IDENTIDADES DE GRUPO EN UNIDADES Y UNIDADES SIMÉTRICAS SOBRE ANILLOS DE GRUPO.

ADRIANA MARÍA ALZATE PATIÑO

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE MATEMÁTICAS
MAESTRÍA EN MATEMÁTICAS
BUCARAMANGA

2016

IDENTIDADES DE GRUPO EN UNIDADES Y UNIDADES SIMÉTRICAS SOBRE ANILLOS DE GRUPO.

ADRIANA MARÍA ALZATE PATIÑO

Trabajo de grado presentado para optar al
título de Magister en Matemáticas

Director
ALEXANDER HOLGUÍN VILLA, Ph.D.

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE MATEMÁTICAS
MAESTRÍA EN MATEMÁTICAS
BUCARAMANGA
2016

Índice general

Lista de Símbolos

$H \lhd G$	H es subgrupo normal de G.
$\mathcal{Q}_8$	Grupo cuaternio de orden 8.
$\zeta(G)$	Centro de G.
$C_G(H)$	Centralizador de H en G.
G'	Conmutador del grupo G.
$\Delta(G)$	Ideal de aumento.
$\Delta(G, N)$	Núcleo del epimorfismo canónico de FG en $F(G/H)$.
$car(R)$	Característica de R.
$p\|\|G\|$	p divide al orden de G.
$p \nmid \|G\|$	p no divide al orden de G.
P	Conjunto de los p-elementos.
Q	Conjunto de los p'-elementos.
$\Phi(G)$	Conjunto de los elementos de conjugación finita.
$\Phi_p(G)$	p-elementos de conjugación finita.
$Cl_g(G)$	Clase de conjugación del elemento g en el grupo G.
$\eta(FG)$	Suma de todos los ideales nilpotentes de FG.
$[G : H]$	Índice del subgrupo H en G.
$J(FG)$	Radical de Jacobson de FG.
$A^{-1}R$	Anillos de fracciones de R con respecto a A.

TÍTULO: IDENTIDADES DE GRUPO EN UNIDADES Y UNIDADES SIMÉTRICAS SOBRE ANILLOS DE GRUPO

AUTOR: ADRIANA MARÍA ALZATE PATIÑO

PALABRAS CLAVES: Anillos de grupo, identidades de grupo, identidades polinomiales, involuciones y unidades simétricas.

RESUMEN:

Motivado por encontrar una conexión entre la estructura aditiva y multiplicativa del álgebra de grupo FG, Brian Hartley conjeturó que si el grupo de unidades verifica una identidad de grupo entonces el álgebra de grupo verifica una identidad polinomial.

Considerando FG el álgebra de grupo del grupo de torsión G sobre un cuerpo infinito F, Giambruno, Sehgal y Valenti en [12] confirman la conjetura. En el presente texto se encuentra detalladamente está respuesta (ver Teorema 2.1.1).

Además, si FG es un álgebra de grupo con involución $*$ inducida por la aplicación $g \mapsto g^{-1}$ (la involución clásica), se plantea una versión de la Conjetura en términos de las unidades simétricas [13, Teorema 6], cuyo objeto era verificar que si $\mathcal{U}^+(FG) \in IG$ implica que $\mathcal{U}(FG) \in IG$ ó directamente que $FG \in IP$. En el tercer capítulo, primero presentamos ciertos resultados donde FG es un anillo con involución clásica y $\mathcal{U}^+(FG) \in IG$, y luego se tiene en detalle la respuesta a la Conjetura de Hartley para las unidades simétricas.

TITTLE: GROUP IDENTITIES ON UNITS AND SYMMETRIC UNITS ABOUT GROUP RINGS

AUTHOR: ADRIANA MARÍA ALZATE PATIÑO

KEY WORDS: Group rings, group identities, polynomial identities, involutions and symmetric units.

ABSTRACT:

Motivated to give a connection between the additive and the multiplicative structure of a group algebra FG, Brian Hartley conjecture that if $\mathcal{U}(FG)$ satisfies a group identity, the FG satisfies a polynomial identity.

Let FG be the group algebra of a torsion group G over an infinite field F, Giambruno, Sehgal y Valenti in [12] confirm a conjecture. In this paper it found specifically this answer (see Theorem 2.1.1).

Also, if FG is the group algebra with involution $*$ induced by the map $g \mapsto g^{-1}$ (classical involution), it propose a of conjecture in therms of the symmetric units [13, Teorema 6], whose purpose was to verify if $\mathcal{U}^+(FG) \in IG$ then $\mathcal{U}(FG) \in IG$ or directly $FG \in IP$. In third chapter, we first present some results where FG is a rings with classical involution and $\mathcal{U}^+(FG) \in IG$, and finally it have in specifically positive answer to Conjecture's Hartley for the symmetric units.

Introducción

Los grupos y los anillos son quizá dos de las ramas más estudiadas del álgebra abstracta. Evidentemente el tiempo y el esfuerzo de muchos a través de la historia las han llevado a formar una gran teoría, de manera independiente para cada una. Los anillos de grupo son un interesante punto de encuentro de estas dos teorías.

Alrededor de los años 80's Brian Hartley estableció su conjetura (ver Conjetura 2.1.1), en un intento por encontrar una conexión entre las estructuras aditiva y multiplicativa del álgebra de grupo FG de un grupo G sobre el cuerpo F. Desde que la conjetura fue planteada, el estudio de identidades de grupo dentro del grupo de unidades $\mathcal{U}(FG)$, del álgebra de grupo FG y sus implicaciones han sido objeto de múltiples estudios (ver [32], [25], [8], [12] y [21]).

Luego del teorema clásico de Amitsur referente a anillos con involución (ver Teorema 1.6.3) y al trabajo desarrollado por Herstein y colaboradores [17], se hizó natural estudiar anillos de grupo desde este punto de vista. Así las cosas, y luego de haberse dado respuesta a la conjetura de Hartley, esta última fue planteada para el subconjunto $\mathcal{U}^+(FG)$ de las unidades $\mathcal{U}(FG)$ para la involución clásica, es decir, para la involución inducida de la aplicación $g \mapsto g^{-1}$ para todo $g \in G$.

En [13], Giambruno, Sehgal y Valenti probaron la conjetura en el contexto anterior, es decir, $\mathcal{U}^+(FG) \in IG$ implica que $FG \in IP$, siendo G un grupo de torsión y F un cuerpo infinito con $car(F) \neq 2$. Además, en ese mismo trabajo, ellos clasificaron los grupos G tales que $\mathcal{U}^+(FG)$ verifican una identidad de grupo; esta clasificación depende de la presencia o no del grupo cuaternio $\mathcal{Q}_8 = \langle x, y : x^4 = 1, x^2 = y^2, yxy^{-1} = x^{-1} \rangle$.

Nuestro propósito fue estudiar los resultados conocidos para la Conjetura de Hartley, tanto en el caso de unidades como en unidades simétricas, dotando a FG de la involución clásica, para escribir detalladamente la respuesta afirmativa a la conjetura en ambos contextos. Por ello, se ha dividido el presente trabajo en tres capítulos. El primero contiene las definiciones y resultados en teoría de grupos, anillos, anillos de grupos e involuciones, necesarios para la compresión del presente texto. En el segundo capítulo se encontrarán enunciados, y en su mayoría demostrados, resultados que llevan a la respuesta afirmativa a la Conjetrua de B. Hartley (Teorema 1.6.3). Para la parte final, se han preparado ciertos resultados que inducen la clasificación de las álgebras de grupo con involución clásica cuyas unidades simétricas satisfacen una identidad de grupo, y por supuesto, se muestra la respuesta afirmativa a la Conjetura 2.1.1 en el contexto de las unidades simétricas, donde la involución es la clásica (Teorema 3.2.6).

Capítulo 1

Preliminares

En el presente capítulo se presentan algunos conceptos básicos y notaciones, necesarios para comprender el resto del escrito. Esto es, definiciones y propiedades clásicas en la teoría de grupos, teoría de anillos y teoría de anillos de grupo. La mayoría de los resultados serán presentados sin demostración, sin embargo estas pueden ser consultados en [29], [27] o en cualquier texto clásico que contenga estos tópicos, por ejemplo [2].

1.1. Grupos y anillos

Recuerde que si un grupo G es finito, entonces el número de elementos de G es llamado *el orden de* G y es denotado por $|G|$. Además si G verifica $ab = ba$ para todos $a, b \in G$ entonces el grupo es *Abeliano*.

Definición 1.1.1. *Sean N un subgrupo de G y $n \in N$, N es un* ***subgrupo normal*** *si y solo si $g^{-1}ng \in N$ para todo $g \in G$.*

El elemento de la forma $g^{-1}ng$, usualmente denotado por n^g, es llamado el conjugado de n por g. Además, se denota por $H \leq G$ para indicar que H es un subgrupo de G y por $H \lhd G$ cuando H sea un subgrupo normal de G. A continuación algunos ejemplos:

Ejemplo 1.1.2. *Dado un grupo G,* el centro de G *se define por*

$$\zeta(G) = \{g \in G : gh = hg, \forall h \in G\}.$$

Además, para un subconjunto H de G se define el centralizador de H en G por

$$C_G(H) = \{g \in G : gh = hg;\ \textit{para todo } h \in H\}.$$

Es fácil ver que $\zeta(G)$ y $C_G(H)$ son subgrupos de G, aún más, $\zeta(G) \lhd G$.

Además, para todo H subgrupo de G se tiene que $N_G(H) = \{g \in G : g^{-1}Hg = H\}$, llamado el normalizador de H en G, *es el mayor subgrupo de G en el que H es normal.*

Sean g, h elementos en un grupo G, el *conmutador de g y h* es el elemento $(g, h) = g^{-1}h^{-1}gh \in G$. El grupo *conmutador o derivado*, denotado por G', es el subgrupo generado por todos los conmutadores de elementos de G. Debido a la importacia que presenta en el desarrollo de esta tesis, se resalta el siguiente teorema.

Teorema 1.1.3. *Sea G un grupo. Entonces,*

- $G' \lhd G$,
- *El grupo factor G/G' es Abeliano,*
- *Si $H \lhd G$, el grupo factor G/H es Abeliano si y solo si $G' \subseteq H$.*

Sean G y H dos grupos. Una aplicación $\varphi : G \to H$ es un *homomorfismo de grupos* si para todos $g, h \in G$ se tiene que $\varphi(gh) = \varphi(g)\varphi(h)$. No es díficil probar que $\varphi(e_G) = e_H$ y $\varphi(h^{-1}) = (\varphi(h))^{-1}$ para todo $h \in G$.

Definición 1.1.4. *Sea $\varphi : G \to H$ un homomorfismo de grupos entonces el* ***kernel*** *y la* ***imagen*** *de φ estan dados por:*

$$Ker(\varphi) = \{x \in G : \varphi(x) = e_H\},$$

$$Im(\varphi) = \{y \in H : y = \varphi(x), \exists x \in G\},$$

los cuales son subgrupos de G y H respectivamente. Más aún, $Ker(\varphi) \lhd G$.

Dado φ un homomorfismo de grupos, φ es un *monomorfismo* si es inyectivo, es decir, $Ker(\varphi) = \{e_G\}$ y φ es un *epimorfismo* si es sobreyectivo, es decir, $Im(\varphi) = H$. Además, φ es llamado *isomorfismo* si es un homomorfismo inyectivo y sobreyectivo. Si existe un isomorfismo $\varphi : G \to H$, se dice que G y H son isomorfos, y se denota por $G \simeq H$.

Sean H y K subgrupos normales de un grupo G. Diremos que G *es el producto directo de* H *y* K, denotado por $G = H \times K$, si $G = HK$ y $H \cap K = \{e_G\}$. Si solo H es normal en G, pero se cumplen las otras condiciones, diremos que G es *el producto semidirecto* de H por K, denotado por $G = H \rtimes K$.

Puede ser mostrado que en el caso donde G es el producto directo de H y K, la multiplicación es dada componente a componente, es decir, dados $hk, h'k' \in H \times K$, $(hk)(h'k') = (hh')(kk')$. En ambos casos, siendo G el producto directo o semidirecto de H y K, la primera condición de la definición implica que cada elemento $g \in G$ puede ser escrito como un producto $g = hk$, donde $h \in H$ y $k \in K$ y, la segunda condición que tal producto es único. El hecho que el subgrupo K no sea necesariamente normal en G, cuando $G = H \rtimes K$, afecta la forma de multiplicar los elementos. En efecto, dados $h_1, h_2 \in H$ y $k_1, k_2 \in K$, se tiene

$$(k_1h_1)(k_2h_2) = k_1k_2k_2^{-1}h_1k_2h_2 = k_1k_2(h_1^{k_2})h_2.$$

A continuación se tiene una clase especial de grupos, los cuales no solo son de importancia en el presente trabajo, sino que también aparecen de manera natural en el estudio de ciertas propiedades en anillos de grupo (ver [21, Capítulos 2,3,4,7]).

Definición 1.1.5. *Un grupo no Abeliano G donde todos sus subgrupos son normales es llamado un grupo Hamiltoniano.*

Como es bien conocido, todo grupo Hamiltoniano G contiene un subgrupo isomorfo al grupo cuaternio de orden 8, [29, Lema 1.8.4], dado por:

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

más aún, es posible mostrar que en G cualquier par de elementos que no conmuten tienen orden potencia de 2. A continuación se presenta una prueba detallada de la caracterización de los grupos Hamiltonianos.

Teorema 1.1.6. *Un grupo G es Hamiltoniano si y solo si G es el producto del grupo cuaternio de orden 8, un 2-grupo Abeliano elemental E y un grupo Abeliano A cuyos elementos son de orden impar.*

Demostración. Suponga que G es Hamiltoniano y denote por $K = \langle x, y\rangle$ al subgrupo de G que es isomorfo a $\mathcal{Q}_8$. Se mostrará la necesidad en varios pasos.

Afirmación 1. $G = KC_G(K)$**.**

Demostración. Por contradicción, suponga que existe un elemento $g \in G \setminus KC_G(K)$. Entonces, g no conmuta ni con x ni con y y así $y^g \neq g$, caso contrario $y = g$. Dado que G es Hamiltoniano $y^g \in \langle y\rangle$. Si $y^g = 1$, se sigue que $y = 1$, que es una contradicción. Como y y g no conmutan, el caso $y^g = y$ no puede darse. Si $y^g = y^2$, entonces $y^g y^g = y^4 = 1$. Ahora bien, $y^g y^g = g^{-1}y^2 g$. Por tanto, $y^2 = 1$ que también es una contradicción. Luego, $y^g = y^3 = y^{-1}$, es decir, $o(y^g) = 4$. Note que

$$y(gx) = g(g^{-1}yg)x = gy^g x = gy^{-1}x = g(y^{-1}x) = g(xy) = (gx)y$$

Si además $(gx)x = x(xg)$, se tendría que $gx \in C_G(K)$, contradiciendo la escogencia de g. Así, $(gx)x \neq x(xg)$. Por tanto, $x^{gx} \neq x$. Si $x^{gx} = 1$ o $x^{gx} = x^2$ se obtiene $x = 1$ y $x^2 = 1$ respectivamente, lo que es una contradicción. Luego $x^{gx} = x^{-1}$. Además como $x^y = x^{-1}$, se tiene que $y = x^{-1}yx^{-1}$. Ahora,

$$x(gxy) = gx[(gx)^{-1}xgx]y = gx(x^{gx})y = gy = gx^{-1}yx^{-1} = gx^3yx^{-1} = (gxy)x.$$

Por otra parte, $y(gxy) = y(gx)y = (gxy)y$ pues gx conmuta con y. Luego $gxy \in C_G(K)$. Así, $g \in KC_G(K)$ pues $g = gxy(xy)^{-1} = (xy)^{-1}gxy \in KC_G(K)$, lo que contradice la escogencia de g. Por lo tanto, $G = KC_G(K)$. □

Afirmación 2. G **es un grupo de torsión.**

Demostración. Como $K \simeq \mathcal{Q}_8$ es un grupo de torsión, es suficiente mostrar que $C_G(K)$ es de torsión. Sean $x, y \in C_G(K)$ tales que $(x, y) = c \neq 1$. Se tiene que $\langle x \rangle \lhd G$ y $\langle y \rangle \lhd G$, pues G un grupo Hamiltoniano. Luego, $c \in \langle x \rangle \cap \langle y \rangle$. Así, existen enteros positivos r y s tales que $c = x^r = y^s$.

Tome $H = \langle x, y \rangle = \langle x \rangle \langle y \rangle$. Note que $c \in \zeta(H)$. Entonces, por las propiedades del conmutador,

$$c^r = (x, y)^r = (x^r, y) = (c, y) = 1.$$

De lo anterior, *o(c)* es finito. Por lo tanto, *o(x)* y *o(y)* son finitos.

Bajo estos argumentos, si g es un elemento arbitrario en $C_G(K)$ tal que $(x, gy) = (x, y)(x, g)^y = (x, y) = c$. Entonces *o(gy)* es finito. Luego *o(g)* también es finito y como g fue arbitrario, se puede concluir que G es de torsión. □

Afirmación 3. $C_G(K)$ **no contiene elementos de orden** 4**.**

Demostración. Por contradicción suponga que existe $g \in C_G(K)$ un elemento de orden 4. Como se vió en la Afirmación 2, $(x, gy) \neq 1$ y *o(gy)*$= 4$. Observe que $(gy)^x = 1$ implica que, $x(gy)^x x^{-1} = xx^{-1} = 1$, es decir, $gy = 1$ lo que es una contradicción. Ahora, si $(gy)^x = gy$ o $(gy)^x = (gy)^2$ también existe una contradicción. En efecto, en el primer caso se tiene que

$$(x, gy) = x^{-1}(gy)^{-1}x(gy) = x^{-1}y^{-1}g^{-1}x(gy)^x = x^{-1}x^2yg^{-1}xx^{-1}gyx = xyyx = x^4 = 1,$$

y en el segundo caso

$$1 = (gy)^2(gy)^2 = (gy)^x(gy)^x = x^{-1}(gy)^2x = x^{-1}(gy)^x x = x^{-2}x^2gy = gy.$$

Así, $(gy)^x = (gy)^3 = (gy)^{-1}$. Entonces $(gy, x) = (gy)^{-1}(gy)^x = (gy)^{-1}(gy)^{-1} = g^{-2}y^{-2}$. Como $g \in C_G(K)$, $(gy, x) = (y, x) = (x, y)^{-1} = c^{-1}$. Pero $(x, y)^{-1} = (x^{-1}y^{-1}xy)^{-1} = (x^{-1}xyy)^{-1} = y^{-2}$. Esto es, $g^{-2}y^{-2} = y^{-2}$, es decir, $g^2 = 1$, lo que es una contradicción. □

Afirmación 4. $G = \mathcal{Q}_8 \times E \times A$.

Demostración. Sea G como en el Teorema 1.1.6. Observe que si dos elementos en G no conmutan, entonces ellos deben ser 2-elementos. Así, los elementos en $C_G(K)$ de orden impar conmutan con todos los elementos en G y por tanto, el conjunto A de tales elementos es un subgrupo central en G.

Entonces $(xy)^2 = xyxy = xyx^{-1}y$ y, por ser $\langle y \rangle$ normal, $(xy)^2 = y^2 = 1$. Así el conjunto de 2-elementos en $\zeta_G(K)$ es un 2-grupo Abeliano elemental.

De otro lado, si $g, h \in C_G(K)$, se sigue de la Afirmación 3 que *o(g)=o(h)*= 2. Luego, $(gh)^2 = ghgh = ghg^{-1}h$. Como $\langle h \rangle$ es normal, $(gh)^2 = 1$ o $(gh)^2 = h$ y en ambos casos, $(gh)^2 = h^2 = 1$. Por tanto, el conjunto de los 2-elementos en $C_G(K)$ es un 2-grupo Abeliano elemental.

Dado que A es central, claramente $C_G(K) = B \times A$. Además como $x^2 \in B$, entonces $B = \langle x^2 \rangle \times E$, donde E es un 2-grupo Abeliano elemental. Entonces se tiene

$$G = C_G(K)K \simeq (B \times A)\mathcal{Q}_8 = (\langle x^2 \rangle \times E \times A)\mathcal{Q}_8 = E \times A \times \mathcal{Q}_8$$

como se queria demostrar. Además, esto implica que E también es central en G. □

Recíprocamente, si $G = \mathcal{Q}_8 \times A \times E = \mathcal{Q}_8 \times E \times A$, sera suficiente mostrar que para todo $g \in G$, el subgrupo $\langle g \rangle$ es normal. Sea $g = xab$ con $x \in \mathcal{Q}_8$, $a \in A$ y $b \in E$.

Si *o(x)*= 2, entonces $x \in \zeta(G)$ y por tanto, g es central. Pero si *o(x)*= 4, la clase de conjugación de x es $\{x, x^{-1}\}$. Luego, la clase de conjugación de g sera $\{g, x^{-1}ab\}$. Es decir, se debe motrar que $x^{-1}ab \in \langle g \rangle$. Como *o(a)* es impar, se tiene que $s = 2o(\mathrm{a})+1 \equiv 3(mod 4)$. Entonces, $g^s = x^s a^s b^s = x^{-1}ab$. Así, $x^{-1}ab \in \langle g \rangle$, como era deseado. □

Es interesante estudiar estructuras algebraicas con más de dos operaciones binarias, por ejemplo los espacios vectoriales y los anillos. Estos últimos fueron estudiados inicialmente por R. Dedekind y L. Kronecker, aunque fue D. Hilbert quien los definió como se conocen en la actualidad [29].

El anillo R bajo las operaciones de "+" y "$\cdot$" se denota por $\langle R, +, \cdot \rangle$. Además si $\langle R, +, \cdot \rangle$ es un anillo donde "$\cdot$" es una operación conmutativa entonces R es un **anillo**

conmutativo y si existe $1 \in R$, $1 \neq 0$, tal que $1a = a1 = a$ entonces R es un **anillo con unidad**.

Todos los anillos que se presentan a lo largo de este trabajo serán anillos con unidad. Un anillo R es un *dominio* si satisface que $ab = 0$ si y solo si $a = 0$ ó $b = 0$. Los elementos $a, b \in R$ no cero verificando $ab = 0$, son llamados divisores de cero, es decir, un dominio es un anillo sin divisores de cero. Además, un *dominio de integridad* es un dominio conmutativo con unidad.

