# El Problema Inverso Asociado a la Constante de Davenport para Algunos Grupos de Rango Tres.

Smelin Teresa Pereira de Camacho.

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

Barquisimeto, julio 2014

# El Problema Inverso Asociado a la Constante de Davenport para Algunos Grupos de Rango Tres.

Por

Smelin Teresa Pereira de Camacho.

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

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

Barquisimeto, julio 2014

# Dedicatoria

$\mathcal{A}$

*Dios mi Creador, Sustentador y Redentor.*

*Mis hijos Samuel y Grecia.*

# Agradecimientos

*A mi Dios, quien hasta aquí me a ayudado. Alabado sea su Nombre.*

*A la doctora Luz Elimar Marchán por su invaluable ayuda e inspiración. Dios bendiga su intelecto.*

*A mi esposo Samuel por animarme con las palabras "sí se puede".*

*A mis hijos Samuel y Grecia. Por ser mi inspiración para concluir éste proyecto.*

*A mi padre Pastor, mi tía Magaly y mi hermana Yeraldine, por amar a mis hijos y cuidarlos en las horas que he dedicado a éste proyecto.*

*A mi hermana Yulimar por preguntar como va todo y desearme lo mejor.*

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

# Resumen

El problema inverso asociado a la constante de Davenport para grupos abelianos finitos, consiste en determinar la estructura de todas las secuencias minimales de suma cero de longitud maximal sobre este grupo. En este trabajo se estudia el problema inverso para grupos de la forma $C_2 \oplus C_2 \oplus C_{2n}$.

# Índice general

# Introducción

El objeto de estudio de la teoría combinatoria de números son las secuencias finitas de elementos en un grupo abeliano finito, generalmente no es necesario que estas secuencias sean ordenadas, sólo que permitan la repetición múltiple de elementos, por esta razón el término "multiconjunto" también es usado por algunos autores para referirse a las secuencias. El número de elementos o términos que aparecen en la secuencia es llamado *longitud de la secuencia*. Decimos que una secuencia es de *suma cero*, si la suma de sus términos es el elemento identidad (o cero) del grupo, en caso que la secuencia sea de suma cero, y no posea subsecuencias de suma cero, esta es llamada *secuencia minimal de suma cero*.

Un célebre problema abierto, introducido y estudiado por Roger en 1962 [11] en conexión con un problema de teoría algebraica de números, y popularizado posteriormente por Davenport, es el siguiente: ¿Cuál es la menor longitud que debe tener una secuencia en un grupo abeliano finito $G$ para que ésta posea una subsecuencia de suma cero?. Éste número es actualmente conocido como la *constante de Davenport* de $G$ y denotado por $\mathsf{D}(G)$, su existencia está garantizada por el, denominado por Erdős, "Lema prehistórico", el cual asegura que toda secuencia en un grupo abeliano finito, de longitud el orden del grupo, posee una subsecuencia de suma cero, es decir,

$\mathsf{D}(G) \leq |G|$. En particular, para grupos cíclicos finitos se conoce que $\mathsf{D}(G) = |G|$. Sin embargo, en general, el problema de hallar $\mathsf{D}(G)$ no es un problema fácil de resolver, para pocos grupos se conoce su valor exacto o resultados que permitan aproximarla a su valor exacto.

Existen diversas aplicaciones de la constante de Davenport en áreas relacionadas tales como la teoría de grafos, la teoría de Ramsey y geometría finita. Una de las aplicaciones más importantes se puede ver en la prueba de la infinitud de los números de Carmichael, por Alford, Granville y Pomerance [1]; además fué útil en un trabajo sobre teoría de números por Brüdern y Godinho [2], entre otras aplicaciones.

Es tradicional, en teoría combinatoria de números, el estudio del problema inverso asociado a diversos problemas directos, particularmente, ha recibido considerable atención el problema inverso asociado a la constante de Davenport, el cual consiste en determinar la estructura de las secuencias minimales de suma cero de longitud $\mathsf{D}(G)$, equivalente al problema de determinar la estructura de las secuencias libres de cero de longitud maximal. La motivación de investigación sobre este y otros problemas inversos de suma cero, no solo se debe al tradicionalismo sino también a las aplicaciones que tiene en la teoría de factorización no única, la cual estudia, entre otras cosas, los diversos fenómenos que surgen cuando se consideran factorizaciones, no necesariamente únicas, de enteros algebraicos, o de elementos de monoides de Krull, en factores irreducibles (ver [6] y [5]).

El problema inverso para grupos cíclicos ya ha sido estudiado sin mucha dificultad. Para grupos de rango 2 el problema inverso fué resuelto recientemente en [4] y [10]. Para grupos de rango 3 o mayor que 3 no se conocen resultados ni conjeturas

relacionadas con el problema inverso, excepto para 2-grupos elementales, donde el problema inverso tiene una solución muy conocida. En este trabajo se presenta una solución al problema inverso para grupos de la forma $C_2^2 \oplus C_{2n}$.

En el Capítulo 1 presentamos algunos resultados básicos relacionados con grupos abelianos finitos e introducimos la notación y terminología que usamos en el trabajo. En el capítulo 2 estudiamos la constante de Davenport, calculamos su valor para algunos grupos y la estimamos para otros, también establecemos una relación entre la constante de Davenport, la constante de Davenport restringida y la constante de Davenprot generalizada, finalmente en el Capítulo 3 mostramos parte de la estrutura de las secuencias minimales de suma cero y mostramos la solución del problema inverso asociado a la constante de Davenprot para grupos cíclicos y grupos de la forma $C_2 \oplus C_2 \oplus C_{2n}$.

La mayor parte de los resultados de este trabajo está fundamentada en [13].

# Capítulo 1

# Preliminares

Este Capítulo está dedicado a definir la terminología que usaremos a lo largo del trabajo, también recordamos algunos resultados básicos sobre grupos abelianos finitos y secuencias sobre grupos abelianos finitos, los cuales juegan un papel muy importante a la hora de tratar problemas de suma cero. Algunos resultados son presentados sin su demostración, dado que son resultados básicos y muy conocidos, sin embargo, los detalles de las pruebas pueden ser encontrados en [8] y [12].
Denotamos los números enteros no negativos y positivos por $\mathbb{N}_0$ y $\mathbb{N}$, respectivamente. Dados $a, b \in \mathbb{N}$ denotamos por $[a, b]$ el intervalo de enteros, es decir el conjunto $\{z \in \mathbb{N} : a \leq z \leq b\}$. Definimos $\max \emptyset = 0$.

## 1.1. Grupos Abelianos Finitos

En general, los problemas de suma cero son estudiados para grupos abelianos finitos, aunque recientemente se han generalizado algunos problemas para grupos no abelianos, donde el problema es aún mas arduo. En adelante trabajaremos con

grupos abelianos finitos los cuales denotaremos por $G$ y cuya operación binaria tendrá notación aditiva.

Un grupo abeliano $G$ se dice *p-elemental*, si existe un número primo $p$ tal que $px = 0$, para todo $x \in G$.

Sean $A$ 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 $A + B = B + A$.

El orden de $G$ es su cardinalidad, es decir, el número de elementos que tiene y lo denotamos por $|G|$.

Para un subconjunto $G_0 \subset G$, el subgrupo generado por $G_0$ es denotado por $\langle G_0 \rangle$. Si $G = \langle G_0 \rangle$ decimos que $G_0$ es un *conjunto generador de* $G$. Dado $g \in G$, el *orden de* $g$ es definido por

$$\text{ord}(g) := |\langle g \rangle| \in \mathbb{N}.$$

Para $n \in \mathbb{N}$, denotamos por $C_n$ a cualquier grupo cíclico de orden $n$. En particular, $C_1 = \{0\}$. Es bien sabido que si $g \in G$ es un elemento de orden $\text{ord}(g) = n \in \mathbb{N}$, entonces $\langle g \rangle \cong C_n$. Denotamos por $C_n^r$ la suma directa de $C_n$, consigo mismo, $r$ veces.

El *exponente de* $G$ se define como

$$\exp(G) := \text{mín}\{n \in \mathbb{N} : ng = 0, \ \forall g \in G\}$$

Sea $G$ un grupo abeliano finito y sea $H$ subgrupo de $G$, denotamos por $\varphi$ al epimorfismo canónico de $G$ en $G/H$.

**Definición 1.1.1** *Sea $G$ un grupo abeliano finito. Un subconjunto $E \subset G\backslash\{0\}$ es llamado independiente si $\sum_{e\in E} a_e e = 0$, con $a_e \in \mathbb{Z}$, implica que $a_e e = 0$ para cada $e \in E$. Un subconjunto de $G$ generador independiente es llamado una base de $G$.*

**Observación 1.1.1** *Si $G_0 \subset G\backslash\{0\}$ y $\prod_{g\in G_0} \mathrm{ord}(g) = |\langle G_0\rangle|$, entonces $G_0$ es independiente.*

*En efecto, sea $g_0 \in G_0$, fijo pero abitrario, y sea $H = \langle g_0\rangle$ y $K = \langle G_0 \setminus \{g_0\}\rangle$, es claro que $\langle G_0\rangle = H + K$, ahora*

$$\begin{aligned} |\langle G_0\rangle| = |H+K| &= \frac{|H||K|}{|H\cap K|} \textit{ ver 1.4.2 en [8]} \\ &\leq \frac{\mathrm{ord}(g_0)\prod_{g\in G_0\setminus\{g_0\}}\mathrm{ord}(g)}{|H\cap K|} = \frac{\prod_{g\in G_0}\mathrm{ord}(g)}{|H\cap K|} = \frac{|\langle G_0\rangle|}{|H\cap K|} \end{aligned}$$

*Luego $|H \cap K| \leq 1$, implicando que $H \cap K = \{0\}$. Hemos probado que para todo $g \in G_0$ tenemos que $\langle g\rangle \cap \langle G_0 \setminus \{g\}\rangle = \{0\}$. Ahora supongamos que $\sum_{g\in G_0} a_g g = 0$ para ciertos $a_g \in \mathbb{N}$. Si para algún $g_0 \in G_0$, $a_{g_0} g_0 \neq 0$, entonces $a_{g_0} g_0 = -\sum_{g\in G_0\setminus\{g_0\}} a_g g \in \langle G_0 \setminus \{g_0\}\rangle$ luego $a_{g_0} g_0 \in \langle g_0\rangle \cap \langle G_0 \setminus \{g_0\}\rangle = \{0\}$, lo cual es una contradicción dado que supusimos $a_{g_0} g_0 \neq 0$. De modo que $a_g g = 0$ para todo $g \in G_0$, en consecuencia $G_0$ es independiente.*

La Observación anterior implica la siguiente proposición.

**Proposición 1.1.1** *([12] pág 310) Un conjunto $G_0$ de elementos no nulos de un grupo abeliano finito $G$ es independiente si, y solo si $\langle G_0\rangle = \bigoplus_{g\in G_0} \langle g\rangle$*

La proposición 1.1.1 implica que un grupo abeliano finito $G$ contiene una base si, y solo si $G$ es suma directa de grupos cíclicos. El siguiente teorema, llamado

teorema fundamental para grupos abelianos finitamente generados, garantiza que todo grupo abeliano finito contiene una base.

**Teorema 1.1.1** *[8] Si $G$ es un grupo abeliano finitamente generado, entonces $G$ es (isomorfo a) suma directa finita de grupos cíclicos, en la cual los sumandos cíclicos finitos (si hay alguno) son de órdenes $n_1, n_2, ..., n_r$ donde $n_1 > 1$ y $n_1|n_2|\ldots|n_r$.*

En particular, si $G$ es un grupo abeliano finito, el teorema anterior implica que

$$G \cong C_{n_1} \oplus \cdots \oplus C_{n_r}$$

con $1 < n_1|...|n_r$. Observemos además que en este caso $\exp(G) = n_r$. Al entero $n_r$ lo llamamos *rango de* $G$, observar que, según el teorema 1.1.1, $n_r$ está únicamente determinado por $G$, por lo que el rango de $G$ está bien definido. También definimos

$$\mathsf{D}^*(G) = 1 + \sum_{i=1}^{r}(n_i - 1)$$

En particular $\mathsf{D}^*(0) = 1$. Si $G$ es cíclico entonces $\mathsf{D}^*(G) = |G|$.

## 1.2. Secuencias sobre Grupos Abelianos Finitos

Al estudiar los problemas de suma cero, el objeto principal de estudio son las *secuencias* finitas $S = g_1 g_2 \cdots g_l$, cuyos términos estan en un grupo abeliano $G$. 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 no única, se ha tratado a las

secuencias como elementos del monoide abeliano libre con base $G$, cuya operación binaria es la concatenación de las secuencias, adoptaremos dicha terminología y la definimos a continuación.

**Definición 1.2.1** *Una* secuencia *sobre un grupo abeliano finito $G$ es un elemento de el monoide abeliano libre sobre $G$, escrito multiplicativamente, denotado por $\mathcal{F}(G)$, esto es, si $S \in \mathcal{F}(G)$, $S$ se escribe de la forma*

$$S = \prod_{g \in G} g^{v_g} \quad con \quad v_g \in \mathbb{N}_0.$$

*Para cada secuencia $S$ existen $g_1, ..., g_l \in G$ únicamente determinados, salvo el orden, tal que*

$$S = \prod_{i=1}^{l} g_i.$$

El elemento neutro de $\mathcal{F}(G)$ es llamada la *secuencia vacía*, y denotada por 1.

**Definición 1.2.2** *Sean $S, T \in \mathcal{F}(G)$.*

1. *$T$ es una subsecuencia de $S$ y lo denotamos $T|S$, si $\mathsf{v}_g(T) \leq \mathsf{v}_g(S)$, $\forall g \in G$.*

2. *Si $T|S$ y $T \neq S$, $T$ es llamada* subsecuencia propia *de $S$.*

3. *si $T|S$, entonces $T^{-1}S$ denota el codivisor de $T$ en $S$, es decir, la única secuencia que satisface $T(T^{-1}S) = S$.*

Para secuencias $S_1, S_2 \in \mathcal{F}(G)$, la notación $\mathrm{mcd}(S_1, S_2)$ es usada para denotar el máximo común divisor de $S_1$ y $S_2$ en $\mathcal{F}(G)$, definido como,

$$\mathrm{mcd}(S_1, S_2) = S \in \mathcal{F}(G),$$

si $S \mid S_1, S \mid S_2$ y $R \mid S$ para cualquier secuencia $R$ con $R \mid S_1$ y $R \mid S_2$.

Sea $S = \prod_{g \in G} g^{v_g} \in \mathcal{F}(G)$. Usaremos la siguiente notación:

- Para cada $g \in G$, el número $\mathbf{v}_g(S) = v_g$ es llamado la *multiplicidad de $g$ en $S$*.
- $|S| := \sum_{g \in G} \mathbf{v}_g(S)$ denota la *longitud de $S$*.
- $h(S) := \max\{\mathbf{v}_g(S) : g \in G\}$ denota la *altura de $S$*.
- $\sigma(S) := \sum_{g \in G} \mathbf{v}_g(S)g$ denota la *suma de $S$*, observemos que $\sigma(1) = 0$ (recordar que la secuencia 1 es la secuencia vacía).
- El conjunto $\sum(S) := \{\sigma(T) : 1 \neq T|S\}$ denota el conjunto de *subsumas de $S$*.
- El conjunto $\text{supp}(S) := \{g \in G : \mathbf{v}_g(S) \geq 1\}$. es llamado *soporte* de $S$.
- $-S$ es usada para denotar la secuencia $\prod_{g \in G}(-g)^{v_g}$, y para $g_0 \in G$, $g_0 + S$ denota la secuencia $\prod_{g \in G}(g_0 + g)^{v_g}$.
- Para $T_1, T_2 \mid S$ decimos que $T_1$ y $T_2$ son subsecuencias disjuntas de $S$ si y sólo si $supp(T_1) \cap supp(T_2) = \emptyset$.

**Definición 1.2.3** *Una secuencia $S \in \mathcal{F}(G)$ es llamada* secuencia corta *si $1 \leq |S| \leq exp(G)$ y es llamada* secuencia libre de cuadrados *si $v_g(S) \leq 1$ para cada $g \in G$.*

**Definición 1.2.4** *Sea $S \in \mathcal{F}(G)$. Decimos que $S$ es*

1. Libre de suma cero *si* $0 \notin \sum(S)$.
2. *Una* secuencia de suma cero *si* $\sigma(S) = 0$.

*3.* Minimal de suma cero *si* $S \neq \emptyset$, $\sigma(S) = 0$ *y* $\sigma(T) \neq 0$ *para cada subsecuencia propia y no vacía* $T$ *de* $S$.

*El conjunto de todas las secuencias de suma cero sobre* $G$ *es denotado por* $\mathcal{B}(G)$*; y el conjunto de todas las secuencias minimales de suma cero es denotado por* $\mathcal{A}(G)$.

