GRUPOS CON AUSENCIA DE CONMUTATIVIDAD

ANGELA PATRICIA ARDILA CABALLERO

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE MATEMÁTICAS
BUCARAMANGA
2020

GRUPOS CON AUSENCIA DE CONMUTATIVIDAD

ANGELA PATRICIA ARDILA CABALLERO

Trabajo de Grado para optar al título de
Matemática

Director
Alexander Holguín Villa
Doctor en Ciencias Matemáticas

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE MATEMÁTICAS
BUCARAMANGA
2020

DEDICATORIA

A mis padres.

AGRADECIMIENTOS

Agradezco enormemente a mis padres, Gloria Consuelo y Hector por confiar en mi y por el esfuerzo hecho para permitirme llegar a este punto, su apoyo incondicional fue fundamental para mi formación.

A mi director, el profesor Alexander Holguín Villa por el tiempo dedicado y el aporte de sus conocimientos para la realización de este trabajo.

Por último, agradezco a todos los profesores que contribuyeron en mi formación académica.

CONTENIDO

LISTA DE SÍMBOLOS

$\|a\|$	|	Orden del elemento a de un grupo
$\|G\|$	|	Orden del grupo G
$[G:H]$	|	Índice del subgrupo H en G
$\mathcal{Z}(G)$	|	Centro del grupo G
$\langle a \rangle$	|	Subgrupo cíclico generado por a
$H \times K$	|	Producto directo de H y K
C_n	|	Grupo de cíclico de orden n
$H \trianglelefteq G$	|	H subgrupo normal de G
G/H	|	Grupo cociente
(g,h)	|	Conmutador multiplicativo
G'	|	Subgrupo conmutador del grupo G
$C(g)$	|	Clase de conjugación
$exp(G)$	|	Exponente del grupo G
$*$	|	Involución
$supp(\alpha)$	|	Soporte del elemento α de RG
$[x,y]$	|	Corchete de Lie de x e y
$\mathcal{C}$	|	Números de Cayley
$\mathcal{Q}_8$	|	Grupo cuaternio de orden 8
$\mathcal{D}_4$	|	Grupo diedral de orden 8
$\mathcal{H}_{\mathbb{R}}$	|	Cuaternios Reales
RG^+	|	Conjunto de elementos simétricos de RG
$car(R)$	|	Característica del anillo R

RESUMEN

TÍTULO: GRUPOS CON AUSENCIA DE CONMUTATIVIDAD [*]

AUTORA: ANGELA PATRICIA ARDILA CABALLERO [**]

PALABRAS CLAVE: ANILLOS DE GRUPO, ANILLOS DE LOOP, SLC-GRUPOS

DESCRIPCIÓN:

Dado un loop y un anillo asociativo, conmutativo y con unidad, se construye el anillo de loop de la misma forma que se construye un anillo de grupo. En esta tesis se trabaja con anillos de loop tales que el anillo tiene característica diferente de 2 y el loop es un loop de Moufang no asociativo, construido a partir de un grupo no abeliano, este tipo de anillos de loop son no asociativos, sin embargo, pueden ser alternativos. De acuerdo con esto, se presenta un resultado que proporciona equivalencias para que estos anillos de loop sean alternativos, una de estas equivalencias establece cierta propiedad sobre grupos no abelianos con una involución, dichos grupos son precisamente los grupos con ausencia de conmutatividad y un único conmutador no trivial o SLC-grupos. Siendo esta la estructura central en este trabajo, se estudia una caracterización de estos, sus propiedades, algunos ejemplos de particular interés y cómo construir grupos de este tipo a partir de uno dado. Por último, se muestra como estos grupos aparecen de manera natural en el estudio de los anillos de grupo, examinando la pregunta de cuándo el conjunto de los elementos simétricos con respecto a la llamada *involución clásica* conmuta.

---

[*] Trabajo de grado

[**] Facultad de Ciencias. Escuela de Matemáticas. Director: Alexander Holguín Villa, Doctor en Ciencias Matemáticas.

ABSTRACT

TITLE: GROUPS WITH LACK OF COMMUTATIVITY [*]

AUTHOR: ANGELA PATRICIA ARDILA CABALLERO [**]

KEYWORDS: GROUP RINGS, LOOP RINGS, SLC-GROUPS.

DESCRIPTION:

Given an associative and commutative ring with unity and a loop, the loop ring is constructed in the same way as a group ring is constructed. In this thesis, we work with loop rings such that the ring has characteristic different from 2 and the loop is a non-associative Moufang loop, constructed from a non-abelian group, this type of loop rings are non-associative, however, they can be alternative. In agreement with this, is presented a result that provides equivalences for these loop rings to be alternative, one of these equivalences establishes a certain property on non-abelian groups with an involution, these groups are precisely the groups with lack of commutativity a unique non-identity commutator or SLC-groups. This is the central structure in this work, we study a characterization of these, their properties, some examples of interest and how to get groups of this type from a given one. Finally, it is shown how these groups naturally appear in the study of group rings, watching carefully the question of when the set of symmetric elements with respect to the so-called *classical involution* commutes.

---

[*] Bachelor Thesis

[**] Facultad de Ciencias. Escuela de Matemáticas. Director: Alexander Holguín Villa, Doctor en Ciencias Matemáticas.

INTRODUCCIÓN

Con los elementos de un grupo G multiplicativo como base para un módulo libre en un anillo R conmutativo, asociativo y con una unidad, y extendiendo la operación en G al módulo a través de las leyes distributivas, se obtiene un anillo asociativo, llamado anillo de grupo de G sobre R y denotado por RG. Estos anillos fueron introducidos implícitamente por A. Cayley en un artículo en 1854, [1]. Se puede repetir la misma construcción, con un loop L en lugar de un grupo G. La idea de no requerir asociatividad y construir anillos de loop o álgebras loop, se debe a R.H Bruck quien las definió en 1944, pero fue hasta 1983 que se consideró un tema significativo. E. G. Goodaire demostró que existen álgebras de loop alternativas (no asociativas) que satisfacen identidades importantes, como las identidades alternativas a derecha y a izquierda [2].

Los anillos alternativos surgieron de los trabajos de R. Moufang en 1930. Gran parte de su atención se dirigió a la estructura multiplicativa de un anillo de división alternativo. Así como los elementos no nulos de un cuerpo forman un grupo multiplicativo, los elementos no nulos de un anillo de división alternativo forman un loop de Moufang con la operación multiplicación.

En este trabajo se mostrará cómo los grupos con ausencia de conmutatividad o LC-grupos están relacionados con los anillos de loop alternativos y a su vez como estos grupos aparecen de forma natural en el estudio de los anillos de grupo [3]. En el

---

[1] C. P MILIES y SEHGAL S. K. *An introduction to group rings*. Vol. 1. Springer Science & Business Media, 2002.

[2] E. G. GOODAIRE, JESPERS E. y MILIES C. P. *Alternative loop rings*. Vol. 184. Elsevier, 1996.

[3] O. B. CRISTO. “Commutativity of symmetric elements in group rings”. En: *Journal of Group Theory* 9.5 (2006), págs. 673-683.

Capítulo 1, se introducen las nociones básicas de teoría de grupos, anillos, módulos y anillos de grupo, que serán de utilidad a lo largo del texto. En la primera parte del Capítulo 2, se introducen las nociones de anillos alternativos, loops y anillos de loop alternativos. Luego de ello se estudiarán los LC-grupos, estructuras centrales en este trabajo, sus propiedades y algunos ejemplos de interés. Finalmente, el Capítulo 3 es dedicado al estudio de la conmutatividad del conjunto de los elementos simétricos RG^{+}, de un anillo de grupo respecto a la involución clásica, esto con el fin de ver como los LC-grupos con un único conmutador no trivial, o SLC-grupos, aparecen de manera natural en los anillos de grupo [3].

1. Preliminares

En este capítulo se presentarán algunas definiciones básicas y resultados ya conocidos que serán necesarios para entender este trabajo.

1.1. Grupos

Los grupos son una de las principales estructuras de interés en este trabajo. En esta sección se recordarán algunas definiciones y resultados básicos, omitiendo la mayoría de sus pruebas, las cuales pueden ser encontradas en cualquier texto de teoría de grupos, ver por ejemplo [4] [5].

Definición 1.1.1. *Un **grupo** es un conjunto no vacío G con una operación binaria (denotada por $\cdot$) tal que, para todos $a, b, c \in G$, se cumplen las siguientes propiedades:*

(i) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,

(ii) *existe un elemento, denotado por $1 \in G$, tal que $a \cdot 1 = 1 \cdot a = a$,*

(iii) *para cada elemento $a \in G$ existe un elemento, denotado por $a^{-1} \in G$, tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1$.*

Si además,

$$a \cdot b = b \cdot a,$$

---

[4] J. GALLIAN. *Contemporary abstract algebra*. Nelson Education, 2009.

[5] O. LEZAMA. *Cuadernos de Álgebra, No. 1: Grupos*. Departamento de Matemáticas, Universidad Nacional de Colombia, sede de Bogotá, 2017.

*para todos $a, b \in G$, se dice que el grupo es **abeliano**. Cabe destacar que en este trabajo, tienen mayor presencia los grupos no abelianos.*
*Si el conjunto G es finito, entonces el número de elementos de G es llamado el **orden** de G y es denotado por $|G|$.*

Definición 1.1.2. *Un subconjunto no vacío H de un grupo G es llamado un **subgrupo** de G, si este tiene estructura de grupo bajo la operación de G. En tal caso se escribe $H \leq G$.*

Proposición 1.1.1. *Sea G un grupo y a un elemento cualquiera de G. Entonces,*

$$\langle a \rangle = \{a^n : n \in \mathbb{Z}\},$$

*es un subgrupo de G, llamado **subgrupo cíclico** de G generado por el elemento a.*

Es posible que el subgrupo generado por algún elemento a del grupo G coincida con todo el grupo, es decir, $\langle a \rangle = G$, tales grupos reciben un nombre especial.

Definición 1.1.3. *Sea G un grupo. Se dice que G es **cíclico** si G coincide con uno de sus subgrupos cíclicos. Es decir, si existe un elemento $a \in G$ tal que $\langle a \rangle = G$. En este caso se dice que a es un **generador** del grupo cíclico G.*

Proposición 1.1.2. *Las siguientes afirmaciones son válidas para grupos cíclicos arbitrarios.*

- (i) *Todo grupo cíclico es abeliano.*
- (ii) *Cada subgrupo de un grupo cíclico es cíclico.*
- (iii) *Sea $G \neq \{1\}$ un grupo. Entonces, G es un grupo cíclico finito de orden primo si y solo si, G no tiene subgrupos diferentes de los triviales.*

Dado un subgrupo H de G y un elemento en G, es posible definir una *partición* del grupo G por subconjuntos disjuntos.

Definición 1.1.4. *Sea H un subgrupo de un grupo G. Dado un elemento $a \in G$, los subconjuntos de la forma*

$$aH = \{ah : h \in H\},$$
$$Ha = \{ha : h \in H\},$$

*son llamados **clase lateral izquierda** y **derecha** (respectivamente) del subgrupo H, determinadas por el elemento a. Este elemento a es llamado **representante** de la clase.*
El conjunto de todas las clases laterales izquierdas (derechas) de H en G es denotado por $G/_lH$ $(G/_rH)$.

La relación $\sim$ sobre G dada por $a \sim b$ si, y solo si, $a^{-1}b \in H$ con $a, b \in G$, es una *relación de equivalencia*. Además, para $a \in G$, su clase de equivalencia es:

$$\overline{a} = \{x \in G : x \equiv a \text{ (mód } H)\} = \{x \in G : a^{-1}x \in H\} = aH,$$

es decir, las clases de equivalencia determinadas por la relación $\sim$ son precisamente las clases laterales izquierdas de H en G. Ahora bien, es conocido que por ser $\sim$ relación de equivalencia sobre G, entonces dados $a, b \in G$, se tiene:

$$aH = bH \text{ o } aH \cap bH = \emptyset \quad \text{y} \quad G = \dot{\bigcup_{g \in G}} gH.$$

Un conjunto completo de representantes de las clases laterales izquierdas (derechas) de H en G es llamado un **transversal** izquierdo (derecho) de H en G.

Proposición 1.1.3. *La aplicación $\varphi : G/_lH \longrightarrow G/_rH$, dada por $\varphi(gH) = Hg^{-1}$ es una biyección.*

Del resultado anterior se deduce que $G/_lH$ y $G/_rH$ tienen la misma cardinalidad. Esto muestra la siguiente definición.

Definición 1.1.5. *Sea $H \leq G$. La cardinalidad del conjunto de clases laterales izquierdas o derechas es llamado el **índice** de H en G y es denotado por $[G : H]$.*

Teorema 1.1.1. *(Teorema de Lagrange) Si G es un grupo finito y H es un subgrupo de G, entonces $|H|$ divide a $|G|$. Además, el número de clases laterales izquierdas (o derechas) de H en G es $|G|/|H|$.*

Corolario 1.1.1. *Sea a un elemento de un grupo finito G. Entonces $|a|$ divide a $|G|$.*

Los subgrupos cuyas clases laterales derechas e izquierdas generadas por el mismo elemento son iguales son de especial importancia. Note que para un elemento a y un subgrupo H de un grupo G, se tiene que $aH = Ha$ si y solo si $a^{-1}Ha = H$. Esto sugiere lo siguiente:

Definición 1.1.6. *Sea H un subgrupo de un grupo G, se dice que H es **normal** en G, y se escribe $H \trianglelefteq G$, si $a^{-1}Ha = H$ para todo $a \in G$.*

Teorema 1.1.2. *Un subgrupo H de G es normal en G si y solo si $a^{-1}Ha \subseteq H$.*

A continuación se presentará un subgrupo que será de gran importancia.

Definición 1.1.7. *Sea G un grupo, el **centro** de G, denotado por $\mathcal{Z}(G)$, es el subgrupo dado por:*

$$\mathcal{Z}(G) = \{x \in G : xg = gx, \forall g \in G\}.$$

Claramente $\mathcal{Z}(G)$ es un subgrupo normal de G.

Sea N un subgrupo normal de un grupo G, entonces toda clase lateral izquierda de N en G es también una clase lateral derecha y viceversa, es decir, estas coinciden. En consecuencia, se denotará el conjunto de todas las clases laterales por G/N.

Definición 1.1.8. *Sea $H \trianglelefteq G$. El conjunto G/H de todas las clases laterales tiene estructura de grupo con la operación*

$$aHbH = (ab)H,\ a, b \in G,$$

*y es llamado **grupo cociente** de G por H.*

Note que el producto definido es asociativo dado que el producto en G lo es; la clase lateral identidad en G/H es $eH = H$ y los elementos inversos son dados por $(gH)^{-1} = g^{-1}H$.
El siguiente resultado será usado en el estudio de los SLC-grupos.