Un elemento $a \in R$ es llamado *invertible*, si existe un elemento, que es denotado por $a^{-1} \in R$ y llamado *el inverso de* a, tal que $aa^{-1} = a^{-1}a = 1$. El conjunto

$$\mathcal{U}(R) = \{a \in R : \text{ a es invertible}\},$$

es llamado *el grupo de unidades de* R. Un anillo es llamado un *anillo con división* si todos sus elementos no cero son invertibles (es decir, si $R \setminus \{0\} = \mathcal{U}(R)$). Un anillo con división que también es conmutativo es llamado *un cuerpo*.

El siguiente ejemplo ilustra algunos de estos conceptos.

Ejemplo 1.1.7. *Sean i, j y k símbolos y considere el conjunto*

$$\mathbf{H}_{\mathbb{R}} = \{x_0 + x_1 i + x_2 j + x_3 k : \ x_0, x_1, x_2, x_3 \in \mathbb{R}\}.$$

Se define la suma de dos elementos en $\mathbf{H}_{\mathbb{R}}$ por:

$$(x_0+x_1i+x_2j+x_3k)+(y_0+y_1i+y_2j+y_3k) = (x_0+y_0)+(x_1+y_1)i+(x_2+y_2)j+(x_3+y_3)k,$$

La multiplicación es definida distributivamente, con multiplicación de los símbolos i, j y k bajo las siguientes reglas:

$$\begin{aligned} i^2 = j^2 = k^2 &= -1, \\ ij = k &= -ji, \\ jk = i &= -kj, \\ ki = j &= -ik. \end{aligned}$$

Es fácil ver que $\mathbf{H}_{\mathbb{R}}$ *dotado de la suma y la multiplicación definidas anteriormente tiene estructura de anillo, llamado el* anillo de cuaternios reales. *Dado* $\alpha = x_0 + x_1 i + x_2 j + x_3 k$ *un cuaternio, su conjugado es definido por* $\bar{\alpha} = x_0 - x_1 i - x_2 j - x_3 k$ *y su* norma *viene dada por:*

$$\|\alpha\| = \alpha\bar{\alpha} = x_0^2 + x_1^2 + x_2^2 + x_3^2.$$

Ahora, si $\alpha \in \mathbf{H}_{\mathbb{R}}$ *es no cero, entonces* $\|\alpha\| \neq 0$*, así el inverso de* α*, denotado por* α^{-1}*, está dado por* $\alpha^{-1} = \bar{\alpha}/\|\alpha\|$*. Por lo tanto, todo elemento no cero de* $\mathbf{H}_{\mathbb{R}}$ *es invertible, es decir,* $\mathbf{H}_{\mathbb{R}}$ *es un anillo con división y, como lo muestra la multiplicación de los símbolos,* i*,* j *y* k *arriba,* $\mathbf{H}_{\mathbb{R}}$ *no es un cuerpo.*

Restringiendo los coeficientes en $\mathbf{H}_{\mathbb{R}}$ *al cuerpo de los número racionales* $\mathbb{Q}$*, se obtiene de manera análoga el anillo de cuaternios racionales* $\mathbf{H}_{\mathbb{Q}}$*, donde todos los argumentos arriba mencionados son válidos, por tanto* $\mathbf{H}_{\mathbb{Q}}$ *también es un anillo de división. De otro lado, tomando los coeficientes en el cuerpo de los números complejos, se tiene que* $\mathbf{H}_{\mathbb{C}}$ *tiene nuevamente estructura de anillo. Sin embargo, es este caso un cuaternio no cero puede tener norma igual a cero. Así,* $\mathbf{H}_{\mathbb{C}}$ *no es un anillo con división.*

Usando la misma construcción se puede definir

$$\mathbf{H}_{\mathbb{Z}} = \{x_0 + x_1 i + x_2 j + x_3 k |\ x_0, x_1, x_2, x_3 \in \mathbb{Z}\},$$

llamado el anillo de cuaternios enteros. *Dado que* $\mathbf{H}_{\mathbb{Z}} \subset \mathbf{H}_{\mathbb{Q}}$*, y este último es un anillo de división, entonces* $\mathbf{H}_{\mathbb{Z}}$ *no tiene divisores de cero. Sin embargo, el conjunto de sus unidades es bastante pequeño. En efecto, si* $\alpha \in \mathcal{U}(\mathbf{H}_{\mathbb{Z}})$ *entonces, de la definición de norma es claro que* $\|\alpha\|$ *es un entero positivo. También se tiene que* $\alpha\alpha^{-1} = 1$*, y así* $\|\alpha\|\ \|\alpha^{-1}\| = 1$ *y siendo enteros positivos se tiene que* $\|\alpha\| = 1$*; es decir,* $\|\alpha\| = x_0^2 + x_1^2 + x_2^2 + x_3^2 = 1$*. Como* x_0, x_1, x_2, x_3 *son enteros, esta igualdad solo puede ocurrir si* $x_i = 1$ *para algún* $0 \leq i \leq 3$*, y* $x_j = 0$ *para* $j \neq i$*. En consecuencia, el conjunto de unidades de* $\mathbf{H}_{\mathbb{Z}}$ *esta dado por:*

$$\mathcal{U}(\mathbf{H}_{\mathbb{Z}}) = \{\pm 1, \pm i, \pm j, \pm k\}.$$

A diferencia de lo que pasa con grupos, donde todo subgrupo H de G tiene como elemento identidad el mismo de G, en los subanillos esto no siempre ocurre. Por ejemplo, es conocido que $\mathbb{Z} \times \{0\}$ es un anillo bajo las operaciones de suma y producto definidas usualmente sobre $\mathbb{Z} \times \mathbb{Z}$ ($\mathbb{Z} \times \{0\}$ es subanillo de $\mathbb{Z} \times \mathbb{Z}$). Pero $e_{\mathbb{Z}\times\{0\}} = (1, 0)$, el elemento identidad del subanillo, es diferente del elemento identidad del anillo, a saber, $e_{\mathbb{Z}\times\mathbb{Z}} = (1, 1)$ y de hecho, $e_{\mathbb{Z}\times\mathbb{Z}} \notin \mathbb{Z} \times \{0\}$.

Sea a un elemento en un anillo R y $m \in \mathbb{Z}^+$. Si se define el producto ma como la suma de m términos de la forma

$$ma = \underbrace{a + a + a + \cdots + a}_{m-veces},$$

entonces *la característica de* R es cero si no existe un entero positivo m tal que $ma = 0$ para todo $a \in R$. De no ser así, el menor entero positivo m tal que $ma = 0$, para todo $a \in R$, es llamado *la característica de* R y denotado por $car(R)$. Si a, b son elementos en un anillo R y p es un entero positivo, en la expresión

$$(a+b)^p = a^p + \begin{pmatrix} p \\ 1 \end{pmatrix} a^{p-1}b + \begin{pmatrix} p \\ 2 \end{pmatrix} a^{p-2}b^2 + \cdots + \begin{pmatrix} p \\ p-1 \end{pmatrix} ab^{p-1} + b^p$$

cada coeficiente es divisible por p. Así las cosas, el coeficiente $\begin{pmatrix} p \\ k \end{pmatrix} \equiv 0 \ mod(p)$, $1 \leq k \leq p-1$. Es claro el siguiente resultado.

Lema 1.1.8. *Sea R un anillo de característica prima p. Entonces, para $x, y \in R$ y un entero positivo n, se tiene que:*

$$(x+y)^{p^n} = x^{p^n} + y^{p^n}.$$

Los ideales han sido una herramienta importante en el estudio de la geometría algebraica desde 1882, cuando Leopold Kronecker realizó las primeras investigaciones alrededor de esta temática. Sin embargo, el concepto actual es atríbuido a Richard Dedekind [29] quien desarrolló la teoría algebraica de números.

Definición 1.1.9. *Un subconjunto L no vacío de un anillo R es un* ***ideal a izquierda*** *de R si las siguientes condiciones se verifican:*

(I_1) *Si $x, y \in L$, entonces $(x - y) \in L$.*

(I_2) *Si $x \in L$ y $a \in R$, entonces $ax \in L$.*

Análogamente, se define ideales a derecha. Un subconjunto no vacío L de un anillo R es un *ideal* (algunas veces llamado ideal bilateral) si él es tanto ideal a izquierda como ideal a derecha de R. Los subconjuntos $\{0\}$ y R de un anillo R son siempre ideales de R. Un ideal L de R, diferente de estos, es llamado un *ideal propio*. Ahora, suponga que L es un ideal a izquierda de un anillo R que contiene un elemento invertible a, entonces $L = R$ y por tanto no es ideal propio. En efecto, sea $a \in L$ invertible con L ideal a izquierda de R. Entonces, $1 = a^{-1}a \in L$ y así $x = x1 \in L$ para todo $x \in R$. Luego $L = R$.

Un ideal propio I de un anillo conmutativo R es llamado *ideal primo de R* si dados $a, b \in R$ y $ab \in I$ implica que $a \in I$ ó $b \in I$. Además, I es llamado ideal maximal de R si, siempre que J ideal de R e $I \subseteq J \subseteq R$, entonces $J = I$ ó $J = R$. Es decir, el único ideal que contiene estrictamente a un ideal maximal I, es el anillo completo R. El siguiente resultado caracteriza los ideales primos y maximales.

Teorema 1.1.10. *Sean R un anillo conmutativo con unidad e I un ideal de R,*

(i) I es un ideal primo si y solo si R/I es dominio entero.

(ii) I es un ideal maximal si y solo si R/I es cuerpo.

Definición 1.1.11. *Dos ideales I y J de un anillo R son llamado primos entre sí (o comaximales) si $I + J = R$.*

Para ideales I, J primos entre sí se tiene que $I \cap J = IJ$. Claramente dos ideales I y J son primos entre sí, si y solo si existen $x \in I$, $y \in J$ tales que $x + y = 1$.

A continuación un teorema clásico, llamado *Teorema Chino del Residuo*:

Teorema 1.1.12. *Si $I_1, I_2, \dots I_n$, son ideales primos dos a dos, entonces* $\prod_{i=1}^{n} I_i = \bigcap_{i=1}^{n} I_i$, *y por tanto,*

$$\frac{R}{\prod I_n} \simeq \frac{R}{I_1} \times \frac{R}{I_2} \times \cdots \times \frac{R}{I_n}.$$

Un elemento e en un anillo R es llamado un *idempotente* si $e^2 = e$. Claramente, 0 y 1 son elementos idempotentes. Un idempotente diferente de estos es llamado *no trivial*. Un elemento a en un anillo R es llamado *nilpotente* si exite $n \in \mathbb{N}$ tal que $a^n = 0$. Para los ideales se tiene la siguiente analogía:

Definición 1.1.13. *Dado R un anillo e I un ideal de R:*

- *I es llamado ideal nil si todo elemento $a \in I$ es nilpotente. I será llamado nil de exponente acotado, si existe $n \in \mathbb{N}$ tal que $a^n = 0$ para todo $a \in I$*
- *I es llamado ideal nilpotente si existe un entero $n > 1$ tal que*

$$I^n = \Big\{ \sum x_1 x_2 \cdots x_n : x_i \in I \Big\} = (0)$$

Note que, de acuerdo a la definición arriba, un ideal I de un anillo R es nilpotente si y solo si existe un entero positivo n tal que $x_1 x_2 \cdots x_n = 0$ para todas las posibles escogencias de elementos $x_1, x_2, x_3, \dots, x_n \in I$. En consecuencia, es claro que un ideal nilpotente es también un ideal nil de exponente acotado, pero existen ejemplos que muestran que su recíproco no es cierto, uno de ellos es el siguiente:

Ejemplo 1.1.14. *Sean p un número primo y $n \in \mathbb{N}$ con $n > 1$. Note que todos los subgrupos de $\mathbb{Z}_{p^n}$ forman la siguiente cadena*

$$0 < p^{n-1}\mathbb{Z}_{p^n} < p^{n-2}\mathbb{Z}_{p^n} < \cdots < p^2\mathbb{Z}_{p^n} < p\mathbb{Z}_{p^n} < \mathbb{Z}_{p^n}.$$

Estos resultan ser los únicos ideales de $\mathbb{Z}_{p^n}$, además todos son nilpotentes. Note que $p\mathbb{Z}_{p^n}$ contiene todos los ideales nilpotentes de $\mathbb{Z}_{p^n}$. Ahora, si

$$I = \{(x_n) \in \prod_{n \in \mathbb{N}^*} \mathbb{Z}_{p^n} : x_n \in I_n \text{ y } (x_n) \text{ tiene un número finito de componentes no cero } \},$$

donde $\prod_{n\in\mathbb{N}^*}\mathbb{Z}_{p^n}$ *denota el producto directo de los* Z_{p^n} *dotado de la suma y producto usuales. Así, el ideal* I *es un ideal nil pues cada elemento tiene un número finito de componentes no cero. Observe que, dado un* $m \in \mathbb{N}^*$ *existe un producto de* $m+1$ *elementos en* I *cuyo producto no es nulo, es decir,* I *no es un ideal nilpotente.*

E. Noether en su libro *Nichtkommutative Algebra* [26], realizó un estudio sistemático de los módulos, concepto que apareció de manera implícita en los trabajos de R. Dedekind sobre teoría de números.

Definición 1.1.15. *Sean* R *un anillo y* M *un grupo Abeliano (en notación aditiva).* M *es llamado un* ***módulo a izquierda*** *o* R*-módulo, si existe una aplicación* $\mu_l : R\times M \to M$ *dada por* $\mu_l(a,m) = am$*, que verifica:*

(M_1) $(a+b)m = am + bm$,

(M_2) $a(m_1+m_2) = am_1 + am_2$,

(M_3) $a(bm) = (ab)m$,

(M_4) $1m = m$,

para todos a, $b \in R$ *y para todos* m, m_1, $m_2 \in M$.

De manera similar, se define *módulo a derecha* o módulo-R, considerando $\mu_r : M \times R \to M$ dada por $\mu_r(m,a) = ma$. Si K es un cuerpo, entonces el concepto de K-módulo coincide con la noción de K-espacio vectorial.

Es claro que todo anillo R puede ser visto como módulo a izquierda o a derecha sobre si mismo. Cuando este sea el caso, se denotara por ${}_RR$ y R_R respectivamente.

Ahora bien si G es un grupo Abeliano, $g \in G$ y $m \in \mathbb{Z}$, definiendo

$$ma = \begin{cases} \underbrace{a+a+a+\cdots+a}_{m-veces}, & m \in \mathbb{N}; \\ 0, & m = 0; \\ m(-a), & m \notin \mathbb{N}, \end{cases}$$

G tiene estructura de $\mathbb{Z}$-módulo.

Un subconjunto no vacío N de un R-módulo M es *un R-submódulo* de M si para todo $x, y \in N$ se tiene que $x + y \in N$ y $rn \in N$ para todo $r \in R$ y $n \in N$. Así definido, todo módulo M posee por lo menos dos submódulos, M y (0). Si N es un submódulo de M diferente de estos, entonces N es llamado *submódulo propio de M*. Además, M es llamado *módulo simple* si sus únicos submódulos son los triviales.

Un R-módulo M satisface la *condición de cadena descendente*, ($C.C.D$), si toda cadena de submódulos de M, $M_1 \supset M_2 \supset \cdots M_i \supset \cdots$ termina. Esto es, si existe un índice t tal que $M_t = M_{t+i}$ para todo $i \in \mathbb{N}$. Si los submódulos de M satisfacen la $C.C.D$, se dice que M es un *módulo Artiniano*.

Sea R un anillo conmutativo. El R-módulo A es llamado un *álgebra a izquierda* o R-álgebra, si existe una multiplicación definida en A tal que con la adición inicial de A y esta multiplicación, A es un anillo que satisface la siguiente condición:

$$r(ab) = (ra)b = a(rb),$$

para todos $a, b \in A$ y todo $r \in R$.

Si A como anillo tiene unidad, dados $r \in R$ y $a \in A$ se tiene que:

$$ra = r(a1) = a(r1) = ar,$$

y como $R1_A \simeq R$, entonces $R \subseteq \zeta(A)$.

Los cuaternios $\mathbf{H}_{\mathbb{R}}$, definidos en el Ejemplo 1.1.7, son un $\mathbb{R}$-álgebra. Note que si R es un anillo conmutativo, entonces el anillo $R[X] = \{p(x) : \ coef(p) \in R\}$ de polinomios con coeficientes en R y el anillo de matrices cuadradas $M_n(R) = \{(a_{ij})_{i,j=1}^n : \ a_{ij} \in R\}$ son ejemplos de R-álgebras.

1.2. Semisimplicidad

Es conocido que todo subespacio W de un K-espacio vectorial V es sumando directo de V ($V = W \oplus W^{\perp}$). Esto no es cierto en el caso más general de módulos sobre un

anillo arbitrario, por ejemplo, $\mathbb{Z}$ no es un sumando directo de $\mathbb{Q}$ como $\mathbb{Z}$-módulo. A continuación se presenta la clase de módulos que si tienen esta propiedad y que son de suma importancia en el desarrollo del presente trabajo.

Definición 1.2.1. *Un R-módulo M es llamado semisimple si cada submódulo de M es un sumando directo de M.*

Como consecuencia de la definición se tiene que un submódulo no nulo N de un R-módulo M semisimple, es semisimple y contiene un submódulo N' simple. A continuación se caracterizan los módulos semisimples.

Teorema 1.2.2. *Sea M un R-módulo. Entonces las siguientes condiciones son equivalentes:*

1. *M es semisimple,*
2. *M es suma directa de submódulos simples, y*
3. *M es suma (no necesariamente directa) de submódulos simples.*

Así, dado un submódulo N de un módulo semisimple M siempre se puede encontrar un subconjunto de índices $J_0 \subset I$ tal que $M = N \oplus N_0$ con $N_0 = \oplus_{i \in J_0} M_i$. Luego

$$N \simeq \frac{M}{N_0} = \frac{\oplus_{i \in I} M_i}{\oplus_{i \in J_0} M_i} \simeq \oplus_{i \in I \setminus J_0} M_i,$$

nos lleva al siguiente resultado.

Corolario 1.2.3. *Sean $M = \oplus_{i \in I} M_i$ una descomposición de un módulo semisimple M como suma directa de submódulos simples y N un submódulo de M. Entonces existe un subconjunto $J \subset I$ tal que $N \simeq \oplus_{j \in J} M_j$.*

Dado que todo anillo R puede ser visto como R-módulo se tiene la siguiente definición natural.

Definición 1.2.4. *Un anillo R es semisimple si el módulo a izquierda sobre si mismo ${}_R R$ es semisimple.*

Como los submódulos de ${}_RR$ son los ideales a izquierda de R, entonces R es semisimple si y solo si todo ideal a izquierda de R es un sumando directo de R. La siguiente es una caracterización de semisimplicidad en términos de elementos idempotentes.

Teorema 1.2.5. *Un anillo R es semisimple si y solo si todo ideal a izquierda L de R es de la forma $L = Re$, donde $e \in R$ es un elemento idempotente.*

Los siguientes dos teoremas nos muestran en parte la estructura de los anillos semisimples. El primero de ellos, conocido en la literatura como *Teorema de descomposición de Peirce*, caracteriza los anillos semisimples como suma directa de ideales a izquierda minimales, usando idempotentes. El segundo resultado, conocido como *Teorema de Wedderburn-Artin*, describe la estructura de anillos semisimples como suma directa de ideales bilaterales minimales.

Teorema 1.2.6 (Teorema de descomposición de Peirce)**.** *Sea $R = \oplus_{i=1}^{t} L_i$ una descomposición de un anillo semisimple como una suma directa de ideales a izquierda minimales. Entonces, existe una familia $\{e_1, e_2, \ldots, e_t\}$ de elementos de R tales que:*

1. *$e_i \neq 0$ es un elemento idempotente, $1 \leq i \leq t$.*
2. *Si $i \neq j$, entonces $e_i e_j = 0$.*
3. *$1 = e_1 + e_2 + \cdots + e_t$*
4. *e_i no puede ser escrito en la forma $e_i = e_i' + e_i''$ donde e_i' y e_i'' son idempotentes tales que e_i', $e_i'' \neq 0$ y $e_i' e_i'' = 0$, $1 \leq i \leq t$.*

Recíprocamente, si existe una familia de idempotentes $\{e_1, e_2, \ldots, e_t\}$ satisfaciendo las condiciones anteriores, entonces los ideales a izquierda $L_i = Re_i$ son minimales y $R = \oplus_{i=1}^{t} L_i$.

Si la familia de idempotentes del teorema anterior satisface las condiciones *1. 2.* y *3.*, se denomina **familia completa de idempotentes ortogonales**. Un idempotente satisfaciendo la condición *4.* anterior, es llamado **primitivo**.

Teorema 1.2.7 (Teorema de Wedderburn-Artin)**.** *Un anillo R es semisimple si y solo si R es una suma directa única de álgebras de matrices sobre anillos con división*

$$R \simeq M_{n_1}(D_1) \oplus \cdots \oplus M_{n_s}(D_s).$$

Sea R un anillo. El *radical de Jacobson de* R, denotado por $J(R)$, es la intersección de todos sus ideales a izquierda maximales. Cuando $J(R) = (0)$ se dice que R *es semisimple* o que no tiene radical de Jacobson. Por el Lema de Zorn se conoce que todo anillo no cero con unidad tiene por lo menos un ideal maximal [29, Lema 2.4.3], entonces $J(R)$ siempre existe. Es posible mostrar que $J(R)$ es un ideal bilateral [29, Proposición 2.7.4], luego se puede contruir el anillo cociente $R/J(R)$. Como consecuencia inmediata de la definición se tiene lo siguiente:

Teorema 1.2.8. *Dado un anillo R. El anillo cociente $R/J(R)$ es semisimple, esto es, $J(R/J(R)) = (0_{R/J(R)})$.*

Una relación que nos interesa entre el radical de Jacobson $J(R)$ y el grupo de unidades del anillo R, $\mathcal{U}(R)$ es la siguiente.

Teorema 1.2.9. *Sea I un ideal de un anillo R. Entonces, $I \subseteq J(R)$ si y solo si cada elemento de la clase lateral $1 + I$ tiene inverso en R, es decir, esta contenido en $\mathcal{U}(R)$.*

Suponga que $I = \langle a \rangle$ es el ideal generado por $a \in J(R)$, usando el anterior teorema, se puede caracterizar el radical de Jacobson en términos de los elementos del anillo.

Corolario 1.2.10. *Sea R un anillo.*

1. *$a \in J(R)$ si y solo si $(1 - ra) \in \mathcal{U}(R)$ para todo $r \in R$.*
2. *$r \in \mathcal{U}(R)$ si y solo $r + J(R) \in \mathcal{U}(R/J(R))$.*
3. *El único elemento idempotente en $J(R)$ es el cero.*
4. *Cada ideal nil I de R esta contenido en $J(R)$.*

Recuerde que todo ideal nilpotente es también un ideal nil, pero no recíprocamente (ver 1.1.14). Sin embargo, en presencia de la $C.C.D$ estos ideales coinciden.