El siguiente resultado esencialmente muestra que toda secuencia de longitud $|G|$ posee una subsecuencia de suma cero, este resultado fué uno de los primeros resultado en el área de teoría combinatoria de números 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 1.2.1** *Toda secuencia sobre un grupo abeliano finito* $G$ *de longitud* $|G|$ *posee una subsecuencia no vacía de suma cero.*

**Demostración.** Sea $m := |G|$ y $S = g_1 g_2 \dots g_m \in \mathcal{F}(G)$. Necesitamos mostrar que $S$ tiene una subsecuencia no trivial de suma cero. Para cada $i \in \{1, \dots m\}$, definimos $S_i = g_1 g_2 \dots g_i$. Notemos que si $\sigma(S_i) = \sigma(S_j)$ con $i < j$, entonces $g_{i+1} \dots g_j$ es una subsecuencia no trivial de $S$ de suma cero, como se deseaba. Supongamos que todos los $\sigma(S_i)$ son distintos, entonces $A = \{\sigma(S_1), \sigma(S_2), \dots, \sigma(S_m)\}$ es un subconjunto de $G$ de cardinalidad $m = |G|$, implicando que $A = G$, de modo que $0 \in A$, es decir, existe $i \in \{1, \dots m\}$ tal que $\sigma(S_i) = 0$, como queríamos demostrar. ■

**Observación 1.2.1** *(i) El conjunto* $\mathcal{B}(G)$ *es un submonoide de* $\mathcal{F}(G)$.

*(ii) Cada función* $f : G \to G'$ *entre grupos abelianos* $G$ *y* $G'$ *puede ser extendida en forma única a un función de monoides de* $\mathcal{F}(G)$ *en* $\mathcal{F}(G')$*, la cual también*

*denotamos por $f$, y está dada por $f(S) = f(g_1 g_2 \dots g_l) = f(g_1) f(g_2) \dots f(g_l)$; observemos que si $f$ es un homomorfismo de grupos, entonces $f(\mathcal{B}(G)) \subset \mathcal{B}(G')$.*

## Una Relación entre el Conjunto de Secuencias de Suma Cero y la Factorización en Monoides Atómicos

Ahora recordamos algunas definiciones sobre factorización en monoides y lo relacionamos con el conjunto de secuencias de suma cero sobre un grupo abeliano finito $G$.

**Definición 1.2.5** *Sea $M$ un monoide abeliano*

1. *Un elemento $u \in M$ es llamado un* átomo, o elemento irreducible, *si $u$ no es invertible en $M$ y, para todo $a, b \in M$, $u = ab$ implica que $a$ es invertible o $b$ es invertible. El conjunto de átomos en $M$ es denotado por $\mathcal{A}(M)$.*

2. *$M$ se llama* monoide atómico *si todo elemento no invertible de $M$ se escribe como producto de un número finito de elementos irreducibles (átomos).*

Sea $M$ un monoide atómico.

- Si $a \in M$ no es invertible, $a = u_1 \cdots u_n$ con $u_i \in M$ irreducible, entonces $n$ es llamada la longitud de ésta factorización de $a$. Además, el *conjunto de longitudes de $a$* , denotado $\mathbf{L}(a)$, es el conjunto de todos los $n$ tal que $a$ tiene una factorización en irreducibles, de longitud $n$. Para $e \in M$ elemento invertible, definimos $\mathbf{L}(e) = \{0\}$.

- El conjunto $\mathcal{L}(M) := \{\mathbf{L}(a) : a \in M\}$ es llamado el sistema de conjuntos de longitudes de $M$.

**Ejemplo 1.2.1** *Sea $G$ un grupo abeliano finito. $\mathcal{B}(G) = \{S \in \mathcal{F}(G)/\ \sigma(S) = 0\}$ es un monoide átomico. El único elemento invertible de $\mathcal{B}(G)$ es la secuencia 1, así los elementos irreducibles de $\mathcal{B}(G)$ son las secuencias minimales de suma cero, es decir, los elementos de $\mathcal{A}(G)$. Por conveniencia de notación, escribiremos $\mathcal{L}(G)$ en lugar de $\mathcal{L}(\mathcal{B}(G))$ y nos referimos a este conjunto como el sistema de conjuntos de longitudes de $G$.*

**Ejemplo 1.2.2** *Consideremos el grupo abeliano finito $\mathbb{Z}_5$ y la secuencia $S = 01233344 \in \mathcal{B}(\mathbb{Z}_5)$. $S$ puede factorizarse como producto de 3 y 4 secuencias minimales de suma cero como sigue:*

$$S = (0)(244)(3331)$$

$$S = (0)(14)(23)(334).$$

*Nótese que no es posible factorizar a $S$ como producto de dos secuencias minimales de suma cero, pues una de ellas tendría que ser 0 y la otra 1233344, la cual no es minimal. Para factorizar a $S$ como producto de 5 o más secuencias minimales de suma cero, dicha factorización debería tener 2 o más secuencias de longitud 1 y suma cero, lo cual no es posible pues $\mathbf{v}_0(S) = 1$. Luego $\mathbf{L}(S) = \{3, 4\}$.*

Si consideramos, para algún $S \in \mathcal{F}(G)$, $S = \prod_{i=1}^{l} S_i$ con secuencias $S_i \in \mathcal{F}(G)$, ésta es llamada una descomposición de $S$. En el caso de que $S_i \in \mathcal{A}(G)$ decimos que se trata de una factorización de $S$, en tal caso se tendrá necesariamente que $S \in \mathcal{B}(G)$.

# Capítulo 2

# Constantes de Suma Cero

En este Capítulo estudiaremos la constante de Davenport y algunas constantes de suma cero relacionadas con ella, además daremos algunos ejemplos del cálculo y estimación de dichas constantes de suma cero para algunos grupos abelianos finitos, en especial para los grupos de la forma $C_2^3$.

## 2.1. La Constante de Davenport y Algunas de sus Variantes

**Definición 2.1.1** *Sea $G$ un grupo abeliano finito. La* constante de Davenport *de $G$, denotada por $\mathsf{D}(G)$, se define como la longitud máxima de una secuencia minimal de suma cero sobre $G$, es decir, el mayor entero positivo $t$ tal que existe una secuencia $g_1 g_2 \dots g_t$ con $g_i \in G$ tal que $\sum_{i=1}^{t} g_i = 0$ y $\sum_{i \in I} g_i \neq 0$ para cada $\emptyset \neq I \subseteq [1,t]$, con nuestra notación,*

$$\mathsf{D}(G) := \max\{|A| : A \in \mathcal{A}(G)\}$$

Notemos que $\mathsf{D}(G)$ también puede definirse como el menor entero positivo $t$ tal que toda secuencia de longitud $t$ posee una subsecuencia no trivial de suma cero. Observemos también que el Teorema 1.2.1 implica que

$$\mathsf{D}(G) \leq |G|.$$

Esta cota garantiza la existencia de $\mathsf{D}(G)$.

**Ejemplo 2.1.1** $\mathsf{D}(C_n) = n$, *donde* $C_n$ *es un grupo cíclico de orden* $n$. *En efecto, la secuencia* $S = e^{|G|-1}$, *donde* $e$ *es el generador de* $C_n$, *no posee subsecuencias de suma cero, así* $\mathsf{D}(Cn) \geq |C_n|$. *Luego el Teorema 1.2.1 implica que* $\mathsf{D}(C_n) = |C_n| = n$.

**Observación 2.1.1** *Sea* $G$ *un grupo abeliano finito entonces*

$$\mathsf{D}^*(G) \leq \mathsf{D}(G) \leq |G|.$$

*Para ver la primera desigualdad supongamos que* $G \cong \bigoplus_{i=1}^{r} C_{n_i}$ *donde* $n_1|n_2|\ldots|n_r$, *sea* $\{e_1, e_2, \ldots, e_{n_r}\}$ *una base de* $G$ *tal que* $|e_i| = n_i$ *y consideremos la secuencia* $S = \prod_{i=1}^{r} e_i^{n_i-1}$ *, es claro que* $|S| = \mathsf{D}^*(G) - 1$ *y como los* $e_i$ *son elementos independientes, entonces* $S$ *no posee subsecuencias de suma cero.*

En particular cuando $G$ es cíclico $\mathsf{D}^*(G) = \mathsf{D}(G)$ (ver Ejemplo 2.1.1). Inicialmente se pensó que siempre se cumplía tal igualdad, pero en general la igualdad no se cumple, por ejemplo, Geroldinger y Schneider [7] en 1992 mostraron que para todo grupo de rango mayor que 3, existen infinitos casos donde $\mathsf{D}(G) > \mathsf{D}^*(G)$.

**Ejemplo 2.1.2** $\mathsf{D}(C_2^3) = 4$. *Por Observación 2.1.1 sabemos que* $\mathsf{D}(C_2^3) \geq \mathsf{D}^*(C_2^3) = (2-1) + (2-1) + (2-1) + 1 = 4$. *Por otro lado, si* $A \in \mathcal{F}(C_2^3)$ *y* $|A| = 4$

*entonces* $A = a_1a_2a_3a_4$ *con* $a_i \in C_2^3$ *para todo* $i \in [1,4]$. *Si* $a_i = 0$ *para algún* $i \in [1,4]$ *entonces* $A$ *posee una subsecuencia no vacía que suma cero, si* $a_i = a_j$ *para* $i, j \in [1,4], i \neq j$ *entonces la secuencia no vacía* $a_ia_j \mid A$ *es de suma cero. Supongamos que* $a_i \neq a_j \neq 0$ *para todo* $i, j \in [1,4], i \neq j$ *entonces el conjunto* $\{a_1, a_2, a_3, a_4\} \subset C_2^3 \setminus \{0\}$ *tiene cardinalidad 4, luego éste debe ser dependiente ya que la base de* $C_2^3$ *tiene cardinalidad 3. Por tanto* $\sum_{i=1}^{4} n_ia_i = 0$, *para* $n_i \in \mathbb{Z}$ *no todos nulos, más aún, debido a que el rango de* $C_2^3 \cong C_2 \oplus C_2 \oplus C_2$ *es dos,* $n_i \in \{0,1\}$, *luego existe una subsecuencia no vacía de* $A$ *de suma cero, de modo que* $\mathsf{D}(C_2^3) \leq 4$.

En general, no es fácil calcular el valor exacto de la constante de Davenport para cualquier grupo abeliano finito. Este es un problema abierto que se ha diversificado mucho y ciertas variantes sobre esta constante han dado lugar a numerosas constantes de suma cero que han sido estudiadas los ultimos años. Una de las variantes de la constante de Davenport es la constante de Davenport generalizada, la cual definimos a continuación.

**Definición 2.1.2** *Sea* $G$ *un grupo abeliano finito y* $k \in \mathbb{N}$. *La* costante de Davenport generalizada *de* $G$, *denotada por* $\mathsf{D}_k(G)$, *se define como el menor entero positivo* $t$ *tal que toda secuencia de longitud* $t$ *posee* $k$ *subsecuencias disjuntas de suma cero. O, equivalentemente*

$$\mathsf{D}_k(G) := \max\{|B| : B \in \mathcal{B}(G), \max \mathbf{L}(B) \leq k\}$$

Nótese que $\mathsf{D}_k(G) \leq k\mathsf{D}(G)$, de manera que $\mathsf{D}_k(G)$ esta bien definida. La constante $\mathsf{D}_k(G)$ fue considerada por primera vez por Halter-Koch [9] al resolver algunos problemas de factorización no única, además se le encontró utilidad, como veremos

mas adelante, como parte de un método inductivo para determinar la constante de Davenport de ciertos grupos [3].

Otra variante conocida de la constante de Davenport, es la constante de Davenport restringida.

**Definición 2.1.3** *Sea $G$ un grupo abeliano finito y $k \in N$, $k \geq \exp(G)$. La* $k$-constante de Davenport restringida *, denotada por $\mathsf{D}^k(G)$, se define como el menor entero positivo $t$ tal que toda secuencia de longitud $t$, posee una subsecuencia de suma cero y longitud menor o igual a $k$. Particularmente la constante $\mathsf{D}^{\exp(G)}(G)$ es denotada por $\eta(G)$.*

Nótese que $\mathsf{D}^k(G) \leq k|G|$, de manera que $\mathsf{D}^k(G)$ esta bien definida, en efecto, Sea $S$ una secuencia de elementos de $G$ con $|S| = k|G|$. Si $\forall g \in supp(S)$, $v_g(S) < k$ entonces $|S| = \sum_{g \in supp(S)} v_g(S) < k|supp(S)| \leq k|G|$, en contradicción con el hecho de que $|S| = k|G|$, luego existe $g \in supp(S)$ tal que $v_g(S) \geq k$. Sea $T = \prod_{i=1}^{\exp(G)} g \mid S$ $(v_g(S) \geq k \geq \exp(G))$ entonces $\sigma(T) = 0$. De modo que, toda secuencia de longitud $k|G|$ posee una subsecuencia de suma cero y longitud menor o igual a k. Por tanto, $\mathsf{D}^k(G) \leq k|G|$.

A continuación presentamos algunos resultados que relacionan las constantes de suma cero que hemos definido.

**Lema 2.1.1** *Sea $G$ un grupo abeliano finito. Si $\mathsf{D}^k(G) \leq \mathsf{D}_i(G) + k$, entonces $\mathsf{D}_{i+1}(G) \leq \mathsf{D}_i(G) + k$.*

**Demostración.** Sea $S$ una secuencia de elementos de $G$ con $|S| = \mathsf{D}_i(G) + k$. Veamos que existen $i+1$ subsecuencias disjuntas de $S$ de suma cero. Como $\mathsf{D}^k(G) \leq \mathsf{D}_i(G) + k$, existe $S^1|S$ con $|S^1| \leq k$ tal que $\sigma(S^1) = 0$. Así $|S(S^1)^{-1}| \geq \mathsf{D}_i(G)$, luego $S(S^1)^{-1}$ contiene $i$ subsecuencias disjuntas, cada una de suma cero. En consecuencia $\mathsf{D}_{i+1}(G) \leq \mathsf{D}_i(G) + k$. ■

**Corolario 2.1.1** *Sea $G$ un grupo abeliano finito. Si $\mathsf{D}^k(G) \leq \mathsf{D}_i(G) + k$, entonces $\mathsf{D}_{i+n}(G) \leq \mathsf{D}_i(G) + nk$.*

**Demostración.** La prueba es por inducción sobre $n$, el caso $n = 1$ es el Lema 2.1.1. Supongamos que es cierto para $n$ y lo probaremos para $n+1$. Sea $S \in \mathcal{F}(G)$ con $|S| = \mathsf{D}_i(G) + (n+1)k$. Por hipótesis, existe $S^1|S$ con $|S^1| \leq k$ y $\sigma(S^1) = 0$. Luego $|S(S_i)^{-1}| \geq \mathsf{D}_i(G) + nk$, y por hipótesis inductiva, es posible construir $n + i$ subsecuencias disjuntas, cada una con suma cero. ■

**Proposición 2.1.1** *Sea $G$ un grupo finito (no necesariamente abeliano). Sea $H$ un subgrupo de $G$. Entonces $\mathsf{D}_k(G) \leq \mathsf{D}_{\mathsf{D}_k(H)}(G/H)$.*

**Demostración.** Sea $M = \mathsf{D}_k(H)$ y $t = \mathsf{D}_M(G/H)$. Sea $S = g_1 g_2 \dots g_t \in \mathcal{F}(G)$, probaremos que existen $k$ subsecuencias disjuntas de $S$ de suma cero. Consideremos el homomorfismo natural $\varphi : G \to G/H$, y la secuencia inducida $\varphi(S) \in \mathcal{F}(G/H)$ dada por $\varphi(S) = \prod_{i=1}^{t}(g_i + H)$. Por definición de $D_M(G/H)$, existen $I_j \subseteq [1, t]$, con $1 \leq j \leq M$, tales que $\sum_{i \in I_j}(g_i + H) = 0_{G/H}$, esto significa que $\sum_{i \in I_j}(g_i) \in H$, para todo $1 \leq j \leq M$. Nótese que $(\sum_{i \in I_1}(g_i))(\sum_{i \in I_2}(g_i)) \dots (\sum_{i \in I_M}(g_i))$ es una secuencia de elementos de $H$ de longitud $M = D_k(H)$. Luego, por definición de

$D_k(H)$, existen $T_r \subseteq [1, M]$, con $1 \leq r \leq k$, tales que $\sum_{j \in T_r} \sum_{i \in I_j} (g_i) = 0$, lo cual prueba la proposición. ■

**Observación 2.1.2** *Sea $G$ un grupo finito y $H$ un subgrupo de $G$. Entonces*

$$\mathsf{D}(G) \leq \mathsf{D}_{\mathsf{D}(H)}(G/H)$$

.

**Observación 2.1.3** $\mathsf{D}^2(C_2^3) \leq 8$*, en efecto, como* $|C_2^3| = 8$ *y los elementos de* $C_2^3$ *son de orden* 2*, entonces toda secuencia de longitud* 8 *sobre* $C_2^3$*, contiene al cero o tiene un elemento de multiplicidad mayor o igual que 2, en cualquier caso es posible encontrar una subsecuencia de suma cero de longitud a lo mas 2.*

**Lema 2.1.2** $\mathsf{D}_k(C_2^3) = 2k + 3$ *para* $k \geq 2$.

**Demostración.** Veamos que $\mathsf{D}_2(C_2^3) \leq 2 \cdot 2 + 3 = 7$. Sea $S \in \mathcal{F}(C_2^3)$ con $|S| = 7$, si $0|S$ o para algún $g|S$ $\mathsf{v}_g(S) \geq 2$, es posible obtener $S_0|S$ tal que $\sigma(S_0) = 0$ y $|S_0| \leq 2$, así $|S(S_0)^{-1}| \geq 5 \geq 4 = \mathsf{D}(C_2^3)$, en consecuencia $S(S_0)^{-1}$ posee una subsecuencia de suma cero, luego $S$ posee dos subsecuencias disjuntas de suma cero. Si $0 \nmid S$ y $\mathsf{v}_g(S) = 1$ para todo $g|S$, entonces $S = \prod_{g \in C_2^3 \setminus \{0\}} (g)$, y es fácil ver que $S$ posee dos subsecuencias de suma cero, en efecto, $S = e_1e_2e_3(e_1+e_2)(e_1+e_3)(e_2+e_3)(e_1+e_2+e_3)$, con $\{e_1, e_2, e_3\}$ base de $C_2^3$ entonces $e_1e_2e_3(e_1+e_2+e_3), (e_1+e_2)(e_1+e_3)(e_2+e_3) \mid S$ suman cero.

