Sumas de Secuencias con Pesos en Grupos Abelianos Finitos.

Luz Elimar Marchan Mendoza.

UNIVERSIDAD CENTROCCIDENTAL "LISANDRO ALVARADO"
Decanato de Ciencias y Tecnología.

Barquisimeto, 2011

Sumas de Secuencias con Pesos en Grupos Abelianos Finitos.

Por

Luz Elimar Marchan Mendoza.

Trabajo de Ascenso presentado como requisito parcial para optar
a la categoría de Agregado en el escalafón del personal
docente e investigación de la UCLA.

UNIVERSIDAD CENTROCCIDENTAL "LISANDRO ALVARADO"
Decanato de Ciencias y Tecnología.

Barquisimeto, 2011

Dedicatoria

$\mathcal{A}$

Dios mi Creador, Sustentador y Redentor.

Mi amado esposo Eduardo.

Agradecimientos

A mi amante y buen Dios, quien nos dirige y sostiene en cada instante de nuestras vidas. Gloria y Honra sean a Ti.

A lo doctores David Grynkiewicz y Oscar Ordaz por su invaluable ayuda e inspiración. Dios bendiga su intelecto.

A mi esposo Eduardo por motivarme a terminar este proyecto y apoyarme incondicionalmente en todo momento.

A la Dra. Isabel Márquez por su ayuda académica y sus consejos oportunos.

Al Departamento de Matématica del Decanato de Ciencias de la UCLA y al DFPA por su apoyo académico y financiero.

Al M.Sc. Dennys Ramos y a las doctoras Isabel Márquez y Maria Luisa Capodieci por dedicar parte de su tiempo a revisar este trabajo, en su rol como jurado evaluador.

A mis compañeros de trabajo por sus comentarios de motivación y aliento.

Mil gracias a todos los que de una u otra manera contribuyeron en la elaboración de este trabajo.

Resumen

Sea G un grupo abeliano finito, una conjetura de Hamidoune ([29]) dice

> Sea $W = w_1 \cdot \ldots \cdot w_n$ una secuencia de enteros tal que todos los términos de W, excepto a lo más uno, son primos relativos con $|G|$, y sea S una secuencia en G de longitud al menos $n + |G| - 1 \geq |G| + 1$. Si la máxima multiplicidad de los término de S es a lo más n, y $\sum_{i=1}^{n} w_i \equiv 0 \pmod{|G|}$, entonces existe un subgrupo no trivial H tal que todo elemento $h \in H$ puede ser representado como una suma ponderada de la forma $h = \sum_{i=1}^{n} w_i s_i$, con $s_1 \cdot \ldots \cdot s_n$ una subsecuencia de S.

En este trabajo se dan dos ejemplos que muestran que la Conjetura de Hamidoune no es cierta en general, sin embargo, se muestra que para $n \geq \frac{1}{2}|G|$ la conjetura es cierta, salvo para una familia de contraejemplos, los cuales se caracterizan.

Índice general

Introducción

El objeto de estudio de los problemas de suma cero son las secuencias, una secuencia es un elemento del monoide abeliano libre con base G, denotado por $\mathcal{F}(G)$. Si $S \in \mathcal{F}(G)$, S se escriben de la forma:

$$S = s_1 \cdot s_2 \cdot \ldots \cdot s_r = \prod_{g \in G} g^{\mathsf{v}_g(S)}$$

donde $s_i \in G$ y $\mathsf{v}_g(S) \geq 0$ es la *multiplicidad* de g en S.

La longitud de $S \in \mathcal{F}(G)$ es $|S| := r = \sum_{g \in G} \mathsf{v}_g(S)$ y

$$\mathsf{h}(S) := \max\{\mathsf{v}_g(S) \mid g \in G\}$$

es la *máxima multiplicidad de los términos* de S.

Una secuencia S_1 es llamada una *subsecuencia* de S si $S_1|S$ en $\mathcal{F}(G)$ (es decir, si $\mathsf{v}_g(S_1) \leq \mathsf{v}_g(S)$ para todo $g \in G$). En ocasiones, si $S_1|S$ es de longitud n, se llama a S_1 *n-subsecuencia de S.*

La *suma* de S es

$$\sigma(S) := \sum_{i=1}^{r} s_i = \sum_{g \in G} \mathsf{v}_g(S) g,$$

Una secuencia S es de *suma cero* si $\sigma(S) = 0$.

Si S es una secuencia con $|S| \geq n$, se define el conjunto suma de *n-subsecuencias de S* como

$$\Sigma_n(S) := \{\sigma(S') : S'|S, |S'| = n\}$$

y el *conjunto suma de subsecuencias* de S como

$$\Sigma(S) := \{\sigma(T) : T|S\}.$$

Básicamente los *problemas de suma cero* consisten en encontrar condiciones suficientes sobre una secuencia para que ésta posea una subsecuencia de suma cero (o equivalentemente para que $0 \in \Sigma(S)$), algunos problemas exigen que la subsecuencia tenga una longitud preestablecida (por ejemplo que $0 \in \Sigma_{|G|}(S)$), y otros han agregado una secuencia de pesos de modo que la suma ponderada (afectada por los pesos) sea cero. En los últimos años los problemas de suma cero se han extendido a encontrar condiciones suficientes sobre una secuencia para que ésta posea una subsecuencia cuya suma de un determinado elemento de G, no necesariamente el cero.

El primer resultado conocido sobre problemas de suma cero, denominado por Erdős "Lema prehistórico", es el siguiente:

> En un grupo abeliano finito G, toda secuencia de longitud $|G|$, contiene una subsecuencia de suma cero.

En 1961, Erdős, Ginzburg y Ziv ([22]) probaron uno de los teoremas básicos en el área de los problemas de suma cero al establecer que:

> En un grupo abeliano finito G, toda secuencia de longitud al menos $2|G| - 1$, contiene una $|G|$-subsecuencia de suma cero.

Este resultado actualmente se ha desarrollado mucho y ha constituido parte esencial en la teoría de factorización (ver [1] y [26]).

En 1967, Mann aporta un resultado que extiende el área de los problemas de suma cero ([8]). En vez de encontrar condiciones sobre una secuencia S para que el cero se pueda escribir como suma de una subsecuencia de S, él encuentra condiciones sobre una secuencia S para que cada elemento de un grupo G, de orden primo, se pueda escribir como la suma de una n-subsecuencia de S. Específicamente mostró que

> Si S es una secuencia en un grupo abeliano finito de orden primo, con $|S| = |G|+n-1$ y $h(S) \leq n$, entonces $G = \Sigma_n(S)$, es decir, todo elemento de G puede representarse como suma de una n-subsecuencia de S

En 1976 Olson generaliza el resultado de Mann para grupos de orden no necesariamente primo, en el caso particular $n = |G|$ ([10]).

Posteriormente empiezan a tratarse problemas de secuencias con peso, se consideran ahora dos secuencias, una secuencia de enteros W, los cuales son llamados pesos, y una secuencia S en un grupo abeliano G, se estudian condiciones para que el cero (o cualquier otro elemento de G) se escriba como suma de términos de la forma $w_i a_i$, donde los a_i forman una subsecuencia de S y los coeficientes o pesos w_i forman una subsecuencia de W.

Las variaciones con peso de los problemas de suma cero fueron iniciadas por Caro en [28] cuando conjeturó la siguiente versión con peso del teorema de Erdős-Ginzburg-Ziv:

> Sea W una secuencia de enteros de longitud al menos $|G|$, con $\sigma(W) \equiv 0$

> (mód $\exp(G)$) y sea S una secuencia en un grupo abeliano finito G. Si $|S| \geq |G|+|W|-1$, entonces $0 = \sum_{i=1}^{|G|} w_i s_i$ con $s_1 \cdot \ldots \cdot s_{|G|} | S$ y $w_1 \cdot \ldots \cdot w_{|G|} | W$.

Esta conjetura fué probada en 2006 por Grynkiewicz ([4]), después de muchos trabajos parciales [17] [27] [29] [30], Grynkiewicz ha llamado a su resultado Teorema EGZW (Erdős-Ginzburg-Ziv with weight). Desde entonces, hubo otros resultados relacionados con representación de grupos por sumas de subsecuencias con pesos ([18], [20], [21], [23] por citar algunos). En [29] Hamidoune, en un trabajo donde hace una prueba parcial de la versión con peso del teorema de Erdős-Ginzburg-Ziv, formula la siguiente conjetura, la cual es una versión con pesos del resultado de Mann antes mencionado ([8]), para grupos de orden no necesariamente primos:

> Sea G un grupo abeliano finito, no trivial, sea $W = w_1 \cdot \ldots w_n$ una secuencia de enteros con $\sigma(W) \equiv 0 \pmod{|G|}$ tal que todos, excepto a lo más un término de W, son primos relativos con $|G|$; y sea S una secuencia en G con $|S| \geq |G| + n - 1 \geq |G| + 1$. Si $\mathsf{h}(S) \leq n$, entonces existe un subgrupo no trivial H de G, tal que todo $h \in H$ puede escribirse como $h = \sum_{i=1}^{n} w_i s_i$, con $s_1 \cdot \ldots \cdot s_n | S$.

Hamidoune ha verificado su conjetura para el caso $|W| = |G|$. Si $\mathsf{h}(S) < |W|$, o si $|W| \geq |G|$, o si todos los términos de W son coprimos con $|G|$; la Conjetura de Hamidoune se sigue del Teorema EGZW, en [4].

En este trabajo se estudia la conjetura de Hamidoune y se obtienen resultados para el caso particular $|W| \geq \frac{1}{2}|G|$. Específicamente se dan dos contraejemplos, mostrando que la conjetura no es cierta en general, y se caracterizan los contraejemplos cuando $|W| \geq \frac{1}{2}|G|$.

Además de la introducción y las Conclusiones, este trabajo consta de tres capítulos.

En el primer Capítulo, se presentan los resultados clásicos de teoría aditiva. Específicamente se presentan algunos comentarios y consecuencias de Teorema de Kneser y otros resultados necesarios para una comprensión plena del enunciado del Teorema de estructura de Kemperman, el cual permite establecer dos nuevos lemas que conducen a caracterizar los contraejemplos de la conjetura de Hamidoune. También se enuncia el reciente Teorema de Devos, Goddyn y Mohar, el cual generaliza el Teorema de Kneser y ha demostrado ser una potente herramienta al tratar problemas de suma cero.

El segundo Capítulo contiene la notación y las definiciones básicas usadas en el contexto de los problemas de suma cero, se presentan los resultados que sirven de base fundamental para demostrar el resultado principal de este trabajo. Algunos resultados son presentados con su demostración, debido a que la técnica usada es ilustrativa.

El tercer y último Capítulo está dedicado al estudio de la Conjetura de Hamidoune y contiene una breve descripción de la metodología empleada en dicho estudio.

Parte de los resultados de este trabajo forman parte de la siguiente publicación

D. J. Grynkiewicz, L. E. Marchan and O. Ordaz, Representation of finite abelian group elements by subsequences sums, *Journal de Téorie des Nombres de Bordeaux*, 21 (2009), no. 3, 559–587. [6]

Capítulo 1

Teoría Aditiva

En este capítulo presentamos algunos resultados básicos de teoría aditiva, la cual, como veremos en el Capítulo 2, juega un papel muy importante a la hora de tratar problemas de suma cero. Básicamente trataremos tres teoremas que son ampliamente usados a lo largo del trabajo, estos son, el Teorema de Kneser, el Teorema de estructura de Kemperman (KST), y el Teorema de Devos, Goddyn y Mohar (DGM).

Sea G un grupo abeliano y A y B subconjuntos no vacíos de G, definimos el *conjunto suma* de A y B, denotado por $A+B$ como

$$A+B=\{a+b:\ a\in A, b\in B\}$$

como G es abeliano tenemos que $A+B=B+A$.

En general el conjunto suma de mas de dos subconjuntos de G, digamos $A_1,\cdots,A_n$, se define como

$$\sum_{i=1}^{n} A_i=\left\{\sum_{i=1}^{n} a_i:\ a_i\in A_i\right\}.$$

Cuando uno de los conjuntos es unitario, escribimos $g + A$ en lugar de $\{g\} + A$, el conjunto $g + A$ es llamado *traslación de* A.

Para $k \in \mathbb{Z}$ definimos $k \cdot A = \{ka : a \in A\}$. El cardinal del conjunto A lo denotamos por $|A|$.

Sean A y B conjuntos no vacíos de un grupo, con $|A| = m$ y $|B| = n$, sabemos que la cardinalidad de $A + B$ esta entre $\max\{m, n\}$ y mn, la teoría aditiva estudia la relación entre estas cardinalidades y la estructura de dichos conjuntos. En teoría aditiva los problemas suelen ser llamados directos o inversos.

Un problema directo es aquel donde se trata de buscar la estructura y/o propiedades de $A + B$ a partir de propiedades conocidas de A y de B, Cauchy y Davenport fueron los primeros en mostrar un problema de este tipo al encontrar una cota inferior para $|A + B|$ en términos de $|A|$ y $|B|$, donde A y B son subconjuntos de los números enteros.

Un problema inverso es aquel donde se deducen propiedades de los conjuntos A y B conociendo propiedades del conjunto suma $A + B$, el problema inverso que tradicionalmente es tratado es que si el número $|A + B|$ es "pequeño", entonces A, B y $A + B$ deben tener una estructura; existen muchos resultados que garantizan este hecho para casos particulares, por ejemplo, si A y B son conjuntos finitos con cardinalidad mayor o igual que 2 y $|A + B| = |A| + |B| - 1$, entonces se puede probar que A y B son progresiones aritméticas. Recientemente estos problemas han encontrado aplicaciones en la teoría de factorización no única.

1.1. Progresiones Aritméticas

Sean a, $b \in \mathbb{R}$, dos números reales, denotamos por $[a, b]$ al conjunto de todos los números enteros entre a y b, es decir,

$$[a, b] := \{x \in \mathbb{Z} \mid \ a \leq x \leq b\}.$$

Usamos $A \uplus B$ para indicar la unión de conjuntos A y B cuando tal unión es disjunta.

Un concepto muy importante al momento de describir la estructura de conjuntos en un grupo abeliano, con conjunto suma de cardinalidad "pequeña", es la idea de progresión aritmética.

Definición 1.1.1 *Sea G un grupo abeliano y $d \in G$ no nulo, de orden al menos $r \in \mathbb{Z}^+$. Una* progresión aritmética de longitud r, con diferencia d, *es un conjunto de la forma $A = \{a_0 + id : i \in [0, r-1]\}$, donde $a_0 \in G$. El elemento a_0 es el primer término de la progresión, y el elemento $a_0 + (r-1)d$ es el último término de la progresión, la forma en que está ordenado el conjunto A es el orden dado por d.*

Observemos que la diferencia de una progresión aritmética de longitud r es única, salvo el signo, pues éste depende de la forma en que ordenemos la progresión, por ejemplo, la progresión A dada anteriormente la podemos ordenar de modo que el primer término sea $a_0 + (r-1)d$, en este caso la diferencia de la progresión será $-d$.

Notemos también que si A es una progresión aritmética con diferencia d y $0 \in A$, entonces $A \subseteq \langle d \rangle$ (si $0 \in A$, $0 = a_0 + kd$ con $k \in [0, r-1]$, así $a_0 \in \langle d \rangle$ implicando que $A \subseteq \langle d \rangle$). Si d tiene orden infinito podemos considerar progresiones aritméticas de longitud infinita con diferencia común d, estas pueden ser de la forma $A = \{a_0 +$

$id : i \in \mathbb{Z}^+ \cup \{0\}\}$, o de la forma $A = \{a_0 + id : i \in \mathbb{Z}\}$, sin embargo, generalmente trabajamos con conjuntos finitos, de modo que las progresiones aritméticas infinitas no seran consideradas con mucha frecuencia.

Ejemplo 1.1.1 *Sea G un grupo abeliano, $d \in G$ y $H = \langle d \rangle$. Entonces toda clase módulo H es una progresión aritmética con diferencia d (Sea $g \in G$. Si d tiene orden finito, $g+H = \{g+id : i \in [0, |\langle d \rangle|-1]\}$. Si d tiene orden infinito, $g+H = \{g+id : i \in \mathbb{Z}\}$).*

Entre las propiedades aditivas de las progresiones aritméticas tenemos la siguiente, si A y B son progresiones aritméticas con diferencia común d y longitudes $|A| = r$ y $|B| = s$, respectivamente, entonces $A + B$ es una progresión aritmética con diferencia común d y longitud $|A + B| = \text{mín}\{|\langle d \rangle|, |A| + |B| - 1\}$. En efecto, sea $A = \{a_0 + id : i \in [0, r-1]\}$ y $B = \{b_0 + jd : j \in [0, s-1]\}$, entonces

$$\begin{aligned} A + B = \bigcup_{i=1}^{r-1}((a_0 + id) + B) &= \bigcup_{i=1}^{r-1}\{a_0 + b_0 + (i+j)d : j \in [0, s-1]\} \\ &= \bigcup_{i=1}^{r-1}\{a_0 + b_0 + kd : k \in [i, i+s-1]\} \\ &= \{a_0 + b_0 + kd : k \in [0, r+s-2]\} \end{aligned}$$

Así $A + B$ es una progresión aritmética de longitud $|A| + |B| - 1 = r + s - 1$ si $r + s - 1 \leq |\langle d \rangle|$, o de longitud $|\langle d \rangle|$, en caso contrario.

1.2. Conjuntos Periódicos y H-hoyos

Sea G un grupo abeliano, H un subgrupo de G y A un subconjunto de G. Es claro que $A+H$ es unión de H-clases $a+H$ con $a \in A$, además A es un subconjunto de $A+H$. Cuando $A = A+H$ decimos que A es H-periódico. A continuación la definicion formal.

Definición 1.2.1 *Sea H subgrupo de un grupo abeliano G, y A un subconjunto no vacío de G, el conjunto A se dice* H-periódico *si A es unión de clases módulo H (o H-clases), es decir, si* $A = \bigcup_{a\in A}(a+H)$.

Observemos que todo subconjunto A de G es $H-$periódico, con H el subgrupo trivial (ya que en este caso las $H-$clases son los conjuntos unitarios formados por los elementos de G), luego siempre es posible, dado un conjunto A, encontrar un subgrupo de G maximal (con respecto a la inclusión) de modo que A sea $H-$periódico. Veremos que este subgrupo maximal es único, lo que permite establecer la siguiente definición.

