**EI MÉTODO ISOPERIMÉTRICO Y SU APLICACIÓN A LOS
CONJUNTOS SUMA PEQUEÑOS**

**EUCLIDES DÍAZ ARCOS
ANDRÉS FERNANDO JARAMILLO MEJÍA**

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

2012

**EI MÉTODO ISOPERIMÉTRICO Y SU APLICACIÓN A LOS
CONJUNTOS SUMA PEQUEÑOS**

**EUCLIDES DÍAZ ARCOS
ANDRÉS FERNANDO JARAMILLO MEJÍA**

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

**Asesor
Wilson Fernando Mutis Cantero
Magister en Matemáticas**

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

2012

Nota de Responsabilidad

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

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

Nota de Aceptación

Wilson Fernando Mutis Cantero
Presidente de Tesis

Fernando Andrés Benavides Agredo Jurado

Oscar Fernando Soto Agreda Jurado

San Juan de Pasto, Noviembre 22 de 2012

Agradecimientos

Primero que todo quiero agradecer a Dios por haberme dado salud para poder culminar mis estudios. Agradecer a nuestro asesor y amigo Mg. Wilson Fernando Mutis, quien con su sabiduría, conocimiento y voluntad supo guiar cada una de las etapas de este trabajo. A mi compañero de Tesis, Andrés Fernando Jaramillo Mejía, por su gran compañerismo y dedicación para la realización del mismo. Agradecer a mi familia, en especial, a mis padres Euclides Díaz e Iliá Arcos, mi hermano José Teófilo Díaz, mi prima Edilia Gómez y el señor Silvio Armando Chavez, fueron las personas que siempre me apoyaron durante toda mi carrera. Finalmente agradecer a los profesores del Departamento de Matemáticas y Estadística de la Universidad de Nariño por sus valiosas enseñanzas.

Euclides Díaz Arcos

Agradezco de corazón a Martha Mejía Guerrero y Fabio Jaramillo Bastidas quienes me dieron el regalo de la vida, todo su amor y valioso apoyo, a ellos me debo por entero.

Gracias a Wilson Fernando Mutis Cantero, amigo y asesor, sin sus conocimientos no hubiera sido posible culminar el presente trabajo.

Gracias a mi amigo Euclides Díaz Arcos, quien me mostró su paciencia y capacidad de comprensión durante todo el proyecto, para él mis mejores deseos.

Por último agradezco a todas aquellas personas que me ayudaron, de una u otra forma, a cerrar esta etapa de mi vida, es muy corto el espacio en esta página para nombrarlos uno por uno.

Andrés Fernando Jaramillo Mejía

Resumen

En el presente trabajo se realiza un estudio detallado de una teoría denominada, El Método Isoperimétrico, desarrollada por Hamidoune y Balandraud, y su aplicación al Problema de los Conjuntos Suma Pequeños. Específicamente como una aplicación de esta teoría se da a conocer que la ecuación $\mu_G(r, s) = \kappa_G(r, s)$ obtenida para el caso en que G es un grupo abeliano no se cumple para grupos finitos no abelianos de la forma $G = \mathbb{Z}_q \rtimes \mathbb{Z}_p$, donde p y q son primos impares tales que $q \equiv 1 \pmod{p}$. Además se desarrolla una serie de algoritmos en el Sistema de Álgebra Computacional GAP 4.4.12, los cuales permiten observar lo complicado que resulta encontrar directamente el valor de $\mu_G(r, s)$.

Abstract

In this work we make a detailed study of a theory called, The Isoperimetric method, developed by Hamidoune and Balandraud, and its application to the Problem of small sumsets. Specifically as an application of this theory is disclosed that the equation $\mu_G(r, s) = \kappa_G(r, s)$ obtained for the case where G is an abelian group does not hold for non-abelian finite groups of the form $G = \mathbb{Z}_q \rtimes \mathbb{Z}_p$, where p and q are odd primes such that $q \equiv 1 \pmod{p}$. It also develops a series of algorithms in Computer Algebra System GAP 4.4.12, which allow us to observe how difficult it is to find directly the value of $\mu_G(r, s)$.

Índice general

Introducción	VII
1. Notación General y Fundamentos Teóricos	1
1.1. Notación y Conceptos Generales	1
1.2. El Problema de los Conjuntos Suma Pequeños	8
2. Herramientas Aditivas	15
2.1. La Aplicación P_B y sus Propiedades	15
2.2. Dualidad Aditiva $D_B : X \rightarrow G \setminus XB$	20
2.3. Ideas Isoperimétricas	25
3. El Método Isoperimétrico y su Aplicación a la Función μ_G	35
3.1. Estructura de 1-Celdas y 1-Núcleos	35
3.2. Estructura de las a_2 -Celdas	41
3.3. Una Aplicación a los Grupos Solubles	44
A. Algoritmos en GAP 4.4.12	54
A.1. Generación del Grupo $P = \mathbb{Z}_q \rtimes \mathbb{Z}_p$	55
A.2. Función $\kappa_G(r, s)$	58
A.3. Función $\mu_G(r, s)$ para Grupos en General	63
A.4. Herramientas Aditivas	64
Problemas Abiertos y Conclusiones	71
Referencias	72
Índice alfabético	74

Introducción

Sea $(G, \cdot)$ un grupo. El conjunto suma (o conjunto producto) de dos subconjuntos no vacíos A y B de G , denotado con $A \cdot B$, o simplemente AB , es el conjunto de todos los elementos de G que se pueden expresar como ab , donde $a \in A$ y $b \in B$, es decir

$$AB = \{ab : a \in A \text{ y } b \in B\}.$$

Cuando hay certeza en la conmutatividad del grupo, el conjunto suma de dos subconjuntos no vacíos A y B de G se denota en forma aditiva,

$$A + B = \{a + b : a \in A \text{ y } b \in B\}.$$

Si $A = \emptyset$ o $B = \emptyset$ se define $AB = \emptyset$ o $A + B = \emptyset$.

Un problema de interés en Teoría Aditiva de Números, denominado: *El Problema de los Conjuntos Suma Pequeños*, consiste en determinar una fórmula explícita que permita calcular el mínimo de los cardinales $|AB|$ donde A y B son subconjuntos finitos y no vacíos de un grupo G sujetos a las condiciones $|A| = r$ y $|B| = s$, es decir, se desea calcular los valores de la función μ_G dada por

$$\begin{aligned} \mu_G : [1, |G|]^2 &\longrightarrow \mathbb{N}^* \\ (r, s) &\longrightarrow \mu_G(r, s) = \min \{|AB| : A, B \subseteq G \text{ y } |A| = r, |B| = s\}. \end{aligned}$$

La función $\mu_G(r, s)$ 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 de $\mu_G(r, s)$ para el caso en que G es un grupo no abeliano. Posiblemente uno de los obstáculos que han impedido generalizar $\mu_G(r, s)$ a cualquier grupo es que no se cuenta con una versión no abelianizada del Teorema de Kneser. En este sentido Balandraud en [4] utilizando una variante del método isoperimétrico desarrollado por Hamidoune en [14, 15], presentó una segunda prueba del teorema de Kneser, lo cual le permitió en [5] dar nuevos valores de la función $\mu_G(r, s)$ para una familia infinita de grupos solubles y también responder negativamente una pregunta formulada en esta problemática sobre esta función (ver Pregunta 3.1, Capítulo 3).

Se ha demostrado (ver [12], [17]) que la fórmula para $\mu_G(r, s)$ obtenida en el caso en que G es un grupo abeliano se cumple para todo grupo diédrico $G = D_n$ de orden $2n$ y para algunos grupos hamiltonianos de la forma $\mathcal{Q} \times (\mathbb{Z}/2\mathbb{Z})^k \times \mathcal{C}$ con $\mathcal{C}$ un grupo cíclico de orden impar y $k \in \mathbb{Z}^+$. También en [11] Elihaou y Kervaire presentan una cota inferior y una cota superior para $\mu_G(r, s)$ en términos de funciones numéricas cuyos valores son sencillos de encontrar.

Para claridad del lector, *el método isoperimétrico* es una teoría que esta compuesta por una serie de definiciones teoremas y proposiciones aplicada a la Teoría Aditiva. Inicialmente la teoría del método isoperimétrico fue trabajada por Hamidoune, posteriormente Balandraud desarrolló algunas herramientas aditivas adicionales que implementó y generalizó en el método isoperimétrico de Hamidoune, las cuales le permitieron dar una segunda prueba del teorema de Kneser (ver [4]), y además obtener nuevos valores de la función $\mu_G(r, s)$ (ver [5]). Con base en estos valores obtenidos para $\mu_G(r, s)$, Balandraud en [5] dio respuesta negativa a la Pregunta 3.1 formulada por los autores de [7] acerca de esta función. Sean G un grupo y B un subconjunto de G tal que $1 \in B$. Considérese la expresión $|XB| - |X|$, donde X es un subconjunto no vacío y finito de G . **El método isoperimétrico** aplicado a la función $\mu_G(r, s)$, que se estudia en este trabajo, consiste en tomar los valores sucesivos dados por $|XB| - |X|$ tales que $|XB| - |X| \leq |B| - 1$, y los conjuntos X de un grupo G que satisfacen esta desigualdad.

El presente trabajo se desarrolló como un requisito parcial para optar al título de Licenciado en Matemáticas de la Universidad de Nariño, bajo la asesoría del Mg. Wilson Fernando Mutís. Tiene como propósito hacer un estudio detallado de una teoría, denominada *el método isoperimétrico*, desarrollada primero por Hamidoune y posteriormente por Balandraud (ver [4, 5, 14, 15]), y dar a conocer una aplicación de esta teoría al problema de los conjuntos suma pequeños. Específicamente como una aplicación de esta teoría se da a conocer que la ecuación $\mu_G(r, s) = \kappa_G(r, s)$ obtenida para el caso en que G es un grupo abeliano arbitrario no se satisface en general para grupos solubles finitos no abelianos de la forma $G = \mathbb{Z}_q \rtimes \mathbb{Z}_p$, donde p y q son primos impares tales que $q \equiv 1 \pmod{p}$.

El trabajo se ha dividido en tres capítulos. En la primera Sección del Capítulo 1 se muestra la notación general utilizada y algunos conceptos generales básicos, incluyendo las pruebas de éstos tal vez no conocidas por el lector. En la segunda Sección se presenta en forma general el problema de los conjuntos suma pequeños y se enuncian los resultados obtenidos para grupos abelianos y otros ya conocidos en grupos finitos no abelianos. En el segundo capítulo se estudian las herramientas aditivas desarrolladas por Balandraud en [5]. En las Secciones 3.1 y 3.2 del Capítulo 3 se aplican algunas propiedades desarrolladas en el Capítulo 2 al estudio del método isoperimétrico y se presentan definiciones y conceptos nuevos relacionados

con 1-celdas, 1-núcleos, j -celdas y a_2 -celdas. Finaliza este Capítulo con la aplicación de esta teoría a la función $\mu_G(r, s)$ en una familia infinita de grupos finitos no abelianos.

Posteriormente se incluye un apéndice donde se muestran los algoritmos desarrollados por los autores en el sistema de algebra computacional GAP 4.4.12. Cada uno de los algoritmos esta acompañado de un ejemplo que ilustra la función que desempeña cada uno de éstos. Finalmente se presenta una pequeña sección denominada problemas abiertos y conclusiones.

Cabe resaltar que las demostraciones del Capítulo 1, Capítulo 2 y la mayoría del Capítulo 3, son producción de los autores tras el estudio de los artículos que al final se referencian. Además, algunos de los teoremas que aquí se plantean fueron reescritos por los autores con el propósito de dar al lector mayor claridad en el tema.

Las referencias más utilizadas en este trabajo son [4, 5, 14, 15, 16, 18]. Los términos y notación que no se definen pueden ser encontrados en estas fuentes.

Capítulo 1

Notación General y Fundamentos Teóricos

En la primera sección de este capítulo se introducen algunas notaciones que serán utilizadas a lo largo del presente trabajo y los conceptos generales básicos de la teoría de grupos. Posteriormente se presenta en forma general **El problema de los Conjuntos Suma Pequeños** y se enuncian algunos teoremas clásicos de la Teoría Aditiva de Números, como son los Teoremas de Cauchy-Davenport, Vosper y Kneser. También se dan a conocer sin demostración tres de los resultados más relevantes obtenidos por Eliahou, Kervaire y Plagne (ver [7], [8], [1, 2]) que permitieron obtener una fórmula explícita para la función $\mu_G(r, s)$ en grupos abelianos arbitrarios. De igual manera se enuncian dos resultados para grupos finitos no abelianos, el primero obtenido por Eliahou y Kervaire (ver [12]) y el segundo por Mutis, Benavides y Castillo (ver [17]).

1.1. Notación y Conceptos Generales

Generalmente se utilizarán letras mayúsculas $A, B, C, \dots, Y, Z$ para representar conjuntos y grupos y letras minúsculas $a, b, c, \dots, y, z$ para representar sus elementos. La expresión $[m, n]$ se usará para representar números enteros que satisfacen $m \leq k \leq n$, donde $m, n, k \in \mathbb{Z}$. Dado un conjunto G , su cardinal se denotará con $|G|$. Los grupos abelianos se representarán en forma aditiva y se utilizará la notación multiplicativa para

representar los grupos no abelianos o aquellos grupos donde no haya conocimiento sobre su conmutatividad. Sean G un grupo y A un subconjunto de G , se denotará con aA al conjunto $\{a\}A$. La identidad en un grupo G se simbolizará con 1 , y con 0 cuando haya claridad sobre su conmutatividad. El conjunto $G \setminus (AB)$ se denotará con $G \setminus AB$ y la expresión $(AB) \setminus A$ se identificará con $AB \setminus A$. Con $\mathbb{N}^*$ se representará al conjunto de los enteros positivos. El grupo cíclico $\mathbb{Z}/n\mathbb{Z}$, de congruencias modulo n , se identificará con $\mathbb{Z}_n = \{0, 1, 2, 3, \dots, n-1\}$, para todo n mayor o igual que dos. En algunas ocasiones se simbolizará el complemento de un conjunto A con A^c .

Aunque en los *conjuntos suma* no hay un orden en las operaciones, en este trabajo se asumirá que el producto de conjuntos domina sobre el complemento de los mismos, esto es, en la expresión $G \setminus XB$, la operación que primero se realiza es el producto XB y luego se aplica el complemento $(XB)^c$, de manera similar se procede en $AB \setminus A$, es decir, determinado el conjunto $Z = AB$ se opera $Z \setminus A$.

Definición 1.1. Grupo

Un grupo es un par $(G, \cdot)$ donde G es un conjunto no vacío y $\cdot$ es una operación binaria definida en G que satisface los siguientes axiomas:

- Para todo $a, b \in G$ se tiene que $a \cdot b \in G$ (cierre).
- Si $a, b, c \in G$ entonces $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (ley asociativa).
- Existe un elemento $e \in G$ tal que $a \cdot e = e \cdot a = a$ para todo $a \in G$ (existencia de un elemento identidad en G).
- Para todo $a \in G$ existe un elemento $a^{-1} \in G$ tal que $a \cdot a^{-1} = a^{-1} \cdot a = e$ (existencia de inversos en G).

Si además, para cualquier $a, b \in G$ se tiene que $a \cdot b = b \cdot a$, se dice que G es *abeliano*.

Definición 1.2. Subgrupo

Un subconjunto H de un grupo G es un subgrupo de G si H es un grupo bajo la operación definida en G .

Definición 1.3. Clases laterales

Sea H un subgrupo de un grupo G . Para cada $g \in G$, la clase lateral izquierda de H en G es el conjunto

$$gH = \{y : y = gh \text{ para algún } h \in H\},$$

y la clase lateral derecha de H en G es el conjunto

$$Hg = \{y : y = hg \text{ para algún } h \in H\}.$$

Observe que un subgrupo H de un grupo G es en sí es una clase lateral izquierda de H en G . Se enuncia el siguiente teorema de acuerdo a la Definición 1.3.

Teorema 1.1. *Dos clases laterales izquierdas (derechas) de H en G son disjuntas ó son conjuntos idénticos. Una clase lateral izquierda (derecha) de H , contiene el mismo número de elementos que H .*

Demostración. Sean $x, y \in G$. Si xH y yH son conjuntos disjuntos, nada hay que probar. Suponga que $xH \cap yH \neq \emptyset$, entonces existe z tal que $z \in xH$ y $z \in yH$. Luego $z = xh_1 = yh_2$, con $h_1, h_2 \in H$. Se sigue que $x = yh_2h_1^{-1}$ y $xh = yh_2h_1^{-1}h = yh'$; de donde $xh \in yH$, es decir $xH \subset yH$. De forma análoga, $yh = xh_2h_1^{-1}h = xh'$ y se deduce que $yH \subset xH$. Por lo tanto $xH = yH$, es decir, los conjuntos xH y yH son idénticos. De forma similar se puede dar la prueba para las clases laterales derechas Hx y Hy . Finalmente para $x \in G$, las aplicaciones

$$\begin{aligned} \varphi : H &\longrightarrow xH & \psi : H &\longrightarrow Hx \\ h &\longrightarrow \varphi(h) = xh & h &\longrightarrow \psi(h) = hx \end{aligned}$$

son biyectivas, esto muestra que H , xH y Hx contienen el mismo número cardinal de elementos. $\square$

Recuerde que un automorfismo es un homomorfismo biyectivo $\varphi : G \longrightarrow G$.

Definición 1.4. Subgrupo normal

Un subgrupo N de un grupo G es un subgrupo normal de G si $g^{-1}Ng = N$ para todas las $g \in G$, esto es, si N permanece invariante bajo todo automorfismo interno de G . Si N es un subgrupo normal de G se escribe $N \triangleleft G$.

Un resultado clásico de la teoría de grupos es que dado un subgrupo N de un grupo G , el conjunto de clases laterales (izquierdas) G/N tiene estructura de grupo si y sólo si N es un subgrupo normal de G . En este caso G/N se denomina el grupo factor de G con respecto a N .

Definición 1.5. Grupo factor

Si N es un subgrupo normal de G , el grupo de las clases laterales de N bajo la operación binaria inducida es el grupo factor de G módulo N y se denota por G/N . Las clases laterales son las clases residuales de G módulo N .

Teorema 1.2. Lagrange

Sean G un grupo finito y H un subgrupo de G . Entonces $|H|$ divide a $|G|$ y el cociente $\frac{|G|}{|H|}$ es el número de clases laterales izquierdas de H en G .

La prueba del Teorema 1.2 se deduce de una aplicación del Teorema 1.1.

Definición 1.6. Grupo soluble

Un grupo G se dice que es soluble si es posible encontrar una cadena finita de subgrupos $G = H_0 \supset H_1 \supset H_2 \supset \cdots \supset H_n = \{1\}$ donde cada H_i sea un subgrupo normal de H_{i-1} y cada grupo factor H_{i-1}/H_i es abeliano.

El Teorema de Feit y Thompson (ver [13]) prueba que todo grupo finito G de orden impar es soluble.

Lema 1.1. Sea G un grupo. Para todo subconjunto X de G y toda $g \in G$ se tiene que

$$|X| = |gX|.$$

Demostración. Defínase la aplicación φ como sigue,

$$\begin{aligned} \varphi : X &\longrightarrow gX \\ x &\longrightarrow \varphi(x) = gx. \end{aligned}$$

Sean $x, y \in X$ y supóngase que $\varphi(x) = \varphi(y)$, luego $gx = gy$, dado que $g \in G$ existe $g^{-1} \in G$ tales que $gg^{-1} = g^{-1}g = 1$, así que $x = y$, esto es, φ es inyectivo. Sea $y \in gX$, entonces existe $x \in X$ tales que $y = gx$, luego $g^{-1}y \in X$, entonces $\varphi(g^{-1}y) = y$, de aquí que φ es sobre. Ahora, como φ es inyectivo y sobre, entonces φ es biyectivo. Por lo tanto,

$$|X| = |gX|. \quad \square$$

Definición 1.7. Complemento de conjuntos

Dados dos conjuntos A y B de un grupo G , el complemento de A relativamente a B , designado por $B \setminus A$, se define como el conjunto: $B \setminus A = \{x \in B : x \notin A\}$.

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 $x - 1 < \xi \leq x$.

Con base en la función techo se define ahora la función $\kappa_G(r, s)$.

Definición 1.9. Función $\kappa_G(r, s)$

Sean G un grupo y r, s enteros positivos tales que $r, s \leq |G|$. Con $\kappa_G(r, s)$ se define el siguiente número entero

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

donde $\mathcal{H}(G) = \{h : h \text{ es el orden de un subgrupo finito de } G\}$.

Definición 1.10. Producto semidirecto

Sean K y H grupos y φ un homomorfismo de grupos de H en automorfismos de K dado por

$$\begin{aligned} \varphi : H &\longrightarrow \text{Aut}(K) \\ h &\longrightarrow \varphi(h) : K \longrightarrow K \\ &k \longrightarrow \varphi(h)(k). \end{aligned}$$

Se puede dar estructura de grupo al conjunto $K \times H$ definiendo la siguiente operación binaria: $(k_1, h_1)(k_2, h_2) = (k_1\varphi(h_1)(k_2), h_1h_2)$. En efecto,

- **Asociativa.** Sean $(k_1, h_1), (k_2, h_2), (k_3, h_3) \in K \times H$, entonces

$$\begin{aligned} (k_1, h_1)[(k_2, h_2)(k_3, h_3)] &= (k_1, h_1)[k_2\varphi(h_2)(k_3), h_2h_3] \\ &= [k_1\varphi(h_1)(k_2\varphi(h_2)(k_3)), h_1(h_2h_3)] \\ &= [k_1\varphi(h_1)(k_2)\varphi(h_2)(k_3), (h_1h_2)h_3] \\ &= [k_1\varphi(h_1)(k_2), h_1h_2](k_3, h_3) \\ &= [(k_1, h_1)(k_2, h_2)](k_3, h_3). \end{aligned}$$

- **Identidad.** El elemento $(1,1)$ es la identidad, ya que si $(k, h) \in K \times H$ entonces

$$\begin{aligned}(1, 1)(k, h) &= (1\varphi(1)(k), 1h) = (1k, h) = (k, h) \\ (k, h)(1, 1) &= (k\varphi(h)(1), h1) = (k1, h) = (k, h).\end{aligned}$$

- **Inverso.** Sea $(k, h) \in K \times H$, entonces $(k, h)^{-1} = (\varphi(h^{-1})(k^{-1}), h^{-1})$. En efecto,

$$\begin{aligned}(k, h)(\varphi(h^{-1})(k^{-1}), h^{-1}) &= (k\varphi(h)(\varphi(h^{-1})(k^{-1})), hh^{-1}) \\ &= (k\varphi(h)\varphi(h^{-1})(k^{-1}), 1) = (k\varphi(h)\varphi^{-1}(h)(k^{-1}), 1) \\ &= (ki(k^{-1}), 1) = (kk^{-1}, 1) = (1, 1).\end{aligned}$$

De forma similar,

$$\begin{aligned}(\varphi(h^{-1})(k^{-1}), h^{-1})(k, h) &= (\varphi(h^{-1})(k^{-1})\varphi(h^{-1})(k), h^{-1}h) \\ &= (\varphi^{-1}(h^{-1})(k)\varphi(h^{-1})(k), 1) = (1, 1).\end{aligned}$$

Por lo tanto, $K \times H$ con la operación definida arriba es un grupo denominado el producto semidirecto de K por H y denotado con $K \rtimes H$.