En la Observación 2.1.3 verificamos que $\mathsf{D}^2(C_2^3) \leq 8$. Sea $\{e_1, e_2, e_3\}$ base de $C_2^3$, la secuencia $S = e_1e_2e_3(e_1 + e_2)(e_1 + e_3)(e_2 + e_3)$ no posee dos subsecuencias disjuntas

de suma cero, entonces $\mathsf{D}_2(C_2^3) \geq 7$. Por lo tanto

$$\mathsf{D}^2(C_2^3) \leq 8 < 2 + 7 \leq 2 + \mathsf{D}_2(C_2^3).$$

Luego aplicando el Corolario 2.1.1 con $n = k-2, i = 2$ y $s = 2$ tenemos $\mathsf{D}_k(C_2^3) \leq 2k+3$ para $k \geq 2$.

Por otra parte, consideremos $g_0 \in G \setminus \{0\}$ y sea $S = g_0^{2k-4} \prod_{g \in G \setminus \{0, g_0\}} \in \mathcal{F}(C_2^3)$, $S$ no contiene $k$ subsecuencias disjuntas de suma cero, luego $\mathsf{D}_k(C_2^3) \geq 2k+3$. ■

## 2.2. Cotas para la Constante de Davenport Generalizada

**Observación 2.2.1** *Si* $|S| \geq \eta(G) + k \exp(G)$ *con* $k \in \mathbb{N}_0$ *entonces* $S$ *tiene al menos* $k+1$ *subsecuencias cortas de suma cero, en particular,* $\mathsf{D}_{k+1}(G) \leq \eta(G) + k \exp(G)$.

En efecto, procederemos por inducción sobre $k$. Para $k = 0$, $|S| \geq \eta(G)$, por definición de $\eta(G)$, $S$ posee una subsecuencia de suma cero de longitud menor o igual que $\exp(G)$. Supongamos que para $S \in \mathcal{F}(G)$ con $|S| \geq \eta(G) + (k-1)\exp(G)$, $S$ posee al menos $k$ subsecuencias de suma cero de longitud menor o igual que $\exp(G)$. Sea $S \in \mathcal{F}(G)$ con $|S| \geq \eta(G) + k\exp(G)$. Dado que $|S| \geq \eta(G) + k\exp(G) \geq \eta(G) + (k-1)\exp(G)$ por hipótesis inductiva, existen $S_1 S_2 \ldots S_k \mid S$ tales que

$\sigma(S_i) = 0$ y $|S_i| \leq \exp(G)$. Sea $T = (S_1 S_2 \dots S_k)^{-1} S \mid S$,

$$\begin{aligned} |T| &= |S| - |S_1 S_2 \dots S_k| \\ &\geq \eta(G) + k\exp(G) - \sum_{i=1}^{k} |S_i| \\ &\geq \eta(G) + k\exp(G) - \sum_{i=1}^{k} \exp(G) \\ &= \eta(G) \end{aligned}$$

así, existe $S_{k+1} \mid T$ tal que $\sigma(S_{k+1}) = 0$ y $|S_{k+1}| \leq \exp(G)$ por tanto $S$ posee al menos $k+1$ subsecuencias de suma cero de longitud menor o igual que $\exp(G)$.■

**Definición 2.2.1** *Sea $G$ un grupo abeliano finito definimos*

$$\mathsf{D}'_0(G) = \text{máx}\{\mathsf{D}(G) - \exp(G), \eta(G) - 2\exp(G)\}.$$

**Observación 2.2.2** *Si es $G$ un grupo abeliano finito y $G_1$ es un subgrupo de $G$ tal que $G \cong G_1 \oplus C_{exp(G)}$, lo cual siempre es posible por el Teorema Fundamental para Grupos Abelianos Finitos (1.1.1), entonces*

$$k\exp(G) + (\mathsf{D}(G_1) - 1) \leq \mathsf{D}_k(G) \leq k\exp(G) + \mathsf{D}'_0(G).$$

Sea $M = k\exp(G) + \text{máx}\{D(G) - \exp(G), \eta(G) - 2\exp(G)\}$. Veamos que $\mathsf{D}_k(G) \leq M$, en efecto,

para $k = 1$,

$$\begin{aligned} \mathsf{D}_k(G) = \mathsf{D}_1(G) = \mathsf{D}(G) &= \exp(G) + [\mathsf{D}(G) - \exp(G)] \\ &\leq \exp(G) + \text{máx}\{\mathsf{D}(G) - \exp(G), \eta(G) - 2\exp(G)\} \\ &= M. \end{aligned}$$

Supongamos $k \geq 2$. Sea $B \in \mathcal{B}(G)$ con $|B| > M$ y sea $N = \left\lceil \frac{|B|-\eta(G)+1}{\exp(G)} \right\rceil$ entonces

$$\begin{aligned} N = \left\lceil \frac{|B| - \eta(G) + 1}{\exp(G)} \right\rceil &> \left\lceil \frac{k\exp(G) + \max\{D(G) - \exp(G), \eta(G) - 2\exp(G)\} - \eta(G) + 1}{\exp(G)} \right\rceil \\ &\geq \left\lceil \frac{k\exp(G) + \eta(G) - 2\exp(G) - \eta(G) + 1}{\exp(G)} \right\rceil \\ &= \lceil (k-2) + \frac{1}{\exp(G)} \rceil \\ &= k - 1 \end{aligned}$$

luego $N > k$.

Además $|B| \geq \left\lceil \frac{|B|-\eta(G)+1}{\exp(G)} \right\rceil \exp(G) - \exp(G) + \eta(G) = (N-1)\exp(G) + \eta(G)$ por la observación 2.2.1, $B$ posee al menos $N$ subsecuencias de suma cero de longitud menor o igual al $\exp(G)$, en consecuencia, existen $U_1, U_2, ..., U_N \in \mathcal{A}(G)$ tal que $U_1U_2...U_N \mid B$, así $\mathbf{L}(B) \geq N > k$, luego $\max \mathbf{L}(B) \geq k$ para todo $B \in \mathcal{B}(G)$ con $|B| > M$, por tanto $\mathsf{D}_k(G) = \max\{|B| : \max \mathbf{L}(B) < k\} \leq M$.■

Es conocido que, existe algún $\mathsf{D}_0(G)$ tal que para todo $k$ suficientemente grande, dependiendo de $G$,

$$\mathsf{D}_k(G) = k\exp(G) + \mathsf{D}_0(G).$$

**Observación 2.2.3** $\mathsf{D}_0(C_2^3) = 3$, *en efecto, dado que* $\exp(C_2^3) = 2$ *y por el Lema 2.1.2, se tiene que*

$$\begin{aligned} \mathsf{D}_0(C_2^3) &= D_k(C_2^3) - 2k \\ &= 2k + 3 - 2k \\ &= 3. \end{aligned}$$

**Observación 2.2.4** *Sea $G$ un grupo abeliano finito, $B \in \mathcal{B}(G)$, y $k \in \mathbb{N}$. Si $|B| > \mathsf{D}_k(G)$, entonces* $\max \mathbf{L}(B) > k$. *En particular, si* $\frac{|B|-\mathsf{D}'_0(G)}{\exp(G)} > k$, *entonces*

$\max \mathbf{L}(B) > k$; *y para 2 grupos elementales, podemos remplazar* $\mathsf{D}_0'(G)$ *por* $\mathsf{D}_0(G)$ *en esta desigualdad.*

En efecto, si $|B| > \mathsf{D}_k(G)$ y $\max \mathbf{L}(B) \leq k$ con $B \in \mathcal{B}(G)$ entonces

$$\begin{aligned} |B| &\leq \max\{|B'| : B' \in \mathcal{B}(G), \max \mathbf{L}(B') \leq k\} \\ &= \mathsf{D}_k(G) \end{aligned}$$

generando una contradiccción, así $\max \mathbf{L}(B) > k$.

$$\begin{aligned} \frac{|B| - \mathsf{D}_0'(G))}{\exp(G)} > k \Rightarrow |B| &> k\exp(G) + \mathsf{D}_0'(G) \\ &\geq k\exp(G) + \eta(G) - 2\exp(G) \\ &= (k-2)\exp(G) + \eta(G) \end{aligned}$$

luego, por la observación 2.2.1, $B$ tiene al menos $k-1$ subsecuencias de suma cero por tanto, $|B| > \mathsf{D}_k(G)$ y así $\max \mathbf{L}(B) > k$.

Si $\mathsf{D}_k(G) \leq k\exp(G) + \mathsf{D}_0(G)$ podemos reemplazar $\mathsf{D}_0'$ por $\mathsf{D}_0(G)$ en esta desigualdad.

$$\begin{aligned} \frac{|B| - \mathsf{D}_0'(G))}{\exp(G)} > k \Rightarrow |B| &> k\exp(G) + \mathsf{D}_0(G) \\ &\geq \mathsf{D}_k(G) \end{aligned}$$

así $\max \mathbf{L}(B) > k$.■

# Capítulo 3

# El Problema Inverso Asociado a la Constante de Davenport

En este Capítulo estudiamos la estructura de las secuencias minimales suma cero, es decir, la estructura de los elementos de $\mathcal{A}(G)$, como consecuencia resolvemos el problema inverso asociado a la constante de Davenport para los grupos cíclicos y para los grupos de la forma $C_2 \oplus C_2 \oplus C_{2n}$.

## 3.1. El Problema Inverso para Grupos Cíclicos y para el Grupo $C_2^3$

El siguiente resultado resuelve el problema inverso asociado a la constante de Davenport para grupos cíclicos finitos.

**Teorema 3.1.1** *Si $S \in \mathcal{A}(C_n)$ y $|S| = n$ entonces $S = a^n$, para algún $a \in C_n$.*

***Demostración.*** *Sea $S = a_1 a_2 ... a_n$, supongamos sin perdida de generalidad que $a_1 \neq a_2$. Sean*

$$\begin{aligned} S_1 &= a_1 \\ S_2 &= a_2 \\ S_3 &= a_1 + a_2 \\ S_4 &= a_1 + a_2 + a_3 \\ &\vdots \\ S_n &= a_1 + a_2 + ... + a_{n-1} \end{aligned}$$

*Si* $S_i = S_j$ *para* $3 \leq j \leq n$ *y* $i \in \{1, 2\}$ *entonces*

$$\sum_{i \neq k=1}^{j-1} a_k = 0,$$

*lo cual es una contradicción pues* $S$ *no posee subsecuencias de suma cero.*

*Si* $S_i = S_j$ *para* $3 \leq i < j \leq n$ *entonces*

$$\sum_{l=1}^{i-1} a_l = \sum_{k=1}^{j-1} a_k \Rightarrow \sum_{k=i}^{j-1} a_k = 0,$$

*lo cual es una contradicción pues* $S$ *no posee subsecuencias de suma cero. De modo que* $S_i \neq S_j$ *para todo* $i, j \in [1, n]$*, luego* $S_1, S_2, ..., S_n$ *son* $n$ *elementos distintos del grupo* $C_n$ *por tanto uno de ellos es el neutro, digamos* $S_i = 0$ *para algún* $i$*, lo cual es nuevamente una contradicción al hecho de que* $S$ *no posee subsecuencias de suma cero. Así* $S = a^n$*, para algún* $a \in C_n$*.* ■

**Proposición 3.1.1** *Sea* $G = C_2^2 \oplus C_2 = C_2 \oplus C_2 \oplus C_2$*,* $A \in \mathcal{F}(G)$ *es minimal de suma cero de longitud* $\mathsf{D}(G)$ *si sólo si existe* $\{e_1, e_2, e_3\} \subset G$ *independiente con*

$\text{ord}(e_1) = \text{ord}(e_2) = \text{ord}(e_3) = 2$, *tal que*

$$A = e_1e_2e_3(e_1 + e_2 + e_3)$$

**Demostración.**

($\Rightarrow$) Sea $A \in \mathcal{F}(C_2 \oplus C_2 \oplus C_2)$, $|A| = \mathsf{D}(G) = 4$ minimal, entonces existe $\{e_1, e_2, e_3\} \subset supp(A) \subset C_2^3$ independiente con $|e_1| = |e_2| = |e_3| = 2$, de lo contrario existiría una subsecuencia de longitud 3 y suma cero lo cual no es posible pues $A$ es minimal de suma cero. Luego, $A = e_1e_2e_3a_4$ y

$$\begin{aligned} & e_1 + e_2 + e_3 + a_4 = 0 \\ \Rightarrow \quad & a_4 = e_1 + e_2 + e_3 \end{aligned}$$

Así,

$$A = e_1e_2e_3(e_1 + e_2 + e_3).$$

($\Leftarrow$) Evidentemente la secuencia dadas suma cero y no posee subsecuencias de suma cero. ■

**Observación 3.1.1** *Sea* $S \in \mathcal{F}(C_2^3)$ *tal que* $\sigma(S) = 0$ *y* $|S| = 5$ *ó* $|S| = 6$ *entonces* $h(S) \geq 2$ *ó* $0 \mid S$.

Para ver esto supongamos que $0 \nmid S \in \mathcal{F}(C_2^3)$ tal que $\sigma(S) = 0$ y $|S| = 5$, es claro que $S$ no es minimal de suma cero, pues $\mathsf{D}(C_2^3) = 4$, de modo que existe $R \mid S$ minimal de suma cero con $2 \leq |R| < 5$.

Si $|R| = 2$ entonces $R = a_1a_2$ y

$$\begin{aligned} \sigma(R) = a_1 + a_2 = 0 \quad & \Rightarrow \quad a_1 = -a_2 = a_2 \\ & \Rightarrow \quad h(S) \geq h(R) = 2 \end{aligned}$$

Si $|R| = 3$ entonces $|R^{-1}S| = 2$, con $\sigma(R^{-1}S) = 0$, por el argumento anterior $h(S) \geq h(R^{-1}S) = 2$.

Si $|R| = 4$ entonces $|R^{-1}S| = 1$, con $\sigma(R^{-1}S) = 0$, luego $R^{-1}S = 0 \mid S$ en contradicción con el hecho de que $0 \nmid S$.

Supongamos que $0 \nmid S \in \mathcal{F}(C_2^3)$ tal que $\sigma(S) = 0$ y $|S| = 6$, es claro que $S$ no es minimal de suma cero, pues $\mathsf{D}(C_2^3) = 4$, de modo que existe $R \mid S$ minimal de suma cero con $2 \leq |R| < 6$.

Si $|R| = 2$ entonces $R = a_1a_2$ y

$$\begin{aligned} \sigma(R) = a_1 + a_2 = 0 \quad &\Rightarrow \quad a_1 = -a_2 = a_2 \\ &\Rightarrow \quad h(S) \geq h(R) = 2 \end{aligned}$$

Si $|R| = 4$ entonces $|R^{-1}S| = 2$, con $\sigma(R^{-1}S) = 0$, por el argumento anterior $h(S) \geq h(R^{-1}S) = 2$.

Si $|R| = 5$ entonces $|R^{-1}S| = 1$, con $\sigma(R^{-1}S) = 0$, luego $R^{-1}S = 0 \mid S$ en contradicción con el hecho de que $0 \nmid S$.

Si $|R| = 3$ entonces $|R^{-1}S| = 3$, con $\sigma(R^{-1}S) = 0$ además $h(R) = h(R^{-1}S) = 1$ ya que $0 \nmid S$ y $\sigma(R) = \sigma(R^{-1}S) = 0$, si $e_1+e_2+e_3 \mid R$ entonces $R = e_k(e_i+e_j)(e_1+e_2+e_3)$ con $i \neq j \neq k$ y $e_ie_j(e_i + e_k)(e_j + e_k)$ es minimal de suma cero, luego no es posible que $R^{-1}S$ tenga longitud 3 y sume cero, el mismo razonamiento es válido si suponemos que $e_1 + e_2 + e_3 \mid R^{-1}S$. Por tanto $e_1 + e_2 + e_3 \nmid S$, $R = e_ie_j(e_i + e_j)$ ó $R = (e_1 + e_2)(e_1 + e_3)(e_2 + e_3)$ en cuyo caso $R^{-1}S = e_k(e_i + e_k)(e_j + e_k)$ ó $R^{-1}S = e_1e_2e_3$ respectivamente, pero en ambos casos $\sigma(R^{-1}S) \neq 0$ lo que es una contradicción.

## 3.2. Estructura de las Secuencias Minimales de Suma Cero

Comenzamos presentando una propiedad del soporte de las secuencias minimales de suma cero de longitud $\mathsf{D}(G)$.

**Teorema 3.2.1** *Sea $G$ un grupo abeliano finito, $S \in \mathcal{A}(G)$ con $|S| = \mathsf{D}(G)$, entonces $\langle \mathrm{supp}(S) \rangle = G$.*

**Demostración.** Sea $G_1 = \langle \mathrm{supp}(S) \rangle$, supongamos que $G_1 \subsetneq G$ entonces $\mathsf{D}(G_1) < \mathsf{D}(G)$. Observemos que $S \in \mathcal{F}(G_1)$, sea $T = Sa^{-1} \mid S$ donde $a \mid S$ entonces $|T| = \mathsf{D}(G) - 1 \geq \mathsf{D}(G_1)$, luego $T$ posee una subsecuencia de suma cero, en consecuencia, $S$ posee una subsecuencia de suma cero, contradiciendo el hecho de que $S$ es minimal de suma cero. Luego $G_1 = G$. ■

Sea $G$ un grupo abeliano finito y sea $H$ subgrupo de $G$, denotamos por $\varphi$ al epimorfismo canónico de $G$ en $G/H$. Una técnica común al abordar el problema inverso, consiste en estudiar la secuencia inducida por $\varphi$ en $G/H$ y luego levantar esta estructura a la secuencia en $G$. Notemos que si $A \in \mathcal{A}(G)$, la secuencia $\varphi(A) \in \mathcal{F}(G/H)$ pertenece a $\mathcal{B}(G/H)$, pero no necesariamente pertenece a $\mathcal{A}(G/H)$, asi $\varphi(A)$ tiene una factorización en $\mathcal{F}(G/H)$, digamos $\varphi(A) = \varphi(F_1) \ldots \varphi(F_k)$, donde $A = F_1 F_2 \ldots F_k$. El siguiente resultado muestra como tiene que ser $\sigma(F_i)$ para cada $i \in [1, k]$ cuando $H$ es un subgrupo cíclico de $G$.