Definición 1.2.2 *Sea A un subconjunto no vacío de un grupo abeliano G, definimos el estabilizador de A, y lo denotamos por $\mathsf{H}(A)$, como el subgrupo maximal (con respecto a la inclusión) para el cual A es H-periódico. Si $\mathsf{H}(A) = 0$ entonces decimos que A es aperiódico, en caso contrario decimos que A es periódico.*

En el siguiente Lema probamos que $\mathsf{H}(A) = \{g \in G : g + A = A\}$, esto muestra la unicidad antes mencionada. Además se muestran algunas propiedades del estabilizador de A.

Lema 1.2.1 *Sea G un grupo abeliano, H un subgrupo de G y A un subconjunto no vacío de G entonces*

(i) A es $H-$periódico si y solo si $A+H = A$, luego $A + \mathsf{H}(A) = A$.

(ii) $\mathsf{H}(A) = \{g \in G : g + A = A\}$.

(iii) Si A *es* $H-$*periódico entonces* H *es un subgrupo de* $\mathsf{H}(A)$.

(iv) Si A *es* $H-$*periódico entonces* $A+B$ *es* $H-$*periódico, luego* $\mathsf{H}(A) \subseteq \mathsf{H}(A+B)$.

(v) $\mathsf{H}(A) = \mathsf{H}(g + A)$ *para todo* $g \in G$.

(vi) $|\mathsf{H}(A)|$ *divide a* $|A|$.

(vii) Si $A \cap \mathsf{H}(A) \neq \emptyset$*, entonces* $\mathsf{H}(A) \subseteq A$.

Demostración. (i) Si A es $H-$periódico entonces $A + H = \bigcup_{a \in A}(a + H) + H = \bigcup_{a \in A}((a + H) + H) = \bigcup_{a \in A}(a + H) = A$. Recíprocamente supongamos que $A + H = H$, si A no es $H-$periódico entonces existe $a \in A$ tal que $a + H \nsubseteq A$, contradiciendo el hecho que $a + H \subseteq A + H = A$.

$(ii), (iii)$ Sea $K = \{g \in G : g + A = A\}$, veamos que K es un subgrupo de G, es claro que $0 \in K$, además, si $k \in K$ entonces $-k \in K$, ya que $x \in -k + A \Leftrightarrow k + x \in A = k + A \Leftrightarrow x \in A$. Sean $k_1, k_2 \in K$, entonces

$$(k_1 - k_2) + A = k_1 + (-k_2 + A) = k_1 + A = A$$

por lo tanto $k_1 - k_2 \in K$ y tenemos que K es un subgrupo de G.

Claramente $A + K = A$, luego la parte $i)$ implica que A es $K-$periódico.

Sea H subgrupo de G tal que A es $H-$periódico, veamos que $H \subseteq K$.

Sea $h \in H$ entonces $i)$ implica que $h + A \subseteq H + A = A + H = A$, sea $a \in A$ entonces $a = h + (a - h) \in h + (A - h) \subseteq h + (A + H) = h + A$, luego $h + A = A$ y en consecuencia $h \in K$, por tanto $H \subseteq K$. Este hecho prueba $ii)$ y además prueba que

K es maximal, implicando que $K = \mathsf{H}(A)$.

(iv) $(A+B)+H = (A+H)+B = A+B$, luego $A+B$ es $H-$periódico.

(v) $x \in \mathsf{H}(A) \Leftrightarrow x+A = A \Leftrightarrow x+(g+A) = g+A \Leftrightarrow x \in \mathsf{H}(g+A)$.

(vi) Sabemos que $A = \bigcup_{a \in A}(a + H(A))$, sea s el número de clases distintas módulo $\mathsf{H}(A)$ tales que $A = \bigcup_{i=1}^{s}(a_i + \mathsf{H}(A))$, con $a_i \in A$, entonces

$$|A| = \mid \bigcup_{i=1}^{s}(a_i + \mathsf{H}(A)) \mid = \sum_{i=1}^{s} \mid a_i + \mathsf{H}(A) \mid = \sum_{i=1}^{s} \mid \mathsf{H}(A) \mid = s \cdot |\mathsf{H}(A)|$$

(vii) Sea $x \in A \cap \mathsf{H}(A)$, entonces $x + \mathsf{H}(A) \subseteq A$ (ya que $x \in A$), pero $x \in \mathsf{H}(A)$, asi $\mathsf{H}(A) = x + H(A) \subseteq A$. ■

Ejemplo 1.2.1 *Sea A una progresión aritmética con diferencia d en un grupo abeliano G. Si $|A| = |\langle d \rangle|$ entonces $\mathsf{H}(A) = \langle d \rangle$, en caso contrario A es aperiódico. En efecto, sea $A = \{a_0 + id : i \in [0, r-1]\}$, si $x \in \mathsf{H}(A)$, entonces para cada $i \in [0, r-1]$, existe $j \in [0, r-1]$, tal que $(a_0 + id) + x = a_0 + jd$, esto implica que $x = (j-i)d \in \langle d \rangle$, luego $\mathsf{H}(A) \subseteq \langle d \rangle$. Si $|A| = |\langle d \rangle|$ entonces $A = a_0 + \langle d \rangle$, luego $A + \langle d \rangle = A$ y tenemos que $\langle d \rangle \subseteq \mathsf{H}(A)$ implicando que $\mathsf{H}(A) = \langle d \rangle$. Si $|A| < |\langle d \rangle|$ entonces $r - 1 < |\langle d \rangle|$, supongamos que $kd \in \mathsf{H}(A)$ para algún $k \in [1, |\langle d \rangle| - 1]$. Es claro que $k \leq r-1$, de lo contrario, $a_0 + kd \notin A$ contradiciendo que $kd \in \mathsf{H}(A)$; de modo que $1 \leq r-k \leq r-1$, así $a_0 + (r-k)d \in A$, pero $(a_0 + (r-k)d) + kd = a_0 + rd \notin A$, contradiciendo el hecho que $kd \in \mathsf{H}(A)$, por tanto $k = 0$ y en consecuencia $\mathsf{H}(A) = 0$.*

Observemos que $\mathsf{H}(A)$, esto es, el estabilizador de A, es el subgrupo maximal con la propiedad de que $A = A + \mathsf{H}(A)$, hemos mostrado que si A es $H-$periódico entonces H es un subconjunto de $\mathsf{H}(A)$.

Definición 1.2.3 *Sea A un subconjunto no vacío de un grupo abeliano G y H subgrupo de G, si A no es H-periódico, cada elemento del conjunto $(A + H) \setminus A$ es llamado H-hoyo de A.*

En otras palabras los H-hoyos de A son los términos que hacen falta en A para que A sea $H-$periódico, notemos que A unido con $(A+H) \setminus A$ es siempre $H-$periódico y el número de $H-$hoyos de A es $|A + H| - |A|$.

Dado un subgrupo H de un grupo abeliano G, usaremos ϕ_H para denotar el homomorfismo canónico

$$\phi_H : G \to G/H.$$

Sea $A \subseteq G$, sabemos que $A + H = \bigcup_{a \in A} (a + H)$ y $s = |\phi_H(A)|$ es el número de clases distintas módulo H tales que $A + H = \bigcup_{i=1}^{s} (a_i + H)$, con $a_i \in A$, luego

$$|A + H| = \sum_{i=1}^{s} \mid a_i + H \mid = \sum_{i=1}^{s} \mid H \mid = s|H| = |\phi_H(A)||H|.$$

Si $H = \mathsf{H}(A)$ entonces $\phi_{\mathsf{H}(A)}(A)$ es aperiódico, esto es, $\mathsf{H}(\phi_{\mathsf{H}(A)}(A)) = \{\phi_{\mathsf{H}(A)}(0)\}$. En efecto,

$$\begin{aligned}
\phi_{\mathsf{H}(A)}(x) \in \mathsf{H}(\phi_{\mathsf{H}(A)}(A)) &\Rightarrow \phi_{\mathsf{H}(A)}(x) + \phi_{\mathsf{H}(A)}(A) = \phi_{\mathsf{H}(A)}(A) \\
&\Rightarrow \phi_{\mathsf{H}(A)}(x + A) = \phi_{\mathsf{H}(A)}(A) \\
&\Rightarrow (x + A) + \mathsf{H}(A) = A + \mathsf{H}(A) \\
&\Rightarrow x + (A + \mathsf{H}(A)) = A \\
&\Rightarrow x + A = A \\
&\Rightarrow x \in \mathsf{H}(A) \\
&\Rightarrow \phi_{\mathsf{H}(A)}(x) = \phi_{\mathsf{H}(A)}(0).
\end{aligned}$$

1.3. Comentarios sobre el Teorema de Kneser

Sean A y B conjuntos en un grupo abeliano G, como hemos dicho anteriormente, estamos interesados en encontrar una cota para $|A+B|$ en términos de $|A|$ y $|B|$. Un argumento comúnmente usado en teoría aditiva es el de traslaciones de conjuntos. Observemos que el cardinal de un conjunto es invariante bajo traslación, es decir, dado $g \in G$

$$|g + A| = |A|$$

En particular

$$|g + A + B| = |A + B|$$

Entonces al abordar problemas de cardinalidad, es indiferente considerar el conjunto A o el conjunto $g+A$, por lo que frecuentemente en lugar de trabajar con un conjunto en particular, se trabaja con traslaciones de dicho conjunto según sea conveniente (frecuentemente es conveniente que $0 \in A$), sin que se pierda generalidad. Mann demostró que cuando $|A|$ y $|B|$ son suficientemente "grandes", todo elemento de G puede ser representado como un elemento de $A + B$.

Teorema 1.3.1 (Teorema de Mann) *[9] Sea G un grupo abeliano finito y sean A y B subconjuntos de G tales que $|A| + |B| \geq |G| + 1$. Entonces*

$$A + B = G.$$

Demostración. Sabemos que $A + B \subseteq G$, veamos que $G \subseteq A + B$. Sea $g \in G$, como $|A \cup (g - B)| = |A| + |g - B| - |A \cap (g - B)| \leq |G|$, entonces $|A \cap (g - B)| \geq |A| + |B| - |G| \geq 1$. Luego $A \cap (g - B) \neq \emptyset$, así existen $a \in A$, $b \in B$ tales que $a = g - b$ o, equivalentemente, $g = a + b \in A + B$, por lo tanto $G = A + B$. $\blacksquare$

El primer resultado en teoría aditiva de grupos fué probado por Cauchy en 1813 y nuevamente en 1935, en forma independiente, por Davenport; éste da una cota inferior para $|A+B|$ cuando A y B son subconjuntos de un grupo finito de orden primo, a continuación presentamos una prueba corta de dicho resultado basada en el Teorema de Mann. Aunque generalmente es presentado para dos conjuntos, puede generalizarse para cualquier colección finita de subconjuntos usando inducción.

Teorema 1.3.2 (Teorema de Cauchy-Davenport) *[3] [7] Si $A_1, A_2, \ldots, A_n$ es una colección de subconjuntos no vacíos de $\mathbb{Z}_p$ con p primo, entonces*

$$|\sum_{i=1}^{n} A_i| \geq \text{mín}\{p, \sum_{i=1}^{n} |A_i| - n + 1\}.$$

Demostración. Haremos la prueba para dos subconjuntos A y B de $\mathbb{Z}_p$, la prueba para mas de dos conjuntos se sigue por inducción. Queremos probar que $|A+B| \geq \min\{p, |A|+|B|-1\}$. Supongamos que $|A+B| < p$. Sea $b \in B$ y consideremos el conjunto $A+B-b$, observemos que $A \subseteq A+B-b$, luego $|(A+B-b) \setminus A| = |A+B-b| - |A| = |A+B| - |A|$, además

$$A+B-b = \bigcup_{x \in B-b} (A+x)$$

Veamos que existe una biyección entre $B-b$ y el conjunto $\{A+x : x \in B-b\}$. Si $x, y \in B-b$ con $x \neq y$ y $A+x = A+y$, entonces $A+(x-y) = A$, así $0 \neq x-y \in H(A)$, luego $H(A) \neq 0$, pero el único subgrupo no trivial de $\mathbb{Z}_p$ es $\mathbb{Z}_p$, entonces $H(A) = \mathbb{Z}_p$ implicando $A = \mathbb{Z}_p$, de allí que $|A|+|B| \geq |\mathbb{Z}_p|+1$, y el Teorema 1.3.1 implica que $|A+B| = p$, contradiciendo nuestra suposición. Por lo tanto

$$|A+B| - |A| = |(A+B-b) \setminus A| = |\, (\bigcup_{b \in B-b} (A+x)) \setminus A \,| \geq |B-b| - 1 = |B| - 1.$$

En consecuencia $|A+B| \geq |A|+|B|-1$. ■

Existen muchas generalizaciones del Teorema de Cauchy-Davenport, sin embargo, la mas completa es el Teorema de Kneser, el cual da una cota inferior para $|A+B|$ relacionada con su grupo estabilizador. Este teorema es uno de los resultados fundamentales en teoría aditiva. No presentamos la demostración del Teorema de Kneser, dado que es muy extensa y no forma parte del objetivo de éste trabajo, sin embargo, este Teorema es clave para abordar muchos problemas de suma cero, por lo que haremos algunos comentarios y mostraremos algunas consecuencias del mismo.

Teorema 1.3.3 (Teorema de Kneser) *[14] [15] Sea G un grupo abeliano, y sea $A_1, A_2 \ldots A_n$ una colección de subconjuntos finitos no vacíos de G. Si $H = \mathsf{H}(\sum_{i=1}^{n} A_i)$ entonces*

$$| \sum_{i=1}^{n} \phi_H(A_i) | \geq \sum_{i=1}^{n} |\phi_H(A_i)| - n + 1.$$

Existen varias alternativas para formular el Teorema de Kneser, la siguiente proposición establece algunas de ellas.

Proposición 1.3.1 *Sea G un grupo abeliano, y sea $A_1, A_2 \ldots A_n$ una colección de subconjuntos finitos no vacíos de G. Si $H = \mathsf{H}(\sum_{i=1}^{n} A_i)$ entonces las siguientes condiciones son equivalentes*

(i) $| \sum_{i=1}^{n} \phi_H(A_i) | \geq \sum_{i=1}^{n} |\phi_H(A_i)| - n + 1.$

(ii) $| \sum_{i=1}^{n} A_i | \geq \sum_{i=1}^{n} |A_i + H| - (n-1)|H|.$

(iii) $| \sum_{i=1}^{n} A_i | \geq \sum_{i=1}^{n} |A_i| - (n-1)|H|.$

(iv) Si $\sum_{i=1}^{n} A_i$ *es aperiódico entonces* $| \sum_{i=1}^{n} A_i | \geq \sum_{i=1}^{n} |A_i| - n + 1.$

Demostración. $(i) \Rightarrow (ii)$ Multiplicando ambos lados de la desigualdad $i)$ por $|H|$ tenemos

$$| \sum_{i=1}^{n} A_i | = | \sum_{i=1}^{n} A_i + H | \geq \sum_{i=1}^{n} |A_i + H| - (n-1)|H|.$$

$(ii) \Rightarrow (iii)$ Como $A_i \subseteq A_i + H$ entonces $|A_i + H| \geq |A_i|$ luego

$$| \sum_{i=1}^{n} A_i | \geq \sum_{i=1}^{n} |A_i + H| - (n-1)|H| \geq \sum_{i=1}^{n} |A_i| - (n-1)|H|.$$

$(iii) \Rightarrow (iv)$ Como $\sum_{i=1}^{n} A_i$ es aperiódico, entonces $H = 0$, luego $|H| = 1$ y $|\phi_H(\sum_{i=1}^{n} A_i)| \, |H| \geq \sum_{i=1}^{n} |\phi_H(A_i)||H| - (n-1)|H|$ luego $iii)$ implica $|\sum_{i=1}^{n} A_i| \geq \sum_{i=1}^{n} |A_i| - (n-1)$.

$(iv) \Rightarrow (i)$ Como $H = \mathsf{H}(A)$ entonces $\phi_H(\sum_{i=1}^{n} A_i) = \sum_{i=1}^{n} \phi_H(A_i)$ es aperiódico y (iv) implica $|\sum_{i=1}^{n} \phi_H(A_i)| \geq \sum_{i=1}^{n} |\phi_H(A_i)| - n + 1$. ■

Como podemos ver, el Teorema de Kneser da la cota de Cauchy-Davenport, en caso que el conjunto suma sea aperiódico, o reduce el problema a trabajar con el grupo G/H y los conjuntos $\phi_H(A_i)$, aquí el conjunto suma $\sum_{i=1}^{n} \phi_H(A_i)$ es aperiódico y se tiene además la cota de Cauchy-Davenport.

Notemos que el Teorema de Kneser implica fácilmente el Teorema de Cauchy-Davenport, pues en $\mathbb{Z}_p$ (con p primo) el subgrupo $H = \mathsf{H}(\sum_{i=1}^{n} A_i)$ es trivial o es $\mathbb{Z}_p$ (ya que cuando G tiene orden primo, G no contiene subgrupos propios no triviales). Si $H = 0$ el Teorema de Kneser implica que $|\sum_{i=1}^{n} A_i| \geq \sum_{i=1}^{n} |A_i| - n + 1 \geq \min\{p, \sum_{i=1}^{n} |A_i| - n + 1\}$ (Proposición 1.3.1 parte iv). Si $H = \mathbb{Z}_p$ entonces $|\sum_{i=1}^{n} A_i| = |\sum_{i=1}^{n} A_i + \mathbb{Z}_p| = |\mathbb{Z}_p| = p \geq \min\{p, \sum_{i=1}^{n} |A_i| - n + 1\}$.

El Teorema de Kneser fué formulado originalmente como el enunciado equivalente dado en la Proposición 1.3.1 $ii)$, la prueba usa un argumento conocido como la $e-$transformada de Dyson del par de conjuntos A y B, dada por $A(e) = (e+A) \cup (-e+B)$ y $B(e) = (e+A) \cap (-e+B)$, la cual tiene las siguiente propiedades: $A(e) + B(e) \subseteq A + B$ y $|A(e)| + |B(e)| = |e + A| + |-e + B| = |A| + |B|$. En la prueba original se demuestra que $|A(e)+B(e)| \geq |A(e)|+|B(e)|-1$ para concluir que $|A+B| \geq |A|+|B|-1$. En [5] Grynkiewicz presenta una nueva prueba, usando una versión simplificada de la $e-$transformada de Dyson, en lugar de ella, usa los conjuntos $A(e) = A \cup B$ y $B(e) = A \cap B$, los cuales tienen las mismas propiedades de la $e-$transformada de Dyson, además utiliza el Teorema de Mann y el Teorema de Kemperman-Scherk.

