UNIVERSIDAD CENTROCCIDENTAL
"LISANDRO ALVARADO"

Decanato de Ciencias y Tecnología
Licenciatura en Ciencias Matemáticas

"Factorización de grupos abelianos Finitos"

Trabajo Especial de Grado presentado por

Br. Jessica Viscaya

como requisito final
para obtener el título de Licenciado
en Ciencias Matemáticas
Área de Conocimiento: Algebra y combinatoria.
Tutor: Prof. Luz Elimar Marchan

Barquisimeto, Venezuela. Marzo de 2015

Universidad Centroccidental
"Lisandro Alvarado"
Decanato de Ciencias y Tecnología
Licenciatura en Ciencias Matemáticas

ACTA
TRABAJO ESPECIAL DE GRADO

Los suscritos miembros del Jurado designado por el Jefe del Departamento de Matemáticas del Decanato de Ciencias y Tecnología de la Universidad Centroccidental "Lisandro Alvarado", para examinar y dictar el veredicto sobre el Trabajo Especial de Grado titulado:

"FACTORIZACIÓN DE GRUPOS ABELIANOS FINITOS"

presentado por la ciudadana BR. JESSICA VISCAYA titular de la Cédula de Identidad No. 17627631, con el propósito de cumplir con el requisito académico final para el otorgamiento del título de Licenciado en Ciencias Matemáticas.

Luego de realizada la Defensa y en los términos que imponen los Lineamientos para el Trabajo Especial de Grado de la Licenciatura en Ciencias Matemáticas, se procedió a discutirlo con el interesado habiéndose emitido el veredicto que a continuación se expresa:

[1] ____________________

Con una calificación de ____________________ puntos.

En fe de lo expuesto firmamos la presente Acta en la Ciudad de Barquisimeto a los _____ días del mes de ____________________ de __________.

TUTOR	FIRMA
PRINCIPAL	FIRMA
PRINCIPAL	FIRMA

OBSERVACIONES:

____

____

____

[1] Aprobado ó Reprobado

A Dios y a mis padres que son mis guías, mis ejemplos a seguir y la razón de todo mi esfuerzo.

Agradecimientos

Para alcanzar una gran meta como esta debe recorrerse un largo camino, camino que casi siempre esta lleno de obstáculos que pueden hacerte tropezar y caer. Si esto ocurre entonces cuando decides levantarte esperas levantar la cabeza y observar a tu alrededor a alguien con la mano extendida que te ayude hacerlo . A veces podemos ser tan afortunados como yo y contar no con una sino con muchas manos extendidas que además te acompañen a seguir el camino cuidando de que no vuelvas a caer.

Algunas de ellas se mantendrán extendidas toda la vida, la de DIOS que es el guiador de mis pasos, el creador de mi destino, a quien agradezco infinitamente cada una de las oportunidades que me dio y me da, sin el nada hubiese sido posible. La de mis amados PADRES que son mi razón de perseverancia, el motivo por el que quería lograr esto, la única opinión que me interesa, debo agradecer su paciencia, su apoyo, sus sacrificios y su amor. La de mis adorados HERMANOS DARWING Y JENE que entre consejos, regaños y bromas se que siempre han deseado lo mejor para mi y estoy muy agradecida por eso, ah lo siento hermanos pero NO HAY BASTÓN!!. La de mis queridas AMIGAS YAQUE Y HANY mi válvula de escape, mi bocanada de aire, estoy convencida de que estarán conmigo toda la vida por su apoyo, su preocupación, su paciencia y su cariño muchas gracias.

Otras sinceramente quisiera que lo estuvieran pero se que debemos tomar caminos diferentes no necesariamente separados, matemáticamente hablando, las de mis amigas MARIANGEL, LISETH Y JOSEIDY a quienes agradezco la maravillosa ocurrencia de incluirme en su grupo de estudio y haberme brindado su amistad, aprendí que tus amigos en serio pueden pensar muy distinto a ti y sin embargo no por eso dejan de ser tus amigos. Las de mis amigos y compañeros EVELYN, CELISMAR, GENESIS, MARIA FERNANDA, ILIANA, EMELY, DIANA, KARLA, DELLYS, ANA, CLEIVER, JUNIOR, JOELVIZ, RICARDO, RAFAEL, WLADIMIR, UVENCIO Y JESUS que me brindaron sus amistad, me animaron a no decaer cuando las cosas no salieron como debían, me enseñaron a ver la carrera de otra perspectiva que no solo es estudiar, estudiar, estudiar sino que cuando toca hacerlo hay que hacerlo en serio pero cuando no puedes hacer otras cosas incluso divertirte gracias son en verdad personas extraordinarias.

Unas ni siquiera alcanzas a imaginar verlas extendidas como la de mis profesores MARIO RODRIGUEZ, VICTOR CARUCI, EBNER PINEDA que son prueba de que la simpatía no tiene por que estar ligada a las risas y a las bromas, que el profesionalismo y el genio no significa ser severos, prepotentes o egocéntricos, gracias por sus enseñanzas en la carrera y en la vida misma, no olvidare nunca las palabras "no es que no te caigas, es que te levantes".

Por ultimo y no por que sea menos importante, es esa mano que si o si te toca pedir por que es necesaria para terminar este largo camino, la de mi tutora LUZ ELIMAR MARCHAN gracias por la oportunidad de trabajar a su lado, por el respeto, por el apoyo, por la dedicación espero haber estado al nivel de sus expectativas, de mi parte usted si lo estuvo.

ASÍ CUANDO ESTE CAMINO TERMINA PODEMOS DECIR CON LA MAYOR SATISFACCIÓN GRACIAS POR TODO ¡LO LOGRE!

Resumen

Sea G un grupo abeliano finito y $n > 1$ un entero. Decimos que G tiene la n-propiedad de Hajós si en toda factorización normalizada de G, como producto directo de subconjuntos, existe al menos un factor que es periódico. Decimos que G tiene la n-propiedad de Rédei si en toda factorización normalizada de G, como producto directo de subconjuntos, existe al menos un factor que no genera a G. En este trabajo se estudian algunos grupos abeliano finitos con respecto a estas dos propiedades y se establece una relación entre ellas.

ÍNDICE

Introducción

En 1907 H. Minkowski [6] planteó una conjetura geométrica muy famosa la cual fué demostrada por primera vez por el matemático húngaro G. Hajós, en 1941 [4], quien hizo una sorprendente reducción del problema geométrico, a un problema de factorización de un grupo abeliano finito en un producto directo de subconjuntos cíclicos. En teoría de grupos, la versión de la conjetura de Minkowski, es el Teorema de Hajós, el cual establece que, si un grupo abeliano finito G se factoriza como producto directo de conjuntos cíclicos, entonces al menos uno de los factores es un subgrupo de G. Se puede demostrar sin dificultad que, todo subconjunto cíclico y periódico de un grupo abeliano finito G es un subgrupo de G. Luego el Teorema de Hajós puede ser reformulado de la siguiente manera: si un grupo abeliano finito G se factoriza como producto directo de conjuntos cíclicos, entonces al menos uno de los factores debe ser periódico. Desde 1941 la consideración de una descomposición de un grupo abeliano finito como producto directo de subconjuntos, ha sido una actividad muy fructífera.

En 1965 Rédei [7] demostró que la conclusión del resultado de Hajós sigue siendo cierta, aún cuando los factores de G no sean subconjuntos cíclicos, basta que contengan al elemento identidad y tengan cardinalidad p, con p primo. En [3] Brujin da algunos ejemplos que muestran que la condición de que los factores tengan cardinalidad un número primo, no puede ser debilitada para ningún factor. De modo que dada una factorización de un grupo abeliano G no siempre se puede obtener que uno de los factores sea un subgrupo de G. Ahora, notemos que si H es un subgrupo de G, entonces para cualquier $h \in H$, $hH = H$. Esta observación dio lugar a la idea de subconjuntos periódicos de G. En este sentido la noción del Teorema de Hajós puede ser generalizada como la n-propiedad de Hajós (considerando que uno de los subconjuntos debe ser periódico en lugar de considerar que uno de los subconjuntos debe ser un subgrupo).

Sea G un grupo abeliano finito y $n > 1$ un entero. Decimos que G tiene la *n-propiedad de Hajós*, si en toda factorización normalizada de G, como producto directo de n subconjuntos de G, existe al menos un factor que es periódico. Decimos que G tiene la *n-propiedad de Rédei* si en toda factorización normalizada de G, como producto directo de n subconjuntos de G, existe al menos un factor que no genera a G.

El problema que usualmente es tratado, consiste en determinar que grupos abelianos finitos tienen las propiedades de Rédei y/o de Hajós. En [2] Amin demostró que todo p-grupo cíclico finito tiene la n-propiedad-Hajós. Entonces el problema que surge naturalmente, y que trataremos en este trabajo, es estudiar los p-grupos abelianos finitos no cíclicos con respecto a la n-propiedad-Hajós. Otro problema que trataremos es el de determinar la relación que existe entre la n-propiedad de Hajós y la n-propiedad de Rédei.

El trabajo consta de dos capítulos. En el primer capítulo damos las definiciones básicas, notación y algunos resultados que sirven como herramientas para construir factorizaciones de un grupo abeliano finito con ciertas características. En el segundo capítulo mostramos los resultados principales de este trabajo, el cual está fundamentado en [1].

CAPÍTULO 1

PRELIMINARES

En este capítulo definimos la terminología y presentamos algunas definiciones, notaciones y resultados elementales, necesarios como base teórica de este trabajo. Las demostraciones que omitimos pueden ser encontrados en cualquier texto de álgebra, entre ellos [5].

1.1. Definiciones Básicas sobre grupos abelianos finitos

Sea G un grupo abeliano, con excepción de algunos casos, consideraremos la operación binaria de G con notación multiplicativa, el cardinal de un subconjunto A de G lo denotamos por $|A|$, en particular, $|G|$ denota al orden de G y, dado $g \in G$, $|g| = |\langle g \rangle|$ denota el orden de g. Para $n \in \mathbb{N}$, denotamos por C_n a cualquier grupo cíclico de orden n (recordar que, salvo isomorfismo, sólo existe un grupo cíclico de orden n).

1.1.1. Producto de subconjuntos de un grupo abeliano

Sean A y B subconjuntos no vacíos de un grupo abeliano G, definimos el *producto (o suma, si la notación es aditiva) de A y B*, denotado por AB (o por $A + B$) como el conjunto

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

(o $A + B = \{a + b : a \in A, b \in B\}$, si la notación es aditiva)

Dado $g \in G$, escribimos gA en lugar de $\{g\}A$. Es claro que si G es abeliano, $AB = BA$. En general, el producto de más de dos subconjuntos de G, digamos $A_1, A_2, \ldots, A_k$, se define como el conjunto

$$A_1A_2\ldots A_k = \prod_{i=1}^{k} A_i = \left\{\prod_{i=1}^{k} a_i : a_i \in A_i\right\}.$$

Ejemplo 1.1. Sea $G = (\mathbb{Z}_7 \setminus \{0\}, \cdot)$, $A = \{1, 2\}$ y $B = \{3, 5\}$, entonces

$$AB = \{1 \cdot 3, 1 \cdot 5, 2 \cdot 3, 2 \cdot 5\} = \{3, 5, 6\}.$$

Sea H un subgrupo de G. Un subconjunto B de G se dice que es un *conjunto completo de representantes de clases laterales de G módulo H* si

$$G = \bigcup_{b \in B} bH$$

y si $b_1H = b_2H$ implica que $b_1 = b_2$.