Teorema 1.2.11 (Hopkins)**.** *Sea R un anillo Artiniano. Entonces $J(R)$ es un ideal nilpotente de R y cada ideal nil es nilpotente.*

Si un ideal I contiene un elemento idempotente e, es claro que $e^n = e$ para todo $n \in \mathbb{N}$. Lo anterior muestra que I no puede ser un ideal nilpotente, luego por el Teorema 1.2.5 se tiene que un anillo semisimple no contiene ideales nilpotentes. El recíproco es un resultado de Brauer, [29, Lema 2.7.15].

Lema 1.2.12. *Sea L un ideal a izquierda minimal de un anillo R. Entonces $L^2 = (0)$ o L es de la forma $L = Re$, donde $e \in R$ es un idempotente.*

El siguiente resultado es la base para comprender la estructura de las álgebras de grupo semisimples, además de caracterizar los anillos semisimples en otro sentido.

Teorema 1.2.13. *Sea R un anillo semisimple. Entonces, R es Artiniano y las siguientes condiciones se verifican*

1. *R no contiene ideales bilaterales nilpotentes no nulos.*
2. *R no contiene ideales a izquierda nilpotentes no nulos.*
3. *$J(R) = (0)$.*

Recíprocamente, si R es Artiniano y una de las anteriores es cierta, entonces R es semisimple.

Los números racionales $\mathbb{Q}$ se construyen básicamente a partir del anillo de los enteros $\mathbb{Z}$. Imitando la construcción anterior para un dominio entero R, se obtiene el llamado *cuerpo de fracciones de R*. Para llevar a cabo este proceso es necesario el siguiente concepto.

Definición 1.2.14. *Sea R un anillo. Un subconjunto S de R es multiplicativamente cerrado si $1 \in R$ y S es cerrado bajo la multiplicación.*

Sea $\equiv$ la relación en $R \times S$ definida por $(a, s) \equiv (b, t)$ si y solo si $(at - bs)u = 0$ para algún $u \in S$. Es claro que esta relación es reflexiva y simétrica. Para probar que es transitiva, suponga que $(a, s) \equiv (b, t)$ y $(b, t) \equiv (c, u)$. Entonces existen v y $w \in S$ tales que $(at - bs)v = 0$ y $(bu - ct)w = 0$. Eliminando b en estas dos ecuaciones se tiene que $(au - cs)tvw = 0$. Como S es cerrado bajo la multiplicación, $tvw \in S$. Así, $(a, s) \equiv (c, u)$. Luego se tiene que $\equiv$ es una relación de equivalencia en $R \times S$, donde a/s denotará la clase de equivalencia de (a, s), es decir, $[(a, s)] = \{(b, t) \in R \times S : (a, s) \equiv (b, t)\}$.

Sea $S^{-1}R$ es el conjunto de las clases de equivalencia dotado de las siguientes operaciones:

$$(a/s) + (b/t) = (at + bs)/st$$

$$(a/s)(b/t) = ab/st.$$

Entonces $S^{-1}R$ es un anillo conmutativo con elemento identidad, llamado *el anillo de fracciones* de R con respecto a S. Luego, la aplicación $f : R \to S^{-1}R$, $x \mapsto f(x) = x/1$ es un homomorfismo de anillos que en general no es inyectivo. En el caso que R sea un dominio de integridad y $S = R - \{0\}$, entonces $S^{-1}R$ es un cuerpo, denominado *cuerpo de fracciones de* R y cumple con las siguiente propiedad universal.

Proposición 1.2.15. *Sea $g : A \to B$ un homomorfismo de anillos tal que $g(s)$ es una unidad de B para todo $s \in S$. Entonces existe un único homomorfismo de anillos $h : S^{-1}A \to B$ tal que $g = h \circ f$.*

Así, el anillo $S^{-1}R$ y el homomorfismo $f : R \to S^{-1}R$ tienen las siguientes propiedades:

1. Si $s \in S$, entonces $f(s)$ es una unidad en $S^{-1}R$,
2. $f(a) = 0$ implica que $as = 0$ para algún $s \in S$, y
3. Cada elemento de $S^{-1}R$ es de la forma $f(r)f(s)^{-1}$ para algún $r \in R$ y algún $s \in S$.

Más aún, estas tres condiciones determinan como es el anillo $S^{-1}R$ salvo isomorfismos. Más precisamente se tiene.

Corolario 1.2.16. *Si $g : A \to B$ es un homomorfismo de anillos tal que:*

1. *Si $s \in S$, entonces $g(s)$ es una unidad en B;*
2. *Si $g(a) = 0$, entonces $as = 0$ para algún $s \in S$;*
3. *Cada elemento de B es de la forma $g(a)g(s)^{-1}$.*

Entonces existe un único isomorfismo $h : S^{-1}A \to B$ tal que $g = h \circ f$.

1.3. Anillos de Grupo

Dado un grupo G y R un anillo con unidad, se desea construir un R-módulo, teniendo los elementos de G como base, y usando conjuntamente las operaciones de G y R para definir una estructura de anillo sobre él. Se denota por RG al siguiente conjunto:

$$RG = \left\{ \sum_{g \in G} \alpha_g g : \alpha_g \in R \text{ y } \alpha_g \neq 0 \text{ para un número finito de } \alpha_g \right\}.$$

Note que los elementos en RG son sumas finitas. Dado un elemento $\alpha = \sum_{g \in G} \alpha_g g$ el *soporte de* α es el conjunto de los elementos de G que efectivamente aparecen en la suma, es decir,

$$supp(\alpha) = \{g \in G : \alpha_g \neq 0\}.$$

Es fácil verificar que el conjunto RG es un anillo con unidad con las operaciones de suma y producto dadas por:

$(+)$ $(\sum_{g \in G} \alpha_g g) + (\sum_{g \in G} \beta_g g) = \sum (\alpha_g + \beta_g) g,$

$(\cdot)$ $\sum_{g \in G} \alpha_g g \sum_{h \in G} \beta_h h = \sum_{g,h \in G} (\alpha_g \beta_h) gh = \sum_{u \in G} c_u u$, donde $c_u = \sum_{gh = u} \alpha_g \beta_h.$

con unidad dada por $1_{RG} = \sum_{g \in G} \alpha_g g$, donde $\alpha_1 = 1$ y $\alpha_g = 0$, para todo $g \neq 1$. Además, $0_{RG} = \sum_{g \in G} 0_g g$ y $-\alpha = \sum_{g \in G} (-\alpha_g) g$ es el inverso aditivo de $\alpha \in RG$.

Note que RG tiene estructura de R-módulo, con el producto $\mu : R \times RG \to RG$ definido por la expresión:

$$(\lambda, \sum_{g \in G} \alpha_g g) \overset{\mu}{\mapsto} \sum_{g \in G} (\lambda \alpha_g) g.$$

Si R es un anillo conmutativo se tiene que RG es un R-álgebra. En particular, tome $R = F$ un cuerpo, FG es un F-álgebra, más aún FG es un F-espacio vectorial.

Definición 1.3.1. *El conjunto RG con las operaciones anteriormente definidas es llamado el* ***anillo de grupo del grupo G sobre el anillo*** *R. Además, si R es un anillo conmutativo, entonces RG también es llamado el* ***álgebra de grupo de G sobre*** *R.*

Observación 1.3.2. *La aplicación $i : G \to RG$ dada por $x \mapsto i(x) = \sum_{g \in G} \alpha_g g$ donde $\alpha_x = 1$ y $\alpha_g = 0$ si $g \neq x$, nos permite ver a G inmerso en RG, que se denota por $G \hookrightarrow RG$. Esta inmersión muestra claramente que G resulta ser una R-base para RG. Además, si R es conmutativo y G finito entonces se puede establecer que el rango de RG sobre R, $rank(RG)$, es precisamente $|G|$.*

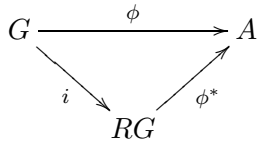
Ahora, considere $\upsilon : R \to RG$ la función dada por $\upsilon(r) = \sum_{g \in G} \alpha_g g$ donde $\alpha_{1_G} = r$ y $\alpha_g = 0$ si $g \neq 1_G$. Así, υ define un monomorfismo de anillos y R puede verse como subanillo de RG.

Teniendo presente las anteriores identificaciones, dados $r \in R$ y $g \in G$, se tiene que $rg = gr$ en RG. Por tanto, si R es conmutativo, $R \subseteq \zeta(RG)$.

A continuación una importante propiedad para los anillos de grupo.

Proposición 1.3.3. *Sean G un grupo y R un anillo. Dado cualquier anillo A tal que $R \subset A$ y cualquier función $\phi : G \to A$ tal que $\phi(gh) = \phi(g)\phi(h)$, para todos $g, h \in G$, existe un único homomorfismo de anillos $\phi^* : RG \to A$, el cual es R-lineal y tal que*

$\phi^* \circ i = \phi$ donde $i : G \hookrightarrow RG$ es la inclusión dada arriba. Es decir, se tiene el siguiente diagrama conmutativo:



Además, si R es central en A (y así A es un R-álgebra) entonces ϕ^* es un homomorfismo de R-álgebras. Luego, se tiene el siguiente caso especial de la anterior proposición:

Corolario 1.3.4. *Sea $\phi : G \to H$ un homomorfismo de grupos. Entonces,*

1. *Existe un único homomorfismo de anillos $\phi^* : RG \to RH$ tal que $\phi^*(g) = \phi(g)$, para todo $g \in G$,*
2. *Si R es un anillo conmutativo, ϕ^* es un homomorfismo de R-álgebras,*
3. *Si ϕ es un monomorfismo (respectivamente epimorfismo) entonces ϕ^* es un monomorfismo (respectivamente epimorfismo).*

Si $H = \{1\}$, entonces del Corolario 1.3.4, la aplicación $G \to \{1\}$ induce el homomorfismo de anillos $\varepsilon : RG \to R$ dado por:

$$\varepsilon\Big(\sum_{g\in G} \alpha_g g\Big) = \sum_{g\in G} \alpha_g.$$

Definición 1.3.5. *El homomorfismo $\varepsilon : RG \to R$ definido arriba, es llamado la* aplicación de aumento de *RG y su núcleo, $Ker(\varepsilon) = \Delta(G)$, es llamado* ideal de aumento de *RG.*

Considere $\alpha = \sum_{g\in G} \alpha_g g \in RG$. Si $\alpha \in \Delta(G)$ entonces $\varepsilon(\sum_{g\in G} \alpha_g g) = \sum_{g\in G} \alpha_g = 0$. Luego, se obtiene que:

$$\alpha = \sum_{g\in G} \alpha_g g - \sum_{g\in G} \alpha_g = \sum_{g\in G} \alpha_g (g-1).$$

Claramente, todos los elementos de la forma $g - 1$ con $g \in G$, pertenecen a $\Delta(G)$, es decir, $\{g - 1 : g \in G \text{ y } g \neq 1\}$ es un conjunto de generadores de $\Delta(G)$ sobre R. Además, es posible mostrar que este conjunto es linealmente independiente. Así,

Proposición 1.3.6. *El conjunto* $\{g-1 : g \in G, \quad g \neq 1\}$ *es una base para* $\Delta(G)$ *sobre* R *y, por tanto:*

$$\Delta(G) = \left\{ \sum_{g \in G} \alpha_g (g-1) : g \in G,\ \alpha_g \in R \right\},$$

donde como es usual, solo un número finito de coeficientes $\alpha_g \neq 0$.

Note que si R es un anillo conmutativo y G es un grupo finito, entonces $\Delta(G)$ es un R-módulo libre de rango $rank(\Delta(G)) = |G| - 1$.

Sea N un subgrupo normal de G, entonces el homomorfismo natural $G \to G/N$ induce el homomorfismo de anillos $\varepsilon_N : RG \to R(G/N)$, cuyo núcleo será denotado por $\Delta(G, N)$. Observe que $\Delta(G, N)$ es el ideal formado por sumas finitas de términos de la forma $rg(n-1)$, con $r \in R$, $g \in G$ y $n \in N$. En particular, cuando $N = G$, se tiene que $\varepsilon = \varepsilon_G$ es la aplicación de aumento y que $\Delta(G) = \Delta(G, G)$ es el ideal de la Definición 1.3.5, que está formado por términos de la forma $r(g-1)$, con $r \in R$ y $g \in G$ como se vió en el resultado anterior. El siguiente teorema, debido a Coleman [29, Teorema 6.3.1] permite clasificar los ideales nilpotentes de RG.

Teorema 1.3.7. *Sea* G *un grupo y* R *un anillo con* $car(R) = p^m$*, para algún* p*-primo. Entonces el ideal de aumento* $\Delta(G)$ *de* RG *es nilpotente si y solo si* G *es un* p*-grupo finito.*

Corolario 1.3.8. *Sean* G *un grupo y* R *un anillo conmutativo con* $car(R) = p^m$ *siendo* p *un primo. Si* N *es un subgrupo normal finito de* G*, entonces* $\Delta(G, N)$ *es un ideal nilpotente si y solo si* N *es un* p*-grupo.*

Demostración. Como $\Delta(G, N) = RG(\Delta(N)) = (\Delta(N))RG$, tenemos que

$$(\Delta(G, N))^n = (RG(\Delta(N)))^n = RG(\Delta(N))^n.$$

Luego, el resultado se sigue del teorema anterior. □

Recuerde que un anillo Artiniano R es semisimple si y solo si R no contiene ideales nilpotentes (Teorema 1.2.13). Para álgebras de grupo FG donde G es un grupo finito, la

semisimplicidad esta dada como consecuencia del siguiente teorema debido a Maschke [29, Teorema 3.4.7].

Teorema 1.3.9 (Teorema de Maschke)**.** *Sea G un grupo. Entonces el anillo de grupo RG es semisimple si y solo si las siguientes condiciones se verifican*

1. *R es un anillo semisimple.*

2. *G es finito.*

3. *$|G|$ es invertible en R.*

Como F es un cuerpo con $car(F) = p$, entonces F es siempre semisimple. Así, $|G|$ será invertible en F si y solo si $|G| \neq 0$ en F, es decir,

Corolario 1.3.10. *Sea G un grupo finito y F un cuerpo. Entonces, FG es semisimple si y solo si $car(F) \nmid |G|$.*

El siguiente resultado es consecuencia del anterior Corolario y de [29, Teorema 6.2.2].

Teorema 1.3.11. *Sea FG el álgebra de grupo del grupo finito G sobre el cuerpo F con $car(F) = p \geq 0$. Entonces FG tiene un ideal nilpotente (no cero) si y solo si $p > 0$ y $p||G|$.*

Sea $G = \langle a \rangle$ con $a^n = 1$ y $a^{n-1} \neq 1$, el grupo cíclico de orden n y F un cuerpo tal que $car(F) \nmid |G|$. La aplicación $\phi : F[x] \to FG$ dada por

$$F[x] \ni f \overset{\phi}{\mapsto} f(a) \in FG,$$

es un epimorfismo de anillos y por tanto,

$$FG \simeq \frac{F[x]}{Ker(\phi)}.$$

Dado que $F[x]$ es un dominio de ideales principales, el $Ker(\phi)$ es el ideal generado por el polimonio mónico f_0 de menor grado, tal que $f_0(a) = 0$. Bajo el último isomorfismo,

$$FG \ni a \mapsto x + \langle f_0 \rangle \in \frac{F[x]}{\langle f_0 \rangle}.$$

Dado que, $a^n = 1$ se sigue que $x^n - 1 \in Ker(\phi)$. Note que si $f = \sum_{i=0}^{r} \alpha_i x^i$ es un polinomio de grado $r < n$, se tiene que $f(a) = \sum_{i=0}^{r} \alpha_i a^i \neq 0$ debido a que $\{1, a, a^2, \ldots, a^r\}$ es linealmente independiente sobre F. Así, $Ker(\phi) = \langle x^n - 1 \rangle$, y por tanto

$$FG \simeq \frac{F[x]}{\langle x^n - 1 \rangle}.$$

Sea $x^n - 1 = f_1 f_2 \cdots f_t$ la descomposición de $x^n - 1$ como producto de polinomios irreducibles en $F[x]$. Dado que $car(F) \nmid |G|$, el polinomio es separable y así, $f_i \neq f_j$ si $i \neq j$. [1] Por el Teorema Chino del Residuo 1.1.12, el anterior isomorfismo se puede reescribir como:

$$FG \simeq \frac{F[x]}{\langle f_1 \rangle} \oplus \frac{F[x]}{\langle f_2 \rangle} \oplus \cdots \oplus \frac{F[x]}{\langle f_t \rangle}. \tag{1.1}$$

Los anillos de grupo semiprimos son decisivos en la clasificación de las álgebras de grupo FG cuyo grupo de unidades $\mathcal{U}(FG)$ satisface una identidad de grupo (su definición se presenta en el siguiente capítulo). Un anillo R es *semiprimo* si no contiene ideales (no cero) nilpotentes. Passman en [27, Lema 4.2.11.], demuestra que un anillo es semiprimo si y solo si no contiene ideales, no cero, de cuadrado cero. En el contexto de los anillos de grupo se tiene la siguiente clasificación, debido a Passman:

Teorema 1.3.12. *Sea FG el álgebra de grupo del grupo G sobre un cuerpo F. Las siguientes afirmaciones son verdaderas:*

1. *([27, Teorema 4.2.12]) Si $car(F) = 0$, entonces FG es semiprimo,*
2. *([27, Teorema 4.2.13]) Suponga que $car(F) = p > 0$. Las siguientes afirmaciones son equivalentes:*
   a) *FG es semiprimo.*
   b) *G no contiene subgrupos normales finitos de orden divisible por p.*

[1] Un polinomio irreducible $f(x) \in F[x]$ es llamado *polinomio separable* si todas sus raíces son simples. Luego, un polinomio $f(x) \in F[x]$ es llamado *separable* si todos sus factores irreducibles son separables.

c) $\Phi(G) = \{g \in G : |cl_G(g)| < \infty\}$ *es un* p'*-grupo, donde* $cl_G(g) = \{h^{-1}gh : h \in G\}$*, es la clase de conjugación de* g *en* G*.*

d) $\eta(FG) = (0)$*, donde* $\eta(FG)$ *denota la suma de todos los ideales nilpotentes de* FG*.*

1.4. Unidades en el anillo de grupo

Desde comienzos de los $90'$s, y ya con algunos resultados en la decada anterior, el grupo de unidades $\mathcal{U}(RG)$ de RG, viene presentando mucha actividad debido en parte, a la conjetura de Hartley y algunos problemas relacionados con esta. La conjetura que B. Hartley estableció, fue un intento por encontrar una conexión entre las estructuras aditiva y multiplicativa del álgebra de grupo FG de un grupo G sobre el cuerpo F. Como es conocido, el álgebra FG es una buena fuente de unidades.

Como se vió al principio de este escrito, el conjunto

$$\mathcal{U}(R) = \{x \in R : xy = yx = 1, \text{ para algún } y \in R\},$$

es llamado el grupo (multiplicativo) de unidades de R. Ahora, si G es un grupo y R un anillo entonces $\mathcal{U}(RG)$ simboliza *el grupo de unidades del anillo de grupo* RG*.*

Como $\varepsilon : RG \to R$ define un homomorfismo de anillos, entones $\varepsilon(u) \in \mathcal{U}(R)$ para todo $u \in \mathcal{U}(RG)$. Se denotará por $\mathcal{U}_1(RG)$ al subgrupo de unidades de aumento 1 en $\mathcal{U}(RG)$, es decir,

$$\mathcal{U}_1(RG) = \{u \in \mathcal{U}(RG) : \varepsilon(u) = 1\}.$$

Sea $u \in \mathcal{U}(\mathbb{Z}G)$ entonces $\varepsilon(u) = \pm 1$ y observe que

$$\mathcal{U}(\mathbb{Z}G) = \pm\mathcal{U}_1(\mathbb{Z}G).$$

Es conocido en la literatura, que si R es cualquier anillo, entonces:

$$\mathcal{U}(RG) = \mathcal{U}(R) \times \mathcal{U}_1(RG).$$

1.5. Teoría de representación

Durante el Coloquio de Matemáticas de 1879 en Evanston-Illinois, F. Klein planteó la posibilidad de representar un grupo abstracto dado por un grupo de transformaciones lineales. Esta idea inquietó a varios investigadores de la época, entres los que estuvieron T. Molien, G. Frobenius, I. Schur, W. Burnside y H. Maschke. A ellos se les atribuye las bases de la teoría de representación de grupos. Sin embargo, quien presentó estas ideas de manera sistemática fue W. Burnside en un clásico libro sobre el tema [29, pag. 167].

Definición 1.5.1. *Sean G un grupo, R un anillo conmutativo y V un R-módulo libre de rango finito. Una representación de G sobre R, con espacio de representación V, es un homomorfismo de grupos $T : G \to GL(V)$, donde $GL(V)$ denota el grupo de R-automorfismos de V. El rango de V es llamado el grado de la representación T, y será denotado por $rank(V) = deg(T)$.*

Para un elemento $g \in G$ se denotara por $T_g : V \to V$ al automorfismo correspondiente bajo T. Luego si g, $h \in G$, debemos tener que $T_{gh} = T_g \circ T_h$ y $T_{1_G} = \mathcal{I}d_V$.

Fijando una R-base en V, se define un isomorfismo de $GL(V)$ en el grupo $GL(n, R)$ de matrices invertibles $n \times n$ con coeficientes en R, donde a cada automorfismo de $GL(V)$ se le asocia una matriz con respecto a la base dada.

Definición 1.5.2. *Sean G un grupo y R un anillo conmutativo. Una representación matricial de G sobre R de grado n es un homomorfismo de grupos $T : G \to GL(n, R)$.*

Si $T : G \to GL(V)$ es una representación de G sobre R con espacio de representación V y se considera el isomorfismo $\phi : GL(V) \to GL(n, R)$ asociado con una base dada como se vió arriba, entonces $\phi \circ T : G \to GL(n, R)$ es una representación matricial de G. De manera similar, dada una representación matricial $T : G \to GL(n, R)$ se tiene que $\phi^{-1} \circ T : G \to GL(V)$ es una representaciónde G sobre R. Debido a este hecho, no se hará distinción entre las representaciones y las representaciones matriciales.

Los siguientes ejemplos ilustran estos conceptos.