Teorema 1.1.3. *Sea G un grupo y sea $\mathcal{Z}(G)$ el centro de G. Si $G/\mathcal{Z}(G)$ es cíclico, entonces G es abeliano.*

Demostración. Sean $g \in G$ tal que $g\mathcal{Z}(G)$ genera a $G/\mathcal{Z}(G)$ y $a \in G$. Entonces existe un entero r tal que $a\mathcal{Z}(G) = (g\mathcal{Z}(G))^r = g^r\mathcal{Z}(G)$. Luego $a = g^r z$ para algún $z \in \mathcal{Z}(G)$. Puesto que g^r y z conmutan con g, a también conmuta con g y como a es arbitrario, sigue que g conmuta con cualquier elemento de G, es decir, $g \in \mathcal{Z}(G)$. Lo cual implica que $g\mathcal{Z}(G) = \mathcal{Z}(G)$ es el único elemento de $G/\mathcal{Z}(G)$. Por lo tanto, $G = \mathcal{Z}(G)$ y G es abeliano. □

Definición 1.1.9. *Sean G y H grupos multiplicativos. Una aplicación $\varphi : G \to H$ tal que $\varphi(ab) = \varphi(a)\varphi(b)$, para todos $a, b \in G$ se denomina un **homomorfismo** de grupos. Si φ es inyectivo se dice que es un **monomorfismo**; si es sobreyectivo se dice que es un **epimorfismo**, y si es biyectivo se dice que es un **isomorfismo**. En este último caso se dice que G y H son isomorfos y se denota por $G \cong H$.*

Definición 1.1.10. *Sea $\varphi : G \longrightarrow H$ un homomorfismo de grupos, se definen el **kernel** y la **imagen** de φ respectivamente como:*

$$\textit{Ker}\,(\varphi) = \{g \in G : \varphi(g) = 1_H\} \quad \textit{y} \quad \textit{Im}\,(\varphi) = \{\varphi(g) : g \in G\}$$

El resultado a continuación muestra las principales características de los homomorfismos.

Proposición 1.1.4. *Sea $\varphi : G \longrightarrow H$ un homomorfismo de grupos, entonces:*

(i) $\varphi(1_G) = 1_H$.

(ii) $\varphi(g^{-1}) = \varphi(g)^{-1}$.

(iii) *Ker* $(\varphi) \trianglelefteq G$.

(iv) φ *es inyectiva si, y solo si, Ker* $(\varphi) = \{1_G\}$.

(v) *Sea* $N \trianglelefteq G$. *La función* $j : G \longrightarrow G/N$ *definida por* $j(x) := \overline{x} = xN$, *es un epimorfismo denominado el* ***homomorfismo canónico***.

Teorema 1.1.4. *(Primer Teorema de Isomorfimos) Sea* $\varphi : G \longrightarrow H$ *un homomorfismo de grupos, entonces*

$$G/\textit{Ker}\,(\varphi) \cong \textit{Im}\,(\varphi).$$

En particular, si φ *es un epimorfismo, entonces* $G/\textit{Ker}\,(\varphi) \cong H$.

Definición 1.1.11. *Sean* H *y* K *subgrupos de* G. *Se dice que* G *es el* ***producto directo*** *de* H *y* K, *denotado por* $G = H \times K$, *si se cumple lo siguiente:*

(i) $G = HK$,

(ii) $H \cap K = \{1\}$,

(iii) $H \trianglelefteq G$ *y* $K \trianglelefteq G$.

Definición 1.1.12. *Dados dos elementos* x, y *en un grupo* G, *el* ***conmutador*** *de* x *e* y *es el elemento* $(x, y) = x^{-1}y^{-1}xy$. *En general, un conmutador de peso* $n > 2$ *es definido inductivamente por la regla*

$$(x_1, x_2, ..., x_n, x_{n+1}) = ((x_1, x_2, ..., x_n), x_{n+1}).$$

Dados dos subconjuntos H *y* K *del grupo* G, *se denotará por* (H, K) *el subgrupo de* G *generado por el conjunto:*

$$\{(h, k) : h \in H, k \in K\}.$$

En particular, el grupo $G' = (G, G)$ es llamado el ***subgrupo conmutador*** *o* ***subgrupo derivado*** *de G.*

En este trabajo, como ya se mencionó, son de mayor interés los grupos no abelianos. Por este motivo serán de gran importancia el *centro* y el *subgrupo conmutador* de un grupo no abeliano.

Proposición 1.1.5. *Sean x, y, z elementos de un grupo G, entonces la siguiente identidad es válida: $(xy, z) = (x, z)^y(y, z)$, donde $(x, z)^y = y^{-1}(x, z)y$.*

Demostración. Sean $x, y, z \in G$, entonces:

$$\begin{aligned}(xy, z) = (xy)^{-1}z^{-1}xyz = y^{-1}x^{-1}z^{-1}xyz = y^{-1}x^{-1}z^{-1}xzz^{-1}yz &= y^{-1}(x, z)z^{-1}yz \\ &= y^{-1}(x, z)yy^{-1}z^{-1}yz \\ &= y^{-1}(x, z)y(y, z).\end{aligned}$$

□

El siguiente resultado caracteriza el subgrupo conmutador.

Teorema 1.1.5. *Sean G un grupo y G' su subgrupo conmutador, entonces*

(i) $G' \trianglelefteq G$.

(ii) *G/G' es abeliano. Además, si $H \trianglelefteq G$, entonces G/H es abeliano si y solo si $G' \subset H$.*

(iii) *Si G es un grupo no abeliano y $H \leq G$ es tal que $G' \subset H$, entonces $H \trianglelefteq G$.*

Definición 1.1.13. *Sean G un grupo y $g \in G$. Se define la* ***clase de conjugación de*** *g como,*

$$C(g) = \{x^{-1}gx : x \in G\}.$$

Note que para todo $h \in G$, $h^{-1}C(g)h = C(g)$, pues si $x \in G$, $h^{-1}(x^{-1}gx)h = (xh)^{-1}g(xh)$.

Previo a la definición de p-subgrupo de Sylow y sus teoremas se presentan algunos conceptos necesarios.

Definición 1.1.14. *Sean G un grupo y p un entero primo:*

(i) *Un elemento $x \in G$ se dice **p-elemento** si su orden es un potencia de p, y x se dice **p′-elemento** si su orden es infinito o no divisible por p.*

(ii) *Si G es finito, se dice que G es **p-grupo**, si su orden, $|G|$, es un potencia de p.*

(iii) *Se dice que G es **abeliano elemental**, si G es abeliano y existe un primo q, tal que todo elemento $g \in G$ (excepto la identidad) tiene orden q.*

Definición 1.1.15. *Sea G un grupo, el **exponente** de G, es el menor entero positivo k tal que $g^k = 1$, para todo $g \in G$. Si tal entero existe se denota por $exp(G) = k$.*

De las definiciones 1.1.14 (iii) y 1.1.15 se obtiene que un grupo G es un p-grupo abeliano elemental si, y solo si, $exp(G) = p$.

El siguiente teorema es un resultado fundamental sobre p-grupos finitos [1].

Teorema 1.1.6. *Sea G un p-grupo finito no trivial. Entonces, $\mathcal{Z}(G) \neq \{1\}$.*

Sea G un grupo finito de orden $p^n m$, donde p es primo y $m \in \mathbb{N}$ es primo relativo con p. Sigue del Teorema de Lagrange 1.1.1, que un p-subgrupo de G no puede tener orden mayor que p^n. Esto último motiva la siguiente definición.

Definición 1.1.16. *Sea G un grupo finito de orden $|G| = p^n m$ donde $p \nmid m$. Un subgrupo de G de orden p^n es llamado un **p-subgrupo de Sylow** de G.*

Teorema 1.1.7. *Sea G un grupo finito de orden $|G| = p^n m$ donde p es primo y $p \nmid m$. Entonces:*

(i) *G contiene p-subgrupos de Sylow y además, cada p-subgrupo de G está contenido en un p-subgrupo de Sylow de G.*

(ii) *Todos los p-subgrupos de Sylow de G son conjugados en G.*

(iii) *Si n_p denota el número de p-subgrupos de Sylow de G, entonces $n_p \equiv 1$(mód p).*

Definición 1.1.17. *Sea G un grupo. Se dice que G es **nilpotente**, si G contiene una serie de subgrupos*

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_n = G,$$

tal que cada subgrupo G_{i-1} es normal en G y cada grupo cociente G_i/G_{i-1} está contenido en el centro de G/G_{i-1}, es decir, $G_i/G_{i-1} \subset \mathcal{Z}(G/G_{i-1})$, $1 \leq i \leq n$.
*Una serie de subgrupos finitos de G con esta propiedad es llamada una **serie central**.*

De la definición anterior sigue que cada grupo abeliano es nilpotente.

Proposición 1.1.6. *Un p-grupo finito es nilpotente.*

El siguiente criterio debido a P. Hall, permite concluir que un grupo G es nilpotente, usando extensión por un subgrupo normal H de G:

Teorema 1.1.8. *Sea G un grupo:*

(i) *Si $H \trianglelefteq G$ y ambos, H y G/H' son nilpotentes, entonces G es nilpotente.*

(ii) *Si $H \leq \mathcal{Z}(G)$ y si G/H es un grupo nilpotente, entonces G también es nilpotente.*

Es posible verificar que si un grupo es abeliano, todos sus subgrupos son normales, sin embargo la afirmación recíproca, en general no es cierta. Un ejemplo de esto es el grupo cuaternio $\mathcal{Q}_8$, el cual es no abeliano pero todos sus subgrupos son normales.
A continuación una clase especial de grupos, de la cual $\mathcal{Q}_8$ es un ejemplo explícito.

Definición 1.1.18. *Un grupo no abeliano G tal que todos sus subgrupos son normales es llamado un* ***grupo Hamiltoniano.***

Los grupos Hamiltonianos juegan un papel importante en este trabajo. A continuación se presenta una clasificación de dichos grupos.

Teorema 1.1.9. *Un grupo G es Hamiltoniano si, y solo si, $G = \mathcal{Q}_8 \times E \times A$, donde E es un 2-grupo abeliano elemental y A es un grupo abeliano con todos sus elementos de orden impar.*

En particular, todo grupo Hamiltoniano G contiene una copia isomorfa de $\mathcal{Q}_8$.

Definición 1.1.19. *Sea G un grupo. La aplicación $\varphi : G \longrightarrow G$ es llamada una* ***involución*** *si es un antihomomorfismo de orden 2, es decir, si para todos $g, h \in G$ se verifican las siguientes 2 condiciones:*

(i) $\varphi(gh) = \varphi(h)\varphi(g)$.

(ii) $\varphi(\varphi(g)) = g$.

Ejemplo 1.1.1. *Sea G un grupo. La aplicación $* : G \longrightarrow G$ definida por $g^* = g^{-1}$, es conocida como la* ***involución clásica****. De la inversión de elementos se tiene que:*

(i) $(gh)^* = (gh)^{-1} = h^{-1}g^{-1} = h^*g^*$

(ii) $(g^*)^* = (g^{-1})^{-1} = g$.

1.2. Anillos y módulos

Definición 1.2.1. *Sea R un conjunto no vacío. R es llamado* ***anillo****, si en R están definidas dos operaciones binarias denotadas por "$+$" y "$\cdot$" tales que:*

(i) $(R, +)$ *es un grupo abeliano.*

(ii) $(R, \cdot)$ *es un semigrupo con elemento identidad $1_R = 1$.*

(iii) *La multiplicación es distributiva respecto a la adición.*

Si además la multiplicación verifica que

$$a \cdot b = b \cdot a; \forall a, b \in R,$$

se dice que $(R, +, \cdot)$ *es un* ***anillo conmutativo****.*

Como se vio en la sección anterior, un homomorfismo de grupos preserva la operación, así mismo un homomorfismo de anillos preserva las operaciones del anillo, como lo muestra la siguiente definición.

Definición 1.2.2. *Sean* R *y* S *anillos. Una aplicación* $\phi : R \longrightarrow S$ *es llamada un* ***homomorfismo de anillos****, si para todos* $a, b \in R$ *se tiene que:*

(i) $\phi(a + b) = \phi(a) + \phi(b)$.

(ii) $\phi(ab) = \phi(a)\phi(b)$.

Se definen de igual manera que en grupos *monomorfismo, epimorfismo* e *isomorfismo.*

Definición 1.2.3. *Sea* R *un anillo. La aplicación* $\psi : R \longrightarrow R$ *es una* ***involución****, si para todos* $r, s \in R$

(i) $\psi(r + s) = \psi(r) + \psi(s)$.

(ii) $\psi(rs) = \psi(s)\psi(r)$.

(iii) $\psi(\psi(r)) = r$,

es decir, ψ *es un antihomomorfismo de anillos, de orden* 2*.*

Ejemplo 1.2.1. *Sea* R *un anillo conmutativo. La aplicación identidad* $i_{d_R} : R \longrightarrow R$ *es una involución en* R*.*

Ejemplo 1.2.2. *Sea* $\mathcal{H}_{\mathbb{R}} = \{a_1 + a_2 i + a_3 j + a_4 k : a_i \in \mathbb{R}, i, j, k$ *símbolos formales*$\}$ *el anillo de los cuaternios reales. Las aplicaciones* $\psi_1, \psi_2 : \mathcal{H}_{\mathbb{R}} \longrightarrow \mathcal{H}_{\mathbb{R}}$ *definidas por* $\psi_1(a_1+a_2 i+a_3 j+a_4 k) = a_1-a_2 i-a_3 j-a_4 k$ *y* $\psi_2(a_1+a_2 i+a_3 j+a_4 k) = a_1+a_3 i+a_2 j+a_4 k$*, respectivamente, son involuciones en* $\mathcal{H}_{\mathbb{R}}$.

Definición 1.2.4. *Sean* R *un anillo y* M *un grupo abeliano (aditivo). Se dice que* M *tiene estructura de* R***-módulo*** *a izquierda, si existe una aplicación* $\mu : R \times M \longrightarrow M$*, dada por* $(a, m) \longmapsto am$*, que verifica para todos* $a, b \in R$ *y* $m, m_1, m_2 \in M$ *las siguientes condiciones:*

(i) $(a + b)m = am + bm$.

(ii) $a(m_1 + m_2) = am_1 + am_2$.

(iii) $(ab)m = a(bm)$.

(iv) $1m = m$.

De manera similar se definen los módulos-R o **módulos a derecha** sobre el anillo R, es decir, se tiene una aplicación $\hat{\mu} : M \times R \longrightarrow M$, donde ahora el anillo R actúa por derecha sobre los elementos de M.

Definición 1.2.5. *Un conjunto* $S = \{s_i\}_{i \in I}$ *de elementos de un* R*-módulo* M*, es llamado:*

(i) ***conjunto de generadores*** *de* M*, si* $M = \{\sum_{i=1}^{n} x_i s_i : x_i \in R, s_i \in S, n \geq 1\}$*; es decir, si cada elemento de* M *puede ser escrito como una combinación lineal de elementos de* S *con coeficientes en* R.