A continuación hacemos algunos comentarios importantes sobre el significado y algunas implicaciones del Teorema de Kneser.

Observación 1.3.1 *Sea $A_1, \ldots, A_n$ una colección de conjuntos finitos en un grupo abeliano G y $H = \mathsf{H}(\sum_{i=1}^{n} A_i)$. Observemos las siguientes implicaciones del Teorema de Kneser.*

(i) El número total de $H-$hoyos de los A_i es $\rho = \sum_{i=1}^{n}(|A_i+H|-|A_i|)$. Esto implica que $\sum_{i=1}^{n}|A_i+H| = \sum_{i=1}^{n}|A_i|+\rho$, luego el Teorema de Kneser (ver Proposición 1.3.1 ii)) implica que

$$|\sum_{i=1}^{n} A_i| \geq \sum_{i=1}^{n}|A_i| - (n-1)|H| + \rho$$

.

(ii) Si $|\sum_{i=1}^{n} A_i| < \sum_{i=1}^{n}|A_i| - n + 1$, entonces por (i) debemos tener que $\sum_{i=1}^{n}|A_i| - (n-1)|H| + \rho < \sum_{i=1}^{n}|A_i| - n + 1$, es decir,

$$\rho < (n-1)(|H|-1)$$

Esto quiere decir que no puede haber muchos $H-$hoyos en los conjuntos A_i, o sea, los conjuntos A_i son $H-$periódicos o estan muy "cerca"de serlos, cada conjunto tiene un promedio ρ/n de a lo más $\frac{n-1}{n}|H|$ hoyos.

(iii) *Si* $|\sum_{i=1}^{n}(A_i+H)| \geq \sum_{i=1}^{n}|A_i+H|-n+2$ *entonces el Teorema de Kneser implica*

$$\begin{aligned} |\sum_{i=1}^{n} A_i| = |(\sum_{i=1}^{n} A_i) + H| = |\sum_{i=1}^{n}(A_i + H)| &\geq \sum_{i=1}^{n}|A_i + H| - n + 2 \\ &= \sum_{i=1}^{n}|A_i| + \rho - n + 2 \\ &> \sum_{i=1}^{n}|A_i| - n + 1 \end{aligned}$$

(iv) *Si* $|\sum_{i=1}^{n} A_i| \leq \sum_{i=1}^{n}|A_i| - n + 1$, *por (iii), debemos tener* $|\sum_{i=1}^{n}(A_i + H)| < \sum_{i=1}^{n}|A_i + H| - n + 2$. *En particular, si* $n = 2$, *usando* A *y* B *en lugar de* A_1 *y* A_2, *tenemos que si* $|A + B| \leq |A| + |B| - 1$, *el Teorema de Kneser implica* $|A + B| = |A + H| + |B + H| - 1$.

Sean A y B conjuntos en un grupo abeliano G. El Teorema Kemperman-Scherk relaciona el cardinal del conjunto $A+B$ con el número de representaciones que tienen los elementos de G como $a + b$ con $a \in A$ y $b \in B$.

Para $g \in G$ definimos

$$r_{A,B}(g) = |\{(a, b) \in A \times B : \ a + b = g\}|,$$

como el número de representaciones de g como una suma de un elemento de A y un elemento de B. Cuando $r_{A,B}(g) = 1$, decimos que g tiene una representación única como elemento de $A+B$. Es claro que $r_{A,B}(g) \geq 1$ si y solo si $g \in A+B$. El número de representaciones de un elemento en G también puede ser definido como

$$r_{A,B}(g) = |(g-A) \cap B| = |(g-B) \cap A|.$$

ya que si $a+b=g$, con $a \in A$ y $b \in B$, entonces $b = g-a$ es un elemento de $(g-A) \cap B$, es decir, cada representación de g define un elemento en $(g-A) \cap B$, y para cada elemento $b = g-a \in (g-A) \cap B$ existe un único $a \in A$ tal que $a+b=g$. Así $(g-A) \cap B$ es precisamente el subconjunto de todos los $b \in B$ para los cuales existe un $a \in A$ que puede ser sumado a b para obtener g, análogamente para $(g-B) \cap A$.

Ejemplo 1.3.1 *Sean A y B progresiones aritméticas con diferencia común d, $|A| = r$, $|B| = s$, sabemos que $A+B$ es una progresión aritmética de longitud $|A+B| = \min\{|\langle d\rangle|, |A|+|B|-1\}$. Si $|A|+|B|-1 \leq |\langle d\rangle|$, $|A| \geq |B|$ y ordenamos los términos de $A+B$ en el orden dado por d, comenzando con el primer término c_1 de la progresión aritmética y terminando con el ultimo término c_{s+r-1}, entonces la secuencia correspondiente al número de representaciones de cada c_i como elemento de $A+B$, es decir, la secuencia $r_{A,B}(c_1), \ldots, r_{A,B}(c_{s+r-1})$, es de la forma*

$$1, 2, \ldots, |B|-1, \underbrace{|B|, |B|, \ldots, |B|}_{|A|-|B|+1}, |B|-1, \ldots, 2, 1. \tag{1.1}$$

Ya que, si $A = \{a_0 + id : i \in [0, r-1]\}$ y $B = \{b_0 + jd : j \in [0, s-1]\}$. El conjunto $A+B$, incluyendo las repeticiones, es $A+B = \bigcup_{i=1}^{r-1}\{a_0+b_0+k_id : k_i \in [i, i+s-1]\}$ (ver Sección 1.1). Luego, si A y B estan en progresión aritmética con diferencia común d, entonces $A+B$ contiene exactamente dos elementos con representacíón única.

Teorema 1.3.4 (Teorema de Kemperman-Scherk) *[11] [19] Sean A y B subconjuntos finitos no vacíos de un grupo abeliano G, y sea r un entero. Si $|A+B| < |A| + |B| - r$, entonces $r_g(A, B) > r$ para todo $g \in A + B$*

La historia del Teorema 1.3.4 data desde 1951 cuando Moser propuso en la revista American Mathematical Monthly un problema que puede ser formulado como sigue:

> Sean A y B subconjuntos finitos del grupo toro $\mathbb{R}/\mathbb{Z}$ tales que $0 \in A \cap B$ y $r_{A,B}(0) = 1$, probar que $|A + B| \geq |A| + |B| - 1$.

En 1955 Scherk publicó una solución a dicho problema [19], la cual se puede adaptar, sin muchas modificaciones, para A y B subconjuntos de un grupo abeliano finito (no necesariamente el grupo toro) y se puede obtener el Teorema 1.3.4. Pero Kemperman ya había establecido el Teorema 1.3.4 ([11], [12]). Sin embargo en [12] Kemperman atribuye el teorema a Scherk; por otro lado, en la solución del problema de Moser, Scherk indica que el argumento sigue las ideas de un artículo que había hecho anteriormente con Kemperman. Por esta razón llamamos al Teorema 1.3.4 "Teorema de Kemperman-Scherk". El Teorema de Kemperman-Scherk puede derivarse fácilmente del Teorema de Kneser.

Otra forma de enunciar el Teorema de Kemperman-Scherk es la siguiente.

> Si A y B son subconjuntos finitos no vacíos de un grupo abeliano G, entonces $|A + B| \geq |A| + |B| - \min\{r_{A,B}(g) : g \in A + B\}$.

En efecto, sea $t = \min\{r_{A,B}(g) : g \in A+B\}$ y supongamos que $|A+B| < |A|+|B|-t$, entonces el Teorema de Kemperman-Scherk implica que $r_{A,B}(g) > t$ para todo $g \in$

$A+B$, luego $t > t$, lo cual es una contradición. Recíprocamente si $|A+B| < |A|+|B|-r$ entonces el enunciado anterior implica que $r < \text{mín}\{r_{A,B}(g) : g \in A+B\} \leq r_{A,B}(g)$ para todo $g \in G$, implicando asi el Teorema de Kemperman-Scherk. De modo que el Teorema de Kemperman-Scherk muestra que si $|A + B|$ es "pequeño", entonces los elementos en $A + B$ tienen un gran número de representaciones.

Notemos que si $|A| + |B| - 1 \geq |G|$, el Teorema de Kemperman-Scherk implica que $G = A + B$, pues si existe $g \in G$ tal que $g \notin A + B$, entonces los conjuntos A y $g - B$ son disjuntos (de otro modo existen $a \in A$ y $b \in B$ tales que $a = g - b$ implicando que $g \in A + B$), luego $|A| + |B| = |A| + |g - B| \leq |G|$, contrario a nuestra suposición. Así el Teorema de Kemperman-Scherk implica el Teorema de Mann (Teorema 1.3.1). El siguiente resultado muestra que el Teorema de Kemperman-Scherk también se cumple cuando las desigualdades son no estrictas.

Corolario 1.3.1 *Sean A y B subconjuntos finitos no vacíos de un grupo abeliano G, y sea r un entero. Si $|A + B| \leq |A| + |B| - r$, entonces $r_g(A, B) \geq r$ para todo $g \in A + B$*

Demostración. Si $r = 1$ el resultado es trivial. Sea $r > 1$ y supongamos que $r_{A,B}(g) \leq r - 1$ para algún $g \in A + B$, entonces podemos remover a lo sumo $r - 2$ elementos de B —especificamente, todos excepto un elemento de $(x - A) \cap B$— y obtenemos un par de conjuntos no vacíos A y B' con $|A + B'| \leq |A + B| \leq |A| + |B| - r \leq |A| + |B'| - 2$ y $r_{A,B'}(g) = 1$, lo que contradice el Teorema 1.3.4 en el caso $r = 2$. ■

Observación 1.3.2 *Sean A y B subconjuntos no vacíos en un grupo abeliano G,* *a continuación algunas implicaciones de algunos resultados que hemos discutido, relacionados con la cota* $|A| + |B| - 1$.

(i) *Si* $|G| \leq |A| + |B| - 1$ *entonces todo elemento en* G *puede ser representado como un elemento de* $A + B$ *(Teorema de Mann (1.3.1)).*

(ii) *Si* $|A + B| < |A| + |B| - 1$ *entonces el Teorema de Kneser implica que* $A + B$ *es periódico y el Teorema de Kemperman-Scherk implica que* $A + B$ *no puede contener un elemento con expresión única.*

(iii) *Si* $A + B$ *contiene un elemento con expresion única, entonces el Teorema de Kemperman-Scherk implica que* $|A + B| \geq |A| + |B| - 1$.

(iv) *Si* A *o* B *contienen un único elemento de alguna* $H-$*clase, entonces* $\rho \geq |H|-1$ *y de la Observación 1.3.1 parte (i),* $|A + B| \geq |A| + |B| - 1$.

(v) *Si* A *y* B *son progresiones aritméticas con diferencia común entonces* $|A+B| = |A| + |B| - 1$ *(Sección 1.1).*

De modo que el valor $|A| + |B| - 1$ *es una especie de "valor crítico", para el cual la estructura de* $A + B$ *es considerablemente diferente dependiendo de si* $|A + B|$ *está por encima o por debajo de* $|A| + |B| - 1$. *Recíprocamente si* A *y* B *o* $A + B$ *tienen determinada estructura, podemos acotar* $|A+B|$ *superior o inferiormente por* $|A|+|B|-1$. *Más adelante discutiremos la estructura de aquellos conjuntos para los cuales* $|A + B| = |A| + |B| - 1$.

1.4. Teoría de los Pares Críticos de Kemperman

En ésta sección revisaremos uno de los resultados inversos mas importantes en Teoría Aditiva, el Teorema de estructura de Kemperman (KST), éste determina todos los subconjuntos finitos, no vacíos A y B de un grupo abeliano G, tales que $|A + B| \leq |A| + |B| - 1$. En adelante, dado $A \subseteq G$, usaremos $\overline{A} := G \setminus A$ para denotar el complemento de A; notemos que

$$-\overline{A} = \overline{-A} \text{ y para todo } g \in G, \; g + \overline{A} = \overline{g + A}.$$

Del Teorema de Cauchy-Davenport, sabemos que cuando $G = C_p$ con p primo, $|A + B| \geq \min\{|G|, |A| + |B| - 1\}$. Cuando $G = \mathbb{Z}$, se ha mostrado que $|A + B| = |A| + |B| - 1$ si, y solo si A y B están en progresión aritmética con diferencia común o cuando $\min\{|A|, |B|\} = 1$ (ver [16]). El siguiente Teorema muestra que, con una pequeña excepción, esto también se cumple para $G = C_p$.

Teorema 1.4.1 (Teorema de Vosper) *[2] Sean A, $B \subseteq C_p$ con p primo, $|A| \geq |B| \geq 2$, y*

$$|A + B| = |A| + |B| - 1. \tag{1.2}$$

(i) Si $|A + B| \leq p - 2$, entonces A y B están en progresión aritmética con diferencia común.

(ii) Si $|A + B| = p - 1$, entonces $A = c - \overline{B}$ para algún $c \in G$.

Observemos que si $|B| = 1$, entonces siempre se cumple que $|A + B| = |A| = |A| + |B| - 1$. Si A y B estan en progresión aritmética con diferencia común d, entonces el conjunto suma es también una progresión aritmética de diferencia d, luego $|A+B| = |A| + |B| - 1$. Finalmente si $A = c - \overline{B}$ para algún $c \in G$, por el Teorema de Cauchy-Davenport, tenemos que $|A+B| = |(c-\overline{B})+B| \geq |B|+|\overline{B}|-1 = p-1$, pero $c \notin (c-\overline{B})+B$ (en caso contrario $0 = b - b_0$ con $b \in B$ y $b_0 \notin B$, lo cual es imposible), así $|A+B| = p-1 = |A|+|B|-1$. En consecuencia, vemos que la información estructural dada por el Teorema de Vosper describe precisamente todos los conjuntos de C_p que satisfacen (1.2).

Para determinar la estructura de todos los conjuntos A y B con $|A+B| \leq |A|+|B|-1$ es suficiente considerar unicamente los casos donde $A+B$ es aperiódico y $|A+B| = |A|+|B|-1$. Pues si $|A+B| \leq |A|+|B|-1$, el Teorema de Kneser implica (ver Observación 1.3.1)

$$|\phi_H(A+B)| = |\phi_H(A)| + |\phi_H(B)| - 1,$$

donde $H = \mathsf{H}(A+B)$ y $\phi_H(A+B)$ es aperiódico, además,

$$|A+B| = |A| + |B| - |H| + \rho,$$

donde $\rho = |A+H| - |A| + |B+H| - |B|$ es el número de H-hoyos en A y B. De modo que podemos trabajar con los conjuntos $\phi_H(A)$, $\phi_H(B)$ y $\phi_H(A)+\phi_H(B)$ en lugar de trabajar con A, B y $A+B$; y conociendo la estructura de $\phi_H(A)$ y $\phi_H(B)$, A y B pueden ser obtenidos de $A+H$ y $B+H$ eliminando los $H-$hoyos de A y B. Los pares de subconjuntos con $|A+B| = |A|+|B|-1$ son conocidos como *pares críticos*.

Observación 1.4.1 *Sean A y B subconjuntos no vacíos de un grupo abeliano G con $|A+B| \leq |A|+|B|-1$ y sean $\alpha \in A$ y $\beta \in B$, consideremos los conjuntos*

$A_\alpha = (\alpha+H)\cap A$ y $B_\beta = (\beta+H)\cap B$, donde $H = \mathsf{H}(A+B)$, entonces $|A_\alpha|+|B_\beta| \geq 2|H|-\rho \geq |H|+1$ (ya que $\rho = |A+B|-|A|-|B|+|H| \leq |H|-1$), luego el Teorema de Mann (Trasladando A_α y B_β por α y β respectivamente para aplicar el Teorema) implica que $A_\alpha + B_\beta = (\alpha+\beta)+H$, así $A_\alpha + B_\beta$ es $H-$periódico, de esta manera, $A+B$ contiene un subconjunto no trivial $H-$periódico.

A veces resulta útil considerar el caso cuando $A+B$ es periódico y tiene un elemento con expresión única, esto es, $r_{A,B}(g) = 1$. En este caso, el Teorema de Kemperman-Scherk implica que $|A+B| = |A|+|B|-1$, y tenemos las siguientes observaciones.

Observación 1.4.2 *Sean A y B subconjuntos no vacíos de un grupo abeliano G con $|A+B| \leq |A|+|B|-1$ y $A+B$ periódico conteniendo un elemento de expresión única, digamos $\alpha+\beta$, con $\alpha \in A$ y $\beta \in B$, sea $H = \mathsf{H}(A+B)$, entonces*

(i) $|A_\alpha|+|B_\beta| \leq |H|+1$, de lo contrario, $|A_\alpha + B_\beta| = |(\alpha+\beta)+H| = |H| < |A_\alpha|+|B_\beta|-1$, implicando, por el Teorema de Kemperman-Scherk que $A_\alpha+B_\beta$ no tiene elementos de expresión única, lo cual es una contradicción. Este hecho y la Observación 1.4.1 implican que

$$|A_\alpha|+|B_\beta| = 2|H|-\rho = |H|+1.$$

(ii) $A_\alpha + B_\beta = (\alpha+\beta)+H$ es un elemento de expresión única módulo H en $\phi_H(A)+\phi_H(B)$, en efecto, supongamos que $\phi_H(\alpha)+\phi_H(\beta) = \phi_H(\alpha_1)+\phi_H(\beta_1)$ con $\alpha_1 \in A$ y $\beta_1 \in B$, entonces $A_\alpha + B_\beta = (\alpha+\beta)+H = (\alpha_1+\beta_1)+H = A_{\alpha_1} + B_{\beta_1}$, de modo que existen $\alpha' \in A_{\alpha_1} \subseteq A$ y $\beta' \in B_{\beta_1} \subseteq B$ tales que

$\alpha+\beta=\alpha'+\beta'$, como $\alpha+\beta$ tiene expresión única, entonces $\alpha=\alpha'$ y $\beta=\beta'$, luego $\alpha+H=\alpha_1+H$ y $\beta+H=\beta_1+H$ (ya que $\alpha=\alpha'\in A_{\alpha_1}\subseteq\alpha_1+H$ y luego $\phi_H(\alpha)+\phi_H(\beta)$ tiene representación única en $\phi_H(A)+\phi_H(B)$ como queríamos ver.