Ejemplo 1.1. Sean p y q dos enteros primos impares tales que $q \equiv 1 \pmod{p}$. El grupo multiplicativo $\mathbb{Z}_q^*$ del campo $\mathbb{Z}_q$ es de orden $q - 1$, luego existe $\alpha \in \mathbb{Z}_q^*$ tal que $\alpha^p = 1$. Entonces la aplicación φ dada por

$$\begin{aligned}\varphi : \mathbb{Z}_p &\longrightarrow \text{Aut}(\mathbb{Z}_q) \\ b &\longrightarrow \varphi(b) : \mathbb{Z}_q \longrightarrow \mathbb{Z}_q \\ &x \longrightarrow \varphi(b)(x) = x\alpha^b,\end{aligned}$$

es un homomorfismo de grupos de $\mathbb{Z}_p$ en automorfismo de $\mathbb{Z}_q$.

Demostración. Dado que $\mathbb{Z}_q$ es un campo y $q \equiv 1 \pmod{p}$, entonces existe $\alpha \in \mathbb{Z}_q^*$ tal que $\alpha^p = 1$, esto porque $p|q - 1$. Se probará primero que la aplicación φ está bien definida. En efecto, sean a, b dos elementos de una misma clase lateral en $\mathbb{Z}_p$, entonces $p|a - b$, luego existe $k \in \mathbb{Z}$ tal que $a - b = pk$, se sigue que $a = pk + b$. Entonces para todo $x \in \mathbb{Z}_q$ se tiene,

$$\varphi(a)(x) = x\alpha^a = x\alpha^{pk+b} = x\alpha^{pk}\alpha^b = x(\alpha^p)^k\alpha^b = x1\alpha^b = x\alpha^b = \varphi(b)(x).$$

Se sigue que $\varphi(a) = \varphi(b)$, esto es, φ esta bien definida. En segundo lugar se probará que φ es un homomorfismo. Sean $a, b \in \mathbb{Z}_p$, entonces para todo $x \in \mathbb{Z}_q$,

$$\varphi(a+b)(x) = x\alpha^{a+b} = x\alpha^{b+a} = \varphi(a)(x\alpha^b) = \varphi(a)\varphi(b)(x).$$

Finalmente se debe probar que $\varphi(b)$ es un isomorfismo. En efecto, sean $x, y \in \mathbb{Z}_q$, entonces,

- **Inyectivo.** $\varphi(b)$ es inyectivo si y sólo si $\ker(\varphi(b)) = 0$. Sea $x \in \ker(\varphi(b))$, entonces $\varphi(b)(x) = x\alpha^b = 0$. Dado que $\alpha^b \neq 0$ se tiene que $x = 0$. Por lo tanto, $\varphi(b)$ es inyectivo.
- **Sobreyectivo.** Dado que $\mathbb{Z}_q$ es finito, se sigue que $\varphi(b)$ es sobre.
- **Estructura.** Sean $x, y \in \mathbb{Z}_q$, entonces

$$\varphi(b)(x+y) = (x+y)\alpha^b = x\alpha^b + y\alpha^b = \varphi(b)(x) + \varphi(b)(y).$$

Por los tres items anteriores, la aplicación $\varphi(b)$ es un isomorfismo.

Por lo tanto, el conjunto formado por $G = \mathbb{Z}_q \rtimes \mathbb{Z}_p = \{(x, y) : x \in \mathbb{Z}_q \text{ y } y \in \mathbb{Z}_p\}$ tiene estructura de grupo respecto a la operación binaria $(a, b)(c, d) = (a + c\alpha^b, b + d)$, denominado el producto semidirecto de $\mathbb{Z}_q$ por $\mathbb{Z}_p$. $\square$

Observación 1.1. El tercer Teorema de Sylow garantiza que el número n de subgrupos en $G = \mathbb{Z}_q \rtimes \mathbb{Z}_p$ de orden q es $n \equiv 1 \pmod{q}$ y divide a pq . Luego el número n de subgrupos de orden q es de la forma $n = qk + 1$ y divide a p , esto porque n no divide a q . Se deduce entonces que $n = 1$ o $n = p$, pero $p \not\equiv 1 \pmod{q}$, así que necesariamente $n = 1$. Por lo tanto, el número de subgrupos de orden q en G es 1.

Lema 1.2. Sean p y q dos enteros primos impares tales que $q \equiv 1 \pmod{p}$. Si $H_q = \mathbb{Z}_q \times \{0\} = \{(x, 0) : x \in \mathbb{Z}_q\}$ y $N_1 = \{0\} \times \mathbb{Z}_p = \{(0, y) : y \in \mathbb{Z}_p\}$, entonces las aplicaciones

$$\begin{aligned} \phi : \mathbb{Z}_q &\longrightarrow H_q & \psi : \mathbb{Z}_p &\longrightarrow N_1 \\ x &\longrightarrow \phi(x) = (x, 0) & y &\longrightarrow \psi(y) = (0, y) \end{aligned}$$

son isomorfismos y $G = H_q \rtimes N_1$. Además los subconjuntos H_q y N_1 son subgrupos del grupo $G = \mathbb{Z}_q \rtimes \mathbb{Z}_p$ y $H_q \triangleleft G$.

Demostración. Se probará que ϕ es un isomorfismo.

- **Inyectivo.** Sean $x, y \in \mathbb{Z}_q$ tales que $\phi(x) = \phi(y)$, entonces $(x, 0) = (y, 0)$, esto implica que $x = y$.
- **Sobreyectivo.** Sea $(x, 0) \in H_q$, entonces $x \in \mathbb{Z}_q$, luego se tiene que $\phi(x) = (x, 0)$.
- **Estructura.** Sean $x, y \in \mathbb{Z}_q$, entonces $\phi(x + y) = (x + y, 0)$, además, observe que $\phi(x)\phi(y) = (x, 0)(y, 0) = (x + y\alpha^0, 0 + 0) = (x + y, 0)$. Por tanto, $\phi(x + y) = \phi(x)\phi(y)$.

En conclusión, $\mathbb{Z}_q$ bajo la suma es isomorfo a H_q bajo el producto $\times$. De forma similar se puede probar que ψ es un isomorfismo de grupos. Además, claramente H_q y N_1 son subgrupos de G , y para todo $(x, y) \in G$ y todo $(z, 0) \in H_q$ se tiene que $(-x\alpha^b, -y)(z, 0)(x, y) \in H_q$. $\square$

1.2. El Problema de los Conjuntos Suma Pequeños

La Teoría Aditiva de Números es una rama de las matemáticas que en general se interesa por el estudio de las sumas de subconjuntos de números enteros. Sea $k \geq 2$, y sean $A_1, A_2, \dots, A_k$ conjuntos de enteros. El conjunto suma $A_1 + A_2 + \dots + A_k$, es el conjunto de todos los enteros de la forma $a_1 + a_2 + \dots + a_k$, donde $a_i \in A_i$ para toda $i = 1, 2, \dots, k$. Los conjuntos suma también se pueden definir en cualquier grupo abeliano y, en verdad, en cualquier conjunto donde se haya definido una operación binaria.

A continuación se da la definición general de conjunto suma en un grupo arbitrario G , para conjuntos suma de dos sumandos.

Definición 1.11. Conjunto suma

Sea G un grupo y sean A y B dos subconjuntos de G , no vacíos. El conjunto suma de A y B , denotado por AB , es el conjunto de todos los elementos en G que se pueden expresar como ab , donde $a \in A$ y $b \in B$. Es decir,

$$AB = \{ab : a \in A, b \in B\}.$$

Si $A = \emptyset$ o $B = \emptyset$, se define $AB = \emptyset$.

Dado un subconjunto X de un grupo G , se designa $X^{-1} = \{x^{-1} : x \in X\}$.

Lema 1.3. *Si A y B son dos subconjuntos no vacíos de un grupo G . Entonces se cumple que*

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

Demostración. Considérese $Z = \{x \in G : A \cap xB^{-1} \neq \emptyset\}$. Se probará que $Z = AB$. Sea $z \in Z$, entonces $A \cap zB^{-1} \neq \emptyset$, luego existe $y \in A \cap zB^{-1}$, se sigue que $y \in A$ y $y \in zB^{-1}$, esto es, $y = zb^{-1}$ para algún $b \in B$. De la última ecuación se tiene $z = yb$, lo que significa que $z = yb \in AB$, es decir $Z \subset AB$. Por otro lado, sea $z \in AB$, luego existen $a \in A$ y $b \in B$ tal que $z = ab$, de aquí $a = zb^{-1} \in zB^{-1}$, esto es $z \in Z$. Se concluye que $AB \subset Z$. Por lo probado anteriormente se tiene $Z = AB$. $\square$

Del Lema 1.3 se tiene que

$$G \setminus AB = \{x \in G : A \cap xB^{-1} = \emptyset\}.$$

Los problemas de interés en Teoría Aditiva de Números se pueden clasificar en dos grandes grupos:

Los problemas directos: Dados 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 $|AB|$ en términos de $|A| = r$ y $|B| = s$.

Los problemas inversos: Dado un grupo G , la problemática general, de los problemas inversos, consiste en describir la estructura de los pares de subconjuntos no vacíos A y B de G para los cuales $|AB|$ es pequeño. Por ejemplo, el teorema de Vosper es uno de los resultados obtenidos dentro de los problemas inversos en Teoría Aditiva de Números.

Sean G un grupo y r, s enteros positivos que satisfacen $r, s \leq |G|$. Dentro de los problemas directos en Teoría Aditiva de Números, se encuentra **El Problema de los Conjuntos Suma Pequeños**, el cual consiste en minimizar el cardinal de $|AB|$, sujeto a las condiciones $A, B \subset G$, $|A| = r$ y $|B| = s$. El Problema de los Conjuntos Suma Pequeños, de acuerdo a Eliahou y Kervaire en [9], también se puede enunciar de la siguiente manera:

Definición 1.12. La función $\mu_G(r, s)$

Sean G un grupo y r, s enteros positivos tales que $r, s \leq |G|$. Con $\mu_G(r, s)$ se define el mínimo de los cardinales $|AB|$, donde A y B son subconjuntos del grupo G con cardinales r y s respectivamente, es decir,

$$\mu_G(r, s) = \min \left\{ |AB| : A \in \binom{G}{r}, B \in \binom{G}{s} \right\},$$

donde $\binom{G}{t} = \{X \subset G : |X| = t\}$. Además, se dice que los subconjuntos A y B de G realizan $\mu_G(r, s)$ si $|A| = r$, $|B| = s$ y $|AB| = \mu_G(r, s)$.

Por lo tanto, el problema de los conjuntos suma pequeños, consiste en hallar el valor de la función $\mu_G(r, s)$, para enteros r, s tales que $r, s \in [1, |G|]$. Evaluar directamente el valor de $\mu_G(r, s)$ es un proceso complicado debido al gran número de operaciones que se deben realizar, en verdad no existe un algoritmo en tiempo polinomial que permita calcular los valores de la función $\mu_G(r, s)$, por tal motivo, adquiere importancia la búsqueda de una fórmula explícita que facilite su cálculo.

Se presenta en la Proposición 1.1 y el Lema 1.4 algunas propiedades de la función $\mu_G(r, s)$.

Proposición 1.1. *Sean G un grupo finito 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 .*

La prueba de éste resultado se puede consultar en [7] Sección 5.

Lema 1.4. Propiedades de $\mu_G(r, s)$

Sean G un grupo finito y r, s enteros tales que $1 \leq r, s \leq |G|$. Entonces

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

La prueba del Lema 1.4 aparece en [10] como Lema 2.1, Teorema 4.1, Teorema 4.2 y Teorema 4.6 respectivamente.

Históricamente el primer resultado que se puede enmarcar dentro del *Problema de los Conjuntos Suma Pequeños*, es el Teorema de Cauchy–Davenport, probado por Cauchy en 1913 en [3] y redescubierto en forma independiente por Davenport en 1935 en [6].

Teorema 1.3. Cauchy–Davenport

Sea p un número primo, y sean A y B subconjuntos no vacíos de $\mathbb{Z}_p$. Entonces

$$|A + B| \geq \min\{p, |A| + |B| - 1\}. \quad (1.2.1)$$

Como se puede observar, el Teorema de Cauchy–Davenport da una cota inferior para $|A + B|$, donde A y B son subconjuntos no vacíos del grupo $G = \mathbb{Z}_p$. Véase la prueba del Teorema 1.3 en ([18], Teorema 2.2 pág. 44).

Una aplicación inmediata del Teorema de Cauchy–Davenport al *Problema de los Conjuntos Suma Pequeños* es el siguiente enunciado:

Teorema 1.4. 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

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

Demostración. Se deben probar dos desigualdades, en primer lugar considérese la desigualdad $\mu_G(r, s) \leq \min\{p, r + s - 1\}$. Sean los subconjuntos $A = \{0, 1, \dots, r - 1\}$ y $B = \{0, 1, \dots, s - 1\}$ del grupo G . Entonces $A + B = \{0, 1, \dots, r + s - 2\}$, luego por definición de $\mu_G(r, s)$ se tiene que

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

Si $|A| + |B| - 1 = r + s - 1 \geq p$, entonces $A + B = G$ y se cumple

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

Si $|A| + |B| - 1 = r + s - 1 < p$, entonces

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

Por lo tanto, en cualquiera de los casos se obtiene $\mu_G(r, s) \leq r + s - 1$. Ahora, la desigualdad $\mu_G(r, s) \geq \min\{p, r + s - 1\}$ es consecuencia inmediata del teorema de Cauchy–Davenport. $\square$

Definición 1.13. Propiedad del conjunto suma pequeño

Se dice que un grupo G tiene la propiedad del conjunto suma pequeño si, para todo par de enteros positivos r, s tales que $r, s \leq |G|$, existen subconjuntos $A, B \subset G$ de cardinales $|A| = r$ y $|B| = s$ que satisfacen $|AB| \leq |A| + |B| - 1$.

La propiedad del conjunto suma pequeño para G , es equivalente a la validez de la fórmula $\mu_G(r, s) \leq r + s - 1$, para todo par de enteros r, s tales que $1 \leq r, s \leq |G|$.

El Teorema de Vosper que data del año 1956 especifica la estructura de los conjuntos que satisfacen la igualdad en el Teorema de Cauchy-Davenport, es decir, en el caso que se cumpla la igualdad de la ecuación (1.2.1).

Teorema 1.5. Vosper

Sea p un número primo, A y B dos subconjuntos de $\mathbb{Z}_p$ que contienen al menos dos elementos y tales que $|A + B| < p - 1$. Si $|A + B| = |A| + |B| - 1$, entonces A y B son progresiones aritméticas con la misma diferencia.

En ([18], Teorema 2.7 pág. 52-55) se presenta una demostración del Teorema 1.5.

Definición 1.14. Estabilizador de un conjunto

Sea A un subconjunto no vacío de un grupo abeliano G . El estabilizador de A es el conjunto

$$H(A) = \{g \in G : g + A = A\},$$

y se dice que A es un conjunto periódico si $H(A) \neq 0$, esto es, si el conjunto $H(A)$ no se reduce al conjunto $\{0\}$. En este caso $H(A)$ es el periodo de A .

El siguiente teorema debido a Kneser es una herramienta importante en Teoría Aditiva de Números. Entre las diferentes formulaciones que existen del Teorema de Kneser (ver [4, 18]), en este trabajo se tendrá en cuenta la dada en el Teorema 1.6, lo que puede ser interpretado como una caracterización de los pares de subconjuntos cuyo conjunto suma es pequeño.

Teorema 1.6. Kneser

Sea G un grupo abeliano y sean A y B dos subconjuntos finitos no vacíos de G . Si $|A + B| < |A| + |B| - 1$, entonces existe un subgrupo propio H de G tal que

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

Un método desarrollado por Hamidoune en [14, 15], denominado el *método isoperimétrico* ha permitido nuevas pruebas y generalizaciones de los teoremas clásicos de la teoría aditiva de números. Por ejemplo, una variante del *método isoperimétrico* ha dado una nueva prueba del Teorema 1.6 (ver [4]). El teorema de Kneser permite extender el teorema de Cauchy a grupos abelianos arbitrarios. De hecho el Teorema de Kneser implica el Teorema de Cauchy–Davenport, pues en el grupo cíclico $G = \mathbb{Z}_p$, con p primo, el único subconjunto periódico no vacío de G es el mismo G .

El Teorema de Cauchy–Davenport da una fórmula explícita para $\mu_G(r, s)$ en grupos abelianos de la forma $G = \mathbb{Z}_p$, p primo. Posteriormente se desarrollaron diversos trabajos especialmente por Bollobás, Eliahou, Kervaire y Plagne encaminados a modelar la función $\mu_G(r, s)$. En 2003, Plagne en [1] obtuvo un resultado muy relevante, cuando prueba que en el grupo cíclico $G = \mathbb{Z}_n$ de orden n se satisface la siguiente fórmula:

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

Eliahou, Kervaire y Plagne en [7] usando el Teorema de Kneser extendieron este resultado a la clase de grupos abelianos finitos, en verdad ellos probaron el siguiente teorema.

Teorema 1.7. *Sean G un grupo abeliano finito de orden n y r, s enteros que satisfacen $1 \leq r, s \leq n$, entonces se cumple que*

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

En 2005, Eliahou y Kervaire en [8], y posteriormente Plagne en 2007 en [2], trabajando en forma independiente lograron determinar una fórmula explícita para la función $\mu_G(r, s)$ donde G es un grupo abeliano arbitrario (no necesariamente finito) en términos de la función

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

El resultado que ellos probaron se enuncia en el siguiente teorema.

Teorema 1.8. *Si G un grupo abeliano arbitrario entonces*

$$\mu_G(r, s) = \kappa_G(r, s), \tag{1.2.2}$$

para todo par de enteros positivos $r, s \leq |G|$.

Este resultado soluciona completamente *El Problema de los Conjuntos Suma Pequeños* en grupos abelianos, pero en grupos no abelianos aún no se tiene una solución. Sin embargo, se han incrementado algunas clases específicas de grupos finitos no conmutativos para los cuales la ecuación (1.2.2) se cumple. En 2010, Elihaou y Kervaire en [12] prueban que la fórmula para $\mu_G(r, s)$ obtenida en el caso en que G es un grupo abeliano se cumple para todo grupo diédrico $G = D_n$ de orden $2n$. El resultado que ellos obtuvieron se enuncia como sigue:

Teorema 1.9. *En el grupo diédrico $G = D_n$ de orden $2n$ se tiene que $\mu_G(r, s) = \kappa_G(r, s)$ para todo par de enteros positivos $r, s \leq |G|$ y todo $n \geq 1$.*

Para el caso $G = D_n$, el conjunto de órdenes de los subgrupos es exactamente el mismo que el conjunto de divisores de $|D_n| = 2n$ (ver [9]).

Un resultado obtenido recientemente para grupos finitos no abelianos de la forma $\mathcal{Q} \times (\mathbb{Z}/2\mathbb{Z})^k \times \mathcal{C}$ con $\mathcal{C}$ un grupo cíclico de orden impar y $k \in \mathbb{Z}^+$, es el dado por los autores de [17]. El resultado que ellos probaron se enuncia en el siguiente teorema.

Teorema 1.10. *Sea k un entero no negativo. En el grupo $H = \mathcal{Q} \times (\mathbb{Z}/2\mathbb{Z})^k \times \mathcal{C}$, con $\mathcal{C} = \langle g \rangle$ 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 tales que $1 \leq r, s \leq |H|$.*

Capítulo 2

Herramientas Aditivas

En todo este capítulo se considera un grupo G y un subconjunto B de G . En la primera sección se da a conocer la teoría de la función P_B , sus propiedades y el conjunto de imágenes C_B de esta función. Posteriormente se introduce la noción de dualidad aditiva D_B , concepto que hace referencia al Teorema de Vosper. Finalmente se definen los conceptos de secuencia de números isoperimétricos, k -celda, k -núcleo y se exponen tres desigualdades fundamentales en términos de la función Φ_B . Estas desigualdades y su relación con las k -celdas constituyen la base del nuevo enfoque isoperimétrico desarrollado por Balandraud en [4, 5]. El propósito de este capítulo es dar a conocer las nuevas herramientas aditivas desarrolladas por Balandraud en [5] adaptadas a lo que él llama, el nuevo enfoque del método isoperimétrico.

2.1. La Aplicación P_B y sus Propiedades

Por cuestión de notación, el conjunto $G \setminus ((G \setminus (XB))B^{-1})$ se denotará mediante la expresión $G \setminus (G \setminus XB)B^{-1}$, con el fin de evitar confusiones en las pruebas debido al gran número de paréntesis que se utilizan.

Definición 2.1. Conjunto potencia

Sea G un grupo, se define el conjunto potencia de G , denotado con $\mathcal{P}(G)$, como la familia de todos sus posibles subconjuntos, esto es: $\mathcal{P}(G) = \{X : X \subset G\}$.

Es conocido que si un conjunto Z tiene n elementos entonces $\mathcal{P}(Z)$ tiene 2^n elementos.

Definición 2.2. La función P_B

Sean G un grupo y B un subconjunto de G . Para todo subconjunto X de G , se define la función P_B como sigue:

$$\begin{aligned} P_B : \mathcal{P}(G) &\longrightarrow \mathcal{P}(G) \\ X &\longrightarrow P_B(X) = G \setminus (G \setminus XB)B^{-1}. \end{aligned}$$

Ejemplo 2.1. Considérese el grupo $G = \mathbb{Z}_5$ y los subconjuntos $B = \{2, 3\}$ y $X = \{1, 4\}$. Luego se tiene $XB = \{1, 2, 3, 4\}$, y como $2^{-1} = 3$ y $3^{-1} = 2$ entonces $B = B^{-1}$. Por lo tanto el conjunto $P_B(X)$ es:

$$P_B(X) = \mathbb{Z}_5 \setminus (\mathbb{Z}_5 \setminus \{1, 2, 3, 4\})\{2, 3\} = \mathbb{Z}_5 \setminus \{0\}\{2, 3\} = \mathbb{Z}_5 \setminus \{2, 3\} = \{0, 1, 4\}.$$

Aunque en el Ejemplo 2.1 se utiliza la notación multiplicativa, debe ser claro que la operación definida en G es la suma módulo 5.

El estudio de esta función permite observar que para un subconjunto dado X , el conjunto $P_B(X)$ está caracterizado, en el sentido de la equivalencia de (2.1.3), por el producto XB . Entre las propiedades de la función P_B se tienen:

Lema 2.1. Para todo subconjunto X de un grupo G se tiene que

$$X \subset P_B(X). \quad (2.1.1)$$

Demostración. Suponga por contradicción que $x \in X \setminus P_B(X)$, es decir, $x \in X$ y $x \notin P_B(X)$. Luego existen $x' \in G \setminus XB$ y $b \in B$ tales que $x = x'b^{-1}$, entonces $x' = xb$, así, $x' \in XB$, pero esto contradice el hecho que $x' \in G \setminus XB$. Por lo tanto $X \subset P_B(X)$. $\square$

Proposición 2.1. Para todo subconjunto X de G se cumple la ecuación

$$XB = P_B(X)B. \quad (2.1.2)$$

Demostración. ■ Se probará la contención $XB \subset P_B(X)B$, sea $y = xb \in XB$ para algún $x \in X$ y $b \in B$. Por Lema 2.1, $X \subset P_B(X)$ así que $x \in P_B(X)$, luego se tiene $y = xb \in P_B(X)B$, lo que significa que $XB \subset P_B(X)B$.