(ii) ***linealmente independiente*** *si, para cualquier combinación lineal de elementos de* S *con coeficientes en* R*,*

$$r_{i_1} s_{i_1} + r_{i_2} s_{i_2} + ... + r_{i_t} s_{i_t} = 0$$

se tiene $r_{i_1} = r_{i_2} = \cdots = r_{i_t} = 0$;

(iii) ***base*** *de* M *sobre* R *(o una* R*-base) si es un conjunto linealmente independiente y un conjunto de generadores.*

Se dice que M *es un módulo* ***libre*** *si tiene una base.*

Observación 1.2.1. *No todos los* R*-módulos tienen una base. Por ejemplo, en el* $\mathbb{Z}$*-módulo* $\mathbb{Z}_6$*, cada elemento* $\overline{a} \in \mathbb{Z}_6$ *cumple* $6\overline{a} = 0$ *y* $6 \in \mathbb{Z} \setminus \{0\}$*, lo cual demuestra que ningún subconjunto de* $\mathbb{Z}_6$ *es linealmente independiente sobre* $\mathbb{Z}$*, luego este no puede tener una base.*

Definición 1.2.6. *Sea* R *un anillo conmutativo. Se dice que el anillo* A *es una* R***-álgebra*** *si* A *tiene estructura de* R*-módulo y, además,*

$$r(ab) = (ra)b = a(rb), \text{ para todo } r \in R \text{ y todos } a, b \in A.$$

Si A es un anillo con unidad 1, entonces la condición de la definición anterior implica que el conjunto $R \cdot 1$ (que es isomorfo a R) está contenido en el centro de A, es decir, $R \cdot 1 \cong R \subset \mathcal{Z}(A)$.

1.3. Anillos de grupo

Los anillos de grupo son una estructura que como su nombre lo indica, relaciona la teoría de grupos y anillos. Dicha estructura es fundamental para este trabajo.

Considere la siguiente construcción. Sean G un grupo y R un anillo. Se define RG como el conjunto de todas las combinaciones lineales formales,

$$\alpha = \sum_{g \in G} a_g g,$$

donde $a_g \in R$ y $a_g = 0$ casi siempre, es decir, el conjunto

$$supp(\alpha) := \{g \in G : a_g \neq 0\},$$

llamado *soporte* de α, es finito. Explícitamente, el $supp(\alpha)$ es el conjunto de los elementos de G que aparecen en la representación de α. De esta definición sigue que dos elementos, $\alpha = \sum_{g\in G} a_g g$ y $\beta = \sum_{b\in G} b_g g$ en RG son iguales, si y solo si $a_g = b_g$ para todo $g \in G$.

Sean $\alpha = \sum_{g\in G} a_g g$, $\beta = \sum_{g\in G} b_g g \in RG$, la adición y multiplicación en RG, son definidas respectivamente por:

(i) $\alpha + \beta = \sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G} (a_g + b_g) g.$

(ii) $\alpha\beta = \left(\sum_{g\in G} a_g g\right)\left(\sum_{h\in G} b_h h\right) = \sum_{g,h\in G} (a_g b_h)(gh).$

Con estas nociones se obtiene:

Definición 1.3.1. *El conjunto*

$$RG = \left\{ \sum_{g\in G} \alpha_g g : \alpha_g \in R \quad \textit{y} \quad \alpha_g = 0 \quad \textit{casi siempre} \right\},$$

con las operaciones definidas anteriormente, es llamado el ***anillo de grupo*** *de G sobre R. En el caso en que R es conmutativo, RG también es llamado álgebra de grupo de G sobre R.*

Teorema 1.3.1. *RG es un anillo con las operaciones adición y multiplicación definidas anteriormente.*

Demostración. Note que:

(i) De la definición de suma "$+$" en RG y el hecho que $(R, +)$ es un grupo abeliano se tiene que

$$(\alpha+\beta)+\gamma=\alpha+(\beta+\gamma) \quad \text{y} \quad \alpha+\beta=\beta+\alpha, \text{ para todos } \alpha,\beta,\gamma\in RG.$$

Tomando $0_{RG}=\sum_{g\in G}0\cdot g$, para todo $\alpha\in RG$, $0_{RG}+\alpha=\alpha+0_{RG}=\alpha$. Además, si $-\alpha:=\sum_{g\in G}(-a_g)g$ entonces $-\alpha+\alpha=\alpha-\alpha=0_{RG}$. Por tanto, $(RG,+)$ es grupo abeliano.

(ii) Ahora bien, como $(R,\cdot)$ y $(G,\cdot)$ son asociativos, sigue de la definición de producto

" $\cdot$ " en RG, que tal producto es asociativo en RG.

Usando las definiciones de suma "$+$" y producto " $\cdot$ " en RG, para $\alpha,\beta,\gamma\in RG$ se tiene:

$$\begin{aligned}\alpha(\beta+\gamma)=\sum_{g\in G}a_g g\left(\sum_{h\in G}(b_h+c_h)h\right) &= \sum_{g,h\in G}a_g(b_h+c_h)gh\\ &= \sum_{g,h\in G}(a_g b_h)gh+\sum_{g,h\in G}(a_g c_h)gh\\ &= \alpha\beta+\alpha\gamma.\end{aligned}$$

y de manera análoga, $(\alpha+\beta)\gamma=\alpha\gamma+\beta\gamma$, es decir, $(RG,\cdot)$ es un semigrupo.

(iii) Finalmente, $1_{RG}=\sum_{g\in G}a_g g$, donde $a_g=0$ para todo $g\neq 1_G$ y $a_{1_G}=1_R$, es la unidad de RG.

□

Ejemplo 1.3.1. *Sean $C_2=\langle g : g^2=1_{C_2}\rangle$, el grupo cíclico de orden 2 y $\mathbb{Z}_2$, el cuerpo de los enteros módulo 2. El anillo de grupo de C_2 sobre $\mathbb{Z}_2$ es dado por:*

$$\begin{aligned}\mathbb{Z}_2C_2 &= \left\{\sum_{g\in C_2}a_g g : a_g\in\mathbb{Z}_2\right\}\\ &= \{a\cdot 1_{C_2}+b\cdot g : a,b\in\mathbb{Z}_2\}\\ &= \{0_{\mathbb{Z}_2}\cdot 1_{C_2}+0_{\mathbb{Z}_2}\cdot g, 1_{\mathbb{Z}_2}\cdot 1_{C_2}+0_{\mathbb{Z}_2}\cdot g, 0_{\mathbb{Z}_2}\cdot 1_{C_2}+1_{\mathbb{Z}_2}\cdot g, 1_{\mathbb{Z}_2}\cdot 1_{C_2}+1_{\mathbb{Z}_2}\cdot g\}\\ &= \{0,1,g,1+g\},\end{aligned}$$

y se obtienen las siguientes tablas de operaciones:

Tabla 1. Suma en $\mathbb{Z}_2C_2$.

$+$	0	1	g	$1+g$
0	0	1	g	$1+g$
1	1	0	$1+g$	g
g	g	$1+g$	0	1
$1+g$	$1+g$	g	1	0

Tabla 2. Producto en $\mathbb{Z}_2C_2$.

$\cdot$	0	1	g	$1+g$
0	0	0	0	0
1	0	1	g	$1+g$
g	0	g	1	$1+g$
$1+g$	0	$1+g$	$1+g$	0

El producto

$$\begin{aligned} \mu : R \times RG &\longrightarrow RG \\ (r, \alpha) &\longmapsto \sum_{g\in G}(ra_g)g, \end{aligned}$$

enriquece un poco más la estructura de RG, más exactamente, el producto μ da a RG estructura de R-módulo.

En efecto, por la demostración del Teorema 1.3.1, $(RG, +)$ es un grupo abeliano y de la definición de μ, sigue que $r\alpha \in RG$, para todo $r \in R$ y $\alpha \in RG$.

Ahora bien, si $r_1, r_2 \in R$ y $\alpha, \beta \in RG$ se tiene que:

(i) $(r_1 + r_2)\alpha = \sum_{g\in G}(r_1 + r_2)a_g g = \sum_{g\in G} r_1 a_g g + \sum_{g\in G} r_2 a_g g = r_1\alpha + r_2\alpha.$

(ii) $r_1(\alpha+\beta) = r_1 \sum_{g\in G}(a_g+b_g)g = \sum_{g\in G} r_1(a_g+b_g)g = \sum_{g\in G} r_1 a_g g+\sum_{g\in G} r_1 b_g g = r_1\alpha+r_1\beta.$

(iii) $r_1(r_2\alpha) = r_1 \sum_{g\in G}(r_2 a_g)g = \sum_{g\in G}(r_1(r_2 a_g))g = \sum_{g\in G}((r_1 r_2)a_g)g = (r_1 r_2)\alpha.$

(iv) $1_R\alpha = \sum_{g\in G}(1_R a_g)g = \sum_{g\in G} a_g g.$

Observación 1.3.1. *1. Considere la aplicación* ***inclusión****,* $i : G \hookrightarrow RG$*, dada por* $x \longmapsto i(x) = \sum_{g\in G} a_g g$*, donde* $a_x = 1$ *y* $a_g = 0$ *si* $g \neq x$*. Esta aplicación*

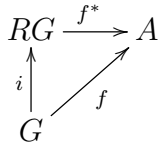
permite ver a G como un subconjunto de RG y por tanto notar que G es una R-base de RG. De esto y de lo anterior es posible afirmar que RG es un R-módulo libre.

Ahora, considere $\nu : R \to RG$ dada por $r \longmapsto \nu(r) = \sum_{g \in G} a_g g$, donde $a_{1_G} = r$ y $a_g = 0$ si $g \neq 1_G$. ν así definido es un monomorfismo de anillos, por lo tanto, R es subanillo de RG.

2. *Como $R \cong R \cdot 1_G$ con la aplicación $r \longmapsto r \cdot 1_G$ y R es subanillo de RG entonces, para todo $r \in R$ y $g \in G$, $gr = rg$, dado que $gr = (1_R g)(r 1_G) = (1_R r)(g 1_G) = rg$. De esto último sigue que para R anillo conmutativo, $R \subset \mathcal{Z}(RG)$, puesto que todo $r \in R$ conmuta con los elementos de la R-base de RG, G, y con los coeficientes de cada elemento de RG.*

La siguiente proposición establece una *propiedad universal* de los anillos de grupo y a su vez puede servir como una definición para estos [6] [1].

Proposición 1.3.1. *Sean G un grupo y R un anillo. Dado cualquier anillo A tal que $R \subset A$ y cualquier aplicación $f : G \longrightarrow A$ tal que $f(gh) = f(g)f(h)$, para todo $g, h \in G$, existe un único homomorfismo de anillos R-lineal $f^* : RG \longrightarrow A$, tal que $f^* \circ i = f$, donde $i : G \hookrightarrow RG$ es la inclusión dada anteriormente, esto es, tal que el siguiente diagrama conmuta:*



El siguiente resultado es un caso especial de la proposición anterior:

---

[6] R. B. DOS SANTOS. “Elementos simétricos sob involuções orientadas em anéis de grupos”. En: (2012).

Corolario 1.3.1. *Sea $f : G \longrightarrow H$ un homomorfimos de grupos. Entonces existe un único homomorfismo de anillos $f^* : RG \longrightarrow RH$ tal que $f^*(g) = f(g)$, para todo $g \in G$. Si f es un monomorfismo (epimorfismo), entonces f^* es un monomorfismo (epimorfismo).*

Teorema 1.3.2. *Sean R un anillo conmutativo con unidad y G, H grupos. Entonces*

$$R(G \times H) \cong (RG)H.$$

Demostración. Considere la aplicación

$$\begin{aligned} \psi : R(G \times H) &\longrightarrow (RG)H \\ \sum_{(g,h)\in G\times H} a_{(g,h)}(g,h) &\longmapsto \sum_{h\in H}\left(\sum_{g\in G} a_{(g,h)}g\right)h. \end{aligned}$$

Se mostrará primero que ψ está bien definida.

Sean $\alpha = \sum_{(g,h)\in G\times H} a_{(g,h)}(g,h)$ y $\beta = \sum_{(g,h)\in G\times H} b_{(g,h)}(g,h)$ en $R(G\times H)$ tales que $\alpha = \beta$, entonces $a_{(g,h)} = b_{(g,h)}$ para todos $g \in G$ y $h \in H$, así,

$$\psi(\alpha) = \sum_{h\in H}\left(\sum_{g\in G} a_{(g,h)}g\right)h = \sum_{h\in H}\left(\sum_{g\in G} b_{(g,h)}g\right)h = \psi(\beta).$$

Además,

$$\begin{aligned} (i)\ \ \psi(\alpha+\beta) &= \sum_{h\in H}\left(\sum_{g\in G}(a_{(g,h)} + b_{(g,h)})g\right)h \\ &= \sum_{h\in H}\left(\sum_{g\in G}(a_{(g,h)})g\right)h + \sum_{h\in H}\left(\sum_{g\in G}(b_{(g,h)})g\right)h = \psi(\alpha) + \psi(\beta), \\ (ii)\ \ \psi(\alpha)\psi(\beta) &= \left[\sum_{h\in H}\left(\sum_{g\in G}(a_{(g,h)})g\right)h\right]\left[\sum_{h_1\in H}\left(\sum_{g_1\in G}(b_{(g_1,h_1)})g_1\right)h_1\right] \\ &= \sum_{h,h_1\in H}\left(\sum_{g,g_1\in G}(a_{(g,h)}b_{(g_1,h_1)})gg_1\right)hh_1 = \psi(\alpha\beta). \end{aligned}$$

Luego ψ es un homomorfismo de anillos.

Para concluir, se demostrará que ψ es biyectiva. Sea $\alpha \in R(G \times H)$, tal que $\psi(\alpha) = 0$, entonces $\sum_{h \in H} \left(\sum_{g \in G} (a_{(g,h)})g \right) h = 0$ y como H es una RG-base para $(RG)H$, sigue que $\sum_{g \in G} (a_{(g,h)})g = 0$, para todo $h \in H$. Además G es una R-base para RG, entonces $a_{(g,h)} = 0$, para todo $g \in G$. Luego $\alpha = 0$, es decir, ψ es inyectiva.

Sea $y \in (RG)H$, como H es una RG-base para $(RG)H$, entonces $y = \sum_{h \in H} \alpha_h h$, donde $\alpha_h \in RG$. Dado que G es una R-base de RG, para $h \in H$, $\alpha_h = \sum_{g \in G} a_{(g,h)} g$. Considere $x = \sum_{(g,h) \in G \times H} a_{(g,h)}(g,h) \in R(G \times H)$, entonces $\psi(x) = \sum_{h \in H} \left(\sum_{g \in G} (a_{(g,h)}g \right) h = \sum_{h \in H} \alpha_h h = y$. Por lo tanto, ψ es sobreyectiva. □

Corolario 1.3.2. *Sean R un anillo conmutativo con unidad y G, H grupos. Entonces*

$$R(G \times H) \cong (RH)G.$$

Demostración. Es conocido que $(G \times H)$ y $(H \times G)$ son grupos isomorfos, así por el Corolario 1.3.1, sigue que $R(G \times H) \cong R(H \times G)$ y del Teorema 1.3.2, $R(H \times G) \cong (RH)G$. Por lo tanto $R(G \times H) \cong (RH)G$. □

Teniendo presente el concepto de *clase de conjugación*, Definición 1.1.13, se introducen los siguientes elementos destacados.

Definición 1.3.2. *Sean G un grupo, R un anillo conmutativo, RG el anillo de grupo de G sobre R y $\{C_i\}_{i \in I}$ el conjunto de las clases de conjugación de G que contienen solo un número finito de elementos. Para cada índice $i \in I$, escriba $c_i = \sum_{x \in C_i} x \in RG$. Estos elementos son llamados* ***sumas de clases*** *de G sobre R.*

El siguiente resultado permite dar una descripción del centro de un anillo de grupo RG, información de interés para determinar la estructura de anillos de grupo semisimples.