Ejemplo 1.5.3. *Sean G un grupo y R un anillo conmutativo, la aplicación $T : G \to GL(n, R)$ que asocia a cada elemento de G la matriz identidad de $GL(n, R)$ es llamada* ***la representación trivial*** *de G sobre R de grado n.*

Ejemplo 1.5.4. *Sea G el 4-grupo de Klein, el grupo $G = \{1, a, b, ab\}$ con tres elementos de orden 2. Es un ejercicio simple verificar que la aplicación*

$$T : G \to GL(2, \mathbb{Z})$$

dado por:

$$T(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \qquad T(a) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix};$$

$$T(b) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}; \qquad T(ab) = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},$$

es una representación de G.

Ejemplo 1.5.5. *Sean G un grupo finito de orden n y R un anillo conmutativo. Tomando RG como espacio de representación, la aplicación $g \mapsto T_g$, donde*

$$T_g : RG \to RG$$
$$g_i \mapsto T_g(g_i) = gg_i,$$

define una representación, llamada la ***representación regular*** *de G sobre R. En efecto,*

$$T_{gh}(y) = (gh)y = g(hy) = T_g(hy) = T_g T_h(y).$$

Como G es una R-base de RG, al etiquetar los elementos de G en algún orden, $G = \{1 = g_1, g_2, \ldots, g_n\}$, es fácil ver que la representación matricial es una matriz de permutación.

Si G es específicamente el 4-grupo de Klein $G = \{1, a, b, ab\}$, con etiquetamiento $g_1 = 1$, $g_2 = a$, $g_3 = b$ y $g_4 = ab$ se obtienen las matrices:

$$\rho(1) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad \rho(a) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

$$\rho(b) = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \qquad \rho(ab) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

1.6. Involuciones y subconjuntos especiales de RG

Después del trabajo de S. A. Amitsur, (ver [27, Sección 5.1]) y el interés en anillos con involución desarrrollado a partir de la decada de los 70′s por Herstein y colaboradores [17], se ha tornado natural estudiar álgebras de grupo desde este punto de vista.

Sea R un anillo cualquiera, una aplicación $* : R \to R$ es una *involución* si verifica las siguientes condiciones:

(i) $(r+s)^* = r^* + s^*$,

(ii) $(rs)^* = s^* r^*$ y,

(iii) $(s)^{**} = s$,

para todos r, $s \in R$.

Note que (i) y (ii) definen un anti-homomorfismo y (iii) muestra que $*$ es de orden 2.

El siguiente ejemplo muestra dos involuciones en el anillo de matrices.

Ejemplo 1.6.1. *Dado un cuerpo F, la función que envia cada matriz de $M_n(F)$ en su transpuesta cumple con las condiciones de la definición anterior. Además, si n es par y $A_{11}, A_{12}, A_{21}, A_{22} \in M_{n/2}(F)$, la involución simplética está dada por:*

$$\begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}^s = \begin{pmatrix} A_{22}^t & -A_{12}^t \\ -A_{21}^t & A_{11}^t \end{pmatrix},$$

donde t es la trasposición usual de matrices.

Todas las involuciones en $M_n(F)$ pueden ser expresadas en términos de estas dos involuciones. Más exactamente, se tiene el siguiente resultado clásico debido a Kaplansky, [21, Proposición 2.1.4].

Proposición 1.6.2. *Sean D un anillo con división de característica diferente de 2 y n un entero positivo. Sea $*$ una involución arbitraria sobre $M_n(F)$. Entonces, excepto automorfismos θ de $M_n(D)$ tal que $\theta(A^*) = (\theta(A))^*$ para todo $A \in M_n(D)$ se tiene que vale solo una de las siguientes*

1. *Existe una involución $^-$ en D y una matriz diagonal invertible*

$$\begin{pmatrix} u_{11} & 0 & \cdots & 0 \\ 0 & u_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & u_{nn} \end{pmatrix}$$

   tal que $\overline{u}_{ii} = u_{ii}$ para todo i, y si $A = (a_{ij}) \in M_n(D)$, entonces $A^* = U^{-1}BU$, donde $b_{ij} = \overline{a}_{ji}$ para todo i y j, o

2. *D es un cuerpo, n es par, y $*$ es la involución simplética.*

Como es usual, si R es un anillo con involución $*$, se denotaran a los conjuntos de *elementos simétricos* y *anti-simétricos* bajo $*$ respectivamente por:

$$R^+ = \{r \in R\colon r^* = r\} \qquad \text{y} \qquad R^- = \{r \in R\colon r^* = -r\}.$$

Además,

$$\mathcal{U}^+(R) = \mathcal{U}(R) \cap R^+,$$

denotará el conjunto de *las unidades simétricas* de R.

La importancia de estos conjuntos radica en conocer cuando propiedades sobre ellos pueden ser extendidos a todo RG. Existen númerosos estudios (ver [31, Teorema V.4.4 y V.6.1], [11], [9], [22], [21, Sección 3.3], [6], entre otros) referentes a este tema que fueron inspirados en uno de los resultados más famosos de Amitsur:

Teorema 1.6.3. *[1, Teorema 1] Si R satisface una identidad polinomial de la forma:*

$$p(x_1, x_2, \ldots, x_r, x_1^*, x_2^*, \ldots, x_r^*),$$

de grado d, entonces R satisface una identidad polinomial que no incluye los x_i^*'s para $i = 1, \ldots, r$. En particular, si R^+ o R^- satisfacen una identidad polinomial, entonces R también satisface una identidad polinomial, no necesariamente la misma.

Dado un anillo R con unidad, se dice que R satisface *una identidad polinomial*, abreviada por $R \in IP$, si existe un polinomio $0 \neq f(x_1, \ldots, x_n)$ en el F-álgebra libre $F\langle x_1, \ldots, x_n, \ldots\rangle$ en el conjunto infinito enumerable $\{x_1, x_2, \ldots, x_n, \ldots\}$ de variables no conmutativas tal que $f(a_1, a_2, \ldots, a_n) = 0$ para todos los $a_i \in R$.

El estudio algebraico de los anillos de grupo satisfaciendo una identidad polinomial fue iniciado en 1949 por I. Kaplansky y fue potencializado doce años después por el trabajo de S. A. Amitsur. Desde entonces, este tópico se ha tornado llamativo entre un número creciente de investigadores de Colombia, Bélgica, Italia, Brasil, Canadá, Estados Unidos, etc, como Castillo, Jespers, Giambruno, Gonçalves, Goodaire, Lee, Passman, Polcino Milies, Spinelli, Sehgal, etc.

El siguiente importante lema, llamado *Lema de Linealización* es debido a Kaplansky, y una demostración bien clara del mismo aparece en [27, Lema 5.1.1].

Lema 1.6.4 (Lema de Linealización)**.** *Si R es un F-álgebra que satisface una identidad polinomial de grado n, entonces R satisface una identidad polinomial lineal en cada variable (multilineal), es decir, R satisface una identidad polinomial de la forma:*

$$f(x_1, x_2, \ldots, x_n) = \sum_{\rho \in S_n} \alpha_\rho x_{\rho(1)}, x_{\rho(2)}, \ldots, x_{\rho(n)}.$$

Las condiciones bajo las cuales álgebras de grupo $FG \in IP$ fueron determinadas en resultados clásicos debidos a Isaacs y Passman. Recuerde que para cualquier primo p, un grupo G es llamado *p-Abeliano* si su subgrupo conmutador G', es un p-grupo finito. Si $p = 0$, G será Abeliano.

Proposición 1.6.5. *Sean F un cuerpo de característica $p \geq 0$ y G un grupo. Entonces $FG \in IP$ si y solo si G contiene un grupo p-Abeliano de índice finito.*

Ahora bien, $f(x_1, x_2, \ldots, x_n)$ es una *identidad polinomial generalizada*, para una F-álgebra R si ella es la suma de términos de la forma:

$$r_0 x_{i_1} r_1 x_{i_2} \cdots r_k x_{i_{k+1}} r_{k+1},$$

donde $r_i \in R$ y k es un entero, tal que $f(a_1, \ldots, a_n) = 0$ para todo $a_i \in R$. Es decir, en este caso no solo los coeficientes del cuerpo son permitidos aparecer en la identidad polinomial generalizada, si no también los elementos del anillo. Aplicando el lema de linealización 1.6.4 a una identidad polinomial generalizada, se obtiene una *identidad polinomial generalizada multilineal*, que es de la forma

$$f(x_1, x_2, \ldots, x_n) = \sum_{\sigma \in S_n} f^{\sigma}(x_1, x_2, \ldots, x_n),$$

donde cada f^{σ} es una suma de términos de la forma:

$$r_0 x_{\sigma(1)} r_1 x_{\sigma(2)} \cdots r_{n-1} x_{\sigma(n)} r_n,$$

para varios $r_i \in R$.

Note que es insuficiente que la identidad polinomial generalizada sea no cero. En efecto, si $r \in R$ es un elemento central, entonces R satisface $rx_1 - x_1 r$, pero esta identidad no es de muy útil. Lo que obliga a exigirle a la identidad polinomial generalizada una condición adicional. Una identidad polinomial generalizada multilineal es llamada *no degenerada* si, para algún $\sigma \in S_n$, f^{σ} no es una identidad polinomial generalizada para R. Los anillos de grupo satisfaciendo una identidad polinomial generalizada multilineal no degenerada fueron clasificados por Passman, [27, Teorema 5.3.15].

Proposición 1.6.6. *Sean F un cuerpo y G un grupo. Entonces FG satisface una identidad polinomial generalizada multilineal no degenerada si y solo si $[G : \Phi(G)] < \infty$ y $(\Phi(G))'$ es finito. En particular, si FG satisface una identidad polinomial, entonces $[G : \Phi(G)] < \infty$ y $|(\Phi(G)|'\infty$.*

En la anterior proposición $[G : \Phi(G)]$ denota el número de clases laterales a izquierda (o derecha) de $\Phi(G)$ en G, conocido como *el índice de $\Phi(G)$ en G*. El siguiente lema será necesario en el último capítulo.

Lema 1.6.7. *Sea R un F-álgebra. Si R contiene un ideal a derecha I tal que $I^r \neq 0$ y satisface una identidad polinomial, entonces R satisface una identidad polinomial generalizada multilineal no degenerada.*

Suponga que R es un F-álgebra con involución $*$. Es posible definir una involución sobre el F-álgebra libre $F\{x_1, y_1, x_2, y_2, \ldots\}$ en un conjunto infinito enumerable de variables, definiendo $x_i^* = y_i$ y $y_i^* = x_i$. Es decir, $F\{x_1, x_1^*, x_2, x_2^*, \ldots\}$ es el álgebra libre con involución $*$, cuyos elementos son naturalmente polinomios en las variables no comutativas x_i y x_i^*.

Se dice que R satisface una $*$-*identidad polinomial*, si existe $0 \neq f(x_1, x_1^*, x_2, x_2^*, \ldots, x_n, x_n^*) \in F\{x_1, x_1^*, \ldots\}$ tal que $f(a_1, a_1^*, \ldots, a_n, a_n^*) = 0$, para todos $a_i \in R$.

Capítulo 2

Identidades de grupo en anillos de grupo

Sean FG el álgebra de grupo de un grupo de torsión G sobre el cuerpo infinito F, y $\mathcal{U}(FG)$ su grupo de unidades. En este capítulo se establece en detalle la confirmación de la conjetura de Brian Hartley, debida a Giambruno, Sehgal y Valenti, [12], es decir, se mostrará que si $\mathcal{U}(FG)$ verifica una identidad de grupo, entonces FG verifica una identidad polinomial.

2.1. Una Conjetura de Brian Hartley

Sea $\mathcal{U}(R)$ el grupo de unidades de un anillo R, $H \subseteq \mathcal{U}(R)$ verifica *una identidad de grupo* abreviada por $H \in IG$, si existe una palabra no-trivial w (es decir, en la representación de w, no existen dos símbolos consecutivos de la forma $x_i^{\epsilon_i} x_i^{-\epsilon_i}$, donde $\epsilon_i = \pm 1$) en el grupo libre $\langle x_1, \ldots, x_n, \ldots \rangle$, sobre un conjunto enumerable de variables tal que $w(u_1, u_2, \ldots, u_n) = 1$, para todos los $u_i \in H$.

El álgebra de grupo FG del grupo G sobre el cuerpo infinito F, es una gran fuente de unidades, [13]. En este espacio vectorial Brian Hartley conjeturó alrededor de 1980 lo siguiente:

Conjetura 2.1.1. *[21, Conjetura 1.1.3] Sean G un grupo de torsión y F un cuerpo infinito. Si el grupo de las unidades $\mathcal{U}(FG)$ de FG satisface una identidad de grupo, entonces FG satisface una identidad polinomial.*

Los estudios para intentar resolver positivamente la conjetura no se hicieron esperar. En 1981, Warhurst en su tesis doctoral, [32], trabajó con un tipo especial de identidades de grupo que satisfacen las unidades $\mathcal{U}(FG)$. En ese mismo año, en carta privada dirigida a B. Hartley, Pere Menal sugirió una solución para algunos p-grupos [25].

En [8] Giambruno, Jespers y Valenti manejaron tanto el caso en característica cero como el de característica $p > 0$, cuando G no tiene p-elementos. Usando la construcción de P. Menal, Giambruno, Sehgal y Valenti muestran en [12], que si $\mathcal{U}(FG)$ satisface una identidad de grupo, entonces FG satisface una identidad polinomial, es decir, confirman la conjetura.

2.2. Algunos resultados clásicos

Los resultados presentados en está sección serán claves en la demostración del Teorema 2.3.2, él cual responde afirmativamente a la Conjetura de Brian Hartley.

Recuerde que $\Delta(G, N)$ denota el kernel del epimorfismo canónico $FG \twoheadrightarrow F(G/N)$, donde N es un subgrupo normal de G y, $\Delta(G) = \Delta(G, G)$ es el ideal de aumento.

Además, $\Phi(G) = \{g \in G : |cl_G(g)| < \infty\}$ representa el conjunto de los elementos de conjugación finita en G. Es posible mostrar que $\Phi(G)$ es un subgrupo normal (llamado el *FC-subgrupo*) de G y que subgrupos y grupos cocientes de un FC-grupos son FC-grupos.

Sean p la característica de F y como es usual $P = \{g \in G : o(\mathrm{g}) = p^k \text{ para algún k}\}$ el conjunto de los p-elementos de G. Un subgrupo asociado a ambos conjuntos, $\Phi(G)$ y P, es $\langle P \cap \Phi(G)\rangle$ denotado por $\Phi_p(G)$. También como es usual, $Q = \{g \in G : p \nmid o(\mathrm{g})\}$ denota el conjunto de los p'-elementos de G. Es claro que si $p = 0$, entonces $P = \{1\}$ y $Q = G$.

Los siguientes resultados serán de ayuda para determinar la estructura de los anillos de grupo que cumplen con la Conjetura 2.1.1.

Lema 2.2.1. *Sean R un anillo con unidad semiprimo y*

$$S = \{a \in R : \text{ para todos } b, c \in R, bc = 0 \text{ implica } bac = 0\}.$$

Si S contiene todos los elementos de cuadrado cero de R, entonces S contiene todos los elementos nilpotentes de R.

Demostración. Sea a un elementos nilpotente. Usando inducción sobre el índice de nilpotencia de a, se probará que si $b, c \in R$ son tales que $bc = 0$, entonces $bac = 0$. Por hipótesis, si $x^2 = 0$, se tiene que $bxc = 0$.

Hipótesis de inducción. Sea $x \in R$, con $x^m = 0$ y $m < n$, entonces $b'xc' = 0$ siempre que $b'c' = 0$ y $b', c' \in R$.

Si $a^n = 0$ para algún $n \geq 2$, entonces $(1-a)(1+a+a^2+\ldots+a^{n-1}) = (1-a^n) = 1$, es decir, $(1-a) \in \mathcal{U}(R)$.

Sean b, $c \in R$ tales que $bc = 0$ y $r \in R$. Tomando $b_1 = b(1-a)^{-1}$ y $c_1 = (1-a)c$ se tiene que

$$b_1c_1 = b(1-a)^{-1}(1-a)c = bc = 0.$$

Además, del hecho que $(crb)^2 = (cr)bc(rb) = 0$, se tiene por por la hipótesis del lema que $b_1crbc_1 = 0$.

Ahora si $m \geq 2$ implica que $m(n-1) \geq n$ y por tanto, $(a^m)^{n-1} = a^{m(n-1)} = 0$. Así, por la hipótesis de inducción $ba^mc = 0$ para todo $m \geq 2$, es decir, a^2, $a^3, \ldots,$ $a^{n-1} \in S$ y por tanto,

$$b_1c = b(1-a)^{-1}c = b(1+a+a^2+\ldots+a^{n-1})c = (bc)+(bac)+(ba^2c)+\ldots+(ba^{n-1}c) = bac$$

y

$$bc_1 = b(1-a)c = bc - bac = -bac.$$

Luego, $b_1crbc_1 = (bac)r(-bac) = -bacrbac$. Por tanto, $bacrbac = 0$, para todo $r \in R$.

Si $bac \neq 0$, el ideal bilateral $RbacR = \{\sum r_i bacs_i : r_i, s_i \in R\}$ será no nulo, pues $bac \in RbacR$.

Además, $RbacR$ será nilpotente. En efecto, sean $x_1 = \sum_{i=1}^{n} r_i bacs_i$ y $x_2 = \sum_{j=1}^{m} t_j bacw_j$ con $r_i, s_i, t_j, w_j \in R$. Luego,

$$\begin{aligned} x_1 x_2 &= \Big(\sum_{i=1}^{n} r_i bacs_i\Big)\Big(\sum_{j=1}^{m} t_j bacw_j\Big) \\ &= \sum_{i,j} r_i bacs_i t_j bacw_j \\ &= \sum_{i,j} r_i bacl_{ij} bacw_j, \qquad s_i t_j = l_{ij} \\ &= 0 \end{aligned}$$

pues $bacl_{ij}bac = 0$, para todo l_{ij}.

Luego $Rbac$ es no nulo y nilpotente de índice 2, lo que contradice el hecho que R sea semiprimo, ver [27, Lema 4.2.11]. Por tanto, $bac = 0$, para todo elemento nilpotente $a \in R$, y todos $b, c \in R$ tales que $bc = 0$ □

En el marco de este trabajo de investigación es de interés particular conocer las álgebras de grupo donde todo elemento idempotente es central.

Lema 2.2.2. *Sea R un álgebra sobre un dominio de integridad A. Suponga que para todos a, b, $c \in R$ tal que $a^2 = bc = 0$ se tiene $bac = 0$. Entonces cada idempotente de $A^{-1}R$ es central.*

Demostración. Sea e un elemento idempotente en $A^{-1}R$. Entonces para algún $r \neq 0$, $r \in A$ y $f = re \in R$ se tiene que $f^2 = (re)^2 = rere = r^2e^2 = r^2e$. Luego

$$f(r - f) = re(r - re) = r^2e - r^2e = 0.$$

Si $u \in A^{-1}R$, se tiene

$$(fu(r - f))^2 = fu(r - f)fu(r - f) = 0,$$

pues

$$(fu(r-f))^2 = (reu(r-re))^2 = (r^2eu - r^2eue)^2$$
$$= r^4eueu - r^4eueue - r^4eueeu + r^4eueeue = 0.$$

Así, por la hipótesis, $f(fu(r-f))(r-f) = 0$. Por tanto, se tiene que

$$f(fu(r-f))r - \underbrace{f(fu(r-f))f}_{0} = 0,$$

y en consecuencia $f(fu(r-f))r = 0 \quad (*)$. Por otro lado,

$$f(fu(r-f))r = rf^2u(r-f) = r^3e^2u(r-re) = r^4eu - r^4eue \quad (**)$$

De $(*)$ y $(**)$, como r no es divisor de cero ($r \in A$), se obtiene que $eu = eue$. De manera análoga, $eue = ue$, y por tanto, se tiene $eu = ue$ para todo idempotente de $A^{-1}R$ y todo $u \in A^{-1}R$, es decir, todo idempotente de $A^{-1}R$ es central. □

El siguiente resultado debido a Levitzki, da una condición necesaria para que el anillo R sea semiprimo, [8, Corolario 3.].

Teorema 2.2.3 (Levitzki)**.** *Sean R un anillo y $\mathcal{H}(R)$ el conjunto*

$$\mathcal{H}(R) = \{a \in R : aR \text{ es ideal nil de índice acotado}\}.$$

Si R es un anillo semiprimo, entonces $\mathcal{H}(R) = (0)$.

El Lema 2.2.2, también se puede aplicar al caso en que e es un idempotente de R, por tanto para que una álgebra R tenga todos sus idempotentes centrales basta que, para todos $a, b, c \in R$, con $a^2 = bc = 0$, se tenga que $bac = 0$. A continuación con la ayuda de [8, Proposición 1] y el Teorema 2.2.3 (Levitzki), se mostrará que si una álgebra R es semiprima y $\mathcal{U}(R) \in IG$ entonces tal condición suficiente es satisfecha.

Teorema 2.2.4. *Sea R un álgebra semiprima sobre un dominio conmutativo infinito A. Si $\mathcal{U}(R) \in IG$, entonces cada idempotente de $A^{-1}R$ es central y para todos b, $c \in R$ tales que $bc = 0$ se tiene que $bac = 0$, para todo elemento nilpotente $a \in R$.*

Demostración. Sean a, b, $c \in R$ tales que $a^n = bc = 0$, para algún $n \in \mathbb{N}$.

Afirmación 5. $a^2 = bc = 0 \Rightarrow bac = 0$.

En efecto, por [8, Proposición 1], $bacR$ es un ideal nil a derecha de índice acotado. Si $bac \neq 0$, se tiene por el Teorema de Levitzki 2.2.3 que R tiene un ideal nilpotente no cero, que contradice la hipótesis de R ser semiprimo. Así $bac = 0$, quedando demostrada la afirmación.

Por el Lema 2.2.2, se tiene que todos los idempotente de $A^{-1}R$ son centrales.

La última afirmación sigue del Lema 2.2.1. □

El resultado anterior será fundamental en la demostración del teorema principal de este capítulo, en el caso en que el anillo de grupo FG sea semiprimo e indirectamente cuando la suma de los ideales nilpotentes sea cero.

Posteriormente, debido al hecho de que un grupo libre no Abeliano no puede satisfacer una identidad de grupo y al siguiente resultado debido a Gonçalves [21, Proposición 1.2.2], es posible preocuparse solo por el caso en que las álgebras de división D_i presentes en la descomposición de Wedderburn-Artin de un anillo semisimple, sean cuerpos.