- Ahora, para probar la contención $P_B(X)B \subset XB$, sea $y \in P_B(X)B \setminus XB$, entonces existen $z \in P_B(X)$ y $b \in B$ tales que $y = zb$, pero $y \notin XB$, luego $y \in G \setminus XB$. Esto implica que $yb^{-1} = z \in (G \setminus XB)B^{-1}$, equivalentemente, $z = yb^{-1} \in (P_B(X))^c$ (complemento de $P_B(X)$), lo cual es una contradicción. Por consiguiente se tiene que $P_B(X)B \subset XB$. Finalmente por los dos items anteriores,

$$XB = P_B(X)B. \quad \square$$

Corolario 2.1. *La aplicación P_B verifica que $P_B^2 = P_B$.*

Demostración. Sea X un subconjunto de un grupo G , entonces

$$\begin{aligned} P_B^2(X) &= P_B(P_B(X)) \\ &= G \setminus (G \setminus P_B(X)B)B^{-1} \\ &= G \setminus (G \setminus XB)B^{-1} \\ &= P_B(X). \end{aligned}$$

Por lo tanto, $P_B^2 = P_B$. □

Corolario 2.2. *Para todo par de subconjuntos X y Y de G se tiene que*

$$XB = YB \quad \text{si y sólo si} \quad P_B(X) = P_B(Y). \quad (2.1.3)$$

Demostración. Supóngase que $XB = YB$, entonces

$$\begin{aligned} G \setminus XB &= G \setminus YB \\ (G \setminus XB)B^{-1} &= (G \setminus YB)B^{-1} \\ G \setminus (G \setminus XB)B^{-1} &= G \setminus (G \setminus YB)B^{-1} \\ P_B(X) &= P_B(Y). \end{aligned}$$

Recíprocamente, si $P_B(X) = P_B(Y)$, por la Proposición 2.1, $XB = P_B(X)B$, luego

$$XB = P_B(X)B = P_B(Y)B = YB. \quad \square$$

Lema 2.2. Función P_B

Sean G un grupo y B un subconjunto de G . Para todo subconjunto X de G se tiene que

$$P_B(X) = \{z \in G : zB \subset XB\}.$$

Demostración. Sea $z \in A = \{g \in G : gB \subset XB\}$, luego $zB \subset XB$, entonces

$$\begin{aligned} G \setminus XB &\subset G \setminus zB \\ (G \setminus XB)B^{-1} &\subset (G \setminus zB)B^{-1} \\ G \setminus (G \setminus zB)B^{-1} &\subset P_B(X) \\ \{z\} &\subset P_B(\{z\}) \subset P_B(X) \\ A &\subset P_B(X). \end{aligned}$$

Por otro lado, sea $z \notin A$, entonces $zB \not\subset XB$, luego existe $b \in B$ tal que $zb \notin XB$, así que $zb \in G \setminus XB$, luego existe $b^{-1} \in B^{-1}$ y $(zb)b^{-1} \in (G \setminus XB)B^{-1}$, es decir, $z \in (P_B(X))^c$ entonces $z \notin P_B(X)$, esto es $P_B(X) \subset A$. En conclusión, $A = P_B(X)$. $\square$

Se denota ahora una cierta familia de subconjuntos dependiendo del conjunto B .

Notación 2.1. Sean G un grupo y B un subconjunto de G . Con C_B se denota a la colección de subconjuntos de G que son imagen bajo P_B de algún subconjunto de G , es decir,

$$C_B = P_B(\mathcal{P}(G)) = \{X \subset G : X = P_B(Y), \text{ para algún } Y \in \mathcal{P}(G)\}.$$

Los elementos de C_B serán llamados celdas para B (o celdas de B).

Estas celdas de acuerdo al Corolario 2.1 se pueden caracterizar como soluciones de la ecuación $P_B(X) = X$. Observe que los conjuntos $\emptyset, G \in C_B$. En efecto,

$$\begin{aligned} P_B(\emptyset) &= G \setminus (G \setminus \emptyset B)B^{-1} & P_B(G) &= G \setminus (G \setminus GB)B^{-1} \\ &= G \setminus (G \setminus \emptyset)B^{-1} & &= G \setminus (G \setminus G)B^{-1} \\ &= G \setminus (GB^{-1}) & &= G \setminus (\emptyset B^{-1}) \\ &= G \setminus G & &= G \setminus \emptyset \\ &= \emptyset & &= G. \end{aligned}$$

El conjunto C_B tiene algunas propiedades interesantes que se mencionan a continuación.

Proposición 2.2. Para todo $X \subset G$ y todo $g \in G$, se tiene que $P_B(gX) = gP_B(X)$. Se deduce de aquí que el conjunto C_B es estable por traslación sobre la izquierda.

Demostración. Se debe probar que

$$P_B(gX) = G \setminus (G \setminus (gX)B)B^{-1} = g(G \setminus (G \setminus XB)B^{-1}) = gP_B(X).$$

Por la asociatividad en G , para todo $X \subset G$ y todo $g \in G$, se tiene que $(gX)B = g(XB)$. Además, $G \setminus gX = g(G \setminus X)$, en efecto, sea $z \in g(G \setminus X)$, entonces existe $y \in G \setminus X$ tal que $z = gy$, luego $y \neq x$ para todo $x \in X$, se sigue que $z = gy \neq gx$, es decir, $z \in G \setminus gX$. En caso contrario, si $z = gy = gx$, entonces $x = y$, lo cual contradice que $y \neq x$. Por otro lado, sea $z \in G \setminus gX$, entonces $z \in G$ y $z \neq gx$ para todo $x \in X$, luego $g^{-1}z \neq x$, se sigue que $g^{-1}z \in G \setminus X$, entonces $g(g^{-1}z) = (gg^{-1})z = z \in g(G \setminus X)$. Por lo tanto,

$$\begin{aligned} P_B(gX) &= G \setminus (G \setminus (gX)B)B^{-1} \\ &= G \setminus g(G \setminus XB)B^{-1} \\ &= g(G \setminus (G \setminus XB)B^{-1}) \\ &= gP_B(X). \end{aligned} \quad \square$$

Proposición 2.3. *La aplicación P_B es creciente, es decir, para todo par de subconjuntos X y Y de G , si $X \subset Y$ entonces $P_B(X) \subset P_B(Y)$.*

Demostración. Sean X y Y dos subconjuntos de un grupo G tales que $X \subset Y$, entonces

$$\begin{aligned} XB &\subset YB \\ G \setminus XB &\supset G \setminus YB \\ (G \setminus XB)B^{-1} &\supset (G \setminus YB)B^{-1} \\ G \setminus (G \setminus XB)B^{-1} &\subset G \setminus (G \setminus YB)B^{-1} \\ P_B(X) &\subset P_B(Y). \end{aligned}$$

Por lo tanto, la función P_B es creciente. □

Corolario 2.3. *El conjunto C_B es cerrado por intersección, es decir, si C_1 y C_2 son elementos de C_B , entonces $C_1 \cap C_2 \in C_B$.*

Demostración. Dado que $C_1, C_2 \in C_B$ entonces existen subconjuntos X_1, X_2 de G tales que $C_1 = P_B(X_1)$ y $C_2 = P_B(X_2)$. Sea $Z = C_1 \cap C_2$, luego $Z \subset C_1$ y $Z \subset C_2$.

Ahora, por la Proposición 2.3 $P_B(Z) \subset P_B(C_1)$ y $P_B(Z) \subset P_B(C_2)$, además, por el Corolario 2.1 se tiene

$$P_B(C_1) = P_B(P_B(X_1)) = P_B^2(X_1) = P_B(X_1) = C_1$$

y

$$P_B(C_2) = P_B(P_B(X_2)) = P_B^2(X_2) = P_B(X_2) = C_2,$$

entonces $P_B(Z) \subset C_1$ y $P_B(Z) \subset C_2$, así que $P_B(Z) \subset C_1 \cap C_2 = Z$. Por Lema 2.1, $Z \subset P_B(Z)$, así que $P_B(Z) = Z = C_1 \cap C_2$. Por lo tanto, $C_1 \cap C_2 \in C_B$. $\square$

2.2. Dualidad Aditiva $D_B : X \longrightarrow G \setminus XB$

La noción de dualidad aditiva de acuerdo a Balandraud en [4] es que $|D_B(X)| \geq 2$. Se puede notar así que en el Teorema de Vosper aparece implícita la noción de dualidad aditiva, ya que $|A + B| < p - 1$ es equivalente a $|D_B(X)| \geq 2$, es por eso que en la hipótesis del Teorema 1.5, $|A| \geq 2$ y $|D_B(X)| \geq 2$.

Definición 2.3. La función D_B

Sean G un grupo y B un subconjunto de G . Para cualquier subconjunto X en G , se define la aplicación D_B de la siguiente manera:

$$\begin{aligned} D_B : \mathcal{P}(G) &\longrightarrow \mathcal{P}(G) \\ X &\longrightarrow D_B(X) = G \setminus XB. \end{aligned}$$

Observe que para todo subconjunto X de G , se satisface la ecuación,

$$P_B(X) = D_{B^{-1}} \circ D_B(X).$$

En efecto,

$$\begin{aligned} D_{B^{-1}} \circ D_B(X) &= D_{B^{-1}}(D_B(X)) \\ &= D_{B^{-1}}(G \setminus XB) \\ &= G \setminus (G \setminus XB)B^{-1} \\ &= P_B(X). \end{aligned}$$

Por lo tanto, $P_B(X) = D_{B^{-1}} \circ D_B(X)$.

Lema 2.3. Si $X \subset G$ entonces se tiene que $D_B(X) = D_B(P_B(X))$.

Demostración. Naturalmente, utilizando la Proposición 2.1, para todo $X \subset G$, se tiene

$$\begin{aligned} D_B(X) &= G \setminus XB \\ &= G \setminus P_B(X)B \\ &= D_B(P_B(X)). \end{aligned} \quad \square$$

Proposición 2.4. La imagen de la función D_B es $C_{B^{-1}}$.

Demostración. El Lema 2.3 permite observar que para un subconjunto X de G , se tiene que $D_B(X) \in C_{B^{-1}}$, en efecto,

$$\begin{aligned} P_{B^{-1}}(D_B(X)) &= G \setminus [G \setminus D_B(X)B^{-1}]B \\ &= D_B([G \setminus D_B(X)B^{-1}]) \\ &= D_B([G \setminus (G \setminus XB)B^{-1}]) \\ &= D_B(P_B(X)) \\ &= G \setminus P_B(X)B \\ &= G \setminus XB \\ &= D_B(X). \end{aligned} \quad \square$$

Proposición 2.5. Para todo subconjunto X de G y todo $g \in G$ se cumple que

$$D_B(gX) = gD_B(X). \quad (2.2.1)$$

Demostración. La prueba de la Proposición 2.5 es consecuencia de la Proposición 2.2. □

Proposición 2.6. La función D_B es decreciente, es decir, para todo par de subconjuntos X y Y de G , si $X \subset Y$ entonces $D_B(Y) \subset D_B(X)$.

Demostración. En efecto, sean X y Y dos subconjuntos de G tales que $X \subset Y$, entonces

$$\begin{aligned} XB &\subset YB \\ (G \setminus XB) &\supset (G \setminus YB) \\ (G \setminus YB) &\subset (G \setminus XB) \\ D_B(Y) &\subset D_B(X). \end{aligned}$$

Se puede deducir entonces que la función D_B es decreciente. $\square$

Proposición 2.7. Si X y Y son dos subconjuntos de G entonces

$$P_B(X \cup Y) = D_{B^{-1}}(D_B(X) \cap D_B(Y)). \quad (2.2.2)$$

Demostración. Inicialmente se probará la igualdad

$$[(G \setminus XB) \cap (G \setminus YB)]B^{-1} = [G \setminus (X \cup Y)B]B^{-1}.$$

Note que para todo par de subconjuntos X y Y de G , se satisface la expresión

$$(X \cup Y)B = XB \cup YB.$$

En efecto, sea $z \in (X \cup Y)B$, luego existen $w \in (X \cup Y)$ y $b \in B$ tal que $z = wb$, entonces $z \in (XB \cup YB)$. De manera similar sea $z \in (XB \cup YB)$, entonces $z \in XB$ o $z \in YB$, luego existen $x \in X$ y $b \in B$ tal que $z = xb$ o existen $y \in Y$ y $b' \in B$ tal que $z = yb'$, esto es, existen $x, y \in X \cup Y$ y $b, b' \in B$ tal que $z = xb$ o $z = yb'$, es decir, $z \in (X \cup Y)B$. Por lo tanto,

$$(X \cup Y)B = XB \cup YB.$$

Luego se tiene,

$$\begin{aligned} D_B(X) \cap D_B(Y) &= (G \setminus XB) \cap (G \setminus YB) \\ &= (XB)^c \cap (YB)^c \\ &= (XB \cup YB)^c \\ &= G \setminus (XB \cup YB) \\ &= G \setminus (X \cup Y)B \\ &= D_B(X \cup Y). \end{aligned}$$

Multiplicando los dos términos de la ecuación anterior por B^{-1} se tiene,

$$[(G \setminus XB) \cap (G \setminus YB)]B^{-1} = [G \setminus (X \cup Y)B]B^{-1}. \quad (*)$$

Finalmente, aplicando complemento a los dos términos de (*) se tiene que,

$$G \setminus [G \setminus (X \cup Y)B]B^{-1} = G \setminus [(G \setminus XB) \cap (G \setminus YB)]B^{-1}.$$

Por lo tanto,

$$P_B(X \cup Y) = D_{B^{-1}}(D_B(X) \cap D_B(Y)). \quad \square$$

Proposición 2.8. *Si G es un grupo abeliano, para todo subconjunto X de G se cumple*

$$D_B(X^{-1}) = (D_{B^{-1}}(X))^{-1}.$$

Demostración. En efecto, para cualquier subconjunto X de G , $X^{-1}B^{-1} = (XB)^{-1}$, luego

$$\begin{aligned} (D_{B^{-1}}(X))^{-1} &= (G \setminus (XB^{-1}))^{-1} \\ &= G \setminus ((XB^{-1})^{-1}) \\ &= G \setminus (X^{-1}(B^{-1})^{-1}) \\ &= G \setminus (X^{-1}B) \\ &= D_B(X^{-1}). \end{aligned} \quad \square$$

Hasta el momento, ningún supuesto se ha hecho sobre las condiciones que debe cumplir el conjunto B . Si algunas suposiciones se hacen sobre B , se pueden deducir algunas propiedades adicionales interesantes.

Lema 2.4. *Si B es un subconjunto finito y no vacío de G , entonces la imagen de todo subconjunto finito X de G bajo P_B , es finita.*

Demostración. Si G es finito no hay nada que probar. Supóngase ahora que G es infinito, entonces para un subconjunto finito X de G , el conjunto XB también es finito, luego por la Proposición 2.1, $XB = P_B(X)B$, de aquí que $P_B(X)B$ es finito y por lo tanto la imagen $P_B(X)$ también lo es. $\square$

Proposición 2.9. Sean G un grupo y B un subconjunto no vacío y finito de G . Entonces D_B es una biyección del subconjunto de celdas finitas de C_B sobre el conjunto de celdas de complemento finito de $C_{B^{-1}}$.

Demostración. La Proposición 2.4 afirma que D_B es imagen de $C_{B^{-1}}$. Si C es una celda finita para B , entonces CB también es finito y por lo tanto $D_B(C) = G \setminus CB$ es de complemento finito. Además, si $D_B(C)$ es una celda de complemento finito para B^{-1} , entonces $D_B(C)B^{-1}$ también es de complemento finito y $C = P_B(C) = G \setminus D_B(C)B^{-1}$ es finito. $\square$

Lema 2.5. Si B un subconjunto de G tal que $1 \in B$. Entonces para todo subconjunto X de G , los tres conjuntos, X , $(XB \setminus X)$ y $D_B(X)$ forman una partición de G . Además, para toda celda C de B se cumple que

$$(CB) \setminus C = (D_B(C)B^{-1}) \setminus D_B(C). \quad (2.2.3)$$

Demostración. Se debe probar que los conjuntos X , $(XB \setminus X)$ y $D_B(X)$ son disjuntos dos a dos. Dado que $1 \in B$ se tiene $X \subset XB$, luego $X \cap (XB \setminus X) = \emptyset$ y $X \cap D_B(X) = \emptyset$, además como XB es el complemento de $D_B(X)$, entonces $D_B(X) \cap (XB) = \emptyset$. Por lo tanto, los conjuntos X , $(XB \setminus X)$ y $D_B(X)$ forman una partición para el grupo G .

Se probará ahora la equivalencia de la ecuación (2.2.3).

Sea $z \in D_B(C)B^{-1} \setminus D_B(C)$, entonces $z \in D_B(C)B^{-1}$ y $z \notin D_B(C)$, luego existen $y \in D_B(C)$ y $b \in B$ tal que $z = yb^{-1}$, así que $y = zb \in G \setminus CB$, $y = zb \in G$ y $y = zb \notin CB$, de aquí que $z \notin C$. Pero $z \notin D_B(C)$, entonces $z \in (G \setminus CB)^c$, luego $z \in CB$ y $z \notin C$, esto es, $z \in CB \setminus C$. Por consiguiente se satisface la contención,

$$[D_B(C)B^{-1} \setminus D_B(C)] \subset (CB \setminus C).$$

Por otro lado, sea $z \in (CB \setminus C) \setminus [D_B(C)B^{-1} \setminus D_B(C)]$, entonces $z \in CB \setminus C$ y $z \notin D_B(C)B^{-1} \setminus D_B(C)$, es decir, $z \in CB$ y $z \in (D_B(C)B^{-1} \setminus D_B(C))^c$, luego $z \in CB$ y $z \in D_B(C)$, esto es, $z \in CB$ y $z \notin CB$, lo cual es una contradicción, entonces se debe tener

$$CB \setminus C \subset [D_B(C)B^{-1} \setminus D_B(C)].$$

Por lo tanto, se satisface la ecuación (2.2.3) $\square$

2.3. Ideas Isoperimétricas

En ésta sección se considera un grupo G y un subconjunto finito B de G tal que $1 \in B$.

Definición 2.4. Número isoperimétrico

Sean G un grupo y B un subconjunto de G tal que $1 \in B$. Para todo subconjunto finito X de G , se define el número isoperimétrico mediante la función Φ_B dada por

$$\begin{aligned} \Phi_B : \mathcal{P}_f(G) &\longrightarrow \mathbb{N} \\ X &\longrightarrow \Phi_B(X) = |XB| - |X|, \end{aligned} \tag{2.3.1}$$

donde $\mathcal{P}_f(G)$ denota los subconjuntos finitos X de G .

Lema 2.6. Sean G un grupo y B un subconjunto no vacío y finito de G . Para todo $g \in G$ se tiene que

$$\Phi_B = \Phi_{Bg}.$$

Demostración. En efecto, sean $g \in G$ y X un subconjunto finito de G . Defínase la aplicación φ como sigue

$$\begin{aligned} \varphi : XB &\longrightarrow X(Bg) \\ z &\longrightarrow \varphi(z) = x(bg). \end{aligned}$$

Por la asociatividad en G , $|X(Bg)| = |(XB)g|$, luego a la luz Lema 1.1 $|XB| = |(XB)g|$. Por lo tanto,

$$\Phi_B(X) = |XB| - |X| = |(XB)g| - |X| = \Phi_{Bg}(X). \quad \square$$

Observación 2.1. Observe que si $g = b^{-1}$, con $b \in B$, se puede considerar que $1 \in B$ sin pérdida de generalidad. De aquí que para todo subconjunto X de G , se tiene $X \subset XB$. Se concluye así que $\Phi_B(X) = |XB \setminus X|$.

En efecto, sea $x \in X$, luego $x = x \cdot 1 \in XB$. Por lo tanto $X \subset XB$ y se satisface la ecuación

$$\Phi_B(X) = |XB| - |X| = |XB \setminus X|.$$

Lema 2.7. Sean G un grupo y B un subconjunto no vacío y finito de G . Para todo $g \in G$ y todo subconjunto finito $X \subset G$ se cumple que

$$\Phi_B(X) = \Phi_B(Xg).$$

Demostración. Por Lema 2.6 se tiene que $|gX| = |X|$ y $|(gX)B| = |g(XB)| = |XB|$. Entonces,

$$\begin{aligned} \Phi_B(gX) &= |(gX)B| - |gX| \\ &= |g(XB)| - |gX| \\ &= |XB| - |X| \\ &= \Phi_B(X). \end{aligned} \quad \square$$

Proposición 2.10. Sean G un grupo y B un subconjunto no vacío y finito de G . Para todo subconjunto finito X de G se tiene

$$\Phi_B(P_B(X)) \leq \Phi_B(X).$$

Además, si $\Phi_B(P_B(X)) = \Phi_B(X)$ implica que $P_B(X) = X$, es decir, $X \in C_B$.

Demostración. En efecto, por Lema 2.1 y Proposición 2.1 se tiene

$$\begin{aligned} \Phi_B(P_B(X)) &= |(P_B(X)B)| - |P_B(X)| \\ &= |XB| - |P_B(X)| \\ &\leq |XB| - |X| \\ &= \Phi_B(X). \end{aligned}$$

Para el caso $\Phi(P_B(X)) = \Phi(X)$, naturalmente se obtiene $|P_B(X)| = |X|$, por Lema 2.1 $X \subset P_B(X)$ y como $P_B(X)$ es finito, entonces $P_B(X) = X$, es decir $X \in C_B$. $\square$

Proposición 2.11. Sean G un grupo y B un subconjunto finito de G tal que $1 \in B$. Para toda celda C de B que es finita o tiene complemento finito se cumple que

$$\Phi_B(C) = \Phi_{B^{-1}}(D_B(C)). \quad (2.3.2)$$

Demostración. Utilizando la ecuación (2.2.3) del Lema 2.5 se tiene

$$\begin{aligned} \Phi_B(C) &= |CB \setminus C| \\ &= |(G \setminus CB)B^{-1} \setminus (G \setminus CB)| \\ &= \Phi_{B^{-1}}(D_B(C)). \end{aligned} \quad \square$$

Estas propiedades permitirán limitar el estudio de los conjuntos suma pequeños a las celdas de B .

Teniendo en cuenta los trabajos [4, 5] de Balandraud, la función Φ_B puede ser extendida a todo subconjunto X de G . Por lo tanto, para B subconjunto finito de G tal que $1 \in B$, se considera la función Φ_B como sigue:

$$\begin{aligned}\Phi_B : \mathcal{P}(G) &\longrightarrow \mathbb{N} \cup \{\infty\} \\ X &\longrightarrow |XB \setminus X|.\end{aligned}$$

Se presentan ahora algunos conceptos relacionados con k -celdas y k -núcleos de acuerdo a los trabajos desarrollados por Balandraud en [4, 5].

Se denota con $C_B^0 = \{\emptyset, G\}$. Por lo estudiado en las Secciones 2.1 y 2.2 se tiene que $C_B^0 \subset C_B$. También se denota $\lambda_0(B) = 0 = \Phi_B(\emptyset) = \Phi_B(G)$. Además, cualquier elemento de C_B^0 se denomina una 0-celda. Se introduce ahora la definición de secuencia isoperimétrica, la cual utiliza las celdas que son finitas o tienen complemento finito, es decir, aquellas celdas C que satisfacen la condición que C sea finita o $G \setminus C = C^c$ sea finita. Se simboliza a esta clase específica de celdas con $C_{B,f}$.

Definición 2.5. Secuencia isoperimétrica

Se llama secuencia de números isoperimétricos, a la secuencia creciente (posiblemente finita) de valores tomados por la función Φ_B sobre el conjunto de celdas de $C_{B,f} \setminus C_B^0$, que son finitas o tienen complemento finito. Se denota esta secuencia con

$$\Phi_B(C_{B,f} \setminus C_B^0) = \{0 \leq \lambda_1(B) < \lambda_2(B) < \dots\}.$$

Observe que el primer valor de esta secuencia de valores puede ser expresado con

$$\lambda_1(B) = \min\{\Phi_B(X) = |XB \setminus X| : X \in C_{B,f} \setminus C_B^0\}.$$

Definición 2.6. k -Celda

Sea k un entero positivo y sea C una celda en $C_{B,f} \setminus C_B^0$, que es finita o tiene complemento finito. Se dice que C es una k -celda si $\Phi_B(C) = \lambda_k(B)$. El conjunto de las k -celdas se denota con C_B^k , es decir,

$$C_B^k = \{X \in C_{B,f} \setminus C_B^0 : \Phi_B(X) = \lambda_k(B)\}.$$

Por ejemplo, si $\lambda_1(B) = 0$, se tiene que

$$C_B^1 = (C_{B,f} \setminus C_B^0) \cap \Phi_B^{-1}(\lambda_1(B)).$$

Para todo entero $k > 1$ si $\lambda_1(B) \neq 0$, se cumple que

$$C_B^k = C_{B,f} \cap \Phi_B^{-1}(\lambda_k(B)), \text{ donde } \Phi_B^{-1}(\lambda_k(B)) = \{X \in \mathcal{P}_f(G) : \Phi_B(X) = \lambda_k(B)\}.$$

Si existen k -celdas finitas, las k -celdas de menor cardinal desarrollan un papel importante en este trabajo. Se presenta la Definición 2.7 para distinguirlas.