Teorema 1.3.3. *Sean G un grupo y R un anillo conmutativo. Entonces el conjunto $\{c_i\}_{i\in I}$ de todas las sumas de clases de G sobre R es una R-base de $\mathcal{Z}(RG)$.*

Demostración. Sea $g \in G$ arbitrario, entonces $g^{-1}c_i g = \sum_{x\in C_i} g^{-1}xg = \sum_{y\in C_i} y = c_i$ puesto que $g^{-1}C_i g = C_i$, para todos $i \in I$ y $g \in G$, como se observó en la Definición 1.1.13. Luego, $c_i g = gc_i$, para todo $g \in G$, así, como G es base para RG y R es conmutativo, sigue que $c_i \in \mathcal{Z}(RG)$, para todo $i \in I$.

Ahora se mostrará que estos elementos son linealmente independientes. Sean $r_i \in R$ tales que $\sum_{i\in I} r_i c_i = 0$, es decir, $\sum_{i\in I} r_i \sum_{x\in C_i} x = 0$. Puesto que la conjugación en G es una relación de equivalencia entonces, sumas de clases diferentes poseen soportes disjuntos y como G es base para RG, la independencia lineal de los elementos en G implica que $r_i = 0$, para todo $i \in I$.

Finalmente, suponga $\alpha = \sum_{g\in G} a_g g \in \mathcal{Z}(RG)$. Si $k \in supp(\alpha)$, entonces cualquier otro elemento h en la clase de conjugación de k, $C(k)$, también pertenece al $supp(\alpha)$. En efecto, si $h = x^{-1}kx$ para algún $x \in G$, por ser α central, se tiene que $\alpha = x^{-1}\alpha x$, es decir,

$$\sum_{g\in G} a_g g = \sum_{g\in G} a_g x^{-1}gx.$$

Comparando el coeficiente de h en ambos lados de la última expresión, se obtiene que $a_h = a_k$, luego $h \in supp(\alpha)$. Esto muestra que se pueden factorizar los coeficientes de los elementos en cada clase de conjugación y escribir

$$\alpha = \sum_{i\in I} a_i c_i.$$

Luego, $\{c_i\}_{i\in I}$ es también un conjunto de generadores para $\mathcal{Z}(RG)$, por lo tanto, $\{c_i\}_{i\in I}$ es una R-base de $\mathcal{Z}(RG)$. □

Se concluye esta sección mostrando que los anillos de grupo sobre anillos conmutativos son anillos con involución.

Proposición 1.3.2. *Sea R un anillo conmutativo. La aplicación $* : RG \longrightarrow RG$ dada por*

$$\alpha^* = \left(\sum_{g\in G} a_g g\right)^* = \sum_{g\in G} a_g g^{-1},$$

es un antihomomorfismo de orden 2, es decir:

(i) $(\alpha+\beta)^* = \alpha^* + \beta^*$,

(ii) $(\alpha\beta)^* = \beta^*\alpha^*$,

(iii) $(\alpha^*)^* = \alpha$.

Demostración. Sean α y $\beta \in RG, entonces$

$$(i)\ (\alpha+\beta)^* = \left(\sum_{g\in G}(a_g+b_g)g\right)^* = \sum_{g\in G}(a_g+b_g)g^{-1}$$
$$= \sum_{g\in G} a_g g^{-1} + \sum_{g\in G} b_g g^{-1}$$
$$= \left(\sum_{g\in G} a_g g\right)^* + \left(\sum_{g\in G} b_g g\right)^* = \alpha^* + \beta^*.$$

$$(ii)\ (\alpha\beta)^* = \left(\sum_{g,h\in G}(a_g b_h)(gh)\right)^* = \sum_{g,h\in G}(a_g b_h)(gh)^{-1}$$
$$= \sum_{g,h\in G}(b_h a_g)h^{-1}g^{-1}$$
$$= \left(\sum_{h\in G} b_h h^{-1}\right)\left(\sum_{g\in G} a_g g^{-1}\right)$$
$$= \left(\sum_{h\in G} b_h h\right)^*\left(\sum_{g\in G} a_g g\right)^* = \beta^*\alpha^*.$$

$$(iii)\ (\alpha^*)^* = \left(\sum_{g\in G} a_g g^{-1}\right)^* = \sum_{g\in G} a_g (g^{-1})^{-1} = \sum_{g\in G} a_g g = \alpha.$$

□

Note que la involución en RG, es dada por la involución clásica en G y la involución identidad en R.

2. LC-grupos y SLC-grupos

En este capítulo se estudiará una clase especial de grupos, los así llamados SLC-grupos, que se definirán posteriormente. Antes de entrar en su estudio se introducirá brevemente la teoría de anillos alternativos y loops, en particular, loops de Moufang que serán necesarios para el entendimiento del teorema en que se desprende este tipo de grupos.

2.1. Anillos alternativos

En todo anillo no necesariamente asociativo $\mathcal{R}$ son definidas dos funciones muy importantes (lineales de sus argumentos), llamadas *conmutador* y *asociador*, dadas respectivamente por:

$$[a,b] = ab - ba \quad \text{y} \quad [a,b,c] = (ab)c - a(bc).$$

Definición 2.1.1. *Un anillo R es **alternativo** si satisface las siguientes identidades*

$$[x,x,y] = 0\text{, identidad alternativa a izquierda}$$

y

$$[y,x,x] = 0\text{, identidad alternativa a derecha,}$$

para todos $x, y \in R$.

De la definición, sigue que todo anillo asociativo es alternativo. En general, la recíproca no es cierta. Por ejemplo, considerando el álgebra de los cuaternios reales,

$$\mathcal{H}_{\mathbb{R}} = \{a + bi + cj + dk : a,b,c \in \mathbb{R};\ i,j,k \quad \text{símbolos formales}\},$$

con la suma " $+$ " usual y la multiplicación " $\times$ " dada por la distributividad y el producto de los elementos base i, j, k, ver la Tabla 3,

Tabla 3. Multiplicación en $\mathcal{H}_{\mathbb{R}}$.

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

se construye el anillo de los ***números de Cayley***

$$\mathcal{C} = \mathcal{C}(\mathcal{H}_{\mathbb{R}}) = \{a + bl : a, b \in \mathcal{H}_{\mathbb{R}}; l \quad \text{símbolo formal}\},$$

también con la suma " $+$ " usual y la multiplicación " $\times$ " dada por

$$(a + bl)(c + dl) = (ac - \overline{d}b) + (da + b\overline{c})l,$$

donde para $q \in \mathcal{H}_{\mathbb{R}}$, $\overline{q} = q_0 - q_1 i - q_2 j - q_3 k$, denota su conjugado. Este es un anillo alternativo que no es asociativo, como se verá en el Ejemplo 2.2.1.

Proposición 2.1.1. *Todo anillo alternativo satisface la identidad flexible,* $[x, y, x] = 0$*, para cualesquiera* x, y*.*

Demostración. Cambiando x por $x+z$ en la identidad alternativa a izquierda, y usando el hecho de que el asociador es una función lineal de cada uno de sus argumentos, se obtiene:

$$0 = [x + z, x + z, y] = [x, x, y] + [x, z, y] + [z, x, y] + [z, z, y].$$

Por hipótesis, el anillo es alternativo, luego $[x, x, y] = [z, z, y] = 0$, lo que implica que $[x, z, y] = -[z, x, y]$. Análogamente, cambiando y por $y + z$ en la identidad alternativa

a derecha, sigue que $[x, y, z] = -[x, z, y]$, por lo tanto $[x, y, z] = [z, x, y]$. En particular, $[x, y, x] = [x, x, y] = 0$. □

Los anillos alternativos derivan su nombre del hecho que en un anillo alternativo, el asociador es una función alternante, esto es, para cualquier permutación σ sobre el conjunto $\{1, 2, 3\}$, el asociador verifica que $[a_{\sigma(1)}, a_{\sigma(2)}, a_{\sigma(3)}] = sgn(\sigma)[a_1, a_2, a_3]$, donde

$$sgn(\sigma) = \begin{cases} 1, & \text{si } \sigma \text{ es par,} \\ -1, & \text{si } \sigma \text{ es impar.} \end{cases}$$

El siguiente resultado contiene algunas identidades válidas en todo anillo alternativo.

Teorema 2.1.1. *En todo anillo alternativo, las siguientes identidades son válidas para cualesquiera* x, y, z*:*

(i) $[x^2, y, z] = x[x, y, z] + [x, y, z]x$

(ii) $[xy, x, z] = [y, x, z]x$

(iii) $[yx, x, z] = x[y, x, z]$

(iv) $((xy)x)z = x(y(xz))$*, identidad de Moufang a izquierda*

(v) $((xy)z)y = x(y(zy))$*, identidad de Moufang a derecha*

(vi) $(xy)(zx) = (x(yz))x$*, identidad media de Moufang.*

Demostración. La demostración de las tres primeras identidades, puede ser consultada en [2]. Únicamente se demostrará la identidad (iv), *identidad de Moufang a izquierda*, dado que posteriormente se establecerá que (iv), (v) y (vi) son equivalentes.

En efecto, sumando y restando $(xy)(xz)$ a la diferencia $((xy)x)z - x(y(xz))$, se obtiene

$$\begin{aligned} ((xy)x)z - x(y(xz)) &= \underbrace{((xy)x)z - (xy)(xz)}_{\text{Def. asociador}} + \underbrace{(xy)(xz) - x(y(xz))}_{\text{Def. asociador}} \\ &= \quad [xy, x, z] \quad + \quad [x, y, xz]. \end{aligned} \tag{1}$$

Por (ii), $[xy, x, z] = [y, x, z]x$ y usando la permutación par (123) y (ii), se tiene que $[x, y, xz] = [xz, x, y] = [z, x, y]x$. Regresando a (1),

$$[xy, x, z] + [x, y, xz] = [y, x, z]x + [z, x, y]x.$$

y con la permutación impar $(13)(2)$ se obtiene: $[y, x, z] = -[z, x, y]$. Por lo tanto,

$$[xy, x, z] + [x, y, xz] = -[z, x, y]x + [z, x, y]x = 0,$$

lo cual implica que $((xy)x)z - x(y(xz)) = 0$, como se requería. □

2.2. Loops

Definición 2.2.1. *Un loop es un par $(L, \cdot)$, donde L es un conjunto no vacío, $(a, b) \mapsto a \cdot b$ es una operación binaria cerrada en L que posee un elemento identidad bilateral, tal que las ecuaciones $a \cdot x = b$ e $y \cdot a = b$ tienen soluciones únicas x e y en L, para todos $a, b \in L$.*

De ahora en adelante, se omitirá la notación de la operación binaria del loop y se escribirá únicamente "el loop L" en lugar de "el loop $(L, \cdot)$". También, se escribirá ab en lugar de $a \cdot b$ para denotar la operación de los elementos en un loop.
Es claro que todo grupo es un ejemplo de un loop. A continuación se presenta un ejemplo de un loop que no es grupo.

Ejemplo 2.2.1. *(Loop de Cayley)*

Sea $\mathcal{B}_{\mathcal{C}} = \{1, i, j, k, l, il, jl, kl\}$ *la base usual de los números de Cayley,* $\mathcal{C}$*. Usando las relaciones*

- $al \cdot bl = -\bar{b}a$*,*
- $a \cdot bl = (ba)l$*,*
- $al \cdot b = (a\bar{b})l$*,*

para $a, b \in \{\pm 1, \pm i, \pm j, \pm k\}$*, se obtiene la siguiente tabla de multiplicación*

Tabla 4. Multiplicación en $\mathcal{B}_{\mathcal{C}}$.

$\cdot$	1	i	j	k	l	il	jl	kl
1	1	i	j	k	l	il	jl	kl
i	i	-1	k	$-j$	il	$-l$	$-kl$	il
j	j	$-k$	-1	i	jl	kl	$-l$	$-il$
k	k	j	$-i$	-1	kl	$-jl$	il	$-l$
l	l	$-il$	$-jl$	$-kl$	-1	i	j	k
il	il	l	$-kl$	jl	$-i$	-1	$-k$	j
jl	jl	kl	l	$-il$	$-j$	k	-1	$-i$
kl	kl	$-jl$	il	l	$-k$	$-j$	i	-1

del loop $L = M_{16}(\mathcal{Q}_8) = \{\pm 1, \pm i, \pm j, \pm k \pm l, \pm il, \pm jl, \pm kl\}$*, que no es un grupo puesto que,* $(ik)l = -jl \neq jl = i(kl)$.

Definición 2.2.2. *Un loop* L *tiene* ***la propiedad del inverso*** *si todo* $x \in L$ *tiene un único inverso bilateral, que se denotará por* x^{-1}*, y si, todos* $x, y \in L$ *satisfacen*

$$x^{-1}(xy) = y, \text{ propiedad del inverso a izquierda}$$

y

$$(yx)x^{-1} = y, \text{ propiedad del inverso a derecha.}$$

El loop de Cayley es un ejemplo de un loop que tiene la propiedad del inverso.

Proposición 2.2.1. *Si L es un loop con la propiedad del inverso. Entonces,*

$$(xy)^{-1} = y^{-1}x^{-1}.$$

Demostración. Sea $z = xy$, por la propiedad del inverso $zy^{-1} = x$, luego $y^{-1} = z^{-1}x$, por lo tanto, $z^{-1} = y^{-1}x^{-1}$. □

2.2.1. Loops de Moufang En este trabajo, todo loop será un loop de Moufang. Dichos loops llevan este nombre en honor a Ruth Moufang, quien los introdujo en un contexto geométrico en 1935, [2].

El siguiente resultado es esencial para la próxima definición y su demostración completa puede consultarse en [2].

Teorema 2.2.1. *En todo loop L, las siguientes identidades son equivalentes, para todo x, y, z:*

(i) $((xy)x)z = x(y(xz))$*, identidad de Moufang a izquierda*

(ii) $((xy)z)y = x(y(zy))$*, identidad de Moufang a derecha*

(iii) $(xy)(zx) = (x(yz))x$*, identidad media de Moufang.*

Si L es un loop que satisface cualquiera de las identidades anteriores, entonces L es un loop con la propiedad del inverso que también satisface las identidades alternativas y la identidad flexible, Definición 2.1.1 y Proposición 2.1.1.

Demostración. Suponga que L satisface la identidad de Moufang a izquierda. Tomando $z = 1$ en esta identidad, se obtiene la identidad flexible, $(xy)x = x(yx)$. En particular, siendo x^λ, x^ρ los inversos a izquierda y a derecha de x, respectivamente, sigue que $(xx^\lambda)x = x(x^\lambda x) = x$, luego $xx^\lambda = 1$ y así de la unicidad de los inversos, $x^\lambda = x^\rho$, es decir, x tiene un único inverso bilateral, x^{-1}. Al tomar $x = y^{-1}$ en (i) se obtiene $y^{-1}z = y^{-1}(y(y^{-1}z))$, para todos y, z. Por definición de loop, para todos

$y, w \in L$, la ecuación $y^{-1}z = w$ tiene solución para z. Luego $w = y^{-1}(yw)$ y se obtiene la propiedad del inverso a izquierda. Tomando $z = x^{-1}$ en (i) se obtiene la propiedad del inverso a derecha, $((xy)x)x^{-1} = xy$. Por lo tanto, L es un loop con la propiedad del inverso. Ahora, con $y = 1$ en (i) se obtiene la identidad alternativa a izquierda y así $(x(xz))^{-1} = (x^2z)^{-1}$, luego por la Proposición 2.2.1, $(z^{-1}x^{-1})x^{-1} = z^{-1}(x^{-1}x^{-1})$, lo cual implica la identidad alternativa a derecha.