Sean $A_1, A_2, \ldots, A_k$ subconjuntos de un grupo abeliano finito G. Si todo elemento $g \in A_1A_2\ldots A_k$ tiene una representación única como un producto $g = a_1a_2\ldots a_k$ con $a_i \in A_i$ para cada $1 \leq i \leq k$, decimos que $A_1A_2\ldots A_n$ es un *producto directo (o suma directa, si la notación es aditiva) de subconjuntos de G*.

Ejemplo 1.2. Siendo G, A y B como en el Ejemplo 1.1, notemos que $AB = \{3, 5, 6\}$ no es un producto directo, dado que 3 tiene dos representaciones como elemento de AB, es decir, $3 = 1 \cdot 3$ con $1 \in A$ y $3 \in B$ y $3 = 2 \cdot 5$ con $2 \in A$ y $3 \in B$.

Definición 1.1. Sean $A_1, A_2, \ldots, A_n$ subconjuntos de un grupo abeliano finito G tales que $G = A_1A_2\ldots A_n$. Si $A_1A_2\ldots A_n$ es un producto directo de subconjuntos, decimos que $G = A_1A_2\ldots A_n$ es una *factorización de G*. Si además cada subconjunto A_i contiene al elemento identidad e de G, decimos que $G = A_1A_2\ldots A_n$ es una *factorización normalizada de G*.

Ejemplo 1.3.

- Sea $G = (\mathbb{Z}_{15}, +)$, $A_1 = \{0, 5, 10\} = \langle 5 \rangle$ y $A_2 = \{0, 3, 6, 9, 12\} = \langle 3 \rangle$, en este caso la notación es aditiva, usamos la notación suma en lugar de producto. $G = A_1 + A_2$ es una factorización de G. En efecto, veamos que todo elemento g de G se escribe como $g = a_1 + a_2$ con $a_1 \in A_1$ y $a_2 \in A_2$

$$\begin{array}{lllll} 0 = 0+0 & 1 = 10+6 & 2 = 5+12 & 3 = 0+3 & 4 = 10+9 \\ 5 = 5+0 & 6 = 0+6 & 7 = 10+12 & 8 = 5+3 & 9 = 0+9 \\ 10 = 10+0 & 11 = 5+6 & 12 = 0+12 & 13 = 10+3 & 14 = 5+9 \end{array}$$

Notemos además que todo elemento de G tiene una representación única como elemento de $A_1 + A_2$. Sea $g \in G$ y supongamos que $g = a_1 + a_2$ y $g = a_1' + a_2'$ donde $a_1, a_1' \in A_1$ y $a_2, a_2' \in A_2$, entonces

$$a_1 + a_2 = a_1' + a_2' \Rightarrow a_1 - a_1' = a_2 - a_2'$$

Como A_1 y A_2 son subgrupos de G entonces $a_2 - a_2' = a_1 - a_1' \in A_1$ y $a_1 - a_1' = a_2 - a_2' \in A_2$, pero $A_1 \cap A_2 = \{0\}$, así

$$a_1 - a_1' = 0 = a_2 - a_2' \Rightarrow a_1 = a_1' \wedge a_2 = a_2'$$

De modo que g tiene una representación única como elemento de $A_1 + A_2$, en consecuencia, $G = A_1 + A_2$ es una factorización normalizada de G.

- Sea $G = C_7 =< g >$ un grupo cíclico de orden 7, sean $A_1 = \{e, g, g^4, g^5\}$ y $A_2 = \{e, g^2\}$. Es claro que $A_1A_2 = \{e, g, g^2, g^3, g^4, g^5, g^6\} = G$, además puede verse sin mucha dificultad que para $a_1, a_1' \in A_1$ y $a_2, a_2' \in A_2$ con $a_1 \neq a_1'$ y $a_2 \neq a_2'$ tenemos que $a_1a_2 \neq a_1'a_2'$, por lo que todo elemento $g \in A_1A_2$ tiene un representación única como elemento de A_1A_2, así $G = A_1A_2$ es una factorización de G.

Proposición 1.1. *Sea G un grupo abeliano finito. Si $G = A_1A_2 \ldots A_n$ es una factorización de G entonces $|G| = |A_1|\,|A_2| \ldots |A_n|$*

Demostración. Sea

$$\psi : A_1 \times A_2 \times \cdots \times A_n \longrightarrow G$$

dada por

$$\psi(a_1, a_2, \ldots, a_n) = a_1a_2 \ldots a_n$$

Veamos que ψ es una biyección. Sean $(a_1, a_2, \ldots, a_n)$ y $(a_1^{'}, a_2^{'}, \ldots, a_n^{'})$ en $A_1 \times A_2 \times \cdots \times A_n$ entonces

$$\begin{aligned} \psi(a_1, a_2, \ldots, a_n) = \psi(a_1^{'}, a_2^{'}, \ldots, a_n^{'}) &\Rightarrow a_1 a_2 \ldots a_n = a_1^{'} a_2^{'} \ldots a_n^{'} \\ &\Rightarrow a_i = a_i^{'} \qquad \forall i \in \{1, 2, \ldots n\} \\ &\Rightarrow (a_1, a_2, \ldots, a_n) = (a_1^{'}, a_2^{'}, \ldots, a_n^{'}). \end{aligned}$$

Luego ψ es inyectiva.

Ahora sea $g \in G$, como $G = A_1 A_2 \ldots A_n$, entonces

$$\begin{aligned} & g = a_1 a_2 \ldots a_n, \quad \text{con } a_i \in A_i \\ \Rightarrow\ & g = \psi(a_1, a_2, \ldots, a_n); \quad \text{con } (a_1, a_2, \ldots, a_n) \in A_1 \times A_2 \times \cdots \times A_n. \end{aligned}$$

Entonces $G \subseteq \psi(A_1 \times A_2 \times \cdots \times A_n)$, por lo que ψ es sobreyectiva.

Por tanto ψ es biyectiva y en consecuencia,

$$|G| = |A_1 \times A_2 \times \cdots \times A_n| = |A_1||A_2| \ldots |A_n|.$$

■

El teorema fundamental para grupos abelianos finitos, el cual enunciamos a continuación, garantiza que todo grupo abeliano finito G es producto directo (o suma directa) de subgrupos cíclicos de G, este hecho se denota por $G = C_{n_1} \oplus C_{n_2} \oplus \cdots \oplus C_{n_r}$, así todo grupo abeliano finito tiene una factorización normalizada.

Teorema 1.1 ([5])**.** *Si G es un grupo abeliano finito no trivial, existen enteros únicos $n_1, n_2, \ldots, n_r$ tales que*

$$G = C_{n_1} \oplus C_{n_2} \oplus \cdots \oplus C_{n_r}$$

con $1 < n_1 \mid n_2 \mid \cdots \mid n_r$.

En el teorema anterior, si $n = n_1 = n_2 = \cdots = n_r$, escribimos $G = C_n^r$, en lugar de $G = \underbrace{C_n \oplus C_n \oplus \cdots \oplus C_n}_{r \text{ veces}}$

Definición 1.2. Sea p primo. Un grupo finito G es un p-*grupo* si y solo si $|G|$ es una potencia de p.

Ejemplo 1.4.

- $G = \{e\}$ es un p-grupo para todo p primo, ya que $|\langle e \rangle| = 1 = p^0$.

- Si $G = C_p^r$, con p primo, G es un p-grupo, pues $|G| = p^r$. En este caso decimos que G es un *p-grupo elemental.*

Definición 1.3. Sea G un grupo abeliano finito, $G = C_{n_1} \oplus C_{n_2} \oplus \cdots \oplus C_{n_r}$, con $1 < n_1 \mid n_2 \mid \cdots \mid n_r$. El entero n_r es llamado *exponente de G* y es denotado por $\exp(G)$.

Observar que para todo $g \in G$, $g^{\exp(G)} = e$.

Decimos que un grupo abeliano finito G *es del tipo* $(p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots p_k^{\alpha_k})$, con p_i primo, si G es producto directo de k grupos cíclicos de órdenes $p_i^{\alpha_i}$, esto es $G = C_{p_1^{\alpha_1}} \oplus C_{p_2^{\alpha_2}} \oplus \cdots \oplus C_{p_k^{\alpha_k}}$. Por ejemplo, un grupo del tipo $(2, 2)$ es un grupo de la forma $G = C_2 \oplus C_2$.

1.1.2. Conjuntos periódicos

Definición 1.4. Sea A un subconjunto no vacío de un grupo G. Diremos que A es *periódico*, si existe $g \in G \setminus \{e\}$ tal que $gA = A$. Este elemento g es llamado *período* de A.

Observación 1.1. Observemos que si A es un subconjunto no trivial de un grupo G tal que $e \in A$ y A es periódico con período g, entonces $g = ge \in gA = A$, luego, en este caso, podemos suponer que el período de A es un elemento de A. Es decir, si $e \in A$, A es periódico si existe $g \in A$ tal que $gA = A$.

Ejemplo 1.5. Sea G un grupo. Todo subgrupo no trivial H de G es periódico, ya que para todo $h \in H$, $hH = H$ por la definición de subgrupo.

Proposición 1.2. *Si A es un subconjunto periódico de un grupo abeliano G, entonces $H = \{g \in G : gA = A\}$ es un subgrupo de G, más aún, $A = AH$.*

Demostración. Es claro que $e \in H$ ya que $eH = H$. Sea $h \in H$ entonces $hA = A$. Luego

$$\begin{aligned} h^{-1}A &= h^{-1}(hA) \\ &= (h^{-1}h)A \\ &= eA \\ &= A. \end{aligned}$$

Asi

$$h \in H \Rightarrow h^{-1} \in H.$$

Ahora, sean $h_1, h_2 \in H$ entonces $h_1 A = A$ y $h_2^{-1} A = A$, luego

$$\begin{aligned}(h_1 h_2^{-1})A &= h_1(h_2^{-1}A)\\ &= h_1 A\\ &= A\end{aligned}$$

entonces $h_1 h_2^{-1} \in H$. Por tanto H es subgrupo de G.

Más aún,

$$\begin{aligned}x \in AH &\Leftrightarrow x = ah, \text{ con } a \in A,\ h \in H\\ &\Leftrightarrow x \in Ah = hA \text{ con } h \in H\\ &\Leftrightarrow x \in A.\end{aligned}$$

Por tanto $A = AH$ ■

El siguiente teorema muestra que para un grupo abeliano finito G, siempre es posible encontrar una factorización de G siendo uno de los factores un subconjunto periódico de G.

Teorema 1.2. *Sea G un grupo abeliano finito y sea A un subconjunto periódico de G, entonces existe H subgrupo de G y C subconjunto de A, tal que A es producto directo de C y H.*

Demostración. Sea $H = \{g \in G : gA = A\}$, por Proposición 1.2, H es un subgrupo de G. Sea $AH/H = \{a_1H, a_2H, \ldots, a_sH\}$ el conjunto formado por todas las clases de equivalencia módulo H tales que $a_i \in A$ y $a_iH = a_jH$ si y solo si $i = j$. Sea $C = \{a_1, a_2, \ldots, a_s\} \subset A$, es claro que $AH = \bigcup_{i=1}^{s} a_iH$, entonces

$$\begin{aligned}A = AH &= \bigcup_{i=1}^{s} a_iH.\\ &= a_1H \cup a_2H \cup \cdots \cup a_sH\\ &= \{a_1, a_2, \cdots, a_s\}H\\ &= CH\end{aligned}$$

Por tanto, cada elemento de A se escribe como el producto ch con $c \in C$ y $h \in H$. Veamos ahora que esta representación es única.