Definición 2.7. k -Núcleo

Sea k un entero positivo para el cual existe una k -celda finita. Se llama k -núcleo a toda k -celda de cardinal mínimo y se denota este cardinal con $\beta_k(B)$.

Observación 2.2. Sea k un entero positivo. Si existen k -celdas, por lo menos uno de los números enteros $\beta_k(B)$ y $\beta_k(B^{-1})$ existe. En efecto, si $\beta_k(B)$ no existe, todas las k -celdas C para B son infinitas, luego por la Definición 2.6, el conjunto $G \setminus C = C^c$ es finito. Ahora, puesto que $C \subset CB$, entonces $(G \setminus CB) \subset (G \setminus C)$, es decir el conjunto $D_B(C)$ es finito. Pero $D_B(C)$ es una k -celda para B^{-1} , por lo tanto $\beta_k(B^{-1})$ existe (es decir, $\beta_k(B^{-1})$ está bien definido).

Lema 2.8. Para todo entero positivo k tal que $\beta_k(B)$ y $\beta_k(B^{-1})$ existen se tiene que

$$\beta_k(B) + \lambda_k(B) + \beta_k(B^{-1}) \leq |G|.$$

Demostración. Si G es infinito, todos los términos del lado izquierdo son finitos, y así la desigualdad se cumple. Supóngase que G es finito, sea N_k un k -núcleo para B . Por la Proposición 2.11 el conjunto $D_B(N_k)$ es una k -celda para B^{-1} y como $\beta_k(B^{-1})$ es una k -celda de cardinalidad mínima se satisface la desigualdad $|D_B(N_k)| \geq \beta_k(B^{-1})$. Ahora, por Lema 2.5, los conjuntos N_k , $(N_k B \setminus N_k)$ y $D_B(N_k)$ forman una partición para el grupo G , entonces se tiene,

$$\begin{aligned} G &= N_k \cup (N_k B \setminus N_k) \cup D_B(N_k) \\ |G| &= |N_k \cup (N_k B \setminus N_k) \cup D_B(N_k)| \\ |G| &= |N_k| + |N_k B \setminus N_k| + |D_B(N_k)| \\ |G| &= \beta_k(B) + \lambda_k(B) + |D_B(N_k)| \\ |G| &\geq \beta_k(B) + \lambda_k(B) + \beta_k(B^{-1}). \end{aligned}$$

□

Finaliza este Capítulo presentando tres desigualdades fundamentales que serán de gran uso en lo que sigue.

Proposición 2.12. *Sean G un grupo y B un subconjunto finito de G tal que $1 \in B$. Para todo par de subconjuntos X y Y de G que son finitos o tienen complemento finito se cumple que*

$$\Phi_B(X \cap Y) + \Phi_B(X \cup Y) \leq \Phi_B(X) + \Phi_B(Y).$$

Demostración. Considérese el siguiente arreglo

$\cap$	Y	$YB \setminus Y$	$G \setminus YB$
X	R_{11}	R_{12}	R_{13}
$XB \setminus X$	R_{21}	R_{22}	R_{23}
$G \setminus XB$	R_{31}	R_{32}	R_{33}

Por Lema 2.5 los R_{ij} por filas o columnas son disjuntos ($i, j = 1, 2, 3$). Luego por la propiedad distributiva de operaciones de conjuntos se tiene que,

$$\begin{aligned} R_{12} \cup R_{22} \cup R_{32} &= [X \cap (YB \setminus Y)] \cup [(XB \setminus X) \cap (YB \setminus Y)] \cup [(G \setminus XB) \cap (YB \setminus Y)] \\ &= [(YB \setminus Y) \cap (X \cup (XB \setminus X))] \cup [(G \setminus XB) \cap (YB \setminus Y)] \\ &= [(YB \setminus Y) \cap (XB)] \cup [(G \setminus XB) \cap (YB \setminus Y)] \\ &= (YB \setminus Y) \cap (XB \cup (G \setminus XB)) \\ &= (YB \setminus Y) \cap G \\ &= YB \setminus Y, \end{aligned}$$

procediendo de manera similar (es suficiente con intercambiar los papeles del conjunto X por el conjunto Y) se obtiene

$$\begin{aligned} R_{21} \cup R_{22} \cup R_{23} &= [(XB \setminus X) \cap Y] \cup [(XB \setminus X) \cap (YB \setminus Y)] \cup [(XB \setminus X) \cap (G \setminus YB)] \\ &= XB \setminus X. \end{aligned}$$

Se probará ahora la siguiente igualdad:

$$R_{32} \cup R_{22} \cup R_{23} = (X \cup Y)B \setminus (X \cup Y).$$

Supóngase que $z \in R_{32} \cup R_{22} \cup R_{23}$, luego z esta en por lo menos uno de estos conjuntos. Si $z \in R_{23}$ entonces, $z \in (G \setminus YB) \cap (XB \setminus X)$. Luego

$$\begin{aligned}
(G \setminus YB) \cap (XB \setminus X) &= [G \cap (YB)^c] \cap [(XB) \cap X^c] \\
&= [G \cap XB] \cap [X^c \cap (YB)^c] \\
&= (XB) \cap [X^c \cap (YB)^c] \\
&\subset [(X \cup Y)B] \cap [X^c \cap (YB)^c], \text{ dado que } XB \subset (X \cup Y)B \\
&\subset [(X \cup Y)B] \cap [X^c \cap Y^c], \text{ dado que } X^c \cap (YB)^c \subset X^c \cap Y^c \\
&= (X \cup Y)B \cap (X \cup Y)^c \\
&= (X \cup Y)B \setminus (X \cup Y).
\end{aligned}$$

De manera similar se demuestra para los otros casos. Por lo tanto se tiene la contención $R_{12} \cup R_{22} \cup R_{32} \subset (X \cup Y)B \setminus (X \cup Y)$.

Por otro lado, sea $z \in (X \cup Y)B \setminus (X \cup Y)$, entonces

$$z \in (X \cup Y)B \text{ y } z \notin (X \cup Y) \implies z \in XB \cup YB \text{ y } z \notin (X \cup Y).$$

Ahora, se pueden presentar los siguientes casos:

$$1. z \in XB \text{ y } z \notin YB \quad 2. z \notin XB \text{ y } z \in YB \quad 3. z \in XB \text{ y } z \in YB$$

- El primer caso implica que $z \in R_{23} \subset R_{32} \cup R_{22} \cup R_{23}$.
- El segundo caso implica que $z \in R_{32} \subset R_{32} \cup R_{22} \cup R_{23}$.
- El tercer caso implica que $z \in R_{22} \subset R_{32} \cup R_{22} \cup R_{23}$.

Luego, $(X \cup Y)B \setminus (X \cup Y) \subset R_{32} \cup R_{22} \cup R_{23}$. Por lo tanto se cumple la ecuación

$$(X \cup Y)B \setminus (X \cup Y) = R_{32} \cup R_{22} \cup R_{23}.$$

Por último se probará la contención

$$(X \cap Y)B \setminus (X \cap Y) \subset R_{12} \cup R_{22} \cup R_{21}. \quad (2.3.3)$$

Sea $w \in ZB \setminus Z$ tales que $Z = X \cap Y$. Luego $w \in ZB$ y $w \notin Z$. Ahora, $Z \subset X$ y $Z \subset Y$, por Proposición 2.1, $ZB \subset XB$ y $ZB \subset YB$, así que $ZB \subset (XB \cap YB)$, esto es, $w \in XB \cap YB$. Por tanto $w \in (XB \cap YB) \setminus (X \cap Y) = R_{22} \subset R_{12} \cup R_{22} \cup R_{21}$.

Ahora, sea $w \in (X \cap Y)B \setminus (X \cap Y)$, luego $w \in (X \cap Y)B$ y $w \notin (X \cap Y)$, entonces existen $a \in X \cap Y$ y $b \in B$ tales que $w = ab$, de aquí se tienen los siguientes casos:

1. $w \in X$ y $w \notin Y$
 2. $w \notin X$ y $w \in Y$
 3. $w \notin X$ y $w \notin Y$
- Primer caso: Dado que $a \in X$, $a \in Y$ y $1 \in B$, entonces $w = a = a \cdot 1 \in YB$ y $w \in X$, así que $w \in X \cap (YB \setminus Y) = R_{12} \subset R_{12} \cup R_{22} \cup R_{21}$.
 - Segundo caso: Como $a \in X$ y $a \in Y$, entonces $w = ab \in XB$ y $w \in Y$, así que $w \in (XB \setminus X) \cap Y = R_{21} \subset R_{12} \cup R_{22} \cup R_{21}$.
 - Tercer caso: Puesto que $a \in X \cap Y$, $1 \in B$ y $w \notin (X \cap Y)$, entonces se tiene que $w \in (XB \setminus X) \cap (YB \setminus Y) = R_{22} \subset R_{12} \cup R_{22} \cup R_{21}$.

Por lo tanto, la contención (2.3.3) se satisface.

Ahora, dado que B es finito y X, Y son finitos o tienen complemento finito, los conjuntos $R_{12}, R_{21}, R_{22}, R_{23}$ y R_{32} de cada partición son finitos. Entonces se tiene lo siguiente:

$$\begin{aligned}\Phi_B(X) &= |R_{21}| + |R_{22}| + |R_{23}|, \\ \Phi_B(Y) &= |R_{12}| + |R_{22}| + |R_{32}|, \\ \Phi_B(X \cup Y) &= |R_{32}| + |R_{22}| + |R_{23}|, \\ \phi_B(X \cap Y) &\leq |R_{12}| + |R_{22}| + |R_{21}|,\end{aligned}$$

sumando las dos primeras filas y luego las dos siguientes se tiene

$$\begin{aligned}\Phi_B(X) + \Phi_B(Y) &= |R_{21}| + 2|R_{22}| + |R_{23}| + |R_{12}| + |R_{32}|, \\ \Phi_B(X \cup Y) + \Phi_B(X \cap Y) &\leq |R_{32}| + 2|R_{22}| + |R_{23}| + |R_{12}| + |R_{21}|.\end{aligned}$$

De aquí se concluye que

$$\Phi_B(X \cap Y) + \Phi_B(X \cup Y) \leq \Phi_B(X) + \Phi_B(Y). \quad \square$$

Se deduce de esta desigualdad el siguiente resultado.

Corolario 2.4. Sean C_i una i -celda para B y C_j una j -celda para B , k y l enteros positivos tal que $C_i \cap C_j$ y $P_B(C_i \cup C_j)$ son una k -celda y una l -celda para B respectivamente. Entonces se tiene que

$$\lambda_k(B) + \lambda_l(B) \leq \lambda_i(B) + \lambda_j(B).$$

Además, si $\lambda_k(B) + \lambda_l(B) = \lambda_i(B) + \lambda_j(B)$, entonces $P_B(C_i \cup C_j) = C_i \cup C_j$.

Demostración. En efecto, utilizando la Proposición 2.12 con $X = C_i$ y $Y = C_j$ se obtiene

$$\Phi_B(C_i \cap C_j) + \Phi_B(C_i \cup C_j) \leq \Phi_B(C_i) + \Phi_B(C_j),$$

luego,

$$\lambda_k(B) + \Phi_B(C_i \cup C_j) \leq \Phi_B(C_i) + \Phi_B(C_j).$$

Ahora, por la Proposición 2.10 se tiene $\lambda_l(B) = \Phi_B(P_B(C_i \cup C_j)) \leq \Phi_B(C_i \cup C_j)$, entonces

$$\lambda_k(B) + \lambda_l(B) \leq \lambda_i(B) + \lambda_j(B).$$

Además, si $P_B(C_i \cup C_j) = C_i \cup C_j$, entonces existe $X_{ij} \in G$ tal que $P_B(X_{ij}) = C_i \cup C_j$. Por el Corolario 2.1,

$$P_B^2(X_{ij}) = P_B(P_B(X_{ij})) = P_B(X_{ij}) = C_i \cup C_j,$$

pero $P_B(P_B(X_{ij})) = P_B(C_i \cup C_j)$, lo que implica que $P_B(C_i \cup C_j) = C_i \cup C_j$. Luego la desigualdad en este caso particular se convierte en una igualdad. $\square$

Lema 2.9. Sean C_i una i -celda finita para B y C_j una j -celda para B , k un entero positivo tal que $C_i \cap C_j$ es una k -celda para B . Si $k \geq j$, entonces

$$\lambda_j(B) + |D_B(C_j) \setminus D_B(C_i)| \leq \lambda_i(B) + |C_i \setminus C_j|.$$

Demostración. La prueba se basa en las particiones consideradas en la Proposición 2.12. Supóngase que se tiene el siguiente arreglo:

$\cap$	C_j	$C_j B \setminus C_j$	$G \setminus C_j B$
C_i	R_{11}	R_{12}	R_{13}
$C_i B \setminus C_i$	R_{21}	R_{22}	R_{23}
$G \setminus C_i B$	R_{31}	R_{32}	R_{33}

Por el Lema 2.5, los R_{ij} son disjuntos dos a dos ($i, j = 1, 2, 3$). Se probará ahora las siguientes expresiones:

$$R_{21} \cup R_{22} \cup R_{23} = C_i B \setminus C_i, \quad (2.3.4)$$

$$(C_i \cap C_j) B \setminus (C_i \cap C_j) \subset R_{21} \cup R_{22} \cup R_{12}. \quad (2.3.5)$$

Para la igualdad (2.3.4), suponga que existe $z \in (R_{21} \cup R_{22} \cup R_{23}) \setminus (C_i B \setminus C_i)$, luego $z \in R_{21} \cup R_{22} \cup R_{23}$ y $z \notin C_i B \setminus C_i$. Ahora, si $z \in R_{21} \cup R_{22} \cup R_{23}$ entonces z esta por lo

menos en alguno de estos conjuntos. Suponiendo que $z \in R_{21} = (C_i B \setminus C_i) \cap C_j$ se tiene que $z \in (C_i B \setminus C_i)$, pero esto contradice el hecho de que $z \notin C_i B \setminus C_i$, luego se cumple la contención $R_{21} \subset R_{21} \cup R_{22} \cup R_{23} \subset C_i B \setminus C_i$. Procediendo de manera similar se prueba para los otros casos. Por lo tanto,

$$R_{21} \cup R_{22} \cup R_{23} \subset C_i B \setminus C_i.$$

Por otro lado, sea $z \in (C_i B \setminus C_i) \setminus (R_{21} \cup R_{22} \cup R_{23})$, entonces $z \notin R_{21} \cup R_{22} \cup R_{23}$, lo que significa que z no está en ninguno de estos conjuntos, en particular $z \notin R_{21}$, es decir, $z \notin (C_i B \setminus C_i) \cap C_j$, esta última expresión contradice lo que inicialmente se había supuesto, dado que la opción $z \in C_i B \setminus C_i$ y $z \notin C_j$ no se puede presentar porque por hipótesis $C_i \cap C_j \neq \emptyset$. De forma análoga se puede probar si $z \notin R_{22}$ o $z \notin R_{23}$. Por lo tanto,

$$C_i B \setminus C_i \subset R_{21} \cup R_{22} \cup R_{23}.$$

Por la veracidad de las dos contenciones anteriores se tiene que

$$R_{21} \cup R_{22} \cup R_{23} = C_i B \setminus C_i.$$

Para probar que (2.3.5) se cumple, se procede de manera similar a la prueba de la contención 2.3.3 de la Proposición 2.12. Ahora, dado que la celda C_i es finita entonces el conjunto $C_i B$ es finito, se deduce así que $R_{11}, R_{12}, R_{13}, R_{21}, R_{22}$ y R_{23} también son finitos. Además, como C_j es una j -celda, entonces $C_j B \setminus C_j$ es finito, luego el conjunto R_{32} también lo es. Se concluye que los dos únicos elementos de esta partición que, posiblemente pueden ser infinitos son R_{31} y R_{33} . Como $C_i \cap C_j$ es una k -celda y C_i es una i -celda entonces por (2.3.4) y (2.3.5) se tiene la siguiente igualdad y desigualdad respectivamente:

$$\lambda_i(B) = |R_{21} \cup R_{22} \cup R_{23}| = |R_{21}| + |R_{22}| + |R_{23}|,$$

$$\lambda_k(B) \leq |R_{21} \cup R_{22} \cup R_{12}| = |R_{21}| + |R_{22}| + |R_{12}|.$$

Por otro parte, observe que por propiedades básicas de teoría de conjuntos, si A, B, C

son conjuntos entonces $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. Se deduce así que

$$\begin{aligned}
 R_{13} \cup R_{23} &= (C_i \cap D_B(C_j)) \cup ((C_i B \setminus C_i) \cap D_B(C_j)) \\
 &= D_B(C_j) \cap (C_i \cup (C_i B \setminus C_i)) \\
 &= D_B(C_j) \cap (C_i B) \\
 &= D_B(C_j) \cap (G \setminus C_i B)^c \\
 &= D_B(C_j) \setminus D_B(C_i).
 \end{aligned}$$

De forma similar,

$$\begin{aligned}
 R_{12} \cup R_{13} &= (C_i \cap (C_j B \setminus C_j)) \cup (C_i \cap D_B(C_j)) \\
 &= C_i \cap ((C_j B \setminus C_j) \cup D_B(C_j)) \\
 &= C_i \cap (G \setminus C_j) \\
 &= C_i \cap (C_j)^c \\
 &= C_i \setminus C_j.
 \end{aligned}$$

Luego se tienen las siguientes expresiones:

$$|D_B(C_j) \setminus D_B(C_i)| = |R_{13} \cup R_{23}| = |R_{13}| + |R_{23}|,$$

$$|C_i \setminus C_j| = |R_{12} \cup R_{13}| = |R_{12}| + |R_{13}|.$$

Así se obtiene que

$$\begin{aligned}
 \lambda_k(B) + |D_B(C_j) \setminus D_B(C_i)| &\leq (|R_{21}| + |R_{22}| + |R_{12}|) + |R_{13}| + |R_{23}| \\
 &= (|R_{21}| + |R_{22}| + |R_{23}|) + (|R_{12}| + |R_{13}|) \\
 &= \lambda_i(B) + |C_i \setminus C_j|.
 \end{aligned}$$

Finalmente, la desigualdad $k \geq j$ implica que $\lambda_k(B) \geq \lambda_j(B)$. En conclusión se tiene,

$$\lambda_j(B) + |D_B(C_j) \setminus D_B(C_i)| \leq \lambda_i(B) + |C_i \setminus C_j|. \quad \square$$

Capítulo 3

El Método Isoperimétrico y su Aplicación a la Función μ_G

En la primera sección de este capítulo se expone la estructura de las 1-celdas C_1 y los 1-núcleos N_1 , para ello se estudian el Lema 3.1, la Proposición 3.1 y el Teorema 3.1, que permiten identificar la teoría del nuevo enfoque isoperimétrico desarrollado por Balandraud en [4, 5]. Posteriormente se da a conocer la estructura de las j -celdas C_j y las a_2 -celdas C_{a_2} , con $1 \leq j < a_2$. Finalmente se presenta una aplicación del método isoperimétrico al problema de los conjuntos suma pequeños, más específicamente se da a conocer de acuerdo a los trabajos desarrollados por Balandraud en [5], que la ecuación $\mu_G(r, s) = \kappa_G(r, s)$ no se satisface en general para algunos valores de r y s en grupos finitos no abelianos de la forma $G = \mathbb{Z}_q \rtimes \mathbb{Z}_p$, donde p y q son primos impares tales que $q \equiv 1 \pmod{p}$. Esta aplicación permite contestar negativamente la pregunta 3.1 formulada por Eliahou, Kervaire y Plagne en [7] sobre la función $\mu_G(r, s)$.

En el presente Capítulo se asumirá que para un subconjunto B de un grupo G , la identidad del grupo G siempre está en B .

3.1. Estructura de 1-Celdas y 1-Núcleos

Se comienza dando a conocer la existencia de las 1-celdas. Sean G un grupo y B un subconjunto finito de G . Si $B = G$, entonces para todo subconjunto no vacío X de G , se tiene $XB = G$. Por lo tanto, de acuerdo a la Definición 2.6, $\emptyset$ y G no corresponde a

1-celdas. Se garantiza la existencia de las 1-celdas como sigue:

Sean G un grupo y B un subconjunto finito de G tal que $1 \in B$. Para todo subconjunto X que esta en $C_{B,f} \setminus C_B^0$ se tiene que $\Phi_B(X) \in \mathbb{N}$, esto es, existe

$$\lambda_1(B) = \min\{\Phi_B(X) : X \in C_{B,f} \setminus C_B^0\},$$

luego $C_B^1 \neq \emptyset$, lo que es lo mismo, la 1-celda X para B existe.

Definición 3.1. Sea G un grupo tal que $\beta_1(B)$ existe. Se llamará condición $E_1(B)$ para una celda C de B , la expresión

$$|G \setminus C| \geq \lambda_1(B) + \beta_1(B).$$

El número $\lambda_1(B) + \beta_1(B)$ es siempre finito. Por lo tanto, si G es infinito esta condición se cumple para cualquier celda finita C .

Lema 3.1. Si existen $\beta_1(B)$ y $\beta_1(B^{-1})$ y además $\beta_1(B) \leq \beta_1(B^{-1})$ entonces toda 1-celda para B satisface la condición $E_1(B)$.

Demostración. Sea C_1 una 1-celda para B , por Proposición 2.11 $D_B(C_1)$ es una 1-celda para B^{-1} , así que se cumple $|D_B(C_1)| \geq \beta_1(B^{-1})$. Luego se tiene,

$$\begin{aligned} |G \setminus C_1| - \lambda_1(B) &= |G \setminus C_1| - |C_1 B \setminus C_1| \\ &= |G| - |C_1| - |C_1 B| + |C_1| \\ &= |G| - |C_1 B| = |D_B(C_1)|. \end{aligned}$$

Pero $|D_B(C_1)| \geq \beta_1(B^{-1}) \geq \beta_1(B)$, luego se concluye que

$$|G \setminus C_1| - \lambda_1(B) \geq \beta_1(B^{-1}) \geq \beta_1(B),$$

es decir,

$$|G \setminus C_1| \geq \lambda_1(B) + \beta_1(B),$$

y C_1 satisface la condición $E_1(B)$. □

Se muestra ahora la importancia que tienen las 1-celdas que cumplen la condición $E_1(B)$.

Proposición 3.1. Sean G un grupo, B un subconjunto finito de G que contiene 1 y tal que $\beta_1(B)$ existe. Sean N_1 un 1-núcleo y C_1 una 1-celda para B tal que C_1 satisface la condición $E_1(B)$. Si $N_1 \cap C_1 \neq \emptyset$ entonces $N_1 \subset C_1$.