(iii) *$A=(A+H)\setminus(\alpha+H)\cup A_\alpha$ y $B=(B+H)\setminus(\beta+H)\cup B_\beta$. Para ver esto suficiente mostrar que $\alpha+H$ y $\beta+H$ contienen todos los $H-$hoyos de A y B respectivamente. Es claro que los $H-$hoyos de A_α y B_β son también $H-$hoyos de A y B, respectivamente, como el número de H-hoyos en A_α y B_β es $|A_\alpha+H|-|A_\alpha|+|B_\beta+H|-|B_\beta|=|\alpha+H|+|\beta+H|-(|A_\alpha|+|B_\beta|)=2|H|-|H|-1=|H|-1$ y A y B tienen $|H|-1$ $H-$hoyos, entonces $\alpha+H$ y $\beta+H$ contienen todos los $H-$hoyos de A y B respectivamente.*

1.4.1. Los Pares Elementales

Un par (A,B) de subconjuntos finitos, no vacíos de un grupo G es llamado un *par elemental*, si satisface al menos una de las siguientes condiciones:

(I) $\min\{|A|,|B|\}=1$.

(II) A y B están en progresión aritmética con diferencia común d, $|A|,|B|\geq 2$ y $|A|+|B|-1\leq|\langle d\rangle|$.

(III) $A\subseteq a_0+H$ y $B\subseteq b_0+H$ (con $a_0\in A$, $b_0\in B$ y $H\leq G$), $|A|+|B|=|H|+1$ y a_0+b_0 es el único elemento de expresión única en $A+B$.

(IV) A es aperiódico, $A\subseteq a_0+H$ y $B\subseteq b_0+H$ (con $a_0\in A$, $b_0\in B$ y $H\leq G$),

$A+B$ no contiene elementos de expresión única, y $B = g-(a_0+H)\setminus A$ (para algún $g \in G$).

Observemos que los pares tipo (I), (II) y (III) son pares críticos (notar que en el caso (III), el Teorema de Mann implica que $A+B = (a_0+b_0)+H$, luego $|A+B| = |H| = |A|+|B|-1$).
Los pares tipo (IV) también son críticos, en efecto, no perdemos generalidad al trasladar A y B de modo que A, $B \subseteq H$ (notar que podemos considerar $g \in H$), así (IV) implica que $B = -\overline{A}$, donde $\overline{A}$ denota el complemento de A con respecto a H. Ahora

$$r_{A,B}(g) = r_{A,-\overline{A}}(g) = r_{-A,\overline{A}}(-g) = |(-g+A)\cap \overline{A}| = |(A\cup(-g+A))\setminus A|$$

Como A es aperiódico, $|(A\cup(-g+A))\setminus A| \geq 1$ para todo $g \in H$ no nulo (ya que $|(A\cup(-g+A))\setminus A| = 0$ implica $A = -g+A$, contradiciendo que A es aperiódico, pues $g \neq 0$). Así $r_{A,B}(g) \geq 1$ para todo $g \in H$ no nulo y $r_{A,B}(0) = 0$, en consecuencia $|A+B| = |H|-1 = |A|+|\overline{A}|-1 = |A|+|B|-1$. Más aún, $A+B = (g+H)\setminus\{g\}$ (ya que $A+B \subseteq (g+H)\setminus\{g\}$ y $|A+B| = |A|+|B|-1 = |A|+|g-(a_0+H)\setminus A|-1 = |A|+|a_0+H|-|A|-1 = |H|-1 = |(g+H)\setminus\{g\}|$)
La condición que $A+B$ no contenga elementos de expresión única que se pide en (IV) es dada para que no existan conjuntos de tipos (I) y (IV) simultánemente. Por esta misma razón se pide en (II) que $|A|$, $|B| \geq 2$, y en (III) que exista un único elemento de expresión única.

1.4.2. Descomposiciones Quasi-periódicas

Ahora procedemos a describir un método mediante el cual se puede tomar un par crítico en G/H que contiene un elemento de expresión única y combinarlo con un par crítico en H para obtener un nuevo par crítico en G. Iterando este proceso, usando como punto de partida los cuatro tipos de pares elementales dados anteriormente, se pueden crear muchos pares críticos en G. El teorema de estructura de Kemperman establece esencialmente que *todo* par crítico (aperiódico) puede ser construido con este simple proceso recursivo. Sin embargo, antes de seguir, necesitamos introducir la noción de quasi-periodicidad.

Definición 1.4.1 *Sea G un grupo abeliano y H un subgrupo no trivial de G, una* descomposición H-quasi-periódica *de un subconjunto A de G es una partición disjunta $A = A_1 \cup A_0$ con A_1 H-periódico o vacío y A_0 un subconjunto de una H-clase. Si A tiene una descomposición H-quasi-periódica para algún $H < G$, digamos $A = A_1 \cup A_0$, con $A_1 \neq \emptyset$, decimos que A es* quasi-periódico *o* $H-$quasi-periódico *si se desea especificar el subgrupo.*

Ejemplo 1.4.1 *En un grupo abeliano las progresiones aritméticas con diferencia $d \in G$, de longitud a lo más $|d| - 2$, no son conjuntos quasi-periódicos.*

Observación 1.4.3 *Sea G un grupo abeliano.*

(i) Todo subconjunto de G tiene un descomposición quasi-periódica con A_1 vacío y $H = G$.

(ii) Existe una sutil diferencia entre decir que el subconjunto A de G es H-quasi-periódico y decir que A tiene una descomposición H-quasi-periódica (en general, pedir que un conjunto sea H-quasi-periódico es más fuerte).

(iii) Todo conjunto periódico es quasi-periódico, pero el recíproco no es cierto, por ejemplo, dado $A \subseteq G$ y $H < G$, el conjunto $A + H \setminus \{g\}$ con $g \in A + H$ es quasi-periódico pero no es periódico.

(iv) Si A y B tienen descomposiciones $H-$quasi-periódicas para algún $H < G$, digamos, $A = A_1 \cup A_0$ y $B = B_1 \cup B_0$, entonces $A + H = (A \setminus A_0) \cup (A_0 + H)$ y $B + H = (B \setminus B_0) \cup (B_0 + H)$, esto implica que $|A + H| = |A| + |H| - |A_0|$ y $|B + H| = |B| + |H| - |B_0|$ (pues A_0 y B_0 estan, cada uno, incluido en una $H-$clase), más aún,

$$\begin{aligned} A + B &= (A_0 + B_0) \cup (A_0 + B_1) \cup (A_1 + B_0) \cup (A_1 + B_1) \\ &= (A_0 + B_0 + H) \cup (A_0 + B_1 + H) \cup (A_1 + B_0 + H) \cup (A_1 + B_1) \\ &= (A + B + H) \setminus (A_0 + B_0 + H) \cup A_0 + B_0 \end{aligned}$$

Luego $|A+B| = |A+B+H| + |A_0+B_0| - |H|$ (dado que A_0+B_0 esta contenido en una $H-$clase)

Ahora mostramos como el uso de descomposiciones quasi-periódicas "levanta" un par crítico en G/H que contiene un elemento de expresión única, a través de un par crítico en H, a un par crítico en G. Sean A_0, $B_0 \subseteq H$ y A', $B' \subseteq G/H$ ambos pares críticos, y supongamos que $A' + B'$ contiene un elemento de expresión única, digamos $\phi_H(a_0) + \phi_H(b_0)$, donde a_0, $b_0 \in G$. Entonces definimos

$$A_1 = \phi_H^{-1}(A' \setminus \phi_H(a_0)) \text{ y } B_1 = \phi_H^{-1}(B' \setminus \phi_H(b_0)),$$

es claro que A_1 y B_1 son $H-$periódicos, además si $A = A_1 \cup (a_0 + A_0)$ y $B = B_1 \cup (b_0 + B_0)$, entonces $\phi_H(A) = A'$ y $\phi_H(B) = B'$ (esencialmente, todo elemento de $A' \subseteq G/H$, excepto $\phi_H(a_0)$, es reemplazado por una H-clase, mientras $\phi_H(a_0)$ es reemplazada por $a_0 + A_0$, igualmente para B). Más aún, $(A+B)+H = (A_1+B_1) \cup (b_0+A_1+B_0) \cup (a_0+A_0+B_1) \cup (a_0+b_0+H) = A \setminus (a_0+b_0+A_0+B_0) \cup (A_0+B_0+H)$, implicando que $A + B = (A + B + H) \setminus (a_0 + b_0 + H) \cup (a_0 + b_0 + A_0 + B_0)$, pero $\phi_H(a_0) + \phi_H(b_0)$ es un elemento de expresión única en $\phi_H(A + B) = A' + B'$, de modo que $(A + B + H) \setminus a_0 + b_0 + H$ y $a_0 + b_0 + A_0 + B_0$ son disjuntos, luego

$$\begin{aligned} |A+B| &= |A+B+H| - |a_0+b_0+H| + |(a_0+b_0)+(A_0+B_0)| \\ &= |A+B+H| - |H| + |A_0+B_0| \\ &= |H|(|\phi_H(A)+\phi_H(B)|-1) + |A_0+B_0| \end{aligned}$$

y como los pares (A_0, B_0) y $(\phi_H(A), \phi_H(B)) = (A', B')$ son críticos, se sigue que

$$\begin{aligned} |A+B| &= |H|(|\phi_H(A)+\phi_H(B)|-1) + |A_0+B_0| \\ &= |H|(|\phi_H(A)|+|\phi_H(B)|-2) + |A_0|+|B_0|-1 \\ &= |H|(|\phi_H(A)|-1) + |A_0| + |H|(|\phi_H(B)|-1) + |B_0| - 1 \\ &= |A|+|B|-1. \end{aligned}$$

Así (A, B) es también un par crítico, como queríamos ver.

1.4.3. El Teorema de Estructura de Kemperman (KST)

A continuación enunciamos el Teorema de estructura de Kemperman, este Teorema, en esencia, muestra que todo par crítico puede ser construido a través del proceso descrito en la sección anterior usando los pares elementales como puntos de partida.

Teorema 1.4.2 (Teorema de estructura de Kemperman (KST)) *[12] Sea G un grupo abeliano, y sean A, $B \subseteq G$ finitos no vacíos. Si $A+B$ es aperiódico o $A+B$ es periódico conteniendo un elemento de expresión única, entonces*

$$|A+B| = |A| + |B| - 1$$

si y solo si, existe $H < G$ tal que A y B tienen descomposiciones H-quasi-periódicas $A = A_1 \cup A_0$ y $B = B_1 \cup B_0$ con A_0, $B_0 \neq \emptyset$, y se cumplen las siguientes condiciones:

(i) $\phi_H(A_0) + \phi_H(B_0)$ *es un elemento de expresión única en* $\phi_H(A) + \phi_H(B)$.

(ii) $|\phi_H(A+B)| = |\phi_H(A)| + |\phi_H(B)| - 1$.

(iii) $|A_0 + B_0| = |A_0| + |B_0| - 1$.

(iv) (A_0, B_0) *es un par elemental de tipo (I), (II), (III) o (IV).*

Aunque no haremos la demostración del Teorema KST, notemos que el recíproco se puede deducir facilmente. Supongamos que A y B tienen tienen descomposiciones $H-$quasi periódicas, digamos $A = A_1 \cup A_0$ y $B = B_1 \cup B_0$, que satisfacen las condiciones *(i)–(iv)*. De *(i)*, *(iii)* y de la observación 1.4.3,

$$\begin{aligned}
|A+B| &= |A+B+H| + |A_0+B_0| - |H| \\
&= |\phi_H(A+B)| \cdot |H| + |A_0| + |B_0| - 1 - |H| \\
&= (|\phi_H(A)| + |\phi_H(B)| - 1)|H| + |A_0| + |B_0| - 1 - |H| \\
&= |A+H| + |B+H| + |A_0| + |B_0| - 2|H| - 1 \\
&= (|A| - |A_0| + |H|) + (|B| - |B_0| + |H|) + |A_0| + |B_0| - 2|H| - 1 \\
&= |A| + |B| - 1.
\end{aligned}$$

Si $A+B$ es periódico, el par (A_0, B_0) no puede ser tipo (IV) (si $A+B$ es tipo (IV), $A_0+B_0 = g+H\setminus\{g\}$ con $g \in G$, luego de la Observación 1.4.3, $A+B = A+B+H\setminus\{g\}$ el cual no es periódico), en vista de *(iii)*, el par (A, B) debe ser tipo (I), (II) o (III) y en consecuencia debe tener un elemento de expresión única, esto muestra el recíproco de KST. Ahora supongamos que $A+B$ es periódico y contiene un elemento de expresión única, digamos a_0+b_0 con $a_0 \in A$ y $b_0 \in B$; sea $A_1 = A+H \setminus a_0+H$, $A_0 = a_0+H \cap A$, $B_0 = B+H \setminus b_0+H$ y $B_1 = b_0+H \cap B$, donde $H = \mathsf{H}(A+B)$, entonces de la Observación 1.4.2, $A = A_1 \cup A_0$ y $B = B_1 \cup B_0$, las cuales son descomposiciones H-quasi-periódicas de A y B respectivamente; $\phi_H(A_0) + \phi_H(B_0)$ es un elemento de expresión única en $\phi_H(A+B)$, $|\phi_H(A+B)| = |\phi_H(A)| + |\phi_H(B)| - 1$; más aún, $|A_0| + |B_0| = |H| + 1$ y $|A_0 + B_0| = |H|$, así $|A_0+B_0| = |A_0| + |B_0|$ y, finalmente, (A_0, B_0) es un par elemental tipo (III), así el directo de KST se cumple.

Finalizamos esta sección mostrando dos nuevos lemas, consecuencias de KST, que serán muy útiles al tratar la Conjetura de Hamidoune.

Lema 1.4.1 *Sea $A_1, \ldots, A_n$, una colección de $n \geq 3$ subconjuntos finitos en un grupo abeliano G de orden m, con $0 \in A_i$ y $|A_i| \geq 2$ para todo i. Supongamos que ningún A_i es quasi-periódico y que $\langle A_i \rangle = G$. Si $\sum_{i=1}^{n} A_i$ es aperiódico y*

$$|\sum_{i=1}^{n} A_i| = \sum_{i=1}^{n} |A_i| - n + 1, \tag{1.3}$$

entonces los conjuntos A_i estan en progresión aritmética con diferencia común.

Demostración. Como $\sum_{i=1}^{n} A_i$ es aperiódico, se sigue que $A_j + A_k$ es aperiódico para cualquier $j \neq k$. Así el Teorema de Kneser implica que $|A_j + A_k| \geq |A_j| + |A_k| - 1$ (Proposición 1.3.1). Si $|A_j + A_k| > |A_j| + |A_k| - 1$, el Teorema de Kneser implica

$$|\sum_{i=1}^{n} A_i| \geq \sum_{\substack{i=1 \\ i \neq j,k}}^{n} |A_i| + |A_j + A_k| - (n-1) + 1 > \sum_{i=1}^{n} |A_i| - n + 2,$$

contradiciendo (1.3), luego

$$|A_j + A_k| = |A_j| + |A_k| - 1,$$

por lo tanto todo par (A_j, A_k) con $j \neq k$ es un par crítico y podemos aplicar KST. Como A_i no es quasi-periódico, para $i = j, k$ concluimos de KST que (A_j, A_k) es un par elemental de tipo (I), (II), (III) o (IV). Pero $|A_j|, |A_k| \geq 2$ y $A_j + A_k$ es aperiódico, luego (A_j, A_k) no puede ser tipo (I) ni tipo (III). Como $n \geq 3$, $|A_i| \geq 2$ para todo i, y $\sum_{i=1}^{n} A_i$ es aperiódico (y en particular, $|\sum_{i=1}^{n} A_i| < |G|$), se sigue, en vista del Teorema de Kneser, que $|A_j + A_k| < |\sum_{i=1}^{n} A_i| < |G|$. Supongamos que el par (A_j, A_k) es tipo (IV), entonces $A_j + A_k = g + H \setminus \{g\}$ para algún $g \in G$; como $0 \in A_j + A_k$ entonces $g \in H$, y como $0 \in A_k$ entonces $A_j \subseteq H$, pero $\langle A_j \rangle = G$, entonces $H = G$, en consecuencia $A_j + A_k = G \setminus \{g\}$, luego para $l \neq j, k$ $|\sum_{i=1}^{n} A_i| \geq |A_i + A_j + A_k| \geq |A_i + A_j| + |A_k| - 1 \geq |G| - 1 + 2 - 1 = |G|$, generando una contradicción. Así (A_j, A_k) no puede ser tipo (IV), más aún, $|A_j|$, $|A_k| \leq |G| - 2$. Por tanto (A_j, A_k) es un par elemental tipo (II), es decir, A_j y A_k estan en progresión aritmética con diferencia común, digamos $d \in G$. Como $0 \in A_j$, entonces $A_j \subseteq \langle d \rangle$, así $\langle d \rangle \supseteq \langle A_j \rangle = G$, es decir, $\mathrm{ord}(d) = |G|$. Sabemos que la diferencia d de una progresión aritmética A es única, salvo el signo, cuando $2 \leq |A| \leq \mathrm{ord}(d) - 2$. Como $2 \leq |A_j|$, $|A_k| \leq |G| - 2$, y como A_j y A_k con $j \neq k$ son arbitrarios, tenemos que todos los A_i estan en progresión aritmética con diferencia común d, como queríamos probar. ■

Lema 1.4.2 *Sea G un grupo abeliano y sea A, $B \subseteq G$ finitos con $|A| \geq 2$ y $|B| = 2$. Si ni A ni B son quasi-periódicos y $|A + B| = |A| + |B| - 1$, entonces A y B estan en progresión aritmética con diferencia común.*

Demostración. Sea $B = \{b_1, b_2\}$ entonces $A + B = (A + b_1) \cup (A + b_2)$, luego $2|A| - |(A + b_1) \cap (A + b_2)| = |A + b_1| + |A + b_2| - |(A + b_1) \cap (A + b_2)| = |A + B| = |A| + |B| - 1 = |A| + 1$, es decir, $|(A + b_1) \cap (A + b_2)| = |A| - 1$ implicando que existen exactamente dos elementos en $A + B$ que tienen representación única.

