A_0 \cup A_1 b$, $B = B_0 \cup B_1 b$ esta dado por

$$A*B = (A_0 * B_0 \cup A_1 * B_1^{-1}) \cup (A_0 * B_1 \cup A_1 * B_0^{-1})b.$$

según lo visto arriba. Luego

$$\mid A*B \mid = \mid A_0 * B_0 \cup A_1 * B_1^{-1} \mid + \mid A_0 * B_1 \cup A_1 * B_0^{-1} \mid .$$

Ahora identificaremos las dos copias del grupo cíclico $C = < a >$ de orden n definido en D_n y G.

Sea $X, Y \subset G = C \cup Cc$ los dos subconjuntos $X = A_0 \cup A_1 c$ y $Y = B_0^{-1} \cup B_1 c$de cardinales r y s respectivamente . Luego

$$X*Y = (A_0 * B_0^{-1} \cup A_1 * B_1) \cup (A_0 * B_1 \cup A_1 * B_0)c,$$

y por tanto

$$\mid X*Y \mid = \mid A_0 * B_0^{-1} \cup A_1 * B_1 \mid + \mid A_0 * B_1 \cup A_1 * B_0^{-1} \mid .$$

Por el teorema 5, se tiene que

$$\mid X*Y \mid \geq \mu_G(r,s) = \kappa_{2n}(r,s) = \kappa_{Dn}(r,s).$$

Por tanto, aunque A, B y X, Y estan en diferentes grupos, se ve que si

$$| A_0 * B_0 \cup A_1 * B_1^{-1} | \geq | A_0 * B_0^{-1} \cup A_1 * B_1 |, \quad (4)$$

entonces

$$| A * B | \geq | X * Y | \geq \kappa_{D_n}(r, s).$$

Obviamente, (4) es verdadero si $A_0 * B_0 = C$.
Esto sucede si $| A_0 | + | B_0 | > | C | = n$ por lo que se ve en teorema 1.1 de [2]. (Ver también [8] teorema 4.1).
Si $| A_i | + | B_j | > n$ para algún otro par de índices $i, j \in \{0, 1\}$, podemos reducir de nuevo el caso $| A_0 | + | B_0 | > n$ pero reemplzando si es necesario, $A = A_0 \cup A_1 b$ por $A' = bA = A_1^{-1} \cup A_0^{-1} b$ y $B = B_0 \cup B_1 b$ por $B' = Bb = B_1 \cup B_0 b$. Esto finaliza la prueba del lema. □

Note que, en cualquier caso, en la busqueda de contraejemplos para la conjetura $\mu_{D_n}(r, s) \geq \kappa_{D_n}(r, s)$, es suficiente examinar subconjuntos $A = A_0 \cup A_1 b \subset D_n$ y $B = B_0 \cup B_1 b \subset D_n$ tal que $| A_0 * B_0 | \leq n - 1$. Esto sigue de la demostración anterior.
Usando los teoremas en la sección 4 de [8] y el lema anterior se ha verificado la conjetura para el compuesto de n por el cálculo de una maquina hasta 15; esto es, $n = 6, 10, 12, 14 y 15$.

Resultados importantes de la función μ_G

Finalmente, se presentarán sin demostración, algunos teoremas de Eliahou y Kervaire sobre el estudio de la función μ_G en grupos finitos no abelianos (Ver sus demostraciones en [8]).

Teorema 13. *Sea G un grupo finito, si r, s son enteros tal que $1 \leq r, s \leq | G |$ y $r + s > | G |$, entonces $\mu_G(r, s) = \kappa_G(r, s) = | G |$.*

Teorema 14. *Sean G un grupo finito y sean r y s enteros positivos tal que $r + s = | G |$, entonces $\mu_G(r, s) = \kappa_G(r, s)$.*

Teorema 15. *Sean G un grupo finito y sean r y s enteros positivos tal que $r + s = | G | - 1$, entonces $\mu_G(r, s) \leq \kappa_G(r, s)$.*

Teorema 16. *Sea G un grupo finito y sean r, s enteros positivos tal que $r, s \leq | G |$. 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:*

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

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

El siguiente corolario es una consecuencia inmediata del teorema anterior.