**Corolario 3.2.1** *Sea $G$ un grupo abeliano finito, $H \subset G$ subgrupo cíclico de $G$ de orden $n$, $A \in \mathcal{A}(G)$, $\varphi : G \mapsto G/H$ el epimorfismo canónico y $A = F_1 F_2 \ldots F_n$ tal*

*que* $\varphi(\sigma(F_i)) = 0$ *para cada* $i \in [1, n]$*, entonces existe* $g \in H$ *con* $H = \langle g \rangle$ *tal que para todo* $i \in [1, n]$*,* $\sigma(F_i) = g$*.*

**Demostración.** Sabemos que

$$\varphi(\sigma(F_i)) = 0 \Rightarrow \sigma(F_i) \in H \Rightarrow S = \prod_{i=1}^{n} \sigma(F_i) \in \mathcal{F}(H)$$

observemos que $S$ es minimal de suma cero, de lo contrario para algún $J \subsetneq [1, n]$, $\sum_{i \in J} \sigma(F_i) = 0$ entonces $\sigma(\prod_{i \in J} F_i) = 0$ pero $\prod_{i \in J} F_i \mid A$ en contradicción con el hecho de que $A \in \mathcal{A}(G)$, así $S \in \mathcal{A}(H)$, $|S| = n = D(H)$, luego por el teorema 3.1.1

$$S = \prod_{i=1}^{n} \sigma(F_i) = \prod_{i=1}^{n} g$$

y por el teorema 3.2.1, $\sigma(F_i) = g$, con $H = \langle g \rangle$. ■

El siguiente resultado muestra una cota para el número de secuencias cortas presentes en la factorización de $\varphi(A) \in G/H$.

**Lema 3.2.1** *Sea* $G$ *un grupo abeliano finito y* $H \subset G$ *un subgrupo. Sea* $A \in \mathcal{A}(G)$ *y* $A = F_1 \ldots F_k$ *tal que* $\varphi(F_1) \ldots \varphi(F_k)$ *es una factorización de* $\varphi(A)$*. Sean* $I_>, I_<$*, y* $I_=$ *denotando los subconjuntos de* $[1, k]$ *tal que para* $i$ *en el respectivo subconjunto tenemos que* $|F_i|$ *es el mayor que, menor que, e igual que, respectivamente, al exponente de* $G/H$*.*

*(i) Entonces* $\max \mathbf{L}(\prod_{i \in I_> \cup I_=} \varphi(F_i)) + |I_<| \leq \mathsf{D}(H)$*. En particular, tenemos que* $|I_<| \leq (\mathsf{D}(H) \exp(G/H) + \mathsf{D}'_0(G/H)) - |A|$*.*

*(ii) Si* $k = \max \mathbf{L}(\varphi(A))$*, entonces* $|\prod_{i \in I_>} \varphi(F_i)| \leq \mathsf{D}_{|I_>|}(G/H)$*; en particular, tenemos que* $|I_>| \leq \mathsf{D}'_0(G/H)$*.*

*En este lema, podemos remplazar* $\mathsf{D}'_0(G/H)$ *por* $\mathsf{D}_0(G/H)$ *para los 2-grupos elementales.*

**Demostración.** Recordemos que $\prod_{i=1}^{k}\sigma(F_i) \in \mathcal{A}(H)$ $(\sigma(\varphi(F_i)) = 0$ así $\sigma(F_i) \in H$ y encontrar una secuencia de $\prod_{i=1}^{k}\sigma(F_i)$ que sume cero es equivalente a encontrar una secuencia de $A$ que sume cero).

(i) Sea $l \in [0,k]$ tal que $I_< = [l+1,k]$ (posiblemente reordenando los $F_i$). Sea $B = \prod_{i=1}^{l} F_i$ y sea $B = F'_1...F'_{l'}$ tal que $\varphi(F'_1)...\varphi(F'_{l'})$ es una factorización de $\varphi(B)$ y $l' = \max \mathbf{L}(\varphi(B))$. Notemos que $\prod_{i=1}^{l'}\sigma(F'_i)\prod_{j=l+1}^{k}\sigma(F_i)$ es una secuencia minimal de suma cero sobre $H$. Así, existe una secuencia en $H$ de longitud $l' + (k-l) < D(H)$ libre de suma cero luego,

$$\begin{aligned} \max L(\prod_{i\in I_>\cup I_=}\varphi(F_i)) + |I_<| &= \max L(\varphi(B)) + |I_<| \\ &= l' + (k-l) \\ &\leq \mathsf{D}(H) \end{aligned}$$

Como $\max \mathbf{L}(\varphi(B)) \leq D(H) - |I_<|$, se sigue por la observación 2.2.4 que

$$\frac{|\varphi(B)| - \mathsf{D}'_0(G/H)}{\exp(G/H)} \leq \mathsf{D}(H) - |I_<|.$$

Notemos que

$$\begin{aligned} |\varphi(B)| = |B| &= |A| - |\prod_{i=l+1}^{k} F_i| \\ &= |A| - \sum_{i\in I_<}|F_i| \\ &\geq |A| - \sum_{i\in I_<}(\exp(G/H) - 1) \\ &= |A| - (\exp(G/H) - 1)|I_<| \end{aligned}$$

combinando las desigualdades anteriores tenemos

$$\begin{aligned}\frac{|A| - (\exp(G/H)-1)|I_<| - \mathsf{D}'_0(G/H)}{\exp(G/H)} &\leq \frac{|\varphi(B)| - \mathsf{D}'_0(G/H)}{\exp(G/H)} \\ &\leq \mathsf{D}(H) - |I_<|\end{aligned}$$

luego,

$$\begin{aligned}& |A| - (\exp(G/H)-1)|I_<| - \mathsf{D}'_0(G/H) \leq \mathsf{D}(H)\exp(G/H) - |I_<|\exp(G/H) \\ \Rightarrow\ & \exp(G/H)|I_<| - (\exp(G/H)-1)|I_<| \leq \mathsf{D}(H)\exp(G/H) + \mathsf{D}'_0(G/H) - |A| \\ \Rightarrow\ & |I_<| \leq \mathsf{D}(H)\exp(G/H) + \mathsf{D}'_0(G/H) - |A|.\end{aligned}$$

(ii) Si $k = \max \mathbf{L}(\varphi(A))$, entonces $\max \mathbf{L}(\prod_{i\in I_>} \varphi(F_i)) = |I_>|$. Sea $T = \prod_{i\in I_>} \varphi(F_i)$, como $|\varphi(F_i)| > |G/H| > 1$ para todo $i \in I_>$, y $\prod_{i\in I_>} \varphi(F_i)$ es una factorización de $T$, entonces $0 \nmid T$. Sea $\varphi(g)|T$ y consideremos la secuencia $T\varphi(g)^{-1}$, es claro que $\sigma(T\varphi(g)^{-1}) \neq 0$ y que $|T\varphi(g)^{-1}| = |I_>| - 1$. Supongamos que $T\varphi(g)^{-1}$ posee $|I_>|$ subsecuencias disjuntas de suma cero, digamos $T_1, T_2, \ldots, T_{|I_>|}$, entonces existe $R|T$, no trivial, tal que $T\varphi(g)^{-1} = T_1T_2\ldots T_{|I_>|}R$, implicando que $T = T_1T_2\ldots T_{|I_>|}R\varphi(g)$, como $\sigma(T) = 0$ y $\sigma(T_i) = 0$ para todo $i \in [1, |I_>|]$, se sigue que $\sigma(R\varphi(g)) = 0$, esto implica que $T$ tiene una factorización en al menos $|I_>|+1$ factores, contradiciendo que $\max \mathbf{L}(\prod_{i\in I_>} \varphi(F_i)) = |I_>|$, por tanto $T$ no posee $|I_>|$ subsecuencias disjuntas de suma cero, en consecuencia,

$$|\prod_{i\in I_>} \varphi(F_i)| = |T| \leq \mathsf{D}_{|I_>|}(G/H)$$

además,

$$\begin{aligned}\mathsf{D}_{|I_>|}(G/H) \geq |\prod_{i\in I_>}\varphi(F_i)| &= \sum_{i\in I_>}|\varphi(F_i)| \\ &= \sum_{i\in I_>}|F_i| \\ &\geq \sum_{i\in I_>}(\exp(G/H)+1) \\ &= (\exp(G/H)+1)|I_>|\end{aligned}$$

así $\mathsf{D}_{|I_>|}(G/H) - \exp(G/H)|I_>| \geq |I_>|$ y por la observación 2.2.2

$$\mathsf{D}'_0(G/H) \geq \mathsf{D}_{|I_>|}(G/H) - \exp(G/H)|I_>| \geq |I_>|.$$

■

**Lema 3.2.2** *Sean $r, n \in \mathbb{N}, G = C_2^{r-1} \oplus C_{2n}$, y sea $H \subset G$ un subgrupo cíclico de orden $n$ tal que $G/H \cong C_2^r$. Sea $T \in \mathcal{F}(G)$ tal que existe $e \in H$ con $2g = e$ para cada $g \mid T$. Si $F \mid T$ tal que $\sigma(F) \in H$, entonces,*

*(i) En caso de que $n$ sea par, $|F|$ es par y $\sigma(F) \in \{\frac{|F|}{2}e, \frac{|F|+n}{2}e\}$.*

*(ii) En caso de que $n$ sea impar, $\sigma(F) = \frac{|F|}{2}e$ si $|F|$ es par, y $\sigma(F) = \frac{|F|+n}{2}e$, si $|F|$ es impar.*

**Demostración.** Sea $F \mid T$ tal que $\sigma(F) \in H$. Consideremos

$$\begin{aligned}2\sigma(F) &= 2\sum_{g|F} g \\ &= \sum_{g|F} 2g \\ &= \sum_{g|F} e \\ &= |F|e\end{aligned}$$

Supongamos que $|H| = n$ es par, digamos $n = 2k$ para algún entero positivo $k$ entonces

$$\begin{aligned} 2\sigma(F) = |F|e &\Rightarrow k|F|e = 2k\sigma(F) \\ &\Rightarrow k|F|e = n\sigma(F) \\ &\Rightarrow k|F|e = 0 \quad (\sigma(F) \in H) \\ &\Rightarrow \text{ord}(e) \mid k|F| \\ &\Rightarrow k|F| = \text{ord}(e)l \\ &\Rightarrow k|F| = nl \\ &\Rightarrow k|F| = 2kl \\ &\Rightarrow |F| = 2l \end{aligned}$$

Por lo tanto $|F|$ es par.

$$\begin{aligned} 2\sigma(F) &= |F|e \\ &= 2le \end{aligned}$$

de donde

$$\begin{aligned} & 2(\sigma(F) - le) = 0 \\ \Rightarrow \quad & \text{ord}(\sigma(F) - le) \mid 2 \\ \Rightarrow \quad & \text{ord}(\sigma(F) - le) = 1 \vee \text{ord}(\sigma(F) - le) = 2 \end{aligned}$$

$$\begin{aligned} & \operatorname{ord}(\sigma(F) - le) = 1 \\ \Rightarrow \quad & \sigma(F) = le \\ \Rightarrow \quad & \sigma(F) = \frac{|F|}{2}e \end{aligned}$$

Como $\sigma(F) \in H$ entonces $\sigma(F) = re$ para algún $r \in [0, n-1]$ de modo que,

$$\begin{aligned} \sigma(F) - le &= re - le \\ &= (r-l)e, \quad r - l < n \end{aligned}$$

por tanto,

$$\begin{aligned} \operatorname{ord}(\sigma(F) - le) = 2 \quad &\Rightarrow \quad 2(r-l)e = 0 \\ &\Rightarrow \quad \operatorname{ord}(e) = n \mid 2(r-l) \\ &\Rightarrow \quad 2(r-l) = ns < 2n \\ &\Rightarrow \quad 2(r-l) = n \\ &\Rightarrow \quad r - l = \frac{n}{2} \\ &\Rightarrow \quad r = \frac{n}{2} + l \\ &\Rightarrow \quad r = \frac{n}{2} + \frac{|F|}{2} \\ &\Rightarrow \quad r = \frac{n + |F|}{2} \end{aligned}$$

Supongamos que $|H| = n$ es impar, digamos $n = 2k + 1$ para algún entero positivo $k$.

Si $|F| = 2l$ entonces

$$2\sigma(F) = |F|e = (2l)e$$

luego,

$$\begin{aligned} 2(\sigma(F) - le) = 0 &\Rightarrow \operatorname{ord}(\sigma(F) - le) \mid 2 \\ &\Rightarrow \operatorname{ord}(\sigma(F) - le) = 1 \vee \operatorname{ord}(\sigma(F) - le) = 2 \end{aligned}$$

si $\operatorname{ord}(\sigma(F) - le) = 2$ entonces

$$\begin{aligned} 2(\sigma(F) - le) = 0 &\Rightarrow 2(re - le) = 0 \\ &\Rightarrow 2(r - l)e = 0 \\ &\Rightarrow 2(r - l) \mid \operatorname{ord}(e) = n \\ &\Rightarrow 2 \mid n \end{aligned}$$

lo cual es una contradicción, luego $\operatorname{ord}(\sigma(F) - le) = 1 \Rightarrow \sigma(F) = le = \frac{|F|}{2}e$.

Si $|F| = 2l + 1$ entonces

$$\begin{aligned} 2\sigma(F) = |F|e = 2\frac{|F|+n}{2}e &\Rightarrow 2(\sigma(F) - \frac{|F|+n}{2}e) = 0 \\ &\Rightarrow \operatorname{ord}(\sigma(F) - \frac{|F|+n}{2}e) \mid 2 \\ &\Rightarrow \operatorname{ord}(\sigma(F) - \frac{|F|+n}{2}e) = 2 \vee \operatorname{ord}(\sigma(F) - \frac{|F|+n}{2}e) = 1 \end{aligned}$$

si $\operatorname{ord}(\sigma(F) - \frac{|F|+n}{2}e) = 2$ entonces

$$\begin{aligned} 2(\sigma(F) - \frac{|F|+n}{2}e) = 0 &\Rightarrow 2(re - \frac{|F|+n}{2}e) = 0 \\ &\Rightarrow 2(r - \frac{|F|+n}{2})e = 0 \\ &\Rightarrow 2(r - \frac{|F|+n}{2}) \mid \operatorname{ord}(e) = n \\ &\Rightarrow 2 \mid n \end{aligned}$$

lo cual es una contradicción, luego $\operatorname{ord}(\sigma(F) - \frac{|F|+n}{2}e) = 1$ y por tanto $\sigma(F) = \frac{|F|+n}{2}e$.

■

## 3.3. El Problema Inverso para el Grupo $C_2 \oplus C_2 \oplus C_{2n}$

**Lema 3.3.1** *Sea $n \in \mathbb{N}$, $G = C_2^2 \oplus C_{2n}$, $H \subset G$ subgrupo isomorfo a $C_n$ tal que $G/H \cong C_2^3$ y $A \in \mathcal{F}(G)$ minimal de suma cero de longitud $2n+2$ con una descomposición $A = F_1...F_{n-1}R$ tal que para cada $i \in [1, n-1]$ $|F_i| = 2$, $|R| = 4$, $F = F_1...F_{n-1}$, $\varphi : G \mapsto G/H$ la función canónica, para cada $i$ $\sigma(\varphi(F_i)) = 0$, $\sigma(\varphi(R)) = 0$ y $\varphi(R) \in \mathcal{F}(G/H)$ libre de cuadrados es minimal de suma cero y $\langle supp(\varphi(R))\rangle = G/H$ entonces:*

*(i) Si $\varphi(h) = \varphi(h')$ para $hh' \mid A$ entonces $h = h'$.*

*(ii) Los elementos en $supp(R)$ ocurren con multiplicidad uno en $A$ y la multiplicidad de los demás elementos es dos. Así la descomposición $A = FR$ es única. Más aún, la descomposición $F = F_1...F_{n-1}$ también es única (salvo el orden).*

*(iii) Para cada $h \in supp(F)$ tenemos que $ord(2h) = n$ y, como $\varphi(h) \neq 0$, el orden de $h$ es par. Así $ord(h) = 2n$. Más aún, existe un elemento generador $g \in H$ tal que, para cada $i \in [1, n-1]$, $\sigma(F_i) = g$ y $\sigma(R) = g$.*

*(iv) Si $\varphi(h_0) = \varphi(h_1) + \varphi(h_2)$ con $h_0 \mid F$ y $h_1h_2 \mid R$, entonces $h_0 = h_1 + h_2$.*

*(v) $supp(\varphi(F))$ es libre de suma, es decir, la ecuación $x + y = z$ no tiene solución en $supp(\varphi(F))$.*

*(vi) Para cada $h \in supp(F) \cap supp(R)$ tenemos $h = \sigma(h^{-1}R)$ y más aún para cada $R' \mid R$ con $|R'| = 3$ y $h \mid R'$ tenemos que $\langle supp(A)\rangle \subset \langle supp(R')\rangle$.*

**Demostración.** Cuando convenga, asumiremos $F_n = R$

(i) Primero supongamos que $h$ y $h'$ ocurren en subsecuencias distintas, es decir, $h \mid F_i$ y $h' \mid F_j$ para $i \neq j$. Consideremos $F_i' = h^{-1}h'F_i$ y $F_j' = (h')^{-1}hF_j$ entonces $\sigma(F_i') = g - h + h'$ y $\sigma(F_j') = g - h' + h$, observemos que $F_iF_j = F_i'F_j'$, así

$$A = \prod_{k=1}^{n} F_k = \prod_{k \neq i,j} F_k F_i' F_j'$$

Como $\varphi(h) = \varphi(h')$ entonces

$$\sigma(\varphi(F_i')) = \sigma(\varphi(F_i)) = 0 \text{ y } \sigma(\varphi(F_j')) = \sigma(\varphi(F_j)) = 0$$

luego por el Corolario 3.2.1 $g - h + h' = \sigma(F_i') = \sigma(F_j') = g$, así $h' = h$.