Como el par (A, B) es crítico podemos aplicar KST, y tenemos que (A, B) es un par elemental de tipo (I), (II), (III) o (IV) (ya que ninguno de ellos es quasi-periódico). Pero (A, B) no puede ser tipo (I) (ya que $|A| \geq 2$) ni tipo (III) ni (IV) (ya que tiene 2 elementos de expresión única), luego debe ser tipo (II) es decir, A y B estan en progresión aritmética con diferencia común. ■

1.5. El Teorema DeVos-Goddyn-Mohar

Finalmente presentamos, sin su demostración, un resultado que vincula el área de los problema de suma cero, con resultados de teoría aditiva. Tal resultado ha tenido mucha trascendencia en dicha área, dado que sus autores consiguieron, como un corolario, demostrar una conjetura de Gao, Thangadurai y Zhuang, y además simplificaron la demostración de varios resultados de suma cero. Recientemente varios autores lo han usado con mucha frecuencia para la solución de algunos problemas abiertos de suma cero. Este Teorema generaliza el Teorema de Kneser. A continuación introducimos una nueva notación.

Sea G un grupo abeliano, $\mathcal{A} = (A_1, ..., A_m)$ una colección de subconjuntos finitos no vacíos de G y $l \leq m$, denotaremos por $\Sigma^l(\mathcal{A})$ al conjunto de todos los elementos que se pueden representar como suma de l elementos de distintos términos de $\mathcal{A}$, es decir:

$$\Sigma^l(A) = \{a_{i_1} + a_{i_2} ... + a_{i_l} : 1 \leq i_1 < ... < i_l \leq m; a_{i_j} \in A_{i_j} \forall j \in \{1, ..., l\}\}$$

Teorema 1.5.1 (Teorema de Devos-Goddyn-Mohar (DGM)) *[13] Sea $\mathcal{A} = (A_1, ..., A_m)$ una colección de subconjuntos finitos de G, sea $l \leq m$, y sea $H = \mathsf{H}(\sum^l(\mathcal{A}))$. Si $\sum^l(A)$ es no vacío, entonces:*

$$|\Sigma^l(A)| \geq |H|(1 - l + \sum_{Q \in G/H} \text{mín}\{l, \#\{i \in \{1, ..., m\} : A_i \cap Q \neq \emptyset\}\})$$

Cuando todo conjunto en $\mathcal{A}$ tiene cardinalidad 1, el Teorema DGM dice esencialmente que el número de elementos, representables como suma de l elementos de distintos términos de $\mathsf{S}(\mathcal{A})$, es grande. Notemos que el caso $l = |A|$ es justamente el

Teorema de Kneser, pues si $\mathcal{A} = (A_1, ...A_n)$ es una colección de subconjuntos finitos de G, entonces $\sum^n(A) = \sum_{i=1}^{n} A_i$, $H = \mathsf{H}(\sum^n(\mathcal{A})) = \mathsf{H}(\sum_{i=1}^{n} A_i)$ y para todo $Q \in G/H$, $\text{mín}\{n, \#\{i \in \{1, ..., n\} : A_i \cap Q \neq \emptyset\}\} = \#\{i \in \{1, ..., n\} : A_i \cap Q \neq \emptyset\}$, luego el Teorema DGM implica

$$|\sum_{i=1}^{n} A_i| \geq |H|(1 - n + \sum_{Q \in G/H} \#\{i \in \{1, ..., n\} : A_i \cap Q \neq \emptyset\})$$

pero $\sum_{Q \in G/H} \#\{i \in \{1, ..., n\} : A_i \cap Q \neq \emptyset\} = \sum_{i=1}^{n} |\phi_H(A_i)|$, luego

$$|\sum_{i=1}^{n} A_i| \geq \sum_{i=1}^{n} |A_i + H| - (n-1)|H|$$

Capítulo 2

Problemas de Suma Cero

Al estudiar los problemas de suma cero, el objeto principal de estudio son las *secuencias* finitas $S = (g_1, g_2, \ldots, g_l)$, cuyos términos estan en un grupo abeliano G (en lugar de pares de conjuntos, usados en Teoría Aditiva). No se necesita que las secuencias sean ordenadas, sólo que éstas permitan la repetición de elementos, por esta razón el término "multiconjunto" también es usado por algunos autores para referirse a las secuencias. Recientemente, dadas las aplicaciones de los problemas de suma cero en teoría de factorización, se ha tratado a las secuencias como elementos del monoide libre abeliano con base G, cuyo producto es la concatenación de las secuencias. En este capítulo revisaremos algunos resultados relacionados con los problemas de suma cero que nos servirán como herramientas para tratar la Conjetura de Hamidoune.

2.1. Notación y Definiciones

Una *secuencia* es un elemento del monoide abeliano libre con base G, el cual denotamos por $\mathcal{F}(G)$. Si $S \in \mathcal{F}(G)$, S se escribe de la forma

$$S = \prod_{g\in G} g^{\mathsf{v}_g(S)}\,, \quad \text{con} \quad \mathsf{v}_g(S) \in \mathbb{N}_0 \quad \text{para todo} \quad g \in G\,.$$

Llamamos a $\mathsf{v}_g(S)$ la *multiplicidad* de g en S, y decimos que S *contiene* a g si $\mathsf{v}_g(S) > 0$. Si una secuencia $S \in \mathcal{F}(G)$ es escrita de la forma $S = g_1 \cdot \ldots \cdot g_l$, asumiremos que $l \in \mathbb{N}_0$ y $g_1, \ldots, g_l \in G$.

Llamamos *longitud* de S al entero

$$|S| = l = \sum_{g\in G} \mathsf{v}_g(S) \in \mathbb{N}_0.$$

Una secuencia S' es llamada una *subsecuencia* de S si $S' \,|\, S$ en $\mathcal{F}(G)$ (o equivalentemente, si $\mathsf{v}_g(S') \le \mathsf{v}_g(S)$ para todo $g \in G$). Si $S' \,|\, S$ y $|S'| = k$, decimos que S' es una k-*subsecuencia* de S.

La *máxima de las multiplicidades* de S es denotada por

$$\mathsf{h}(S) = \max\{\mathsf{v}_g(S) \mid g \in G\} \in [0, |S|].$$

El *soporte* de S es el conjunto

$$\operatorname{supp}(S) = \{g \in G \mid \mathsf{v}_g(S) > 0\} \subset G.$$

La *suma* de S la definimos como

$$\sigma(S) = \sum_{i=1}^{l} g_i = \sum_{g\in G} \mathsf{v}_g(S) g \in G.$$

Dado $k \in \mathbb{N}$, $k \leq |S|$, el conjunto *suma de k-subsecuencias* de S es

$$\Sigma_k(S) = \Big\{ \sum_{i \in I} g_i \;\Big|\; I \subset [1, l] \text{ con } |I| = k \Big\}.$$

y el conjunto *suma de subsecuencias* de S es

$$\Sigma(S) = \bigcup_{j \geq 1} \Sigma_j(S).$$

$S \in \mathcal{F}(G)$ es *de suma cero* si $\sigma(S) = 0$. $S \in \mathcal{F}(G)$ es *libre de suma cero* si $0 \notin \Sigma(S)$.

Los problemas de suma cero tratan el estudio de condiciones necesarias y suficientes para que una secuencia dada contenga una subsecuencia (o una $|G|$-subsecuencia) de suma cero (o equivalentemente, para que dada $S \in \mathcal{F}(G)$ se tenga que $0 \in \Sigma(S)$ o que $0 \in \Sigma_{|G|}(S)$). Dentro de los problemas de suma cero se consideran también aquellos problemas que consisten en establecer condiciones suficientes para que una secuencia dada represente al grupo G, o a un subgrupo no trivial de G, con nuestra notación esto significa: hallar condiciones sobre $S \in \mathcal{F}(G)$ para que $\Sigma(S) = G$ o para que $\Sigma_{|G|}(S) = G$.

2.2. El Teorema de Erdős-Ginzburg-Ziv

Comenzaremos revisando uno de los teoremas más básicos en el área de los problemas de suma cero. Este fué probado por Erdős, Ginzburg y Ziv en (1961), y desde entonces ha tenido muchas generalizaciones. Con nuestra notación el Teorema es el siguiente

Teorema 2.2.1 (Teorema de Erdős-Ginzburg-Ziv (EGZ)) *[22] Sea G un grupo abeliano finito. Si $S \in \mathcal{F}(G)$ con $|S| \geq 2|G| - 1$, entonces $0 \in \Sigma_{|G|}(S) = 0$.*

Existen al menos 13 pruebas diferentes de este teorema. Presentaremos la prueba original, la cual usa métodos muy generales, cuya técnica consiste en combinar resultados de teoría aditiva con el argumento de particionar las secuencias en conjuntos.

Para un subconjunto G_0 de un grupo abeliano, sea $\mathcal{S}(G_0) = \mathcal{F}(X)$, donde X es el conjunto de todos los subconjuntos finitos, no vacíos de G_0. Una *partición* sobre G_0 es una secuencia $\mathcal{A} = A_1 \cdot \ldots \cdot A_n \in \mathcal{S}(G_0)$, donde $A_i \subseteq G_0$ son finitos y no vacíos. Cuando hablamos de una *n-partición*, nos referimos a una partición de longitud n. La secuencia particionada por A es

$$\mathsf{S}(\mathcal{A}) := \prod_{i=1}^{n} \prod_{g \in A_i} g \in \mathcal{F}(G_0).$$

Dada una secuencia $S \in \mathcal{F}(G_0)$ decimos que S tiene una n-partición en conjuntos, o simplemente que tiene una n-partición, si $S = \mathsf{S}(\mathcal{A})$ para algún $\mathcal{A} \in \mathcal{S}(G_0)$ con $|\mathcal{A}| = n$.

La relación entre la teoría inversa aditiva y los problemas de suma cero parte del siguiente hecho, si un elemento g pertenece al conjunto $\sigma(\ A) = \sum_{i=1}^{n} A_i$ de alguna n-partición $\mathcal{A} = A_1 \cdot \ldots \cdot A_n$ de una secuencia S, entonces una selección apropiada de los términos de cada A_i forma una n-subsecuencia de S cuyos términos suman g, es decir

$$\sigma(\mathcal{A}) = \sum_{i=1}^{n} A_i = \Sigma_n(S).$$

En particular, si $|\sum_{i=1}^{n} A_i| \geq |G|$, entonces todo elemento, incluyendo el cero, puede ser representado como la suma de una n-subsecuencia de S. De modo que si estamos buscando una n-subsecuencia de suma cero, entonces por contradicción, toda

n-partición de S debe tener conjuntos sumas de cardinalidades pequeñas, así los teorema de estructura inversa, como el Teorema de Kneser o el Teorema de Cauchy-Davenport, pueden ser usados para obtener información estructural de los conjuntos A_i y, en consecuencia acerca de la secuencia S particionada por los A_i.

Ahora podríamos preguntarnos si dada una secuencia $S \in \mathcal{F}(G)$, siempre existe una n-partición en conjuntos de S, la siguiente proposición muestra las condiciones para que tal n-partición pueda existir, y en caso de existir, muestra que una n-partición en conjuntos puede encontrarse siempre con cardinalidades tan cercanas como sea posible.

Proposición 2.2.1 *[24] Sea $n \in \mathbb{Z}^+$. Una secuencia S tiene una n-partición en conjuntos $\mathcal{A} = A_1 \cdot A_2 \cdot \ldots \cdot A_n$ sí y sólo si $|S| \geq n$ y $h(S) \leq n$. Además, si S tiene una n-partición en conjuntos, entonces S tiene una n-partición en conjuntos $\mathcal{B} = B_1 \cdot B_2 \cdot \ldots \cdot B_n$ con $||Bi| - |Bj|| \leq 1$, para todo i y todo j.*

Observemos que toda aplicación de grupos abelianos $\varphi \colon G \to H$ se extiende a un homomorfismo $\varphi \colon \mathcal{F}(G) \to \mathcal{F}(H)$ donde $\varphi(S) = \varphi(g_1) \cdot \ldots \cdot \varphi(g_l)$. De manera que si φ es un homomorfismo, entonces $\varphi(S)$ es una secuencia de suma cero si, y sólo si $\sigma(S) \in \mathrm{Ker}(\varphi)$. En particular si $H < G$ y consideramos el homomorfismo canónico $\phi_H : G \to G/H$ entonces $\phi_H(S)$ es de suma cero si y sólo si $\sigma(S) \in H$. El método inductivo para mostrar que una secuencia dada $S \in \mathcal{F}(G)$ posea una n-subsecuencia de suma cero, mas o menos funciona como sigue

- Encontramos un subgrupo adecuado H de G (generalmente el mas adecuado es $H = \mathsf{H}(\Sigma_n(S)))$, y consideramos el homomorfismo canónico $\phi_H : G \to G/H$.

- Consideramos una n-partición de S (así tendremos que considerar los casos $\mathsf{h}(S) \leq n-1$ y $\mathsf{h}(S) \geq n$)

- Estudiamos la secuencia $\phi_H(S)$ a la que podemos aplicar la hipótesis inductiva, frecuentemente se puede aplicar en forma recursiva, siempre que $H \neq 0$.

- En general los casos $\mathsf{h}(S) \geq n$ y $H = 0$ salen sin mucha dificultad haciendo uso del Teorema de Cauchy-Davenport, del Teorema de Kneser o del Teorema DGM.

Prueba del Teorema EGZ (2.2.1)

Sea $S \in \mathcal{F}(G)$ con $|S| \geq 2|G| - 1$. Podemos suponer $\mathsf{h}(S) \leq |G| - 1$, de lo contrario tomamos una subsecuencia de S consistente de $|G|$ términos, todos iguales, la cual es de suma cero. De la Proposición 2.2.1, se sigue que S tiene una $|G|$-partición $\mathcal{A} = A_1 \cdot \ldots \cdot A_{|G|}$.

Supongamos que $|G|$ es primo. Entonces por el Teorema de Cauchy-Davenport se sigue que

$$|\sum_{i=1}^{|G|} A_i| \geq \text{mín}\{|G|, \sum_{i=1}^{|G|} |A_i| - |G| + 1\} = \text{mín}\{|G|, |S| - |G| + 1\} = |G|.$$

En consecuencia $\sum\limits_{i=1}^{|G|} A_i = G$, y así, seleccionando apropiadamente términos de cada A_i, obtenemos una $|G|$-subsecuencia de suma cero.

Ahora procedemos por inducción sobre el número de primos que dividen a $|G|$, el caso anterior es la base del proceso inductivo. Sea $p|\,|G|$ un primo, sea $H \leq G$ un subgrupo de orden p, recordemos que $\phi_H : G \to G/H$ es el homorfismo natural.

Entonces

$$|\phi_H(S)| = (2p-2)\frac{|G|}{p} + 2\frac{|G|}{p} - 1 = (2p-2)|G/H| + 2|G/H| - 1,$$

y así, aplicando recursivamente la hipótesis inductiva a $\phi_H(S)$, obtenemos $2p-1$ subsecuencias $S_1, \ldots, S_{2p-1}$ tales que $S_1 \cdot \ldots \cdot S_{2p-1}|S$,

$$|S_i| = \frac{|G|}{p},$$

y $\sigma(\phi_H(S_i)) = 0$ para todo i, o equivalentemente, $\sigma(S_i) \in H$. Así podemos definir una secuencia $T \in \mathcal{F}(H)$ por $T := \prod_{i=1}^{2p-1} \sigma(S_i)$. Sin embargo, aplicando la hipótesis inductiva a T, encontramos una subsecuencia de longitud p digamos, sin perder generalidad (re-indizando), $\prod_{i=1}^{p} \sigma(S_i)$, la cual suma cero en $H \le G$. Pero ahora $S_1 \cdot \ldots \cdot S_p$ es una subsecuencia de S de suma cero y longitud $\sum_{i=1}^{p} |S_i| = p\frac{|G|}{p} = |G|$, completando la prueba. ■

2.3. La Constante de Davenport y la Constante de Erdős-Ginzburg-Ziv

Notemos que el Teorema de Erdős-Ginzburg-Ziv da una cota sobre la longitud minimal que necesita tener una secuencia para que esta posea una subsecuencia de longitud $|G|$ que sume cero. Con el nacimiento de esta área, en el año de 1961, aparece la constante de Erdős-Ginzburg-Ziv, $\mathsf{ZS}(G)$.

Definición 2.3.1 *Sea G un grupo abeliano finito. La constante de Erdős-Ginzburg-Ziv, $\mathsf{ZS}(G)$, es el menor entero positivo t tal que toda secuencia de longitud t contiene una subsecuencia de longitud $|G|$ y suma cero.*

El Teorema 2.2.1 implica que $\mathsf{ZS}(G) \leq 2|G| - 1$. Ahora, podemos preguntarnos que longitud debe tener una secuencia $S \in \mathcal{F}(G)$ para garantizar la existencia de una subsecuencia no trivial de suma cero, sin importarnos que longitud tenga. De esta manera Davenport, en 1966, dió origen a su célebre constante $\mathsf{D}(G)$, la cual definimos a continuación.

Definición 2.3.2 *Sea G un grupo abeliano finito. La constante de Davenport, $\mathsf{D}(G)$, es el menor entero positivo t tal que toda secuencia de longitud t en G contiene una subsecuencia de suma cero.*

El siguiente resultado da una cota superior para $\mathsf{D}(G)$, esencialmente muestra que toda secuencia de longitud $|G|$ posee una subsecuencia de suma cero, este resultado fué uno de los primeros resultado en esta área y fué denominado por Erdős como Lema Prehistórico, aunque la demostración es muy simple, la idea central es muy versátil y aparece con mucha frecuencia en las pruebas de otros teoremas mas complejos.

Teorema 2.3.1 $\mathsf{D}(G) \leq |G|$ *para todo grupo abeliano finito G.*

Demostración. Sea $m := |G|$ y $S = a_1 \cdot \ldots \cdot a_m \in \mathcal{F}(G)$. Necesitamos mostrar que $0 \in \Sigma(S)$, es decir, que S tiene una subsecuencia no trivial de suma cero. Para cada $i \in [1, m]$, definimos $S_i = a_1 \cdot \ldots \cdot a_i$. Notemos que si $\sigma(S_i) = \sigma(S_j)$ con $i < j$, entonces $a_{i+1} \cdot \ldots \cdot a_j$ es una subsecuencia no trivial de S de suma cero, como se deseaba. Supongamos que todos los $\sigma(S_i)$ son distintos, entonces $A = \{\sigma(S_1), \sigma(S_2), \ldots, \sigma(S_m)\}$ es a subconjunto de G de cardinalidad $m = |G|$, implicando que $A = G$, de modo que $0 \in A$, es decir, existe $i \in [1, m]$ tal que $\sigma(S_i) = 0$, como queríamos demostrar. ∎

Ejemplo 2.3.1 *$\mathsf{D}(C_n) = n$, donde C_n es un grupo cíclico de orden n. En efecto, la secuencia $S = 1^{|G|-1}$, donde 1 es el generador de C_n, no posee subsecuencias de suma cero, así $\mathsf{D}(Cn) \geq |C_n|$. Luego el Teorema 2.3.1 implica que $\mathsf{D}(C_n) = |C_n| = n$.*

En general no es fácil determinar el valor exacto de la constante de Davenport, existen varios resultados que dan cotas inferiores y superiores para $\mathsf{D}(G)$ y estudian problemas inversos asociados a tal constante. En [25] Gao prueba que hallar $\mathsf{ZS}(G)$ y $\mathsf{D}(G)$ es equivalente, al mostrar que $\mathsf{ZS}(G) = |G| + \mathsf{D}(G) - 1$. A continuación mostramos tal resultado, no daremos la prueba original, usaremos el Teorema 1.5.1 (DGM), de esta manera veremos lo potente que es este teorema como herramienta para resolver problemas de suma cero en forma mas simple. Antes de continuar, enunciamos una nueva versión del Teorema DGM 1.5.1 en términos de secuencias y particiones.