$(i) \Rightarrow (iii)$ Reemplazando z por $x^{-1}z$ en (i), se tiene $((xy)x)(x^{-1}z) = x(yz)$ y tomando el inverso en cada lado de (i) se obtiene la identidad de Moufang a derecha, luego L satisface (ii), entonces

$$\begin{aligned}
(x(yz))x &= [((xy)x)(x^{-1}z)]x \\
&= (xy)[x((x^{-1}z)x)] \quad \text{Identidad de Moufang a derecha} \\
&= (xy)[(x(x^{-1}z))x] \quad \text{Identidad flexible} \\
&= (xy)(zx).
\end{aligned}$$

Por lo tanto, L satisface la identidad media de Moufang.

Para demostrar las implicaciones $(iii) \Rightarrow (ii)$ y $(ii) \Rightarrow (i)$ y concluir en cada caso que L satisface las identidades alternativas, la identidad flexible y la propiedad del inverso, se usan argumentos similares a los anteriores. □

Definición 2.2.3. *Un loop L es llamado un **loop de Moufang** si satisface alguna de las tres identidades (equivalentes) de Moufang.*

Ejemplos de loops de Moufang

Ejemplo 2.2.2. *Como el anillo de los números de Cayley, $\mathcal{C}$, es un anillo alternativo, sigue del Teorema 2.1.1 que este anillo verifica las identidades de Moufang. El loop de Cayley, $M_{16}(\mathcal{Q}_8)$, está contenido en $\mathcal{C}$, por lo tanto es un loop de Moufang.*

Ejemplo 2.2.3. *Sea G un grupo no abeliano, $g_0 \in G$ un elemento central, $g \mapsto g^*$ una involución en G tal que $g_0^* = g_0$ y $gg^* \in \mathcal{Z}(G)$, para todo $g \in G$. Sea u un símbolo. Defina $L = G \dot{\cup} Gu$ (unión disjunta) y extienda la operación de G a L por las reglas:*

$$\begin{aligned} g(hu) &= (hg)u, \\ (gu)h &= (gh^*)u, \\ (gu)(hu) &= g_0 h^* g, \end{aligned} \tag{2}$$

para todo $g, h \in G$. Para ver que L con la operación definida es un loop de Moufang se mostrará inicialmente que L es un loop. Note que la operación binaria definida anteriormente es cerrada en L, además L posee el elemento 1_G como identidad bilateral.

Sean $gu, hu \in L$, entonces existe un único elemento $x \in L$ tal que $gu \cdot x = hu$. En efecto, para que esta igualdad se cumpla x debe pertenecer a G, de lo contrario si $x \in Gu$ entonces $gu \cdot x \in G$ y $G \cap Gu = \emptyset$. Así $x \in G$ y por (2) sigue que

$$gu \cdot x = hu \;\Rightarrow\; (gx^*)u = hu \;\Rightarrow\; gx^* = h \;\Rightarrow\; x^* = g^{-1}h \;\Rightarrow\; x = (g^{-1}h)^*.$$

Ahora, dados $gu, h \in L$, el elemento x que satisface $gu \cdot x = h$ debe pertenecer a Gu y utilizando las ecuaciones (2) se obtiene que $x = (hg_0^{-1}g^{-1})^*u$. Si $g, hu \in L$, entonces $x = (hg^{-1})u$ es tal que $g \cdot x = hu$. Con esto, se probó que dados $a, c \in L$ existe un único $b \in L$ tal que $a \cdot b = c$. Análogamente se muestra que dados $b, c \in L$ existe un único $a \in L$ tal que $b \cdot a = c$. De esto se concluye que L es un loop. Sin embargo, L no es grupo. En efecto, si L fuese grupo, entonces, para todos $g, h \in G$, $(gh)u = g(hu) = (hg)u$, esto implica que $gh = hg$, es decir, G es abeliano, lo que contradice la hipótesis sobre G. Luego, la condición de que G sea no abeliano, implica que L es no asociativo.

Ahora se probará que L satisface la identidad de Moufang a izquierda. Para esto, existen 2 posibilidades para cada elemento, es decir, $x = g$ o $x = gu$, $y = h$ o

$y = hu$ *y* $z = m$ *o* $z = mu$*, con* $g, h, m \in G$*, lo que da un total de* 8 *posibilidades. Se mostrarán solamente* 3 *de ellas, ya que las otras son análogas.*
Suponga que $x = gu$*,* $y = hu$ *y* $z = mu$*, entonces*

$$\begin{aligned}((gu \cdot hu)gu)mu &= ((g_0h^*g)gu)mu \\ &= ((gg_0h^*g)u)mu \\ &= g_0m^*gg_0h^*g \\ &= g_o^2m^*gh^*g\end{aligned} \qquad \textit{y} \qquad \begin{aligned}gu(hu(gu \cdot mu)) &= gu(hu(g_0m^*g)) \\ &= gu(h(g_0m^*g)^* \cdot u) \\ &= g_0g_0m^*gh^*g \\ &= g_o^2m^*gh^*g.\end{aligned}$$

Ahora, suponga que $x = gu$*,* $y = h$ *y* $z = mu$*. Así*

$$\begin{aligned}((gu \cdot h)gu)mu &= ((gh^*)u \cdot gu)mu \\ &= (g_0g^*gh^*)mu \\ &= (mg_0g^*gh^*)u\end{aligned} \qquad \textit{y} \qquad \begin{aligned}gu(h(gu \cdot mu)) &= gu(hg_0m^*g) \\ &= (g(hg_0m^*g)^*)u \\ &= (gg^*mg_o^*h^*)u.\end{aligned}$$

Como gg^* *es central,* g *conmuta con* g^**, además* $g_0 = g_0^*$*, por lo tanto las dos ecuaciones anteriores son iguales.*
Si $x = gu$*,* $y = h$ *y* $z = m$*, se tiene que*

$$\begin{aligned}((gu \cdot h)gu)m &= ((gh^*)u \cdot gu)m \\ &= (g_0g^*gh^*)m \\ &= g_0g^*gh^*m\end{aligned} \qquad \textit{y} \qquad \begin{aligned}gu(h(gu \cdot m)) &= gu(h \cdot (gm^*)u) \\ &= gu((gm^*h)u) \\ &= g_oh^*mg^*g.\end{aligned}$$

Como gg^* *es central en* G *sigue que* g *conmuta con* g^* *y se obtiene la igualdad. De esto se concluye que* L *satisface la identidad a izquierda de Moufang. Por lo tanto,* L *es un loop de Moufang. Este loop es denotado* $M(G, *, g_o)$ *y será de gran importancia en este trabajo.*

El menor loop de Moufang que no es grupo es $M(S_3, *, 1)$, donde S_3 es el grupo

simétrico de orden 6 y la involución en S_3 es dada por $g^* = g^{-1}$, para todo $g \in S_3$ [7]. Note que si $G = \mathcal{Q}_8$ y $g^* = g^{-1}$, entonces $M(\mathcal{Q}_8, *, -1)$ es el loop de Cayley, donde u es el elemento l del Ejemplo 2.2.1.

El siguiente resultado proporciona condiciones equivalentes para que el anillo de loop, del loop Moufang, $L = M(G, *, g_0)$, sea un anillo alternativo. Su demostración puede ser consultada en [2].

Teorema 2.2.2. *(Anillos de loop alternativos) Sea R un anillo conmutativo, asociativo y con unidad y sea $L = M(G, *, g_0)$ un loop de Moufang construido a partir de un grupo no abeliano G. Las siguientes implicaciones son equivalentes:*

(i) RL *es alternativo*

(ii) $g + g^* \in \mathcal{Z}(RG)$*, para todo* $g \in G$.

(iii) *Si* $car(R) \neq 2$*, entonces para cada* $g \in G$*,* $h^{-1}gh \in \{g, g^*\}$ *para todo* $h \in G$*; si* $car(R) = 2$*, entonces, para cada* $g \in G$*, o* $g = g^*$ *o* $h^{-1}gh \in \{g, g^*\}$ *para todo* $h \in G$.

Será de particular interés para el estudio de los SLC-grupos el ítem (iii), en el caso especial que $*$ es la función inversa en un grupo no abeliano y la característica del anillo es diferente de 2.

2.3. LC-grupos y SLC-grupos

Definición 2.3.1. *Un grupo no abeliano G posee la propiedad de **"ausencia de conmutatividad"**, que se denotará por **LC** (del inglés, lack commutativity), si para cualquier par de elementos $g, h \in G$, $gh = hg$ si, y solo si, $g \in \mathcal{Z}(G)$ o $h \in \mathcal{Z}(G)$ o $gh \in \mathcal{Z}(G)$.*

---

[7] O. CHEIN y PFLUGFELDER H. O. "The smallest Moufang loop". En: *Archiv der Mathematik* 22.1 (1971), págs. 573-576.

Observación 2.3.1. *De la definición anterior es un hecho que los cuadrados son centrales en los grupos LC. Por lo tanto, los conmutadores también son centrales puesto que* $(g,h) = g^{-1}h^{-1}gh = g^{-1}(g^{-1}g)h^{-1}g(h^{-1}h)h = g^{-2}(gh^{-1})^2h^2$*, para todos* $g, h \in G$*.*

Definición 2.3.2. *Sea* G *un grupo no abeliano. Se dice que un elemento* $s \in G$ *es el único conmutador no trivial de* G *si* $s \neq 1$ *y para todos* $x, y \in G$, $(x,y) \in \{1, s\}$.

A continuación se presenta el grupo cuaternio de orden 8, $\mathcal{Q}_8$, el cual no solo muestra la validez de la Definición 2.3.1, sino que además es un grupo que aparece repetidamente en el estudio de anillos de grupo, [3].

Ejemplo 2.3.1. *1. Considere el grupo cuaternio,* $\mathcal{Q}_8$*, con presentación*

$$\mathcal{Q}_8 = \langle x, y : x^4 = 1, x^2 = y^2, x^y = x^{-1} \rangle = \{1, x, x^2, x^3, y, xy, x^2y, x^3y\},$$

donde $x^y = y^{-1}xy$*, es decir, conjugar a* x *por* y*. Su tabla de multiplicación es:*

Tabla 5. Multiplicación en $\mathcal{Q}_8$.

$\cdot$	1	x	x^2	x^3	y	xy	x^2y	x^3y
1	1	x	x^2	x^3	y	xy	x^2y	x^3y
x	x	x^2	x^3	1	xy	x^2y	x^3y	y
x^2	x^2	x^3	1	x	x^2y	x^3y	y	xy
x^3	x^3	1	x	x^2	x^3y	y	xy	x^2y
y	y	x^3y	x^2y	xy	x^2	x	1	x^3
xy	xy	y	x^3y	x^2y	x^3	x^2	x	1
x^2y	x^2y	xy	y	x^3y	1	x^3	x^2	x
x^3y	x^3y	x^2y	xy	y	x	1	x^3	x^2

De la tabla anterior se verifica que $\mathcal{Z}(\mathcal{Q}_8) = \{1, x^2\}$ *y que* $\mathcal{Q}_8$ *es un LC-grupo.*

Además, $\mathcal{Z}(\mathcal{Q}_8) = \mathcal{Q}_8' = \{1, x^2\}$*, donde* $\mathcal{Q}_8'$ *denota el subgrupo conmutador. En efecto, para* $1 \leq j, k \leq 4$ *y* $0 \leq i \leq 1$

- $(1, x^j y^i) = (x^j y^i)^{-1} x^j y^i = y^{-i} x^{-j} x^j y^i = 1$.
- $(x^k, x^j) = x^{-k} x^{-j} x^k x^j = 1$.
- $(x, x^j y) = x^{-1} y^{-1} x^{-j} x x^j y = x^{-1} y^{-1} x y = x^{-1} x^{-1} = x^{-2} = x^2$.
- $(x^2, x^j y) = 1$*, puesto que* $x^2 \in \mathcal{Z}(\mathcal{Q}_8)$.
- $(x^3, x^j y) = x^{-3} y^{-1} x^{-j} x^3 x^j y = x^{-3} y^{-1} x^3 y = x^{-3} x^{-3} = xx = x^2$.
- $(y, x^j y) = y^{-1} y^{-1} x^{-j} y x^j y = y^{-1} x^j x^j y = y^{-1} x^{2j} y = x^{-2j}$*, para* $j = 1, 3$ *se obtiene* $(y, x^j y) = x^2$ *y para* $j = 2, 4$ *se obtiene* $(y, x^j y) = 1$.
- $(xy, x^2 y) = y^{-1} x^{-1} y^{-1} x^{-2} x y x^2 y = y^{-1} x^{-1} y^{-1} x^{-1} y x^2 y = y^{-1} x^{-1} x y x^2 = x^2$.
- $(xy, x^3 y) = y^{-1} x^{-1} y^{-1} x^{-3} x y x^3 y = y^{-1} x^{-1} x^2 x^3 y = 1$.
- $(x^2 y, x^3 y) = y^{-1} x^{-2} y^{-1} x^{-3} x^2 y x^3 y = y^{-1} x^{-2} x x^3 y = x^{-2} = x^2$.

2. *Sea* $\mathcal{D}_4 = \langle a, b : a^4 = 1 = b^2, a^b = a^{-1} \rangle$ *el grupo diedral de orden* 8*. Como en el ejemplo anterior se puede verificar que* $\mathcal{Z}(\mathcal{D}_4) = \mathcal{D}_4' = \{1, a^2\}$ *y que* $\mathcal{D}_4$ *es un LC-grupo.*

Observe que la propiedad LC no caracteriza los grupos, en el sentido que dos o más grupos pueden tener el mismo orden y satisfacer la propiedad LC, pero no necesariamente son isomorfos, como lo evidencian $\mathcal{Q}_8$ y $\mathcal{D}_4$ que son LC-grupos y además tienen un único conmutador no trivial $s = x^2 \neq 1$ y $s = a^2 \neq 1$, respectivamente.

El siguiente ejemplo muestra que la condición de tener un único conmutador no trivial es independiente de la condición de tener la propiedad LC.