Teorema 2.2.5. *[21, Proposición 1.2.2] Sea D un álgebra con división no conmutativa tal que D es finito dimesional sobre su centro. Entonces, $\mathcal{U}(D)$ contiene un grupo libre no Abeliano.*

Si R es un anillo e I un ideal de R es posible obtener identidades de grupo para $\mathcal{U}(R/I)$ a partir de las identidades de grupo satisfechas por $\mathcal{U}(R)$ y viceversa. Ese es el contenido de los siguientes dos resultados, cuyas demostraciones se pueden encontrar en [21, Lema 1.2.17] [21, Lema 1.2.18] respectivamente.

Lema 2.2.6. *Sean R un anillo e I un ideal de R. Si $\mathcal{U}(R)$ satisface la identidad de grupo $\omega(x_1, \ldots, x_n) = 1$, entonces $\mathcal{U}(R/I)$ satisface la misma identidad de grupo. Recíprocamente, si $car(R) = p$ primo, I es ideal nil de exponente p^k, y $\mathcal{U}(R/I)$ satisface la identidad de grupo $\upsilon(x_1, \ldots x_n) = 1$, entonces $\mathcal{U}(R)$ satisface $(\upsilon(x_1, \ldots x_n))^{p^k} = 1$.*

Sea G un grupo. Si para todo H subgrupo de G finitamente generado, se tiene que H es finito, entonces G es llamado un *grupo localmente finito*. Del Teorema de Schmidt [30, Teorema 14.3.1], es posible mostrar que si H y G/H son localmente finitos, entonces G es localmente finito. En el contexto de álgebras de grupo ese resultado es usado de la siguiente manera.

Lema 2.2.7. *Sea F un cuerpo de característica $p > 0$ y G un grupo, tal que $\mathcal{U}(FG)$ satisface la identidad $\omega(x_1, x_2, \ldots, x_n) = 1$. Si N es un p-grupo normal de G, y N es finito o G es localmente finito, entonces $\mathcal{U}(F(G/N))$ satisface $\omega(x_1, x_2, \ldots, x_n) = 1$.*

El siguiente lema será necesario en la prueba del teorema principal de este capítulo.

Lema 2.2.8. *Sean G un grupo finito y F un cuerpo infinito tal que $\mathcal{U}(FG) \in IG$. Si $car(F) = p > 0$ entonces G es p-Abeliano.*

Demostración. Como la $dim_F(FG) = |G| < \infty$ y todo ideal I de FG es visto como un F-espacio vectorial de dimensión finita, entonces toda cadena decreciente de ideales en FG se detiene, por tanto FG es Artiniano. Sea $J(FG)$ el radical de Jacobson de FG. Del hecho que FG es Artiniano se sigue que $FG/J(FG)$ también lo es, y además por el Teorema 1.2.8, $J(FG/J(FG)) = (0)$. Así, del Teorema 1.2.13, $FG/J(FG)$ es semisimple.

Usando el Teorema de Wedderburn-Artin (Teorema 1.2.7), se tiene que:

$$\frac{FG}{J(FG)} \simeq \bigoplus_{i \in I} M_{n_i}(D_i).$$

Como $FG/J(FG)$ es semisimple, por el Teorema 1.2.13(i), será semiprimo y así del Teorema 2.2.4, se tiene que todo idempotente de $FG/J(FG)$ es central. Luego en la descomposición arriba, $n_i = 1$ para todo i, es decir,

$$\frac{FG}{J(FG)} \simeq \bigoplus_{i \in I} D_i,$$

donde cada D_i es un anillo con división tal que $F \subseteq \zeta(D_i)$.

Como G es finito, se tiene que $dim_F(D_i) < \infty$, y por tanto del Teorema 2.2.5, cada D_i es conmutativo, caso contrario, D_i contendría un grupo libre no Abeliano y así su grupo de unidades $\mathcal{U}(D_i)$, no podría satisfacer ninguna identidad de grupo, que es una contradición dado que siendo $J(FG)$ un ideal nilpotente (Teorema de Hopkins), por el Teorema 2.2.6, $\mathcal{U}(FG/J(FG)) \in IG$. Luego $FG/J(FG)$ es suma directa de cuerpos, y así es conmutativo. Entonces para todo $x, y \in G$, $(x, y) = 1\ mod(J(FG))$ y así, $G' \subseteq 1 + J(FG)$, y por [29, Proposición 3.2.10] $\Delta(G') \subseteq J(FG)$. Así, $\Delta(G')$ será nilpotente.

Si $p > 0$, por el Teorema 1.3.7 se tiene que G' es un p-grupo finito. Si $p = 0$, entonces como consecuencia del mismo teorema, $G' = \{1\}$, y por tanto G es Abeliano. □

A continuación, se tiene una especie de reciproca del lema anterior, removiendo la hipótesis de G ser finito.

Lema 2.2.9. *Sean G un grupo y F un cuerpo con $car(F) = p > 0$. Si G es p-Abeliano entonces $\mathcal{U}(FG) \in IG$, y FG satisface la identidad polinomial $[x, y]^{p^m} = 0$ para algún $m \in \mathbb{N}$.*

Demostración. Sea $\pi' : FG \to F(G/G')$ el epimorfismo canónico. Del Teorema 1.1.3 se tiene que G/G' es Abeliano, luego $F(G/G') \simeq FG/\Delta(G, G')$ es conmutativo. Entonces para todos u, $v \in FG$ se tiene que $1 - (u, v) \in Ker(\pi')$.

Del Corolario 1.3.8 se sigue que el $Ker(\pi') = \Delta(G, G')$ es nilpotente. Así, existe un $m \in \mathbb{N}$, tal que

$$(1 - (u, v))^{p^m} = 0,$$

y como $car(F) = p > 0$, entonces $(1 - (u, v))^{p^m} = 1 - (u, v)^{p^m}$. Luego se tiene que $(u, v)^{p^m} = 1$ y por tanto $\mathcal{U}(FG)$ satisface la identidad de grupo

$$\omega(x, y) = (x, y)^{p^m}.$$

Más aún, para $x, y \in FG$ se tiene que

$$\begin{aligned}
[x,y] &= \Big[\sum_{g\in G}\alpha_g g, \sum_{h\in G}\beta_h h\Big] \\
&= \sum_{g,h\in G}\gamma_{gh}[g,h] \\
&= \sum_{g,h\in G}\gamma_{gh}(gh-hg) \\
&= \sum_{g,h\in G}\gamma_{gh}(-hg)(1-g^{-1}h^{-1}gh) \\
&= \sum_{g,h\in G}\underbrace{\lambda_{gh}}_{\in FG}\underbrace{(1-(g,h))}_{\in\Delta(G')}.
\end{aligned}$$

Así, $[x,y] \in FG\Delta(G') = \Delta(G,G')$. Nuevamente por el Corolario 1.3.8, existe $k \in \mathbb{N}$ tal que $[x,y]^{p^k} = 0$, para todos $x, y \in FG$, es decir, $FG \in IP$. □

El siguiente resultado clásico, junto con la caracterización de álgebras de grupo semiprimas debida a Isaacs y Passman (Teorema 1.3.12), serán claves en la demostración del teorema principal del capítulo.

Lema 2.2.10. *(Passman) Suponga que $car(F) = p > 0$. Entonces $\eta(FG)$ es nilpotente si y solo si $\Phi_p(G)$ es finito.*

Recuerde que $\eta(FG)$ denota la suma de todos los ideales nilpotentes de FG.

2.3. Respuesta afirmativa a la Conjetura de Brian Hartley

En esta sección se presenta en detallle la respuesta afirmativa a la Conjetura de Brian Hartley, debida a Giambruno, Sehgal y Valenti en [12].

Antes de enunciar y demostrar tal resultado, es necesaria la siguiente proposición, conocida en la literatura como el *Argumento de Magnus*. Se denota por $\mathcal{A} = F\langle x_1, x_2, \ldots, x_n\rangle[|t|]$ al anillo de series de potencias en la variable conmutativa t sobre el F-álgebra libre $F\langle x_1, x_2, \ldots, x_n\rangle$.

Proposición 2.3.1. *Sean F un cuerpo de característica $p > 0$ y $\mathcal{A} = F\langle x_1, x_2, \dots x_n\rangle[|t|]$. Entonces los elementos $1+x_1t, 1+x_2t, \dots, 1+x_nt$, generan un subgrupo libre de $\mathcal{U}(\mathcal{A})$.*

Ahora se tienen las herramientas necesarias para enunciar y demostrar el teorema principal de este capítulo.

Teorema 2.3.2. *Sea FG el álgebra de grupo de un grupo de torsión G sobre un cuerpo infinito F. Si $\mathcal{U}(FG)$ satisface una identidad de grupo, entonces FG satisface una identidad polinomial.*

Por comodidad del lector la demostración será divida en tres casos excluyentes bajo los siguientes teoremas. Para empezar se tiene el caso donde $\eta(FG)$ es el ideal nulo, es decir, FG semiprimo (ver Teorema 1.3.122d).

Teorema 2.3.3. *Sea FG el álgebra de grupo de un grupo de torsión G sobre un cuerpo infinito F. Si $\mathcal{U}(FG)$ satisface una identidad de grupo y FG es semiprima, entonces FG satisface una identidad polinomial.*

Demostración. Sea $car(F) = p$. Si $y \in G$ es tal que su orden es m con $p \nmid m$, considere

$$e = \frac{\widehat{y}}{m} = \frac{1}{m}\sum_{k=0}^{m-1} y^k \in FG.$$

Luego,

$$\begin{aligned}
e^2 &= \frac{1}{m^2}(1 + y + y^2 + \cdots + y^{m-1})(1 + y + y^2 + \cdots + y^{m-1}) \\
&= \frac{1}{m^2}\underbrace{[(1 + y + y^2 + \cdots + y^{m-1}) + (1 + y + y^2 + \cdots + y^{m-1}) + \cdots + (1 + y + y^2 + \cdots + y^{m-1})]}_{m-veces} \\
&= \frac{1}{m^2}m(1 + y + y^2 + \cdots + y^{m-1}) \\
&= \frac{1}{m}(1 + y + y^2 + \cdots + y^{m-1}) = e,
\end{aligned}$$

y así $e = \frac{\widehat{y}}{m} \in FG$ es idempotente. Por tanto, del Lema 2.2.4, e es central.

Por tanto, $g\widehat{y} = \widehat{y}g$ para todo $g \in G$. Así,

$$g\widehat{y}g^{-1} = \widehat{y}$$

$$1 + gyg^{-1} + \cdots + gy^{m-1}g^{-1} = 1 + y + y^2 + \cdots + y^{m-1}.$$

Luego existe j tal que $gyg^{-1} = y^j$. Por lo tanto, $\langle y \rangle \lhd G$ para todo $y \in G$.

Por el Teorema 1.1.6, se tiene que G es Abeliano o Hamiltoniano.

- Suponga que $car(F) = 0$.

  En caso de G ser Hamiltoniano, pues en este caso tendríamos que $\mathcal{Q}_8 \leq G$ y así, $\mathcal{U}(F\mathcal{Q}_8) \in IG$, lo que es imposible debido al el Lema 2.2.8 ($\mathcal{Q}_8$ sería Abeliano).

  Luego G es Abeliano y FG es conmutativo. Por tanto, FG satisface la identidad polinomial

  $$\rho(x, y) = [x, y] = xy - yx.$$

- Suponga que $p > 0$.

  Recordemos que P y Q denotan el conjunto de los p-elementos y los p'-elementos respectivamente.

  Afirmación 6. $P = \{1\}$ **y** $G = Q$**.**

  Demostración. Considere $g \in P$, entonces $o(g) = p^k$ para algún $k \in \mathbb{N}$. Luego $(1-g)^{p^k} = 1 - g^{p^k} = 0$. Sea $h \in P$,

  $$\widehat{h}(1-h) = \widehat{h} - \widehat{h}h = 0.$$

  Luego del Teorema 2.2.4 se tiene

  $$0 = \widehat{h}(1-g)(1-h) = (\widehat{h} - \widehat{h}g)(1-h) = \underbrace{\widehat{h}(1-h)}_{0} - \widehat{h}g + \widehat{h}gh,$$

  es decir,

  $$\widehat{h}gh = \widehat{h}g,$$

  $$gh + hgh + \cdots + h^{p^{l-1}}gh = g + hg + h^2g + \cdots + h^{p^{l-1}}g,$$

  Multiplicando a derecha por g^{-1} se tiene

$$1 + h + h^2 + \cdots + h^{p^{l-1}} = ghg^{-1} + \cdots h^{p^{l-1}} ghg^{-1},$$

y por tanto existe $m \in \mathbb{N}$ tal que $h^m = ghg^{-1}$, es decir, $\langle h \rangle \lhd P$.

Observe que: Para todo $q \in Q$ y todo $h \in P$, se tiene $qhq^{-1} = h$. En efecto, como $\langle q \rangle \trianglelefteq G$, pues G es Abeliano o Hamiltoniano, el subgrupo $H = \langle q, h \rangle$ es finito, dado que $\langle q \rangle$ y $\langle h \rangle$ lo son (G es de torsión), y además para todo t, existe s tal que $hq^t = q^s h$ ($hq^t h^{-1} = q^s \in \langle q \rangle \lhd G$).

Usando el hecho que $\mathcal{U}(FG) \in IG$ y que $H \subseteq G$ se tiene que $\mathcal{U}(FH) \in IG$, luego por el Lema 2.2.8, $H = \langle q, h \rangle$ es p-Abeliano.

Así,

$$(q, h) = q^{-1} \underbrace{h^{-1} q h}_{\in \langle q \rangle} = q^{r-1} \in \langle q \rangle,$$

para algún r.

Por tanto, un elemento en $\langle q \rangle$ es de orden p^s para algún s, es decir es p-elemento y p'-elemento. Luego $(q, h) = 1$, es decir,

$$qhq^{-1} = h,$$

para todo $q \in Q$ y todo $h \in P$. Luego $\langle h \rangle$ es normalizado por los elementos de Q y de P (h es p-elemento), por tanto por todos los elementos en G.

Dado que FG es semiprima, G no contiene subgrupos normales finitos de orden divisibles por p, ver Teorema 1.3.12(2b). Así, $h = 1$ y por tanto, $P = \{1\}$ y $G = Q$. □

En el caso particular de $p = 2$, Q no puede tener 2-elementos, no es posible que $Q = \mathcal{Q}_8 \times E \times A$ pues tanto E como $\mathcal{Q}_8$ contienen 2-elementos. Así $Q = G$ es Abeliano.

En todos los casos, G resulta ser Abeliano, luego FG satisface la identidad polinomial

$$\rho(x, y) = xy - yx.$$

Así, queda demostrada la Conjetura 2.1.1 para el caso semiprimo. □

Debido al Teorema 1.3.12(1), en adelante se puede suponer $car(F) = p > 0$. Ahora se tiene el segundo caso.

Teorema 2.3.4. *Sea FG el álgebra de grupo de un grupo de torsión G sobre un cuerpo infinito F. Si $\mathcal{U}(FG)$ satisface una identidad de grupo y $\eta(FG)$ es un ideal nilpotente no nulo, entonces FG satisface una identidad polinomial.*

Demostración. Aunque en general, los p-elementos de un grupo no forman un grupo, bajo las hipótesis de este teorema se establece que:

Afirmación 7. $\Phi_p(G) \lhd G$**.**

Demostración. En efecto, sea $h \in \Phi_p(G)$. Luego $h = h_1 h_2 \dots h_k$ con $h_1, h_2, \dots, h_k \in P \cap \Phi(G)$.

Luego para $g \in G$,

$$g^{-1}hg = (g^{-1}h_1g)(g^{-1}h_2g)\dots(g^{-1}h_kg).$$

Es claro que $o(g^{-1}h_ig)$=$o(h_i)$ y

$$\begin{aligned} cl_G(g^{-1}h_ig) &= \{x^{-1}g^{-1}h_igx : x \in G\} \\ &= \{(gx)^{-1}h_i(gx) : x \in G\} \\ &= \{\widetilde{g}^{-1}h_i\widetilde{g} : \widetilde{g} \in G\} \\ &= cl_G(h_i). \end{aligned}$$

Por tanto, para cada i, se tiene que $g^{-1}h_ig \in P \cap \Phi(G)$, es decir, $g^{-1}hg \in \Phi_p(G)$, para todo $h \in \Phi_p(G)$ y todo $g \in G$. Luego $\Phi_p(G) \lhd G$. □

Como $\eta(FG)$ es nilpotente, se tiene por el Lema 2.2.10 que $\Phi_p(G)$ es finito y por tanto, del Lema 2.2.7, $\mathcal{U}(F(G/\Phi_p(G))) \in IG$.

Sean $N = \Phi_p(G)$ y $\overline{h} = hN \in G/\Phi_p(G)$.

Afirmación 8. (a) $h \in \Phi(G)$ (b) $\Phi(G/\Phi_p(G))$ **es p'-grupo.**

Demostración. (a) Si $\overline{h} = hN \in \Phi(G/\Phi_p(G))$, entonces el conjunto

$$cl_{G/\Phi_p(G)}(\overline{h}) = \{g^{-1}hgN : gN \in G/N\},$$

es finito. Como N es un conjunto finito, el conjunto

$$S = \{x : x \in g^{-1}hgN, g \in G\},$$

también será finito. Luego si $q \in G$ es tal que existe g con $q = g^{-1}hg$, entonces $q \in S$, y así $cl_{G/\Phi_p(G)}(\overline{h})$ es finito. Así se tiene que $h \in \Phi(G)$.

(b) Si el *o(h)*$= m$, m puede escribirse como $m = p^k a$, con $(a, p) = 1$. Del Teorema de Bezout, existen r, $s \in \mathbb{Z}$ tales que $1 = rp^k + sa$, y por tanto

$$h = h^{rp^k+sa} = h^{sa}h^{rp^k}.$$

Además, se tiene que

$$(h^{sa})^{p^k} = h^{(s)(ap^k)} = h^{sm} = 1$$

y

$$(h^{rp^k})^a = h^{(r)(ap^k)} = h^{rm} = 1.$$

Luego de la definición de orden, *o(h^{sa})* divide a p^k, y por tanto $h^{sa} \in P$. Además $p \nmid$*o(h^{rp^k})*, caso contrario, p dividiría a a. Luego $h^{rp^k} \in Q$.

Por tanto para todo $h \in G$, $h = h_1h_2$ con $h_1 \in P$ y $h_2 \in Q$.

Así con las hipótesis sobre h, $h = h_1h_2$ con $h_1 \in P$ y $h_2 \in Q$, $h_2^a = 1$ y $h_1 \in N$. Por tanto,

$$(hN)^a = (h_1Nh_2N)^a = \underbrace{(h_1N)^a}_{h_1 \in N}(h_2N)^a = h_2^aN = N.$$

Luego *o(hN)*$|\ a$, y como $p \nmid a$ entonces $p \nmid$*o(hN)*. Luego $\Phi(G/\Phi_p(G))$ no contiene p-elementos.

□

Del Teorema 1.3.12(2b), $F[G/\Phi_p(G)]$ es semiprima y como $\mathcal{U}(F[G/\Phi_p(G)]) \in IG$, por el Caso 1., $G/\Phi_p(G)$ es Abeliano.

Del Teorema 1.1.3, $G' \subseteq \Phi_p(G)$, es decir, G' es un p-grupo finito (G es p-Abeliano). Por tanto, del Lema 2.2.9, para algún $m \in \mathbb{N}$, FG satisface una identidad polinomial de la forma

$$\rho(x, y) = [x, y]^{p^m},$$

lo que demuestra la Conjetura 2.1.1 en este caso. □

Finalmente se establece la Conjetura para $\eta(FG)$ nil no nilpotente. Está distición es necesaria ya que existen ideales nil no nilpotentes, (ver Ejemplo 1.1.14).

Teorema 2.3.5. *Sea FG el álgebra de grupo de un grupo de torsión G sobre un cuerpo infinito F. Si $\mathcal{U}(FG)$ satisface una identidad de grupo y $\eta(FG)$ es un ideal nil no nilpotente, entonces FG satisface una identidad polinomial.*

Demostración. Por [21, Lema 1.1.2], se puede suponer que $\mathcal{U}(FG)$ satisface la identidad en dos varibles $\omega(x_1, x_2) = 1$.

Sea $\mathcal{A} = F\langle x_1, x_2\rangle[|t|]$ el anillo de series de potencias sobre el F-álgebra libre $F\langle x_1, x_2\rangle$. Por el Argumento de Magnus (Proposición 2.3.1), $1 + x_1 t$ y $1 + x_2 t$ generan un grupo libre en $\mathcal{U}(\mathcal{A})$.

Luego

$$\omega(1 + x_1 t, 1 + x_2 t) - 1 = \sum_{i \geq 1} \rho_i(x_1, x_2) t^i \neq 0 \tag{2.1}$$

donde los ρ_i's son polinomios homogéneos de grado i en $F\langle x_1, x_2\rangle$.

Así por la ecuación 2.1, existe $l \in \mathbb{N}$ tal que $\rho_l(x_1, x_2)$ es un polinomio no cero.

Afirmación 9. $\eta(FG)$ **satisface** $\rho_l(x_1, x_2) = 0$**.**

Demostración. Sean r_1, $r_2 \in \eta(FG)$ y $\lambda \in FG$. Luego los elementos $1 + r_i\lambda \in \mathcal{U}(FG)$, con inverso

$$(1 + r_i\lambda)^{-1} = 1 - r_i\lambda + r_i^2\lambda^2 - \cdots + (-1)^{d_i - 1} r_i^{d_i - 1} \lambda^{d_i - 1},$$

donde d_i es el menor entero tal que $r_i^{d_i} = 0$.