Sea G un grupo abeliano, sea $\mathcal{A} \in \mathcal{S}(G)$ una partición en conjuntos, y sea $n \in \mathbb{Z}^+$ con $n \leq |\mathcal{A}|$. Si $H = \mathsf{H}(\Sigma_n^{\cup}(\mathcal{A}))$, entonces

$$|\Sigma_n^{\cup}(\mathcal{A})| \geq (\sum_{g \in G/H} \text{mín}\{n, \mathsf{v}_g(\mathsf{S}(\phi_H(\mathcal{A}))\} - n + 1)|H|.$$

Sea $S = a_1 \cdot \ldots \cdot a_{|S|}$ una secuencia en un grupo abeliano G, es claro que S tiene una $|S|$-partición en conjuntos unitarios, digamos $\mathcal{A} = \{a_1\} \cdot \ldots \cdot \{a_{|S|}\}$, en este caso $\Sigma_n^{\cup}(\mathcal{A}) = \Sigma(S)$, $\mathsf{S}(\mathcal{A}) = S$ y la versión anterior del Teorema DGM implica directamente el siguiente Corolario.

Corolario 2.3.1 *Sea G un grupo abeliano, sea $S \in \mathcal{F}(G)$ y $n \in \mathbb{Z}^+$ con $n \leq |S|$. Si $H = \mathsf{H}(\Sigma_n(S))$, entonces*

$$|\Sigma_n(S)| \geq |H|(1 - n + \sum_{g \in G/H} \min\{n, \mathsf{v}_g(\phi_H(S))\}).$$

Teorema 2.3.2 *[25] $\mathsf{ZS}(G) = \mathsf{D}(G) + |G| - 1$ para todo grupo finito abeliano G.*

Demostración. Sea $S \in \mathcal{F}(G)$ con $|S| = \mathsf{D}(G) - 1$ tal que $0 \notin \Sigma(S)$, entonces la secuencia $S0^{|G|-1}$ tiene longitud $\mathsf{ZS}(G) = \mathsf{D}(G) + |G| - 1$ y no posee subsecuencias de longitud $|G|$ de suma 0, así $\mathsf{ZS}(G) \geq \mathsf{D}(G) + |G| - 1$.

Ahora veamos que $\mathsf{ZS}(G) \leq \mathsf{D}(G) + |G| - 1$, lo haremos por inducción sobre $|G|$. Es evidente que para $|G| = 1$ se satisface el teorema, supongámoslo cierto para cualquier subgrupo propio de G. Sea $m = \mathsf{ZS}(G) = \mathsf{D}(G) + |G| - 1$, necesitamos probar que $0 \in \Sigma_m(S)$. Sea $H = \mathsf{H}(\Sigma_m(S))$.

Si $H \neq 0$, consideremos la secuencia $\phi(S) = \phi(a_1) \cdot \phi(a_2) \cdot \ldots \cdot \phi(a_m)$, donde $\phi : G \to G/H$ es el homomorfismo canónico. Como $\mathsf{D}(G/H) \leq \mathsf{D}(G)$ y $|G/H| \leq |G|$, podemos aplicar la hipótesis inductiva a G/H y obtener una subsecuencia de $\phi(S)$ de longitud $[G : H] = |G/H|$ que suma $0 \pmod{H}$. Removemos esta subsecuencia de $\phi(S)$ y aplicamos nuevamente la hipótesis inductiva a la secuencia que queda para obtener otra subsecuencia de $\phi(S)$ de suma $0 \pmod{H}$. Repitiendo este procedimiento $|H|$ veces vamos a obtener $|H|$ subsecuencias disjuntas de $\phi(S)$ cada una de las cuales suma $0 \pmod{H}$, al concatenarlas a todas obtenemos una subsecuencia de $\phi(S)$ de longitud $|H|[G : H] = |G|$, digamos $\phi_H(a_{i_1}) \cdot \phi_H(a_{i_2}) \cdot \ldots \cdot \phi_H(a_{i_{|G|}})$, tal que $\sum_{j=1}^{|G|} \phi_H(a_{i_j}) = \phi_H(0)$, es decir, $\sum_{j=1}^{|G|}(a_{i_j} + H) = H$, implicando que $-\sum_{j=1}^{|G|}(a_{i_j}) \in H$.

Como $H = \mathsf{H}(\Sigma_{|G|}(S))$, se sigue que $0 = \sum_{j=1}^{|G|}(a_{i_j}) - \sum_{j=1}^{|G|}(a_{i_j}) \in \Sigma_m(S)$.

Supongamos que $H = 0$. Si $\mathsf{h}(S) < \mathsf{D}(G)$, entonces $\mathsf{v}_g(S) < \mathsf{D}(G)$ para todo $g \in G$ y por Corolario 2.3.1

$$\begin{aligned} |\Sigma_{\mathsf{D}(G)-1}| &\geq |H|(1 - (\mathsf{D}(G) - 1) + \Sigma_{g\in G} \min\{\mathsf{D}(G) - 1, \mathsf{v}_g(S)\}) \\ &= 1 - \mathsf{D}(G) + 1 + m = 2 - \mathsf{D}(G) + \mathsf{D}(G) + |G| - 1 \\ &= |G| + 1 \end{aligned}$$

obtenemos una contradicción, luego existe $g \in G$ tal que $\mathsf{v}_g(S) \geq \mathsf{D}(G)$. Consideremos la secuencia $S' = b_1 \cdot \ldots \cdot b_m$ donde $b_i = a_i - g$, en este caso $\mathsf{v}_0(S') > \mathsf{D}(G)$, además sabemos que $\Sigma_{|G|}(S) = \Sigma_{|G|}(S')$, entonces será suficiente ver que $0 \in \Sigma_{|G|}(S')$. Podemos reordenar la secuencia S' y suponer que $b_{|G|+1}$, $b_{|G|+2}, \ldots, b_{|G|+\mathsf{D}(G)-1}$ son todos nulos. Por definición de $\mathsf{D}(G)$, podemos seleccionar subsecuencias disjuntas de $b_1 \cdot \ldots \cdot b_{|G|}$, cada una de las cuales tiene suma 0, concatenado estas subsecuencias, y adicionando un número apropiado de términos b_i con $i > |G|$, obtenemos una subsecuencia de longitud $|G|$ con suma 0. ■

Finalizamos esta sección mencionando un resultado de Olson, el cual extiende el área de los problemas de suma cero. En vez de encontrar condiciones sobre una secuencia S para que el cero se pueda escribir como suma de una subsecuencia de S, él encuentra condiciones suficientes sobre una secuencia S para que cada elemento de un grupo G, se pueda escribir como la suma de una $|G|$-subsecuencia de S.

Teorema 2.3.3 (Teorema de Olson) *[10]En un grupo abeliano finito G toda secuencia $S \in \mathcal{F}(G)$ con $|S| = 2|G| - 1$ y $h(S) \leq |G|$, cumple una de las siguientes* *alternativas:*

(i) $G = \Sigma_{|G|}(S)$.

(ii) Existe un subgrupo propio, no trivial H *tal que* $H \subseteq \Sigma_{|G|}(S)$, *y todos, excepto a lo sumo* $|G/H| - 2$ *términos de* S, *pertenecen a una* H*-clase.*

2.4. Variación con Peso de Algunos Problemas de Suma Cero

Una variante interesante en los problemas de suma cero, originada por Y. Caro, es la siguiente, se fija una secuencia de números enteros $W = w_1 \cdot \ldots \cdot w_n$ y una secuencia S de un grupo G con $|S| \geq n$, en vez de buscar subsecuencias $S' = s_1 \cdot \ldots \cdot s_n$ de S cuya suma sea determinado elemento, se buscan subsecuencias de S cuya W-suma $(\sum_{i=1}^{n} w_i \cdot s_i)$ sea determinado elemento. Esto le da al problema una estructura aditiva y multiplicativa. Los enteros $w_1, \ldots, w_n$ son llamados pesos. En este caso los problemas de suma cero (sin peso) son casos particulares. A continuación introducimos la notación para sumas de subsecuencias con peso.

Dados $m, n \in \mathbb{Z}$, denotamos por $\gcd(m, n)$ al máximo común divisor de m y n.

Sea $S \in \mathcal{F}(G)$, $W \in \mathcal{F}(\mathbb{Z})$ con $|S| \geq |W| \geq n$, definimos

$$\begin{aligned} \Sigma_n(W, S) &= \left\{ \sum_{i=1}^{n} w_i s_i : w_1 \cdot \ldots \cdot w_n | W \quad \text{y} \quad s_1 \cdot \ldots \cdot s_n | S \right\} \\ \Sigma(W, S) &= \bigcup_{n=1}^{|W|} \Sigma_n(W, S) \end{aligned}$$

Con nuestra notación los problemas de suma cero con peso consisten en hallar condiciones sobre la secuencia S para que $0 \in \Sigma(W, S)$ o $0 \in \Sigma_n(W, S)$. En este caso, que la secuencia S represente un subgrupo H de G, significa que $H \subseteq \Sigma(W,\, S)$; y que la secuencia S n-represente un subgrupo H de G, significa que $H \subseteq \Sigma_n(W,\, S)$. Cuando estudiamos secuencias con peso también consideramos una n-partición apropiada $\mathcal{A} = A_1 \cdot \ldots \cdot A_n$ de la secuencia S con el objetivo de aplicar el Teorema de Kneser, KST o DGM; sólo que en vez de aplicar tales teoremas a los conjuntos A_i los aplicamos a los conjuntos $w_i \cdot A_i$.

Observación 2.4.1 *Sea $S \in \mathcal{F}(G)$ y $W \in \mathcal{F}(\mathbb{Z})$ con $|S| \geq |W|$, $\mathsf{h}(S) \leq |W|$ y $W = w_1 \cdot \ldots \cdot w_n$.*

(i) *Como $\mathsf{h}(S) \leq |W|$, la Proposición 2.2.1 implica que S tiene un n-partición en conjuntos $\mathcal{A} = A_1 \cdot \ldots \cdot A_n$, así*

$$\sum_{i=1}^{n} w_i \cdot A_i \subseteq \Sigma(W,\, S)$$

.

(ii) *$|w_i \cdot A_i| \leq |A_i|$ para todo $i \in [1, n]$.*

(iii) *Si cada término de W es primo relativo con $\exp(G)$ (o con $|G|$), entonces $|w_i \cdot A_i| = |A_i|$, de modo que si conocemos alguna cota para $|A_i|$, por ejemplo $\sum_{i=1}^{n} |A_i| = |S|$, esta misma nos servirá para acotar $|w_i \cdot A_i|$. Esta es la razón por la cual muchos resultados tienen como hipótesis que los términos de W sean primos relativos con $\exp(G)$ (o con $|G|$).*

(iv) *Supongamos que $\sigma(W) \equiv 0 \pmod{n}$. Si $\mathsf{h}(S) \geq |n|$ entonces S tiene un término, digamos g, que se repite al menos n veces, luego $0 = (\sum_{i=1}^{n} w_i)g = \sum_{i=1}^{n} w_i g \in \Sigma(W,\, S)$.*

En [28] Caro conjeturó la siguiente versión con peso del teorema de Erdős-Ginzburg-Ziv:

> Sea G un grupo abeliano finito, y sea $S \in \mathcal{F}(G)$ y $W \in \mathcal{F}(\mathbb{Z})$ con $\sigma(W) \equiv 0 \pmod{\exp(G)}$. Si $|S| \geq |W| + |G| - 1$, entonces $0 \in \Sigma_{|W|}(W, S)$.

Observemos que el caso $W = 1^{|G|}$ es justamente el Teorema de Erdős-Ginzburg-Ziv. En la década de 1990, N. Alon demostró la Conjetura de Caro en el caso $n = m$ con m primo [17], en adelante otros casos particulares de la conjetura de Caro fueron demostrados ([17], [27], [29], [30]). Finalmente fué probada en 2006 (en [4]) por Grynkiewicz, cuya prueba original damos a continuación.

Teorema 2.4.1 (Teorema de Erdős-Ginzburg-Ziv con peso (EGZP)) *[4] Sea G un grupo abeliano finito no trivial, sea $W = w_1 \cdot \ldots \cdot w_n \in \mathcal{F}(\mathbb{Z})$ con $\sigma(W) \equiv 0$ $\pmod{\exp(G)}$, y sea $S \in \mathcal{F}(G)$ con $|S| \geq |W| + |G| - 1$. Entonces*

$$0 \in \Sigma_n(W,\, S).$$

Más aún, supongamos que S tiene una n-partición $\mathcal{A} = A_1 \cdot \ldots \cdot A_n$ tal que $|w_i \cdot A_i| = |A_i|$ para todo i. Entonces existe un subgrupo no trivial H de G y una n-partición $\mathcal{A}' = A'_1 \cdot \ldots \cdot A'_n$ de S con

$$H \subseteq \sum_{i=1}^{n} w_i \cdot A'_i \subseteq \Sigma_n(W, S)$$

y $|w_i \cdot A'_i| = |A'_i|$ para todo i.

Demostración. Si $\mathsf{h}(S) \geq n$, como $\sigma(W) = 0 \pmod{\exp(G)}$, la Observación 2.4.1 parte (3) implica que $0 \in \Sigma_n(W,\, S)$, como S no tiene n-particiones, la prueba esta lista.

Supongamos que $h(S) \leq n-1$, entonces S tiene una n-partición en conjuntos $\mathcal{A} = A_1, \cdots, A_n$. Seleccionemos $\mathcal{A}$ de tal forma que $\sum_{i=1}^{n} |w_i \cdot A_i|$ sea máxima.

Supongamos que $|w_j \cdot A_j| < |A_j|$ para algún j, entonces existen $x, y \in A_j$ con $x \neq y$ tal que $w_j x = w_j y$, más aún, $w_j x \in w_i \cdot A_i$ para todo $i \in [1, n]$, de lo contrario, si existe $r \in [1, n]$ tal que $w_j x \notin w_r \cdot A_r$, entonces la n-partición definida por $A'_j = A_j \setminus \{x\}$, $A'_r = A_r \cup \{x\}$ y $A'_i = A_i$ para $i \neq j, r$ contradice la maximalidad de $\sum_{i=1}^{n} |w_i \cdot A_i|$. Por tanto $w_j x \in w_i \cdot A_i$ para todo $i \in [1, n]$, luego, $0 = (\sum_{i=1}^{n} w_i)x = \sum_{i=1}^{n} w_i x \in \sum_{i=1}^{n} w_i \cdot A_i \subseteq \Sigma_n(W,\, S)$.

Supongamos $|w_i \cdot A_i| = |A_i|$ para todo i. Consideremos $\mathcal{A} = A_1 \cdot \ldots \cdot A_n$ una n-partición de S tal que $|\sum_{i=1}^{n} w_i \cdot A_i|$ sea maximal con la condición $|w_i \cdot A_i| = |A_i|$ para todo i.

Si $|\sum_{i=1}^{n} w_i \cdot A_i| \geq |G|$, entonces se tiene el Teorema con $H = G$.

Supongamos $|\sum_{i=1}^{n} w_i \cdot A_i| < |G|$. Como $|w_i \cdot A_i| = |A_i|$ para todo i, tenemos $|G| = |S| - n + 1 = \sum_{i=1}^{n} |w_i \cdot A_i| - n + 1$. Luego

$$|\sum_{i=1}^{n} w_i \cdot A_i| < \sum_{i=1}^{n} |w_i \cdot A_i| - n + 1 \tag{2.1}$$

Esto implica, por la Proposición 1.3.1 parte (iv), que $\sum_{i=1}^{n} w_i \cdot A_i$ es H- periódico con $H = \mathsf{H}(\sum_{i=1}^{n} w_i \cdot A_i)$ subgrupo propio no trivial de G. Supongamos que $\mathcal{A}$ fue seleccionado entre todas las n-particiones $\mathcal{A}' = A'^1 \cdot \ldots \cdot A'_n$ de S tales que $|w_i \cdot A'_i| = |A'_i|$, $\sum_{i=1}^{n} w_i \cdot A^1_i = \sum_{i=1}^{n} w_i \cdot A_i$ y $\sum_{i=1}^{n} |\phi_H(w_i \cdot A_i)|$ es también maximal.

Si para cada $i \geq 2$, $w_i \cdot A_i$ contiene un único elemento de alguna H-clase, entonces hay al menos $(n-1)(|H|-1)$ hoyos en todos los $w_i \cdot A_i$, pero la ecuación (2.1) y la Observación 1.3.1 parte (ii) nos llevan a una contradicción. Luego existe $j \leq 2$ tal que $w_j \cdot A_j$ no contiene elementos que sean el único representante de su $H-$clase en $w_j \cdot A_j$. En consecuencia $|\phi_H(w_j \cdot A_j)| < |w_j \cdot A_j|$ para algún $j \geq 2$. Supongamos que

$$\sum_{i=1}^{j} w_i \cdot A_i = \sum_{i=1}^{j-1} w_i \cdot A_i + w_j \cdot (A_j \setminus \{x\}) \tag{2.2}$$

para algún $x \in A_j$ tal que $\phi_H(w_j \cdot A_j) = \phi_H(w_j \cdot (A_j \setminus \{x\}))$.