Demostración. Por definición el 1-núcleo N_1 es finito, de cardinalidad $\beta_1(B)$. Ahora, como C_1 y N_1 son 1-celdas entonces $C_1 \cap N_1$ es una k -celda finita para algún $k \geq 1$. Considérese ahora la unión $C_1 \cup N_1$ y sea l el número entero tal que $P_B(C_1 \cup N_1)$ es una l -celda. Se probará que $l \geq 1$ (lo que es lo mismo, que $P_B(C_1 \cup N_1)$ no es una 0-celda). Por Lema 2.9 se tiene que

$$\lambda_1(B) + |D_B(C_1) \setminus D_B(N_1)| \leq \lambda_1(B) + |N_1 \setminus C_1|, \text{ es decir, } |D_B(C_1) \setminus D_B(N_1)| \leq |N_1 \setminus C_1|.$$

Además, puesto que C_1 satisface la condición $E_1(B)$, entonces

$$|D_B(C_1)| \geq \beta_1(B) = |N_1|.$$

Así, se puede mostrar que $D_B(C_1) \cap D_B(N_1) \neq \emptyset$. Observe la siguiente igualdad:

$$\begin{aligned} D_B(C_1) \setminus [D_B(C_1) \setminus D_B(N_1)] &= D_B(C_1) \cap [D_B(C_1) \setminus D_B(N_1)]^c \\ &= D_B(C_1) \cap [D_B(C_1) \cap (D_B(N_1))^c]^c \\ &= D_B(C_1) \cap [(D_B(C_1))^c \cup D_B(N_1)] \\ &= [D_B(C_1) \cap (D_B(C_1))^c] \cup [D_B(C_1) \cap D_B(N_1)] \\ &= \emptyset \cup [D_B(C_1) \cap D_B(N_1)] \\ &= D_B(C_1) \cap D_B(N_1). \end{aligned}$$

Luego,

$$\begin{aligned} |D_B(C_1) \cap D_B(N_1)| &= |D_B(C_1)| - |D_B(C_1) \setminus D_B(N_1)| \\ &\geq |D_B(C_1)| - |N_1 \setminus C_1| \\ &\geq |N_1| - |N_1 \setminus C_1| \\ &= |N_1 \cap C_1| > 0. \end{aligned}$$

Por la ecuación (2.2.2) de la Proposición 2.7 $D_B(C_1 \cup N_1) = D_B(C_1) \cap D_B(N_1)$ y como se probó que este conjunto es no vacío, entonces $P_B(C_1 \cup N_1)$ es una l -celda para B , con $l \geq 1$.

Entonces el Corolario 2.4 muestra que

$$\lambda_k(B) + \lambda_l(B) \leq |N_1B \setminus N_1| + |C_1B \setminus C_1| = \lambda_1(B) + \lambda_1(B).$$

Esta desigualdad se cumple cuando $k \geq 1$ y $l \geq 1$. Dado que la secuencia de valores $\lambda_i(B)$, con $i \geq 1$ es estrictamente creciente, se debe tener necesariamente $k = l = 1$. La ecuación $k = 1$ implica que $C_1 \cap N_1$ es una 1-celda, pero $C_1 \cap N_1 \subset N_1$, entonces

$$|C_1 \cap N_1| \leq |N_1|. \quad (3.1.1)$$

Además, N_1 es un 1-núcleo, entonces

$$|N_1| \leq |C_1 \cap N_1|. \quad (3.1.2)$$

De la ecuación (3.1.1) y (3.1.2) se tiene que $|N_1| = |C_1 \cap N_1|$, además $C_1 \cap N_1 \subset N_1$ y N_1 es finito, luego $N_1 = C_1 \cap N_1$, lo que implica que $N_1 \subset C_1$. $\square$

Con base en la Proposición 3.1 se presenta un enunciado estructural para los 1-núcleos de B , y para todas las 1-celdas que cumplen la condición $E_1(B)$.

Teorema 3.1. *Sean G un grupo y B un subconjunto finito de G tal que $1 \in B$. Si existen $\beta_1(B)$ y una 1-celda C_1 para B que satisface la condición $E_1(B)$, entonces existe un subgrupo finito N_1 de G que es un 1-núcleo para B o para B^{-1} tal que para cualquier 1-celda C_1 , se tiene que C_1 o C_1B es periódico por la derecha módulo N_1 , es decir, $C_1N_1 = C_1$ o $(C_1B)N_1 = C_1B$.*

Demostración. Para el caso $\lambda_1(B) = |N_1B| - |N_1| = |B| - 1$, el subgrupo $N_1 = \{1\}$ cumple la condición. Considérese que se tiene $\lambda_1(B) = |N_1B| - |N_1| < |B| - 1$, entonces cualquier 1-núcleo N para B satisface la condición $E_1(B)$ dado que $|G \setminus N| \geq |G \setminus C_1|$. Suponga que existen dos 1-núcleos N y N_1 para B tales que $N \cap N_1 \neq \emptyset$. Por la Proposición 3.1 $N \subset N_1$ y $N_1 \subset N$, esto es, $N = N_1$. Por lo tanto dos 1-núcleos o son iguales o son disjuntos. Por otro lado, sin pérdida de generalidad se puede suponer que si N_1 es un 1-núcleo para B entonces $1 \in N_1$. En efecto, sea $x \in N_1$ con $x \neq 1$, entonces

$$\begin{aligned} |(x^{-1}N_1)B \setminus (x^{-1}N_1)| &= |(x^{-1}N_1)B| - |x^{-1}N_1| \\ &= |x^{-1}(N_1B)| - |N_1| \\ &= |N_1B| - |N_1| = \lambda_1(B). \end{aligned}$$

Lo que significa que $x^{-1}N_1$ es un 1-núcleo para B y además $1 \in x^{-1}N_1$. Para todo $x \in N_1$ se tiene que $1 \in N_1 \cap x^{-1}N_1$, esto es, $N_1 \cap x^{-1}N_1 \neq \emptyset$, por lo tanto como dos 1-núcleos o son iguales o son disjuntos entonces $N_1 = x^{-1}N_1$. Sean $x, y \in N_1$, entonces $x^{-1}, y^{-1} \in N_1$ y $(x^{-1})^{-1}N_1 = N_1$, luego $xN_1 = N_1$. Ahora, como $N_1 = x^{-1}N_1$, existe $z \in N_1$ tal que $y = x^{-1}z$, luego $z = xy \in N_1$. Por lo tanto N_1 es un subgrupo finito de G . Por traslación todas las clases laterales izquierdas módulo N_1 son 1-núcleos, ya que para cualquier $a \in G$, se tiene que $|(aN_1)B| - |aN_1| = |N_1B| - |N_1| = \lambda_1(B)$, y como todas las clases laterales izquierdas de N_1 forman una partición de G , entonces son todos los 1-núcleos posibles.

Ahora, sea C_1 una 1-celda para B que satisface la condición $E_1(B)$, la Proposición 3.1 afirma que ésta contiene todos los 1-núcleos que intersectan a C_1 , lo que implica que $C_1 \cap N_1 \neq \emptyset$. Así que C_1 es una unión de clases laterales izquierdas de N_1 , es decir,

$$\bigcup_{c \in C_1} cN_1 = C_1 \text{ y por lo tanto } C_1N_1 = C_1.$$

Si $\beta_1(B) \leq \beta_1(B^{-1})$, por Lema 3.1 toda 1-celda para B satisface la condición $E_1(B)$ y por tanto cumple todas las condiciones anteriores, así el teorema queda demostrado.

Intercambiando los papeles, si $\beta_1(B) > \beta_1(B^{-1})$, existe un subgrupo finito N_1 que es un 1-núcleo para B^{-1} y toda 1-celda C para B^{-1} satisface la condición $E_1(B^{-1})$, luego C es periódica por la derecha módulo N_1 . Si C_1 es una celda para B , entonces $D_B(C_1)$ es una 1-celda para B^{-1} y cumple que $D_B(C_1)N_1 = D_B(C_1)$. Ahora, observe que el complemento de $D_B(C_1) = G \setminus C_1B$ equivalente a C_1B también es periódico por la derecha módulo N_1 , es decir, $(C_1B)N_1 = C_1B$.

En efecto, dado que $1 \in N_1$ se tiene que $C_1B \subset (C_1B)N_1$. Por otro lado, supóngase por contradicción que existe $z \in (C_1B)N_1 \setminus C_1B$, entonces $z \in (C_1B)N_1$ y $z \notin C_1B$, luego $z = yx$ para algún $y \in C_1B$ y $x \in N_1$. De aquí se sigue que $zx^{-1} = y \in C_1B$. Pero $z \in (C_1B)^c$ y $x^{-1} \in N_1$, luego $zx^{-1} = y \in (C_1B)^cN_1 = (C_1B)^c$. Por consiguiente, $y \in C_1B$ y $y \in (C_1B)^c$, lo cual es una contradicción. Por lo tanto $(C_1B)N_1 \subset C_1B$. Finalmente, de las dos contenencias probadas se tiene que $(C_1B)N_1 = C_1B$. $\square$

Corolario 3.1. *Sea G un grupo y B un subconjunto finito de G tal que $1 \in B$. Entonces existe un subgrupo finito N_1 de G tal que $\lambda_1(B) = \left(\left\lceil \frac{|B|}{|N_1|} \right\rceil - 1 \right) |N_1|$. Además, para toda 1-celda finita C_1 , $|C_1|$ y $|C_1B|$ son múltiplos de $|N_1|$.*

Demostración. Según el Teorema 3.1, si $\beta_1(B) \leq \beta_1(B^{-1})$, entonces un 1-núcleo N_1 para B tal que $1 \in B$, es un subgrupo finito de G y se tiene

$$\lambda_1(B) = |N_1B| - |N_1| < |B| - 1 < |N_1B|. \quad (3.1.3)$$

Luego, como N_1B es la unión de clases laterales derechas módulo N_1 , entonces se puede escribir $N_1B = \bigcup_{b \in B} N_1b$, equivalentemente $N_1B = N_1b_1 \cup N_1b_2 \cup \dots \cup N_1b_r$. Se sigue de esta última ecuación que $|N_1B| = r|N_1|$. Ahora, utilizando la expresión (3.1.3) se obtiene $|N_1B| - |N_1| = (r - 1)|N_1| < |B| \leq r|N_1|$. Dividiendo el lado derecho de esta ecuación por $|N_1|$ se deduce lo siguiente:

$$r - 1 < \frac{|B|}{|N_1|} \leq r.$$

La función techo del Capítulo 1 permite establecer $\left\lceil \frac{|B|}{|N_1|} \right\rceil = r$ y $\left\lceil \frac{|B|}{|N_1|} \right\rceil - 1 = r - 1$. De la ecuación (3.1.3) se observa que $\lambda_1(B)$ es el mayor múltiplo de $\beta_1(B)$ estrictamente menor que $|B|$. Entonces se puede escribir

$$\lambda_1(B) = \left(\left\lceil \frac{|B|}{|N_1|} \right\rceil - 1 \right) |N_1|.$$

Por otra lado, para toda 1-celda C_1 finita, C_1 es periódica por la derecha módulo N_1 , es decir, $C_1 = C_1N_1$. Se sigue que C_1 es la unión disjunta de clases laterales por la izquierda módulo N_1 , esto es,

$$C_1 = c_1N_1 \cup c_2N_1 \cup \dots \cup c_sN_1,$$

y como todas las clases laterales de N_1 tienen la misma cantidad de elementos, y además comparten el mismo cardinal de $|N_1|$, entonces $|C_1| = s|N_1|$, lo que significa que $|C_1|$ es múltiplo de $|N_1|$. Para el producto C_1B se tiene $|C_1B| = |\lambda_1(B)| + |C_1|$, pero $\lambda_1(B)$ y $|C_1|$ son múltiplos de $|N_1|$, lo que implica que $|C_1B|$ también lo es.

Si $\beta_1(B) \geq \beta_1(B^{-1})$, entonces un 1-núcleo N_1 para B^{-1} que contiene al 1 es un subgrupo finito de G . Por tanto, como $|B| = |B^{-1}|$, entonces para B^{-1} se tiene que

$$\lambda_1(B^{-1}) = \left(\left\lceil \frac{|B^{-1}|}{|N_1|} \right\rceil - 1 \right) |N_1| = \left(\left\lceil \frac{|B|}{|N_1|} \right\rceil - 1 \right) |N_1| = \lambda_1(B).$$

Además, para cualquier 1-celda finita C_1 para B , su dualidad $D_B(C_1)$ es periódico por la derecha módulo N_1 , por Teorema 3.1 su complemento C_1B también cumple esta propiedad. Por lo tanto, $|C_1B|$ es múltiplo de $|N_1|$. Para terminar, puesto que $|C_1| = |C_1B| - \lambda_1(B)$, se sigue que $|C_1|$ es múltiplo de $|N_1|$. $\square$

Proposición 3.2. Sean G un grupo y B un subconjunto finito de G , si $\beta_1(B)$ y $\beta_1(B^{-1})$ existen y son tales que $\beta_1(B) < \beta_1(B^{-1})$, entonces $\beta_1(B)$ divide $\beta_1(B^{-1})$.

Demostración. En efecto, considérese un 1-núcleo N_1 para B que contiene 1, por Teorema 3.1, N_1 es un subgrupo finito de G y se tiene $\lambda_1(B) = |N_1B| - |N_1|$, donde N_1B es la unión de clases laterales por la derecha módulo N_1 . Además, del Corolario 3.1 se sigue que $\beta_1(B) = |N_1|$ es múltiplo de $\lambda_1(B)$, es decir, $\beta_1(B)$ divide a $\lambda_1(B)$.

En este orden de ideas, por Lema 3.1, si N'_1 es un 1-núcleo para B^{-1} , entonces $D_{B^{-1}}(N'_1)$ es una 1-celda para $(B^{-1})^{-1} = B$ que satisface la condición $E_1(B)$. Por lo tanto, de acuerdo al Teorema 3.1, $D_{B^{-1}}(N'_1)$ es una unión de clases laterales por la izquierda módulo N_1 , lo que es lo mismo, $D_{B^{-1}}(N'_1)N_1 = D_{B^{-1}}(N'_1)$. Ahora, dado que $|D_{B^{-1}}(N'_1)|$ es múltiplo de $|N_1|$, se sigue del Corolario 3.1 que su complemento $|G \setminus D_{B^{-1}}(N'_1)|$ también lo es. Por consiguiente, $\beta_1(B)$ divide $|G \setminus D_{B^{-1}}(N'_1)|$. Para concluir, puesto que la 1-celda $D_{B^{-1}}(N'_1)$ satisface la condición $E_1(B)$, entonces del Lema 3.1 se tiene que

$$|G \setminus D_{B^{-1}}(N'_1)| - \lambda_1(B) = \beta_1(B^{-1}).$$

Por lo tanto, $\beta_1(B)$ divide $\beta_1(B^{-1})$. □

3.2. Estructura de las a_2 -Celdas

Al igual que en el Teorema 3.1, donde se estudió la estructura de las 1-celdas C_1 , en esta sección se estudia la estructura de las a_2 -celdas.

Definición 3.2. Sean G un grupo, B un subconjunto de G y $\beta_1(B) \leq \beta_1(B^{-1})$. Se denota con a_2 el menor índice tal que existe una a_2 -celda incluida propiamente en un 1-núcleo N_1 o una a_2 -celda que no satisface la condición $E_1(B)$.

Se sigue del Lema 3.1 y la Proposición 3.1 que $a_2 > 1$, es decir, $\lambda_{a_2}(B) > \lambda_1(B)$. En efecto, si $a_2 = 1$, puesto que $|C_{a_2}| < |N_1|$, se tiene que $|N_1| > |C_1|$, lo cual contradice que N_1 es una 1-celda de cardinalidad mínima. De forma similar, si $a_2 = 1$ se estaría contradiciendo el Lema 3.1, ya que ninguna 1-celda podrá satisfacer la condición $E_1(B)$. Por lo tanto, $a_2 > 1$.

Lema 3.2. Sean G un grupo y B un subconjunto finito de G tal que $1 \in B$ y $\beta_1(B) \leq \beta_1(B^{-1})$. Cada j -celda que satisface la condición $E_1(B)$, es una unión disjunta de 1-núcleos y k -celdas, cada k -celda incluida en un 1-núcleo, con $k \leq j$.

Además, toda a_2 -celda que satisface la condición $E_1(B)$, es una unión disjunta de 1-núcleos y a lo sumo una a_2 -celda incluida en un 1-núcleo.

Demostración. A la luz del Lema 3.1, $\beta_1(B)$ existe. Considérese a C_j una j -celda para B que satisface la condición $E_1(B)$ y N_1 un 1-núcleo que intersecta a C_j . Sea k un entero positivo tal que $N_1 \cap C_j$ es una k -celda. Supóngase que $k \geq j$, por Lema 2.9 se tiene que

$$\lambda_j(B) + |D_B(C_j) \setminus D_B(N_1)| \leq \lambda_1(B) + |N_1 \setminus C_j|,$$

lo que equivale a la expresión

$$|D_B(C_j) \setminus D_B(N_1)| \leq \lambda_1(B) - \lambda_j(B) + |N_1 \setminus C_j|.$$

Ahora, puesto que C_j satisface la condición $E_1(B)$, entonces

$$|G \setminus C_j| \geq \lambda_1(B) + \beta_1(B), \tag{3.2.1}$$

lo cual puede ser escrito en la forma

$$|D_B(C_j)| \geq \beta_1(B) + \lambda_1(B) - \lambda_j(B). \tag{3.2.2}$$

Por la Proposición 3.1 y las desigualdades (3.2.1) y (3.2.2) se tiene lo siguiente:

$$\begin{aligned} |D_B(C_j) \cap D_B(N_1)| &= |D_B(C_j)| - |D_B(C_j) \setminus D_B(N_1)| \\ &\geq |D_B(C_j)| - \lambda_1(B) + \lambda_j(B) - |N_1 \setminus C_j| \\ &\geq (\beta_1(B) + \lambda_1(B) - \lambda_j(B)) - \lambda_1(B) + \lambda_j(B) - |N_1 \setminus C_j| \\ &= |N_1| - |N_1 \setminus C_j| \\ &= |N_1 \cap C_j| > 0. \end{aligned}$$

La última afirmación implica que $P_B(C_j \cup N_1)$ es una l -celda con $l \geq 1$.

Teniendo en cuenta la desigualdad del Corolario 2.4 se tiene que

$$\lambda_k(B) + \lambda_l(B) \leq \lambda_1(B) + \lambda_j(B).$$

Pero, la desigualdad anterior no se cumple con los supuestos $k > j$ y $l \geq 1$. Luego necesariamente se debe tener $k \leq j$.

Por otro lado, considérense una a_2 -celda C_{a_2} que satisface la condición $E_1(B)$ y que no es una unión de 1-núcleos, entonces existe un 1-núcleo N_1 tal que $N_1 \cap C_{a_2} \neq \emptyset$ y $N_1 \not\subseteq C_{a_2}$. Sean k y l enteros positivos tal que $N_1 \cap C_{a_2}$ es una k -celda y $P_B(N_1 \cup C_{a_2})$ es una l -celda. Por el Corolario 2.4 se tiene,

$$\lambda_k(B) + \lambda_l(B) \leq \lambda_1(B) + \lambda_{a_2}(B).$$

Esta desigualdad se cumple con $k \leq a_2$ y $l \geq 1$. Puesto que la k -celda $N_1 \cap C_{a_2}$ está incluida propiamente en N_1 , por la definición de a_2 también se debe tener $k \geq a_2$. Se sigue así que $k = a_2$ y $l = 1$, luego la desigualdad anterior se transforma en una igualdad. Ahora, el Corolario 2.4 garantiza que $P_B(N_1 \cup C_{a_2}) = N_1 \cup C_{a_2}$ es una 1-celda y como $\beta_1(B) \leq \beta_1(B^{-1})$, por Proposición 3.1 y Teorema 3.1 existe un subgrupo N'_1 de G que es un 1-núcleo para B tal que $(N_1 \cup C_{a_2})N'_1 = N_1 \cup C_{a_2}$. Esto implica que $N_1 \cup C_{a_2}$ es unión de 1-núcleos, de aquí que C_{a_2} es una unión de 1-núcleos. Pero este hecho contradice lo que inicialmente se había supuesto. Por lo tanto, C_{a_2} es una unión disjunta de 1-núcleos y, al menos un 1-núcleo de esta unión contiene a lo sumo una a_2 -celda. $\square$

Se sigue entonces que toda j -celda C_j , con $1 \leq j < a_2$, comparte una estructura similar a las 1-celdas de la Sección 3.1.

Proposición 3.3. *Sean G un grupo y B un subconjunto finito de G tal que $1 \in B$. Existe un subgrupo finito N_1 de G tal que para toda j -celda C_j con $1 \leq j < a_2$, C_j o $C_j B$ es una unión de clases laterales izquierdas de N_1 .*

Demostración. Asúmase que existen $\beta_1(B)$ y $\beta_1(B^{-1})$ tales que $\beta_1(B) \leq \beta_1(B^{-1})$. Considérese una j -celda C_j , con $1 \leq j < a_2$, por definición de a_2 esta j -celda satisface la condición $E_1(B)$. Por otro lado, sea N'_1 un 1-núcleo que interseca a C_j , por Lema 3.2, la intersección es una k -celda incluida en un 1-núcleo, con $k \leq j$, luego $k < a_2$. Por la definición de a_2 , necesariamente se tiene $k = 1$. Luego, por Lema 3.1 y Teorema 3.1, existe un 1-núcleo N_1 que es un subgrupo de G tal que la j -celda C_j es una unión de 1-núcleos y por lo tanto es periódica por la derecha módulo el 1-núcleo N_1 . Por otro lado, si $\beta_1(B) > \beta_1(B^{-1})$, considérese una j -celda C_j para B , por lo probado en el Teorema 3.1, la expresión $D_B(C_j)$ es una unión de clases laterales izquierdas de N_1 ,

donde N_1 es un 1-núcleo para B^{-1} que contiene a 1. Por lo tanto, el complemento $C_j B$ de $D_B(C_j)$, es una unión de clases laterales izquierdas de N_1 . $\square$

Teorema 3.2. *Sean G un grupo y B un subconjunto finito de G que contiene a 1 tal que $\lambda_{a_2}(B) < |B| - 1$, entonces existe un subgrupo propio finito N_{a_2} de G tal que $\lambda_{a_2}(B) = \left(\left\lceil \frac{|B|}{|N_{a_2}|} \right\rceil - 1\right)|N_{a_2}|$. Además para cualquier a_2 -celda C_{a_2} finita, $|C_{a_2}|$ y $|C_{a_2}B|$ son múltiplos de $|N_{a_2}|$.*

La prueba del Teorema 3.2 el lector la puede consultar en ([5], Teorema 21).

3.3. Una Aplicación a los Grupos Solubles

En esta sección se presenta un ejemplo que permite dar respuesta negativa a la siguiente pregunta formulada por los autores de [7].

Pregunta 3.1. Sean G un grupo finito y r, s enteros positivos tales que $r, s \leq |G|$, es cierto que

$$\mu_G(r, s) = \kappa_G(r, s) = \min_{h \in \mathcal{H}(G)} \left\{ \left(\left\lceil \frac{r}{|h|} \right\rceil + \left\lceil \frac{s}{|h|} \right\rceil - 1 \right) |h| \right\}?, \quad (3.3.1)$$

de hecho se prueba que, en todo grupo no abeliano y soluble de la forma $G = \mathbb{Z}_q \rtimes \mathbb{Z}_p$, con p y q primos impares tales que $q \equiv 1 \pmod{p}$, existen enteros positivos $r, s \leq pq$ para los cuales la ecuación (3.3.1) no se satisface. El Teorema de Feit y Thompson (ver [13]) garantiza que el grupo $G = \mathbb{Z}_q \rtimes \mathbb{Z}_p$ es soluble por ser de orden impar.