Evaluando $1 + r_1\lambda, 1 + r_2\lambda$ en la identidad de grupo, se obtiene

$$\omega(1 + r_1\lambda, 1 + r_2\lambda) = 1,$$

es decir,

$$\sum_{i=1}^{k} \rho_i(r_1, r_2)\lambda^i = 0,$$

para algún entero positivo k y $\rho_i(r_1, r_2) = 0$ para todo $t > k$. Por tanto, si $l \geq k$, entonces $\rho_l(r_1, r_2) = 0$. De otro lado, si $l < k$, dado que F es infinito por el argumento Vandermonde usual [21, Lema 1.2.4], existen elementos no cero $\lambda_1, \ldots, \lambda_{k+1} \in F$ tales que $\sum_{i=1}^{k} \rho_i(r_1, r_2)\lambda_j^i = 0$, para todo $j = 1, \ldots, k+1$. Es decir, vale la siguiente igualdad:

$$\begin{pmatrix} 1 & \lambda_1 & \cdots & \lambda_1^k \\ 1 & \lambda_2 & \cdots & \lambda_2^k \\ \vdots & \vdots & & \vdots \\ 1 & \lambda_{k+1} & \cdots & \lambda_{k+1}^k \end{pmatrix} \begin{pmatrix} 0 \\ \rho_1(r_1, r_2) \\ \vdots \\ \rho_n(r_1, r_2) \end{pmatrix} = 0,$$

donde es claro que la matriz arriba (matriz Vandermonde) es invertible y por tanto,

$$\rho_1(r_1, r_2) = \cdots = \rho_k(r_1, r_2) = 0.$$

Entonces, para todo $r_1, r_2 \in \eta(FG)$, se tiene que $\rho_l(r_1, r_2) = 0$. Así, $\eta(FG) \in IP$. □

Del Lema de Linealización 1.6.4 debido a Kaplansky, $\eta(FG)$ satisface una identidad polinomial multilineal de la forma

$$f(x_1, x_2, \ldots, x_l) = \sum_{\sigma \in S_l} \alpha_\sigma x_{\sigma(1)} \cdots x_{\sigma(l)},$$

donde $\alpha_\sigma \in F$ y S_l es el grupo simétrico de grado l. Como $\eta(FG)$ no es nilpotente, se escogen $a_1, a_2, \ldots, a_l \in \eta(FG)$ con $a_1 a_2 \cdots a_l \neq 0$. Entonces,

$$a_1 FG a_2 FG \cdots a_l FG \neq (0)$$

y

$$\sum_{\sigma \in S_l} \alpha_\sigma a_{\sigma(1)} x_{\sigma(1)} a_{\sigma(2)} x_{\sigma(2)} \cdots a_{\sigma(l)} x_{\sigma(l)}$$

es una identidad polinomial multilineal no degenerada para FG (ver página 33). Por la Proposición 1.6.6, se tiene que $[G : \Phi(G)] < \infty$ y $|(\Phi(G))'| < \infty$.

Afirmación 10. $\Phi(G)$ **es localmente finito.**

Demostración. Sea $G_0 = \langle g_1, \ldots, g_r \rangle \leq \Phi(G)$ con un número finito de generadores. Como G_0 es un grupo de conjugación finita, entonces para todo g_i se tiene

$$[G_0 : C_{G_0}(g_i)] < \infty$$

y por tanto,

$$[G_0 : \bigcap_{i=1}^{r} C_{G_0}(g_i)] < \infty.$$

Más aún $\bigcap_{i=1}^{r} C_{G_0}(g_i) = \zeta(G_0)$. En efecto, si $z \in \zeta(G)$, $zg = gz$ para todo $g \in G$, es decir, $z \in C_G(g)$ para todo $g \in G$ y así, $z \in \bigcap_{i=1}^{r} C_G(g)$. Recíprocamente, se obtiene que $z \in \bigcap_{i=1}^{r} C_G(g)$ implica que $z \in \zeta(G)$.
Así,

$$[G_0, \zeta(G_0)] < \infty.$$

Por [30, Teorema 1.6.], $\zeta(G_0)$ es finitamente generado.

Además, $\zeta(G_0)$ es de torsión y Abeliano, luego es finito. Por tanto G_0 también es finito ($[G_0 : \zeta(G_i)] = |G|/|\zeta(G_0)| < \infty$), y así $\Phi(G)$ es localmente finito. □

Por el Teorema de Schmidt [30, Teorema 14.3.1], con $\Phi(G)$ localmente finito y $[G : \Phi(G)] < \infty$, se tiene que G es localmente finito.

Ahora bien, sea $\alpha = (\alpha_1, \alpha_2), \ldots, (\alpha_{r-1}, \alpha_r) \in \Phi'(G)$ donde cada $\alpha_i \in \Phi(G)$, y considere $H = \langle \alpha_1, \alpha_2 \ldots, \alpha_r \rangle$. Como H es finito ($\Phi(G)$ es localmente finito), y $\mathcal{U}(FH) \in IG$,

del Lema 2.2.8 se concluye que H' es p-grupo finito. Dado que $\alpha \in H'$, se tiene que $o(\alpha)$ es potencia de p. Por tanto, $\Phi'(G)$ es un p-grupo.

Así G contiene un subgrupo p-Abeliano de índice finito, a saber $\Phi(G)$. Luego, de la Proposición 1.6.5, $FG \in IP$.

□

Capítulo 3

Unidades simétricas: IG Vs. IP

Desde que Brian Hartley planteó su conjetura (Conjetura 2.1.1), el estudio de identidades de grupo dentro del grupo de unidades $\mathcal{U}(RG)$, del anillo de grupo RG y sus implicaciones han sido objeto de múltiples estudios ([32], [25], [8], [12] y [21]).

Con el Teorema clásico de Amitsur referente a anillos con involución (Teorema 1.6.3) y el trabajo desarrollado por Herstein y colaboradores [17], que motivó fuertemente el estudio de los anillos de grupo RG vistos como anillos con involución, fue planteada a finales de los 90's una versión de la conjetura de Hartley para las unidades simétricas [13], cuyo objetivo es verificar si una identidad de grupo en $\mathcal{U}^+(RG)$ implica ó una identidad de grupo en $\mathcal{U}(RG)$ ó directamente una identidad polinomial en el anillo de grupo RG.

El propósito del presente capítulo será dar respuesta afirmativa a la conjetura en este contexto y además, se obtendrá una caracterización de los grupos de torsión G tal que $\mathcal{U}^+(RG) \in IG$, donde RG está dotado de la involución clásica $*$, inducida por $g \mapsto g^{-1}$.

3.1. Anillos semiprimos con involución

Esta sección contiene inicialmente algunos resultados clásicos referente a anillos con involución. Posteriormente, se mostrarán ciertos resultados para anillos semiprimos cuyas unidades simétricas satisfacen una identidad de grupo, con algunas analogías de resultados del capítulo anterior, para el caso de las unidades simétricas.

En adelante, A será un dominio conmutativo infinito de característica diferente de 2, R un A-álgebra con unidad, tal que los elementos de A no son divisores de cero en R y $\zeta(R)$ denota el centro de R. Además, R está dotado de la involución clásica $*$, inducida por $g \mapsto g^{-1}$.

La demostración del siguiente teorema clásico puede ser encontrada en [13, Teorema 1], no se presenta aquí pues se escapa de los objetivos del presente trabajo.

Teorema 3.1.1. *Sean R un anillo semiprimo, $N \geq 1$ un entero y $\alpha \in \zeta(R)$. Si $a \in R$ es tal que $(ar(\alpha - a)r^*)^N = 0$ para todo $r \in R$, entonces $a \in \zeta(R)$.*

En consecuencia, se tiene que

Corolario 3.1.2. *Si R es un anillo semiprimo y $a \in R^+$ es tal que $(as)^N = 0$ para todo $s \in R^+$, entonces $a \in \zeta(R)$.*

Demostración. Sean $a \in R^+$ y $r \in R$. Como $rar^* \in R^+$, entonces $(ar(-a)r^*)^N = 0$ para todo $r \in R$. Del teorema anterior, tomando $\alpha = 0$, se tiene que $(ar(\alpha - a)r^*)^N = 0$ implica que $a \in \zeta(R)$. □

Sean $x \in R$ y $s \in R^+$ tales que $x^2 = s^2 = 0$, entonces tanto $(1 + x)(1 + x^*)$ como $1 + s$ son unidades simétricas. En efecto,

A continuación, algunos resultados de anillos cuyas unidades simétricas satisfacen una identidad de grupo.

Lema 3.1.3. *Si $\mathcal{U}^+(R)$ satisface la identidad $\omega(x, y) = 1$. Entonces existe un entero positivo $N > 1$ dependiendo solo de ω, tal que:*

1. *Si $a \in R$ y $a^2 = 0$, entonces $(aa^*)^N = 0$.*

2. *Si* s, $t \in R^+$ *y* $s^2 = t^2 = 0$, *entonces* $(stsd)^N = 0$ *para todo* $d \in R^+$.

Demostración. 1. Sea $\omega = \omega(x_1, x_2) = 1$ una identidad de grupo para $\mathcal{U}^+(R)$. Si $s, t \in R^+$ entonces, para todo $i \geq 0$, $t^i s t^i \in R^+$. Suponga que x y y son varibles no conmutativas tales que $x_1 = x$ y $x_2 = yxy$, ..., $x_n = y^{n-1}xy^{n-1}$. Así, se obtiene la identidad de grupo para $\mathcal{U}^+(R)$ en dos variables

$$\nu(x, y) = x^{i_1} y^{j_1} \dots x^{i_k} y^{j_k} = 1,$$

donde $k \geq 1$, j_i son enteros mayores que cero.

Tomando $a \in R$ tal que $a^2 = 0$ y como $(1 + a)(1 + a^*)$ y $(1 + a^*)(1 + a)$ son unidades simétricas, se tiene que

$$\nu((1 + a)(1 + a^*), (1 + a^*)(1 + a)) = 1,$$

lo que implica que

$$((1+a)(1+a^*))^{i_1}((1+a^*)(1+a))^{j_1} \dots ((1+a)(1+a^*))^{i_k}((1+a^*)(1+a))^{j_k} = 1 \quad (3.1)$$

Note que $(1 \pm a)^2 = 1 \pm 2a$ y $(1 \pm a^*)^2 = 1 \pm 2a^*$. Además, de la Ecuación 3.1, se obtiene que si $(1 \pm a)$ ó $(1 \pm a^*)$ aparecen con exponente i, entonces $i = 1, 2$.

Sea $\lambda = \lambda^*$ en A. Sustituyendo en la Ecuación 3.1, a por λa y a^* por λa^* y expandiendo la expresión se obtiene

$$((1+\lambda a)(1+\lambda a^*))^{i_1}((1+\lambda a^*)(1+\lambda a))^{j_1} \dots ((1+\lambda a)(1+\lambda a^*))^{i_k}((1+\lambda a^*)(1+\lambda a))^{j_k} = 1$$

$$\vdots$$

$$\lambda p_1(a, a^*) + \lambda^2 p_2(a, a^*) + \ldots + \lambda^N p_N(a, a^*) = 0$$

donde, para todo i, $p_i(a, a^*)$ es una expresión polinomial con coeficientes en a y a^*. Como los elementos en A no son divisores de cero en R, y A (por tanto, A^+)

es infinito, entonces por el argumento de Vandermonde usual [21, Lema 1.2.4], se obtiene que $p_i(a, a^*) = 0$ para $i \geq 1$.

Así, $p_N(a, a^*) = 0$ y esto implica que $2^r(aa^*)^M = 0$ para un $r \geq 0$ adecuado y $M \geq 1$. Como $car(A) \neq 2$ se obtiene que $(aa^*)^M = 0$.

2. Sea $s, t \in R^+$ tal que $s^2 = t^2 = 0$. Como $(1+s)(1+t)(1+s)$ y $(1+t)(1+s)(1+t)$ son unidades simétricas, entonces

$$((1+s)(1+t)(1+s))^{i_1}((1+t)(1+s)(1+t))^{j_1}\ldots = 1$$

Otra vez por el Argumento determinante de Vandermonde se tiene que $2^r(st)^M = 0$ para un $r \geq 0$ adecuado y $M \geq 1$. Entonces $(tstd)^{M+1} = 0$ y $tdt \in R^+$ implican que $(stdt)^M = 0$. Por tanto, $(tstd)^{M+1} = 0$.

□

Sean R semiprimo, e un elemento idempotente simétrico y $r \in R$. Como $(er(1-e))^2 = 0$, del lema anterior, exite $n \in \mathbb{N}$ tal que

$$0 = ((er(1-e))((er(1-e)))^*)^n = (er(1-e)r^*e)^n.$$

Como e es idempotente, entonces $e^n \neq 0$. Luego $(er(1-e)r^*)^n = 0$. Así, del Corolario 3.1.2 se tiene que e es un elemento central, siendo $r(1-e)r^* \in R^+$. Luego,

Lema 3.1.4. *Sean R semiprimo y $\mathcal{U}^+(R) \in IG$, entonces todo elemento idempotente simétrico de R es central.*

Como consecuencia, en los anillos de grupo se tiene:

Lema 3.1.5. *Sean F una cuerpo infinito de característica diferente de 2 y G un grupo tal que FG es semiprimo y $\mathcal{U}^+(FG)$ satisfacen una identidad de grupo. Si g es un elemento de orden finito en G, y $car(F)$ no divide al orden de g, entonces $\langle g \rangle$ es un subgrupo normal.*

Demostración. Sea $g \in G$, tal que $o(g) = m$. Esta prueba se sigue de la demostración de la Afirmación 1. del Teorema 2.3.2.

Así, se tiene que $\frac{1}{m}\hat{g}$ es idempotente. Además, debido a la involución clásica sobre FG inducida por $g \mapsto g^{-1}$ se tiene

$$(\frac{1}{m}\hat{g})^* = \frac{1}{m}(g^{m-1} + g^{m-2} + \cdots + g + 1) = \frac{1}{m}(1 + g + \cdots + g^{m-1}) = \frac{1}{m}\hat{g},$$

es decir, $\frac{1}{m}\hat{g}$ también es simétrico. Luego, por el Lema 3.1.4, $\frac{1}{m}\hat{g}$ es central. Por tanto, $h\widehat{g} = \widehat{g}h$ para todo $h \in G$. Luego,

$$h\widehat{g}h^{-1} = \widehat{g}$$

$$1 + hgh^{-1} + hg^2h^{-1} + \cdots + hg^{m-1}h^{-1} = 1 + g + g^2 + \cdots + g^{m-1}.$$

Luego existe j tal que $hgh^{-1} = g^j \in \langle g \rangle$. Por lo tanto, $\langle g \rangle \lhd G$ para todo $g \in G$. □

Recuerde que un grupo no Abeliano G es un grupo Hamiltoniano si todo subgrupo de G es normal; en este caso se tiene que $G = \mathcal{Q}_8 \times E \times A$ donde E es un 2-grupo Abeliano elemental y A es grupo Abeliano cuyos elementos son de orden impar (Teorema 1.1.6). Si $A = \{1\}$, G es llamado 2-*grupo Hamiltoniano*. La siguiente observación será crucial para la clasificación de las álgebras de grupo tales que el grupo es de torsión, y cuyas unidades simétricas satisfacen una identidad de grupo.

Lema 3.1.6. *Sean F un cuerpo y G un 2-grupo Hamiltoniano. Entonces en el álgebra de grupo FG todos los elementos simétricos conmutan.*

Demostración. Para esta prueba, note que $G = E \times \mathcal{Q}_8$ y $FG \cong FE(\mathcal{Q}_8)$. Dado que la involución sobre FG es la clásica, los elementos de FE son fijados por ella.

Considere ahora, $\alpha \in FG$. Entonces $\alpha \in \zeta(FG)$, si y solo si,

$$\alpha = h^{-1}\alpha h = \sum_{g \in G} \alpha_g h^{-1}gh = \sum_{u = h^{-1}gh \in G} \alpha_u u,$$

para todo $h \in G$, es decir, si y solo si $\alpha_g = \alpha_{h^{-1}gh}$ para todos $g, h \in G$. Es claro que todo elemento de orden 1 ó 2 es central, caso contrario $h^{-1}ah = a$ ó $h^{-1}ah = a^{-1}$. Así, los elementos $\alpha \in FG$ centrales son exactamente combinaciones lineales de elementos

de orden 1 ó 2 y términos de la forma $a + a^{-1}$, que son los elementos simétricos en FG. □

En el capítulo anterior se mostró esencialmente que en presencia de suficientes elementos nilpotentes, si $\mathcal{U}(R)$ verifica una identidad de grupo entonces R verifica una identidad polinomial. Modificando los argumentos allí expuestos y con el objetivo de analizar la Conjetura de Hartley en el contexto de las unidades simétricas, Giambruno, Sehgal y Valenti obtuvieron la siguiente analogía.

Lema 3.1.7. *Suponga que $\mathcal{U}^+(R) \in IG$. Sea S un subanillo nil de R invariante bajo $*$. Entonces S satisface una identidad polinomial.*

Demostración. Sea $\omega(x, y) = 1$ la identidad de grupo que satisfacen $\mathcal{U}^+(R)$ y considere el anillo de series de potencias $F\{x_1, x_2\}[t]$. Por el Argumento de Magnus (Proposición 2.3.1), $1+x_1t$ y $1+x_2t$ genera un subgrupo libre en el grupo de unidades $\mathcal{U}(R)$, entonces

$$\omega(1 + x_1t, 1 + x_2t) - 1 = \sum_{i\geq 0} \rho_i(x_1, x_2)t^i \neq 0,$$

donde para algún m, ρ_m no es el polinomio cero. Escogiendo s_1, $s_2 \in S^+$ y $\lambda \in A^+$, se tiene para $i = 1, 2$ que $1+\lambda s_i$ son unidades simétricas en R con inverso $(1+s_i\lambda)^{-1} = 1 - s_i\lambda + s_2^2\lambda^2 - \cdots$. Evaluando ω en estos elementos, de la expresión arriba se obtiene

$$\sum_{i=1}^{k} \rho_i(s_1, s_2)\lambda^i = 0,$$

para algún $k > 0$, y $\rho_t(s_1, s_2) = 0$ para todo $t > k$. Ahora como A (por tanto A^+) es infinito, se pueden escoger elementos distintos $\lambda_1, \ldots, \lambda_{j+1} \in F$ tales que

$$\begin{pmatrix} 1 & \lambda_1 & \lambda_1^2 & \cdots & \lambda_1^k \\ 1 & \lambda_2 & \lambda_2^2 & \cdots & \lambda_2^k \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \lambda_{k+1} & \lambda_{k+1}^2 & \cdots & \lambda_{k+1}^k \end{pmatrix} \begin{pmatrix} \rho_0(s_1, s_2) \\ \rho_1(s_1, s_2) \\ \vdots \\ \rho_k(s_1, s_2) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Por el Argumento de Vandermonde usual [21, Lema 1.2.4], se obtienen que $\rho_t(s_1, s_2) = 0$ para todo $t \leq k$. Entonces $\rho_k(x_1, x_2)$ satisface una $*$-identidad polinomial en S^+. El Teorema de Amitsur 1.6.3 implica que $S \in IP$. $\square$

Ahora bien, sea $\mathcal{L}$ el subanillo de R generado por todos los elementos simétricos de cuadrado cero.

Teorema 3.1.8. *Sea R un anillo semiprimo tal que $\mathcal{U}^+(R)$ satisfacen una identidad de grupo. Entonces,*

1. *$\mathcal{L}$ es un subanillo nil de R tal que $\mathcal{L}$ satisface una identidad polinomial.*
2. *Si $e \in R^+$ es tal que $e^2 = e$, entonces $e \in \zeta(R)$ y $A^{-1}R$ es central.*

Demostración. 1. Sea $\mathcal{L} = \langle a \in R : t^i = 0 \rangle$. A continuación se motrará que L contiene todo los elementos simétrico nilpotentes de R, analogamente al Lema 2.2.1.

Sean $s, t_1, t_2, \ldots, t_n \in R^+$ tales que $s^2 = t^2 = \cdots = t_n^2 = 0$. Entonces $st_1 \cdots t_n s = 0$ para todo $n \geq 1$. Se realizara inducción sobre n.

Para $n = 1$, se tiene por [21, Lema 2.2.7.1], que $sts = 0$. Es decir, el enunciado es cierto.

Ahora supongamos que $n > 1$ y $st_1 \ldots t_{n-1} s = 0$. Dado que $t_n \in R^+$ y $t_n^2 = 0$, por [21, Lema 2.2.7.2], se tiene que $st_1 t_2 \cdots t_{n-1} s = 0$ implica que

$$(st_1 t_2 \cdots t_{n-1}) t_n s = 0,$$

es decir, el enunciado vale para todo $n \geq 1$.

Claramente, $\mathcal{L}$ contiene todo los elementos simétricos nilpotenes de R, luego $\mathcal{L}$ es un subanillo nil de R y, del Lema 3.1.7, se tiene que $\mathcal{L} \in IP$.

2. Sea $A^{-1}R$ el cuerpo de fracciones de R. Como R es un A-álgebra y $AR \subseteq R$, se puede suponer que $a \in A^+$, dado que

$$a^{-1}r = a^{-1}(a^*)^{-1}a^*r = \underbrace{(aa^*)^{-1}}_{\in A^+}\underbrace{(a^*r)}_{\in R}.$$

Sea e un elemento idempotente simétrico de $A^{-1}R$, luego existe $\alpha \in A^+$ tal que $\alpha e = f \in R$ ($e = \alpha^{-1}f$, $\alpha \in A^+$ y $f \in R$). Así,

$$f^* = (\alpha e)^* = \alpha^* e^* = \alpha e = f,$$

$$f^2 = (\alpha e)^2 = \alpha^2 e^2 = \alpha^2 e = \alpha(\alpha e) = \alpha f.$$

Luego $(f - \alpha)f = 0$ y para todo $r \in R$, se tiene

$$[fr(f-\alpha)]^2 = fr\underbrace{(f-\alpha)f}_{0}r(f-\alpha) = 0.$$

Por el Lema 3.1.3(1), existe $N \geq 1$ tal que $[fr(f-\alpha)(fr(f-\alpha)^*)]^N = 0$. Como

$$\begin{aligned}[fr(f-\alpha)(fr(f-\alpha)^*)]^N &= [fr(f-\alpha)[fr(f-\alpha)^*]^*]^N \\ &= [fr(f-\alpha)(f-\alpha)^* fr^*]^N \\ &= [fr(f-\alpha)^2 fr^*]^N = 0,\end{aligned}$$

es decir, para todo $r \in R$, $[fr(f-\alpha)^2 r^* f]^N = 0$. Multiplicando por $r(f-\alpha)^2 r^*$ se tiene que,

$$[fr(f-\alpha)^2 r^*]^{N+1} = 0,$$

con $\alpha \in \zeta(R)$. Del Teorema 3.1.1, $f \in \zeta(R)$ pues $e = \alpha^{-1}f \in A^{-1}R$ implica que $e \in \zeta(A^{-1}R)$.

Lo anterior también muestra que si e es un elemento idempotente tal que $e \in R^+$, entonces $e \in \zeta(R)$.

□

En general, el conjunto P de los p-elementos de cualquier grupo no es subgrupo, sin embargo para un grupo finito se tiene que:

Lema 3.1.9. *Sea G un grupo finito. Si para todo $g \in P$, $(g-1)^2 \in J(FG)$, entonces P es un subgrupo (normal) de G.*

Demostración. Las hipótesis del lema se heredan por subgrupos y grupos factores. En efecto, sean $H \leq G$ y $g \in H \cap P$. Entonces $(g-1)^2 \in J(FG) \cap FH \subset J(FH)$.