Sea $a \in A$ y supongamos que

$$c_1 h_1 = a = c_2 h_2 \tag{1.1}$$

donde $c_1 = a_i \in C$, $c_2 = a_j \in C$ y $h_1, h_2 \in H$, entonces

$$\begin{aligned} & c_1 h_1 = c_2 h_2 \\ \Rightarrow\ & c_1 h_1 H = c_2 h_2 H \\ \Rightarrow\ & c_1 H = c_2 H \\ \Rightarrow\ & a_i H = a_j H \\ \Rightarrow\ & a_i = a_j \\ \Rightarrow\ & c_1 = c_2 \end{aligned}$$

ahora sustituyendo en la ecuación (1.1) se tiene que

$$\begin{aligned} & c_1 h_1 = c_1 h_2 \\ \Rightarrow\ & h_1 = h_2 \end{aligned}$$

Por lo tanto, A es producto directo de C y H.

En particular, si tomamos $A = G$ en el enunciado, entonces existe H subgrupo de G y C subconjunto de G, tal que G es producto directo de C y H, como H es subgrupo de G, H es periódico, lo que implica que G tiene una factorización con un factor periódico. ■

Sea A un subconjunto de un grupo abeliano finito G, decimos que A *es cíclico* si $A = \{e, a, a^2, \ldots, a^k\}$, para algún $a \in G$ con $k \leq |a| - 1$, observemos que si $k = |a| - 1$, $A = \langle a \rangle$.

Lema 1.1. *Todo subconjunto cíclico y periódico de un grupo abeliano finito G es un subgrupo de G*

Demostración. Sea A subconjunto cíclico de G, esto es, $A = \{e, a, a^2, \ldots, a^k\}$, para algún $a \in G$ con $k \leq |a| - 1$, es claro que $a^i \neq a^j$ para $i \neq j$ siempre que $0 \leq i, j \leq k$. Si A es periódico, existe $g \in G \setminus \{e\}$ tal que $gA = A$, podemos suponer que $g = a^t$ con $1 \leq t \leq k$, notemos que $1 \leq k - t + 1 \leq k$. Ahora

$$\begin{aligned} a^{k+1} &= a^t a^{k-t+1} \text{ con } 1 \leq k-t+1 \leq k \\ &= g a^{k-t+1} \text{ con } 1 \leq k-t+1 \leq k \\ \Rightarrow a^{k+1} &\in gA = A. \end{aligned}$$

Luego $a^{k+1} = e$ o $a^{k+1} = a^r$ con $1 \leq r \leq k$. Si $a^{k+1} = e$, entonces $|a| = k+1$ ($k+1$ sería el menor entero positivo tal que $a^{k+1} = e$), implicando que $k = |a|-1$ y en consecuencia, $A = \langle a \rangle$. Si $a^{k+1} = a^r$ con $1 \leq r \leq k$ entonces, $a^k = a^{r-1}$ con $0 \leq r-1 \leq k-1$, lo cual contradice nuestra suposición. ■

1.2. Caracteres y aniquiladores de grupos

En esta sección probamos algunas propiedades de los caracteres de un grupo abeliano fnito G. El propósito es usar los caracteres como una herramienta para que dados A y B subconjuntos de un grupo abeliano finito G, $G = AB$ sea una factorización de G.

Definición 1.5. Una función $\chi : (G, \cdot) \longrightarrow (\mathbb{C} \setminus \{0\}, \cdot)$, donde $(G, \cdot)$ es un grupo abeliano y $(\mathbb{C} \setminus \{0\}, \cdot)$ es el conjunto de los números complejos no nulos, es llamada un *caracter* de G si

$$\chi(gh) = \chi(g)\chi(h), \text{ para todo } g,\, h \in G.$$

esto es, χ es un caracter del grupo G si χ es un homomorfismo de grupos.

Ejemplo 1.6. Consideremos la función $\chi : (G, \cdot) \longrightarrow (\mathbb{C} \setminus \{0\}, \cdot)$ dada por:

$$\chi(g) = 1 \text{ para todo } g \in G,$$

entonces $\chi(gh) = 1 = (1)(1) = \chi(g)\chi(h)$, así χ es un caracter, tal caracter es llamado *caracter principal de G.*

Sea G un grupo abeliano, denotamos por G^* al conjunto de todos los caracteres de G. Observemos que G^* tiene estructura de grupo abeliano bajo la multiplicación, para ver esto, notemos que el caracter principal de G es el elemento neutro de G^*, y para $\chi \in G^*$, la función $\chi' : G \to \mathbb{C} \setminus \{0\}$, dada por $\chi(g) = [\chi(g)]^{-1}$, es un caracter de G tal que $\chi\chi'$ es el caracter principal de G.

Es conocido que para un grupo abeliano finito G, el conjunto de funciones $\phi : G \to \mathbb{C}$ es un espacio vectorial $|G|$-dimensional con producto interno dado por

$$\langle \phi_1, \phi_2 \rangle = \frac{1}{|G|} \sum_{g \in G} \phi_1(g)\overline{\phi_2(g)}.$$

En general, el contexto nos impide confundir la notación de producto interno con la notación de subgrupo generado por ciertos elementos, en todo caso aclararemos cuando hablamos del producto interno.

Lema 1.2. *Si χ es un caracter de un grupo finito G, entonces $|\chi(g)| = 1$ para todo $g \in G$, más aún, $\chi(G) \subset \mu_n$ donde n es el exponente de G y μ_n es el grupo de las n-raices de la unidad en $\mathbb{C}$.*

Demostración. Como n es el exponente de G, si $g \in G$ entonces $g^n = 1$, así $\chi(g)^n = 1$ implicando que $\chi(g) \in \mu_n$ y $|\chi(g)| = 1$. ■

Lema 1.3. *Si G es un grupo abeliano finito y χ , $\theta \in G^*$, entonces*

$$\langle \chi, \theta \rangle = \begin{cases} 1 & si\ \chi = \theta \\ 0 & en\ otro\ caso \end{cases}$$

donde $\langle \chi, \theta \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\theta(g)}$, *denota el producto interno de χ y θ.*

Demostración. Por Lema 1.2, $|\theta(g)| = 1$, así $\overline{\theta(g)} = \theta(g)^{-1}$ para todo $g \in G$. Ahora

Si $\chi = \theta$ entonces

$$\langle \chi, \theta \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\theta(g)} = \frac{1}{|G|} \sum_{g \in G} \chi(g)\theta(g)^{-1} = \frac{1}{|G|} \sum_{g \in G} \chi(g)\chi(g)^{-1} = \frac{1}{|G|} \sum_{g \in G} 1 = 1$$

por otra parte si $\chi \neq \theta$ entonces $\chi(x) \neq \theta(x)$ para algún $x \in G$

$$\langle \chi, \theta \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\theta(g)} = \frac{1}{|G|} \sum_{g \in G} \chi(g)\theta(g)^{-1}$$

Dado que $xG = G$, podemos sustituir g por xg y tenemos

$$\begin{aligned} \langle \chi, \theta \rangle &= \frac{1}{|G|} \sum_{g \in G} \chi(xg)\theta(xg)^{-1} \\ &= \frac{1}{|G|} \sum_{g \in G} \chi(x)\chi(g)\theta(x)^{-1}\theta(g)^{-1} \\ &= \chi(x)\theta(x)^{-1} \frac{1}{|G|} \sum_{g \in G} \chi(g)\theta(g)^{-1} \\ &= \chi(x)\theta(x)^{-1} \langle \chi, \theta \rangle \end{aligned}$$

Por tanto $\langle \chi, \theta \rangle = 0$. ■

El Lema 1.3 muestra que los caracteres de un grupo abeliano finito G son ortonormales.

Corolario 1.1. *Si G es un grupo abeliano finito entonces $|G^*| \leq |G|$.*

Demostración. Para un grupo finito G el conjunto de las funciones $f : G \longrightarrow \mathbb{C}$ es un espacio vectorial de dimensión $|G|$. Además por el Lema 1.3 los caracteres son ortonormales y por tanto son linealmente independientes, de este modo, $|G^*| \leq |G|$. ■

Lema 1.4. *Si G es un grupo abeliano finito, H un subgrupo propio de G y $\chi \in H^*$, entonces χ puede ser extendido a un subgrupo K de G que contiene propiamente a H.*

Demostración. Queremos encontrar un subgrupo K de G que contenga propiamente a H y un caracter $\tilde{\chi}$ de K tal que $\tilde{\chi}(h) = \chi(h)$ cuando $h \in H$. Sea $x \in G \setminus H$, existe un menor entero positivo d que cumple $x^d \in H$ (notar que $x^{|x|} = e \in H$). Supongamos que $x^n \in H$, por el algoritmo de la división, $n = dq + r$ con $q, r \in \mathbb{Z}$ y $0 \leq r < d$, luego $x^n = x^{dq+r} = (x^d)^q x^r$, como $x^r, (x^d)^q \in H$, $x^r = x^n (x^d)^{-q} \in H$ y la minimalidad de d implica que $r = 0$, asi n debe ser un múltiplo de d, de modo que $x^n \in H$ si y solo si n es múltiplo de d. Ahora sea $a \in \mathbb{C}$ una raíz d-ésima de $\chi(x^d)$, es decir,

$$a^d = \chi(x^d)$$

Sea $K = \langle H, x \rangle$ el subgrupo de elementos de G que pueden ser escritos de la forma $x^n h$ para algún $h \in H$, es claro que K contiene propiamente a H. Definamos $\tilde{\chi} : K \to \mathbb{C}$ por

$$\tilde{\chi}(x^n h) = a^n \chi(h)$$

Veamos que $\tilde{\chi}$ esta bien definida. Sea $x^n h, x^m h' \in K$ con n, m múltiplos de d si $x^n h = x^m h'$ entonces $h'h^{-1} = x^{n-m}$, donde $n - m$ es múltiplo de d, esto es, $n - m = dk$. Así,

$$\begin{aligned}
\chi(h')\chi(h)^{-1} &= \chi(h')\chi(h^{-1}) \\
&= \chi(h'h^{-1}) \\
&= \chi(x^{n-m}) \\
&= \chi(x^{dk}) \\
&= \chi(x^d)^k \\
&= (a^d)^k \\
&= a^{dk} \\
&= a^{n-m}
\end{aligned}$$

Lo que implica que $a^n \chi(h) = a^m \chi(h')$ por lo tanto,

$$\tilde{\chi}(x^n h) = \tilde{\chi}(x^m h')$$

Solo resta probar que $\tilde{\chi}$ es homomorfismo.

$$\begin{aligned}
\tilde{\chi}((x^n h)(x^m h')) &= \tilde{\chi}(x^{n+m}(hh')) \\
&= a^{n+m}\chi(hh') \\
&= a^n a^m \chi(h)\chi(h') \\
&= a^n \chi(h) a^m \chi(h') \\
&= \tilde{\chi}(x^n h)\tilde{\chi}(x^m h')
\end{aligned}$$

De esta manera hemos demostrado que $\tilde{\chi}$ extiende χ a K ∎

Proposición 1.3. *Sea G un grupo abeliano finito y sea H un subgrupo de G. Sea χ un caracter de H entonces χ puede extenderse a un caracter de G.*

Demostración. Si $H = G$ no hay nada que demostrar, supongamos que G contiene propiamente a H. Sea Σ el conjunto de los subgrupos K de G tal que $K \supsetneq H$ y χ puede ser extendido a K. Por Lema 1.4, Σ es no-vacío.