Lema 3.3. *Sean G un grupo y H un subgrupo finito de G . Si A es un subconjunto de una clase lateral izquierda aH y B es un subconjunto de una clase lateral derecha Hb y $|A| + |B| > |H|$, entonces $AB = aHb$.*

Demostración. Sea $z = xy \in AB$ con $x \in A$ y $y \in B$. Luego existen $h_1, h_2 \in H$ tales que $x = ah_1$ y $y = h_2b$, entonces $z = (ah_1)(h_2b) = a(\underbrace{h_1h_2}_{\in H})b$, luego, $AB \subset aHb$. Por

otro lado, el Lema 1.3 afirma que

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

Sean $A' = \{h \in H : ah \in A\}$ y $B' = \{h \in H : hb \in B\}$, se sigue que $A' \subset H$ y $B' \subset H$. Luego $|A| = |A'|$ y $|B| = |B'|$ porque $|aH| = |H|$ y $|Hb| = |H|$. Luego, para

todo $x \in H$ se tiene que $A' \cap xB'^{-1} \neq \emptyset$, porque $A' \cup xB'^{-1} \subset H$ y $|A' \cup xB'^{-1}| \leq |H|$. Supóngase que $A' \cap xB'^{-1} = \emptyset$, entonces $|A' \cup xB'^{-1}| = |A'| + |xB'^{-1}| = |A| + |B| > |H|$, lo cual es una contradicción. Por lo tanto, $A' \cap xB'^{-1} \neq \emptyset$ para toda $x \in H$. Por Lema 1.3 $A'B' = H$ y se tiene que

$$|AB| = |A'B'| = |H| = |aHb|,$$

pero H es finito, se concluye así que $AB = aHb$. $\square$

Los Lemas 3.3 y 3.4 serán de gran utilidad en la prueba de la Proposición 3.4.

Lema 3.4. Sean p y q dos enteros primos impares tales que $q \equiv 1 \pmod{p}$ y sea $P = \{a, a + r, a + 2r, \dots, (l - 1)r\}$ una progresión aritmética en $\mathbb{Z}_q$ de longitud $2 \leq l \leq \frac{q-1}{2}$. Si $P = \{a', a' + r', a' + 2r', \dots, (l - 1)r'\}$ entonces $r' = \pm r$.

Demostración. Supóngase por contradicción que $r' \neq \pm r$. Dado que $a', a + r' \in P$ entonces existen enteros $i, j \in [0, l - 1]$ tal que $a' = a + ir$ y $a' + r' = a + jr$, luego de estas ecuaciones se tiene $r' = (j - i)r$, donde $2 \leq |j - i| \leq l - 1$. Primero suponga que $2 \leq j - i \leq l - 1$ y observe que

$$((q - 1) - i) - (l - i) = q - 1 - l \geq \frac{q - 1}{2} > l - 1 \geq j - i.$$

Luego existe $k_0 \in [0, l - 1]$ tal que $l - 1 - i < k_0(j - i) \leq q - 1 - i$, o equivalentemente $l - 1 < i + k_0(j - i) \leq q - 1$, así que $a + [i + k_0(j - i)]r \in P$ y existe $t_0 \in [0, l - 1]$ tal que

$$a + [i + k_0(j - i)]r = a + t_0r \text{ en } \mathbb{Z}_q.$$

Dado que $\mathbb{Z}_q$ es un campo, se tiene que $i + k_0(j - i) = t_0$, lo cual es una contradicción, dado que $t_0 \in [0, l - 1]$. Por lo tanto, se debe tener que $-(l - 1) \leq j - i \leq -2$.

Ahora, de $(j - i) \leq -2$ se tiene que $i - j \geq 2$, luego el intervalo $[i, l + i]$ tiene longitud estrictamente mayor que $i - j$ y $|i - j| > 0$. Realizando un proceso similar al anterior, existe $k_0 \in [0, l - 1]$ tal que $i < k_0(i - j) \leq (l + i)$, multiplicando por -1 se tiene la expresión $-(l + i) \leq k_0(j - i) < -i$, y finalmente $-l \leq i + k_0(j - i) < 0$. Así que, $a + [i + k_0(j - i)]r \in P$ y existe $t_0 \in [0, l - 1]$ tal que $a + [i + k_0(j - i)]r = a + t_0r$ en $\mathbb{Z}_q$, luego se tiene que $i + k_0(j - i) = t_0$, lo cual es una contradicción. En conclusión, se tiene que $r' = \pm r$. $\square$

Proposición 3.4. Sean p y q dos enteros primos impares tales que $q \equiv 1 \pmod{p}$. Entonces en el grupo $G = \mathbb{Z}_q \rtimes \mathbb{Z}_p$ se tiene que

$$\mu_G(q + p - 1, q - 1) = 2q,$$

$$\text{y } \kappa_G(q + p - 1, q - 1) = 2q - 2.$$

Demostración. Observe que $\mathcal{H}(G) = \{1, p, q, pq\}$. Entonces

$$\kappa_G(q + p - 1, q - 1) = \min_{d \in \{1, p, q, pq\}} \left\{ \left(\left\lceil \frac{q + p - 1}{d} \right\rceil + \left\lceil \frac{q - 1}{d} \right\rceil - 1 \right) d \right\}.$$

Estos cuatro valores pueden ser calculados fácilmente teniendo en cuenta que por hipótesis p divide a $q - 1$. Luego, llamando $r = q + p - 1$ y $s = q - 1$ se tiene lo siguiente:

- Si $d = 1$ entonces $\left(\left\lceil \frac{q + p - 1}{1} \right\rceil + \left\lceil \frac{q - 1}{1} \right\rceil - 1 \right) = 2q + p - 3$.

- Si $d = p$ entonces

$$\begin{aligned} \left(\underbrace{\left\lceil \frac{q + p - 1}{p} \right\rceil}_{\in \mathbb{Z}} + \underbrace{\left\lceil \frac{q - 1}{p} \right\rceil}_{\in \mathbb{Z}} - 1 \right) p &= \left[\left(\frac{q + p - 1}{p} \right) + \left(\frac{q - 1}{p} \right) - 1 \right] p \\ &= (q + p - 1) + (q - 1) - p \\ &= 2q - 2. \end{aligned}$$

- Si $d = q$ observe que $q < p + q - 1 < 2q$, luego $\left\lceil \frac{q + p - 1}{q} \right\rceil = 2$ y se tiene que

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

- Si $d = pq$ observe que $pq > q + p - 1$ y $pq > q - 1$, entonces

$$\left(\left\lceil \frac{q + p - 1}{pq} \right\rceil + \left\lceil \frac{q - 1}{pq} \right\rceil - 1 \right) pq = (1 + 1 - 1)pq = pq$$

Por lo tanto,

$$\kappa_G(q + p - 1, q - 1) = \min \{ 2q + p - 3, 2q - 2, 2q, pq \} = 2q - 2.$$

Ahora se probará que $\mu_G(q + p - 1, q - 1) = 2q$. Para ello se deben establecer las siguientes desigualdades:

$$\mu_G(q + p - 1, q - 1) \leq 2q \quad (3.3.2) \quad \mu_G(q + p - 1, q - 1) \geq 2q \quad (3.3.3)$$

Desigualdad (3.3.2).

Para probar esta desigualdad se construirán un par de subconjuntos A y B de G tal que $|A| = q + p - 1$, $|B| = q - 1$ y $|AB| = 2q$.

En el producto semidirecto $G = \mathbb{Z}_q \rtimes \mathbb{Z}_p$, denótese con H_q el único subgrupo de G de cardinalidad q . Considérese un subconjunto B de H_q tal que $|B| = q - 1$, y para toda $a \notin H_q$, un subconjunto A de $H_q \cup aH_q$ tal que $|A| = p + q - 1$. Dado que $A \subset H_q \cup aH_q$ y $B \subset H_q$ se sigue que $AB \subset (H_q \cup aH_q)H_q$, además por la prueba de la Proposición 2.7 se tiene que $AB \subset H_q \cup aH_q$. Ahora, puesto que $|A| = p + q - 1$, $|H_q| = |aH_q| = q$ y $p \geq 3$, entonces $|A| \geq q + 2$. Por el principio del palomar, las clases laterales H_q y aH_q contienen cada una por lo menos 2 elementos de A . El Lema 3.3 garantiza que $\underbrace{(A \cap H_q)}_{A_1} B = H_q$ y $\underbrace{(A \cap aH_q)}_{A_2} B = aH_q$. Finalmente observe que se cumple la ecuación $AB = H_q \cup aH_q$. En efecto,

$$\begin{aligned} \underbrace{[(A \cap H_q)B]}_{H_q} \cup \underbrace{[(A \cap aH_q)B]}_{aH_q} &= [(A \cap H_q) \cup (A \cap aH_q)]B \\ &= [A \cap (H_q \cup aH_q)]B \\ &= AB. \end{aligned}$$

Entonces, $AB = H_q \cup aH_q$ y $|AB| = |H_q \cup aH_q| = 2q$. Por lo tanto, $\mu_G(r, s) \leq 2q$.

Desigualdad (3.3.3).

Supóngase que existen dos subconjuntos A' y B' de G tales que $|A'| = q + p - 1$, $|B'| = q - 1$ y $|A'B'| < 2q$. Entonces se tiene $|A'B'| - |A'| < 2q - (q + p - 1) = q - p + 1$, y como $p \geq 3$ se sigue que $q - p + 1 \leq |B'| - 1 = q - 2$. Se deduce del Corolario 3.1 que existe un subgrupo propio N_1 de G que es un 1-núcleo para B' o para B'^{-1} tal que

$$\lambda_1(B') = \left(\left\lceil \frac{q-1}{|N_1|} \right\rceil - 1 \right) |N_1| < q - p + 1. \quad (3.3.4)$$

Ahora, puesto que $\mathcal{H}(G) = \{1, p, q, pq\}$, entonces se pueden calcular los posibles valores de la función $\lambda_1(B')$. El subgrupo $N_1 = \{1\}$ de cardinal $|N_1| = 1$ no satisface la expresión (3.3.4) porque $p \geq 2$ y $q - p + 1 \leq |B'| - 1 = q - 2$. Por otro lado, el grupo G no es una 1-celda porque $G \in C_B^0 = \{\emptyset, G\}$, luego hay dos posibilidades para el cardinal de N_1 , $|N_1| = q$ o $|N_1| = p$.

Primer caso. Si se tiene $|N_1| = q$, puesto el grupo G tiene un único subgrupo de cardinal q , el 1-núcleo N_1 es el subgrupo normal H_q . Por lo tanto el subgrupo H_q es un 1-núcleo para B' y para B'^{-1} , esto es, $\lambda_1(B') = \lambda_1(B'^{-1})$. Luego se tiene que

$$\lambda_1(B') = |H_q B'| - |H_q| = \left(\left\lceil \frac{q-1}{q} \right\rceil - 1 \right) q = (1-1)q = 0.$$

Esto implica que $|H_q B'| = |H_q|$, lo que significa que en la expresión

$$H_q B' = \bigcup_{b \in B'} H_q b = H_q b_1 \cup H_q b_2 \cup \dots \cup H_q b_{q-1},$$

las clases laterales son iguales, esto es, para todo $s, t \in B'$ se tiene $H_q s = H_q t$. Luego existe $b \in B'$ tal que $B' \subset H_q b$.

Por otro lado, existen $a_1, a_2, \dots, a_p$ elementos en G tal que $G = \bigcup_{i=1}^p a_i H_q$, entonces

$$A' = A' \cap G = A' \cap \left(\bigcup_{i=1}^p a_i H_q \right) = \bigcup_{i=1}^p \left(\underbrace{A' \cap a_i H_q}_{A'_i} \right) = \bigcup_{i=1}^p A'_i.$$

Se sigue que el conjunto A' se puede considerar como la unión disjunta de sus mismas intersecciones con todas las clases laterales modulo H_q en G . Ahora, puesto que el $\max\{|A'_i| : i \in \{1, 2, \dots, p\}\}$ es q , y $|A'| = p + q - 1$, entonces por lo menos dos de los conjuntos A'_i son no vacíos. Por lo tanto, el producto $A'B'$ es la unión disjunta

$$A'B' = \left(\bigcup_{i=1}^p A'_i \right) B'.$$

Sin pérdida de generalidad, supóngase que A'_1, A'_2, A'_3 son no vacíos, entonces se tiene que $(A'_1 \cup A'_2 \cup A'_3)B' \subset A'B'$, es decir, $A'_1 B' \cup A'_2 B' \cup A'_3 B' \subset A'B'$. Entonces

$$\begin{aligned} |A'B'| &\geq |A'_1 B'| + |A'_2 B'| + |A'_3 B'| \\ &\geq |B'| + |B'| + |B'| \\ &= 3|B'| = 3(q-1) > 2q, \end{aligned}$$

lo cual contradice el hecho que $|A'B'| < 2q$. Se deduce de aquí que exactamente dos de los A'_i con $i \in \{1, 2, 3\}$ son no vacíos. Sin pérdida de generalidad supóngase que

estos dos conjuntos son A'_1 y A'_2 , por el principio del palomar, los conjuntos A'_1 y A'_2 deben contener cada uno al menos dos elementos. Se puede observar que A'_1 y A'_2 son subconjuntos de una clase lateral izquierda a_1H_q y a_2H_q respectivamente. Luego, por el Lema 3.3 se tiene que $A'_1B' = (A' \cap a_1H_q)B' = a_1H_q$ y $A'_2B' = (A' \cap a_2H_q)B' = a_2H_q$. Se sigue de estas dos igualdades que

$$A'B' = A_1B' \cup A_2B' = a_1H_q \cup a_2H_q.$$

Por lo tanto, $|A'B'| = 2q$. Esto contradice lo que inicialmente se había supuesto, lo que significa que $(|N_1| \neq q)$.

Segundo caso. Supóngase que $|N_1| = p$, entonces se tiene

$$\lambda_1(B') = \left(\left\lceil \frac{q-1}{p} \right\rceil - 1 \right) p = q - 1 - p.$$

Además, por Teorema 3.2 no existe ninguna a_2 -celda con $\lambda_{a_2}(B') < |B'| - 1$, luego el único valor posible sería $\lambda_{a_2}(B') = (\lceil \frac{q-1}{q} \rceil - 1)q = 0$, entonces $P_{B'}(A')$ es una j -celda con $1 \leq j < a_2$. Por otro lado, observe que A' es una j -celda para B' , es decir,

$$|A'B'| - |A'| < 2q - (p + q - 1) = q - p + 1 \leq |B'| - 1.$$

Luego por la ecuación (2.2.3) del Lema 2.5 $D_{B'}(A')$ es una j -celda para B'^{-1} . El Teorema 3.1 garantiza que el subgrupo N_1 es un 1-núcleo, ya sea para B' o B'^{-1} , se probará ahora que N_1 es un 1-núcleo para B' . En efecto, si N_1 es un 1-núcleo para B'^{-1} , entonces $D_{B'}(A')$ es una unión de clases laterales izquierdas módulo N_1 . Se sigue que $|D_{B'}(A')|$ es un múltiplo de p . Ahora, dado que $|D_{B'}(A')| = |G| - |A'B'| > pq - 2q$, se tiene la expresión

$$|D_{B'}(A')| \geq \left\lceil \frac{pq - 2q}{p} \right\rceil p = pq - 2(q - 1). \quad (3.3.5)$$

De lo anterior se tiene que $|A'B'| \leq 2(q - 1)$. Luego,

$$|A'B'| - |A'| \leq 2(q - 1) - (p + q - 1) = q - p - 1 = \lambda_1(B').$$

Se puede deducir de la última expresión que A' es una 1-celda para B' . Además,

$$|G \setminus A'| = pq - (p + q - 1) = (p - 1)(q - 1) \geq (q - 1 - p) + p = \lambda_1(B') + \beta_1(B'),$$

entonces A' satisface la condición $E_1(B)$, luego cualquier 1-núcleo para B' también cumple la condición $E_1(B')$ y el 1-núcleo para B' que contiene a 1 será un subgrupo de cardinalidad p . Por lo tanto N_1 es un 1-núcleo para B' . Dado que $\lambda_1(B) = |N_1B'| - |N_1| = q - 1 - p$ y $|B| = q - 1$, $|N_1| = p$, se tiene $|N_1B'| = |B'|$, pero $B' \subset N_1B'$, se deduce así que $N_1B' = B'$.

De acuerdo al Lema 1.2 presentado en el Capítulo 1, el grupo $G = \mathbb{Z}_q \rtimes \mathbb{Z}_p$ se puede expresar como $H_q \rtimes N_1$, tal que $H_q = \{(x, 0) : x \in \mathbb{Z}_q\}$ y $N_1 = \{(0, y) : y \in \mathbb{Z}_p\}$, donde la operación definida en G viene dada por $(a, b)(c, d) = (a + c\alpha^b, b + d)$, con $\alpha \in (\mathbb{Z}_q \setminus \{0\})$.

Ahora, dado que B' es periódico módulo N_1 se tiene $|B'| = q - 1 = |N_1|t = pt$, se sigue que B' está completamente determinado por un conjunto $B_0 \subset H_q$ de cardinal $t = \frac{q-1}{p}$. En efecto, defínase el conjunto B_0 como sigue:

$$B_0 = \{(a\alpha^{-b}, 0) \in G : (a, b) \in B', \text{ para algún } b \in \mathbb{Z}_p\}.$$

Se probará que $N_1B_0 = B'$. Sea $(a, b) \in B'$, entonces $(a\alpha^{-b}, 0) \in B_0$ y $(0, b) \in N_1$, así que $(0, b)(a\alpha^{-b}, 0) = (0 + a\alpha^{-b}\alpha^b, b + 0) = (a, b) \in B'$, esto es, $B' \subset N_1B_0$. Recíprocamente, sean $(0, b) \in N_1$ y $(a\alpha^{-c}, 0) \in B_0$, entonces $(0, b)(a\alpha^{-c}, 0) = (a\alpha^{b-c}, b)$, pero $b - c \in \mathbb{Z}_p$, luego $(0, b - c) \in N_1$ y como B' es periódico módulo N_1 , entonces se tiene que $(0, b - c)(a, c) = (a\alpha^{b-c}, b) \in B'$, luego $N_1B_0 \subset B'$. Por tanto, $B' = N_1B_0$. De esta forma el conjunto B' se puede expresar como sigue,

$$B' = \{(b_0\alpha^x, x) : (b_0, 0) \in B_0, x \in \mathbb{Z}_p\}.$$

Por otro lado, $P_{B'}(A')$ es una j -celda, con $1 \leq j < a_2$, luego por Proposición 3.3 se tiene $P_{B'}(A')N_1 = P_{B'}(A')$, además por Proposición 2.10 se tiene que $|P_{B'}(A')B'| - |P_{B'}(A')| \leq |A'B'| - |A'|$ y dado que A' es una 1-celda entonces $|P_{B'}(A')B'| - |P_{B'}(A')| = |A'B'| - |A'|$, por lo tanto, $|P_{B'}(A')| = |A'|$. Por Lema 2.1 $A' \subset P_{B'}(A')$ y como $P_{B'}(A')$ es finito entonces $P_{B'}(A') = A'$. Procediendo de forma similar como se hizo para el conjunto B' se tiene que $|A'| = s|N_1| = ps$, para algún $s \in \mathbb{Z}$. Por lo tanto A' está completamente determinado por un conjunto $A_0 \subset H_q$ de cardinal $s = \frac{q-1+p}{p} = \frac{q-1}{p} + 1$. En efecto, defínase el conjunto A_0 como sigue:

$$A_0 = \{(x, 0) \in G : (x, y) \in A', \text{ para algún } y \in \mathbb{Z}_p\}.$$

Se debe probar que $A' = A_0N_1$. Sea $(x, y) \in A'$, entonces $(x, 0) \in A_0$ y $(0, y) \in N_1$, luego $(x, 0)(0, y) = (x + 0\alpha^0, 0 + y) = (x, y) \in A$, de aquí que $A' \subset A_0N_1$. Recíprocamente, sea

$(x, 0) \in A_0$ y $(0, y) \in N_1$, luego existe $z \in \mathbb{Z}_p$ tal que $(x, z) \in A'$, entonces $(0, y-z) \in N_1$, así se tiene $(x, z)(0, y-z) = (x + 0\alpha^z, z + y-z) = (x, y) \in A'$, luego $A_0N_1 \subset A'$. Por lo tanto, $A_0N_1 = A'$. De esta forma se deduce que,

$$A' = \{(a_0, x) : (a_0, 0) \in A_0, x \in \mathbb{Z}_p\}.$$

Con las condiciones descritas anteriormente, se puede calcular el producto $A'B'$. Así,

$$\begin{aligned} A'B' &= \{(a_0, x)(b_0\alpha^y, y) : (a_0, 0) \in A_0, (b_0, 0) \in B_0, (x, y) \in (\mathbb{Z}_p \times \mathbb{Z}_p)\} \\ &= \{(a_0 + b_0\alpha^{x+y}, x+y) : (a_0, 0) \in A_0, (b_0, 0) \in B_0, (x, y) \in (\mathbb{Z}_p \times \mathbb{Z}_p)\} \\ &= \{(s, x) : x \in \mathbb{Z}_p, s \in (\pi(A_0) + \pi(B_0)\alpha^x)\}, \end{aligned}$$

donde π es la proyección de G en $\mathbb{Z}_q$, es decir,

$$\begin{aligned} \pi : G = \mathbb{Z}_q \times \mathbb{Z}_p &\longrightarrow \mathbb{Z}_q \\ (z, w) &\longrightarrow \pi(z, w) = z. \end{aligned}$$

Ahora, para cada $x \in \mathbb{Z}_p$, sea

$$M_x = \{(s, x) : s \in (\pi(A_0) + \pi(B_0)\alpha^x)\},$$

entonces $A'B' = \bigcup_{x \in \mathbb{Z}_p} M_x$, y $M_x \cap M_y = \emptyset$, siempre que $x \neq y$. Luego se tiene,

$$|A'B'| = \left| \bigcup_{x \in \mathbb{Z}_p} M_x \right| = \sum_{x \in \mathbb{Z}_p} |M_x| = \sum_{x \in \mathbb{Z}_p} |\pi(A_0) + \pi(B_0)\alpha^x|. \quad (3.3.6)$$

De acuerdo al Teorema de Cauchy–Davenport 1.3, para todo $x \in \mathbb{Z}_p$ se tiene que

$$|\pi(A_0) + \pi(B_0)\alpha^x| \geq |\pi(A_0)| + |\pi(B_0)\alpha^x| - 1 = |A_0| + |B_0| - 1 = \frac{2(q-1)}{p}.$$

Supóngase que existen dos valores x_1 y x_2 en $\mathbb{Z}_p$ tal que se cumple,

$$|\pi(A_0) + \pi(B_0)\alpha^{x_1}| > \frac{2(q-1)}{p} \text{ y } |\pi(A_0) + \pi(B_0)\alpha^{x_2}| > \frac{2(q-1)}{p},$$

entonces de la ecuación (3.3.6) para toda $x \in (\mathbb{Z}_p \setminus \{x_1, x_2\})$ se tiene,

$$\begin{aligned} |A'B'| &= |\pi(A_0) + \pi(B_0)\alpha^{x_1}| + |\pi(A_0) + \pi(B_0)\alpha^{x_2}| + \sum |\pi(A_0) + \pi(B_0)\alpha^x| \\ &\geq \left(\frac{2(q-1)}{p} + 1 \right) + \left(\frac{2(q-1)}{p} + 1 \right) + (p-2) \left(\frac{2(q-1)}{p} \right) = 2q, \end{aligned}$$

lo cual es una contradicción. Entonces a lo sumo un valor x_0 de $\mathbb{Z}_p$ puede dar como resultado $|\pi(A_0) + \pi(B_0)\alpha^{x_0}| > \frac{2(q-1)}{p}$. Y por lo tanto para todo $x \in (\mathbb{Z}_p \setminus \{x_0\})$ se cumple que,

$$|\pi(A_0) + \pi(B_0)\alpha^x| = |\pi(A_0)| + |\pi(B_0)\alpha^x| - 1 = |A_0| + |B_0| - 1 = \frac{2(q-1)}{p}.$$

Luego, de la expresión (3.3.6) se tiene

$$\begin{aligned} |A'B'| &= |\pi(A_0) + \pi(B_0)\alpha^{x_0}| + \sum |\pi(A_0) + \pi(B_0)\alpha^x| \\ &\geq \left(\frac{2(q-1)}{p} + 1\right) + (p-1) \left(\frac{2(q-1)}{p}\right) = 2q - 1. \end{aligned}$$

Pero esto contradice la ecuación (3.3.5), la cual afirma que $|A'B'| \leq 2q - 2$. Finalmente para todo $x \in \mathbb{Z}_p$ se debe tener

$$|\pi(A_0) + \pi(B_0)\alpha^x| = |\pi(A_0)| + |\pi(B_0)\alpha^x| - 1 = |A_0| + |B_0| - 1 = \frac{2(q-1)}{p}.$$

El Teorema de Vosper 1.5, afirma que si la ecuación anterior se cumple, entonces $\pi(A_0)$ y $\pi(B_0)\alpha^x$ son progresiones aritméticas con la misma diferencia. Por otro lado, el Lema 3.4 garantiza que la diferencia r de una progresión aritmética P de longitud $l \leq \frac{q-1}{2}$ esta determinada únicamente por su signo, y como $|\pi(B_0)\alpha^x| = \frac{q-1}{p} < |\pi(A_0)| = \frac{q-1}{p} + 1 \leq \frac{q-1}{p}$, entonces estos dos conjuntos cumplen las condiciones. Luego, denótese con r la diferencia de la progresión aritmética $\pi(A_0)$, es claro que $r \neq 0$, en caso contrario la progresión aritmética P estaría compuesta por un único elemento, lo cual no puede suceder. Se demostrará ahora que $\pi(B_0)$ es una progresión aritmética. Dado que $p \geq 3$, sean $x_1, x_2 \in \mathbb{Z}_p$ con $x_1 \neq x_2$ y considérense los conjuntos

$$\pi(B_0)\alpha^{x_1} = \{b_1\alpha^{x_1}, b_2\alpha^{x_1}, \dots, b_{\frac{q-1}{p}}\alpha^{x_1}\} \text{ y } \pi(B_0)\alpha^{x_2} = \{b_1\alpha^{x_2}, b_2\alpha^{x_2}, \dots, b_{\frac{q-1}{p}}\alpha^{x_2}\},$$

donde $b_i \in \pi(B_0)$ para toda $i \in \{1, 2, \dots, \frac{q-1}{p}\}$. Supóngase que b_i, b_{i+1} y b_j, b_{j+1} son dos elementos consecutivos de $\pi(B_0)\alpha^{x_1}$ y $\pi(B_0)\alpha^{x_2}$ respectivamente. Por el Teorema de Vosper 1.5, puesto que $\pi(A_0)$ y $\pi(B_0)\alpha^x$, $x \in \mathbb{Z}_p$, son progresiones aritméticas con la misma diferencia, entonces $b_{i+1}\alpha^{x_1} - b_i\alpha^{x_1} = r = b_{j+1}\alpha^{x_2} - b_j\alpha^{x_2}$. Ahora, como α es un elemento del campo $\mathbb{Z}_q$, entonces existe su inverso multiplicativo,

luego $(b_{i+1} - b_i) = r\alpha^{-x_1}$ y $(b_{j+1} - b_j) = r\alpha^{-x_2}$. Entonces $\pi(B_0)$ es una progresión aritmética de diferencia $r\alpha^{-x_1}$ y también de diferencia $r\alpha^{-x_2}$.