Sean $H \lhd G$ y $\overline{g} \in G/H$ un p-elemento, entonces $(\overline{g}-1)^2 \in J(F(G/H))$. En efecto, si $\overline{g}$ es un p-elemento entonces existe $k \in \mathbb{Z}$ tal que $(k,p)=1$. Como g^k también es un p-elemento, entonces $(g^k-1)^2 \in J(FG)$. De [21, Lema 1.3.3](1), se tiene que $J(FG)$ es nilpotente, por tanto la imagen de $J(FG)$ bajo $\pi : FG \to F(G/H)$ es ideal nilpotente de $F(G/H)$. Luego $\overline{(g^k-1)^2} = (\overline{g}^k-1)^2 \in \varepsilon_H(J(FG)) \subseteq J(F\overline{G})$ ya que cada ideal nil de FG esta contenido en $J(FG)$. Es claro que para todo $l \in \mathbb{Z}$, g^{k^l} es un p-elemento de G, al igual que $\overline{g}$. Entonces $\overline{g}^{k^l} = \overline{g}$. Aplicando varias veces el argumento anterior, se obtiene que $(\overline{g}^{k^l}-1)^2 \in \varepsilon_H(FG) \subseteq J(F(G/H))$ y remplazando g^{k^l} por g, tenemos que $(\overline{g}-1)^2 \in J(F(G/H))$ como queriamos.

Suponga que $F = \overline{\mathbb{Z}}_p$ es la clausura de $\mathbb{Z}_p$ como en [21, Lema 2.3.3]. Sea G el menor subgrupo satisfaciendo las hipótesis del lema pero no la conclusión. Luego, existen g, $h \in P$ tal que su producto no es un p-elemento. Como $\langle g,h\rangle \leq G$, entonces $\langle g,h\rangle = G$ pues gh no es un p-elemento.

Supongamos que G tiene una representación ρ irreducible de grado mayor que 1. Caso contrario, cada representación ρ_i de G es de grado exactamente uno, $deg(\rho_i) = 1 = dim_K(I_i)$. Por el Teorema 1.2.8 $R = FG/J(FG)$ es semisimple, luego del Teorema de Wedderburn-Artin (Teorema 1.2.7) se tiene que,

$$R = \bigoplus_{i=1}^{l} M_{n_i}(D_i)$$

Como $F = \mathbb{Z}_p$, entonces cada $D_i = F$ y así $F(G/J(FG)) \cong \bigoplus_i^l F$ es conmutativo. Luego para x, $y \in G$ se tiene que $(x,y) = x^{-1}y^{-1}xy = 1\ mod(J(FG))$. Por tanto, para cada $g \in G'$, $g-1 \in J(FG)$ es nilpotente y así, g es un p-elemento. Por tanto, G' es un p-grupo (2.2.8). Entonces G es conmutativo módulo G', pues se conoce del Teorema 1.1.3, que G/G' es Abeliano. Pero esto contradice la suposición, ya que los p-elementos de G no pueden formar un subgrupo. Por lo tanto, G tiene una representación ρ irreducible de grado mayor que 1 (ver página 28).

Afirmación 11. ρ es una representación irreducible fiel.

Demostración. Sea $K = Ker(\rho) \neq 1$. Claramente $K \neq G$. Por la minimalidad de G, tenemos que los p-elementos de K forman un subgrupo N que es normal. Note que para algún $n \in N$, $(g^{-1}ng)^{p^k} = g^{-1}n^{p^k} \in N$. Pero si $N \neq \{1\}$, nuevamente por la minimalidad del orden de G, los p-elementos de G/N forman un subgrupo, también normal. Por lo tanto, los p-elementos de G forman un subgrupo pues $(gh)^{p^{k_1}p^{k_2}} \mapsto (ghN)^{p^{k_1}p^{k_2}} = N$ para algún $k \in \mathbb{N}$. Luego, $(gh)^{k_1+k_2} \in N$ si y solo si $(gh)^{k_1+k_2+k_3} = 1 mod N$. Así, gh es un p-elemento, que es una contradicción. Por lo tanto, K es un p'-grupo.

Es claro que los p-elementos de G/K forman un subgrupo normal L/K, donde $K \subseteq L$. Como $\rho : G \to GL(V)$ induce de manera natural una representación sobre $G \setminus K$ que es irreducible y fiel. Luego, $\Delta(G/K, L/K) = K$ es nilpotente (Corolario 1.3.8) y así, $\Delta(G/K, L/K) \subseteq J(FG/K)$. Es decir, todo elemento de L/K hace parte de K de alguna representación irreducible de G/K. Como dichas representaciones son fieles en G/K se tiene que $L = K$ y G no contiene p-elementos, contradicción. Por lo tanto, ρ es una representación irreducible fiel. □

Finalmente, si g es un p-elemento en G, entonces $(g-1)^2 \in J(FG)$, luego el polinomio minimal de $\rho(g)$ es lineal o cuadrático. De ser lineal, $\rho(g)$ seria multiplo escalar de la matriz identidad pero esto no es posible pues $car(F) = p$. Luego $G \neq K$ ya que K es un p'-grupo. Así, se tienen todas las condiciones en [21, Proposición 2.3.3]. Por tanto, G contiene un subgrupo isomorfo a $SL_2(\mathbb{Z}_p)$.

Como $SL_2(\mathbb{Z}_p)$ satisface las hipotesis del lema pero sus p-elementos no forman un subgrupo, entonces $G = SL_2(\mathbb{Z}_p)$. Note que $\zeta(G) = PSL_2(\mathbb{Z}_p)$ donde nuevamente los p-elementos no forman un subgrupo, contradiciendo la minimalidad del grado de G. Por lo tanto, los p-elementos de G forman un subgrupo. □

3.2. Teoremas de clasificación

Esta sección contiene la prueba de la respuesta afirmativa a la Conjetura de B. Hartley en unidades simétricas planteada por Giambruno, Sehgal y Valenti en [13].

Además, se presentan los teoremas de clasificación de grupos de torsión tales que las unidades simétricas satisfacen una identidad de grupo.

Primero, un resultado análogo al Lema 2.2.7, que será útil en la clasificación de los grupos finitos cuyas unidades simétricas satisfacen una identidad de grupo.

Lema 3.2.1. *Sean F un cuerpo con $car(F) = p > 2$ y G un grupo tal que $\mathcal{U}^+(FG)$ satisfacen la identidad $\omega(x_1, \ldots, x_n) = 1$. Si N es un p-grupo de G, y N es finito o G localmente finito, entonces $\mathcal{U}^+(F(G/N))$ satisface $\omega(x_1, \ldots, x_n) = 1$.*

Sea G es un grupo finito y $\mathcal{U}^+(FG) \in IG$, entonces por el Lema 3.2.1, $\mathcal{U}^+(F(G/P) \in IG$. Supongamos que G no posee elementos de orden p. Luego, del Lema 3.1.5, todo subgrupo de G es normal. Por tanto, G es Abeliano o Hamiltoniano. En caso de ser Hamiltoniano, $G = \mathcal{Q}_8 \times E \times A$, (Teorema 1.1.6). Para concretar la clasificación de los grupos finitos se necesita que $A = \{1\}$. El siguiente resultado ayudará a resolver esta cuestión.

Lema 3.2.2. *Sea F un cuerpo infinito de $car(F) = p > 2$. Si $\mathcal{U}^+(\mathcal{Q}_8 \times \langle c \rangle)$ satisface la identidad de grupo $\omega(x, y) = 1$, entonces existe un entero m, dependiendo solo de ω, tal que $o(c)$ divide a $2p^m$.*

Demostración. Como $car(F) \geq 0$, existe λ, $\mu \in F$ tal que $\lambda^2 + \mu^2 = -1$. Se conoce que $\mathcal{Q}_8 = \langle g, , h : g^4 = 1, g^2 = h^2, gh = h^{-1}g \rangle$ y $F\mathcal{Q}_8 \cong 4F \oplus M_{2x2}(F\langle c \rangle)$. Luego,

$$\theta : F(\mathcal{Q}_8 \times \langle c \rangle) \to M_{2x2}(F\langle c \rangle)$$

$$\theta(g) = \begin{pmatrix} \lambda & \mu \\ \mu & -\lambda \end{pmatrix}, \quad \theta(h) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \text{ y } \quad \theta(c) = \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix}$$

es un homomorfismo. Ahora bien, sean

$$\alpha = \frac{1}{4}(c + c^{-1}g^2)(\mu g - h + \lambda gh)(1 - g^2), \text{ y}$$

$$\beta = \frac{1}{4}(c + c^{-1}g^2)(\mu g + h + \lambda gh)(1 - g^2)$$

elementos simétricos de cuadrado cero. En efecto, como $(c + c^{-1}g^2)(c + c^{-1}g^2) = c^2 + 2g^2 + c^{-2}$ y $(1 - g^2)(1 - g^2) = 1 - 2g^2 + g^4 = 2(1 - g^2)$ se tiene que:

$$[(c + c^{-1}g^2)(1 - g^2)]^2 = c^2 - c^2h^2 + c^{-2} - c^{-2}h^2 + 2h^2 - 2 \tag{3.2}$$

Recuerde que en $\mathcal{Q}_8$, $h^{-1} = h^3 = g^2h$, $h^2hg = gh$ y $h^2gh = hg$. Luego,
$(\mu g - h + \lambda gh)(\mu g - h + \lambda gh) =$

$$= \mu^2g^2 - \mu gh + \mu\lambda g^2h - \mu hg + h^2 - \lambda hgh + \mu\lambda ghg - \lambda gh^2 + \lambda^2 ghgh$$

$$= \mu^2g^2 - \mu gh + \mu\lambda g^2h - \mu hg + g^2 - \lambda g + \mu\lambda h - \lambda gh^2 + \lambda^2h^2$$

$$= (\mu^2 + 1)g^2 + \lambda g^2 - \mu gh + \mu\lambda g^2h - \mu hg - \lambda g + \mu\lambda h - \lambda gh^2$$

$$= -\mu gh + \mu\lambda g^2h - \mu hg - \lambda g + \mu\lambda h - \lambda gh^2 \tag{3.3}$$

De la Ecuación 3.2 y la Ecuación 3.3, se tiene

$$\alpha^2 = [\frac{1}{4}(c + c^{-1}g^2)(\mu g - h + \lambda gh)(1 - g^2)]^2 = 0,$$

ya que todos los términos en la siguiente lista se cancelan con el númeral anterior, como esta indicado. Así,
$\frac{1}{16}(c^2 - c^2h^2 + c^{-2} - c^{-2}h^2 + 2h^2 - 2)(-\mu gh + \mu\lambda g^2h - \mu hg - \lambda g + \mu\lambda h - \lambda gh^2) =$

1. $-\mu c^2gh + \mu\lambda c^2g^2h - \mu c^2hg - \lambda c^2g + \mu\lambda c^2h - \lambda c^2gh^2$
2. $\underbrace{\mu c^2hg}_{3} - \underbrace{\mu\lambda c^2h}_{5} + \underbrace{\mu c^2gh}_{1} + \underbrace{\lambda c^2gh^2}_{6} - \underbrace{\mu\lambda c^2h^3}_{2} + \underbrace{\lambda c^2g}_{4}$
3. $-\mu c^{-2}gh + \mu\lambda c^{-2}g^2h - \mu c^{-2}hg - \lambda c^{-2}g + \mu\lambda c^{-2}h - \lambda c^{-2}gh^2$
4. $\underbrace{\mu c^{-2}hg}_{3} - \underbrace{\mu\lambda c^{-2}h}_{5} + \underbrace{\mu c^{-2}gh}_{1} + \underbrace{\lambda c^{-2}gh^2}_{6} - \underbrace{\mu\lambda c^{-2}g^2h}_{2} + \underbrace{\lambda c^{-2}g}_{4}$
5. $-2\mu hg + 2\mu\lambda h - 2\mu gh - 2\lambda gh^2 + 2\mu\lambda g^2h - 2\lambda g$
6. $\underbrace{2\mu gh}_{3} - \underbrace{2\mu\lambda g^2h}_{5} + \underbrace{2\mu hg}_{1} + \underbrace{2\lambda g}_{6} - \underbrace{2\mu\lambda h}_{2} + \underbrace{2\lambda gh^2}_{4}$

Revisando los términos de β se tiene que $(\mu g + h + \lambda gh)(\mu g + h + \lambda gh) =$

$$= \mu^2 g^2 + \mu gh + \mu\lambda g^2 h + \mu hg + h^2 + \lambda hgh + \mu\lambda ghg + \lambda gh^2 + \lambda^2 ghgh$$

$$= \mu^2 g^2 + \mu gh + \mu\lambda g^2 h + \mu hg + g^2 + \lambda g + \mu\lambda h + \lambda gh^2 + \lambda^2 h^2$$

$$= (\mu^2 + \lambda^2) g^2 + g^2 + \mu gh + \mu\lambda g^2 h + \mu hg + \lambda g + \mu\lambda h + \lambda gh^2$$

$$= \mu gh + \mu\lambda g^2 h + \mu hg + \lambda g + \mu\lambda h + \lambda gh^2 \tag{3.4}$$

Por la Ecuación 3.2 y la Ecuación 3.4 se tiene que β es de cuadrado cero, pues todos los términos en la siguiente lista se anulan, respectivamente con el literal anterior.

$$\beta^2 = [\frac{1}{4}(c + c^{-1}g^2)(\mu g + h + \lambda gh)(1 - g^2)]^2 =$$

$\frac{1}{8}(c^2 - c^2h^2 + c^{-2} - c^{-2}h^2 + 2h^2 - 2)(\mu gh + \mu\lambda g^2 h + \mu hg + \lambda g + \mu\lambda h + \lambda gh^2) =$

1. $\mu c^2 gh + \mu\lambda c^2 g^2 h + \mu c^2 hg + \lambda c^2 g + \mu\lambda c^2 h + \lambda c^2 gh^2$
2. $\underbrace{-\mu c^2 h^2 gh}_{3} - \underbrace{\mu\lambda c^2 h^2 g^2 h}_{5} - \underbrace{\mu c^2 h^2 hg}_{1} - \underbrace{\lambda c^2 h^2 g}_{6} - \underbrace{\mu\lambda c^2 g^2 h}_{2} - \underbrace{\lambda c^2 g}_{4}$
3. $\mu c^{-2} gh + \mu\lambda c^{-2} g^2 h + \mu c^{-2} hg + \lambda c^{-2} g + \mu\lambda c^{-2} h + \lambda c^{-2} gh^2$
4. $\underbrace{-\mu c^{-2} h^2 gh}_{3} - \underbrace{\mu\lambda c^{-2} h}_{5} - \underbrace{\mu c^{-2} h^2 hg}_{1} - \underbrace{\lambda c^{-2} h^2 g}_{6} - \underbrace{\mu\lambda c^{-2} h^2 h}_{2} - \underbrace{\lambda c^{-2} g}_{4}$
5. $-2\mu gh - 2\mu\lambda g^2 h - 2\mu hg - 2\lambda g - 2\mu\lambda h - 2\lambda gh^2$
6. $\underbrace{2\mu h^2 gh}_{3} + \underbrace{2\mu\lambda h}_{5} + \underbrace{2\mu h^2 hg}_{1} + \underbrace{2\lambda h^2 g}_{6} + \underbrace{2\mu\lambda h^2 h}_{2} + \underbrace{2\lambda g}_{4}$

Finalmente se tiene que α y β son elementos simétricos.

$$\begin{aligned}
\alpha^* &= [\frac{1}{4}(c + c^{-1}g^2)(\mu g - h + \lambda gh)(1 - g^2)]^* \\
&= \frac{1}{4}[(1 - g^2)^*(\mu g - h + \lambda gh)^*(c + c^{-1}g^2)^*] \\
&= \frac{1}{4}[(1^{-1} - (g^2)^{-1})(\mu g^{-1} - h^{-1} + \lambda(gh)^{-1})(c^{-1} + (c^{-1}g^2)^{-1})] \\
&= \frac{1}{4}[(1 - g^2)(\mu g^{-1} - hh^2 + \lambda ghh^2)(c^{-1} + g^2 c)] \\
&= \frac{1}{4}[(1 - g^2)(\mu g - h + \lambda h^{-1} gh)h^2 g^2 (c + c^{-1}g^{-2})] \\
&= \frac{1}{4}[(c + c^{-1}g^{-2})(\mu g - h + \lambda h^{-1} gh)(1 - g^2)] \\
&= \alpha.
\end{aligned}$$

$$\begin{aligned}
\beta^* &= [\frac{1}{4}(c+c^{-1}g^2)(\mu g+h+\lambda gh)(1-g^2)]^* \\
&= \frac{1}{4}[(1-g^2)^*(\mu g+h+\lambda gh)^*(c+c^{-1}g^2)^*] \\
&= \frac{1}{4}[(1^{-1}-(g^2)^{-1})(\mu g^{-1}+h^{-1}+\lambda(gh)^{-1})(c^{-1}+(c^{-1}g^2)^{-1})] \\
&= \frac{1}{4}[(1-g^2)(\mu g^{-1}+hh^2+\lambda ghh^2)(c^{-1}+g^2c)] \\
&= \frac{1}{4}[(1-g^2)(\mu g+h+\lambda h^{-1}gh)h^2g^2(c+c^{-1}g^{-2})] \\
&= \frac{1}{4}[(c+c^{-1}g^{-2})(\mu g+h+\lambda h^{-1}gh)(1-g^2)] \\
&= \beta.
\end{aligned}$$

Por lo tanto, α y β son elementos simétricos de cuadrado cero. Entonces, por el Lema 3.1.3(2), existe n, dependiendo solo de ω, tal que $(\alpha\beta\alpha\beta)^k = (\alpha\beta)^n = 0$ para algún $n = 2k \in \mathbb{N}$ y $d = \beta$.

Aplicando el homomorfismo se tiene que $0 = \theta[(\alpha\beta)^n] = [\theta(\alpha)\theta(\beta)]^n$. Es decir,

$$\begin{aligned}
\theta(\alpha) &= \theta[\frac{1}{4}(c+c^{-1}g^2)(\mu g-h+\lambda gh)(1-g^2)] \\
&= \frac{1}{4}\theta(1)[\underbrace{\theta(c)+\theta^{-1}(c)\theta^2(g)}_{1}][\underbrace{\mu\theta(g)-\theta(h)+\lambda\theta(gh)}_{2}][\underbrace{\theta(1)-\theta^2(g)}_{3}].
\end{aligned}$$

1. $\begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix} + \begin{pmatrix} c^{-1} & 0 \\ 0 & c^{-1} \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} c-c^{-1} & 0 \\ 0 & c-c^{-1} \end{pmatrix}$.

2. $\mu\begin{pmatrix} \lambda & \mu \\ \mu & -\lambda \end{pmatrix} - \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + \lambda\begin{pmatrix} \lambda & \mu \\ \mu & -\lambda \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} \mu\lambda-\lambda\mu & \mu^2+\lambda^2-1 \\ -\lambda^2+\lambda^2 & -\mu\lambda+\lambda\mu \end{pmatrix} = \begin{pmatrix} 0 & -2 \\ 0 & 0 \end{pmatrix}$.

3. $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} \lambda^2+\mu^2 & \lambda\mu-\mu\lambda \\ \mu\lambda-\lambda\mu & \mu^2\lambda^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$.

Por lo tanto,

$$\begin{aligned}\theta(\alpha) &= \frac{1}{4}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} c-c^{-1} & 0 \\ 0 & c-c^{-1} \end{pmatrix}\begin{pmatrix} 0 & -2 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \\ &= \begin{pmatrix} \frac{1}{4}(c-c^{-1}) & 0 \\ 0 & \frac{1}{4}(c-c^{-1}) \end{pmatrix}\begin{pmatrix} 0 & -4 \\ 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & -(c-c^{-1}) \\ 0 & 0 \end{pmatrix}.\end{aligned}$$

Así, $\theta(\alpha) = \begin{pmatrix} 0 & -(c-c^{-1}) \\ 0 & 0 \end{pmatrix}$ y de manera análoga, $\theta(\beta) = \begin{pmatrix} 0 & 0 \\ -(c-c^{-1}) & 0 \end{pmatrix}$.

Retomando, se tiene que $[\theta(\alpha)\theta(\beta)]^n = \begin{pmatrix} (c^{-1}-c)^2 & 0 \\ 0 & 0 \end{pmatrix}^n = \begin{pmatrix} (c^{-1}-c)^{2n} & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$,

es decir, $(c^{-1}-c)^{2n} = 0$.

Escogiendo $m \in \mathbb{N}$ tal que $p^m > 2n$, $0 = (c^{-1}-c)^{p^m} = c^{-p^m} = c^{p^m}$. Se obtiene finalmente que $c^{2p^m} = 1$, que significa que el orden de c es divisible por $2p^m$. □

Por tanto, si $G/P = \mathcal{Q}_8 \times E \times A$, entonces A no tiene p-elementos, es decir, $A = \{1\}$, y así,

Teorema 3.2.3. *Sean G un grupo finito y F un cuerpo infinito tal que $car(F) = p > 2$. $\mathcal{U}^+(FG) \in IG$ si y solo si P es un subgrupo normal de G y G/P es Abeliano o un 2-grupo Hamiltoniano.*

También es importante conocer las álgebras de grupo cuyas unidades simétricas no satisfacen una identidad de grupo.

Lema 3.2.4. *Sea $G = \mathcal{Q}_8 \times \langle c \rangle$, donde $c \neq 1$ tiene orden impar. Entonces $\mathcal{U}^+(\mathbb{Q}G)$ no satisface una identidad de grupo.*

Demostración. Suponga que *o(c)*= q un número primo impar. Observe que si ξ es la raíz q-ésima de la unidad, la aplicación $\mathbb{Q}\langle c \rangle \to \mathbb{Q}(\xi)$ define un epimorfismo y como

$1 + x + \cdots + x^{q-1} = (x-1)(x^{q-1} + \cdots + x + 1)$ es el polinomio minimal de ξ sobre $\mathbb{Q}$ se tiene que:

$$\mathbb{Q}\langle c\rangle \cong \frac{\mathbb{Q}(\xi)}{\langle 1 + x + \cdots + x^{q-1}\rangle},$$

es decir, el núcleo del epimorfismo es claramente $\mathbb{Q}\langle c\rangle(\frac{1}{q}\hat{c})$. Sea $e_1 = 1 - \frac{1}{q}\hat{c}$ tal que

$$[1 - \frac{1}{q}\hat{c}]^2 = 1 - 2\frac{1}{q}\hat{c} + \frac{1}{q^2}\sum_c c\hat{c} = 1 - 2\frac{1}{q}\hat{c} + \frac{1}{q^2}q\hat{c} = 1 - 2\frac{1}{q}\hat{c} + \frac{1}{q}\hat{c} = 1 - \frac{1}{q}\hat{c} \quad y,$$

$$[1 - \frac{1}{q}\hat{c}]^* = 1 - \frac{1}{q}(1 + c + \cdots + c^{q-1})^* = 1 - \frac{1}{q}(c^{q-1} + \cdots + c + 1) = 1 - \frac{1}{q}\hat{c}$$

Así, e_1 es un elemento simétrico idempotente central, por lo tanto,

$$\mathbb{Q}\langle c\rangle = \mathbb{Q}\langle c\rangle e_1 \oplus \mathbb{Q}\langle c\rangle(1 - e_1).$$

Luego el epimorfismo, $\mathbb{Q}\langle c\rangle \to \mathbb{Q}(\xi)$, puede restringirse al isomorfismo $\mathbb{Q}\langle c\rangle e_1 \to \mathbb{Q}(\xi)$.