Ahora, supongamos $hh' \mid F_i$ para algún $i$. Si $i = n$ entonces $\varphi(h)\varphi(h') = [\varphi(h)]^2 \mid \varphi(F_n)$, contradiciendo el hecho de que $\varphi(F_n)$ es libre de cuadrados. Así $i \neq n$, sin perder generalidad, supongamos que $i = n - 1$, es decir, $F_{n-1} = hh'$. $-\varphi(h) \in G/H = \langle supp(\varphi(F_n)) \rangle$, así $-\varphi(h) = \sigma(\varphi(U))$ con $U \mid F_n$, pues $exp(G/H) = 2$.

Sea $U' = U^{-1}F_n$ entonces $\sigma(\varphi(U')) = \sigma(\varphi(U))$; consideremos $F_{n-1}' = hU$ y

$F'_n = h'U'$ entonces

$$\begin{aligned}
\varphi(\sigma(F'_n)) &= \varphi(\sigma(h'U')) \\
&= \varphi(h' + \sigma(U')) \\
&= \varphi(h') + \varphi(\sigma(U')) \\
&= \varphi(h) + \varphi(\sigma(U)) \\
&= \varphi(h) - \varphi(h) \\
&= 0
\end{aligned}$$

Análogamente,

$$\varphi(\sigma(F'_{n-1})) = 0.$$

Además observemos que $F'_{n-1}F'_n = F_{n-1}F_n$, por tanto $A = F_1...F'_{n-1}F'_n$ de modo que por el Corolario 3.2.1 existe $g \in H$ con $H = \langle g \rangle$ tal que

$$\sigma(F'_{n-1}) = \sigma(F'_n) = g$$

Consideremos $F''_{n-1} = h'U$ y $F''_n = hU'$. Usando el mismo argumento $\sigma(F''_{n-1}) = \sigma(F''_n) = g$. Así,

$$\begin{aligned}
& \sigma(F'_n) = \sigma(F''_n) \\
\Rightarrow \quad & \sigma(h'U') = \sigma(hU') \\
\Rightarrow \quad & \sigma(h') + \sigma(U') = \sigma(h) + \sigma(U') \\
\Rightarrow \quad & \sigma(h') = \sigma(h) \\
\Rightarrow \quad & h' = h
\end{aligned}$$

(ii) Dado que $|F_i| = 2\ \forall i \in [1, n-1]$, supongamos $F_i = a_{i1}a_{i2} \in \mathcal{F}(C_2 \oplus C_2 \oplus C_{2n})$ entonces

$$\begin{aligned} 0 &= \sigma(\varphi(F_i)) \\ &= \varphi(a_{i1}) + \varphi(a_{i2}) \end{aligned}$$

$\Rightarrow \varphi(a_{i1}) = -\varphi(a_{i2}) = \varphi(a_{i2})$, por (i) $a_{i1} = a_{i2}$, luego $F_i = a_i^2$ para algún $a_i \in G$.

Como $\varphi(R)$ es minimal de suma cero y de longitud cuatro, por la proposición 3.1.1 $\varphi(R) = e_1e_2e_3(e_1 + e_2 + e_3)$ para $\{e_1, e_2, e_3\}$ base de $C_2^3$ de modo que $v_x(\varphi(R)) = 1, \forall x \mid \varphi(R)$ en consecuencia $R = g_1g_2g_3g_{123}$ donde $\varphi(g_i) = e_i$, $\varphi(g_{123}) = \sum_{i=1}^{3} e_i$ y por (i) $v_x(R) = 1$, $\forall x \mid R$, luego

$$A = \prod_{i=1}^{n-1} a_i^2 g_1g_2g_3g_{123}.$$

(iii) Sea $h \in supp(F)$ entonces por (ii) existe $i \in [1, n-1]$ tal que $F_i = h^2$ pero por el corolario 3.2.1 $\sigma(F_i) = g$ con $H = \langle g \rangle$, luego $2h = g \Rightarrow ord(2h) = ord(g) = n$. Supongamos que $ord(h) = 2k + 1$ entonces

$$\begin{aligned} & (2k+1)h = 0 \\ \Rightarrow\ & 2kh + h = 0 \\ \Rightarrow\ & 2kh = -h \\ \Rightarrow\ & k(2h) = -h \\ \Rightarrow\ & -h \in \langle 2h \rangle \\ \Rightarrow\ & h \in \langle g \rangle = H \\ \Rightarrow\ & \varphi(h) = 0 \quad \text{contradicción,} \quad \text{pues} \quad \varphi(h) \neq 0 \end{aligned}$$

luego, $ord(h)$ es par, además $(2n)h = n(2h) = 0 \Rightarrow \text{ord}(h) \leq 2n$.

Supongamos que $\text{ord}(h) = 2m$ entonces

$$\begin{aligned} & (2m)h = 0 \\ \Rightarrow \quad & m(2h) = 0 \\ \Rightarrow \quad & n \mid m \\ \Rightarrow \quad & n \leq m \\ \Rightarrow \quad & 2n \leq 2m = \text{ord}(h). \end{aligned}$$

Por tanto $\text{ord}(h) = 2n$.

(iv) Supongamos que $\varphi(h_0) = \varphi(h_1) + \varphi(h_2)$ con $h_0 \mid F$ y $h_1h_2 \mid R$, sin perder generalidad supongamos que $h_0 \mid F_{n-1}$, es decir, $h_0^2 = F_{n-1}$. Sea $R = h_1h_2h_3h_4$. Notemos que,

$$\begin{aligned} & \varphi(\sigma(R)) = \sigma(\varphi(R)) = 0 \\ \Rightarrow \quad & \varphi(\sigma(h_1h_2h_3h_4)) = 0 \\ \Rightarrow \quad & \varphi(h_1 + h_2 + h_3 + h_4) = 0 \\ \Rightarrow \quad & \varphi(h_1) + \varphi(h_2) + \varphi(h_3) + \varphi(h_4) = 0 \\ \Rightarrow \quad & \varphi(h_1) + \varphi(h_2) = \varphi(h_3) + \varphi(h_4) \qquad (\varphi(h_i) \in C_2^3) \end{aligned}$$

Sea $F'_{n-1} = h_0h_1h_2$ y $F'_n = h_0h_3h_4$, notemos que $\varphi(\sigma(F_i)) = 0$ para $i \in [1, n-2]$

y además

$$\begin{aligned}\varphi(\sigma(F'_{n-1})) &= \varphi(h_0+h_1+h_2)\\ &= \varphi(h_0)+\varphi(h_1)+\varphi(h_2)\\ &= \varphi(h_1)+\varphi(h_2)+\varphi(h_1)+\varphi(h_2)\\ &= 0.\end{aligned}$$

$$\begin{aligned}\varphi(\sigma(F'_{n})) &= \varphi(h_0+h_3+h_4)\\ &= \varphi(h_0)+\varphi(h_3)+\varphi(h_4)\\ &= \varphi(h_1)+\varphi(h_2)+\varphi(h_3)+\varphi(h_4)\\ &= 0.\end{aligned}$$

Entonces por el Corolario 3.2.1 existe $g \in H$ con $H = \langle g \rangle$ tal que $\sigma(F_1)...\sigma(F_{n-2})\sigma(F'_{n-1})\sigma(F'_n) = g^n$. En particular,

$$\begin{aligned}&\sigma(F'_n) = g = \sigma(R)\\ \Rightarrow\ & h_0+h_3+h_4 = h_1+h_2+h_3+h_4\\ \Rightarrow\ & h_0 = h_1+h_2.\end{aligned}$$

(v) Procedamos por reducción al absurdo, supongamos que existen $f_1, f_2, f_3 \in supp(F)$ tales que $\varphi(f_1)+\varphi(f_2) = \varphi(f_3)$.

Si $f_1 = f_2$ entonces $2\varphi(f_1) = \varphi(f_3) \Rightarrow 0 = \varphi(f_3)$ contradicción, pues $0 \nmid \varphi(A)$.

Si $f_1 = f_3$ entonces $\varphi(f_1)+\varphi(f_3) = \varphi(f_2) \Rightarrow \varphi(f_2) = 2\varphi(f_1) = 0$ contradicción.

Si $f_2 = f_3$, por un procedimiento análogo, tenemos $\varphi(f_1) = 0$ contradicción.

Así, $f_1, f_2, f_3$ son distintos dos a dos, como F tiene longitud par entonces

$|F| \geq 4$, más aún $n-1 \geq 2$ implicando que $n \geq 3$.

Ahora,

$$\begin{aligned} & \varphi(f_1)+\varphi(f_2)=\varphi(f_3) \\ \Rightarrow \quad & \varphi(f_1)+\varphi(f_2)+\varphi(f_3)=0 \\ \Rightarrow \quad & f_1+f_2+f_3 \in H=\langle g \rangle \\ \Rightarrow \quad & f_1+f_2+f_3=kg \quad \text{con} \quad 0 \leq k \leq n-1 \\ \Rightarrow \quad & 2f_1+2f_2+2f_3=2kg \end{aligned}$$

Por otro lado sabemos que $2f_1+2f_2+2f_3=3g$ así $2kg=3g \Rightarrow (2k-3)g=0$ luego $2k-3=qn$, $q \in \mathbb{Z}$.

Si $k=0$ ó $k=3$, $3g=0$ así $\text{ord}(g)=n=3$ y $|F|=2n-2=4$ y $supp(F)=f_1f_2f_3f_4$, por tanto $0=\varphi(\sigma(F))=\varphi(f_1)+\varphi(f_2)+\varphi(f_3)+\varphi(f_4)=\varphi(f_4)$ luego $0 \mid \varphi(A)$ contradicción.

Si $k=1$ ó $k=2$, $g=0$ contradicción.

Luego $k \geq 4 \Rightarrow 2k-3 \geq 5$, en consecuencia $q>0$ además $k \leq n-1 \Rightarrow 2k-3 \leq 2n-5$, así $qn \leq 2n-5 \Rightarrow q<2$ luego $q=1$ por tanto $2k-3=n \Rightarrow k=\frac{n+3}{2}$, de modo que $f_1+f_2+f_3=(\frac{n+3}{2})g$. Sea $T=f_1f_2f_3$ por el Lema 3.2.2, y dado que n es impar, entonces $\sigma(T)=\frac{|T|+n}{2}g=\frac{3+n}{2}g$. Supongamos, sin perder generalidad, que $T \mid F_1F_2F_3$ y sea

$$T_0=F_4F_5...F_k \mid T^{-1}F$$

como $\sigma(F_i)=g$ entonces $\sigma(T_0)=(k-3)g=(\frac{n-3}{2})g$, luego $\sigma(T_0T)=ng=0$ contradicción, pués $F$ no posee subsecuencias de suma cero.

(vi) Sea $h \in supp(F) \cap supp(R)$, supongamos que $R = hh_1h_2h_3$ entonces $h^{-1}R = h_1h_2h_3$ y $\sigma(h^{-1}R) = h_1 + h_2 + h_3$. Como $h \in supp(F)$ entonces $h^2 \mid F$ y así $2h = g = \sigma(R) = h+h_1+h_2+h_3$ implicando que $h = h_1+h_2+h_3 = \sigma(h^{-1}R)$. Ahora sea $h \mid R' \mid R$ donde $|R'| = 3$, entonces podemos escribir $R'$ como $R' = hh_ih_j$ con $i, j \in \{1, 2, 3\}$, $i \neq j$ y $R = hh_ih_jh_k$ con $k \in \{1, 2, 3\} \setminus \{i, j\}$, luego $R = R'h_k \Rightarrow h_k = \sigma(R) - \sigma(R') = 2h - \sigma(R') \in \langle supp(R')\rangle$, por tanto

$$supp(R) \subset \langle supp(R')\rangle. \tag{3.1}$$

Por otro lado $\varphi(R)$ es minimal de suma cero de longitud 4 en $G/H \cong C_2^3$, así por la Proposición 3.1.1 $supp(\varphi(R)) = \{e_1, e_2, e_3, e_1+e_2+e_3\}$ con $\{e_1, e_2, e_3\}$ base de $G/H$, de modo que

$$G/H \setminus supp(\varphi(R)) = \{e_1 + e_2, e_1 + e_3, e_2 + e_3, 0\}.$$

Nótese entonces que todo elemento no nulo de $G/H$ fuera del soporte de $\varphi(R)$ es suma de dos elementos distintos de $supp(\varphi(R))$.

Sea $f \in supp(F)$,

si $f \in supp(R)$ entonces $f \in \langle supp(R')\rangle$,

si $f \notin supp(R)$ entonces $\varphi(f) \notin \langle supp(\varphi(R))\rangle$ ($\varphi/supp(A)$ es inyectiva por(i)),

luego $\varphi(f) = \varphi(f_1) + \varphi(f_2)$, $f_1, f_2 \mid R$ por (iv)

$$\begin{aligned} f &= f_1 + f_2 \\ &\in supp(R) + supp(R) \\ &\subset \langle supp(R')\rangle \end{aligned}$$

por tanto

$$supp(F) \subset \langle supp(R')\rangle \tag{3.2}$$

de 3.1 y 3.2

$$\begin{aligned} & supp(A) \subset \langle supp(R') \rangle \\ \Rightarrow \quad & \langle supp(A) \rangle \subset \langle supp(R') \rangle. \end{aligned}$$

■

**Teorema 3.3.1** *Sea $n \in \mathbb{N}$ y $G = C_2^2 \oplus C_{2n}$. Entonces $A \in \mathcal{F}(G)$es una secuencia minimal de suma cero de longitud $\mathsf{D}(G)$ si y sólo si existe una base $\{e_1, e_2, e_3\}$ de $G$, donde $\mathrm{ord}(e_1) = \mathrm{ord}(e_2) = 2$ y $\mathrm{ord}(e_3) = 2n$, tal que $A$ es igual a una de las siguientes secuencias:*

*(1)* $e_3^{v_3}(e_3 + e_2)^{v_2}(e_3 + e_1)^{v_1}(-e_3 + e_2 + e_1)$ *con* $v_i \in \mathbb{N}$ *impar,* $v_3 \geq v_2 \geq v_1$ *y* $v_3 + v_2 + v_1 = 2n + 1$.

*(2)* $e_3^{v_3}(e_3 + e_2)^{v_2}(ae_3 + e_1)(-ae_3 + e_2 + e_1)$ *con* $v_2, v_3 \in \mathbb{N}$ *impar,* $v_3 \geq v_2$ *y* $v_2 + v_3 = 2n$ *y* $a \in [2, n-1]$.

*(3)* $e_3^{2n-1}(ae_3 + e_2)(be_3 + e_1)(ce_3 + e_2 + e_1)$ *con* $a + b + c = 2n + 1$ *donde* $a \leq b \leq c$ *y* $a, b \in [2, n-1]$, $c \in [2, 2n-3] \setminus \{n, n+1\}$.

*(4)* $e_3^{2n-1-2v}(e_3+e_2)^{2v}e_2(ae_3+e_1)((1-a)e_3+e_2+e_1)$ *con* $v \in [0, n-1]$, *y* $a \in [2, n-1]$.

*(5)* $e_3^{2n-2}(ae_3 + e_2)((1-a)e_3 + e_2)(be_3 + e_1)((1-b)e_3 + e_1)$ *con* $a, b \in [2, n-1]$, *y* $a \geq b$.

*(6)* $\prod_{i=1}^{2n}(e_3 + d_i)e_2e_1$ *donde* $S = \prod_{i=1}^{2n} d_i \in \mathcal{F}(\langle e_1, e_2 \rangle)$ *con* $\sigma(S) = e_1 + e_2$.

**Demostración.**

$\Longleftarrow$) El caso $n = 1$ sale por 3.1.1.

Supongamos $n \geq 2$. Es claro que todas las secuencias listadas tienen longitud $2n+2$ y suman cero. Veamos que son minimales de suma cero.

Sea $A = e_3^{v_3}(e_3 + e_2)^{v_2}(e_3 + e_1)^{v_1}(-e_3 + e_2 + e_1)$ con $v_i \in \mathbb{N}$ impar, $v_3 \geq v_2 \geq v_1$ y $v_3 + v_2 + v_1 = 2n + 1$ (como en (1)).

Sea $1 \neq U|A$ una subsecuencia de suma cero.

Supongamos que $(-e_3 + e_2 + e_1) \nmid U$, $U = e_3^{m_3}(e_3 + e_2)^{m_2}(e_3 + e_1)^{m_1}$

$$\begin{aligned}
\sigma(U) = 0 \quad &\Rightarrow \quad m_3e_3 + m_2(e_3 + e_2) + m_1(e_3 + e_1) = 0 \\
&\Rightarrow \quad (m_3 + m_2 + m_1)e_3 = 0 \ \ \wedge \ \ m_2e_2 = 0 \ \ \wedge \ \ m_1e_1 = 0 \\
&\Rightarrow \quad 2n|(m_3 + m_2 + m_1) \ \ \wedge \ \ 2|m_2 \ \ \wedge \ \ 2|m_1 \\
&\Rightarrow \quad |U| \geq 2n \ \ \wedge \ \ m_1, m_2, m_3 \ \text{son pares}
\end{aligned}$$

así $m_i < v_i$ para cada $i$ ($v_i$ es impar) luego,

$2n \leq |U| = m_3 + m_2 + m_1 \leq (v_3 - 1) + (v_2 - 1) + (v_1 - 1) = 2n - 2$ contradicción.