Ahora, si $r\alpha^{-x_1} = r\alpha^{-x_2}$, entonces $\alpha^{x_2-x_1} = 1$, y de aquí $x_1 = x_2$, lo cual contradice que $x_1 \neq x_2$. De otro lado, si $r\alpha^{-x_1} = -r\alpha^{-x_2}$ entonces $\alpha^{x_2-x_1} = -1$, elevando al cuadrado se tiene $(\alpha^{x_2-x_1})^2 = \alpha^{2(x_2-x_1)} = 1$. Además, como $\langle \alpha \rangle$ es cíclico, por Teorema de Lagrange $1.2 \ q - 1 | 2(x_2 - x_1)$, pero $p | q - 1$, entonces $p | 2(x_2 - x_1)$, luego $p | (x_2 - x_1)$ porque $p \nmid 2$, lo cual es una contradicción. Por lo tanto las dos diferencias no existen. Como se puede observar, por todos los lados se llega a una contradicción. Finalmente se concluye que $\mu_G(r, s) \geq 2q$. Por lo tanto, de las desigualdades (3.3.2) y (3.3.3) se tiene que

$$\mu_G(r, s) = 2q.$$

□

Apéndice A

Algoritmos en GAP 4.4.12

En el presente apéndice se muestran los algoritmos desarrollados por los autores en programación de GAP¹ 4.4.12, los cuales permiten apreciar lo complicado que resulta encontrar el valor de la función $\mu_G(r, s)$ en algunos grupos finitos no abelianos. GAP es un entorno de cálculo algebraico discreto de libre distribución que hace énfasis en la Teoría de Grupos Computacional, pero que no se restringe sólo a ella. Se puede encontrar información acerca de este software en la página oficial de GAP www.gap-system.org.

Dentro de los tópicos que atañen a la teoría aditiva de números, los métodos computacionales han resultado ser de gran utilidad debido a las mejoras en sus características, en especial las que se refieren a la velocidad del procesador. Lo dicho anteriormente se cumple también para el problema de los conjuntos suma pequeños, aunque no se puede pensar en estos métodos como una solución al problema, éstos ofrecen una forma segura de fortalecer o refutar posibles conjeturas.

Dado que los grupos de la forma $G = \mathbb{Z}_q \rtimes \mathbb{Z}_p$, donde p y q son números primos impares tales que $q \equiv 1 \pmod{p}$, son objeto de estudio del presente trabajo, se proporciona a continuación los comandos para la creación de estos grupos en el software GAP.

¹Grupos Algoritmos y Programación.

A.1. Generación del Grupo $P = \mathbb{Z}_q \rtimes \mathbb{Z}_p$

El siguiente algoritmo permite crear el grupo P como producto semidirecto de los grupos $\mathbb{Z}_q$ por $\mathbb{Z}_p$, bajo el homomorfismo formado a partir de uno de los elementos de orden p del grupo de automorfismos de $\mathbb{Z}_q$.

```

ProdSemidirecto:=function(q,p)
local Zp,Zq,au,Au,hom,P;
if (IsPrime(q) and IsPrime(p)) then
  if q mod p=1 then
    Zp:=CyclicGroup(p);
    Zq:=CyclicGroup(q);
    au:=AutomorphismGroup(Zq);
    Au:=First(Elements(au),i->Order(i)=p);
    Au:=Group(Au);
    hom:=GroupHomomorphismByImages(Zp,Au,GeneratorsOfGroup(Zp),
    GeneratorsOfGroup(Au));
    P:=SemidirectProduct(Zp,hom,Zq);
  else
    P:=List([q,"mod",p,"<>1"]);
  fi;
else
  P:=List([p,q,"no son primos"]);
fi;
return P;
end;

```

Ejemplo A.1. Dados los valores de $p = 3$ y $q = 7$, en la ventana de GAP se ve lo siguiente:

```

>P:=ProdSemidirecto(7,3);
[<pc group of size 21 with 2 generators>
>StructureDescription(P);
["C7 : C3"
>Elements(P);
[[ <identity> of ..., f1, f2, f1^2, f1*f2, f2^2, f1^2*f2, f1*f2^2, f2^3,
f1^2*f2^2, f1*f2^3, f2^4, f1^2*f2^3, f1*f2^4, f2^5, f1^2*f2^4, f1*f2^5,

```

$f2^6, f1^2*f2^5, f1*f2^6, f1^2*f2^6]$

Como resultado del procedimiento anterior se obtiene un grupo $P = \mathbb{Z}_7 \rtimes \mathbb{Z}_3$ de orden 21, el cual tiene 2 generadores. Además, el comando `StructureDescription(P)` informa sobre la estructura del grupo, en este caso es el producto semidirecto de dos grupos cíclicos de orden 7 y 3 respectivamente, y la lista de sus elementos se obtiene con `Elements(P)`.

Se presenta la tabla de Cayley para el grupo $P = \mathbb{Z}_7 \rtimes \mathbb{Z}_3$ creado en GAP de la forma mencionada, donde los elementos `<identity>of ...`, `f1` y `f2` se reemplazaron por `e`, `a`, y `b` respectivamente.

Tabla 1. Tabla de Cayley para el grupo $P = \mathbb{Z}_7 \rtimes \mathbb{Z}_3$

*	e	a	b	a ²	ab	b ²	a ² b	ab ²	b ³	a ² b ²	ab ³	b ⁴	a ² b ³	ab ⁴	b ⁵	a ² b ⁴	ab ⁵	b ⁶	a ² b ⁵	ab ⁶	a ² b ⁶
e	e	a	b	a ²	ab	b ²	a ² b	ab ²	b ³	a ² b ²	ab ³	b ⁴	a ² b ³	ab ⁴	b ⁵	a ² b ⁴	ab ⁵	b ⁶	a ² b ⁵	ab ⁶	a ² b ⁶
a	a	a ²	ab	e	a ² b	ab ²	b	a ² b ²	ab ³	b ²	a ² b ³	ab ⁴	b ³	a ² b ⁴	ab ⁵	b ⁴	a ² b ⁵	ab ⁶	b ⁵	a ² b ⁶	b ⁶
b	b	ab ²	b ²	a ² b ⁴	ab ³	b ³	a ² b ⁵	ab ⁴	b ⁴	a ² b ⁶	ab ⁵	b ⁵	a ²	ab ⁶	b ⁶	a ² b	a	e	a ² b ²	ab	a ² b ³
a ²	a ²	e	a ² b	a	b	a ² b ²	ab	b ²	a ² b ³	ab ²	b ³	a ² b ⁴	ab ³	b ⁴	a ² b ⁵	ab ⁴	b ⁵	a ² b ⁶	ab ⁵	b ⁶	ab ⁶
ab	ab	a ² b ²	ab ²	b ⁴	a ² b ³	ab ³	b ⁵	a ² b ⁴	ab ⁴	b ⁶	a ² b ⁵	ab ⁵	e	a ² b ⁶	ab ⁶	b	a	b ²	a ² b	b ³	b ³
b ²	b ²	ab ⁴	b ³	a ² b	ab ⁵	b ⁴	a ² b ²	ab ⁵	b ⁵	a ² b ³	a	b ⁶	a ² b ⁴	ab	e	a ² b ⁵	ab ²	b	a ² b ⁶	ab ³	a ²
a ² b	a ² b	b ²	a ² b ²	ab ⁴	b ³	a ² b ³	ab ⁵	b ⁴	a ² b ⁴	ab ⁶	b ⁵	a ² b ⁵	a	b ⁶	a ² b ⁶	ab	e	a ²	ab ²	b	ab ³
ab ²	ab ²	a ² b ⁴	ab ³	b	a ² b ⁵	ab ⁴	b ²	a ² b ⁶	ab ⁵	b ³	a ²	ab ⁶	b ⁴	a ² b	a	b ⁵	a ² b ²	ab	b ⁶	a ² b ³	e
b ³	b ³	ab ⁶	b ⁴	a ² b ³	a	b ⁵	a ² b ⁶	ab	b ⁶	a ²	ab ²	e	a ² b	ab ³	b	a ² b ²	ab ⁴	b ²	a ² b ³	ab ⁵	a ² b ⁴
a ² b ²	a ² b ²	b ⁴	a ² b ³	ab	b ⁵	a ² b ⁴	ab ²	b ⁶	a ² b ⁵	ab ³	e	a ² b ⁶	ab ⁴	b	a ²	ab ⁵	b ²	a ² b	ab ⁶	b ³	a
ab ³	ab ³	a ² b ⁶	ab ⁴	b ⁵	a ²	ab ⁵	b ⁶	a ² b	ab ⁶	e	a ² b ²	a	b	a ² b ³	ab	b ²	a ² b ⁴	ab ²	b ³	a ² b ⁵	b ⁴
b ⁴	b ⁴	ab	b ⁵	a ² b ²	ab ²	b ⁶	a ² b ³	ab ³	e	a ² b ⁴	ab ⁴	b	a ² b ⁵	ab ⁵	b ²	a ² b ⁶	ab ⁶	ab ²	b ³	a	a ² b
a ² b ³	a ² b ³	b ⁶	a ² b ⁴	ab ⁵	e	a ² b ⁵	ab ⁶	b	a ² b ⁶	a	b ²	a ²	ab	b ³	a ² b	ab ²	b ⁴	a ² b ²	ab ³	b ⁵	ab ⁴
ab ⁴	ab ⁴	a ² b	ab ⁵	b ²	a ² b ²	ab ⁶	b ³	a ² b ³	a	b ⁴	a ² b ⁴	ab	b ⁵	a ² b ⁵	ab ²	b ⁶	a ² b ⁶	ab ³	e	a ²	b
b ⁵	b ⁵	ab ³	b ⁶	a ² b ⁶	ab ⁴	e	a ²	ab ⁵	b	a ² b	ab ⁶	b ²	a ² b ²	a	b ³	a ² b ³	ab	b ⁴	a ² b ⁴	ab ²	a ² b ⁵
a ² b ⁴	a ² b ⁴	b	a ² b ⁵	ab ²	b ²	a ² b ⁶	ab ³	b ³	a ²	ab ⁴	b ⁴	a ² b	ab ⁵	b ⁵	a ² b ²	ab ⁶	b ⁶	a ² b ³	a	e	ab
ab ⁵	ab ⁵	a ² b ³	ab ⁶	b ⁶	a ² b ⁴	a	e	a ² b ⁵	ab	b	a ² b ⁶	ab ²	b ²	a ²	ab ³	b ³	a ² b	ab ⁴	b ⁴	a ² b ²	b ⁵
b ⁶	b ⁶	ab ⁵	e	a ² b ³	ab ⁶	b	a ² b ⁴	a	b ²	a ² b ⁵	ab	b ³	a ² b ⁶	ab ²	b ⁴	a ²	ab ³	b ⁵	a ² b	ab ⁴	a ² b ²
a ² b ⁵	a ² b ⁵	b ³	a ² b ⁶	ab ⁶	b ⁴	a ²	a	b ⁵	a ² b	ab	b ⁶	a ² b ²	ab ²	e	a ² b ³	ab ³	b	a ² b ⁴	ab ⁴	b ²	ab ⁵
ab ⁶	ab ⁶	a ² b ⁵	a	b ³	a ² b ⁶	ab	b ⁴	a ²	ab ²	b ⁵	a ² b	ab ³	b ⁶	a ² b ²	ab ⁴	e	a ² b ³	ab ⁵	b	a ² b ⁴	b ²
a ² b ⁶	a ² b ⁶	b ⁵	a ²	ab ³	b ⁶	a ² b	ab ⁴	e	a ² b ²	ab ⁵	b	a ² b ³	ab ⁶	b ²	a ² b ⁴	a	b ³	a ² b ⁵	ab	b ⁴	ab ²

Por otra parte, la Tabla 2 es creada independientemente de GAP y representa el grupo $G = \mathbb{Z}_7 \rtimes \mathbb{Z}_3$ bajo la operación $(a, b)(c, d) = (a + ca^b, b + c)$, donde $(a, b), (c, d) \in G$, $\alpha \in \mathbb{Z}_7 \setminus \{0\}$ y $\alpha^3 = 1$.

Tabla 2. Tabla de Cayley para el grupo $G = \mathbb{Z}_7 \rtimes \mathbb{Z}_3$

*	(0,0)	(0,1)	(1,0)	(0,2)	(4,1)	(2,0)	(2,2)	(1,1)	(3,0)	(4,2)	(5,1)	(4,0)	(6,2)	(2,1)	(5,0)	(1,2)	(6,1)	(6,0)	(3,2)	(3,1)	(5,2)
(0,0)	(0,0)	(0,1)	(1,0)	(0,2)	(4,1)	(2,0)	(2,2)	(1,1)	(3,0)	(4,2)	(5,1)	(4,0)	(6,2)	(2,1)	(5,0)	(1,2)	(6,1)	(6,0)	(3,2)	(3,1)	(5,2)
(0,1)	(0,1)	(0,2)	(4,1)	(0,0)	(2,2)	(1,1)	(1,0)	(4,2)	(5,1)	(2,0)	(6,2)	(2,1)	(3,0)	(1,2)	(6,1)	(4,0)	(3,2)	(3,1)	(5,0)	(5,2)	(6,0)
(1,0)	(1,0)	(1,1)	(2,0)	(1,2)	(5,1)	(3,0)	(3,2)	(2,1)	(4,0)	(5,2)	(6,1)	(5,0)	(0,2)	(3,1)	(6,0)	(2,2)	(0,1)	(0,0)	(4,2)	(4,1)	(6,2)
(0,2)	(0,2)	(0,0)	(2,2)	(0,1)	(1,0)	(4,2)	(4,1)	(2,0)	(6,2)	(1,1)	(3,0)	(1,2)	(5,1)	(4,0)	(3,2)	(2,1)	(5,0)	(5,2)	(6,1)	(6,0)	(3,1)
(4,1)	(4,1)	(4,2)	(1,1)	(4,0)	(6,2)	(5,1)	(5,0)	(1,2)	(2,1)	(6,0)	(3,2)	(6,1)	(0,0)	(5,2)	(3,1)	(1,0)	(0,2)	(0,1)	(2,0)	(2,2)	(3,0)
(2,0)	(2,0)	(2,1)	(3,0)	(2,2)	(6,1)	(4,0)	(4,2)	(3,1)	(5,0)	(6,2)	(0,1)	(6,0)	(1,2)	(4,1)	(0,0)	(3,2)	(1,1)	(1,0)	(5,2)	(5,1)	(0,2)
(2,2)	(2,2)	(2,0)	(4,2)	(2,1)	(3,0)	(6,2)	(6,1)	(4,0)	(1,2)	(3,1)	(5,0)	(3,2)	(0,1)	(6,0)	(5,2)	(4,1)	(0,0)	(0,2)	(1,1)	(1,0)	(5,1)
(1,1)	(1,1)	(1,2)	(5,1)	(1,0)	(3,2)	(2,1)	(2,0)	(5,2)	(6,1)	(3,0)	(0,2)	(3,1)	(4,0)	(2,2)	(0,1)	(5,0)	(4,2)	(4,1)	(6,0)	(6,2)	(0,0)
(3,0)	(3,0)	(3,1)	(4,0)	(3,2)	(0,1)	(5,0)	(5,2)	(4,1)	(6,0)	(0,2)	(1,1)	(0,0)	(2,2)	(5,1)	(1,0)	(4,2)	(2,1)	(2,0)	(6,2)	(6,1)	(1,2)
(4,2)	(4,2)	(4,0)	(6,2)	(4,1)	(5,0)	(1,2)	(1,1)	(6,0)	(3,2)	(5,1)	(0,0)	(5,2)	(2,1)	(1,0)	(0,2)	(6,1)	(2,0)	(2,2)	(3,1)	(3,0)	(0,1)
(5,1)	(5,1)	(5,2)	(2,1)	(5,0)	(0,2)	(6,1)	(6,0)	(2,2)	(3,1)	(0,0)	(4,2)	(0,1)	(1,0)	(6,2)	(4,1)	(2,0)	(1,2)	(1,1)	(3,0)	(3,2)	(4,0)
(4,0)	(4,0)	(4,1)	(5,0)	(4,2)	(1,1)	(6,0)	(6,2)	(5,1)	(0,0)	(1,2)	(2,1)	(1,0)	(3,2)	(6,1)	(2,0)	(5,2)	(3,1)	(3,0)	(0,2)	(0,1)	(2,2)
(6,2)	(6,2)	(6,0)	(1,2)	(6,1)	(0,0)	(3,2)	(3,1)	(1,0)	(5,2)	(0,1)	(2,0)	(0,2)	(4,1)	(3,0)	(2,2)	(1,1)	(4,0)	(4,2)	(5,1)	(5,0)	(2,1)
(2,1)	(2,1)	(2,2)	(6,1)	(2,0)	(4,2)	(3,1)	(3,0)	(6,2)	(0,1)	(4,0)	(1,2)	(4,1)	(5,0)	(3,2)	(1,1)	(6,0)	(5,2)	(5,1)	(0,0)	(0,2)	(1,0)
(5,0)	(5,0)	(5,1)	(6,0)	(5,2)	(2,1)	(0,0)	(0,2)	(6,1)	(1,0)	(2,2)	(3,1)	(2,0)	(4,2)	(0,1)	(3,0)	(6,2)	(4,1)	(4,0)	(1,2)	(1,1)	(3,2)
(1,2)	(1,2)	(1,0)	(3,2)	(1,1)	(2,0)	(5,2)	(5,1)	(3,0)	(0,2)	(2,1)	(4,0)	(2,2)	(6,1)	(5,0)	(4,2)	(3,1)	(6,0)	(6,2)	(0,1)	(0,0)	(4,1)
(6,1)	(6,1)	(6,2)	(3,1)	(6,0)	(1,2)	(0,1)	(0,0)	(3,2)	(4,1)	(1,0)	(5,2)	(1,1)	(2,0)	(0,2)	(5,1)	(3,0)	(2,2)	(2,1)	(4,0)	(4,2)	(5,0)
(6,0)	(6,0)	(6,1)	(0,0)	(6,2)	(3,1)	(1,0)	(1,2)	(0,1)	(2,0)	(3,2)	(4,1)	(3,0)	(5,2)	(1,1)	(4,0)	(0,2)	(5,1)	(5,0)	(2,2)	(2,1)	(4,2)
(3,2)	(3,2)	(3,0)	(5,2)	(3,1)	(4,0)	(0,2)	(0,1)	(5,0)	(2,2)	(4,1)	(6,0)	(4,2)	(1,1)	(0,0)	(6,2)	(5,1)	(1,0)	(1,2)	(2,1)	(2,0)	(6,1)
(3,1)	(3,1)	(3,2)	(0,1)	(3,0)	(5,2)	(4,1)	(4,0)	(0,2)	(1,1)	(5,0)	(2,2)	(5,1)	(6,0)	(4,2)	(2,1)	(0,0)	(6,2)	(6,1)	(1,0)	(1,2)	(2,0)
(5,2)	(5,2)	(5,0)	(0,2)	(5,1)	(6,0)	(2,2)	(2,1)	(0,0)	(4,2)	(6,1)	(1,0)	(6,2)	(3,1)	(2,0)	(1,2)	(0,1)	(3,0)	(3,2)	(4,1)	(4,0)	(1,1)

Las Tablas 1 y 2 permiten observar, con ayuda de las casillas resaltadas, la correspondencia entre los elementos de P y G . En consecuencia se tiene que el grupo P generado con GAP, es isomorfo al grupo $G = \mathbb{Z}_7 \rtimes \mathbb{Z}_3$.

Observación A.1. La Tabla 1 se obtuvo con el siguiente algoritmo:

```

tabla_p:=function(Gr)
local i,j,m,h;
m:=Elements(Gr);
for i in m do
  for j in m do
    h:=i*j; Print (h,",");
  od;
  Print(";", "\n");
od;
end;

```

A.2. Función $\kappa_G(r, s)$

La pregunta 3.1 también se responde parcialmente con ayuda de los siguiente algoritmos, probados en el grupo $\mathbb{Z}_7 \rtimes \mathbb{Z}_3$ entre otros.

Las funciones, `eSubcon` y `ListOrd`, se han creado para encontrar el conjunto $\mathcal{H}(G)$.