Sea K un elemento maximal de Σ, entonces existe $\tilde{\chi}$ extensión de χ a K con $H \subseteq K$. Supongamos que K es un subgrupo propio de G, como K es maximal, χ no puede ser extendido a un subgrupo que contenga propiamente a K, pero el Lema 1.4 garantiza que $\tilde{\chi}$ puede ser extendido a un subgrupo que contenga propiamente a K y toda extensión de $\tilde{\chi}$ es extensión de χ, contradiciendo la maximalidad de K. Por tanto $K = G$. ∎

Proposición 1.4. *Sea G un grupo abeliano finito y sea $x, y \in G$. Si $\chi(x) = \chi(y)$ para todo $\chi \in G^*$ entonces $x = y$*

Demostración. Sea $z = xy^{-1}$ con $|z| = n$. Sea $\chi : \langle z \rangle \to \mathbb{C} \setminus \{0\}$ dada por dada por

$$\chi(z^k) = e^{2\pi i \frac{k}{n}}$$

$\chi(z^k z^l) = e^{2\pi i \frac{k+l}{n}} = e^{2\pi i \frac{k}{n}} e^{2\pi i \frac{l}{n}} = \chi(z^k)\chi(z^l)$, así χ es un caracter de $\langle z \rangle$. Observemos que si $\chi(z) = 1$, entonces $\chi(z) = e^{2\pi i \frac{1}{n}} = \cos(\frac{2\pi}{n}) + i \sin(\frac{2\pi}{n}) = 1$, implicando que $\frac{2\pi}{n} = 2k\pi$ para algún $k \in \mathbb{Z}$, luego $1 = n = |z|$, asi $z = e$. Supongamos que $z \neq e$ entonces $\chi(z) \neq 1$. Por Proposición 1.3, podemos extender χ a un caracter $\widetilde{\chi} \in G^*$ tal que $\widetilde{\chi}(z) = \chi(z) \neq 1$, entonces

$$\begin{aligned} & 1 \neq \widetilde{\chi}(z) = \widetilde{\chi}(xy^{-1}) \\ \Rightarrow \quad & 1 \neq \widetilde{\chi}(x)\widetilde{\chi}(y^{-1}) \\ \Rightarrow \quad & 1 \neq \widetilde{\chi}(x)\widetilde{\chi}(y)^{-1} \\ \Rightarrow \quad & \widetilde{\chi}(y) \neq \widetilde{\chi}(x) \end{aligned}$$

lo cual contradice la hipótesis de que $\chi(x) = \chi(y)$ para todo $\chi \in G^*$, Así, $xy^{-1} = z = e$, es decir, $x = y$ ∎

Definición 1.6. Sea G un grupo abeliano finito, para todo subconjunto A de G se define $\chi(A)$ como sigue

$$\chi(A) = \sum_{a\in A} \chi(a).$$

Si $A = \emptyset$ entonces $\chi(A)$ es 0.

Ejemplo 1.7. Sea G un grupo abeliano finito y sea χ un caracter no principal de G, entonces $\chi(G) = 0$.

En efecto, sea $y \in G$ tal que $\chi(y) \neq 1$. Dado que $yG = G$, tenemos

$$\begin{aligned} &\chi(y)\sum_{x\in G}\chi(x) = \sum_{x\in G}\chi(y)\chi(x) = \sum_{x\in G}\chi(xy) = \sum_{x\in G}\chi(x) \\ \Rightarrow\quad &(\chi(y)-1)\sum_{x\in G}\chi(x) = 0, \end{aligned}$$

como $\chi(y) \neq 1$ tenemos

$$\chi(G) = \sum_{x\in G}\chi(x) = 0$$

Teorema 1.3. *Si G es un grupo abeliano finito, entonces $|G^*| = |G|$.*

Demostración. Sabemos que todo grupo abeliano finito G es isomorfo a un producto directo de grupos cíclicos, podemos suponer que

$$G \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_r}. \tag{1.2}$$

Probaremos que el grupo cíclico $\mathbb{Z}_n$ tiene n caracteres y que si G_1 y G_2 son subgrupos de un grupo abeliano G con $|G_1|$ y $|G_2|$ caracteres, respectivamente, tales que $G = G_1 \oplus G_2$ entonces su producto $G = G_1 \oplus G_2$ tiene $|G_1|\,|G_2|$ caracteres, luego por inducción obtenemos el teorema.

Para probar la primera parte, para cada $t \in \{1, \ldots, n-1\}$ consideremos la función $\chi_t : \mathbb{Z}_n \longrightarrow \mathbb{C}$ dada por

$$\chi_t(\bar{x}) = e^{2\pi i t \frac{x}{n}}$$

Para cada $t \in \{1, \ldots, n-1\}$, χ_t está bien definida, en efecto, supongamos que $\overline{x} = \overline{y}$, entonces $x = y + nk$ con $k \in \mathbb{Z}$, luego

$$\begin{aligned}
\chi_t(\overline{x}) = e^{2\pi it\frac{x}{n}} &= e^{2\pi it\frac{y+nk}{n}} \\
&= e^{2\pi it\frac{y}{n}} e^{2\pi itk} \\
&= e^{2\pi it\frac{y}{n}} (\cos(2\pi tk) + i\sin(2\pi tk)) \\
&= e^{2\pi it\frac{y}{n}} \\
&= \chi_t(\overline{y}).
\end{aligned}$$

Ahora veamos que para cada $t \in \{1, \ldots, n-1\}$, χ_t es un caracter de $\mathbb{Z}_n$.

Sean $\bar{x}$ y $\bar{y} \in \mathbb{Z}/n\mathbb{Z}$ entonces

$$\begin{aligned}
\chi_t(\bar{x} + \bar{y}) &= e^{2\pi it\frac{x+y}{n}} \\
&= e^{(2\pi it\frac{x}{n} + 2\pi it\frac{y}{n})} \\
&= e^{2\pi it\frac{x}{n}} e^{2\pi it\frac{y}{n}} \\
&= \chi_t(\bar{x})\chi_t(\bar{y}).
\end{aligned}$$

Así, χ_t es un caracter de $\mathbb{Z}_n$. Ahora supongamos que para algún par de elementos $t_1, t_2 \in \{1, \ldots, n-1\}$ con $t_2 \leq t_1$ se tiene que

$$\begin{aligned}
& \chi_{t_1}(\bar{1}) = \chi_{t_2}(\bar{1}) \\
\Rightarrow\ & e^{2\pi i\frac{t_1}{n}} = e^{2\pi i\frac{t_2}{n}} \\
\Rightarrow\ & e^{2\pi i\frac{t_1-t_2}{n}} = 1 \\
\Rightarrow\ & \cos(2\pi\frac{t_1-t_2}{n}) + i\sin(2\pi i\frac{t_1-t_2}{n}) = 1 \\
\Rightarrow\ & 2\pi\frac{t_1-t_2}{n} = 2k\pi,\ \text{con } k \in \mathbb{Z} \\
\Rightarrow\ & t_1 - t_2 = kn,\ \text{con } k \in \mathbb{N} \text{ (pues } t_1 - t_2 \geq 0) \\
\Rightarrow\ & t_1 = t_2 (\text{pues }\ t_1 - t_2 < n).
\end{aligned}$$

Luego $\chi_t(\bar{1})$ es diferente para diferentes valores de t. Así, $\mathbb{Z}_n$ tiene al menos n caracteres distintos, pero por Corolario 1.1 $\mathbb{Z}_n$ tiene a lo mas n caracteres distintos. En consecuencia, $\mathbb{Z}_n$ tiene exactamente n caracteres.

Ahora notemos que si χ_1 es un caracter de G_1 y χ_2 es un caracter de G_2, entonces $\chi : G_1 \oplus G_2 \to \mathbb{C}$ dada por

$$\chi(xy) = \chi_1(x)\chi_2(y)$$

es caracter de $G_1 \oplus G_2$. En efecto,

$$\begin{aligned}
\chi[(xy)(x'y')] &= \chi[(xx')(yy')] \\
&= \chi_1(xx')\chi_2(yy') \\
&= \chi_1(x)\chi_1(x')\chi_2(y)\chi_2(y') \\
&= \chi_1(x)\chi_2(y)\chi_1(x')\chi_2(y') \\
&= \chi(xy)\chi(x'y').
\end{aligned}$$

Finalmente sean χ_1, χ_1' caracteres de G_1 y χ_2, χ_2' caracteres de G_2 tales que los pares caracteres (χ_1, χ_2) y (χ_1', χ_2') son distintos, entonces las funciones $\chi, \chi' : G_1 \oplus G_2 \longrightarrow \mathbb{C}$ dadas por $\chi(xy) = \chi_1(x)\chi_2(y)$ y $\chi'(xy) = \chi_1'(x)\chi_2'(y)$ son dos caracteres distintos de $G_1 \oplus G_2$ ya que existe $a \in G_1$ tal que $\chi_1(a) \neq \chi_1'(a)$ implicando que $\chi(ae) \neq \chi'(ae)$ o existe un $b \in G_2$ tal que $\chi_2(b) \neq \chi_2'(b)$ implicando que $\chi(eb) \neq \chi'(eb)$. Entonces $G_1 \oplus G_2$ tiene al menos $|G_1|\,|G_2|$ caracteres distintos pero por Corolario 1.1 podemos concluir que son exactamente $|G_1|\,|G_2|$.

Por lo tanto, $G \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_r}$ tiene exactamente $n_1 n_2 \ldots n_k = n$ caracteres. ■

Definición 1.7. Sea G un grupo finito abeliano y sea A un subconjunto de G. Llamaremos *conjunto aniquilador de* A, o *aniquilador* de A, al conjunto de todos los caracteres χ de G tal que $\chi(A) = 0$ y lo denotaremos por $Ann(A)$, esto es,

$$Ann(A) = \{\chi \in G / \chi(A) = 0\}$$

Observación 1.2. Si A y B son subconjuntos de un grupo abeliano finito G y si $\chi(A) = \chi(B)$ para cada caracter de G entonces $A = B$.