Ejemplo 2.3.2. *Sea* G *un grupo con la siguiente presentación:*

$$G = \langle x_1, x_2, x_3 \mid {x_i}^4 = ({x_i}^2, x_j) = ((x_i, x_j), x_k) = 1; \;\; \textit{i, j, k distintos} \rangle.$$

Afirmación 1: *$G/\mathcal{Z}(G)$ tiene exponente 2.*

De la presentación de G se tiene que los cuadrados y conmutadores son centrales. Sea $g \in G$ un elemento arbitrario, entonces g es de la forma

$$g = x_{i_1}^{\delta_{i_1}} x_{i_2}^{\delta_{i_2}} \cdots x_{i_r}^{\delta_{i_r}},$$

con $x_{i_j} \in \{x_1, x_2, x_3\}$ y $\delta_{i_j} = \pm 1$. Luego,

$$g^2 = x_{i_1}^{\delta_{i_1}} x_{i_2}^{\delta_{i_2}} \cdots x_{i_r}^{\delta_{i_r}} x_{i_1}^{\delta_{i_1}} x_{i_2}^{\delta_{i_2}} \cdots x_{i_r}^{\delta_{i_r}}.$$

Como $(a,b) = a^{-1}b^{-1}ab$, se tiene que $ab = ba(a,b)$, así

$$\begin{aligned} g^2 &= x_{i_1}^{\delta_{i_1}} x_{i_2}^{\delta_{i_2}} \cdots (x_{i_r}^{\delta_{i_r}} x_{i_1}^{\delta_{i_1}}) x_{i_2}^{\delta_{i_2}} \cdots x_{i_r}^{\delta_{i_r}} \\ &= x_{i_1}^{\delta_{i_1}} x_{i_2}^{\delta_{i_2}} \cdots x_{i_1}^{\delta_{i_1}} x_{i_r}^{\delta_{i_r}} (x_{i_r}^{\delta_{i_r}}, x_{i_1}^{\delta_{i_1}}) x_{i_2}^{\delta_{i_2}} \cdots x_{i_r}^{\delta_{i_r}} \\ &= x_{i_1}^{\delta_{i_1}} x_{i_2}^{\delta_{i_2}} \cdots x_{i_1}^{\delta_{i_1}} x_{i_r}^{\delta_{i_r}} x_{i_2}^{\delta_{i_2}} \cdots x_{i_r}^{\delta_{i_r}} (x_{i_r}^{\delta_{i_r}}, x_{i_1}^{\delta_{i_1}}), \end{aligned}$$

donde la última igualdad se obtiene del hecho que $(x_{i_r}^{\delta_{i_r}}, x_{i_1}^{\delta_{i_1}}) \in \mathcal{Z}(G)$. Repitiendo este proceso un número finito de veces, se obtiene

$$g^2 = (x_{i_1}^{\delta_{i_1}})^2 (x_{i_2}^{\delta_{i_2}})^2 \cdots (x_{i_r}^{\delta_{i_r}})^2 z_{i_1} z_{i_2} \cdots z_{i_r}, \text{ con } z_{i_j} \in \mathcal{Z}(G).$$

Por lo tanto $g^2 \in \mathcal{Z}(G)$, lo cual implica que $\overline{g}^2 = g^2\mathcal{Z}(G) = \mathcal{Z}(G) = \overline{1}$.

Afirmación 2: *Dos elementos no centrales $g, h \in G$ conmutan si y solo si, $g, h \in x_i\mathcal{Z}(G)$, es decir, si están en la misma clase lateral del centro de G.*

Suponga que $g, h \notin \mathcal{Z}(G)$, pero g y h conmutan. Si $g = x_i z_1$ y $h = x_j z_2$, con $i \neq j$ y $z_1, z_2 \in \mathcal{Z}(G)$, entonces por hipótesis, $x_i z_1 x_j z_2 = x_j z_2 x_i z_1$ y así $x_i x_j = x_j x_i$, lo cual es una contradicción, puesto que los únicos elementos centrales en G son cuadrados y conmutadores de los generadores.

Recíprocamente, si $g, h \in x_i\mathcal{Z}(G)$ *entonces* $g = x_i z_1$ *y* $h = x_i z_2$ *con* $z_1, z_2 \in \mathcal{Z}(G)$*, así*

$$gh = x_i z_1 x_i z_2 = x_i z_2 x_i z_1 = hg.$$

En este caso, $gh = x_i^2 z_2 z_1 \in \mathcal{Z}(G)$*. Esto es,* G *tiene la propiedad* LC*.*
Por otro lado, G *posee* 3 *conmutadores no triviales* (x_1, x_2)*,* (x_1, x_3) *y* (x_2, x_3)*.*

El siguiente resultado caracteriza los grupos no abelianos, que tienen una involución que satisface (iii) del Teorema 2.2.2, en el caso que R tiene característica diferente de 2.

Teorema 2.3.1. *Sea* G *un grupo no abeliano. Entonces* G *tiene una involución* $g \longmapsto g^*$ *con la propiedad que* $h^{-1}gh \in \{g, g^*\}$ *para todos* $g, h \in G$ *si, y solo si,* G *tiene la propiedad LC y un único conmutador no trivial. Para tal grupo la involución es dada por:*

$$g^* = \begin{cases} g, & \textit{si } g \textit{ es central}, \\ sg, & \textit{otro caso}, \end{cases} \tag{3}$$

donde s *es el único conmutador no trivial en* G*.*

Demostración. Suponga primero que G tiene un único conmutador $s \neq 1$, entonces $s^{-1} \neq 1$ y también es conmutador, pero como s es el único conmutador no trivial sigue que $s = s^{-1}$, luego $s^2 = 1$. Además, si $gs \neq sg$ para algún $g \in G$, entonces $gs = (sg)s$, luego $g = sg$ y $s = 1$, contradicción. Por lo tanto, s *es central y de orden* 2.
Defina g^* por (3). Entonces, si g es central $(g^*)^* = g^* = g$ y si g no es central $(g^*)^* = (sg)^* = s^2 g = g$ ya que $s^2 = 1$. Luego $(g^*)^* = g$, para cualquier $g \in G$.
Ahora suponga también que G tiene la propiedad LC. Se mostrará que $g \longmapsto g^*$ es un antihomomorfismo (y por lo tanto una involución) considerando 2 casos:

Caso 1: $gh \neq hg$**.**

En este caso $hg = sgh$, además ni g, ni h ni gh son centrales (de serlo se obtendría que $gh = hg$), luego

$$h^*g^* = (sh)(sg) = hg = sgh = (gh)^*.$$

Caso 2: $gh = hg$.

Para este caso hay 4 posibilidades correspondientes a si cada uno de g, h es central.

- Si ambos elementos g y h son centrales, entonces gh también debe serlo y así $h^*g^* = hg = gh = (gh)^*$
- Si por el contrario ninguno de los dos es central, entonces gh debe serlo ya que $gh = hg$ y G tiene la propiedad LC, luego $h^*g^* = (sh)(sg) = hg = gh = (gh)^*$.
- Si uno de los dos es central y el otro no, por ejemplo, si g es central y h no lo es, entonces gh no puede ser central. En efecto, si gh es central, $(gh)x = x(gh)$, para todo $x \in G$, así $g^{-1}ghx = g^{-1}xgh$ y como g es central g^{-1} también lo es, luego $g^{-1}ghx = xg^{-1}gh$ y $hx = xh$, para todo $x \in G$, es decir, h es central, lo cual es una contradicción. Por lo tanto, $h^*g^* = (sh)g = shg = sgh = (gh)^*$.

De esto se concluye que, $g \longmapsto g^*$ es una involución y note que

$$h^{-1}gh = g(g^{-1}h^{-1}gh) = \begin{cases} g, & \text{si } gh = hg \\ gs = sg, & \text{si } gh \neq hg \end{cases},$$

luego $h^{-1}gh \in \{g, g^*\}$ para todo $g, h \in G$.

Recíprocamente, suponga que G es un grupo no abeliano con una involución, $g \longmapsto g^*$ tal que $h^{-1}gh \in \{g, g^*\}$, para todo $g, h \in G$. Si $g = g^*$ para algún $g \in G$, entonces $h^{-1}gh = g$, luego $gh = hg$ para todo $h \in G$, lo que implica que g es central. En

particular, note que $(gg^*)^* = (g^*)^*g^* = gg^*$, por lo tanto, gg^* es central para todo $g \in G$. Entonces $(gg^*)g^{-1} = g^{-1}(gg^*)$, luego $gg^* = g^*g$ y $g^*g^{-1} = g^{-1}g^*$, es decir, g^* conmuta con g y con g^{-1}, para todo $g \in G$.

Ahora suponga que $gh \neq hg$, para $g, h \in G$. Entonces $g^{-1}hg = h^*$, luego $hg = gh^*$. Además, $h^{-1}g^*h = g$, pues de lo contrario, $h^{-1}g^*h = g^*$, entonces $g^*h = hg^*$, luego $gg^*h = ghg^*$ y como gg^* es central, $gg^*h = hgg^*$, luego $ghg^* = hgg^*$, así $gh = hg$, que es una contradicción. Por lo tanto $g^*h = hg$, entonces $g^*h = gh^*$, así $g^{-1}g^* = h^*h^{-1}$ y dado que h^{-1} conmuta con h^* se tiene que $g^{-1}g^* = h^{-1}h^*$.

Afirmación: Si $g \notin \mathcal{Z}(G)$, entonces el elemento $s = g^{-1}g^*$ es independiente de g.

Para ver esto, fije $g, h \in G$, con $gh \neq hg$ y sea x cualquier elemento no central de G. Si $xg \neq gx$ y $xh = hx$ (o viceversa), entonces, por lo mostrado anteriormente, $x^{-1}x^* = g^{-1}g^*$. Si $xh \neq hx$ y $xg \neq gx$, entonces $x^{-1}x^* = h^{-1}h^* = g^{-1}g^*$. En el caso que $xg = gx$ y $xh = hx$, se tiene:

$$h^{-1}(gx)h = gx \quad \text{o} \quad h^{-1}(gx)h = (gx)^* = (xg)^* = g^*x^*,$$

además $h^{-1}(gx)h = (h^{-1}gh)(h^{-1}xh) = g^*x$ entonces $gx = g^*x$ o $g^*x^* = g^*x$, luego $g = g^*$ o $x^* = x$, en cualquiera de los dos casos se produce una contradicción ya que ni g ni x son centrales. Esto establece la afirmación.

Así, si $gh \neq hg$, entonces $(g, h) = g^{-1}h^{-1}gh = g^{-1}g^*$, luego $s = g^{-1}g^*$ es el único conmutador no trivial de G y $g^* = h^{-1}gh = g(g^{-1}h^{-1}gh) = gs = sg$. Si g es central y h no lo es, entonces gh no es central y se tiene:

$$(sh)g^* = h^*g^* = (gh)^* = s(gh) = shg \quad \Rightarrow \quad g^* = g.$$

Así, g^* está definida por (3).

Por último, si $gh = hg$ y $g, h \notin \mathcal{Z}(G)$, entonces

$$(gh)^* = h^*g^* = (sh)(sg) = s^2hg = hg = gh.$$

Luego $gh \in \mathcal{Z}(G)$. Por lo tanto, G es un LC-grupo. □

En vista de los Teoremas 2.2.2 y 2.3.1, el siguiente corolario es inmediato.

Corolario 2.3.1. *Sea R un anillo conmutativo, asociativo, con unidad y característica diferente de 2. Sea L el loop $M(G, *, g_0)$. Entonces RL es un anillo alternativo no asociativo si, y solo si, G tiene la propiedad LC y un único conmutador no trivial s. En este caso, la involución en G es dada por (3).*

Definición 2.3.3. *Sea G un grupo no abeliano con una involución. Se dice que G es un LC-grupo especial o un **SLC-grupo** con respecto a la involución, si G es un LC-grupo con un único conmutador no trivial s.*

El Teorema 2.3.1 se enfoca en los grupos LC con un único conmutador no trivial. Tales grupos son caracterizados por el siguientes teorema.

Teorema 2.3.2. *Sea G un grupo no abeliano. Entonces G es un LC-grupo con un único conmutador no trivial si, y solo si, $G/\mathcal{Z}(G) \cong C_2 \times C_2$, donde C_2 es el grupo cíclico de orden 2.*

Demostración. Suponga que G es un LC-grupo con único conmutador no trivial, s. De la observación 2.3.1 los cuadrados son centrales en los grupos con ausencia de conmutatividad, luego $G/\mathcal{Z}(G)$ en un 2-grupo abeliano elemental, en efecto, sea $\overline{g} = g\mathcal{Z}(G) \in G/\mathcal{Z}(G)$, entonces $(\overline{g})^2 = (g\mathcal{Z}(G))^2 = g^2\mathcal{Z}(G) = \mathcal{Z}(G) = \overline{1}$, además si $\overline{g}, \overline{h} \in G/\mathcal{Z}(G)$, por lo anterior $(\overline{gh})^2 = \overline{1}$, luego $\overline{g}\,\overline{h} = \overline{gh} = (\overline{gh})^{-1} = (\overline{g}\,\overline{h})^{-1} = (\overline{h})^{-1}(\overline{g})^{-1} = \overline{h}\,\overline{g}$. Con esto, si $g \notin \mathcal{Z}(G)$, $\langle\overline{g}\rangle = \langle g\mathcal{Z}(G)\rangle$ es un grupo cíclico de orden 2. Suponga que $G/\mathcal{Z}(G)$ contiene al producto directo $\langle\overline{a}\rangle \times \langle\overline{b}\rangle \times \langle\overline{c}\rangle$ (3 copias del grupo cíclico de orden 2), con $\overline{a}, \overline{b}$ y $\overline{c}$ diferentes y $a, b, c \notin \mathcal{Z}(G)$. Como G es un LC-grupo, a, b y c no pueden conmutar dos a dos. De hecho, por ejemplo, si $ab = ba$, entonces $a \in \mathcal{Z}(G)$ o $b \in \mathcal{Z}(G)$ o $ab \in \mathcal{Z}(G)$, como se mencionó anteriormente $a, b \notin \mathcal{Z}(G)$. Si $ab \in \mathcal{Z}(G)$, entonces $\overline{ab} = ab\mathcal{Z}(G) = \mathcal{Z}(G) = \overline{1}$, y como $G/\mathcal{Z}(G)$ es

2-grupo abeliano elemental sigue que, $\overline{b} = \overline{a}$, lo que contradice la elección de $\overline{a}$ y $\overline{b}$. Los casos en que a o b conmutan con c son análogos.
Ahora, la relación $(xy, z) = y^{-1}(x, z)y(y, z)$ se cumple en todo grupo (ver 1.1.5), y puesto que los conmutadores son centrales en un LC-grupo, se tiene que:

$$(xy, z) = y^{-1}(x, z)y(y, z) = (x, z)y^{-1}y(y, z) = (x, z)(y, z),$$

para todo $x, y, z \in G$. Con esto, $(ab, c) = (a, c)(b, c) = s^2 = 1$, es decir, $(ab)c = c(ab)$, luego $ab \in \mathcal{Z}(G)$ o $c \in \mathcal{Z}(G)$ o $abc \in \mathcal{Z}(G)$, lo cual no ocurre. De hecho, $c \notin \mathcal{Z}(G)$, si $ab \in \mathcal{Z}(G)$, ab conmuta con a, y así $(ab)a = a(ab)$, luego $ba = ab$, absurdo. Si $abc \in \mathcal{Z}(G)$, entonces $\overline{abc} = (abc)\mathcal{Z}(G) = \mathcal{Z}(G) = \overline{1}$, y como $(\overline{c})^2 = 1$, sigue que $\overline{ab} = \overline{c}$, así $\langle\overline{a}\rangle\langle\overline{b}\rangle \cap \langle\overline{c}\rangle = \langle\overline{a}\rangle\langle\overline{b}\rangle \cap \langle\overline{ab}\rangle \neq \{\overline{1}\}$, lo cual es una contradicción. Luego, $G/\mathcal{Z}(G)$ contiene a lo sumo el producto directo de dos copias de C_2, y como G es no abeliano, $G/\mathcal{Z}(G)$ no es cíclico, por tanto, $G/\mathcal{Z}(G)$ contiene exactamente dos copias de C_2, es decir, $G/\mathcal{Z}(G) \cong C_2 \times C_2$.