Corolario 5. *Sea G un grupo finito, si r, s son enteros positivos tal que $r, s \leq \mid G \mid$, y $\kappa_G(r,s) = s + \left[\frac{r}{2}\right]$, entonces $\mu_G(r,s) \geq \kappa_G(r,s)$.*

Teorema 17. *Sea G un grupo finito. Si $1 \leq r \leq 3$, entonces $\mu_G(r,s) = \kappa_G(r,s)$.*

Conclusiones

Al presentar un panorama general del problema de los conjuntos suma pequeños en grupos abelianos y finitos no abelianos, se motiva al lector a iniciar investigaciones tendientes a comprender la función μ_G en ciertas clases de grupos.
Se considera que este trabajo hecho como monografía del artículo (Sumsets in dihedral groups) escrito por Eliahou y Kervaire, contribuye a sentar las bases necesarias para continuar el estudio del problema de los conjuntos suma pequeños, especialmente para la clase de p-grupos finitos.

Como se pudo apreciar, para los grupos diédricos que cumplen la condición de que n es potencia de un número primo, entonces la función μ_{D_n} tiene una fórmula explícita. A manera de concluir y particularmente se sugiere adelantar investigaciones que den respuesta a los siguientes problemas abiertos:

a. Probablemente se tenga la igualdad $\mu_{D_n}(r,s) = \kappa_{D_n}(r,s)$ para todo entero $n \geq 2$.

b. La desigualdad $\mu_G(r,s) \geq \kappa_G(r,s)$ se da para cualquier grupo finito y todo entero positivo $r, s \leq \mid G \mid$ (Ver [8]).

c. Para un grupo abeliano finito G esta el problema de caracterizar los pares de subconjuntos A y B de G que realizan $\mu_G(r,s)$.

d. Haciendo un analisis de los p-grupos finitos y de los grupos de Hamilton, es posible encontrar resultados para la función μ_G, tales como; Si G es un grupo Hamiltoniano de la forma $G \cong Q \times (\mathbb{Z}_2)^n \times \mathbb{Z}_p$, con p primo mayor que 2, es posible que se cumpla la igualdad $\mu_G(r,s) = \kappa_G(r,s)$, para todo par de enteros r y s tales que $0 \leq r, s \leq \mid G \mid$.

Bibliografía

[1] Bollobás, Béla; Leader, Imre. Sums in the grid. Discrete math. 162 (1996), 1-3, 31-48.

[2] Henry B. Mann, Addition theorems, Interscience Publishers, John Wiley and Sons, 1965.

[3] Plagne, Alain; Additive number theory sheds extra light on the Hopf-Stiefel function. Enseign. Math. (2)49 (2003), No. 1-2, 109 - 116.

[4] Shalom Eliahou, Michel Kervaire. Sumsets in vector spaces over finite fields, J. Number Theory 71 (1998) 12-39.

[5] Shalom Eliahou, Michel Kervaire, Alain Plagne. Optimally small sumsets in finite abelian groups. J. Number Theory 101 (2003) 338-348.

[6] Shalom Eliahou, Michel Kervaire. Sumsets in dihedral groups, Eur. J. Combinatorics 27 (2006) 617-628.

[7] Shalom Eliahou, Michel Kervaire. The small sumsets property for solvable finite groups, Eur. J. Combinatorics 27 (2006) 1102-1110.

[8] Shalom Eliahou, Michel Kervaire. Some results on minimal sumset size in finite non-abelian groups, J. Number Theory 124 (2007) 234-247.

[9] Shalom Eliahou, Michel Kervaire. Bounds on the minimal sumset size funtion in groups, International journal of number theory. Vol. 3, No. 4 (2007) 503-511.

[10] Shalom Eliahou, Michel Kervaire. Minimal sumsets in finite solvable groups. Discrete Mathematics 310 (2010) 471-479.