La aplicación $\mathbb{Q}\mathcal{Q}_8 \to \mathbb{H}(\mathbb{Q})$ dada por $g \to i$ y $h \to j$ es un epimorfismo. Para ver que esto es cierto, es suficiente con definir la aplicación para i, j ya que $gh \mapsto ij = k$. Observe que $-g^2 \mapsto 1$, luego $\frac{1+g^2}{2} \mapsto 0$ y, como se definió para el epimorfismo anterior, tenemos que $\frac{1}{2}\hat{g}^2 \mapsto 0$, es decir, este epimorfismo tiene núcleo $\mathbb{Q}\mathcal{Q}_8(\frac{1+g^2}{2})$.

Sea $e_2 = 1 - \frac{1+g^2}{2}$ tal que

$$\big[\frac{1+g^2}{2}\big]^2 = \frac{(1+g^2)^2}{2^2} = \frac{1 + 2g^2 + 1}{4} = \frac{2(1+g^2)}{4} = \frac{1+g^2}{2} \quad y,$$

$$\big[\frac{1+g^2}{2}\big]^* = \frac{1}{2}(1+g^2)^* = \frac{1}{2}(1+g^{-2}) = \frac{1+g^2}{2}$$

Luego e_2 también es un elemento simétrico idempotente central. De manera similar, se restringe el epimorfismo al isomorfismo

$$\mathbb{Q}\mathcal{Q}_8 e_2 \to \mathbb{H}(\mathbb{Q}).$$

Como

$$\mathbb{Q}G \cong \mathbb{Q}(\mathcal{Q}_8 \times \langle c\rangle) \cong \mathbb{Q}\mathcal{Q}_8 \oplus_{\mathbb{Q}} \mathbb{Q}\langle c\rangle,$$

Como $e = e_1e_2$ es un elemento simétrico idempotente central, el epimorfismo

$$\theta\colon \mathbb{Q}G \to \mathbb{H}(\mathbb{Q}(\xi))$$

$$g \mapsto i \quad h \mapsto j \quad c \mapsto \xi.$$

puede restringirse al isomorfismo $\mathbb{Q}Ge \to \mathbb{H}(\mathbb{Q}(\xi))$.

Recuerde que los elementos de la forma $\lambda + \mu i$ en $\mathbb{C}$, con λ, $\mu \in \mathbb{Q}(\xi)$, tienen esta única forma de expresarse. Note que si $i \in \mathbb{Q}(\xi)$, entonces $\mathbb{Q}(\xi)$ contiene la $4q$-esíma raíz primitiva de la unidad. Pero el polinomio minimal ξ sobre $\mathbb{Q}$ tiene grado $\varphi(4q) = 2(q-1)$, donde φ es la función Euler. Esto es una contradicción pues $\varphi(q) = q - 1$.

Luego $i \notin \mathbb{Q}(\xi)$, por tanto se identificarán los elementos de la forma $\lambda+\mu i \in \mathcal{H}(\mathbb{Q}(\xi))$ con los elementos del subcampo $\mathbb{Q}(\xi, i)$ de $\mathbb{C}$. Equivalentemente, identificaremos los elementos $\lambda + \mu j$ con los elementos del subcampo $\mathbb{Q}(\xi, i)$.

Observe que $(1 + \xi i)(1 - \xi^{-1}i)$ y $(1 + \xi j)(1 - \xi^{-1}j)$ son unidades en $\mathbb{H}(\mathbb{Q}(\xi))$ y

$$\theta((1 + cg)(1 + (cg)^*)e) = (1 + \xi i)(1 - \xi^{-1}i) \quad y,$$

$$\theta((1 + ch)(1 + (ch)^*)e) = (1 + \xi j)(1 - \xi^{-1}j).$$

Luego $(1 + cg)(1 + (cg)^*)e$ y $(1 + ch)(1 + (ch)^*)e$ son unidades en $\mathbb{Q}Ge$ por el isomorfismo. Así $(1+cg)(1+(cg)^*)e+(1-e)$ y $(1+ch)(1+(ch)^*)e+(1-e) \in \mathcal{U}^+(\mathbb{Q}G)$. Por lo tanto, $u = (1 + \xi i)(1 - \xi^{-1}i)$ y $v = (1 + \xi j)(1 - \xi^{-1}j)$ son imagenes bajo el isomorfismo θ de unidades simétricas en $\mathbb{Q}G$. Así, se tiene que $\omega(u, v) = 1$ si $\omega(x, y) = 1$ es una identidad de grupo para $\mathcal{U}^+(\mathbb{Q}G)$.

Considere $\mathbb{H}(\mathbb{Q}(\xi))$ como un $\mathbb{Q}(\xi, i)$-espacio vectorial a derecha con base $\{1, j\}$. Sea $r \mapsto \rho_r$ la representación regular a izquierda en $\mathbb{H}(\mathbb{Q}(\xi))$, es decir, la aplicación donde $\rho_r(s) = rs$ para todo s. Si $\omega(\rho_u, \rho_v) = 1$, entonces la matriz asociada a ρ_u con respecto a la base $\{1, j\}$ es:

$$A = \begin{pmatrix} 2 - (\xi^{-1} - \xi)i & 0 \\ 0 & 2 + (\xi^{-1} - \xi)i \end{pmatrix},$$

y la matriz asociada a la representación ρ_v es:

$$B = \begin{pmatrix} 2 & \xi^{-1} - \xi \\ \xi - \xi^{-1} & 2 \end{pmatrix}.$$

Además,

$$\begin{aligned} det(A - \alpha I_2) &= det\Big(\begin{pmatrix} 2 - (\xi^{-1} - \xi)i & 0 \\ 0 & 2 + (\xi^{-1} - \xi)i \end{pmatrix} - \alpha \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Big) \\ &= det\Big(\begin{pmatrix} -(\xi^{-1} - \xi)i + 2 - \alpha & 0 \\ 0 & (\xi^{-1} - \xi)i + 2 - \alpha \end{pmatrix} \Big) \\ &= [(2 - \alpha) - (\xi^{-1} - \xi)i][(2 - \alpha) + (\xi^{-1} - \xi)i] \\ &= (2 - \alpha)^2 - [(\xi^{-1} - \xi)i]^2 \\ &= (2 - \alpha)^2 + (\xi^{-1} - \xi)^2 = 0, \end{aligned}$$

y

$$\begin{aligned} det(B - \alpha I_2) &= det\Big(\begin{pmatrix} 2 & (\xi^{-1} - \xi) \\ -(\xi^{-1} - \xi) & 2 \end{pmatrix} - \alpha \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Big) \\ &= det\Big(\begin{pmatrix} 2 - \alpha & (\xi^{-1} - \xi) \\ -(\xi^{-1} - \xi) & 2 - \alpha \end{pmatrix} \Big) \\ &= (2 - \alpha)^2 + (\xi^{-1} - \xi)^2 = 0. \end{aligned}$$

Es decir, tanto A como B poseen los mismos valores propios pero con vectores propios diferentes, a saber $(i, 0)$ y $(0, i)$ para A y $(i, -1)$, $(1, i)$, $(i, 1)$ y $(-1, i)$ para B. Luego, por [21, Proposición 2.3.9], se obtiene que para potencias adecuadas de A y B, se genera un grupo libre, contradiciendo la hipótesis que $\omega(u, v) = 1$ satisface una identidad de grupo. □

El siguiente teorema caracteriza las álgebras de grupo semiprimas de grupos de torsión cuyas unidades satisfacen una identidad de grupo.

Teorema 3.2.5. *Suponga que F es un cuerpo infinito de $car(F) = p > 2$. Si G es un grupo de torsión y FG es semiprima entonces $\mathcal{U}^+(FG) \in IG$ si y solo si G es Abeliano o un 2-grupo Hamiltoniano.*

Demostración. Sea $g \in G$ tal que $o(g) = p$, siguiendo la demostración de la Afirmación 1 del caso semiprimo del Teorema 2.3.2, se tiene que $\langle g \rangle \lhd G$. Pero esto contradice que FG sea semiprima (ver Teorema 1.3.12(2b)). Entonces G no contiene p-elementos. Como conclusión del Lema 3.1.5, G es Abeliano o Hamiltoniano. En el caso Hamiltoniano, $G = \mathcal{Q}_8 \times E \times A$, el Lema 3.2.4 implica que $A = \{1\}$. Por tanto, G es un 2-grupo Hamiltoniano.

Recíprocamente, tomando G como 2-grupo Hamiltoniano, por el Lema 3.1.6, se tiene que todos los elementos simétricos conmutan.

Por tanto, si G es Abeliano o 2-grupo Hamiltoniano se concluye que $\mathcal{U}^+(FG)$ conmutan lo que implica que $\mathcal{U}^+(FG)$ satisface una identidad de grupo. □

A continuación tenemos la respuesta afirmativa a la Conjetura de Brian Hartley en el contexto de las álgebras de grupo dotadas de la involución clásica.

Teorema 3.2.6. *Suponga que G es un grupo de torsión y $\mathcal{U}^+(FG)$ satisface una identidad de grupo. Entonces FG satisface una identidad polinomial.*

Demostración. Dividiremos la demostración en tres casos:

1. FG **es semiprima.**

   Por el Teorema 3.2.5, G es Abeliano o 2-grupo Hamiltoniano. En ambos casos los elementos simétricos conmutan, luego FG satisface una identidad polinomial.

2. $\eta(FG)$ **es nilpotente diferente de cero.**

   Por la Afirmación 2 en la demostración del Teorema 2.3.2, $\Phi_p(G)$ es un grupo normal. Además, $\Phi_p(G)$ resulta ser finito, [27, Teorema 8.1.12]. Así, por Lema 3.2.1, $\mathcal{U}^+(F(G/\Phi_p(G)))$ satisface una identidad de grupo. Usando la Afirmación

8b. en la demostración del Teorema 2.3.2, $\Phi(G/\Phi_p(G))$ es un p'-grupo. Del Teorema 1.3.12($2b$), $F(G/\Phi_p(G))$ es semiprima. Luego, por el Teorema 3.2.5, $G/\Phi_p(G)$ es Abeliano o 2-grupo Hamiltoniano.

Si $G/\Phi_p(G)$ es Abeliano, entonces $F(G/\Phi_p(G))$ es conmutativo y por el epimorfismo canónico $FG/\Delta(G,\Phi_p(G))$ también lo será. Note que para todo $x, y \in FG$,

$$[\overline{x},\overline{y}] = \overline{0}$$

$$[x\Delta(G,\Phi_p(G)), y\Delta(G,\Phi_p(G))] = \overline{0}$$

$$xy\Delta(G,\Phi_p(G)) = yx\Delta(G,\Phi_p(G))$$

$$(xy - yx)\Delta(G,\Phi_p(G)) = \overline{0}$$

$$[x,y] \in \Delta(G,\Phi_p(G))$$

Por lo tanto, $[FG, FG] \subseteq \Delta(G,\Phi_p(G))$. Como $\Phi_p(G) \trianglelefteq G$ p-grupo finito entonces $\Delta(G/\Phi_p(G))$ es nilpotente (ver Corolario 1.3.8). Luego, FG satisface $[x,y]^{p^l} = 0$ para algún $l \in \mathbb{N}$.

Supongamos ahora que G/Φ_p un 2-grupo Hamiltoniano, entonces por el Lema 3.1.6, los elementos simétricos en $F[G/\Phi_p(G)]^+$ conmutan. Por un argumento similar al planteado para el caso anterior donde G era un grupo Abeliano, $[(FG)^+, (FG)^+] \subseteq \Delta(G,\Phi_p(G))$ para todo $x, y \in FG^+$. Así, FG satisface una $*$-identidad polinomial $(x + x^*, y + y^*)^{p^l} = 0$. Pero por el clásico Teorema de Amitsur 1.6.3, FG satisface una identidad polinomial.

3. $\eta(FG)$ **es nil no nilpotente.**

Por el Lema 3.1.7, η satisface una identidad polinomial, y como consecuencia del Lema 1.6.7, FG satisface una identidad polinomial generalizada no degenerada. Entonces, $[G : \Phi(G)] < \infty$ y $|\Phi(G)'| < \infty$ (ver Proposición 1.6.6) y por la Afirmación 10 en la demostración del Teorema 2.3.2, se tiene que G es localmente finito. Tomando los subgrupos finitos de G, se sabe que sus p-elementos forman un subgrupo normal P (ver Teorema 3.2.3).

Por el Lema 3.2.1, $\mathcal{U}^+(F(G/P)) \in IG$. Como $F(G/P)$ es semiprimo, se tiene por el Teorema 3.2.5 que G/P es Abeliano o 2-grupo Hamiltoniano. De ser Abeliano, G' es un p-grupo, por el Teorema 1.1.3(3), por tanto $(\Phi(G))'$ es un p-grupo finito. Así, FG satisface una identidad polinomial ya que G contine un p-grupo Abeliano de índice finito (ver Proposición 1.6.5). Ahora, si $G/P \cong \mathcal{Q}_8 \times E$, es un 2-grupo, entonces existe un subgrupo normal H de G, conteniendo a P, tal que $G/H \cong \mathcal{Q}_8$ y $H/P \cong E$. Luego H/P es Abeliano y como se vió anteriormente, FH satisface una identidad polinomial. Es decir, H contiene un p-grupo Abeliano de índice finito que también esta en G. Por lo tanto, FG satisface una identidad polinomial.

□

Ahora bien, si $\mathcal{U}^+(FG)$ satisface un identidad de grupo entonces FG satisface una identidad polinimial. Por tanto, G contiene un subgrupo p-Abeliano de índice finito Proposición 1.6.5, y así,

Corolario 3.2.7. *Suponga que G es un grupo de torsión. Si $\mathcal{U}^+(FG)$ satisface una identidad de grupo entonces G es localmente finito.*

La caracterización de grupos de torsión G tal que $\mathcal{U}^+(FG) \in IG$ esta completa. En el caso $car(F) = 0$, FG es semiprima. Luego se trabajará con $car(F) = p > 2$ y G un grupo de torsión. Esta clasificación depende de la presencia o no del grupo cuaternio $\mathcal{Q}_8$.

Teorema 3.2.8. *Sea FG un álgebra de grupo de un grupo de torsión G sobre un cuerpo infinito F dotado de la involución clásica.*

1. *Si $car(F) = 0$, $\mathcal{U}^+(FG) \in IG$ si y solo si G es un grupo Abeliano o G es un 2-grupo Hamiltoniano,*

2. *Si $car(F) = p > 2$, entonces $\mathcal{U}^+(FG) \in IG$ si y solo si $FG \in IP$ y vale solo una de las siguientes:*

   (i) Si $\mathcal{Q}_8 \nsubseteq G$, G' es de exponente acotado p^k, para algún $k \geq 0$.

(ii) Si $\mathcal{Q}_8 \subseteq G$, $\mathcal{U}^+(FG) \in IG$ *si y solo si*

(a) Los p-elementos de G *forman un subgrupo (normal)* P *de* G *y* G/P *es un* 2*-grupo Hamiltoniano,*

(b) G *es de exponente acotado* $4p^s$*, para algún* $s \geq 0$*.*

Una buena referencia donde se puede encontrar la demostración del teorema es [21, Teorema 2.4.8] para el caso en que G no contiene a $\mathcal{Q}_8$ y [21, Teorema 2.4.9] en caso contrario.

Conclusiones

Aunque a lo largo del presente escrito se evidencian pruebas detalladas en la mayoría de los resultados, cumpliendo así con el objetivo del presente trabajo, queremos destacar los siguientes resultados debido a la importancia que tuvieron durante el estudio de las identidades de grupo en unidades y unidades simétricas e identidades polinomiales en FG.

- En el Teorema 1.1.6 se presenta todos los detalles en la demostración de la caracterización de los grupos Hamiltonianos.

- En virtud del Teorema 1.3.12 se conoce que FG es semiprima cuando FG es de característica cero o cuando $\eta(FG) = (0)$. Además, en FG también existen ideales nilpotentes no nulos e ideales nil pero no nilpotentes (ver Ejemplo 1.1.14). Es por ello que la demostración de la respuesta afirmativa a la Conjetura 2.1.1 está dividida en estos tres casos.

- Mostrar que $\Phi_p(G)$ es un subgrupo normal de G fue crucial para el caso en que $\eta(FG)$ es nilpotente no nulo, en la respuesta afirmativa a la Conjetura 2.1.1, tanto para las unidades como para la unidades simétricas.

- Usando [21, Lema 1.1.2], se estableció la demostración del Teorema 2.3.5 reduciendo la identidad $\omega(x_1, x_2, \ldots, x_n) = 1$ a la identidad en dos variables $\omega(x_1, x_2) = 1$.

- Apesar de que autores como G. Lee en [21] y Giambruno, Sehgal y Valenti en [12] y [13] asumen que G es localmente finito bajo las hipótesis de la Conjetura,

encontramos que lo verdaderamente importante era tener que $\Phi(G)$ es localmente finito (ver Teorema 2.3.5. Afirmación 10), ya que con $[G : \Phi(G)] < \infty$ y el Teorema de Schmidt [30, Teorema 14.3.1], es claro que G será localmente finito.

- Todos los resultado mencionados anteriormente también fueron muy útiles en la prueba de la respuesta afirmativa a la Conjetura de Brian Hartley en la versión de las unidades simétricas.

- En el estudio de la unidades simétricas solo se trabajó bajo la involución clásica. Sin embargo, se podría estudiar este conjunto bajo otras involuciones, como objetivo de futuros trabajos.

Bibliografía

[1] S. A. Amitsur: Identities in rings with involution, Israel J. Math. 7 (1968): 63-68.

[2] M. F. Atiyah, I.G. Macdonald. Introduction to conmutative algebra. Addison-Wesley Publishing Company, Inc., Massachusetts. (1980).

[3] O. Broche Cristo. Commutativity of symmetric elements in group rings. J. Group Theory 9 (2006): 673-683.

[4] O. Broche Cristo, E. Jespers, C. Polcino Milies and M. Ruiz Marín. Antisymmetric elements in group rings II. J. Algebra Appl. 8 (2009): 115-127.

[5] O. Broche Cristo and C. Polcino Milies. Symmetric elements under oriented involutions in group rings. Comm. Algebra 34 (2006): 3347-3356.

[6] J. H. Castillo Gómez and C. Polcino Milies. Lie properties of symmetric elements under oriented involutions. Commun. Algebra 40 (2012): 4404-4419.

[7] A. Dooms and M. Ruiz. Symmetric units satisfying a group identity. J. Algebra 308 (2007): 742-750.

[8] A. Giambruno, E. Jespers and A. Valenti: Group identities on units of rings, Arch. Math. (Basel) 63 (1994): 291-296.

[9] A. Giambruno, C. Polcino Milies and S. K. Sehgal. Lie properties of symmetric elements in group rings. J. Algebra 321 (2009): 890-902.

[10] A. Giambruno, C. Polcino Milies and S. K. Sehgal. Group identities on symmetric units. J. Algebra 322 (2009): 2801-2815.

[11] A. Giambruno and S. K. Sehgal. Lie nilpotence of group rings. Comm. Algebra 21 (1993): 4253-4261.

[12] A. Giambruno, S. K. Sehgal, A. Valenti: Group algebras whose units satisfy a group identity, Proc. Amer. Math. Soc. 125 (1997): 629-634.

[13] A. Giambruno, S. K. Sehgal and A. Valenti. Symmetric units and group identities. Manuscripta Math. 96 (1998): 443-461.

[14] J. Z. Gonçalves and A. Mandel: Semigroup identities on units of group algebras, Arch. Math. (Basel) 57 (1991): 539-545.

[15] E. G. Goodaire, E. Jespers and C. Polcino Milies. Alternative loop rings. North-Holland, Amsterdam. (1996).

[16] E. G. Goodaire and C. Polcino Milies. Oriented involutions, symmetric and skew-symmetric elements in group rings. (2011). Preprint. arXiv:1108.4648v1 [math.GR].

[17] I. N. Herstein. Rings with involution. University of Chicago Press, Chicago (1976).

[18] A. Holguín Villa. Involuções de grupo orientadas em algebras de grupo, Tese de Doutorado, Universidade de São Paulo (2013). São Paulo, Brasil.

[19] E. Jespers and M. Ruiz Marín. On symmetric elements and symmetric units in group rings. Comm. Algebra 34 (2006): 727-736.

[20] T. Y. Lam. Afirst course in non-comutative rings. Springer Verlag, New York (1991).

[21] G. T. Lee. Group Identities on Units and Symmetric Units of Group Rings. Springer-Verlag, London (2010).

[22] G. T. Lee, S. K. Sehgal and E. Spinelli. Lie properties of symmetric elements in group rings II. J. Pure Appl. Algebra 213 (2009): 1173-1178.

[23] C. H. Liu: Group algebras with units satisfying a group identity, Proc. Amer. Math. Soc. 127 (1999): 327-336.

[24] C. H. Liu, D. S. Passman: Group algebras with units satisfying a group identity II, Proc. Amer. Math. Soc. 127 (1999): 337-341.

[25] P. Menal: Private letter to B. Hartley, April 6, (1981).

[26] E. Noether, Nichtkommutative Algebra, Math. Z. 37 (1933): 513-541.

[27] D. S. Passman. The algebraic structure of group rings. Wiley, New York (1977).

[28] D. S. Passman: Group algebras whose units satisfy a group identity II, Proc. Amer. Math. Soc. 125 (1997): 657-662.

[29] C. Polcino Milies and S. K. Sehgal. A Course in Group Rings. Kluwer, Dordrecht (2002).

[30] D. J. S. Robinson: A course in the theory of groups. Springer Verlag, New York (1995).

[31] S. K. Sehgal. Topics in Group Rings. Marcel Dekker, New York, (1978).

[32] D. S. Warhurst: Topics in group rings, Ph. D. Thesis, Manchester, (1981).