Recíprocamente, si G es un grupo tal que $G/\mathcal{Z}(G) \cong \langle\overline{a}\rangle \times \langle\overline{b}\rangle$ con $\langle\overline{a}\rangle \cong C_2 \cong \langle\overline{b}\rangle$, entonces $|G/\mathcal{Z}(G)| = 4$ y $G/\mathcal{Z}(G) = \{\overline{1}, \overline{a}, \overline{b}, \overline{ab}\}$, luego $ab \neq ba$, pues de lo contrario a, b y ab conmutarían entre sí, lo cual contradice el hecho de que G es no abeliano. Sean $x, y \notin \mathcal{Z}(G)$, puesto que a y b no conmutan, se tiene que $xy = yx$ si, y solamente si, $\overline{x} = \overline{y}$. De hecho, si $\overline{x} = \overline{a}$ y $\overline{y} = \overline{b}$, entonces existen $z_1, z_2 \in \mathcal{Z}(G)$ tales que $x = az_1$ e $y = bz_2$. Así, si $xy = yx$, se tiene que $az_1bz_2 = bz_2az_1$, luego $abz_1z_2 = baz_1z_2$ y $ab = ba$, absurdo. Para los otros casos se procede de forma análoga. Entonces, dos elementos no centrales, $x, y \in G$, conmutan si, y solo si, $x, y \in a\mathcal{Z}(G)$ o $x, y \in b\mathcal{Z}(G)$ o $x, y \in ab\mathcal{Z}(G)$, es decir, ambos están en la misma clase. Así, si $xy = yx$ sigue que $\overline{x} = \overline{y}$ y como $\langle\overline{a}\rangle \cong C_2 \cong \langle\overline{b}\rangle$, se tiene que $(\overline{a})^2 = (\overline{b})^2 = \overline{1}$, luego $\overline{xy} = \overline{x}\,\overline{y} = (\overline{x})^2 = \overline{1}$, es decir, $xy \in \mathcal{Z}(G)$, por lo tanto, G es un LC-grupo. Sea $s = (a, b)$ y $x, y \in G$, tales que $xy \neq yx$, entonces, por lo que se concluyó anteriormente x e y no pertenecen simultáneamente a una de las clases

$\overline{a}, \overline{b}, \overline{ab}$. Además, $G/\mathcal{Z}(G)$ es abeliano, luego, $G' \subseteq \mathcal{Z}(G)$, es decir, todo conmutador es central lo que implica que se cumple la siguiente relación, $(xy, z) = (x, z)(y, z)$, para todo $x, y \in G$. Por lo tanto, $(x, y) = (a, b) = s$, en efecto, suponga sin pérdida de generalidad que $x \in \overline{a}$ e $y \in \overline{b}$, entonces existen $z_1, z_2 \in \mathcal{Z}(G)$ tales que $y = bz_2$ y $x = az_1$, así $(x, y) = (az_1, bz_2)$ y de $(xy, z) = (x, z)(y, z)$ sigue que,

$$(x, y) = (az_1, bz_2) = (a, b)(z_1, b)(a, z_2)(z_1, z_2) = (a, b) = s.$$

Luego s es el único conmutador no trivial en G. □

Ejemplo 2.3.3. *Sea $G = \mathcal{Q}_8$ descrito en el Ejemplo 2.3.1, $\mathcal{Q}_8/\mathcal{Z}(\mathcal{Q}_8)$ tiene orden 4, luego $\mathcal{Q}_8/\mathcal{Z}(\mathcal{Q}_8) \cong C_2 \times C_2$ o $\mathcal{Q}_8/\mathcal{Z}(\mathcal{Q}_8) \cong C_4$, puesto que C_4 es cíclico la segunda opción no es posible, ya que $\mathcal{Q}_8$ es no abeliano. Por lo tanto, $\mathcal{Q}_8$ es un LC-grupo con un único conmutador no trivial $s = x^2$. Más aún, $\mathcal{Q}_8$ es un SLC-grupo con respecto a la involución clásica. En efecto, es sabido que $\mathcal{Z}(\mathcal{Q}_8) = \{1, x^2\}$, entonces para 1 y x^2 se obtiene trivialmente que $(1)^{-1} = 1$ y $(x^2)^{-1} = x^{-2} = x^2$. Ahora, para $x, x^3, y, xy, x^2y, x^3y \notin \mathcal{Z}(G)$ se tiene:*

- $(x)^{-1} = x^3 = x^2x = sx$,
- $(x^3)^{-1} = x^{-3} = x^2x^{-1} = x^2x^3 = sx^3$,
- $(y)^{-1} = y^3 = y^2y = x^2y = sy$,
- $(xy)^{-1} = y^{-1}x^{-1} = sysx = s(syx) = sxy$,
- $(x^2y)^{-1} = y^{-1}(x^2)^{-1} = syx^2 = sx^2y$,
- $(x^3y)^{-1} = y^{-1}(x^3)^{-1} = sysx^3 = s(syx^3) = sx^3y$.

De esto se concluye que $g^{-1} = g$ si $g \in \mathcal{Z}(\mathcal{Q}_8)$ y $g^{-1} = sg$ si $g \notin \mathcal{Z}(\mathcal{Q}_8)$.

Otros ejemplos de LC-grupos con un único conmutador son: D_4, $\mathcal{Q}_8 \times C_2$, $\mathcal{Q}_8 \times C_3$, $D_4 \times C_2$ y $D_4 \times C_3$. Mas ejemplos de estos grupos pueden ser consultados en [2].
Si G es cualquiera de estos grupos y s es el único conmutador no trivial de G, la función $g \mapsto g^*$ dada por (3) es una involución , [2]. Mas aún, si R es un anillo conmutativo, asociativo, con unidad y de característica diferente de 2 y si g_0 es cualquier elemento en $\mathcal{Z}(G)$, el anillo de loop RL del loop $L = M(G, *, g_0)$ es un anillo alternativo pero no asociativo, según el Corolario 2.3.1.

Corolario 2.3.2. *Sean R un anillo conmutativo y G un LC-grupo con un único conmutador no trivial, s. Entonces, el conjunto*

$$\mathcal{Z}(G) \cup \{g + sg : g \in G \backslash \mathcal{Z}(G)\},$$

es una R-base de $\mathcal{Z}(RG)$.

Demostración. Sea $g \in G$, si $g \in \mathcal{Z}(G)$ entonces $C(g) = \{x^{-1}gx : x \in G\} = \{g\}$. Ahora, para todos $x, y \in G$, tales que $xy \neq yx$, se tiene que $s = (x, y) = x^{-1}y^{-1}xy$. Luego, $y^{-1}xy = sx$, así, si $g \notin \mathcal{Z}(G)$, $C(g) = \{g, sg\}$. Por el Teorema 1.3.3, sigue el resultado. □

El siguiente Corolario permite decir más sobre la estructura de los LC-grupos con un único conmutador [8].

Corolario 2.3.3. *Sea G un grupo no abeliano tal que $G/\mathcal{Z}(G) \cong C_2 \times C_2$. Si $g \notin \mathcal{Z}(G)$ es de orden finito, entonces el orden de g es par. Equivalentemente, el conjunto G_{odd} de los elementos de orden impar es un subgrupo central. Además, si $H \times K$ es un producto directo de subgrupos de G, entonces al menos uno entre H y K es central.*

Demostración. Sea $g \in G_{odd}$, entonces existe algún $t \in \mathbb{N}$ tal que, $g^{2t+1} = g^{2t}g = 1$, luego $g = (g^{-t})^2$, lo cual implica que g es central ya que G es un LC-grupo, por lo

---

[8] A. H. VILLA. "Involuções de grupo orientadas em álgebras de grupo". Tesis doct. Tese de Doutorado, Universidade de Sao Paulo, 2013.

tanto, $G_{odd} \subseteq \mathcal{Z}(G)$. Ahora, sean $g_1, g_2 \in G_{odd}$ entonces $d = m.c.m(|g_1|, |g_2|)$ es impar y $(g_1 g_2^{-1})^d = 1$, luego $g_1 g_2^{-1} \in G_{odd}$, esto es, $G_{odd} \leq \mathcal{Z}(G)$.
De la definición de producto directo, 1.1.11, se tiene que, $hkh^{-1}k^{-1} = 1$ o equivalentemente $hk = kh$ para todo $h \in H$ y $k \in K$. Así, como G es LC-grupo, $h \in \mathcal{Z}(G)$ o $k \in \mathcal{Z}(G)$ o $hk \in \mathcal{Z}(G)$. Por lo tanto, $H \leq \mathcal{Z}(G)$ o $K \leq \mathcal{Z}(G)$ o $HK \leq \mathcal{Z}(G)$. □

Sea G es un grupo no abeliano tal que $G/\mathcal{Z}(G) \cong C_2 \times C_2$, entonces como $C_2 \times C_2$ es abeliano, por el Teorema 1.1.8 se tiene que G es nilpotente. A continuación se mostrará un resultado a partir del Corolario 2.3.3 y la teoría de Sylow.

Proposición 2.3.1. *Sea G un grupo finito tal que $G/\mathcal{Z}(G) \cong C_2 \times C_2$. Entonces G es nilpotente y su 2-grupo de Sylow contiene al subgrupo conmutador G'.*

Demostración. Por el isomorfismo $G/\mathcal{Z}(G) \cong C_2 \times C_2$, se tiene que $G/\mathcal{Z}(G)$ es abeliano, entonces por el Teorema 1.1.5, $G' \subset \mathcal{Z}(G)$. Como G tiene un único conmutador no trivial, $|G'| = 2$, lo que implica que el orden de $\mathcal{Z}(G)$ es múltiplo de 2, es decir, $|\mathcal{Z}(G)| = 2^n m$, donde $n \geq 1$ y $m \in \mathbb{N}$ es tal que $2 \nmid m$. Así, dado que $|G/\mathcal{Z}(G)| = 4$, se tiene que $|G| = 2^{n+2}m$, entonces por el inciso (i) del Teorema 1.1.7, G contiene un subgrupo G_2 tal que $|G_2| = 2^{n+2}$ y $G' \subset G_2$, dado que $|G'| = 2$. Como $G = G_2 G_{odd}$ y $G_2 \cap G_{odd} = \{1\}$, sigue que $G = G_2 \times G_{odd}$. Del Corolario 2.3.3, G_{odd} es un subgrupo central, por tanto es nilpotente y por la Proposición 1.1.6, G_2 también es nilpotente, entonces el producto directo de estos dos grupos, G, es nilpotente. □

La siguiente proposición, permite obtener LC-grupos con un único conmutador, de un grupo inicial G con las mismas características.

Proposición 2.3.2. *Sean G un grupo no abeliano tal que $G/\mathcal{Z}(G) \cong C_2 \times C_2$ y H un grupo abeliano. Entonces*

$$(G \times H)/\mathcal{Z}(G \times H) \cong C_2 \times C_2.$$

Demostración. Es sabido que $\mathcal{Z}(G)$ y $\mathcal{Z}(H)$ son subgrupos normales de G y H, respectivamente. Considere $f : G \times H \longrightarrow (G/\mathcal{Z}(G)) \times (H/\mathcal{Z}(H))$ el homomorfismo canónico dado por $f(g,h) = (g\mathcal{Z}(G), h\mathcal{Z}(H))$, el cual es sobreyectivo. Observe además que

$$\begin{aligned} ker(f) &= \{(g,h) \in G \times H : f(g,h) = (g\mathcal{Z}(G), h\mathcal{Z}(H)) = (\mathcal{Z}(G), \mathcal{Z}(H))\} \\ &= \{(g,h) \in G \times H : g \in \mathcal{Z}(G), h \in \mathcal{Z}(H)\} \\ &= \mathcal{Z}(G) \times \mathcal{Z}(H), \end{aligned}$$

por el primer teorema de isomorfismos sigue que

$$(G \times H)/(\mathcal{Z}(G) \times \mathcal{Z}(H)) \cong (G/\mathcal{Z}(G)) \times (H/\mathcal{Z}(H))$$

y como H es abeliano, $H = \mathcal{Z}(H)$, entonces $(G/\mathcal{Z}(G)) \times (H/\mathcal{Z}(H)) \cong G/\mathcal{Z}(G) \cong C_2 \times C_2$, luego $(G\times H)/(\mathcal{Z}(G)\times\mathcal{Z}(H)) \cong C_2 \times C_2$. Note que $\mathcal{Z}(G\times H) = \mathcal{Z}(G)\times\mathcal{Z}(H)$, en efecto, sean $(g,h) \in \mathcal{Z}(G) \times \mathcal{Z}(H)$ y $(g_1,h_1) \in G \times H$, entonces $(g,h)(g_1,h_1) = (gg_1, hh_1) = (g_1g, h_1h) = (g_1,h_1)(g,h)$, luego $(g,h) \in \mathcal{Z}(G \times H)$. Por otro lado, sean $(g_1,h_1) \in \mathcal{Z}(G \times H)$ y $(g,h) \in G \times H$, entonces $(g_1,h_1)(g,h) = (g,h)(g_1,h_1)$ y $(g_1g, h_1h) = (gg_1, hh_1)$, luego $g_1g = gg_1$ y $h_1h = hh_1$, así $g_1 \in \mathcal{Z}(G)$ y $h_1 \in \mathcal{Z}(H)$, por lo tanto, $(g_1,h_1) \in \mathcal{Z}(G) \times \mathcal{Z}(H)$. De esto se concluye que $(G \times H)/\mathcal{Z}(G \times H) \cong C_2 \times C_2$. □

Observación 2.3.2. *Del Teorema 2.3.2 sigue que $G \times H$ (con las condiciones dadas para G y H en la proposición anterior), es un LC-grupo con un único conmutador no trivial, es decir, la propiedad LC se preserva por producto de grupos abelianos.*

Proposición 2.3.3. *Sean G un LC-grupo con un único conmutador no trivial y H un subgrupo no abeliano de G, entonces*

(i) *H es un LC-grupo con un único conmutador no trivial.*

(ii) *Si* $\mathcal{Z}(G) \subset H$*, entonces* $H = G$.

Demostración. (i) Sean $a, b \in H$ tales que $a, b \notin \mathcal{Z}(H)$ y $ab = ba$. Como G tiene la propiedad LC y $a, b \in G$, sigue que a o b o $ab \in \mathcal{Z}(G)$, sin embargo, las dos primeras opciones no son posibles, pues caso contrario, si a o $b \in \mathcal{Z}(G)$, entonces a o $b \in \mathcal{Z}(H)$, lo cual es absurdo. Luego $ab \in \mathcal{Z}(G)$ y así $ab \in \mathcal{Z}(H)$, por lo tanto, H es un LC-grupo. Ahora, sea s el único conmutador no trivial de G y suponga que existe un conmutador no trivial, r en H, entonces para $x, y \in H \subset G$ se tiene que $xyr = yx$, esto es $r = y^{-1}x^{-1}yx = s$, por lo tanto H tiene un único conmutador no trivial que es precisamente el conmutador de G. De esto se concluye que H es un LC-grupo con un único conmutador no trivial, luego $H/\mathcal{Z}(H) \cong C_2 \times C_2$.

(ii) Por hipótesis $H \leq G$, luego $H \subseteq G$. Además H es no abeliano, entonces existen $x, y \in H$ tales que $xy \neq yx$, así $T := \{1, x, y, xy\} \subset H$, y como $|H/\mathcal{Z}(H)| = 4$ entonces T es un conjunto transversal de $\mathcal{Z}(H)$ en H y a su vez T es un conjunto transversal de $\mathcal{Z}(G)$ en G, puesto que $|G/\mathcal{Z}(G)| = 4$ y $x, y, xy \in H \subseteq G$. De esta forma $G = \dot{\bigcup_{t \in T}} t\mathcal{Z}(G)$ y así si $g \in G$, entonces $g \in t\mathcal{Z}(G) \subset H$, para algún $t \in T$. Por lo tanto, $G \subseteq H$ y consecuentemente $G = H$.