Supongamos que $(-e_3 + e_2 + e_1) \mid U, U = e_3^{m_3}(e_3 + e_2)^{m_2}(e_3 + e_1)^{m_1}(-e_3 + e_2 + e_1)$

$$\begin{aligned}
\sigma(U) = 0 \quad &\Rightarrow \quad m_3e_3 + m_2(e_3 + e_2) + m_1(e_3 + e_1) + (-e_3 + e_2 + e_1) = 0 \\
&\Rightarrow \quad (m_3 + m_2 + m_1 - 1)e_3 = 0 \\
&\Rightarrow \quad 2n|(m_3 + m_2 + m_1 - 1) \\
&\Rightarrow \quad m_3 + m_2 + m_1 - 1 = 2nk \ \text{para algún entero positivo k} \\
&\Rightarrow \quad m_3 + m_2 + m_1 + 1 = 2nk + 2
\end{aligned}$$

así $|A| = 2n + 2 \leq 2nk + 2 = |U| \leq |A|$ luego, $A = U$.

Sea $A = e_3^{v_3}(e_3 + e_2)^{v_2}(ae_3 + e_1)(-ae_3 + e_2 + e_1)$ con $v_2, v_3 \in \mathbb{N}$ impar $v_3 \geq v_2$; $v_2 + v_3 = 2n$ y $a \in [2, n-1]$ (como en (2)).

Sea $U|A$ tal que $\sigma(U) = 0$.

Supongamos que $(ae_3 + e_1)(-ae_3 + e_2 + e_1) \nmid U$ entonces

$U = e_3^{m_3}(e_3 + e_2)^{m_2}$ con $m_3 \leq v_3$ y $m_2 \leq v_2$

$$\begin{aligned}
\sigma(U) = 0 &\Rightarrow m_3e_3 + m_2(e_3 + e_2) = 0 \\
&\Rightarrow (m_3 + m_2)e_3 = 0 \ \wedge \ m_2e_2 = 0 \\
&\Rightarrow 2n|(m_3 + m_2), \ 2|m_2, \ 2|m_3 \\
&\Rightarrow 2n|(m_3 + m_2) \ \wedge \ m_2 < v_2 \ \wedge \ m_3 < v_3 \\
&\Rightarrow m_2 + m_3 \geq 2n \ \wedge \ m_2 + m_3 \leq (v_2 - 1) + (v_3 - 1) = 2n - 2 \\
&\Rightarrow |U| \geq 2n \ \wedge \ |U| \leq 2n - 2 \ \text{ contradicción.}
\end{aligned}$$

Supongamos que $(ae_3 + e_1)(-ae_3 + e_2 + e_1)|U$ entonces

$U = e_3^{m_3}(e_3 + e_2)^{m_2}(ae_3 + e_1)(-ae_3 + e_2 + e_1)$ con $m_3 \leq v_3$ y $m_2 \leq v_2$

$$\begin{aligned}
\sigma(U) = 0 &\Rightarrow m_3e_3 + m_2(e_3 + e_2) + ae_3 + e_1 - ae_3 + e_2 + e_1 = 0 \\
&\Rightarrow (m_3 + m_2)e_3 + (m_2 + 1)e_2 = 0 \\
&\Rightarrow 2n|m_3 + m_2 \\
&\Rightarrow m_3 + m_2 \geq 2n
\end{aligned}$$

luego, $2n \leq m_3 + m_2 \leq v_3 + v_2 = 2n$

por tanto, $m_3 + m_2 = 2n$

así, $|U| = m_3 + m_2 + 2 = 2n + 2 = |A|$ en consecuencia $A = U$.

Sea $A = \prod_{i=1}^{2n}(e_3 + d_i)e_2e_1$ donde $S = \prod_{i=1}^{2n} d_i \in \mathcal{F}(\langle e_1, e_2\rangle)$ y $\sigma(S) = e_1 + e_2$ (como en (6)).

Sea $U|A$ con $\sigma(U) = 0$.

Supongamos que $e_2e_1 \nmid U$,

si $e_2 \nmid U,\ e_1 \nmid U$, podemos suponer sin perdida de generalidad que

$$U = \prod_{i=1}^{m}(e_3 + d_i) \quad con \quad m \leq 2n$$

$$\begin{aligned} \sigma(U) = 0 \ &\Rightarrow \ me_3 + \sum_{i=1}^{m} d_i = 0 \\ &\Rightarrow \ me_3 + \alpha_1e_1 + \alpha_2e_2 = 0 \\ &\Rightarrow \ 2n|m \\ &\Rightarrow \ m \geq 2n \end{aligned}$$

Así,

$$U = \prod_{i=1}^{2n}(e_3 + d_i) \quad pero$$

$$\begin{aligned} \sigma(U) = 0 \ &\Rightarrow \ 2ne_3 + \sum_{i=1}^{2n} d_i = 0 \\ &\Rightarrow \ e_1 + e_2 = 0 \ \text{ contradicción.} \end{aligned}$$

Si $e_j|U, \quad j \in \{1, 2\}$

$$U = \prod_{i=1}^{m}(e_3 + d_i)e_j \ \ m \leq 2n$$

$$\begin{aligned}\sigma(U)=0 &\Rightarrow me_3+\sum_{i=1}^{m}d_i+e_j=0\\ &\Rightarrow me_3+\alpha_1e_1+\alpha_2e_2+e_j=0\\ &\Rightarrow 2n|m\\ &\Rightarrow m\geq 2n\end{aligned}$$

Así,

$$U=\prod_{i=1}^{2n}(e_3+d_i)e_j$$

luego,

$$\begin{aligned}\sigma(U)=0 &\Rightarrow \sum_{i=1}^{2n}d_i+e_j=0\\ &\Rightarrow e_1+e_2+e_j=0 \quad \text{contradicción.}\end{aligned}$$

Si $e_1e_2|U$,

$$U=\prod_{i=1}^{m}(e_3+d_i)e_1e_2, \quad m\leq 2n$$

$$\begin{aligned}(U)=0 &\Rightarrow me_3+\sum_{i=1}^{m}d_i+e_1+e_2=0\\ &\Rightarrow me_3+\alpha_1e_1+\alpha_2e_2+e_1+e_2=0\\ &\Rightarrow 2n|m\\ &\Rightarrow m\geq 2n\end{aligned}$$

luego,

$$U=\prod_{i=1}^{2n}(e_3+d_i)e_1e_2=A.$$

Análogamente se prueba que las secuencias (3)-(5) son minimales.

$\Longrightarrow$) Sea $H$ un subgrupo de $G$ isomorfo a $C_n$ tal que $G/H \cong C_2^2 \oplus C_{2n}/C_n \cong C_2^3$ y sea $\varphi : G \to G/H$ la función canónica. Sea $A \in \mathcal{A}(G)$ con $|A| = D(G)$. Por la Observación 2.1.1 tenemos $|A| \geq 2n+2$. Recíprocamente por la Observación 2.1.2 y el Lema 2.1.2, tenemos $|A| \leq 2n+3$.

Comenzemos por investigar la estructura de $B = \varphi(A)$.

Sea $B_i = \varphi(A_i)$, $A_i|A$ , $B = B_1...B_r$ y supongamos $r \geq n+1$

$\sigma(B_i) = 0 \Leftrightarrow A_i \in \mathcal{F}(C_n)$, luego obviamente la secuencia

$$A = A_1...A_r = A_1...A_nA_{n+1}...A_r$$

posee una subsecuencia que suma cero, en franca contradicción con el hecho de que $A$ es minimal de suma cero, por tanto $\max \mathbf{L}(B) \leq n$, por otro lado y debido a las Observaciones 2.2.4 y 2.2.3

$$\begin{aligned} 2n+2 \leq D(G) \leq 2n+3 &\Rightarrow D(G) > 2n+1 \\ &\Rightarrow \frac{D(G)-3}{2} > n-1 \\ &\Rightarrow \max \mathbf{L}(B) > n-1 \\ &\Rightarrow \max \mathbf{L}(B) \geq n \end{aligned}$$

Luego, $\max \mathbf{L}(B) = n$

Sea $B = S_1...S_kT_1...T_l$ una factorización, donde $S_i$ denota una secuencia corta de suma cero minimal para cada $i \in \{1, ...k\}$ y la, posiblemente vacía, secuencia de suma cero $T = T_1...T_l$ no divisible por una secuencia corta de suma cero. $T$ es libre de cuadrado y $0 \nmid T$, pues para $i \neq j$, $T_i \cap T_j = \emptyset$ y $T \subset C_2^3$ con $|C_2^3| = 8$. Notar

que como $|T| \leq 7$, obtenemos $k + l = n$. Por otra parte, sea $A = F_1...F_kR_1...R_l$ tal que $\varphi(F_i) = S_i$ y $\varphi(R_j) = T_j$; además sea $F = F_1...F_k$ y $R = R_1...R_l$. Ya que

$$\begin{aligned} |B| - |T| &= \sum_{i=1}^{k} |S_i| + \sum_{i=1}^{l} |T_i| - \sum_{i=1}^{l} |T_i| \\ &= \sum_{i=1}^{k} |S_i| \\ &\leq \exp(C_2^3)k \\ &= 2k \end{aligned}$$

Entonces, $n \geq k \geq (|B| - |T|)/2$, de donde, $|T| \neq 0$, de lo contrario $n \geq k \geq |B|/2 \geq (2n + 2)/2 = n + 1$, lo cual es imposible, por lo tanto $n - 1 \geq k \geq (|B| - |T|)/2$, pues $n = k + l$. Esto implica que

$$\begin{aligned} 2n - 2 \geq |B| - |T| \Rightarrow |T| &\geq |B| - 2n + 2 \\ &\geq 2n + 2 - 2n + 2 \\ &= 4 \end{aligned}$$

Así, $4 \leq |T| \leq 7$ por la Observación 3.1.1 tenemos que $|T| \in \{4, 7\}$. Adicionalmente, observemos que si $|A| = 2n + 3$, entonces

$$\begin{aligned} 2n - 2 \geq |B| - |T| \Rightarrow |T| &\geq |A| - 2n + 2 \\ &= 2n + 3 - 2n + 2 \\ &= 5 \end{aligned}$$

por tanto, $|T| = 7$.

Afirmamos que $0 \nmid B$, es decir, $|S_i| = 2$ para cada $i$, y que $|A| = 2n + 2$, es

decir, $D(G) = 2n + 2$. Supongamos que $0 \mid B$. Por Lema 3.2.1 y dado que $D(H) = D(C_n) = n$, $\exp(G/H) = \exp(C_2^3) = 2$, $D_0(G/H) = 3$ (Lema 2.2.3) y $|I < | = \mathbf{v}_0(B)$ obtenemos

$$\begin{aligned} 2n + 2 \leq |A| &\leq (D(H)\exp(G/H)) + D_0'(G/H) - |I_<| \\ &= 2n + 3 - \mathbf{v}_0(B) \end{aligned}$$

$\Longrightarrow \mathbf{v}_0(B) \leq 1$, luego $\mathbf{v}_0(B) = 1$, de allí que $|A| \leq 2n + 3 - 1 = 2n + 2$, por tanto $|A| = 2n+2$. Por otra parte, tenemos que $T^{-1}B$ tiene una sola secuencia de longitud 1 y las restantes $(k-1)$ secuencias tienen longitud 2 de modo que

$$\begin{aligned} |B| - |T| = 2(k-1) + 1 = 2k - 1 &\Rightarrow |T| = 2n + 2 - 2k + 1 \\ &\Rightarrow |T| = 2(n-k) + 3 \\ &\Rightarrow |T| = 2l + 3 \\ &\Rightarrow |T| \in \{5, 7\} \end{aligned}$$

Por la Observación 3.1.1 concluimos que $|T| = 7$.

Así, si $0 \mid B$ ó $|A| = 2n + 3$, entonces $|T| = 7$. Suponemos que $|T| = 7$, es decir, $supp(T) = G/H \setminus \{0\}$, por ser $T$ libre de cuadrado.

De la desigualdad $n - 1 \geq k \geq (|B| - |T|)/2$, tenemos

$$\begin{aligned} n - 1 \geq k \geq (|B| - |T|)/2 &\geq (2n + 2 - 7)/2 \\ &= n - 2{,}5 \end{aligned}$$

luego, $n - 2{,}5 \leq k \leq n - 1$, de modo que $n - 2 \leq k \leq n - 1$.

Si $k = n - 1$ entonces $B = S_1 ... S_{n-1} T$, donde $S_i$ son secuencias minimales de suma

cero y dado que $\sigma(T) = 0$ y $|T| = 7$, entonces existen $T_1', T_2'$, secuencias de suma cero tal que $T = T_1'T_2'$, luego

$$B = S_1...S_{n-1}T_1'T_2', \quad con \quad S_i, T_1', T_2' \in \mathcal{B}(G/H),$$

esto implica, $n + 1 \leq \max \mathbf{L}(B) = n$, lo cual es imposible, de modo que $k = n - 2$ y por tanto $l = n - k = n - n + 2 = 2$, luego dado que $\varphi(\sigma(F_i)) = 0$, $\varphi(\sigma(R_j)) = 0$ para $i \in [1, n-2], j \in [1, 2]$ por el Corolario 3.2.1 tenemos,

$$\begin{aligned} & B = S_1...S_{n-2}T_1T_2 \\ \Rightarrow \quad & A = F_1...F_{n-2}R_1R_2 \\ \Rightarrow \quad & \sigma(F_1)...\sigma(F_{n-2})\sigma(R_1)\sigma(R_2) = g^n \text{ para algún } g \in H \text{ con } H = \langle g \rangle \end{aligned}$$

Recordemos que estamos suponiendo $supp(T) = G/H \setminus \{0\}$, es decir,
$T = e_1e_2e_3(e_1 + e_2)(e_1 + e_3)(e_2 + e_3)(e_1 + e_2 + e_3)$, donde $\{e_1, e_2, e_3\}$ es base de $C_2^3$. Para $I \subset [1, 3]$ sea $g_I \mid R$ tal que $\varphi(g_I) = \sum_{i \in I} e_i$, de modo que $R = \prod_{I \subset [1,3]} g_I$, $A = F_1...F_{n-2}R$. Como $\sigma(\varphi(R)) = \sigma(T) = 0$, si $R_1' \mid R$, con $\sigma(\varphi(R_1')) = 0$ entonces $R = R_1'R_2'$ y $\sigma(\varphi(R_1')) = \sigma(\varphi(R_2')) = 0$, luego $A = F_1...F_{n-2}R_1'R_2'$ y por el Corolario 3.2.1 $\sigma(R_i') = g$ con $\langle g \rangle = H$.
Así, como $\sigma(\varphi(g_{\{1,2,3\}}g_1g_2g_3)) = 0$ entonces

$$g_{\{1,2,3\}} + g_1 + g_2 + g_3 = g$$

y como para $k \neq i, j$, $\sigma(\varphi(g_{\{i,j\}}g_kg_{\{1,2,3\}})) = 0$ entonces

$$g_{\{i,j\}} + g_k + g_{\{1,2,3\}} = g$$

así,

$$\begin{aligned} & g_{\{1,2,3\}} + g_1 + g_2 + g_3 = g_{\{i,j\}} + g_k + g_{\{1,2,3\}} \\ \Rightarrow \quad & g_i + g_j + g_k = g_{\{i,j\}} + g_k \\ \Rightarrow \quad & g_i + g_j = g_{\{i,j\}} \end{aligned}$$

además, $\sigma(\varphi(g_i g_j g_{\{i,j\}})) = 0$ entonces

$g_i + g_j + g_{\{i,j\}} = g$ y así $2g_{\{i,j\}} = g$

y también $\sigma(\varphi(g_{\{1,2\}} g_{\{1,3\}} g_{\{2,3\}})) = 0$ entonces

$$\begin{aligned} & g_{\{1,2\}} + g_{\{1,3\}} + g_{\{2,3\}} = g \\ \Rightarrow \quad & 2g_{\{1,2\}} + 2g_{\{1,3\}} + 2g_{\{2,3\}} = 2g \\ \Rightarrow \quad & g + g + g = g \\ \Rightarrow \quad & 3g = g \\ \Rightarrow \quad & g = 0 \ \text{ contradicción.} \end{aligned}$$

En consecuencia, tenemos $|A| = 2n + 2$ y $0 \nmid B$. Además, $|T| = 4$ y $T$ es una secuencia de suma cero minimal; en particular,

$$\begin{aligned} & |B| - |T| = 2k \\ \Rightarrow \quad & 2n + 2 - 4 = 2k \\ \Rightarrow \quad & k = n - 1 \wedge l = 1. \end{aligned}$$

Obsevemos que por la Proposición 3.1.1 para cada $T' \mid T$ de longitud 3 el conjunto $supp(T')$ es una base de $G/H$.

De nuevo, por el Corolario 3.2.1 tenemos $\sigma(F_1)...\sigma(F_{n-1})\sigma(R) = g^n$, para algún

elemento generador $g$ de $H$. Por conveniencia de notación asumimos $F_n = R$.

Como $\varphi(R) = T$ es minimal de suma cero y de longitud cuatro, por la Proposición 3.1.1 $\varphi(R) = e_1e_2e_3(e_1+e_2+e_3)$ para $\{e_1, e_2, e_3\}$ base de $C_2^3$ de modo que $v_x(\varphi(R)) = 1, \forall x \mid \varphi(R)$ en consecuencia $R = g_1g_2g_3g_{\{1,2,3\}}$ donde $\varphi(g_i) = e_i$, $\varphi(g_{\{1,2,3\}}) = \sum_{i=1}^{3} e_i$.

Dado que $|A| = 2n + 2 = \mathsf{D}(G)$, por el Teorema 3.2.1 el resultado (vi) del Lema 3.3.1 es aún más fuerte pues en ese caso $\langle supp(A)\rangle = G$. De aquí en adelante al hacer referencia al resultado (vi) del Lema 3.3.1 tendremos en cuenta éste hecho.