Demostración. Sea $G = \{g_1, g_2, \cdots, g_n\}$ y sean $\chi_1, \chi_2, \ldots, \chi_n$ todos los caracteres de G. La relación $\chi(A) - \chi(B) = 0$ corresponde al sistema de ecuaciones

$$\begin{cases}
(x_1 - y_1)\chi_1(g_1) & + \cdots + & (x_n - y_n)\chi_1(g_n) = 0 \\
\vdots & \ddots & \vdots \\
(x_1 - y_1)\chi_n(g_1) & + \cdots + & (x_n - y_n)\chi_n(g_n) = 0
\end{cases}$$

donde,

$$x_i = \begin{cases} 1, & \text{si} \quad g_i \in A, \\ 0, & \text{si} \quad g_i \notin A, \end{cases} \qquad y_i = \begin{cases} 1, & \text{si} \quad g_i \in B, \\ 0, & \text{si} \quad g_i \notin B. \end{cases}$$

Ahora, los caracteres son ortogonales por lo que la matriz $(\chi_i(g_i))_{n\times n}$ es ortogonal, así el sistema de ecuaciones anterior tiene solo solución trivial $x_i - y_i = 0$, esto es, $x_i = y_i$ para todo i y podemos concluir que $A = B$ ■

Teorema 1.4. *Si A y B son subconjuntos de un grupo abeliano finito G, $|G| = |A||B|$ y cada caracter no-principal de G esta en $Ann(A)$ o en $Ann(B)$ entonces $G = AB$ es una factorización de G.*

Demostración. Sea $\chi \in G^*$

- Caso 1. χ es trivial

  $$\chi(C) = \sum_{c\in C} \chi(c) = \sum_{c\in C} 1 \quad = \quad |C| \tag{1.3}$$

  para todo subconjunto C de G

  Ahora,

  $$\begin{aligned} \chi(G) &= |G| \quad ; \text{por la ecuación } 1.3 \\ &= |A||B| \quad ; \text{por hipótesis} \\ &= \chi(A)\chi(B); \text{por la ecuación } 1.3 \\ &= \chi(AB) \quad ; \text{def. de carácter} \end{aligned}$$

  Por tanto, $\chi(G) = \chi(AB)$

- Caso 2. χ es un caracter no principal de G. Entonces

  $$\begin{aligned} \chi(G) &= 0 \quad ; \text{por Ejemplo } 1.7 \\ &= \chi(A)\chi(B) \quad ; \text{ya que} \quad \chi(A) = 0 \quad \text{o} \quad \chi(B) = 0 \quad ; \text{por hipótesis} \\ &= \chi(AB) \quad ; \text{def. de caracter} \end{aligned}$$

  Como χ es arbitrario entonces

$$\chi(G) = \chi(AB) \text{ para todo } \chi \in G^*$$

Luego, por la Observación 1.2

$$G = AB$$

■

CAPÍTULO 2

PROPIEDADES DE HAJÓS Y DE RÉDEI

Sea G un grupo abeliano finito. Si $a_1, a_2, ..., a_n$ son elementos de G y $r_1, r_2, ..., r_n$ son enteros positivos tal que cada elemento de G es expresado de forma única como $a_1^{x_1}, a_2^{x_2}, ..., a_n^{x_n}$, donde $0 \leq x_i \leq r_n - 1$ entonces $a_i^{r_i} = e$ para algún $i, 1 \leq i \leq n$.

Sea G un grupo abeliano finito y sean $A_1, A_2, ...A_i, ..., A_n$ subconjuntos de G, cada uno conteniendo el elemento identidad e de G. Si $G = A_1A_2...A_i...A_n$ es una factorización de G y cada uno de los A_i es cíclico entonces al menos uno de los subconjuntos A_i es un subgrupo de G.

Estas son dos versiones del teorema de Hajós, teorema que no es mas que una transformación de una famosa conjetura de H. minkowski a un problema de grupos abelianos finito hecha por Gyorgy Hajós para así resolverla. Luego Lazlo Rédei prueba el siguiente teorema, el cual puede ser considerado como una generalización de la segunda versión del teorema de Hajós.

Teorema 2.1. *[7] Sea G un grupo abeliano finito y sean $A_1, ..., A_i, ..., A_n$ subconjuntos de G cada uno conteniendo el elemento identidad e de G tal que $G = A_1...A_i...A_n$ es una factorización de G y cada A_i tiene un número primo de elementos, entonces al menos unos de los subconjuntos A_i es un subgrupo de G.*

El siguiente ejemplo muestra que no siempre a partir de una factorización podemos obtener que uno de los factores es un subgrupo.

Ejemplo 2.1. Sea $G = \langle g \rangle$ un grupo cíclico de orden 8 con generador $g \in G$ y escojamos $A = \{e, g, g^4, g^5\}$ y $B = \{e, g^2\}$. Entonces $G = AB$ es una factorización de G, dado que

$$\begin{aligned}
e &= ee \\
g &= ge \\
g^2 &= eg^2 \\
g^3 &= gg^2 \\
g^4 &= g^4e \\
g^5 &= g^5e \\
g^6 &= g^4g^2 \\
g^7 &= g^5g^2
\end{aligned}$$

Además, es evidente que ni A ni B son subgrupos de G pues $(g^2)^{-1} = g^6 \notin B$ y $(g^5)^{-1} = g^3 \notin A$.

2.1. Grupos de Hajós

Definición 2.1. Un grupo G para el cual de cualquier factorización normalizada $G = AB$ de G se tiene que A o B es periódico, se denomina *grupo de Hajós*. Los grupos de Hajós son llamados también grupos *"buenos"* y a los grupos que no son grupos de Hajós, grupos *"malos"*. Otra manera de llamar a un grupo de Hajós es diciendo que el grupo posee o tiene la *propiedad de Hajós*.

La clasificación de grupos abelianos finitos, que son grupos de Hajós, fué hecha por Sands y De Bruijn. La lista de estos grupos es la siguiente:

$$\begin{gathered}
(p^\alpha, q), (p^2, q^2), (p^2, q, r), (p, q, r, s) \\
(p^3, 2, 2), (p^2, 2, 2, 2), (p, 2^2, 2), (p, 2, 2, 2) \\
(p, q, 2, 2), (p, 3, 3), (3^2, 3), (2^\alpha, 2) \\
(2^2, 2^2), (p, p)
\end{gathered}$$

Donde p, q, r y s son primos distintos y $\alpha \geq 1$ es un entero. En consecuencia, cualquier grupo cíclico de orden n es un grupo de Hajós, si n es de la forma $p^\alpha, p^\alpha q, p^\alpha qr,$ $pqrs$, donde p, q, r y s son primos distintos y $\alpha \geq 1$ es un entero. La propiedad de Hajós se puede generalizar como sigue.

Definición 2.2. Sea G un grupo abeliano finito. Si para cada factorización normalizada $G = A_1...A_i...A_n$ de G se tiene que al menos uno de los A_i es periódico, entonces decimos que G tiene la *n-propiedad de Hajós* o G es *n-bueno.*

En [2] Amin mostró que todo grupo cíclico de orden p^α con p primo, tiene la n-propiedad de Hajós. Estudiaremos algunos p-grupos no cíclicos con respecto a la n-propiedad de Hajós y daremos algunos ejemplos de grupos que no poseen la n-propiedad de Hajós.

Lema 2.1. *Sea G un grupo abeliano finito tal que G no es un 2-grupo elemental. Sea H subgrupo no-trivial de G tal que $[G : H] = p$, p primo, entonces existe $B \subset G$, con $e \in B$ conjunto completo de representantes de clases laterales de G módulo H, tal que B no es periódico.*

Demostración. Sean G y H grupos abelianos finitos satisfaciendo las hipótesis, y supongamos que todo conjunto completo B, de representantes de clases laterales de G módulo H, es periódico. Como $|G/H| = p$ con p primo, G/H es un grupo cíclico, así podemos suponer que $G/H = \{H, bH, b^2H, \cdots, b^{p-1}H\}$ para algún $b \in G$. Sea $B = \{e, b, \cdots, b^{p-1}\}$, entonces B debe ser periódico, el Lema 1.1 implica que $B = \langle b \rangle$ y $|b| = p$.

Supongamos que $p \geq 3$. Sea $h \in H \setminus \{e\}$, consideremos el conjunto

$$B' = \{e, b, b^2, \cdots, b^{p-2}, hb^{p-1}\},$$

es claro que B' es un conjunto completo de representantes de clases laterales de G módulo H, así B' debe ser periódico, es decir, existe $g \in B' \setminus \{e\}$ tal que $gB' = B'$.

Si $g = b^r$ con $1 \leq r \leq p-2$ entonces

$$\begin{aligned} b^{p-1} &= b^r b^{p-r-1} \\ &= gb^{p-r-1} \quad (1 \leq p-(r+1) \leq p-2) \\ &\in B' \end{aligned}$$

Pero $b^{p-1} \notin B'$ por lo que $g = hb^{p-1}$, en consecuencia

$$h = hb^p = (hb^{p-1})b = gb \in B' \tag{2.1}$$

pero $h \notin B'$ obteniendo una contradicción.

Supongamos ahora que $p = 2$ y supongamos que existe $h \in H$ tal que $|h| > 2$, consideremos el conjunto $B' = \{e, hb\}$, es claro que B' es un conjunto completo de representantes de clases laterales de G módulo H, por lo que debe ser periódico, luego $hbB' = B'$ así $h^2 = h^2b^2 = (hb)(hb) \in (hb)B' = B'$, como $|h| \geq 3$ entonces $(hb)^2 = h^2 = hb$ implicando $hb = e$ lo cual es una contradicción.

Finalmente, si todo elemento de $H \setminus \{e\}$ tiene orden 2, entonces dado $g \in G = H \cup bH$, se tiene que $g = h \in H$ o $g = bh$ con $h \in H$, asi g debe tener orden 2, como g es arbitrario, todo elemento de G tiene orden 2, por el Teorema 1.1, G es un 2-grupo elemental lo que contradice nuestra hipótesis. Por lo tanto debe existir B conjunto completo de representantes de clases laterales de G módulo H, tal que B no es periódico. ■

Lema 2.2. *Sea G un grupo abeliano finito tal que G no es un 2-grupo elemental y sea H subgrupo de G tal que $|\frac{G}{H}| = p$, para algún numero primo p. Si H no tiene la n-propiedad de Hajós entonces G tampoco tiene la n-propiedad de Hajós.*

Demostración. Dado que H no tiene la n- propiedad de Hajós, podemos considerar $H = A_1A_2 \cdots A_i \cdots A_n$ una factorización de H en la cual ninguno de los A_i es periódico. Como $|G/H| = p$ entonces, por Lema 2.1, existe un conjunto completo $B = \{b_1, b_2, \cdots, b_p\}$ de representantes de clases laterales de G módulo H, el cual no es periódico. Ahora

$$\begin{aligned} G &= (b_1H) \cup (b_2H) \cup \cdots \cup (b_pH) \\ &= \{b_1, b_2, \cdots, b_p\}H \\ &= BH. \end{aligned}$$

Sea $D = BA_1$ entonces

$$\begin{aligned} DA_2 \cdots A_i \cdots A_n &= [BA_1]A_2 \cdots A_i \cdots A_n \\ &= B(A_1A_2 \cdots A_i \cdots A_n) \\ &= BH \\ &= G \end{aligned}$$

Ahora que sea $g \in G$, supongamos que $g = da_2 \cdots a_i \cdots a_n$ y $g = d'a'_2 \cdots a'_i \cdots a'_n$ con $d, d' \in D$ y $a_i, a'_i \in A_i$. Entonces

$$
\begin{aligned}
& da_2 \cdots a_i \cdots a_n = d'a'_2 \cdots a'_i \cdots a'_n \\
\Rightarrow\ & (ba_1)a_2 \cdots a_i \cdots a_n = (b'a'_1)a'_2 \cdots a'_i \cdots a'_n \\
\Rightarrow\ & (ba_1)a_2 \cdots a_i \cdots a_n H = (b'a'_1)a'_2 \cdots a'_i \cdots a'_n H \\
\Rightarrow\ & b(a_1a_2 \cdots a_i \cdots a_n)H = b'(a'_1a'_2 \cdots a'_i \cdots a'_n)H \\
\Rightarrow\ & bH = b'H \\
\Rightarrow\ & b = b' \quad ; \quad b, b' \in B \\
\Rightarrow\ & b(a_1a_2 \cdots a_i \cdots a_n) = b(a'_1a'_2 \cdots a'_i \cdots a'_n) \\
\Rightarrow\ & a_1a_2 \cdots a_i \cdots a_n = a'_1a'_2 \cdots a'_i \cdots a'_n \\
\Rightarrow\ & a_i = a'_i \forall i \in \{1, \ldots, n\} \quad ; \text{ ya que } \ H = A_1A_2 \cdots A_i \cdots A_n \ \text{ una factorizacion de } \ H
\end{aligned}
$$

Por lo tanto la representación es única y como g es arbitrario, $G = DA_2 \cdots A_i \cdots A_n$ es una factorización de G.