Si existe r tal que $\phi_H(w_r x) \notin \phi_H(w_r \cdot A_r)$. Entonces la n-partición en conjuntos definida por $A'_j = A_j \setminus \{x\}$, $A'_r = A_r \cup \{x\}$ y $A'_i = A_i$ para $i \neq j, r$, contradice la maximalidad de $\sum_{i=1}^{n} |w_i \cdot A_i|$ o de $\sum_{i=1}^{n} |\phi_H(w_i \cdot A_i)|$. Luego $\phi_H(w_i x) \in \phi_H(w_i \cdot A_i)$ para todo i. Como $\sum_{i=1}^{n} w_i = 0 \pmod{\exp(G)}$, se tiene que $0 = \sum_{i=1}^{n} \phi_H(w_i x) \in \sum_{i=1}^{n} \phi(w_i \cdot A_i)$. Es decir, $H \subseteq (\sum_{i=1}^{n} w_i \cdot A_i) + H = \sum_{i=1}^{n} w_i \cdot A_i + H = \sum_{i=1}^{n} w_i \cdot A_i$ (dado que $\sum_{i=1}^{n} w_i \cdot A_i$ es H-periódico). En consecuencia $H \subseteq \sum_{i=1}^{n} w_i \cdot A_i \subseteq \Sigma_n(W, S)$ y se completa la prueba.

Supongamos que (2.2) no se cumple, entonces $\sum_{i=1}^{j} w_i \cdot A_i$ posee un elemento con expresión única, luego el Teorema 1.3.4 implica que

$$|\sum_{i=1}^{j} w_i \cdot A_i| \geq |\sum_{i=1}^{j-1} w_i \cdot A_i| + |w_j \cdot A_j| - 1. \tag{2.3}$$

Sea l, con $2 \leq l \leq n$, el menor entero, posiblemente reindizando los $w_i \cdot A_i$, tal que se cumple (2.3) para todo $j \geq l$ (notemos que de (2.3) y reindizando podemos suponer $j = n$, y se sigue que l existe). Entonces

$$|\sum_{i=1}^{l-1} w_i \cdot A_i| < \sum_{i=1}^{l-1} |w_i \cdot A_i| - (l-1) + 1. \tag{2.4}$$

De lo contrario, (2.3) implica $|\sum_{i=1}^{n} w_i \cdot A_i| \geq \sum_{i=1}^{n} |w_i \cdot A_i| - n - 1$, contradiciendo (2.1). Luego por la Proposición 1.3.1 parte (iv), $\sum_{i=1}^{l-1} w_i \cdot A_i$ es H'-periódico, con $H' < H$. Supongamos que para todo $2 \leq i \leq l-1$, $w_i \cdot A_i$ contiene un único elemento de alguna H-clase, entonces hay $(l-2)(|H'|-1)$ hoyos en todos los $w_i \cdot A_i$ y la Observación 1.3.1 parte (ii) nos llevan a una contradicción con la expresión (2.4). Luego debe existir un conjunto A_j, con $2 \leq j \leq l-1$, tal que $w_j \cdot A_j$ no contiene un elemento el cual es el único elemento de alguna H-clase en $w_j \cdot A_j$, así $|\phi(w_i \cdot A_i)| < |w_i \cdot A_j|$, para algún $2 \leq j \leq l-1$. Como $H' < H$, se tiene también que $|\phi(w_i \cdot A_i)| < |w_i \cdot A_j|$, para algún $2 \leq j \leq l-1$. Entonces por (2.3) se contradice la minimalidad de l. $\blacksquare$

Observemos que la condición $\sigma(W) \equiv 0 \pmod{\exp(G)}$ en el Teorema EGZP (2.4.1) es necesaria, de lo contrario, S con $\mathrm{supp}(S) = \{1\}$ puede generar un contraejemplo.

En [29] Hamidoune muestra el siguiente Teorema.

Teorema 2.4.2 *[29] Sea G un grupo abeliano finito, no trivial, sea W una secuencia de enteros de longitud $|G|$ con $\sigma(W) \equiv 0 \pmod{|G|}$ tal que todos, excepto a lo más un término de W, son primos relativos con $|G|$; y sea S una secuencia en G con $|S| \geq 2|G|-1$. Si $\mathsf{h}(S) \leq |G|$, entonces $\Sigma_{|G|}(W, S)$ contiene un subgrupo no trivial de G.*

Observemos que si $W = 1^{|W|}$, el Teorema 2.4.2 implica el Teorema EGZ y el Teorema de Olson (Teorema 2.3.3). Observar también que no es posible reemplazar la condición "primos relativos con $|G|$,"de los términos de W, por "no nulos"; ya que $G = \mathbb{Z}_{p^2}$, $W = (p)^{p^2}$ y $S = (p)^{p^2}(2p)^{p^2-2}$ generaría un contraejemplo, dado que, en este caso, $\Sigma_{|G|}(W, S) = \{0\}$. A partir del Teorema 2.4.2, Hamidoune formula la siguiente conjetura:

> Sea G un grupo abeliano finito, no trivial, sea $W = w_1 \cdot \ldots \cdot w_n$ una secuencia de enteros con $\sigma(W) \equiv 0 \pmod{|G|}$ tal que todos, excepto a lo más un término de W, son primos relativos con $|G|$; y sea S una secuencia en G con $|S| \geq |G| + n - 1 \geq |G| + 1$. Si $\mathsf{h}(S) \leq n$, entonces $\Sigma_n(W,\, S)$ contiene un subgrupo no trivial de G.

Esta conjetura será el tema de discusión en el Capítulo 3.

Capítulo 3

Sobre la conjetura de Hamidoune

Como hemos dicho en el Capítulo 2, en este Capítulo estudiaremos la Conjetura de Hamidoune.

Conjetura de Hamidoune: *Sea G un grupo abeliano finito, no trivial, sea $W = w_1 \cdot \ldots \cdot w_n$ una secuencia de enteros con $\sigma(W) \equiv 0 \pmod{|G|}$ tal que todos, excepto a lo más un término de W, son primos relativos con $|G|$; y sea S una secuencia en G con $|S| \geq |G| + n - 1 \geq |G| + 1$. Si $\mathsf{h}(S) \leq n$, entonces $\Sigma_n(W, S)$ contiene un subgrupo no trivial de G.*

Es claro que si todos los términos de W son primos relativos con $|G|$, la Conjetura de Hamidoune se sigue del Teorema EGZP (2.4.1). Otros ejemplos donde el Teorema EGZP implica la Conjetura de Hamidoune son los siguientes.

Ejemplo 3.0.1 *Si $W = w_1 \cdot \ldots \cdot w_n \in \mathcal{F}(\mathbb{Z})$ y $S \in \mathcal{F}(G)$ satisfacen las hipótesis de la Conjetura de Hamidoune y además $n \geq |G|$, entonces $\Sigma_n(W, S)$ contiene un* *subgrupo no trivial de G.*

Como $\mathsf{h}(S) \leq n$, existe una n-partición de S, digamos $A_1 \cdot \ldots \cdot A_n$. Si $|A_i| \geq 2$ para todo i, entonces $|S| \geq 2n \geq 2|G|$ pero $2|G| - 1 \leq |G| + n - 1 = |S|$, luego $2|G| - 1 \geq 2|G|$ lo cual es una contradicción, de modo que debe existir $j \in [1, n]$ tal que $|A_j| = 1$, sin perder generalidad supongamos $j = n$, entonces $|A_i| = |w_i \cdot A_i|$ para todo i y el Teorema EGZP (2.4.1) implica que se cumple la Conjetura de Hamidoune.

Ejemplo 3.0.2 *Si $W = w_1 \cdot \ldots \cdot w_n \in \mathcal{F}(\mathbb{Z})$ y $S \in \mathcal{F}(G)$ satisfacen las hipótesis de la Conjetura de Hamidoune y además $\mathsf{h}(S) < n$, entonces $\Sigma_n(W, S)$ contiene un subgrupo no trivial de G.*

$\mathsf{h}(S) < n$ implica que existe una $(n-1)$-partición de S, digamos $A_1 \cdot \ldots \cdot A_{n-1}$, es claro que existe $j \in [1, n]$ tal que $|A_j| \geq 2$ (ya que $|S| = |G| + n - 1 > n - 1$), sin perder generalidad, podemos suponer $j = n$, sea $a \in A_{n-1}$ y sea $A_n = \{a\}$, entonces $A_1 \cdot \ldots \cdot A_{n-1} \setminus \{a\} \cdot A_n$ es un n-partición de S con $|w_i \cdot A_i| = |A_i|$ para todo i, así el Teorema EGZP (2.4.1) implica que se cumple la Conjetura de Hamidoune.

3.1. Dos Contraejemplos a la Conjetura de Hamidoune

En la Sección anterior hemos visto algunos casos especiales donde se cumple la Conjetura de Hamidoune. Sin embargo los siguientes ejemplos muestran que la Conjetura de Hamidoune es falsa, en general. En el primer ejemplo, la secuencia de enteros W que hemos escogido es tal que $2 \leq |W| < \frac{1}{2}|G|$, y en el segundo, es tal que $\frac{1}{2}|G| \leq |W| \leq |G|$

Ejemplo 3.1.1 *Sea* $p > 3$ *primo tal que* $p \equiv -1 \pmod 4$, *sea* $G = \mathbb{Z}/p\mathbb{Z}$, $n = \frac{p-1}{2}$, $W = w_1 \cdot \ldots \cdot w_n$ *con* $w_i = 1$ *para* $i \in [1, (n-1)/2]$, $w_i = -1$ *para* $i \in [(n-1)/2+1, n-1]$ *y* $w_n = 0$; *y sea* $S = 0^n 1^n 2^n$. *Notemos que* $\mathsf{h}(S) = n = |W|$, $|W| = n = \frac{p-1}{2} < \frac{p}{2}$, $|S| = 3n = |G| + n - 1$, $\sigma(W) = 0$. *Para* $i \in [1, n]$, *sea* $A_i := \{0, 1, 2\}$, *es claro que los* A_i *forman una* n*-partición de* S. *Entonces por el Teorema de Cauchy-Davenport (Teorema 1.3.2),*

$$\begin{aligned} |\Sigma_n(W, S)| &= |\sum_{i=1}^{n} w_i \cdot A_i| \\ &\geq \min\{p, \sum_{i=1}^{n} |w_i \cdot A_i| - n + 1\} \end{aligned}$$

como $\sum_{i=1}^{n} |w_i \cdot A_i| - n + 1 = \sum_{i=1}^{n-1} |\{0, 1, 2\}| + 1 - n + 1 = 3(n-1) - n + 2 = p - 2$, *entonces* $|\Sigma_n(W, S)| \geq p - 2$, *así* $\Sigma_n(W, S) \neq \{0\}$. *Por otro lado* $\{\frac{p+1}{2}, \frac{p-1}{2}\} = \{n, n+1\} \nsubseteq \sum_{i=1}^{(n-1)/2} \{0, 1, 2\} - \sum_{i=1}^{(n-1)/2} \{0, 1, 2\} = \sum_{i=1}^{n} w_i \cdot A_i = \Sigma_n(W, S)$, *así* $\Sigma_n(W, S) \neq G$, *pero* $|G|$ *es primo, entonces* $\Sigma_n(W, S)$ *no contiene subgrupos propios no triviales, es decir, no se cumple la conjetura de Hamidoune.*

Ejemplo 3.1.2 *Sea* $m = 2^r$ *con* $r > 2$, $G = \mathbb{Z}/m\mathbb{Z}$, $n = m - 1$, $W = w_1 \cdot \ldots \cdot w_n$ *con* $w_i = 1$ *para* $i \in [1, (n-1)/2]$, $w_i = -1$ *para* $i \in [(n-1)/2+1, n-1]$ *y* $w_n = 0$; *y sea* $S = 0^n 1^n$. *Notemos que* $\mathsf{h}(S) = n = |W|$, $|W| = n = m - 1 = 2^r - 1 > 2^{r-1} = \frac{1}{2}|G|$ $|S| = 2n = |G| + n - 1$, $\sigma(W) = 0$. *Para* $i \in [1, n]$ *sea* $A_i := \{0, 1\}$, *es claro que los*

A_i forman una n-partición de S tal que $\Sigma_n(W,S) = \sum_{i=1}^{n} w_i \cdot A_i$, además

$$\begin{aligned}
\Sigma_n(W,S) &= \sum_{i=1}^{n} w_i \cdot A_i \\
&= \sum_{i=1}^{(n-1)/2} \{0,1\} - \sum_{i=1}^{(n-1)/2} \{0,1\} \\
&= \sum_{i=1}^{m/2-1} \{0,1\} - \sum_{i=1}^{m/2-1} \{0,1\} \\
&= \{0,1,2,\cdots,\frac{m}{2}-1\} + \{0,-1,-2,\cdots,-\frac{m}{2}+1\} \\
&= \{0,1,2,\cdots,\frac{m}{2}-1,\frac{m}{2}+1,\cdots,m-1\} \\
&= G \setminus \{\frac{m}{2}\}.
\end{aligned}$$

Pero todo subgrupo no trivial de $G \cong \mathbb{Z}/2^r\mathbb{Z}$ contiene un elemento de orden 2, y $\frac{m}{2} = 2^{r-1}$ es el único elemento de orden 2 de $G \cong \mathbb{Z}/2^r\mathbb{Z}$, luego $\Sigma_n(W,S)$ no contiene subgrupos propios no triviales.

3.2. Caracterización de los Contraejemplos a la Conjetura de Hamidoune Cuando $|W| \geq \frac{|G|}{2}$

En esta sección mostramos un resultado que caracteriza los contrajemplos de la Conjetura de Hamidoune cuando la secuencia de enteros W es suficientemente grande, específicamente cuando $|W| \geq \frac{|G|}{2}$, sin embargo, hemos vimos en la sección anterior un caso con $|W| \leq \frac{|G|}{2}$ donde la Conjetura también falla.

La Metodología que usamos está basada en

1. Teoremas de Teoría Aditiva, específicamente el Teorema de Kneser y los Lemas 1.4.1 y 1.4.2 (consecuencias del Teorema KST). El Teorema de Kneser es usado

para acotar inferiormente el conjunto suma de los términos de una partición de una secuencia dada, con el objeto de lograr que ésta represente a un grupo (o a un subgrupo) dado. El Teorema KST es usado cuando algún par de términos de la partición, digamos (A_i, A_j), es un par crítico, esto es, $|A_i + A_j| = |A_i| + |A_j| - 1$, especificamente tratamos el caso cuando cada término del par no es quasi periódico, este es el caso de los Lemas 1.4.1 y 1.4.2.

2. El Teorema EGZP (2.4.1) el cual confirma la Conjetura de Hamidoune en algunos casos.

Supongamos que se cumplen las hipótesis de la Conjetura de Hamidoune, sea $W = w_1 \cdot \ldots \cdot w_n$, donde w_n no necesariamente es primo relativo con $|G|$, y sea $A_1 \cdot \ldots \cdot A_n$ una n-partición de S, como w_i y $|G|$ son primos relativos para todo $i \in [1, n-1]$, entonces $|w_i \cdot A_i| = |A_i|$ para todo $i \in [1, n-1]$. Si lográramos construir una n-partición, digamos $\mathcal{A} = A_1 \cdot \ldots \cdot A_n$, de S de modo que $|w_n \cdot A_n| = |A_n|$, entonces el Teorema EGZP (2.4.1) garantiza que se cumple la conjetura de Hamidoune. Sin embargo, cuando $\mathsf{h}(S) = n - 1$ y más de un término en S tiene multiplicidad n no podemos garantizar que $|w_n \cdot A_n| = |A_n|$. Estudiaremos el caso $n \geq \frac{|G|}{2}$, lo que implica que S tiene a lo más 2 términos de multiplicidad n. Cuando $n < \frac{|G|}{2}$ perdemos el control sobre el número de términos de S con multiplicidad n y el estudio de la conjetura es más difícil.

Teorema 3.2.1 *Sea G un grupo abeliano finito, no trivial, sea $W = w_1 \cdot w_2 \cdot \ldots \cdot w_n$ una secuencia de enteros, de longitud $n \geq \frac{1}{2}|G|$, con $\sigma(W) \equiv 0 \pmod{|G|}$ tal que todos, excepto a lo más un término de W, son primos relativos con $|G|$; y sea S una* *secuencia en G con $|S| \geq |G| + n - 1 \geq |G| + 1$. Si $\mathsf{h}(S) \leq n$, entonces se cumple una de las siguientes alternativas.*

(i) $\Sigma_n(W, S) = W \cdot S$ *contiene un subgrupo no trivial.*

(ii) $|\mathrm{supp}(S)| = 2$, $|W| = |G| - 1$, $G \cong \mathbb{Z}/2^r\mathbb{Z}$ *y*

$$W \equiv x^{(n-1)/2}(-x)^{(n-1)/2}0 \pmod{|G|},$$

para algunos r, n, $x \in \mathbb{Z}^+$.

Demostración Podemos suponer $\mid S \mid = |G| + n - 1$. Si $\mathsf{h}(S) \leq n - 1$ entonces el Ejemplo 3.0.2 muestra que se cumple (i). Supongamos $\mathsf{h}(S) = n$, consideremos el conjunto $A_n := \{x_1, \ldots, x_r\}$ de todos los elementos diferentes en S con multiplicidad n, entonces la secuencia $S' = SA_n^{-1}$ tiene todos los elementos con multiplicidad menor o igual que $n - 1$, así existe una $(n-1)$-partición de S', digamos $\mathcal{A}' = A_1, ..., A_{n-1}$, y en consecuencia $\mathcal{A} = A_1 \cdot \ldots \cdot A_{n-1} \cdot A_n$ es una n-partición de S. Sabemos que $\mid w_i \cdot A_i \mid = \mid A_i \mid$ para todo $i \in [1, n-1]$.

Si $\mid w_n \cdot A_n \mid = \mid A_n \mid$, El Teorema EGZP implica que se cumple (i).

Si $\mid w_n \cdot A_n \mid < \mid A_n \mid$ entonces existe un par de elementos distintos $x, y \in A_n$ tal que $w_n x = w_n y$, es decir, tenemos que $x^n y^n \mid S$ y $w_n(x - y) = 0$. Sin perder generalidad, por traslación, podemos suponer que $x = 0$, así $\{0, y\} \subseteq A_i$ para todo $i \in [1, n]$. Observemos que la condición $n \geq \frac{|G|}{2}$ implica $|S| = |G| + n - 1 \leq 3n - 1$, de modo que existen exactamente dos términos de S con multiplicidad n, luego

$$2n \leq |S| \leq 3n - 1$$

1. Supongamos que $ord(y) < |G|$, donde $ord(y)$ denota el orden de y en G.

   Consideremos el conjunto $\sum_{i=1}^{n-1} w_i \cdot \{0, y\} + w_n 0 \subset W \cdot S$.