Comenzemos la investigación detallada de la secuencia $A$. Distinguimos varios casos de acuerdo con el número de elementos en $supp(F) \cap supp(R)$. Sea $N = |supp(F) \cap supp(R)|$. Notemos que en el caso $n = 2$ se tiene $|supp(F)| = 1$ (F tiene $n - 1$ subsecuencias de longitud 2) y así $N \leq 1$.

Supongamos $N \geq 1$ y que $g_3 \in supp(F) \cap supp(R)$. Si $supp(F)\backslash supp(F) \cap supp(R) \neq \emptyset$, consideremos $g' \in supp(F)\backslash supp(F) \cap supp(R)$ por el Lema 3.3.1 $(vi)$

$B_0 = \{g_1, g_2, g_3\}$ es base de $G$ ($g_1g_2g_3 \mid R$ y $g_3 \in supp(F)$), así

$$g' = \alpha_1 g_1 + \alpha_2 g_2 + \alpha_3 g_3 \text{ con } \alpha_i \in \{0, 1\}$$

$$\Rightarrow \quad \varphi(g') = \alpha_1\varphi(g_1) + \alpha_2\varphi(g_2) + \alpha_3\varphi(g_3)$$

Si $\varphi(g') = \varphi(g_1) + \varphi(g_2) + \varphi(g_3) = \varphi(g_{\{1,2,3\}})$ $\quad (\varphi(g_I) = \sum_{i\in I} e_i)$ por el Lema 3.3.1 (i) $g' = g_{\{1,2,3\}} \in supp(R)$ contradicción, de modo que

$$\varphi(g') = \varphi(g_i) + \varphi(g_j) \text{ con } i, j \in \{1, 2, 3\}, i \neq j. \tag{3.3}$$

Si $\varphi(g') = \varphi(g_1) + \varphi(g_2)$ entonces por el Lema 3.3.1 (iv)

$$g' = g_1 + g_2 \tag{3.4}$$

Además, $B = \{g_2, g_3, g_{\{1,2,3\}}\}$ es también una base de $G$ ($g_3 \in supp(F) \cap supp(R)$) luego,

$$g' = \alpha_1 g_2 + \alpha_2 g_3 + \alpha_3 g_{\{1,2,3\}} \text{ con } \alpha_i \in \{0,1\}$$
$$\Rightarrow \quad \varphi(g') = \alpha_1 \varphi(g_2) + \alpha_2 \varphi(g_3) + \alpha_3 \varphi(g_{\{1,2,3\}})$$

Si $\varphi(g') = \varphi(g_2) + \varphi(g_3) + \varphi(g_{\{1,2,3\}}) = \varphi(g_1)$ $\quad (\varphi(g_I) = \sum_{i \in I} e_i)$ por el Lema 3.3.1 (i) $g' = g_1 \in supp(R)$ contradicción.

Si $\varphi(g') = \varphi(g_2) + \varphi(g_3)$ por el lema 3.3.1 (iv) $g' = g_2 + g_3 = g_1 + g_2$ (por 3.4) por tanto, $g_3 = g_1$ contradicción (los elementos de $R$ tienen multiplicidad 1).

Si $\varphi(g') = \varphi(g_2) + \varphi(g_{\{1,2,3\}})$ por el Lema 3.3.1 (iv) $g' = g_2 + g_{\{1,2,3\}} = g_1 + g_2$ (por 3.4) por tanto, $g_{\{1,2,3\}} = g_1$ contradicción (los elementos de $R$ tienen multiplicidad 1).

De modo que,

$$\varphi(g') = \varphi(g_3) + \varphi(g_{\{1,2,3\}}) \tag{3.5}$$

De 3.3 y 3.5 concluimos que

$$\varphi(g') = \varphi(g_3) + \varphi(g_i) \text{ con } i \in \{1, 2, \{1,2,3\}\}$$

y por el lema 3.3.1 (iv)

$$g' = g_3 + g_i \text{ con } i \in \{1, 2, \{1,2,3\}\} \tag{3.6}$$

Supongamos $N = 4$. $F = F_1 ... F_{n-1}$ por el Lema 3.3.1 (ii), $F_i = f_i^2$. Como $4 = |supp(F) \cap supp(R)|$, $|R| = 4$ con $R$ libre de cuadrado y por el Lema 3.3.1 (iii)

entonces

$$\begin{aligned} & R = g_1 g_2 g_3 g_4 \ \text{ con } \ g_j \mid F_{i_j} \\ \Rightarrow \quad & R^2 = g_1^2 g_2^2 g_3^2 g_4^2 = F_{i_1} ... F_{i_4} \mid F \\ \Rightarrow \quad & \sigma(R^2) = \sigma(F_{i_1}) + ... + \sigma(F_{i_4}) \\ \Rightarrow \quad & \sigma(R^2) = 4g \end{aligned}$$

pero $\sigma(R^2) = 2\sigma(R) = 2g$, luego $4g = 2g$ contradicción.

Supongamos $N = 3$. Sea $R = g_1 g_2 g_3 g_{\{1,2,3\}}$ tal que $g_j | F, g_{\{1,2,3\}} \nmid F$ y $v_3 = v_{g_3}(A) \geq v_2 = v_{g_2}(A) \geq v_1 = v_{g_1}(A)$. Sea $g' \in supp(F) \backslash \{g_1, g_2, g_3\}$ entonces por el Lema 3.3.1 (vi)

$$\begin{aligned} & g' = \alpha_1 g_1 + \alpha_2 g_2 + \alpha_3 g_3 \\ \Rightarrow \quad & \varphi(g') = \alpha_1 \varphi(g_1) + \alpha_2 \varphi(g_2) + \alpha_3 \varphi(g_3) \ \text{ con } \ \alpha_i \in \{0, 1\} \end{aligned}$$

Si $\alpha_i = 1 \forall i \in \{1, 2, 3\}$ entonces

$$\begin{aligned} \varphi(g') &= \varphi(g_1) + \varphi(g_2) + \varphi(g_3) \\ &= -\varphi(g_{\{1,2,3\}}) \quad (\sigma(\varphi(R)) = 0) \\ &= \varphi(g_{\{1,2,3\}}) \end{aligned}$$

luego por el Lema 3.3.1 (i) $g' = g_{\{1,2,3\}}$ contradicción ($g_{\{1,2,3\}} \nmid F$).

Supongamos que existe $j \in \{1, 2, 3\}$ tal que $\alpha_i = 0$ entonces

$$\varphi(g') = \varphi(g_k) + \varphi(g_l), \quad \{k, l\} \subset \{1, 2, 3\}$$

lo cual no es posible pues de acuerdo al Lema 3.3.1 (v) la ecuación anterior no tiene solución en $supp(\varphi(F))$.

De modo que,

$$supp(F) = \{g_1, g_2, g_3\}$$

Sean $f_3 = g_3$, $f_2 = g_2 - g_3$, $f_1 = g_1 - g_3$. Por el Lema 3.3.1 (iii) $2g_j = g$ para cada $j \in \{1, 2, 3\}$, por tanto $ord(f_1) = ord(f_2) = 2$, además, $ord(f_3) = 2n$ y por el mismo Lema (vi) se sigue que $\{g_1, g_2, g_3\}$ es un conjunto generador de $G$ y dado que $g_3 = f_3, g_2 = f_2 + f_3, g_1 = f_1 + f_3$ entonces $\{f_1, f_2, f_3\}$ es también un conjunto generador de $G$ y, debido al orden de cada elemento, una base. Recordando que por el Lema 3.3.1 (vi), $g_{\{1,2,3\}} = g_3 - g_2 - g_1$, obtenemos

$$A = f_3^{v_3}(f_3 + f_2)^{v_2}(f_3 + f_1)^{v_1}(-f_3 + f_2 + f_1),$$

donde $v_3 \geq v_2 \geq v_1$, cada $v_i$ es impar por el Lema 3.3.1 (ii). Así, A es de la forma dada en 1.

Supongamos $N = 2$. Sea $R = g_1g_2g_3g_{\{1,2,3\}}$ con $g_1g_{\{1,2,3\}} \nmid F$, $g_2g_3 \mid F$. Si existe algún $g' \in supp(F) \backslash supp(F) \cap supp(R) = supp(F) \backslash \{g_2, g_3\}$ entonces, por el Lema 3.3.1 (vi), se tiene que

$$g' = \alpha_1 g_1 + \alpha_2 g_2 + \alpha_3 g_3 \text{ con } \alpha_i \in \{0, 1\}$$
$$\Rightarrow \quad \varphi(g') = \alpha_1\varphi(g_1) + \alpha_2\varphi(g_2) + \alpha_3\varphi(g_3)$$

Si $\alpha_i = 1, \forall i \in \{1, 2, 3\}$ entonces

$$\begin{aligned} \varphi(g') &= \varphi(g_1) + \varphi(g_2) + \varphi(g_3) \\ &= -\varphi(g_{\{1,2,3\}}) \qquad\qquad (\sigma(\varphi(R)) = 0) \\ &= \varphi(g_{\{1,2,3\}}) \end{aligned}$$

luego, por el Lema 3.3.1 (i) $g' = g_{\{1,2,3\}} \notin supp(F) \rightarrow\leftarrow$, además por el mismo Lema (v) $\varphi(g') \neq \varphi(g_2) + \varphi(g_3)$. Luego, debe cumplirse que

$$\varphi(g') = \varphi(g_j) + \varphi(g_1) \text{ para } j \in \{2, 3\}$$

y por el Lema 3.3.1 (iv) $g' = g_j + g_1$ con $j \in \{2, 3\}$, de modo que $|supp(F)| \leq 4$. En el caso $supp(F)\backslash\{g_2, g_3\} \neq \emptyset$, acordamos que este conjunto contiene un elemento $g_{\{1,3\}}$ con $\varphi(g_{\{1,3\}}) = \varphi(g_1) + \varphi(g_3)$. Por el Lema 3.3.1 (iv) tenemos $g_{\{1,3\}} = g_1 + g_3$. Similar a la anterior, sea $f_3 = g_3$ y $f_2 = g_2 - g_3$. Como $2g_3 = 2g_2 = g$ tenemos que $ord(f_2) = 2$, y de nuevo $g_{\{1,2,3\}} = g_3 - g_2 - g_1$. Supongamos que $2g_1 \neq 0$ (en el caso de que $2f_{i_1} = 0$ tenemos que $g_1 - 0g_3$ tiene orden 2) entonces

$$\begin{aligned}
& 2\varphi(g_1) = 0 \\
\Rightarrow\ & 2g_1 \in H = \langle g \rangle \\
\Rightarrow\ & 2g_1 = ag \text{ con } a \in [0, n-1] \\
\Rightarrow\ & 2g_1 = a2g_3 \quad (g_3 \in supp(F)) \\
\Rightarrow\ & 2(g_1 - ag_3) = 0 \\
\Rightarrow\ & \text{ord}(g_1 - ag_3) \leq 2
\end{aligned}$$

Note que $\text{ord}(g_1 - ag_3) = 1$ no ocurre, de modo que para algún $a \in [0, n-1]$, $f_1 = g_1 - ag_3$ tiene orden 2. De nuevo, el conjunto $\{f_1, f_2, f_3\}$ es un conjunto generador de $G$ y en consecuencia una base.

Si $|supp(F)| = 2$, entonces

$$A = f_3^{v_3}(f_3 + f_2)^{v_2}(af_3 + f_1)(-af_3 + f_2 + f_1)$$

donde de nuevo $v_i \geq 3$ es impar. Posiblemete cambiando la base, obtenemos $v_3 \geq v_2$. Notemos que en el caso $a = 0$ ó $a = 1$ la secuencia es de la forma dada en 6. y 1., respectivamente, y en caso contrario es de la forma dada en 2.

Ahora, supongamos $|supp(F)| = 3$. Como acordamos, el tercer elemento en $supp(F)$ es $g_{\{1,3\}} = g_1 + g_3$. Por otra parte ya que $2g_{\{1,3\}} = g = 2g_3$, se sigue que $2g_1 = 0$ y así $a = 0$. Por lo tanto,

$$A = f_3^{v_3}(f_3 + f_2)^{v_2}(f_3 + f_1)^{v_1} f_1(f_2 + f_1)$$

donde $v_2, v_3 \geq 3$ impar, y $v_1 \geq 2$ par. Así la secuencia es, después de un cambio de base, de la forma dada en 6.

Finalmente, si $|supp(F)| = 4$, entonces de nuevo por lo acordado $g_{\{1,3\}} \in supp(F)$, y el cuarto elemento en $supp(F)$ es igual a $g_1 + g_2$, es decir

$$A = f_3^{v_3}(f_3 + f_2)^{v_2}(f_3 + f_1)^{v_1}(f_3 + f_2 + f_1)^{v_4} f_1(f_2 + f_1)$$

$v_2, v_3 \geq 3$ impar, y $v_1, v_4 \geq 2$ par. Así de nuevo la secuencia es, después de un cambio de base, de la forma dada en 6.

Supongamos $N = 1$. Sean $R = g_1 g_2 g_3 g_{\{1,2,3\}}$, $supp(F) \cap supp(R) = \{g_3\}$. Por 3.6 sabemos que cada elemento de $supp(F) \backslash \{g_3\}$ es la suma de $g_3$ y otro elemento de $supp(R)$. Si $|supp(F)| \geq 2$, entonces sea $g_{\{2,3\}} = g_2 + g_3 \in supp(F)$ y si $|supp(F)| = 3$, entonces sea adicionalmente $g_{\{1,3\}} = g_1 + g_3 \in supp(F)$. Si $|supp(F)| = 4$ entonces

$supp(F) = \{g_3, g_3 + g_1, g_3 + g_2, g_3 + g_{\{1,2,3\}}\}$, pero

$$\begin{aligned} & \sigma(\varphi(R)) = 0 \\ \Rightarrow \quad & \varphi(g_1 + g_2 + g_3 + g_{\{1,2,3\}}) = 0 \\ \Rightarrow \quad & \varphi(g_1) + \varphi(g_2) = \varphi(g_3 + g_{\{1,2,3\}}) \\ \Rightarrow \quad & (\varphi(g_1) + \varphi(g_3)) + (\varphi(g_2) + \varphi(g_3)) = \varphi(g_3 + g_{\{1,2,3\}}) \\ \Rightarrow \quad & \varphi(g_1 + g_3) + \varphi(g_2 + g_3) = \varphi(g_3 + g_{\{1,2,3\}}) \end{aligned}$$

por el Lema 3.3.1 (v) la igualdad anterior es una contradicción, de modo que $|supp(F)| \leq 3$.

Sea $f_3 = g_3$. como antes existen $a, b \in [0, n-1]$ tal que el orden de $g_2 - af_3 = f_2$ y de $g_1 - bf_3 = f_1$ es dos. El conjunto $\{f_1, f_2, f_3\}$ es una base de $G$. También por el Lema 3.3.1 (vi) tenemos $g_3 = g_1 + g_2 + g_{\{1,2,3\}}$. Así, si $|supp(F)| = 1$, entonces

$$A = f_3^{2n-1}(af_3 + f_2)(bf_3 + f_1)(cf_3 + f_2 + f_1)$$

donde $c \in [0, 2n-1]$ y $(a+b+c)f_3 = f_3$ $(a+b+c \equiv 1(mod 2n))$. Posiblemente cambiando la base, obtenemos $a \leq b \leq c$. Si $a = b = 0$, entonces la secuencia es de la forma dada en 6. Si $a = 0$ y $b \geq 2$, es de la forma dada en 4. Si $a = b = 1$ entonces es de la forma dada en 1. Si $a = 1$ y $b \geq 2$, entonces es de la forma dada en 2. Queda por considerar el caso $a \geq 2$; notemos que esto implica $a + b + c = 2n + 1$. Si $c = n$ ó $c = n + 1$, consideramos la base $\{f_1' = f_2, f_2' = nf_3 + f_2 + f_1, f_3' = f_3\}$ entonces

$$\begin{aligned} A &= (f_3')^{2n-1}(af_3' + f_1')(bf_3' + f_2' - nf_3' - f_1')(cf_3' + f_1' + f_2' - nf_3' - f_1') \\ &= (f_3')^{2n-1}(af_3' + f_1')((b-n)f_3' + f_2' + f_1')((c-n)f_3' + f_2') \end{aligned}$$

si $c = n$ entonces $a + b + c = 2n + 1 \Rightarrow b - n = 1 - a$ y

$$A = (f_3')^{2n-1}(af_3' + f_1')((1-a)f_3' + f_2' + f_1')f_2'$$

luego la secuencia es de la forma dada en 4.

Si $c = n + 1$ entonces $a + b + c = 2n + 1 \Rightarrow b - n = -a$ y

$$A = (f_3')^{2n-1}(af_3' + f_1')(-af_3' + f_2' + f_1')(f_3' + f_2')$$

luego la secuencia es de la forma dada en 2., si $c \notin \{n, n+1\}$ $A$ es de la forma dada en 3.

Supongamos $|supp(F)| \geq 2$. Como $g_3, g_{\{2,3\}} \in supp(F) \Rightarrow 2g_{\{2,3\}} = g = 2g_3 \Rightarrow 2g_2 + 2g_3 = 2g_3 \Rightarrow 2g_2 = 0$, tenemos $ord(g_2) = 2$, esto es $a = 0$ $(g_2 - af_3 = f_2, ord(f_2) = 2$ , $ord(f_3) = 2n$ y $a \in [0, n-1])$.