Función subconjuntos `eSubcon`

La función `eSubcon` encuentra todos los subconjuntos de cardinal `u` del grupo `Gr` donde la identidad del grupo está en cada uno de ellos.

```
eSubcon:=function(Gr,u)
local i,L,M;
L:=Set(Gr); SubtractSet(L,[L[1]]);
M:=Combinations(L,u-1);
for i in M do
  AddSet(i,Set(Gr)[1]);
od; return M;
end;
```

Función `ListOrd`

`ListOrd` construye el conjunto $\mathcal{H}(G)$ para el grupo `Gr` recurriendo a la función `eSubcon(Gr,u)`, donde el argumento `u` es reemplazado sucesivamente por los divisores del orden del grupo, ya que sólo se busca los ordenes de los posibles subgrupos en G .

```
ListOrd:=function(Gr)
local g,i,j,hq,gr1,Cn,L,Pr;
Cn:=Set(Gr); hq:=Set([]); g:=Order(Gr); L:=Set(DivisorsInt(g));
SubtractSet(L,[1,g]);
for i in L do
  gr1:=eSubcon(Gr,i);
  for j in gr1 do
    Pr:=IsSubgroup(Gr,AsGroup(j));
    if Pr then hq:=Union(hq,[Number(j)]); break; fi;
  od; AddSet(hq,1); AddSet(hq,g);
od; return hq;
```

```
end;
```

Función techo

Esta función corresponde a la presentada en la Definición 1.8.

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

Función Funkappa_1

Cuando un grupo finito G es abeliano o diédrico, el conjunto $\mathcal{H}(G)$ coincide con los divisores del orden del grupo (ver [8]); por lo tanto, para calcular la función $\kappa_G(r, s)$ en éstos grupos se emplea `Funkappa_1` ya que la lista de los divisores, se obtiene fácilmente con `L:=DivisorsInt(g)` donde g es el orden de Gr .

```
Funkappa_1:=function(Gr,r,s)
local g, i,L,K_, N_;
g:=Order(Gr);
if r+s>g then return g; else N_:=g; L:=DivisorsInt(g);
for i in L do
  K_:=(Ceill(r,i)+Ceill(s,i)-1)*i;
  if K_<N_ then N_:=K_; fi;
od;
return N_;
fi;
end;
```

Función Funkappa_2

Las bibliotecas de GAP permiten obtener subgrupos de un grupo finito con la función `Subgroup(Gr, [gens])`, donde `gens` son los generadores del grupo Gr , luego el conjunto $\mathcal{H}(G)$ se puede obtener para grupos con dos generadores y finalmente obtener $\kappa_G(r, s)$.

```

FunKappa_2:=function(Gr,r,s)
local gr,i,j,L,JS,Sb,N_,K_;
gr:=Order(Gr);
if r+s>gr then return gr;
else
N_:=gr;
L:=Elements(Gr); JS:=Set([]);
for i in L do
  for j in L do
    Sb:=Subgroup(Gr,[i,j]);
    JS:=Union(JS,[Order(Sb)]);
  od;
od;
for i in JS do
  K_:=Ceill(r,i)+Ceill(s,i)-1*i;
  if K_<N_ then
    N_:=K_;
  fi;
od;
return N_;
fi;
end;

```

Función FunKappa_3

De manera similar que FunKappa_2, la función FunKappa_3 encuentra el valor de la función $\kappa_G(r, s)$ para grupos finitos con tres generadores.

```

FunKappa_3:=function(Gr,r,s)
local gr,i,j,k,L,JS,Sb,N_,K_;
gr:=Order(Gr);
if r+s>gr then return gr;
else
N_:=gr;
L:=Elements(Gr); JS:=Set([]);
for i in L do
  for j in L do

```

```

        for k in L do
            Sb:=Subgroup(Gr,[i,j,k]);
            JS:=Union(JS,[Order(Sb)]);
        od;
    od;
od;
for i in JS do
    K_:=Ceill(r,i)+Ceill(s,i)-1)*i;
    if K_<N_ then
        N_:=K_;
    fi;
od;
return N_;
fi;
end;

```

Sin embargo, para grupos con cuatro o más generadores, el número de operaciones se incrementa de forma exponencial, ya que dicho número es proporcional a $|G|^n$, donde n representa el número de generadores, por lo que se presenta la siguiente función.

Función Funkappa_4

Para todo grupo finito G , la función `Funkappa_4` encuentra el conjunto $\mathcal{H}(G)$, recurriendo a la función `ListOrd(Gr)`, explicada al principio del apéndice, y bota el resultado de la función $\kappa_G(r, s)$ para valores r y s dados.

```

Funkappa_4:=function(Gr,r,s)
local g, i,L,K_, N_;
g:=Order(Gr);
if r+s>g then return g; else
N_:=g; L:=ListOrd(Gr);
for i in L do
    K_:=Ceill(r,i)+Ceill(s,i)-1)*i;
    if K_<N_ then N_:=K_; fi;
od;
return N_;
fi;
end;

```

Función kappa generalizada Funkappa_

$\text{Funkappa}_-(\text{Gr}, r, s)$ generaliza la función $\kappa_G(r, s)$, aplicando alguno de los algoritmos anteriores al grupo Gr , según la clasificación que se muestra en las siguientes líneas.

```

Funkappa_:=function(Gr,r,s)
local R;
if IsAbelian(Gr) then
  R:=Funkappa_1(Gr,r,s);
elif Number(GeneratorsOfGroup(Gr))=2 then
  R:=Funkappa_2(Gr,r,s);
elif Number(GeneratorsOfGroup(Gr))=3 then
  R:=Funkappa_3(Gr,r,s);
else
  R:=Funkappa_4(Gr,r,s);
fi;
return R;
end;

```

Ejemplo A.2. El resultado de la función $\kappa_P(3, 4)$ para el grupo $P = \mathbb{Z}_7 \rtimes \mathbb{Z}_3$ es:

```

>Funkappa_(P,3,4);
[6

```

Además, para valores de $r = p + q - 1 = 7 + 3 - 1 = 9$ y $s = q - 1 = 7 - 1 = 6$, la función $\kappa_P(9, 6)$ da el siguiente resultado,

```

>Funkappa_(P,9,6);
[12

```

El desarrollo de la Sección 3.3 permite mostrar que para este ejemplo el valor de la función $\kappa_P(9, 6) = 12 < 14 = \mu_P(9, 6)$

A.3. Función $\mu_G(r, s)$ para Grupos en General

Función cardinal del producto AB

Esta función toma como argumentos dos subconjuntos A y B de el grupo G , y posteriormente multiplica uno a uno sus elementos para obtener el conjunto AB . como resultado devuelve el cardinal del conjunto así obtenido.

```

CardiAB:=function(A,B)
local i,j,A_B,H;
A_B:=Set([]);
for i in A do
  for j in B do
    H:=i*j;
    A_B:=Union(A_B,[H]);
  od;
od;
return Number(A_B);
end;

```

Función $\mu_G(r, s)$

La función $\mu_G(r, s)$ que se presenta es un algoritmo de búsqueda exhaustiva, ya que debe probar uno a uno todos los productos de los subconjuntos obtenidos de G con cardinal r y todos los de cardinal s , para posteriormente devolver el cardinal mas pequeño encontrado.

```

FunMu:=function(Gr,r,s)
local n,m,g1,g2,GS,A,B,l,i,j;
GS:=Set(Gr); l:=Number(GS);
g1:=Combinations(GS,r);
g2:=Combinations(GS,s);
for i in g1 do
  for j in g2 do
    m:=CardiAB(i, j);
    if m<l then
      l:=m; Print (l," ",i," ",j,"\n");
    end if;
  od;
od;

```

```

    fi;
  od;
od;
return [1];
end;

```

Ejemplo A.3. Se encontrará el valor de $\mu_P(3,4)$ para el grupo $P = \mathbb{Z}_7 \rtimes \mathbb{Z}_3$.

```

>FunMu(P,3,4);
8,[ <identity> of ..., f1, f2 ],[ <identity> of ..., f1, f2, f1^2 ]
6,[ <identity> of ..., f1, f1^2 ],[ <identity> of ..., f1, f2, f1^2 ]
[ 6 ]

```

Además de encontrar el cardinal más pequeño del conjunto AB , se muestran dos conjuntos que satisfacen la ecuación $\kappa_P(3,4) = \mu_P(3,4)$.

Pero, para determinar el valor $\mu_P(9,6)$ se deben realizar

$$\binom{21}{9} \times \binom{21}{6} \times 9 \times 6 \approx 8,61 \times 10^{11}$$

operaciones, y se ha calculado aproximadamente ², que en este grupo la función $\text{FunMu}(P,9,6)$ realiza 4.63×10^6 operaciones por minuto, es decir que es necesario alrededor de 3200 horas o 130 días para realizar todo el cálculo.

A.4. Herramientas Aditivas

En seguida se definen los algoritmos auxiliares que serán utilizados para programar las herramientas aditivas.

Función subconjuntos de G SetB

Para encontrar un subconjunto B de G , tal que $1 \in B$, con un cardinal u , se emplea el algoritmo que se muestra a continuación:

²Utilizando un procesador de 2.53 GHz y 4 GB de RAM

```

SetB:=function(Gr,u)
local Pi,Si;
Pi:=Set(Gr);
if u>Number(Pi) then Print ("u debe ser menor"); else
Si:=[Pi[1]];
while Number(Si)<u do
  Si:=Union(Si,[Random(Gr)]);
od;
return Si;
fi;
end;

```

el cual construye una lista con elementos escogidos de forma aleatoria mas la identidad, por ejemplo $B:=\text{SetB}(G,3)$ fija un subconjunto B de G de cardinal 3 y tal que la identidad del grupo esta en B .

Función producto de X por B , ProdXB

Esta función permite calcular el conjunto $AB \subseteq G$.

```

ProdXB:=function(A,B)
local p,Pr,H,i,j;
Pr:=Set([]);
for i in A do
  for j in B do
    H:=i*j;
    Pr:=Union(Pr,[H]);
  od;
od;
return Pr;
end;

```

Función cálculo de B^{-1} SetBinv

El resultado de $\text{SetBinv}(Gr,Bset)$ es el conjunto B^{-1} para un conjunto B representado por $Bset$.

```

SetBinv:=function(Gr,Bset)
local i, j, Hr, Binvset;
Hr:=Set(Gr);
Binvset:=Set([]);
for i in Hr do
  for j in Bset do
    if (i*j= Set(Gr)[1]) then
      Binvset:=Union(Binvset, [i]);
    fi;
  od;
od;
return Binvset;
end;

```

Función $P_B(X)$

Esta función permite encontrar el conjunto C_B para un subconjunto X de G dados B y G .

```

FunP_BX:=function(Gr,Bset,Xset)
return Difference(Gr,ProdXB(Difference(Gr,ProdXB(Xset,Bset)),SetBinv(Gr,Bset)));
end;

```

Función $D_B(X)$

Para calcular $D_B(X)$ dados los subconjuntos X, B en G .

```

FunD_BX:=function(Gr,Bset,Xset)
return Difference(Gr,ProdXB(Xset,Bset));
end;

```

Función $\Phi_B(X)$

Esta función permite obtener el número isoperimétrico para todo subconjunto X de G , y además, la secuencia isoperimétrica cuando actúa sobre el conjunto C_B .

```

FunPhi_BX:=function(Bset,Xset)

```

```
return Number(ProdXB(Xset,Bset))-Number(Xset);
end;
```

Observación A.2. Todos los algoritmos programados pueden ser copiados en algún procesador de texto y guardados en un archivo con el formato `nombrearchivo.g`, para ser leídos posteriormente desde su ubicación. En las dos primeras líneas del ejemplo siguiente se muestra como llamar los archivos desde una sesión abierta de GAP.

Ejemplo A.4. Los siguientes procedimientos permiten encontrar el conjunto C_B .

```
>dir:=Directory("D:/TesisGap");;
>Read(Filename(dir,"ProductoSemidirecto.g"));
>Read(Filename(dir,"Isoperimetricas.g"));
>P:=ProdSemidirecto(7,3);
[<pc group of size 21 with 2 generators>
#Desde aquí empieza el procedimiento para encontrar las celdas.
#Conjuntos B
>B:=SetB(P,5);
#L1 es la colección de subconjuntos del grupo P y g es el número de estas.
>L1:=Combinations(Set(P));; g:=Number(L1);
[2097152
#Con el siguiente procedimiento se encuentra el conjuntos C_B de celdas de B.
#Como también el número de celdas para B dado.
>C_B:=Set([]); for i in L1 do
  C_B:=Union(C_B,[FunP_BX(P,B,i)]);
od; h:=Number(C_B);
[[ ]
[14905
```

Aproximadamente luego de 5 horas se obtiene el conjunto C_B , con 14905 elementos. Los comandos `SubtractSet(C_B,[Set(P)])`; y `SubtractSet(C_B,[[]])`; eliminan de C_B las 0-celdas.

Ejemplo A.5. Para encontrar la secuencia isoperimétrica se escriben las siguientes instrucciones, luego de la última línea del ejemplo anterior.

```

>mi:=Set([]); for i in C_B do
  mi:=Union(mi,[FunPhi_BX(B,i)]);
od;
>ssiso:=mi; #esta línea imprime la secuencia isoperimétrica
[[ 4, 6, 7, 8, 9, 10, 11, 12 ]

```

Además, con el siguiente proceso se encuentran las 1-celdas de B :

```

>UnoCeld:=List([]); for i in C_B do
if FunPhi_BX(B,i)=ssiso[1] then
Add(UnoCeld,i);
fi;
od;Number(UnoCeld);
[[ ]
[42

```

con la línea `Number(UnoCeld)`, se sabe que hay 42 elementos y para listarlos se debe escribir `UnoCel`; luego de lo cual se vera en la pantalla la lista de las 1-celdas para B .

Ejemplo A.6. Los siguientes procedimientos permiten establecer una conjetura respecto a la cardinalidad de C_B y su relación con la secuencia isoperimétrica.

```

#Para cargar los archivos necesarios
dir:=Directory("D:/TesisGap");;
Read(Filename(dir,"ProductoSemidirecto.g"));
Read(Filename(dir,"Isoperimetricas.g"));
Read(Filename(dir,"FunKappa.g"));
P:=ProdSemidirecto(5,2);; #Crea el Grupo P.
B:=eSubcon(P,3);;#Subconjuntos de P con cardinal 3, identidad en P.
L:=Combinations(Set(P));; #todos los subconjuntos de P.

```

De la siguiente manera se calculan los cardinales de todas las posibles colecciones C_B .

```

card:=Set([]);
for p in B do C_B1:=Set([]);
for h in L do
C_B1:=Union(C_B1,[FunP_BX(P,p,h)]);

```

```

od;
c1:=Number(C_B1)-2; #2 representa las 0-celdas
if not(c1 in card) then
card:=Union(card,[c1]);
fi;
od;

```

El resultado obtenido después de escribir `card;` es `[ 120, 142 ]`. Luego se imprimen todas las secuencias isoperimétricas para las cuales el cardinal de C_B tiene uno de los cardinales encontrados.

```

for i in B do
C_B:=Set([]);
for j in L do
C_B:=Union(C_B,[FunP_BX(P,i,j)]);
od;
SubtractSet(C_B,[Set(P)]); SubtractSet(C_B,[[]]);
if Number(C_B)=142 then #Este valor es uno de [ 120, 142 ]
mi:=Set([]);
for h in C_B do
phi:=FunPhi_BX(i,h);
if not(phi in mi) then
mi:=Union(mi,[phi]);
fi;
od;
Print (mi,i,"\n"); fi;
od;

```

El resultado en este caso es la secuencia `[ 0, 2, 4 ]` y se repite seis veces, lo que nos permite asegurar que permanece invariante para todo $|B| = 3$ y $|C_B| = 142$. El subconjunto asociado a la secuencia aparece a la derecha de la misma.

```

[ 0, 2, 4 ][ <identity> of ..., f2, f2^2 ]
[ 0, 2, 4 ][ <identity> of ..., f2, f2^3 ]
[ 0, 2, 4 ][ <identity> of ..., f2, f2^4 ]
[ 0, 2, 4 ][ <identity> of ..., f2^2, f2^3 ]
[ 0, 2, 4 ][ <identity> of ..., f2^2, f2^4 ]
[ 0, 2, 4 ][ <identity> of ..., f2^3, f2^4 ]

```

Sea C_{B_1} la colección de celdas para B_1 y C_{B_2} la colección asociada al subconjunto B_2 , es de especial interés probar que $C_{B_1} \neq C_{B_2}$, y para ello se emplean las siguientes instrucciones:

```
#dos conjuntos B tomados del resultado anterior
>B1:=( [Set(P) [1],Set(P) [3],Set(P) [5]] ); B2:=( [Set(P) [1],Set(P) [3],Set(P) [7]] );
[ <identity> of ..., f2, f2^2 ]
[ <identity> of ..., f2, f2^3 ]
```

Se crean las celdas para B_1 y B_2 .

```
>C_B1:=Set( [] );
for j in L do
C_B1:=Union(C_B1, [FunP_BX(P,B1,j)]);
od;
C_B2:=Set( [] );
for j in L do
C_B2:=Union(C_B2, [FunP_BX(P,B2,j)]);
od;
od;
```

Si se toma un elemento al azar de C_{B_1} se puede ver fácilmente si se encuentra en C_{B_2} ;

```
>C_B1[76] in C_B2;
[false
```

ya que la respuesta es negativa se tiene que C_{B_1} , en general, no tiene los mismos elementos que C_{B_2} .

Problemas Abiertos y Conclusiones

Problemas Abiertos

- Utilizar la teoría del método isoperimétrico para tratar de encontrar una función numérica que modele $\mu_G(r, s)$ en algunos grupos finitos no abelianos.
- Adaptar la teoría del método isoperimétrico dentro de la programación de GAP, con el propósito de crear un algoritmo de mayor eficiencia que permita encontrar el valor de $\mu_G(r, s)$ en grupos finitos no abelianos.
- Utilizar la teoría del método isoperimétrico para tratar de caracterizar los subconjuntos A y B de un grupo finito no abeliano G de cardinales $|A| = r$ y $|B| = s$ tales que $|AB| = \mu_G(r, s)$.

Conclusiones

- Se presenta en forma general y explícita la teoría del método isoperimétrico para un público con una formación no tan fuerte en el tema. Además, se considera que este trabajo busca una forma novedosa de acercarse al estudio de $\mu_G(r, s)$.
- Para grupos de la forma $G = \mathbb{Z}_q \rtimes \mathbb{Z}_p$ donde p y q son números primos impares tales que $q \equiv 1 \pmod{p}$, la teoría del método isoperimétrico permite concluir que $\mu_G(q + p - 1, p - 1) = 2q$, diferente al valor de $\kappa_G(r, s) = 2q - 2$.
- Para los grupos antes mencionados, computacionalmente se prueba que $\kappa_G(r, s)$ modela en general $\mu_G(r, s)$, para valores de r y s tales que $r \neq q + p - 1$ o $s \neq q - 1$.
- Dada la gran cantidad de cálculos que se presentan en el cálculo de $\mu_G(r, s)$, los algoritmos que se implementan facilitan la obtención de resultados en un tiempo relativamente pequeño para establecer posibles conjeturas.

Referencias

- [1] Alian Plagne. *Additive number theory sheds extra light on the Hopf-Stiefel $\circ$ function*. Enseign. Math. (2) **49** (2003) 109-116.
- [2] Alian Plagne. *Optimally small sumsets in general abelian groups*. Adv. in Appl. Math. **38** (2007), 324-326.
- [3] A.L. Cauchy. *Recherches sur les nombres*. J. École Polytechnique **9** (1813) 99-123.
- [4] Éric Balandraud. *Une variante de la méthode isopérimétrique de Hamidoune, appliquée au théorème de Kneser*. Annales de L'Institut Fourier **Tomé 58, No. 3** (2008) 915-943.
- [5] Éric Balandraud. *The Isoperimetric Method in Non-Abelian Groups With an Application to Optimally Small Sumsets*. International Journal of Number Theory **Vol. 4, No. 6** (2008) 927-958.
- [6] H. Davenport. *On the addition of residue classes*. J. London Math. Soc **10** (1935) 30-32.
- [7] S. Eliahou, M. Kervaire and A. Plagne. *Optimally small sumsets in finite abelian groups*. Journal of Number Theory **101** (2003) 338-348.
- [8] S. Eliahou and M. Kervaire. *Minimal sumsets in infinite abelian groups*. Journal of Algebra **287** (2005) 499-497.
- [9] S. Eliahou and M. Kervaire. *Sumsets in dihedral groups*. European Journal of Combinatorics **27** (2006) 617-628.
- [10] S. Eliahou and M. Kervaire. *Some results on minimal sumset sizes in finite non-abelian groups*. J. Number Theory **124** (2007), No. 1, 234-247. [MR2321003](#) (2008d:11022)
- [11] S. Eliahou and M. Kervaire. *Bonds on the minimal sumset size function in groups*. International Journal of Number Theory **Vol. 3, No. 4** (2007) 503-511.

-
- [12] S. Eliahou and M. Kervaire. *Minimal sumsets in finite solvable groups*. Discrete Mathematics. **310** (2010), 471-479.
- [13] W. Feit and J. G. Thompson. *Solvability of groups of odd order*. Pacific J. Math. **13** (1963), 775-1029. [MR0166261](#)
- [14] Y. Ould Hamidoune. *An Isoperimetric Method in Additive Theory*. Journal of Algebra **179** (1996) 622-630.
- [15] Y. Ould Hamidoune. *Some results in additive number theory I: The critical pair theory*. Acta Arithmetica **96** (2) (2000) 97-119.
- [16] Marshall Hall, Jr. *The Theory of Groups*. The Macmillan Company, New York, N.Y (1959). xiii+434 pp. [MR0103215](#).
- [17] W. Mutis, F. Benavides & J. Castillo. *Conjuntos Suma Pequeños en Grupos Hamiltonianos*. Revista de la Unión Matemática Argentina. **No. 1** (2012), 1-9.
- [18] Melvyn B. Nathanson. *Additive Number Theory. Inverse problems and the geometry of sumsets*. Graduate Texts in Mathematics, 165. Springer-Verlag, New York, (1996). xiv+293 pp. ISBN: 0-387-94655-1 [MR1477155](#) (**98f:11011**).

Índice alfabético

Algoritmos en GAP

- Función $\kappa_G(r, s)$, 57
- Función $\mu_G(r, s)$, 62
- Generación del grupo $P = \mathbb{Z}_q \rtimes \mathbb{Z}_p$, 54
- Herramientas aditivas, 64
- Tablas de Cayley para $P = \mathbb{Z}_7 \rtimes \mathbb{Z}_3$, 56

Definición

- k -Celda, 27
- k -Núcleo, 28
- Clases laterales, 2
- Complemento de conjuntos, 5
- Condición $E_1(B)$, 36
- Conjunto potencia, 15
- Conjunto suma, 8
- Estabilizador de un conjunto, 12
- Grupo, 2
- Grupo factor, 4
- Grupo soluble, 4
- Número isoperimétrico, 25
- Producto semidirecto, 5
- Secuencia isoperimétrica, 27
- Subgrupo, 2
- Subgrupo normal, 3

Función

- Función $\kappa_G(r, s)$, 5
- Función $\mu_G(r, s)$, 9
- Función D_B , 20
- Función P_B , 15
- Función techo, 5

Lema

Función P_B , 17

- Partición del grupo G , 24
- Progresión aritmética, 45
- Propiedades de $\mu_G(r, s)$, 10

Pregunta

- $\mu_G(r, s) = \kappa_G(r, s)?$, 44

Problema

- Conjuntos suma pequeños, 9
- Problema directo, 9
- Problema inverso, 9

Propiedad del conjunto suma pequeño, 12

Proposición

- C_B es estable sobre la izquierda, 18
- Desigualdad $\mu_G(r, s) > \kappa_G(r, s)$, 45
- Desigualdad fundamental, 29

Teorema

- Cauchy–Davenport, 11
- Kneser, 12
- Lagrange, 4
- Vosper, 12