   Si $\sum_{i=1}^{n-1} w_i \cdot \{0, y\}$ es H-periódico entonces $H \subset \sum_{i=1}^{n-1} w_i \cdot \{0, y\} + w_n 0 \subset \Sigma_n(W, S)$.

   Supongamos que $\sum_{i=1}^{n-1} w_i \cdot \{0, y\} + w_n 0$ es aperiódico, entonces, por el Teorema de Kneser se tiene:

$$
\begin{aligned}
\mid \sum_{i=1}^{n-1} w_i \cdot \{0, y\} + w_n 0 \mid &\geq \sum_{i=1}^{n-1} \mid w_i \cdot \{0, y\} \mid + \mid \{w_n 0\} \mid -n + 1 \\
&= 2(n-1) - n + 2 = n \geq \frac{|G|}{2} \quad (hipotesis) \\
&\geq ord(y)
\end{aligned}
$$

   Es claro que $\sum_{i=1}^{n-1} w_i \cdot \{0, y\} + w_n 0 \subseteq \langle y \rangle$. Por lo tanto $\langle y \rangle = \sum_{i=1}^{n-1} w_i \cdot \{0, y\} + w_n 0 \subset \Sigma_n(W,\ S)$

2. Supongamos $\mathrm{ord}(y) = |G|$.

   En este caso G es cíclico. Sin perder generalidad podemos suponer $y = 1$, como $w_n(x - y) = 0$ y $x \neq y$ entonces $w_n \equiv 0 \pmod{|G|}$, luego $\sigma(W') = 0$, donde $W' = W w_n^{-1}$. Sea $\mathcal{A} = A_1 \cdot \ldots \cdot A_{n-1}$ una $(n-1)$-partición de $S' = S(01)^{-1}$. Notemos que $\{0, 1\} \subset A_i$ para todo i, luego $0 \in \sum_{i=1}^{n-1} w_i \cdot A_i + w_n 0 \subseteq \Sigma_n(W, S)$. Si $\sum_{i=1}^{n-1} w_i \cdot A_i + w_n 0$ es periódico, entonces $0 \neq \mathsf{H}(\sum_{i=1}^{n-1} w_i \cdot A_i + w_n 0) \subseteq \sum_{i=1}^{n-1} w_i \cdot A_i + w_n 0 \subseteq \Sigma_n(W, S)$ y se cumple la parte (i), análogamente, si algún $w_j \cdot A_j$ contiene un subconjunto H-periódico, como cada A_i contiene al cero, entonces $H \subseteq \sum_{i=1}^{n-1} w_i \cdot A_i + w_n 0 \subseteq \Sigma_n(W, S)$. Supongamos que $\sum_{i=1}^{n-1} w_i \cdot A_i + w_n 0$ es aperiódico y ningún A_i es quasi-periódico, entonces por el Teorema de Kneser:

$$\begin{aligned} \mid \sum_{i=1}^{n-1} w_i \cdot A_i \mid &= \mid \sum_{i=1}^{n-1} w_i \cdot A_i + w_n 0 \mid \\ &\geq \sum_{i=1}^{n-1} \mid w_i \cdot A_i \mid + \mid \{w_n 0\} \mid -n+1 \\ &= |G| + n - 1 - n + 2 - 2 \\ &= |G| - 1 \end{aligned}$$

Estudiaremos el caso

$$|\sum_{i=1}^{n} w_i \cdot A_i + w_n 0| = |G| - 1 \tag{3.1}$$

Pues de lo contrario $G \subset \sum_{i=1}^{n-1} w_i \cdot A_i + w_n 0 \subseteq \Sigma_n(W,S)$.

2.1 Si $|G|$ no es potencia de un primo.

Existen primos distintos p y q que dividen a $\mid G \mid$ entonces podemos seleccionar H, K subgrupos de G con $\mid H \mid = p$ y $\mid K \mid = q$ tales que $H \cap K = \{0\}$ (1er teorema de Sylow). En vista de (3.1), existe un único elemento en G que no está en $\Sigma_{|W|}(W,S)$ el cual es distinto de 0. Entonces $H \subseteq \sum_{i=1}^{n-1} w_i \cdot A_i \subseteq \Sigma_n(W,S)$ o $K \subseteq \sum_{i=1}^{n-1} w_i \cdot A_i \subseteq \Sigma_n(W,S)$.

2.2 Supongamos que $|G|$ es potencia de un primo, $m = p^r$, $r \geq 1$.

2.2.1 Supongamos que $2n+1 \leq \mid S \mid \leq 3n-2$ y $x(-x) \mid W'$ para algún $x \in \mathbb{Z}$.

Como $\mid S \mid \leq 3n-2$ y $\mathcal{A}$ es arbitraria, se sigue que $\mid A_i \mid = 2$ para algún i, digamos $i = n-1$ y que $\mid A_j \mid \geq 3$ para algún j, digamos

$j = n-2$, en consecuencia podemos suponer $x = w_{n-2}$ y $-x = w_{n-1}$. Sea $\alpha \in A_{n-2} \setminus \{0,1\}$. Observemos que:

$$\begin{aligned}
& \sum_{i=1}^{n-2} w_i \cdot A_i + w_{n-1}.(A_{n-1} \cup \alpha) \\
= \quad & \sum_{i=1}^{n-1} w_i \cdot A_i \cup \sum_{i=1}^{n-2} w_i \cdot A_i + w_{n-1} \cdot \alpha \\
= \quad & \sum_{i=1}^{n-1} w_i \cdot A_i \cup \sum_{i=1}^{n-3} w_i \cdot A_i + w_{n-2} \cdot A_{n-2} \setminus \{\alpha\} + w_{n-1} \cdot \alpha \\
& \cup \sum_{i=1}^{n-3} w_i \cdot A_i + w_{n-2}\alpha + w_{n-1}\alpha
\end{aligned}$$

Notar que los dos primeros términos de la derecha están contenidos en $\Sigma_n(W,S)$. Mas aún,

$$\begin{aligned}
w_{n-2}\alpha + w_{n-1}\alpha &= x\alpha - x\alpha = 0 \\
&= w_{n-2}0 + w_{n-1}0 \\
&\in w_{n-2} \cdot A_{n-2} + w_{n-1} \cdot A_{n-1}
\end{aligned}$$

Así $\sum_{i=1}^{n-2} w_i \cdot A_i + w_{n-1}.(A_{n-1} \cup \alpha) \subset \sum_{i=1}^{n-1} w_i \cdot A_i + w_n \cdot 0 \subset \Sigma_n(W,\, S)$. Como $\sum_{i=1}^{n-1} w_i \cdot A_i$ es aperiódico y $w_{n-1}\alpha \notin w_{n-1} \cdot A_{n-1}$ tenemos, por el Teorema de Kneser, que:

$$\begin{aligned}
\mid \sum_{i=1}^{n-2} w_i \cdot A_i + w_{n-1}(A_{n-1} \cup \alpha) \mid \quad &\geq \quad \sum_{i=1}^{n-2} \mid A_i \mid + \mid A_{n-1} \cup \alpha \mid \\
& \quad\; -(n-1) + 1 \\
&= \quad |G| + n - 1 - 2 + 1 - n + 1 + 1 \\
&= \quad |G|
\end{aligned}$$

Por lo tanto $G \subseteq \Sigma_n(W, S)$

2.2.2 Supongamos ahora que $\mid S \mid = 2n$.

Notemos que en este caso la partición es tal que $A_i = \{0, 1\}$ para todo i. Si $n = 2$ entonces $w_n = 0$ y $\sigma(W) = 0$ implican $w_1 = 0$ contradiciendo $\gcd(w_i, m) = 1$ para $i \leq n - 1$. Luego $n \geq 3$. Como $\mid S \mid = n + |G| - 1 = 2n$ y $n \geq 3$ se sigue que $|G| \geq 4$.

Consideremos un par de conjuntos arbitrarios A_i, A_j de la partición A, sabemos que ni $w_i \cdot A_i$ ni $w_j \cdot A_j$ contienen subconjuntos H-periódicos, así toda representación quasi-periódica de $w_i \cdot A$ y de $w_j \cdot A_j$ tiene parte H-periódica vacía y parte aperiódica $w_i \cdot A_i$ y $w_j \cdot A_j$ respectivamente. Por el Teorema de Kneser y (3.1) se tiene que $\mid w_i \cdot A_i + w_j \cdot A_j \mid = \mid A_i \mid + \mid A_j \mid -1$. Como cada $w_i \cdot A_i$ genera a G y contiene a 0 entonces, por el Lema 1.4.1, el par $(w_i \cdot A_i, w_j \cdot A_j)$ está en progresión aritmética con diferencia común, pero $w_i \cdot A_i = \{0, w_i\}$ y $w_j \cdot A_j = \{0, w_j\}$ entonces $w_i = \pm w_j$. Tenemos que $w_i = \pm w_j$ para todo i, j. Si todos los w_i son iguales entonces $0 = \sigma(W') = n \cdot w_i$ implicando que $w_1 = 0$ pero $\gcd(w_1, m) = 1$, luego $w_1(-w_1) \mid W'$, es decir, existe $x \in G$ tal que $x(-x) \mid W'$. En consecuencia, como $\sigma(W') = 0$, se tiene que $W' = (x)^{(n-1)/2}(-x)^{(n-1)/2}$ y $n - 1$ tiene que ser par. Dado que $|G| = n + 1$ es par y es potencia de un primo entonces $|G| = 2^r$ para algún $r > 0$ y se cumple (ii).

2.2.3 Supongamos $\mid S \mid > 2n$.

Si $n = 3$. Entonces, $w_n = 0$ y $\sigma(W) = 0$ implican $w_1 = -w_2$, es decir, existe $x \in G$ tal que $x(-x) \mid W'$. Como $2n <\mid S \mid \leq 3n-1$, entonces debido al caso 4.2.1 solo falta estudiar el caso $\mid S \mid = 3n-1 = 8$. Ahora $8 =\mid S \mid = n + |G| - 1 \Rightarrow 8 = 3 + |G| - 1 \Rightarrow |G| = 6$, contradiciendo el hecho que $|G|$ es potencia de un primo. Luego $n \geq 4$.

Como que $\{0, 1\}$ aparece n veces en la secuencia S y $\mid S \mid \leq 3n-1$ podemos seleccionar una partición A tal que $\mid A_i \mid \in \{2, 3\}$ para todo i. Sabemos que ningún $w_i \cdot A_i$ es quasi-periodico. Consideremos un par arbitrario $(w_i \cdot A_i, w_j \cdot A_j)$, por Lema 1.4.2, el par $(w_i \cdot A_i, w_j \cdot A_j)$ esta en progresión aritmética con diferencia común , entonces A_i y A_j están en progresión aritmética con diferencia común; pero la única forma que cualquier A_i esté en progresión aritmética es que su diferencia sea 1 o d donde d es tal que $2d = 1$, entonces la diferencia común es 1 o d tal que $2d = 1$, así el par $(w_i \cdot A_i, w_j \cdot A_j)$ está en progresion aritmética con diferencia común $w_i = \pm w_j$ o $w_i d = \pm w_j d$ en este último caso $(w_i \pm w_j)d = 0$ implica $w_i = \pm w_j (mod\ |G|)$,ya que $ord(d) = |G|$.

Como el par tomado anteriormente es arbitrario tenemos que $w_i = \pm w_j$ para todo i, j. Como en el caso anterior, no todos los w_i pueden ser iguales, luego $w_1(-w_1) \mid W'$, es decir existe $x \in G$ tal que $x(-x) \mid W'$. En consecuencia, como $\sigma(W') = 0$ se tiene que $W' = (x)^{(n-1)/2}(-x)^{(n-1)/2}$ y n tiene que ser impar. Debido a la parte 2.2.1 nos queda suponer $\mid S \mid = |G| + n - 1 = 3n - 1$ implicando $2n = |G|$. En consecuencia $|G|$ es par, como $|G|$ es potencia de un primo, se sigue que $|G| = 2^r$, pero $2n = |G| \geq 5$ implica que n es par, generando una contradicción. ■

Observemos que este Teorema extiende el Teorema de Hamidoune (Teorema 2.4.2), el cual verifica su conjetura en el caso $|W| = |G|$.

Conclusiones

En este trabajo se estudió la siguiente conjetura de Hamidoune [29]: Sea G un grupo abeliano finito, no trivial, sea $W \in \mathcal{F}(\mathbb{Z})$ con $|W| = n$ y $\sigma(W) \equiv 0(\mod |G|)$ tal que todos, excepto a lo más un término de W, son coprimos con $|G|$, y sea $S \in \mathcal{F}(G)$ con $|S| \geq |G| + n - 1 \geq |G| + 1$ tal que $\mathsf{h}(S) \leq n$, entonces $\Sigma_n(W, S)$ contiene un subgrupo no trivial de G.

Como resultado de este estudio se caracterizaron los contraejemplos a la Conjetura de Hamidoune cuando $n \geq \frac{|G|}{2}$, como herramientas principales se usaron el Teorema EGZP, el Teorema de Kneser y el Teorema de Estructura de Kemperman. También se mostró un contraejemplo a la conjetura con $n < \frac{|G|}{2}$. Como un problema abierto planteamos lo siguiente ¿Sera posible caracterizar los contraejemplos cuando $n < \frac{|G|}{2}$?

Hamidoune verificó su conjetura en el caso particular $|W| = |G|$ mediante el siguiente resultado: Sea G un grupo abeliano finito, no trivial, sea $W \in \mathcal{F}(\mathbb{Z})$ con $|W| = |G|$ y $\sigma(W) \equiv 0(\mod |G|)$ tal que todos, excepto a lo más un término de W, son coprimos con $|G|$, y sea $S \in \mathcal{F}(G)$ con $|S| \geq 2|G| - 1 \geq |G| + 1$ tal que $\mathsf{h}(S) \leq |G|$, entonces $\Sigma_{|G|}(W, S)$ contiene un subgrupo no trivial de G. Como un problema abierto planteamos la siguiente pregunta ¿Bajo que condiciones se puede disminuir el número de términos de W que son coprimos con $\exp(G)$ en el Teorema de Hamidoune?

Bibliografía

[1] A. Geroldinger and F. Halter-Koch, *Non-unique factorizations: Algebraic, combinatorial and analytic theory.* Pure and Applied Mathematics (Boca Raton), 278. Chapman & Hall/CRC, Boca Raton, FL, 2006.

[2] A.G. Vosper, The critical pairs of subsets of a group of prime order, *J. London Math. Soc*, 31 (1956) 200-205

[3] A. L. Cauchy, Recherches sur les nombres, *J. ´ Ecole polytech.*, 9 (1813), 99–116.

[4] D. J. Grynkiewicz, A Weighted Erdős-Ginzburg-Ziv Theorem, *Combinatorica*, 26 (2006), no. 4, 445–453.

[5] D. J. Grynkiewicz, *Sumsets, Zero-sums and Extremal Combinatorics*, Ph.D. Dissertation, Caltech (2005).

[6] D. J. Grynkiewicz, L. E. Marchan and O. Ordaz, Representation of finite abelian group elements by subsequences sums, *Journal de Téorie des Nombres de Bordeaux*, 21 (2009), no. 3, 559–587.

[7] H. Davenport, On the addition of residue classes, *J. London Math. Society*, 10 (1935), 30–32.

[8] H. B. Mann. Two addition theorems. *J. combinatorial Theory*, 3 (1967), 233-235.

[9] H. B. Mann. Addition theorem: The addition theorems of group theory and number theory., *Interscience publisher*, (1965).

[10] J. E. Olson, An addition theorem for finite abelian groups, *J. Number Theory*, 9 (1977), no. 1, 63-–70.

[11] J.H.B. Kemperman, On complexes in a semiroup, *Indag. Math*, 18 (1956), 247–254.

[12] J. H. B. Kemperman, On Small Sumsets in an Abelian Group, *Acta Math.*, 103 (1960), 63–88.

[13] M. DeVos, L. Goddyn and B. Mohar, A generalization of Kneser's Addition Theorem, *Advances in mathematics* 220 (2009), no 5, 1531–1548.

[14] M. Kneser, Abschätzung der asymptotischen Dichte von Summenmengen, *Math. Z.*, 58 (1953), 459–484.

[15] M. Kneser, Ein Satz über abelsche Gruppen mit Anwendungen auf die Geometrie der Zahlen, *Math. Z.*, 64 (1955), 429–434.

[16] M.Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Graduate Texts in Mathematics 165, Springer-Verlag, New York, 1996.

[17] N. Alon, A. Bialostocki and Y. Caro, The extremal cases in the Erdős-Ginzburg-Ziv Theorem, unpublished.

[18] O. Ordaz and D. Quiroz, Representation of group elements as subsequences sums, *Discrete Mathematics*, 308 (2008), no. 15, 3315–3321.

[19] P. Scherk, Distinct elements in a set of sums, *Amer. Math. Monthly*, 62 (1955), 46–47.

[20] Sukumar das Adhikari and Purusottam Rath, Davenport constant with weights and some related questions, *Integers*, 6 (2006), A30, 6 pp (electronic).

[21] Sukumar das Adhikari and Yong-Gao Chen, Davenport constant with weights and some related questions II, *J. Combin. Theory Ser. A*, 115 (2008), no. 1, 178–184.

[22] P. Erdős, A. Ginzburg and A. Ziv, Theorem in Additive Number Theory, *Bull. Res. Council Israel*, 10F (1961), 41–43.

[23] S. Griffiths, The Erdős-Ginzberg-Ziv theorem with units, to appear in *Discrete math.*

[24] A. Bialostocki, P. Dierker, D. J. Grynkiewicz, and M. Lotspeich, On Some Developments of the Erdős-Ginzburg-Ziv Theorem II, *Acta Arith.*, 110 (2003), no. 2, 173–184.

[25] W. Gao, Addition theorems for finite abelian groups, *J. Number Theory*, 53 (1995), 241–246.

[26] W. Gao and A. Geroldinger, Zero-sum problems in finite abelian groups: A survey, *Expositiones Mathematicae*, 24 (2006), no. 4, 337–369.

[27] W. Gao, and W. Jin, Weighted sums in finite cyclic groups, *Discrete Math.*, 283 (2004), no. 1-3, 243–247.

[28] Y. Caro, Zero-sum problems—a survey, *Discrete Math.*, 152 (1996), no. 1–3, 93–113.

[29] Y. O. Hamidoune, On weighted sequence sums, *Comb. Prob. Comput.*, 4 (1995), 363–367.

[30] Y. O. Hamidoune, On weighted sums in abelian groups, *Discrete Math.*, 162 (1996), 127–132.