Si $|supp(F)| = 2$, tenemos

$$\begin{aligned}
A &= g_3^{v_3}(g_{\{2,3\}})^{v_2} g_1 g_2 g_{\{1,2,3\}} \\
&= g_3^{v_3}(g_2 + g_3)^{v_2} g_1 g_2 (g_3 - g_1 - g_2) \\
&= f_3^{v_3}(f_2 + f_3)^{v_2}(f_1 + bf_3) f_2 (f_3 - f_1 - bf_3 - f_2) \\
&= f_3^{v_3}(f_2 + f_3)^{v_2}(f_1 + bf_3) f_2 ((1-b)f_3 + f_1 + f_2) \\
&= f_3^{v_3}(f_2 + f_3)^{v_2}(f_1 + bf_3) f_2 (cf_3 + f_1 + f_2), \quad \text{con } b + c \equiv 1 (mod 2n)
\end{aligned}$$

con $v_3$ impar y $v_2$ par, por lo que $v_3 + 2v + 3 = 2n + 2$, donde $v_2 = 2v$, así $v_3 = 2n - 1 - 2v$, luego

$$A = f_3^{2n-1-2v}(f_2 + f_3)^{2v}(f_1 + bf_3) f_2 (cf_3 + f_1 + f_2)$$

con $(b+c)f_3 = f_3$. Si $b = 0$, la secuencias es de la forma dada en 6., si $b = 1$ y consideramos la base $\{f_1' = f_1 + f_2, f_2' = f_2, f_3' = f_3\}$ entonces

$$A = (f_3')^{2n-1-2v}(f_2' + f_3')^{2v}(f_1' + f_2' + f_3')f_2'f_1'$$

es de la forma dada en 6., de lo contrario es de la forma dada en 4.

Ahora, si $|supp(F)| = 3$. Entonces, adicionalmente, $g_{\{1,3\}} = g_1 + g_3 \in supp(F)$, luego $2g_1 + 2g_3 = g = 2g_3 \Rightarrow 2g_1 = 0 \Rightarrow \text{ord}(g_1) = 2$ por tanto, $0 = 2f_1 = 2g_1 - 2bf_3 \Rightarrow 2bf_3 = 0 \Rightarrow b = 0$ pues $b \in [0, n-1]$ y $\text{ord}(f_3) = 2n$. Así

$$\begin{aligned} A &= g_3^{v_3}(g_{\{2,3\}})^{v_2}(g_{\{1,3\}})^{v_1}g_1g_2g_{\{1,2,3\}} \\ &= g_3^{v_3}(g_2 + g_3)^{v_2}(g_1 + g_3)^{v_1}g_1g_2(g_3 - g_1 - g_2) \\ &= f_3^{v_3}(f_2 + f_3)^{v_2}(f_1 + f_3)^{v_1}f_1f_2(f_3 - f_1 - f_2) \\ &= f_3^{v_3}(f_2 + f_3)^{v_2}(f_1 + f_3)^{v_1}f_1f_2(f_3 + f_1 + f_2) \end{aligned}$$

con $v_3$ impar y $v_2, v_1$ par, por tanto $v_1 + v_2 + v_3 + 3 = 2n + 2 \Rightarrow v_3 = 2n - 1 - 2v - 2w$ con $v_2 = 2v, v_1 = 2w$. Así

$$A = f_3^{2n-1-2v-2w}(f_2 + f_3)^{2v}(f_1 + f_3)^{2w}f_1f_2(f_3 + f_1 + f_2)$$

y la secuencia es de la forma dada en 6.

Supongamos $N = 0$. Sea $R = g_1g_2g_3g_{\{1,2,3\}}$. $\varphi(R)$ es minimal de suma cero de longitud 4 en $G/H \cong C_2^3$, así por la Proposición 3.1.1 $supp(\varphi(R)) = \{e_1, e_2, e_3, e_1 + e_2 + e_3\}$ con $\{e_1, e_2, e_3\}$ base de $G/H$, de modo que $G/H \backslash supp(\varphi(R)) = \{e_1 + e_2, e_1 + e_3, e_2 + e_3, 0\}$. Si $f \notin supp(R)$ entonces $\varphi(f) \notin supp(\varphi(R))$ ($\varphi$ es inyectiva en $\varphi(A)$). De modo que si $f \in supp(F)$ entonces $\varphi(f) = e_i + e_j$ con $i, j \in \{1, 2, 3\}, i \neq j$,

es decir $\varphi(f) = \varphi(g_i) + \varphi(g_j)$ y por el Lema 3.3.1 (iv) se tiene $f = g_i + g_j$ con $i, j \in \{1, 2, 3\}, i \neq j$. Si $|supp(F)| = 3$ entonces

$$\begin{aligned} \varphi(g_1 + g_2) &= \varphi(g_1) + \varphi(g_2) \\ &= \varphi(g_1) + \varphi(g_3) + \varphi(g_2) + \varphi(g_3) \\ &= \varphi(g_1 + g_3) + \varphi(g_2 + g_3) \end{aligned}$$

con $g_1 + g_2, g_1 + g_3, g_2 + g_3 \in supp(F)$ lo cual contradice el Lema 3.3.1 (v). Por tanto $|supp(F)| \leq 2$. Sea $g_{\{2,3\}} = g_2 + g_3 \in supp(F)$ y, en el caso $|supp(F)| = 2$ sea $g_{\{1,3\}} = g_1 + g_3 \in supp(F)$.

Sea $f_3 = g_{\{2,3\}}$ y $f_1, f_2 \in G$ tal que $\{f_1, f_2, f_3\}$ es una base de $G$. Como $g_2 + g_3 \in supp(F)$ entonces por el Lema 3.3.1 (iii) $\text{ord}(f_3) = \text{ord}(g_2 + g_3) = 2n$, por tanto $\text{ord}(f_1) = \text{ord}(f_2) = 2$. Para $I \in \{1, 2, 3, \{1, 2, 3\}\}$, sea $g_I = a_I f_3 + b_I f_2 + c_I f_1$ con $a_I \in [0, 2n-1]$ y $b_I, c_I \in \{0, 1\}$. Nótemos que

$$\begin{aligned} & \sigma(\varphi(R)) = 0 \\ \Rightarrow \quad & \varphi(g_1 + g_2 + g_3 + g_{\{1,2,3\}}) = 0 \\ \Rightarrow \quad & \varphi(g_2 + g_3) = \varphi(g_1 + g_{\{1,2,3\}}) \end{aligned}$$

por el Lema 3.3.1 (i) se tiene

$$g_2 + g_3 = g_1 + g_{\{1,2,3\}} \tag{3.7}$$

además,

$$\begin{aligned} & f_3 = g_2 + g_3 = (a_2 + a_3)f_3 + (b_2 + b_3)f_2 + (c_2 + c_3)f_1 \\ \Rightarrow \quad & f_3 = (a_2 + a_3)f_3 \ \wedge \ (b_2 + b_3) \equiv 0(mod 2) \ \wedge \ (c_2 + c_3) \equiv 0(mod 2) \\ \Rightarrow \quad & a_2 + a_3 \equiv 1(mod 2n) \ \wedge \ b_2 = b_3 \ \wedge \ c_2 = c_3, \end{aligned}$$

por 3.7 se tiene,

$$\begin{aligned}(a_2+a_3)f_3 &= (a_1+a_{\{1,2,3\}})f_3\\ (b_2+b_3)f_2 &= (b_1+b_{\{1,2,3\}})f_2\\ (c_2+c_3)f_1 &= (c_1+c_{\{1,2,3\}})f_1\end{aligned}$$

de donde,

$$\begin{aligned}1\equiv a_2+a_3 &\equiv a_1+a_{\{1,2,3\}}(mod 2n)\\ 0\equiv b_2+b_3 &\equiv b_1+b_{\{1,2,3\}}(mod 2)\\ 0\equiv c_2+c_3 &\equiv c_1+c_{\{1,2,3\}}(mod 2)\end{aligned}$$

así, $a_1+a_{\{1,2,3\}}\equiv 1(mod 2n)$, $b_1=b_{\{1,2,3\}}$, y $c_1=c_{\{1,2,3\}}$. Además, $\{g_1,g_2,g_3\}$ es un conjunto generador de $G$. ($G=\{g_1,g_2,g_3,g_{\{1,2,3\}}=g_2+g_3-g_1,g_i+g_j,ag\}$ con $i,j\in\{1,2,3\}, i\neq j$ y $a\in[0,n-1]$, como $\sigma(R)=g$ entonces $2g_1+2g_2+2g_3=g\Rightarrow ag=2a(g_1+g_2+g_3)$).

Si $g_2,g_3\in H$ entonces $\varphi(g_2)=0=\varphi(g_3)$ por el Lema 3.3.1 (i) $g_2=g_3$ contradicción, luego o $g_2$ ó $g_3$ es un elemento de $H$, se sigue que $(b_3,c_3)\neq(0,0)$. Por cambio de base, asumimos $b_3=1$ y $c_3=0$. Como $\{g_1,g_2,g_3\}$ es un conjunto generador de $G$ y $c_2=c_3=0$, se sigue que $c_1\neq 0$, y por cambio de base, podemos asumir que $b_1=0$. Si $supp(F)=\{g_{\{2,3\}}\}$, entonces

$$\begin{aligned}A &= (g_{\{2,3\}})^{2n-2}g_1g_2g_3g_{\{1,2,3\}}\\ &= (g_2+g_3)^{2n-2}g_1g_2g_3(g_2+g_3-g_1)\\ &= (f_3)^{2n-2}(a_1f_3+f_1)(a_2f_3+f_2)(a_3f_3+f_2)((a_2+a_3-a_1)f_3+2f_2-f_1)\\ &= (f_3)^{2n-2}(a_1f_3+f_1)((1-a_3)f_3+f_2)(a_3f_3+f_2)((1-a_1)f_3+f_1)\end{aligned}$$

posiblemente cambiando la base, obtenemos $a_1, a_3 \in [0, n-1]$ y $a_3 \geq a_1$. Si $a_3 \in \{0,1\}$ la secuencia es de la forma dada en 6., si $a_3 \geq 2$ y $a_1 \in \{0,1\}$ la secuencia es de la forma dada en 4., y de lo contrario es de la forma dada en 5.

Ahora, supongamos $|supp(F)| = 2$. Por acuerdo $g_{\{1,3\}} = g_1 + g_3 \in supp(F)$. Sea $g_{\{1,3\}} = a_{\{1,3\}}f_3 + b_{\{1,3\}}f_2 + c_{\{1,3\}}f_1$ con $a_{\{1,3\}} \in [0, 2n-1]$ y $b_{\{1,3\}}, c_{\{1,3\}} \in \{0,1\}$. Como $g_{\{2,3\}}, g_{\{1,3\}} \in supp(F)$ entonces $2g_{\{2,3\}} = g = 2g_{\{1,3\}}$ y $\sigma(\varphi(R)) = 0 \Rightarrow \varphi(g_{\{1,3\}}) = \varphi(g_1 + g_3) = \varphi(g_2 + g_{\{1,2,3\}}) = \varphi(g_2) + \varphi(g_{\{1,2,3\}})$, luego por el Lema 3.3.1 (iv) se tiene $g_{\{1,3\}} = g_1 + g_3 = g_2 + g_{\{1,2,3\}}$. En consecuencia $a_{\{1,3\}} \in \{1, 1+n\}$ y $b_{\{1,3\}} = c_{\{1,3\}} = 1$.

Observemos que $\sigma(g_{\{1,3\}}g_1g_2) = g_{\{1,3\}} + g_1 + g_2 = (a_{\{1,3\}} + a_1 + a_2)f_3 + 2f_1 + 2f_2 = (a_{\{1,3\}} + a_1 + a_2)f_3 \in \langle f_3 \rangle$. Sea $k \in \mathbb{N}$ tal que $2k = \mathbf{v}_{f_3}(A)$. Observemos que si $\Pi = [0, 2k] \times [0, 2l]$ entonces

$$\begin{aligned}
\Sigma(g_{\{1,3\}}^{-2}F) &= \{\Sigma(g_{\{2,3\}}^i g_{\{1,3\}}^j) : (i,j) \in \Pi\backslash\{(0,0)\}\} \\
&= \{ig_{\{2,3\}} + jg_{\{1,3\}} : (i,j) \in \Pi\backslash\{(0,0)\}\} \\
&= \{i(a_{\{2,3\}}f_3 + b_{\{2,3\}}f_2 + c_{\{2,3\}}f_1) + j(a_{\{1,3\}}f_3 + b_{\{1,3\}}f_2 + c_{\{1,3\}}f_1) : (i,j) \in \Pi\backslash\{(0,0)\} \\
&= \{i(f_3 + 2f_2 + 0f_1) + j(a_{\{1,3\}}f_3 + f_2 + f_1) : (i,j) \in \Pi\backslash\{(0,0)\}\} \\
&= \{if_3 + j(a_{\{1,3\}}f_3 + f_2 + f_1) : (i,j) \in \Pi\backslash\{(0,0)\}\}
\end{aligned}$$

Si $j$ es par entonces $\Sigma(g_{\{1,3\}}^{-2}F) \subset \langle f_3 \rangle$ y además si $a_{\{1,3\}} = n+1$ entonces $j(n+1)f_3 = jf_3$ de modo que

$$\sum(g_{\{1,3\}}^{-2}F) \cap \langle f_3 \rangle = \{if_3 + j(2f_3) : (i,j) \in [0,2k] \times [0,l]\backslash\{(0,0)\}\}$$

con $2l + 2k + 4 = 2n \Rightarrow l = n - 2 - k$ por tanto

$$\begin{aligned}\sum(g_{\{1,3\}}^{-2}F) \cap \langle f_3 \rangle &= \{(i+2j)f_3 : (i,j) \in [0,2k] \times [0,n-2-k] \backslash \{(0,0)\}\} \\ &= \{jf_3 : j \in [1,2n-4]\}.\end{aligned}$$

Como $-\sigma(g_{\{1,3\}}g_1g_2) \notin \Sigma(g_{\{1,3\}}^{-2}F) \cup \{0\}$, se sigue que $\sigma(g_{\{1,3\}}g_1g_2) \in \{f_3, 2f_3, 3f_3\}$. Usando $g_{\{1,3\}} = g_1 + g_3$ y $a_2f_3 = (1 - a_3f_3)$, resulta que $\sigma(g_{\{1,3\}}g_1g_2) = (1 + 2a_1)f_3$. Por consiguiente, $a_1 \in \{0, 1, n, 1+n\}$. Además, si $a_1 \in \{\delta, \delta + n\}$ para $\delta \in \{0, 1\}$, entonces, como $a_{\{1,3\}} \in \{1, 1+n\}$, tenemos $a_3 \in \{1-\delta, 1-\delta+n\}$. Sea $a_1 = \delta + \epsilon n$ y $a_3 = 1 - \delta + \epsilon' n$ con $\epsilon, \epsilon' \in \{0, 1\}$. Cambiando la base a $\{f_1' = f_1 + \epsilon n f_3, f_2' = f_2 + \epsilon' n f_3, f_3\}$ y recordando que $g_{\{1,3\}} = g_1 + g_3$, tenemos

$$A = f_3^{2v}(f_3 + f_2' + f_1')^{2n-2-2v}(f_3 + f_2')f_2'(f_3 + f_1')f_1'$$

y la secuencia es de la forma dada en 6. ■

# Capítulo 4

# Conclusiones

En el estudio de las secuencias de suma cero minimal sobre un grupo abeliano finito estudiamos la Constante de Davenport y algunas constantes de suma cero relacionadas con ésta, dimos algunos ejemplos del cálculo y estimación de dichas constantes de suma cero para algunos grupos abelianos finitos, en especial para el grupo $C_2^3$. Estudiamos la estructura de las secuencias minimales de suma cero, como consecuencia resolvimos el problema inverso asociado a la constante de Davenport para los grupos cíclicos, para el grupo $C_2^3$ y para los grupos de la forma $C_2 \oplus C_2 \oplus C_{2n}$. Pese a que éste trabajo no es original se ha presentado de forma detallada y didáctica de modo que todo investigador que desee ahondar en éste tema lo pueda usar como consulta.

# Bibliografía


[1] W. R. Alford, A. Granville and C. Pomerance, There are infinitely many Carmichael numbers, *Annals of Math.*, 139 (2) , no. 3, 703–722 (1994).

[2] J. Brüdern and H. Godinho, On Artin's conjecture, II: Pairs of additive forms, *Proc. Londan Math. Soc.* 84 (3).

[3] Ch. Delorme, O. Ordaz, D. Quiroz, Some remarks on Davenport constant, *Discrete Math.* 237 (2001), 119–128.

[4] W. Gao, A. Geroldinger, and D. Grynkiewicz. Inverse zero-sum problems III. *Acta Arith.*, 2 (2010) no. 141, 103–152.

[5] W. Gao and A. Geroldinger. On products of k atoms. *Monatsh. Math.*, 2 (2009) no. 156, 141– 157.

[6] A. Geroldinger and F. Halter-Koch. Non-unique factorizations. Algebraic, Combina- torial and Analytic Theory. Chapman & Hall/CRC, (2006).

[7] A. Geroldinger and R. Schneider. On Davenport's constant. *J. Combin. Theory Ser.*, 1 (1992) no.61, 147–152.

[8] T. Hungerford, *Algebra*, Springer-Verlag, New York, 1974.

[9] F. Halter-Koch, A generalization of Davenport's constant and its arithmetical applications, *Colloq. Math.* 63 (1992), 203–210.

[10] C. Reiher. A proof of the theorem according to which every prime number possesses Property B. Preprint.

[11] K. Rogers. A combinatorial problems in abelians groups. *Proc. Cam. Phil. Soc* 59 (1963) 559–562.

[12] J. Rotman, *An Introduction to the Theory of Groups*, Springer-Verlag, $4^{th}$ ed. 1999.

[13] W. Schmid , The inverse problem associated to the Davenport constant for $C_2 \oplus C_2 \oplus C_{2n}$ and applications to the arithmetical characterization of class groups, *the electronic journal of combinatorics* 18 (2011), no.33, 1–42.