Sabemos que los conjuntos $A_2, \cdots, A_i, \cdots, A_n$ no son periódicos, mostraremos entonces que $D = BA_1$ es no periódico, de esta manera estaremos probando que G no tiene la n-propiedad de Hajós.

Supongamos que D es periódico, esto es, existe $g = b_j a \neq e$ con $b_j \in B$ y $a \in A_1$ tal que $g(D) = D$. Ahora sea $b_k \in B$ como

$$ gb_kA_1 \subseteq g(D) = D \tag{2.2} $$

y $gb_kA_1 \subseteq gb_kH = b'H$, con $b' \in B$ entonces

$$ gb_kA_1 \subset (D \cap b'H) \tag{2.3} $$

Es claro que $b'A_1 \subset b'H$ y $b'A_1 \subset BA_1 = D$ entonces así

$$ b'A_1 \subset (D \cap b'H). $$

Además $x \in D = BA_1 \cap (b'H)$ entonces

$$
\begin{aligned}
& x \in b_mA_1 \wedge x \in b'H \quad ; \quad \text{para algún } \ b_m \in B \\
\Rightarrow\ & x \in b_mH \wedge x \in b'H \\
\Rightarrow\ & b_m = b' \quad ; \text{pues } \ b_m, b' \in B \\
\Rightarrow\ & x \in b'A_1 \quad ; \text{pues } \ x \in b_mA_1
\end{aligned}
$$

De modo que

$$D \cap b'H \subset b'A_1$$

y en consecuencia

$$D \cap b'H = b'A_1 \tag{2.4}$$

Luego, de las ecuaciones 2.3 y 2.4, se obtiene que

$$gb_kA_1 \subset b'A_1 \tag{2.5}$$

Por otro lado de la ecuación 2.4 tenemos que $b'A_1 = D \cap b'H = gD \cap gb_kH$ de manera que

$$\begin{aligned}
x \in b'A_1 &\Rightarrow x \in gD \wedge x \in gb_kH \\
&\Rightarrow x \in gbA_1 \wedge x \in gb_kH \quad ; \quad b \in B \\
&\Rightarrow x \in gbH \wedge x \in gb_kH \\
&\Rightarrow gbH = gb_kH \\
&\Rightarrow bH = b_kH \\
&\Rightarrow b = b_k \quad ;\text{pues } \ b, b_k \in B \\
&\Rightarrow x \in gb_kA_1 \quad ;\text{pues } \ x \in gbA_1
\end{aligned}$$

por lo tanto $b'A_1 \subset gb_kA_1$ y por la ecuación 2.5 tenemos que

$$gb_kA_1 = b'A_1.$$

Si $gb_k = b'$ entonces $gb_kb' \neq e$ y $gb_k(b')^{-1}A_1 = A_1$ implicando que A_1 es periódico, contradiciendo nuestra suposición. Por tanto

$$gb_k = b'.$$

Como $b_k \in B$ es arbitrario, $gB \subset B$. Ahora

$$B = g^{|g|}B = g(g^{|g|-1}B) \subset gB. \tag{2.6}$$

Así, $gB = B$ como $g \neq e$, B es periódico, lo cual es una contradicción. Por tanto D no es periódico. Entonces G no posee la n-propiedad de Hajós. ■

Teorema 2.2. *Sea G un grupo abeliano finito y sea H subgrupo de G. Si G no posee subgrupos 2-elementales de orden mayor que $|H|$ y H no tiene la n- propiedad de Hajós entonces G tampoco tiene la n-propiedad de Hajós.*

Demostración.

- Caso 1: Si $H = G$, la prueba es inmediata.
- Caso 2: Supongamos que H es sugrupo propio de G.
  Sea p_1 un número primo tal que $p_1| \left|\frac{G}{H}\right|$, entonces G/H debe poseer un subgrupo de orden p_1, por lo que existe $K_1 \leq G$ con $H \subsetneq K_1$ tal que $|\frac{K_1}{H}| = p_1$.
  Como H no tiene la n-propiedad de Hajós y K_1 no es un grupo 2-elemental ($|K_1| > |H|$), entonces, por Lema 2.2, K_1 tampoco tiene la n-propiedad de Hajós.
  Si $K_1 = G$ entonces termina la prueba, en otro caso, $|\frac{G}{K_1}| > 1$ y existe $p_2 \left| |\frac{G}{K_1}\right|$ y $K_2 \leq G$ con $K_1 \subsetneq K_2$ tal que $|\frac{K_2}{K_1}| = p_2$, p_2 numero primo, entonces de nuevo por Lema 2.2, K_2 no tiene la n-propiedad de Hajos. Si $K_2 = G$ entonces termina la prueba, de lo contrario, $|\frac{G}{K_2}| > 1$ y volvemos a proceder de manera similar al paso anterior.
  Del hecho de que G es un grupo finito y continuando con el proceso anterior en forma recursiva podemos afirmar que existe un K_n que no tiene la n-propiedad de Hajós tal que $K_{n-1} \subsetneq K_n$, $|\frac{K_n}{K_{n-1}}| = p_n$ y $K_n = G$.

∎

Ahora veremos un ejemplo de un grupo del tipo (p^2, p) con p primo que no posee la n-propiedad de Hajós para $n \neq 3$. Notemos que las posibilidades no triviales para el valor de n son $n = 2$ y $n = 3$.

Ejemplo 2.2. Sea $G = \langle x\rangle\langle y\rangle$, con $|x| = p^2$ y $|y| = p$. G no tiene la n-propiedad de Hajós si $n \neq 3$.

Demostración. Observemos que cualquier factorización de G en n conjuntos se reduce a una factorización no trivial de G de dos o tres conjuntos. Por el Teorema 2.1, G tiene la 3-propiedad de Hajós, pues si G tiene una factorización normalizada en 3 en conjuntos, cada uno de tales conjuntos debe tener cardinalidad p. Probaremos que G no tiene la 2-propiedad de Hajós. Construiremos una factorización $G = AB$ de G en la cual ni A ni B son conjuntos periódicos.

Consideremos

$$\begin{aligned} A &= \langle x^p \rangle \cup x\langle y \rangle \cup x^2\langle y \rangle \cup \ldots \cup x^{p-1}\langle y \rangle \\ B &= \{e, x^p y, (x^p y)^2, \ldots, (x^p y)^{p-3}, x^{p(p-2)}y^{p-1}, x^{p(p-1)}y^{p-2}\} \end{aligned}$$

Ahora, usemos el teorema 1.4 para probar que $G = AB$ es una factorización de G. Es claro que $|G| = |A||B|$. Veamos que cada $\chi \in G^*$ con χ no-principal pertenece a $Ann(A) \cup Ann(B)$.

$$\begin{aligned} \chi(A) &= \sum_{a \in A} [\chi(a)] \\ &= \sum_{k=1}^{p} [\chi(x^{pk})] + \sum_{k=1}^{p} [\chi(xy^k)] + \cdots + \sum_{k=1}^{p} [\chi(x^{p-1}y^k)] \\ &= \sum_{k=1}^{p} [\chi(x^{pk})] + \sum_{k=1}^{p} [\chi(x)\chi(y^k)] + \cdots + \sum_{k=1}^{p} [\chi(x^{p-1})\chi(y^k)] \\ &= \sum_{k=1}^{p} [\chi(x^{pk})] + \sum_{k=1}^{p} [\chi(x)\chi(y)^k] + \cdots + \sum_{k=1}^{p} [\chi(x)^{p-1}\chi(y)^k] \\ &= \sum_{k=1}^{p} [\chi(x^{pk})] + (\sum_{k=1}^{p} [\chi(y)^k](\chi(x) + \cdots + \chi(x)^{p-1})) \\ &= \sum_{k=1}^{p} \chi(x^{pk}) + \sum_{k=1}^{p} [\chi(y)^k](\sum_{k=1}^{p-1} [\chi(x)^k)] \\ &= \chi(\langle x^p \rangle) + \chi(\langle y \rangle)(\sum_{k=1}^{p-1} [\chi(x)^k]) \end{aligned}$$

$$\begin{aligned} \chi(B) &= \sum_{b \in B} [\chi(b)] \\ &= \chi(e) + \sum_{k=1}^{p-3} [\chi((x^p y)^k)] + \chi(x^{p(p-2)}y^{p-1}) + \chi(x^{p(p-1)}y^{p-2}) \\ &= \chi(e) + \sum_{k=1}^{p-3} [\chi(x)^{pk}\chi(y)^k] + \chi(x)^{p(p-2)}\chi(y)^{p-1} + \chi(x)^{p(p-1)}\chi(y)^{p-2} \end{aligned}$$

Observemos que las posibilidades para el orden de $\chi(x)$ son $1, p$ y p^2 y las posibilidades para el orden de $\chi(y)$ son $1, p$. En total hay 6 casos diferentes a considerar:

- Caso 1: $|\chi(x)| = 1$ y $|\chi(y)| = 1$.
  En este caso χ es trivial así que lo descartamos.

- Caso 2: $|\chi(x)| = 1$ y $|\chi(y)| = p$.
  Como $|\chi(x)| = 1$ entonces $\chi(x) = 1$ y como $|\chi(y)| = p$ entonces $\chi(y)^p = 1$, Así:

$$\begin{aligned}
\chi(B) &= \chi(e) + (\sum_{k=1}^{p-3}[\chi(x)^{pk}\chi(y)^k]) + \chi(x)^{p(p-2)}\chi(y)^{p-1} + \chi(x)^{p(p-1)}\chi(y)^{p-2} \\
&= \chi(e) + (\sum_{k=1}^{p-3}[1^{pk}\chi(y)^k)]) + 1^{p(p-2)}\chi(y)^{p-1} + 1^{p(p-1)}\chi(y)^{p-2} \\
&= \chi(e) + (\sum_{k=1}^{p-3}[\chi(y)^k]) + \chi(y)^{p-1} + \chi(y)^{p-2} \\
&= \sum_{k=1}^{p}[\chi(y)^k] \\
&= \chi(\langle y\rangle)
\end{aligned}$$

  Supongamos que χ es trivial, esto es, para todo $c \in \langle y\rangle$, $c \neq e$ se tiene que $\chi(c) = 1$ entonces

$$\begin{aligned}
& \chi(y^r) = 1 \quad , 1 \leq r < p \\
\Rightarrow\ & \chi(y)^r = 1 \quad , 1 \leq r < p \\
\Rightarrow\ & p|r \quad , |\chi(y)| = p \\
\Rightarrow\ & r = pk \quad , \text{para algún} \quad k \in \mathbb{Z}
\end{aligned}$$

  Entonces $p \leq r$ lo cual es una contradicción, por lo tanto $\chi(c) \neq 1$ para algún $c \in \langle y\rangle$ y por Ejemplo 1.7 $\chi(\langle y\rangle) = 0$.