□

3. SLC-grupos y anillos de grupo

En este capítulo se estudiaran algunas condiciones necesarias y suficientes para que el conjunto de elementos simétricos de RG, RG^+ sea conmutativo, o equivalentemente, para que RG^+ sea subanillo de RG.

El anillo RG tiene una *involución natural*, $*$, que se obtiene extendiendo la involución de G ($g^* = g^{-1}$, $g \in G$), por linealidad a RG. Es decir, $(\sum \alpha_g g)^* = \sum \alpha_g g^{-1}$, ver 1.3.2. Sea

$$RG^+ = \{\alpha \in RG \mid \alpha^* = \alpha\},$$

el conjunto de los *elementos simétricos* de RG. En general, RG^+ no es subanillo de RG. En efecto, si $\alpha, \beta \in RG^+$, entonces $(\alpha\beta)^* = \beta^*\alpha^* = \beta\alpha$, así $(\alpha\beta)^* = \alpha\beta$ si, y solo si, α y β conmutan. Luego RG^+ es subanillo de RG si, y solo si, los elementos de RG^+ conmutan. Nuestro objetivo en este capítulo es caracterizar los grupos G tales que los elementos simétricos de RG, con respecto a la involución clásica, conmutan.

Definición 3.0.1. *Un elemento $\alpha \in RG$ es **simétrico** si*

$$\alpha^* = \left(\sum_{g\in G} a_g g\right)^* = \sum_{g\in G} a_g g^{-1} = \sum_{g\in G} a_g g = \alpha,$$

esto es, si el coeficiente de g coincide con el coeficiente de g^{-1} (es decir, $a_g = a_{g^{-1}}$) para todo $g \in G$.

Así, RG^+ es generado, como R-módulo, por el conjunto

$$\{g + g^{-1} \mid g \in G, g^2 \neq 1\} \cup \{g \in G \mid g^2 = 1\}.$$

Como se quiere estudiar la conmutatividad de RG^+, bastará con analizar la conmutatividad de los elementos en este conjunto. Para simplificar la notación, se usará el

corchete de Lie de elementos en RG, definido por $[\alpha, \beta] = \alpha\beta - \beta\alpha$.

Ejemplo 3.0.1. *Sean R un anillo conmutativo con unidad, $\mathcal{Q}_8$ el grupo cuaternio de orden 8 y $*$ la involución clásica. Por el Ejemplo 2.3.3 se tiene que $\mathcal{Q}_8$ es un SLC-grupo con respecto a $*$, además $\mathcal{Q}_8^+ = \{g \in \mathcal{Q}_8 : g^2 = 1\} = \mathcal{Z}(\mathcal{Q}_8)$. Luego $R\mathcal{Q}_8^+$ es generado como R-módulo por el conjunto $\{g + sg : g \in \mathcal{Q}_8 \backslash \mathcal{Z}(\mathcal{Q}_8)\} \cup \mathcal{Z}(\mathcal{Q}_8)$ que, por el Corolario 2.3.2, es una R-base para $\mathcal{Z}(R\mathcal{Q}_8)$. Por lo tanto $R\mathcal{Q}_8^+$ es conmutativo.*

Lema 3.0.1. *Si RG^+ es conmutativo, entonces los elementos de orden 2 en G son centrales.*

Demostración. Sean $x \in G$ un elemento de orden 2 e $y \in G$ un elemento arbitrario. Se mostrará que x e y conmutan.
Si $y^2 = 1$ entonces ambos elementos $x, y \in RG^+$ y por hipótesis RG^+ es conmutativo, luego $xy = yx$. Suponga ahora que $y^2 \neq 1$. Entonces $y + y^{-1} \in RG^+$ y así,

$$0 = [x, y + y^{-1}] = x(y + y^{-1}) - (y + y^{-1})x = xy + xy^{-1} - yx - y^{-1}x.$$

Luego $xy + xy^{-1} = yx + y^{-1}x$. Puesto que $y^2 \neq 1$ se tiene que $xy \neq xy^{-1}$, entonces $xy = yx$ o $xy = y^{-1}x$. Si $xy = y^{-1}x$ sigue que $(xy)^2 = x^2 = 1$ y, por el caso anterior, xy y x conmutan. Consecuentemente, $(xy)x = x(xy)$ y así $yx = xy$. Por lo tanto, x es central en G. □

Lema 3.0.2. *Suponga que RG^+ es conmutativo y sean $x, y \in G$.*

(i) *Si $car(R) \neq 2$, entonces xy es igual a uno de yx, yx^{-1} o $y^{-1}x$.*

(ii) *Si $car(R) = 2$, entonces vale una de las siguientes condiciones:*

a) xy es igual a uno de yx, yx^{-1} o $y^{-1}x$.

b) $xy = x^{-1}y^{-1}$ y ambos x e y tienen orden 4.

Demostración. Los casos en que $x^2 = 1$ o $y^2 = 1$ (o ambos al tiempo) se reducen al Lema 3.0.1. Entonces, suponga que $x^2 \neq 1$ y $y^2 \neq 1$. Luego

$$0 = [x + x^{-1}, y + y^{-1}] = xy + xy^{-1} + x^{-1}y + x^{-1}y^{-1} - yx - yx^{-1} - y^{-1}x - y^{-1}x^{-1}.$$

(i) Si $car(R) \neq 2$, entonces xy coincide por lo menos con dos términos diferentes con coeficiente positivo o con algún término con coeficiente negativo. Como $x^2 \neq 1$ y $y^2 \neq 1$, se tiene que $xy \neq xy^{-1}$ y $xy \neq x^{-1}y$. Por lo tanto la primera posibilidad es eliminada y así xy debe coincidir con algún término de coeficiente negativo. Si $xy = y^{-1}x^{-1}$ entonces, $(xy)^2 = xyy^{-1}x^{-1} = 1$ y, por Lema 3.0.1, $(xy)x = x(xy)$, luego, $xy = yx$.

(ii) Si $car(R) = 2$ también se debe analizar la posibilidad que $xy = x^{-1}y^{-1}$ (y equivalentemente $yx = y^{-1}x^{-1}$). Con estas condiciones,

$$0 = [x + x^{-1}, y + y^{-1}] = xy^{-1} + x^{-1}y + yx^{-1} + y^{-1}x,$$

y se tienen tres posibilidades para xy^{-1}. Si $xy^{-1} = yx^{-1}$, entonces $(xy^{-1})^2 = 1$ y por Lema 3.0.1, xy^{-1} es central, luego $(xy^{-1})y = y(xy^{-1})$, esto es, $xy = yx$. Ahora, si $xy^{-1} = y^{-1}x$, entonces $x = y^{-1}xy$ así $xy = yx$. Finalmente, si $xy^{-1} = x^{-1}y$, entonces $x^2 = y^2$ y como $xy = x^{-1}y^{-1}$ se tiene que $x^2 = x^{-2}$ y $y^2 = y^{-2}$. Luego $x^4 = 1$ y $y^4 = 1$, por lo tanto, x e y tienen orden 4 ya que $x^2, y^2 \neq 1$. □

Es conveniente estudiar por separado los casos en que $car(R) \neq 2$ y $car(R) = 2$ [3]. Este trabajo se centra en el caso que $car(R) \neq 2$.

Lema 3.0.3. *Sea $G = \langle x, y \rangle$ un grupo no abeliano generado por dos elementos x e y tales que $y^{-1}xy = x^{-1}$. Si RG^+ es conmutativo y $car(R) \neq 2$, entonces $\langle x, y \rangle$ es isomorfo a $\mathcal{Q}_8$, el grupo cuaternio de orden 8.*

Demostración. Aplicando la parte (i) del Lema 3.0.2, a los elementos y y xy, se

tienen 3 posibilidades para el producto $(xy)y = xy^2$:

- $xy^2 = y(xy)$, entonces $xy = yx$;
- $xy^2 = y(xy)^{-1} = yy^{-1}x^{-1} = x^{-1}$, lo que implica que $y^2 = x^{-2}$;
- $xy^2 = y^{-1}(xy) = x^{-1}$, de esto se obtiene nuevamente, $y^2 = x^{-2}$.

Puesto que G es no abeliano sus generadores no conmutan, es decir, $xy \neq yx$ así $y^2 = x^{-2}$. Luego

$$x^{-2} = (y^{-1}xy)^2 = y^{-1}x^2y = y^{-1}y^{-2}y = y^{-2} = x^2,$$

lo que implica que $x^4 = 1$. Por lo tanto, el orden de x es igual a 4 pues, caso contrario, x conmutaría con y, por Lema 3.0.2. De esto,

$$\langle x, y \mid x^4 = 1,\ x^2 = y^2,\ y^{-1}xy = x^{-1} \rangle \cong \mathcal{Q}_8.$$

□

La siguiente proposición muestra la relación entre la propiedad LC y los grupos Hamiltonianos caracterizados por el Teorema 1.1.9.

Proposición 3.0.1. *Sea G un SLC-grupo con respecto a la involución clásica. Entonces G es un 2-grupo Hamiltoniano.*

Demostración. Sean s el único conmutador no trivial de G y g un elemento arbitrario de G. Si $g \in \mathcal{Z}(G)$, $g^{-1} = g$, entonces $g^2 = 1$, si por el contrario $g \notin \mathcal{Z}(G)$, entonces $g^{-1} = sg$, así $g^2 = s$. En consecuencia, G es un 2-grupo con exponente menor o igual a 4.
Para mostrar que G es Hamiltoniano basta mostrar que todo subgrupo de G es normal. Sean $g \in G$ y $h \in H$, donde H es un subgrupo de G, entonces

- si $gh = hg$, se tiene que $g^{-1}hg = h \in H$, luego $g^{-1}Hg \subseteq H$,
- si $gh \neq hg$, como G es SLC-grupo, $g^{-1}hg = h^{-1} \in H$, luego $g^{-1}Hg \subseteq H$.

Por lo tanto, H es normal en G y así G es un 2-grupo Hamiltoniano. □

A continuación se presenta el teorema principal, el cual caracteriza a los grupos G, tales que RG^+ sea subanillo de RG.

Teorema 3.0.1. *Sean G un grupo y R un anillo conmutativo con unidad de característica diferente de 2. Entonces, RG^+ es conmutativo si, y solo si, G es un grupo abeliano o G es un 2-grupo Hamiltoniano.*

Demostración. Suponga que G es no abeliano. Se probará entonces que G debe ser un 2-grupo Hamiltoniano.
Sea $x \in G$ un $2'$-elemento, es decir, un elemento cuyo orden es impar o infinito. Observe que x es central en G. Sea y un elemento arbitrario de G y suponga que x no conmuta con y, entonces, por (i) del Lema 3.0.2, se tiene que $xy = yx^{-1}$ o $xy = y^{-1}x$. En ambos casos sigue del Lema 3.0.3 que $\langle x, y\rangle \cong \mathcal{Q}_8$, luego el orden de x es par, lo que contradice que x sea $2'$-elemento. De esto, $xy = yx$ y x es central en G.
Como G es no abeliano, existen $g, h \in G$ tales que $gh \neq hg$. Entonces, por los Lemas 3.0.2 y 3.0.3, sigue que $\langle g, h\rangle \cong \mathcal{Q}_8$. Aplicando la parte (i) de Lema 3.0.2 a los elementos gx y hx, se tienen tres casos a considerar, para el producto $gxhx = ghx^2$:

- $ghx^2 = hxgx = hgx^2$, así $gh = hg$, lo cual no puede pasar;
- $ghx^2 = hx(gx)^{-1} = hg^{-1}$, luego $x^2 = (gh)^{-1}hg^{-1}$, lo cual implica que $x^2 \in \langle g, h\rangle$;
- $ghx^2 = (hx)^{-1}gx = h^{-1}g$, entonces $x^2 = (gh)^{-1}h^{-1}g$ y nuevamente $x^2 \in \langle g, h\rangle$.

Así, x^2 es un 2-elemento, lo que implica que x tiene orden par, contradiciendo el hecho de ser $2'$-elemento. Por lo tanto G es un $2-$grupo.

Ahora se mostrará que G es un grupo Hamiltoniano. Sean $x, y \in G$ elementos arbitrarios en G. Entonces, por Lema 3.0.2, (i) y Lema 3.0.3 se tiene que $xy = yx$ o $\langle x, y\rangle \cong \mathcal{Q}_8$, luego $y^{-1}xy = x^{\pm 1}$, así, todo subgrupo de G es normal. Por lo tanto, G es un 2-grupo Hamiltoniano.

Recíprocamente se analizan los dos casos:

- Si G es abeliano el resultado sigue fácilmente. Debido a que G es base para RG y R es conmutativo, esto implica que RG es conmutativo, por lo tanto, $RG^+ \subseteq RG$ es conmutativo.

- Si G es 2-grupo Hamiltoniano, entonces por Teorema 1.1.9, $G \cong \mathcal{Q}_8 \times E$ (no pueden haber elementos de orden impar). Así, $RG = R(\mathcal{Q}_8 \times E) \cong (RE)\mathcal{Q}_8$ por Corolario 1.3.2. Además, por el Ejemplo 2.3.3 es sabido que, $\mathcal{Q}_8$ es un SLC-grupo y como E es un 2-grupo abeliano elemental y R es un anillo conmutativo con unidad, entonces RE es un anillo conmutativo con unidad. Luego por el Ejemplo 3.0.1 sigue que $(RE)\mathcal{Q}_8^+$ es conmutativo.

□

Condiciones necesarias y suficientes para que el conjunto de elementos simétricos, RG^+ sea conmutativo cuando $car(R) = 2$ pueden ser encontradas en [3].

BIBLIOGRAFÍA

CHEIN, O. y PFLUGFELDER H. O. “The smallest Moufang loop”. En: *Archiv der Mathematik* 22.1 (1971), págs. 573-576 (vid. pág. 44).

CRISTO, O. B. “Commutativity of symmetric elements in group rings”. En: *Journal of Group Theory* 9.5 (2006), págs. 673-683 (vid. págs. 11, 12, 45, 60, 63).

DOS SANTOS, R. B. “Elementos simétricos sob involuções orientadas em anéis de grupos”. En: (2012) (vid. pág. 29).

GALLIAN, J. *Contemporary abstract algebra*. Nelson Education, 2009 (vid. pág. 13).

GOODAIRE, E. G., JESPERS E. y MILIES C. P. *Alternative loop rings*. Vol. 184. Elsevier, 1996 (vid. págs. 11, 37, 40, 44, 54).

LEZAMA, O. *Cuadernos de Álgebra, No. 1: Grupos*. Departamento de Matemáticas, Universidad Nacional de Colombia, sede de Bogotá, 2017 (vid. pág. 13).

MILIES, C. P y SEHGAL S. K. *An introduction to group rings*. Vol. 1. Springer Science & Business Media, 2002 (vid. págs. 11, 20, 29).

VILLA, A. H. “Involuções de grupo orientadas em álgebras de grupo”. Tesis doct. Tese de Doutorado, Universidade de Sao Paulo, 2013 (vid. pág. 54).