  Por tanto $\chi(B) = \chi(\langle y\rangle) = 0$

- Caso 3: $|\chi(x)| = p$ y $|\chi(y)| = 1$.

Tenemos que $\chi(x)^p = 1$ y $\chi(y) = 1$, entonces

$$\begin{aligned}
\chi(A) &= \chi(\langle x^p \rangle) + \chi(\langle y \rangle) \sum_{k=1}^{p-1} [\chi(x)^k] \\
&= |\langle x^p \rangle| + |\langle y \rangle| \sum_{k=1}^{p-1} [\chi(x)^k] \\
&= p + p \sum_{k=1}^{p-1} [\chi(x)^k] \\
&= p(1 + \sum_{k=1}^{p-1} [\chi(x)^k]) \\
&= p(\chi(x)^p + \sum_{k=1}^{p-1} [\chi(x)^k]) \\
&= p \sum_{k=1}^{p} [\chi(x)^k] \\
&= p\chi(\langle x \rangle)
\end{aligned}$$

Razonando de forma análoga a el caso anterior concluiremos que $\chi(\langle x \rangle) = 0$ y por lo tanto,

$$\chi(A) = p(\chi(\langle x \rangle)) = p(0) = 0$$

- Caso 4: $|\chi(x)| = p$ y $|\chi(y)| = p$.
  Tenemos que $\chi(x)^p = 1$ y $\chi(y)^p = 1$, entonces

$$\begin{aligned}
\chi(B) &= \chi(e) + (\sum_{k=1}^{p-3} [\chi(x)^{pk} \chi(y)^k]) + \chi(x)^{p(p-2)} \chi(y)^{p-1} + \chi(x)^{p(p-1)} \chi(y)^{p-2} \\
&= \chi(e) + (\sum_{k=1}^{p-3} 1^k [\chi(y)^k + 1^{p-2}] \chi(y)^{p-1} + 1^{p-1} \chi(y)^{p-2} \\
&= \chi(e) + (\sum_{k=1}^{p-3} [\chi(y)^k]) + \chi(y)^{p-1} + \chi(y)^{p-2} \\
&= \sum_{k=1}^{p} [\chi(y)^k] \\
&= \chi(\langle y \rangle)
\end{aligned}$$

Una vez mas razonamos de la misma forma que en el caso 2 para concluir que $\chi(\langle y\rangle) = 0$ y por lo tanto $\chi(B) = 0$.

- Caso 5: $|\chi(x)| = p^2$ y $|\chi(y)| = 1$.
  Entonces $\chi(x)^{p^2} = 1$ y $\chi(y) = 1$

$$\begin{aligned}
\chi(B) &= \chi(e) + (\sum_{k=1}^{p-3}[\chi(x)^{pk}\chi(y)^k]) + \chi(x)^{p(p-2)}\chi(y)^{p-1} + \chi(x)^{p(p-1)}\chi(y)^{p-2} \\
&= \chi(e) + (\sum_{k=1}^{p-3}[\chi(x)^{pk}1^k]) + \chi(x)^{p(p-2)}1^{p-1} + \chi(x)^{p(p-1)}1^{p-2} \\
&= \chi(e) + (\sum_{k=1}^{p-3}[\chi(x)^{pk}]) + \chi(x)^{p(p-1)} + \chi(x)^{p(p-2)} \\
&= \sum_{k=1}^{p}[\chi(x)^{pk}] \\
&= \chi(\langle x^p\rangle)
\end{aligned}$$

Supongamos que χ es trivial, esto es, para todo $c \in \langle x^p\rangle$, $c \neq e$ se tiene que $\chi(c) = 1$ entonces

$$\begin{aligned}
& \chi(x^{pr}) = 1 \quad ,1 \leq r < p \\
\Rightarrow\ & \chi(x)^{pr} = 1 \quad ,1 \leq r < p \\
\Rightarrow\ & p^2|pr \quad ,|\chi(x)| = p^2 \\
\Rightarrow\ & pr = p^2k \quad \text{, para algún} \quad k \in \mathbb{Z} \\
\Rightarrow\ & r = pk \quad \text{, para algún} \quad k \in \mathbb{Z}
\end{aligned}$$

Entonces $p \leq r$ lo cual es una contradicción, por lo tanto $\chi(c) \neq 1$ para algún $c \in \langle x^p\rangle$ y por ejemplo 1.7 $\chi(B) = \chi(\langle x^p\rangle) = 0$.

- Caso 6: $|\chi(x)| = p^2$ y $|\chi(y)| = p$.

$$\chi(A) = \chi(\langle x^p\rangle) + \chi(\langle y\rangle)\sum_{k=1}^{p-1}[\chi(x)^k]$$

Usando el mismo razonamiento que en los casos 2 y 5 podemos obtener que

$\chi(\langle x^p\rangle) = 0$ y $\chi(\langle y\rangle) = 0$ y sustituyendo en la ecuación anterior obtenemos.

$$\begin{aligned}\chi(A) &= \chi(\langle x^p\rangle) + \chi(\langle y\rangle)\sum_{k=1}^{p-1}[\chi(x)^k] \\ &= 0 + (0\sum_{k=1}^{p-1}[\chi(x)^k]) \\ &= 0\end{aligned}$$

Asi, $G = AB$ es una factorizacion de G.

Ahora veamos que ni A ni B son periódicos. Supongamos que A es periódico entonces debe existir un $a \neq e \in A$ tal que $aA = A$ y ocurrirá también que $a^\alpha A = A$ para todo α, en particular, como $e \in A$ entonces $\langle a\rangle \subset A$. Como $|a|$ es divisor de $|G|$ entonces este puede ser p o p^2 ya que si fuese 1 entonces a seria e lo cual no es posible por la escogencia misma del a y no puede ser p^3 pues esto obligaría a G a ser un grupo cíclico y este no es el caso. Observemos que A no es un grupo, en efecto, $x^{p-1}, x^2 \in A$ pero $x^{p-1}x^2 = x^{p+1} \notin A$ ya que de lo contrario, $x^{p+1} = (x^p)^r$ con $1 \leq r \leq p-1$ o $x^{p+1} = x^r y^s$ con $r, s \in \{1, \cdots, p-1\}$. Sin embargo

$$\begin{array}{cc|cc} & x^{p+1} = (x^p)^r & & x^{p+1} = x^r y^s \\ \Rightarrow & x^{pr-p-1} = e & \Rightarrow & x^{p-r+1} = y^s \\ \Rightarrow & p^2|(pr-p-1) & \Rightarrow & x^{p-r+1} \in \langle x\rangle \cap \langle y\rangle \\ \Rightarrow & pr-p-1 = p^2k \ \ (k \in \mathbb{Z}) & \Rightarrow & x^{p-r+1} = e \\ \Rightarrow & pr-p-p^2k = 1 & \Rightarrow & p^2|(p-r+1) \\ \Rightarrow & p|1 & & pero \ \ 2 \leq p-r+1 \leq p \\ & Contradiccion!! & & \text{así } \ p^2\not|(p-r+1) \ \ Contradiccion!! \end{array}$$

Supongamos Ahora que $|a| = p^2$

Si $a = x^r$ con $1 \leq r \leq p-1$, entonces $\operatorname{mcd}(r, p^2) = 1$ asi $|a| = |x^r| = |x| = p^2$, luego $\langle x\rangle = \langle a\rangle \subset A$, en consecuencia $x^{p+1} \in A$ lo cual como ya vimos es una contradiccion.

Si $a = (x^p)^r$ con $1 \leq r \leq p-1$ entonces

$$a^p = [(x^p)^r]^p = (x^{p^2})^r = e$$

pero esto es una contradiccion ya que $|a| = p^2$.

Supongamos ahora que $a = x^r y^s$ con $r, s \in \{1, \cdots, p-1\}$. Asi $\operatorname{mcd}(r, p^2) = 1$ y

$\text{mcd}(s, p) = 1$ esto impica que

$$\begin{array}{lccc} & |x^r| = |x| = p^2 & \wedge & |y^s| = |y| = p \\ \Rightarrow & \langle x^r \rangle = \langle x \rangle & \wedge & \langle y^s \rangle = \langle y \rangle \end{array}.$$

Ahora Sean $a_1, a_2 \in A$ entonces $a_1 = x^i y^j$ y $a_2 = x^l y^m$. Luego

$$\begin{aligned} a_1 a_2^{-1} &= (x^i y^j)(x^l y^m)^{-1} \\ &= x^{i-l} y^{j-m} \\ &= (x^r)^{n_1} (y^s)^{n_2} \quad ; \quad n_1, n_2 \in \mathbb{Z} \\ &= (x^r y^s)^{n_1 - 1} x^r y^{n-2-n_1+1} \\ &= a^{n_1-1} x^r y^{n-2-n_1+1} \end{aligned}$$

Entonces $a_1 a_2^{-1} \in a^{n_1-1} x^r \langle y \rangle \in a^{n_1-1} A \in A$ por lo que A es un subgrupo pero ya vimos que esto no es posible.

Supongamos ahora que $|a| = p$, entonces si $a = x^r y^s$ $1 \leq r \leq p-1$ y $1 \leq s \leq p$ tenemos que

$$\begin{aligned} e &= a^p \\ &= (x^r y^s)^p \\ &= (x^r)^p (y^s)^p \\ &= x^{rp} (y^p)^s \\ &= x^{rp} e \\ &= x^{rp} \end{aligned}$$

por lo que $p^2 | pr$ pero esto es una contradiccion. Si $a = (x^p)^\alpha$ para algun $a \leq \alpha \leq p-1$ entonces por ejemplo $(x^p)^\alpha (xy)$ debe ser un elemento de A y esto no es cierto pues $(x^p)^\alpha (xy) = x^{p\alpha+1} y \notin A$ ya que $p\alpha + 1 \geq p+1$, asi A no es periodico.

Si B es periodico entonces un $b \neq e \in B$ tal que $bB = B$ y ocurrirá también que $b^\beta B = B$ para todo β, ademas como $e \in B$ entonces $\langle b \rangle \subset B$. De nuevo como $|b|$ es divisor de $|G|$ entonces este puede ser p o p^2 ya que si fuese 1 entonces b seria e lo cual no es posible por la escogencia misma del b y no puede ser p^3 pues esto obligaría a G a ser un grupo cíclico. Ahora si $|b| = p^2$ entonces $|\langle b \rangle| = p^2$ lo cual es una contradiccion ya que B contendria un subconjunto con mas elementos que el y esto es imposible. Si $|b| = p$ entonces $|\langle b\rangle| = p$ ademas es claro que $|B| = p$, Asi $\langle b\rangle = B$ y por tanto B seria un grupo sin embargo es no es cierto pues por ejemplo $x^p y \in B$ pero $(x^p y)^{p-1} \notin B$, luego B no es periodico.

Concluimos asi que G no tiene la 2-propiedad de Hajós. ∎

Observación 2.1. El Teorema 2.2 y el Ejemplo 2.2 muestran que los grupos del tipo $(p^{\alpha_1}, p^{\alpha_2}, \ldots p^{\alpha_n})$ con $p \geq 3$ primo, no tiene la n-propiedad de Hajós para $1 \leq n < \alpha_1 + \alpha_2 + \ldots \alpha_n$,

Lema 2.3. *Sea G un grupo abeliano finito y H un subgrupo propio de G. Si G posee la n-propiedad de Hajós, entonces G/H también la tiene.*

Demostración. Sea $G/H = (A_1/H)(A_2/H)\cdots(A_n/H)$ una factorizacion de G/H y sea $g \in G$. Como
$$G = \bigcup_{b_i \in G} b_i H$$
entonces $g \in g_1 H \in G/H$, luego existen $a_1, a_2, \ldots, a_n$ unicos tal que $a_i \in A_1$ y $g_1 H = a_1 H a_2 H \cdots a_n H = (a_1 a_2 \cdots a_n)H$ entonces existe un unico $h \in H$ tal que
$$\begin{aligned} &\Rightarrow \quad g = (a_1 a_2 \cdots a_n)h \\ &\Rightarrow \quad g = a_1 a_2 \cdots (a_n h) \end{aligned}$$
Entonces de la unicidad de $a_1, a_2, \ldots, a_n, h$ y del hecho de que g es arbitrario entonces $G = A_1 A_2 \cdots (A_n H)$ es una factorizacion de G. Ahora como G tiene la n-propiedad de Hajós entonces $A_n H$ es periodico o alguno de los A_i con $i \in \{1, \ldots, n_1\}$ es periodico. Si $A_n H$ es periodico entonces existe $a_n h \neq e$ tal que $a_n h A_n H = A_n H$. Sea $aH \in A_n/H$ entonces
$$\begin{aligned} aH &= a_n h a' H \quad ; \ \text{para algún } \ a' \in A_n \\ &= a_n a' h H \\ &= a_n a' H \\ &= a_n H a' H \end{aligned}$$
Asi, como aH es arbitrario entonces $a_n H$ un periodo de A_n/H y por lo tanto este es Periodico. Ahora supongamos que uno de los A_i con $i \in \{1, \ldots, n_1\}$ es periodico.Como

A_i es periódico entonces existe un $a \in A_i$ tal que $aA_i = A_i$. Entonces para todo $a_j \in A_i$ tenemos que $aa_j = a_k$ con $a_k \in A_i$. Veamos que A_iH/H es un conjunto periódico. Sea $a_jH \in A_iH/H$ veamos que $aHa_jH = a_kH$ para algún $a_kH \in A_iH/H$.

$$\begin{aligned} aHa_jh &= aa_jhH \quad \forall h \in H \\ ; &= aa_jH \\ &= a_kH \end{aligned}$$

Esto es, $aHa_jH \subset a_kH$ luego como ambos conjuntos tienen el mismo orden entonces

$$aHa_jH = a_kH \quad \forall a_jH \in A_1H/H$$

Por lo tanto $aHA_iH/H \subset A_iH/H$ y de nuevo como los conjuntos tienen el mismo orden entonces $aH(A_iH/H) = A_iH/H$. Así A_iH/H es periódico.
Luego, como $G/H = (A_1/H)(A_2/H)\cdots(A_n/H)$ es una factorizacion cualquiera entonces G/H tiene la n-propiedad de Hajos. ∎

2.2. Propiedad de Rédei

Ahora veamos algunos resultados acerca de la propiedad de Rédei, antes de enunciar el teorema que nos proporciona una relación entre ambas propiedades.

Definición 2.3. Sea G un grupo abeliano finito, si para toda factorización $G = A_1...A_i...A_n$ de G en subconjuntos se tiene que al menos uno de los A_i es tal que $\langle A_i\rangle \neq G$, decimos que G tiene la *n-propiedad de Rédei*.

Lema 2.4. *Sea $G = A_1A_2\cdots A_n$ una factorización del grupo abeliano finito G. Supongamos que H es un subgrupo de G. Si de la factorización*

$$G/H = (A_1H/H)(A_2H/H)\cdots(A_nH/H)$$

al menos uno de los A_iH/H es tal que $\langle(A_iH/H)\rangle \neq G/H$ entonces para al menos uno de los A_i se tiene que $\langle A_i\rangle \neq G$

Demostración. Supongamos por reducción a lo absurdo que para todo A_i se tiene que $\langle A_i \rangle = G$. Sea $g \in G$ entonces existen $a_{i1}, a_{i2}, \cdots, a_{ik} \in A_i$ tal que

$$
\begin{aligned}
& g = a_{i1}^{\alpha_i 1} a_{i2}^{\alpha_i 2} \cdots a_{ik}^{\alpha_i k} \quad ; \forall i \\
\Rightarrow \; & gH = (a_{i1}^{\alpha_i 1} a_{i2}^{\alpha_i 2} \cdots a_{ik}^{\alpha_i k})H \quad ; \forall i \\
\Rightarrow \; & gH = (a_{i1}^{\alpha_i 1} H)(a_{i2}^{\alpha_i 2} H) \cdots (a_{ik}^{\alpha_i k} H) \quad ; \forall i \\
\Rightarrow \; & gH = (a_{i1} H)^{\alpha_i 1} (a_{i2} H)^{\alpha_i 2} \cdots (a_{ik} H)^{\alpha_i k} \quad ; \forall i
\end{aligned}
$$

por lo tanto $G/H = \langle (A_i H/H) \rangle$ para todo $A_i \in G/H$, lo cual es una contradicción. Así, se tiene que al menos uno de los A_i es tal que $\langle A_i \rangle \neq G$. ■

Usando este lema podemos demostrar de forma inmediata el siguiente teorema.

Teorema 2.3. *Sea G un grupo abeliano finito y H un subgrupo de G. Si G/H tiene la n-propiedad de redei entonces G tiene la n-propiedad de redei.*

2.2.1. Relación entre la n-propiedad de Hajós y la n-propiedad de Rédei

Finalmente damos un resultado que nos relaciona la n-propiedad de Hajós con la n-propiedad de Rédei.

Teorema 2.4. *Si G grupo abeliano finito tiene la n-propiedad de Hajós entonces tiene la n-propiedad de Rédei.*

Demostración. Sea G un grupo abeliano finito que tiene la n-propiedad de Hajós y consideremos una factorización $G = A_1 \cdots A_i \cdots A_n$ de G. Procederemos por inducción sobre el numero de factores primos no necesariamente distintos k de $|G|$. Supongamos que $k = 1$, como $|G| = |A_1| \cdots |A_i| \cdots |A_n|$ entonces uno de los A_i digamos A_1(ya que podemos reordenar a los A_i) tiene orden primo p y el resto tiene orden 1. Así $A_1 = G$,$A_2 = \{e\}$,…,$A_n = \{e\}$ para todo i. Luego, $\langle A_i \rangle \neq G$ para todo $i \geq 2$.
Ahora supongamos que el teorema se cumple para todo grupo G con menos de k factores primos no necesariamente distintos. Probemos ahora que para todo grupo G con exactamente k factores primos no necesariamente distintos se cumple. Como G tiene la n-propiedad alguno de los A_i es periódico, entonces por teorema 1.2 $A_i = HC$ es una factorizacion de A_i donde H es un subgrupo propio y C un subconjunto de G. Ahora,

de la factorización $G = A_1 \cdots A_i \cdots A_n$ obtenemos una factorización del grupo cociente G/H, en efecto veamos que $G/H = A_1/H \cdots CH/H \cdots A_nH/H$ es una factorización de G/H.

Sea $g \in G$, como $G = A_1 \cdots A_i \cdots A_n$ es una factorización de G entonces podemos escribir a g de manera único como

$$g = a_1 a_2 \cdots a_i \cdots a_n \quad ,\text{con} \quad a_i \in A_i, \forall i \tag{2.7}$$

Como $A_i = HC$ es una factorización de A_i entonces a_i puede escribirse en forma única como

$$a_i = hc \quad ,\text{con} \quad c \in C, h \in H \tag{2.8}$$

por lo tanto $g = a_1 a_2 \cdots hc \cdots a_n$, Asi

$$\begin{aligned} gH &= (a_1 a_2 \cdots hc \cdots a_n)H \\ &= a_1 H a_2 H \cdots hcH \cdots a_n H \\ &= a_1 H a_2 H \cdots cH \cdots a_n H \end{aligned}$$

Ahora, por la unicidad de los $a_1, a_2, \cdots, a_n, h, c$ se tiene que la representación anterior es única. Luego, como g es arbitrario entonces gH también lo es y por lo tanto se tiene que

$$G/H = A_1H/H \cdots CH/H \cdots A_nH/H \tag{2.9}$$

es una factorización de G/H. Ahora por lema 2.3 se tiene que G/H tambien tiene la n-propiedad de Hajos, ademas $|G/H| = |G|/|H| < |G|$ entonces por hipótesis inductiva G/H tiene la n-propiedad de Rédei. Luego por Teorema 2.3 tenemos que G posee la n-propiedad de Rédei. ■

CONCLUSIONES

En este trabajo determinamos condiciones sobre subconjuntos de un grupo abeliano finito G para que éstos formen una factorización de G, algunas de tales condiciones relacionadas con el conjunto de caracteres del grupo G. Mostramos que si un grupo abeliano finito G, el cual no es 2-elemental, no tiene la n-propiedad de Hajós, entonces G no tiene la n propiedad de Hajós, este hecho nos permitió construir una familia de p-grupos no cíclicos que no tienen la n propiedad de Hajós, cuando n es menor o igual que el rango del grupo. Además mostramos que si un grupo abeliano finito tiene la n-propiedad de Hajós, entonces debe tener la n-propiedad de Rédei, estableciendo de esta forma una relación entre ambas propiedades. Como un tema próximo de estudio proponemos el estudiar la n-propiedad de Hajós para 2-grupos elementales.

REFERENCIAS BIBLIOGRÁFICAS

[1] K. Amin. Factorization of Finite Abelian Groups. *International Journal of Algebra* **Vol. 6, nº3**, (2012) 101-107.

[2] K. Amin. The Hajós Factorization of Elementary 3-Groups, *Journal of Algebra.* **Vol. 224** (2000), 241-247.

[3] N.G. de Bruijn. On the factorization of finite abelian groups, *Indag. Math.* **Vol 15** (1953), 258–264.

[4] G. Hajós. Sur la factorization des groups abeliens, *Casopis Pest, Mat.Fys.***Vol 74** (1949), 157-162.

[5] T. Hungerford. Algebra. *Springer-Verlag* **2º edicion**, (1980).

[6] H. Minkowsjki, Diphantische Approximationem (Leipzig, 1907).

[7] L. Rédei. Die neue Theorie der endlichn abelschn Gruppen und Berallgeminerung des Hauptsatz von Hajós, *Acta math.Acad.hunar.***Vol 16**(1965), 357-364.

[8] A. Sands, S. Zsabo. Factoring Groups into Subsets *Chapman and Hall/CRC* **Vol. 256**, (2009).

[9] S. Zsabo. Topics in Factorization of Abelian Groups. *Birkhäuser Verlag* (2004).